Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Нігловського Олександра Олександровича

на здобуття ступеня вищої освіти Бакалавра

Система захисту інформації комерційного офісного приміщення

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

Шифр КРБКБ.2102159.21.02.37 ПЗ

Виконав студент 4 курсу група КБ-21-2 Олександр НІГЛОВСЬКИЙ

Керівник кандидат технічних наук, доцент Віктор ЧЕШУН

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

11 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
15 лютого 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Нігловський Олександр Олександрович

1 Тема роботи Система захисту інформації комерційного офісного приміщення

Керівник роботи канд. техн. наук, доцент Віктор ЧЕШУН

Затверджено наказом ректора університету від 07 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 02.06.2025

3 Проаналізувати предметну область теми кваліфікаційної роботи. Вивчити загрози інформаційної безпеки для малих комерційних підприємств. Дослідити специфіку інформаційного функціонування офісів, які займаються розробкою цифрового контенту. Ознайомитися з державними та міжнародними нормативними документами щодо захисту інформації. Провести аналіз інформаційних потоків у структурі компанії ArcadiaWorks. Побудувати моделі загроз та порушника, які притаманні типовому офісу невеликої ІТ-компанії. Виявити основні вразливості у безпековій інфраструктурі приміщення. Спроєктувати систему захисту інформації, провести її імплементацію, апробацію та оцінку ефективності. Розробити настанови щодо впровадження та експлуатації системи захисту інформації. Оцінити ресурси, необхідні для реалізації системи захисту.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз предметної області та дослідження чинних нормативних документів. Аналіз типових загроз та методів протидії інформаційним витокам у малому бізнесі. Аналіз інформаційних потоків в ІТ-компанії. Визначення основних вразливостей та проблем інформаційної безпеки. Побудова моделі загроз та моделі порушника інформаційної системи. Проєктування системи захисту інформації. Імплементація системи на експериментальному об'єкті. Оцінка ефективності та ресурсів проєкту. Розробка рекомендацій щодо впровадження та експлуатації. Висновки

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Схема інформаційних потоків компанії ArcadiaWorks. Ієрархічна структура приміщення. Схема комунікаційної мережі офісу (створена в Cisco Packet Tracer). Таблиця класифікації корпоративної інформації. Таблиці аналізу вразливостей та недоліків безпекової інфраструктури. Модель загроз для офісу. Модель типового порушника. Архітектура запропонованої системи захисту. Політика безпеки паролів. Схеми резервного копіювання даних. Налаштування обмежень доступу в середовищі ОС Windows. Діаграми оцінки ресурсів для впровадження системи. Скріншоти результатів апробації системи захисту. Рекомендації щодо експлуатації системи..

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

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

Студент Олександр НІГЛОВСЬКИЙ

Керівник кваліфікаційної роботи Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту інформації комерційного офісного приміщення.

Автор роботи: Нігловський Олександр Олександрович.

Керівник роботи: Чешун Віктор Миколайович

Пояснювальна записка: 95 с., 2 додатків, 20 рисунків, 16 таблиці, 43 джерел.

Графічна частина: 12 плакатів.

ЗАХИСТ ІНФОРМАЦІЇ, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЗАХИСТ КОМЕРЦІЙНОГО ПРИМІЩЕННЯ, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ КОМЕРЦІЙНОГО ОФІСНОГО ПРИМІЩЕННЯ.

Кваліфікаційна робота присвячена розробці системи захисту інформації для офісного приміщення IT-компанії ArcadiaWorks, яка спеціалізується на створенні цифрових ігор. У роботі проведено аналіз предметної області, досліджено типові загрози інформаційної безпеки, особливості функціонування інформаційних потоків та типові вразливості офісної IT-структури.

Розроблено модель загроз і модель порушника для конкретного середовища, а також спроєктовано комплексну систему захисту з урахуванням обмежених ресурсів приміщення. Система включає організаційні, технічні та програмні заходи безпеки.

Проведено впровадження на тестовому майданчику, оцінено ефективність запропонованих рішень та підготовлено настанови щодо експлуатації. Результати роботи мають практичне значення для захисту даних малих комерційних структур в IT-сфері.

06.06.2025 _____

ABSTRACT

Subject of qualification work: Information protection system for a commercial office space.

Author: Nihlovskiy Oleksandr Oleksandrovich.

Head of work: Cheshun Viktor Mykolayovych.

Explanatory note: 95 p, 2 appendices, 20 figures, 17 tables, 43 sources

Graphic part: 12 posters.

INFORMATION PROTECTION, INFORMATION PROTECTION SYSTEM, PROTECTION OF A COMMERCIAL ENTERPRISE, INFORMATION PROTECTION SYSTEM OF A SMALL COMMERCIAL OFFICE ENTERPRISE.

The bachelor's qualification work focuses on the development of an information security system for a small IT company, ArcadiaWorks, engaged in digital game development. The work analyzes the domain area, identifies typical threats to information infrastructure, and examines the specifics of internal data flows and vulnerabilities in a small office environment.

A threat model and an intruder model tailored to the selected environment were developed. Based on this, a comprehensive protection system was designed, incorporating organizational, technical, and software-based security measures suitable for enterprises with limited resources.

The system was implemented in a test environment, evaluated for effectiveness, and accompanied by usage guidelines. The results have practical value for small commercial IT companies aiming to secure their information assets against internal and external threats.

06.06.2025 _____

ЗМІСТ

ВСТУП

У сучасному цифровому середовищі інформація є критично важливим ресурсом для стабільної роботи будь-якого приміщення. Зі зростанням кількості кіберзагроз питання інформаційної безпеки стає особливо актуальним для бізнесу, який часто має обмежені ресурси. Ефективна система захисту інформації повинна поєднувати організаційні, технічні та правові заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності даних.

До ключових компонентів системи належать політики безпеки, контроль доступу, шифрування, антивірусний захист, системи виявлення загроз, а також навчання персоналу. В умовах обмежених бюджетів малим компаніям доцільно впроваджувати прості й доступні рішення, зокрема хмарні сервіси, багатофакторну автентифікацію, резервне копіювання тощо.

Сучасні виклики вимагають активного моніторингу, аналізу ризиків та швидкого реагування на інциденти. Надійна система захисту дозволяє мінімізувати наслідки атак, підтримувати безперервність бізнесу та відповідати нормативним вимогам. Таким чином, впровадження комплексної системи захисту інформації є важливою умовою безпечної та ефективної діяльності приміщення. Об'єктом дослідження є приватна IT-компанія ArcadiaWorks, яка займається розробкою комп'ютерних ігор для ПК, мобільних платформ та консолей. У своїй діяльності вона використовує ігрові рушії Unity та Unreal Engine, а також інструменти 3D/2D-моделювання: Autodesk Maya, Blender і Adobe Photoshop. Для спільної роботи та управління проєктами застосовуються Git, Slack, Trello та Google Диск.

Метою роботи є проєктувати систему захисту інформації комерційного приміщення, розробити настонови що до в провадження та експлуатації даної системи на прикладі офісу конкретної айті компанії.

Для досягнення поставленої мети необхідно виконати такі завдання:

– проаналізувати предметну область теми кваліфікаційної роботи;

– проаналізувати типові загрози інформаційній інфраструктурі малих комерційних офісних підприємств та методи протидії їм;

– дослідити державні нормативні документи та кращі міжнародні практики побудови та впровадження систем захисту інформації;

– провести аналіз специфіки інформаційного функціонування малих комерційних підприємств;

– дослідити типові інформаційні потоки комерційного приміщення;

– побудувати модель загроз комерційного приміщення;

– побудувати модель порушника комерційного приміщення;

– спрєктувати систему захисту інформації комерційного приміщення;

– впровадити та апробувати спроєктовані рішення;

– розробити настанови щодо впровадження та експлуатації системи захисту інформації.

За темою кваліфікаційної роботи було опубліковано тези конференції, що містять ключові результати дослідження та важливі висновки, зроблені автором. У публікації також описуються методологічні підходи та інноваційні рішення, представлені на конференції, що підкреслюють наукову значущість та практичну цінність виконаної роботи.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ДОСЛІДЖЕННЯ ІСНУЮЧИХ НАСТАНОВ, НОРМАТАВНИХ ДОКУМЕНТІВ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

1.1 Аналіз типових загроз та методів комплексної протидії їм

Розпочнемо роботу з аналізу загроз, які можуть вплинути на інформаційну безпеку організацій. Сучасні приміщення стикаються з широким спектром ризиків, що можуть призвести до порушення роботи бізнес-процесів, витоку даних, фінансових та репутаційних втрат. Загрози інформаційній безпеці поділяються на технічні, фізичні та організаційні. Технічні пов’язані з атаками на програмне чи апаратне забезпечення — це віруси, зломи, фішинг, вразливості систем. Фізичні загрози включають крадіжку обладнання, пожежі чи інші пошкодження інфраструктури. Організаційні виникають через людський фактор: недотримання політик, помилки персоналу або відсутність контролю доступу [1,2].

Забезпечення системи захисту інформації є ключовим фактором для мінімізації цих загроз та захисту інформаційних активів організації. Також ми розглянемо такі класифікації як: цілісність, доступність і конфіденційність. Конфіденційність: загрози включають несанкціонований доступ до даних, шпигунство, крадіжку інформації та викрадення особистих даних. Цілісність: пошкодження або неналежна зміна даних через шкідливе програмне забезпечення, помилки програмування або злочинну діяльність. Доступність: атаки, такі як DDoS, технічні збої та фізичні пошкодження серверів, які можуть призвести до недоступності критично важливих систем та інформації [3].

Як наведено на рисунку 1.1, загрози для інформаційного простору компанії можуть виникати з різних напрямів, які охоплюють як технічні, так і організаційні складові.

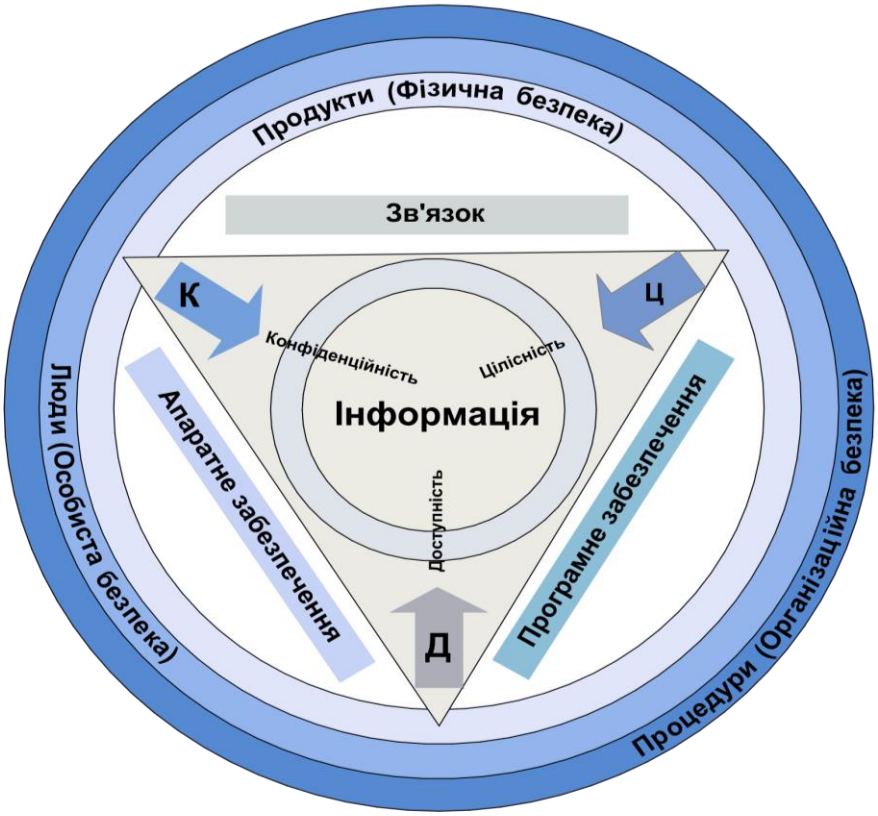


Рисунок.1.1 – Модель забезпечення інформаційної безпеки

Технічні загрози включають атаки шкідливого програмного забезпечення, серед яких віруси, трояни, шпигунські програми, програмне забезпечення для вимагання (ransomware). Ці загрози можуть блокувати доступ до даних, красти конфіденційну інформацію або завдавати шкоди IT-інфраструктурі. Окремо слід виділити фішингові атаки, які використовують соціальну інженерію для отримання логінів і паролів користувачів [4].

Для забезпечення захисту від несанкціонованого доступу необхідно реалізовувати заходи з контролю доступу, шифрування даних та моніторингу активності в інформаційних системах. Зокрема, використання багаторівневої системи аутентифікації, мережевих екранів та систем виявлення вторгнень допомагає значно знизити ризики. Також рекомендується застосування криптографічного захисту інформації для забезпечення конфіденційності даних.

Дедалі частіше зустрічаються атаки на мережеву інфраструктуру, такі як перехоплення трафіку, атаки типу «людина посередині», розподілені атаки відмови в обслуговуванні. Використання застарілого програмного забезпечення

створює додаткові ризики, оскільки вразливості, знайдені в старих версіях, можуть бути використані зловмисниками. Для захисту інформаційних систем важливо проводити регулярне оновлення програмного забезпечення та застосовувати контрольні заходи для зменшення ймовірності кібератак [5,6].

Фізичні загрози включають ризики, пов’язані з безпосереднім доступом до приміщень і обладнання. Однією з основних загроз є несанкціонований фізичний доступ до приміщень, що може стати причиною викрадення інформації або обладнання. Відсутність охорони, відеоспостереження та систем контролю доступу підвищує ризик проникнення зловмисників [7].

Забезпечення фізичного захисту передбачає необхідність застосування заходів, таких як обмеження доступу до серверних кімнат, встановлення систем ідентифікації та автентифікації користувачів, а також використання спеціалізованих засобів сигналізації та відеоспостереження. Особливу увагу слід приділяти запобіганню витоку інформації через побічні електромагнітні випромінювання.

Фізичне втручання у комунікаційне обладнання, зокрема встановлення шпигунських пристроїв, може призвести до перехоплення даних. Не слід також нехтувати загрозами, пов’язаними з пожежами або стихійними лихами, які можуть знищити важливі інформаційні ресурси, якщо не передбачено належних заходів резервного копіювання та аварійного відновлення [8].

Організаційні загрози стосуються недостатньої кваліфікації персоналу, відсутності чітких політик безпеки, соціальної інженерії та недостатнього контролю за інформаційними системами. Однією з основних проблем є брак обізнаності співробітників у сфері інформаційної безпеки, що призводить до відкриття шкідливих електронних листів, використання ненадійних паролів, передачі критичної інформації стороннім особам. Відсутність чітких політик безпеки та регламентів роботи з конфіденційними даними також є серйозною загрозою.

Для зменшення ризиків необхідно впроваджувати систему захисту інформації, що включає регулярне навчання персоналу, розробку правил доступу

до інформаційних систем та заходи з моніторингу безпеки. Також передбачено проведення планових аудитів безпеки, що дозволяють виявляти можливі вразливості до їх експлуатації зловмисниками [9].

Також важливим аспектом є проведення регулярних аудитів безпеки, без яких можуть залишатися приховані вразливості в системах. Відсутність механізмів резервного копіювання може призвести до втрати критичних даних у випадку атаки чи збоїв. Недотримання нормативних вимог щодо захисту інформації може викликати штрафні санкції та погіршення репутації компанії.

Методи комплексної протидії загрозам:

- використання сучасного антивірусного програмного забезпечення;
- впровадження багатофакторної аутентифікації;
- захист мережевої інфраструктури за допомогою міжмережевих екранів (фаєрволів);
- обмеження фізичного доступу до критичних систем;
- навчання персоналу правилам кібербезпеки;
- впровадження політик управління доступом та проведення аудитів безпеки;
- використання резервного копіювання даних та його регулярне тестування;
- зашифровані канали зв’язку для передачі конфіденційної інформації [10].

Впровадження системи захисту інформації вимагає системного підходу, що включає як технологічні рішення, так і організаційні заходи. Такий підхід дозволяє створити надійний рівень безпеки, що мінімізує можливість порушення цілісності, доступності та конфіденційності даних. У результаті організація може забезпечити стабільність своїх бізнес-процесів, підвищити довіру клієнтів та уникнути значних фінансових втрат, пов’язаних із кібератаками або іншими інцидентами.

Також ми розглядаємо загрози в різних класифікаціях а саме конфіденційність, цілісність і доступність

– загрози конфіденційності спрямовані на несанкціонований доступ до інформації: перехоплення даних під час передавання (через мережу), шпигунське програмне забезпечення, несанкціонований доступ до баз даних, витік паролів або облікових записів;

– загрози цілісності спричиняють зміну, пошкодження або знищення інформації: віруси та шкідливі програми, що змінюють файли, несанкціоноване редагування даних ,збої програмного забезпечення, атаки типу "man-in-the-middle";

– загрози доступності унеможливлюють або обмежують доступ до інформації чи систем: атаки типу ddos, збої електроживлення, фізичне знищення серверів, програмні помилки, що виводять систему з ладу [11].

1.2 Дослідження державних нормативних документів та міжнародних практик побудови та впровадження системи захисту інформації

Операючися на інформацію сказану в розділі вище можемо почати дослідження державних нормативних документів та міжнародних практик побудови та впровадження системи захисту інформації.

У сучасному бізнес-середовищі, де інформаційні технології відіграють ключову роль, захист інформації стає невід'ємною частиною управління будь-якою організацією, включаючи малі комерційні приміщення. Дослідження державних нормативних документів та міжнародних практик допомагає забезпечити надійний захист інформації, який відповідає сучасним викликам та загрозам. В Україні законодавство вимагає дотримання певних стандартів захисту інформації. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про захист персональних даних» встановлюють правову основу для побудови системи захиту інформації.

Закон України «Про інформацію»: Цей закон визначає основні принципи інформаційної діяльності, права та обов'язки суб'єктів інформаційних відносин, а також встановлює вимоги до захисту інформації [12].

Закон України «Про захист персональних даних»: Цей закон регулює обробку персональних даних, встановлює права суб'єктів персональних даних та обов'язки володільців і розпорядників таких даних [13].

Окрім законів та нормативних документів кібербезпека на рівні держави керується стратегією кібербезпеки визначеною на 2021-2025 роки. Це документ який прийнятий і затверджена Указом Президента України від 26 серпня 2021 року, він визначає ключові напрямки, цілі та завдання для забезпечення захисту кіберпростору. Її мета – створити безпечні умови для використання цифрових технологій в інтересах громадян, суспільства та держави [14].

Кібербезпека є одним із пріоритетних напрямків національної безпеки України. Для її зміцнення передбачено розвиток національної системи кіберзахисту, що дозволить ефективно протидіяти сучасним кіберзагрозам.

В свою чергу було взято за основу державні нормативні документи Служби бкзпеки України що без посередньо повязані із тематикою характером робіт що необхідно виконати в рамках даної кваліфікаційної роботи. Вони визначають основні принципи захисту інформації та встановлюють механізми контролю та відповідальності, що особливо важливо для малих комерційних приміщень, де ресурси можуть бути обмеженими.

Один з основних нормативних документів який я використовував є НД ТЗІ 3.7-003 -2005 яки свідчить про порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Цей документ визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-телекомунікаційних системах (ІТС). Він встановлює правила прийняття рішень щодо складу системи захисту інформації, визначення обсягу і змісту робіт, етапів та завдань кожного етапу.

Документ застосовується тільки до ІТС, де інформація обробляється автоматизовано, і систематизує вимоги з чинних нормативних документів. Він

містить перелік робіт та посилання на нормативні документи, а також короткий опис робіт та очікувані результати, якщо деякі етапи не нормовано.

Документ призначений для суб'єктів інформаційних відносин, таких як власники ІТС, користувачі, розробники систем захисту, постачальники компонентів ІТС та оцінювачі захищеності інформації [15].

Встановлений порядок обов'язковий для всіх суб'єктів системи ТЗІ в Україні, де обробляється інформація, яка належить до державних ресурсів або потребує захисту за законодавством. Для інших видів інформації, вимоги документа можуть використовуватись як рекомендації.

Використовува я також НД ТЗІ 2.5-004-99 - це нормативний документ системи технічного захисту інформації, який встановлює критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Цей документ був затверджений Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України у 1999 році.

Основні положення НД ТЗІ 2.5-004-99 включають:

- критерії конфіденційності: визначають вимоги до захисту інформації від несанкціонованого доступу та розголошення;
- критерії цілісності: забезпечують захист інформації від несанкціонованої модифікації або знищення;
- критерії доступності: гарантують, що інформація доступна уповноваженим користувачам тоді, коли вони її потребують.

Документ також містить методичні рекомендації щодо оцінки ефективності захисту інформації та визначення загроз безпеці інформації в автоматизованих системах. Він є важливим інструментом для забезпечення високого рівня захисту інформації в інформаційно-телекомунікаційних системах України [16].

На рахунок міжнародних практик можна виділити такі стандарти як ISO/IEC 27001, ISO/IEC 27002.

ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою, розроблений ISO та IEC. Він встановлює вимоги до створення,

впровадження та вдосконалення системи управління інформаційною безпекою, допомагаючи організаціям захищати інформаційні активи.

Основними положеннями ISO/IEC 27001 є: аналіз ризиків інформаційної безпеки (загрози, вразливості, впливи); впровадження заходів для управління ризиками; постійний моніторинг і вдосконалення системи управління інформаційною безпекою [17].

ISO/IEC 27002 – міжнародний стандарт, що містить рекомендації з управління інформаційною безпекою. Він доповнює ISO/IEC 27001, надаючи найкращі практики з контролю доступу, криптографії, безпеки персоналу та реагування на інциденти.

Основними положеннями ISO/IEC 27002 є: детальні рекомендації з інформаційної безпеки; впровадження заходів для захисту інформаційних активів; підвищення довіри серед зацікавлених сторін [18].

Згідно з НД ТЗІ 3.7-003 -2005 при побудові системи захисту інформації передбачено такі етапи:

Підготовчий етап включає, аналіз поточного стану інформаційної безпеки, оцінка ризиків та визначення потенційних загроз. Формується концепція кіберзахисту та загальні вимоги до майбутніх заходів.

– розробка та впровадження включає, створення нормативних актів, політики безпеки та технічні рішення, впровадження сучасної системи захисту, навчається персонал, організовуються центри моніторингу та реагування;

– моніторинг і контроль в цьому етапі, запускаються системи постійного нагляду за кіберпростором, аналізується безпека інформаційних ресурсів, відстежуються загрози та оцінюється ефективність захисних заходів;

– реагування на інциденти цей етап передбачає оперативне виявлення атак, аналіз їх наслідків, нейтралізація загроз і відновлення безпечного функціонування систем. взаємодія з відповідними службами та організаціями;

– удосконалення та адаптація це етеп в якому проводиться аналіз попередніх кіберінцидентів, оновлення стратегій безпеки та впровадження нових технологій захисту. проведення тренінгів і вдосконалення механізмів реагування.

1.3 Аналіз специфіки інформаційного функціонування малих комерційних підприємств

При створенні комплексу системи захисту інформації відповідно до нормативних документів з технічного захисту інформації можуть бути застосовані певні етапи та підходи.

Якщо приміщення не використовує гриф для службового користування і в ньому не обробляється державна таємниця, то перед ним не висуваються вимоги щодо повної відповідності всіх документів.

Однак можуть бути винятки. Якщо Приміщення працює з державними замовленнями або належить до сектору безпеки й оборони, його система захисту потребуватиме індивідуального дослідження та суворої відповідності нормативним документам. У такому випадку необхідно враховувати додаткові вимоги щодо захисту інформації [19].

Проте в цьому аналізі не розглядаються такі специфічні випадки, оскільки типовими є малі комерційні приміщення, які не пов’язані із зазначеними сферами діяльності.

Також ми розглянемо основні характеристики такого приміщення:

Обмежені ресурси. Малі приміщення зазвичай мають обмежені фінансові, людські та технічні ресурси. Це впливає на можливості впровадження складних інформаційних систем та їх захисту. Гнучкість. Малі приміщення швидко адаптуються до змін ринку та нових технологій. Вони можуть легко впроваджувати інноваційні рішення, що підвищує їхню конкурентоспроможність [20].

Високий рівень довіри. У малих приміщеннях взаємодія між співробітниками часто базується на високому рівні довіри, що зменшує потребу в складних системах контролю доступу, але водночас може створювати ризики для безпеки інформації [21].

Відносно встановленої раніше класифікації малі комерційні приміщення: можуть стати обєктом для наступних видів загроз:

Інформаційна загроза є однією з основних, вона представляє – несанкціонований доступ до даних, який може відбуватися через хакерські атаки, внутрішній витік інформації або випадкові дії персоналу. Використання ненадійних каналів зв’язку або незахищених пристроїв також може призвести до втрати важливої інформації. У 2022 році в Україні було зафіксовано випадок, коли особа за допомогою шкідливого програмного забезпечення здійснила несанкціонований доступ до електронної пошти іншої особи, отримавши її персональні дані, і таких випадків є безліч і щоб протидіяти їм потрібно використовувати сучасне ПЗ, шифрувати передачу даних, обмежувати доступ, регулярно оновлюватии резервні копії та навчати персонал кібербезпеці [22].

Загроза, пов'язана із конфіденційністю, виникає через недостатній захист персональних даних, що дозволяє хакерам отримувати доступ до фінансової інформації, використовувати фішингові атаки чи скористатися зламом корпоративної пошти, а також через можливий витік інформації з боку невдоволених співробітників [23]. У Києві невелика рекламна компанія стала жертвою фішингової атаки: хакери отримали доступ до її фінансових даних через фальшивий сайт, що призвело до значних фінансових втрат. Загрозу конфіденційності можна зменшити, використовуючи надійне ПЗ, шифруючи дані, обмежуючи доступ, впроваджуючи двофакторну автентифікацію, проводячи навчання персоналу та створюючи резервні копії.

Небезпека з боку цілісності полягає в навмисній або випадковій зміні критично важливих даних. Наприклад, зловмисники можуть змінювати бухгалтерські звіти, прайс-листи або бази даних клієнтів. Віруси, шкідливе ПЗ або неправильне налаштування програмного забезпечення можуть пошкоджувати або змінювати дані без можливості їх відновлення. Для захисту цілісності даних використовуйте резервне копіювання, надійне ПЗ, контроль доступу, антивіруси та регулярні перевірки системи [24].

Проблеми доступності виникають через DDoS-атаки, вірусне блокування файлів або фізичні поломки серверного обладнання, що робить бізнес недоступним для клієнтів. Відсутність резервного копіювання даних може

призвести до втрати інформації, що паралізує діяльність компанії [25]. У листопаді 2024 року чотири українські місцеві медіа зазнали DDoS-атак та фішингових спроб, що призвело до тимчасової недоступності їхніх вебсайтів для читачів. Щоб боротися з проблемами доступності, використовуйте резервне копіювання, антивірусне ПЗ, захищені сервери, моніторинг трафіку та плани відновлення після інцидентів [26].

Комунікаційні загрози включають перехоплення електронних листів, телефонних дзвінків або повідомлень у месенджерах. Фішингові атаки можуть спричинити розголошення корпоративних паролів або фінансової інформації. Недостатня захищеність Wi-Fi-мереж також може стати лазівкою для зловмисників [27]. У жовтні 2024 року CERT-UA зафіксувала фішингові атаки на бухгалтерів українських підприємств. Зловмисники розсилали підроблені листи від Державної податкової служби, намагаючись викрасти конфіденційну інформацію або заразити системи шкідливим ПЗ. Для захисту від комунікаційних загроз потрібно використовувати шифрування, захищений Wi-Fi, фільтри фішингових атак, антивірусне ПЗ та навчайте персонал кібербезпеці [28].

Апаратне забезпечення також може стати джерелом загроз. Фізична крадіжка комп’ютерів, серверів або жорстких дисків може призвести до втрати важливих даних. Використання несправного обладнання або незахищених USB-носіїв може спричинити збої в роботі систем і витоки інформації. У 2021 році інженер-програміст компанії «Епіцентр К» викрав 24 комп'ютери з робочого місця, продавав їх за заниженою ціною, а отримані кошти витрачав на онлайн-казино. Для захисту обладнання в малих комерційних приміщеннях слід встановити відеоспостереження, замки та контроль доступу, вести облік техніки, обмежити доступ сторонніх осіб, шифрувати дані, налаштувати автоматичне блокування пристроїв, використовувати резервне копіювання та захищені USB-носії. Це мінімізує ризики крадіжок і втрати інформації [29].

Використання нелегального або застарілого програмного забезпечення може призвести до вразливостей у системі. Шкідливе ПЗ, віруси, трояни або бекдори можуть бути встановлені разом із сумнівним програмним забезпеченням,

що ставить під загрозу безпеку даних [30]. У 2017 році СБУ встановила, що близько 300 компаній, зокрема "Укргазвидобування" та "Dragon Capital", використовували ПЗ "Стахановець", яке могло застосовуватися для негласного збору даних під контролем ФСБ РФ. Щоб уникнути датих ситуацій потрібно використовувати лише ліцензоване ПЗ, регулярно оновлювати його та перевіряти систему антивірусами [31].

До фізичних загроз відносяться крадіжки товарів, несанкціонований доступ до складів або торгових приміщень, недостатній контроль за відеоспостереженням. Відсутність сигналізації або неналежний контроль доступу підвищують ризик фізичних атак на приміщення. Для захисту бізнесу від фізичних загроз потрібно встановити відеоспостереження, сигналізацію, контроль доступу, тривожні кнопки та фізичну охорону. Навчити персонал безпеці, перевіряти кандидатів на роботу, забезпечити освітлення і розробити внутрішні політики безпеки. Співпраця з поліцією також важлива для оперативної реакції [32].

Соціальна інженерія – одна з найпоширеніших загроз. Зловмисники можуть видавати себе за партнерів, постачальників або навіть співробітників служби підтримки, щоб отримати доступ до конфіденційної інформації. Недостатнє навчання персоналу з питань кібербезпеки також створює додаткові ризики. Соціальна інженерія є поширеною загрозою для малих підприємств в. Зловмисники видають себе за партнерів або співробітників служби підтримки, щоб отримати доступ до конфіденційної інформації, наприклад, через фішингові листи з шкідливими вкладеннями або посиланнями. Для боротьби з соціальною інженерією на малих приміщеннях необхідно проводити тренінги з кібербезпеки для персоналу, використовувати багатофакторну автентифікацію, встановлювати антивірусне ПЗ, перевіряти достовірність запитів через офіційні канали та впроваджувати політики безпеки [33].

Відсутність чітких правил безпеки призводить до хаосу в управлінні доступом до даних. Якщо не встановлено правила використання паролів, двофакторної автентифікації та резервного копіювання, приміщення залишається

вразливим до атак. У 2020 році в Україні було зафіксовано кілька випадків, коли зловмисники, видаючи себе за представників державних органів, телефонували підприємцям з вимогою надати фінансову інформацію або перерахувати кошти на "безпечні" рахунки. Ці дзвінки мали на меті отримання доступу до конфіденційних даних або безпосередньо до фінансових ресурсів підприємств. Для боротьби з соціальною інженерією на малих приміщеннях потрібно проводити регулярні тренінги з кібербезпеки для персоналу, верифікувати всі підозрілі запити через офіційні канали, використовувати сучасні засоби захисту, такі як антивірусне ПЗ та фаєрволи, а також регулярно робити резервне копіювання даних [34].

Як ми можемо бачити що для безпечної роботи потрібно дотримуватися багатьох правил і не нехтувати ними, так як наслідки можуть привести до фінансових втрат, репутаційних збитків і правових наслідків.

Також є дуже важливим навчання співробітників кібербезпеці, оскільки більшість кіберзагроз спричинені людським фактором. Співробітники, не маючи достатніх знань, можуть випадково відкривати фішингові листи, використовувати слабкі паролі чи передавати конфіденційну інформацію зловмисникам. Навчання дозволяє працівникам розпізнавати загрози, правильно діяти в критичних ситуаціях та мінімізувати ризик атак [35].

Тож усі ці рекомендації допоможуть забезпечити надійний рівень захисту інформації, мінімізувати ризики несанкціонованого доступу та збереження цілісності і доступності даних.

1.4 Постановка задачі проєктування кваліфікаційної роботи

Перед початком розробки ефективної системи захисту інформації для комерційного офісного приміщення, підведемо підсумки вивченої теоретичної інформації та проведеного аналізу. Зі знайдених даних стає зрозуміло, що основними вимогами до сучасних систем захисту інформації є надійність проти

несанкціонованого доступу, висока швидкодія та підтверджена ефективність роботи.

Модульна структура системи захисту позитивно впливає на її надійність та є характерною для практично усіх сучасних інформаційних безпекових систем. Окрім звичайних методів захисту інформації, важливу роль у системі захисту інформації також займають методи стеганографічного захисту. Це перспективна галузь інформаційної безпеки, яка стрімко розвивається та вже на сьогодні має широкий спектр прикладного застосування, зокрема у корпоративному захисті та прихованій передачі даних, які не викликають підозри у потенційних зловмисників.

Надійність системи має базуватися на складності обчислень, необхідних для успішного злому системи. Використання сучасних методів безпеки прогнозовано позитивно вплине на систему захисту, за умови їх продуманого використання та мінімізації негативних особливостей.

На основі цього можемо сформувати задачу проектування кваліфікаційної роботи. Відповідно до мети кваліфікаційної роботи, задачею проектування є розробка та програмна реалізація надійної системи захисту інформації для комерційного офісного приміщення.

Для досягнення мети кваліфікаційної роботи, згаданої вище, необхідно послідовно виконати такі задачі:

– проаналізувати предметну область теми кваліфікаційної роботи;

– проаналізувати типові загрози інформаційній інфраструктурі малих комерційних офісних підприємств та методи протидії їм;

– дослідити державні нормативні документи та кращі міжнародні практики побудови та впровадження систем захисту інформації;

– провести аналіз специфіки інформаційного функціонування малих комерційних підприємств;

– дослідити типові інформаційні потоки комерційного приміщення;

– побудувати модель загроз комерційного приміщення;

– побудувати модель порушника комерційного приміщення;

– спрєктувати систему захисту інформації комерційного приміщення;

– впровадити та апробувати спроєктовані рішення;

– розробити настанови щодо впровадження та експлуатації системи захисту інформації.

2 ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОМЕРЦІЙНОГО ПРИМІЩЕННЯ.

2.1 Дослідження типових інформаційних потоків комерційного приміщення.

Об'єктом дослідження є невелика приватна IT-компанія (ArcadiaWorks), що спеціалізується на розробці комп'ютерних ігор для різних платформ (ПК, мобільних пристроїв та консолей). Компанія працює у сфері цифрового виробництва, поєднуючи творчі та технічні процеси, використовуючи ігрові рушії:

– Unity - це багатоплатформовий інструмент і рушій для розробки відеоігор та додатків, які працюють на ньому;

– Unreal Engine - це ігровий рушій, розроблений і підтримуваний компанією Epic Games.

Інструменти 3D/2D моделювання:

– Autodesk Maya - це програма і графічний редактор для моделювання, анімації, композиції та візуалізації 3D-об'єктів;

– Blender - програмний пакет для створення тривимірної комп'ютерної графіки, що включає інструменти для моделювання, анімації, рендерингу та постобробки відзнятого матеріалу;

– Adobe Photoshop призначений насамперед для редагування цифрових фотографій і створення растрової графіки.

Системи контролю версій Git - це розподілена система контролю версій файлів та спільної роботи, а також цифрові платформи для комунікації та обміну даними:

– Slack — корпоративний месенджер;

– Trello - це безкоштовна багатоплатформенна система управління проектами;

– Google Диск - це сервіс, який дозволяє безпечно зберігати та працювати з файлами на будь-якому пристрої.

Для подальшого дослідження ми глибше занурюємося у внутрішню структуру інформаційних потоків компанії, проводимо аналіз через спілкування з персоналом, вивчаючи яким чином дані переходять із рук в руки, хто є їхніми основними відправниками та отримувачами, а також які канали й інструменти для цього використовуються. З цією метою будуть налагоджені індивідуальні бесіди з ключовими учасниками процесу — від директора до лідерів команд і менеджерів — щоб з’ясувати реальну динаміку обміну повідомленнями, виявити “вузькі місця” та потенційні ризики.

Структура компанії налічує п’ятнадцять осіб, кожен з яких виконує чітко визначену роль у процесі створення та підтримки продукту:

Директор відповідає за загальне управління компанією, формує її стратегію, визначає пріоритети роботи та контролює виконання проєктів. Він приймає ключові управлінські рішення щодо внутрішніх процесів, ресурсів, кадрів і бюджетів, веде переговори з партнерами, інвесторами та клієнтами, представляючи компанію на різних заходах.Після проведеного дослідження було виявлено що відділ розробки включає в себе девять осіб і ділиться на дві команди.

Перша команда складається з чотирйох осіб які відповідають за технічне втілення ігрового процесу. Розробники займаються створенням логіки гри, фізики, поведінки персонажів та інтеграцією всіх компонентів у єдину систему. Вони використовують рушії Unity або Unreal Engine, програмують на C# або C++, забезпечуючи стабільну і плавну роботу гри. Команда тісно взаємодіє з дизайнерами, художниками та тестувальниками, перетворюючи творчі ідеї на повноцінну, захопливу гру. Пізніше в цій команді було призначено лідера, який взяв на себе координацію технічних завдань, розподіл ролей та контроль за дотриманням термінів розробки. Для покращення ефективності взаємодії між учасниками було розроблено структуру комунікації.

Однак, в компанії відсутність системного адміністратора створює значні проблеми для цього відділу. Деякі співробітники з команди змушені брати на себе додаткові обов'язки, пов'язані з технічною підтримкою обладнання та налаштуванням його. Це знижує ефективність основної роботи розробників,

відволікаючи їх від створення ігрових механік, а також негативно впливати на дотримання термінів і якість кінцевого продукту. Така ситуація підкреслює необхідність окремої спеціалізованої посади для забезпечення стабільної підтримки IT-інфраструктури компані

Друга команда це п’ять осіб які займаються творчим і візуальним оформленням гри, а також її якісним тестуванням. Лідер команди якого теж було вибрано пізніше координує роботу над концепцією гри, слідкує за стилістичною цілісністю проєкту та організовує процеси тестування. Геймдизайнери розробляють сюжет, рівні, механіки та інтерфейс гри, формуючи унікальний ігровий досвід. Художники створюють візуальні елементи — персонажів, середовище, іконки та анімації, працюючи з такими інструментами як Blender, Photoshop та інші. Тестувальники перевіряють гру на помилки, оцінюють її зручність і стабільність, щоб кінцевий продукт був бездоганним. Завдяки злагодженій роботі цієї команди гра стає привабливою, цікавою та якісною.

Також у компанії є відділ який об'єднує трьох фахівців, кожен з яких є менеджером у своїй сфері відповідальності. Менеджер проєктів керує розробкою ігор, планує етапи роботи, координує дії між командами та контролює строки виконання. Маркетинговий менеджер займається аналізом ринку, розробкою стратегій просування ігор, визначенням цільової аудиторії та підвищенням продажів. Піар-менеджер відповідає за публічне обличчя компанії — веде соціальні мережі, налагоджує зв’язки зі ЗМІ та формує позитивний імідж бренду. Разом вони забезпечують ефективну організацію роботи, впізнаваність продуктів компанії та стабільне зростання бізнесу.

Бухгалтерський відділ забезпечує фінансову стабільність компанії та чітке ведення всіх облікових процесів. Двоє бухгалтерів відповідають за підготовку фінансової звітності, ведення внутрішнього та зовнішнього документообігу, а також нарахування заробітної плати працівникам. Завдяки їхній роботі, всі фінансові операції здійснюються точно, вчасно та відповідно до чинних норм.

Підсумок цього дослідження демонструє чітку ієрархічну побудову IT-компанії із 15 працівників і це наглядно показано в таблиці 2.1.

Таблиця 2.1 – Ієрархічна побудова компанії

Відділ / Роль	Шифр	Кількість	Опис
Директор	ДИР	1	Стратегічне управління і зовнішні контакти.
Відділ розробки	ВІД-Р	4	Програмісти і розробка механік.
Головний відділу розробки	ВІД-Р-ГОЛ	1	Координація завдань і якості.
Відділ геймдизайну й тестування	ВІД-Г	5	Концепція, графіка та тестування.
Головний відділу ВІД-Г	ВІД-Г-ГОЛ	1	Організація і контроль процесу.
Менеджер проєктів	МП	1	Планування і координація..
Маркетинговий менеджер	МК	1	Просування і аналіз ринку.
Піар-менеджер	ПР	1	Комунікація з медіа і соцмережі.
Лідер бухгалтерії	БГР-ЛІД	1	Координація звітності.
Бухгалтери	БГР	2	Облік і нарахування зарплат.

Система комунікації організації базується на принципі централізації інформації, де головною фігурою є директор. Вся інформація, включаючи

рішення, запити, дані та ідеї, проходить через директора, який є ключовим координатором і стратегічним лідером компанії. Директор збирає пропозиції від різних відділів, аналізує їх, приймає рішення та розподіляє завдання для подальшого виконання. На рисунку 2.1 ми можемо бачити схему яка розроблена в Packet Tracer і наглядно показує як відбуваюця комунікація в компанії.

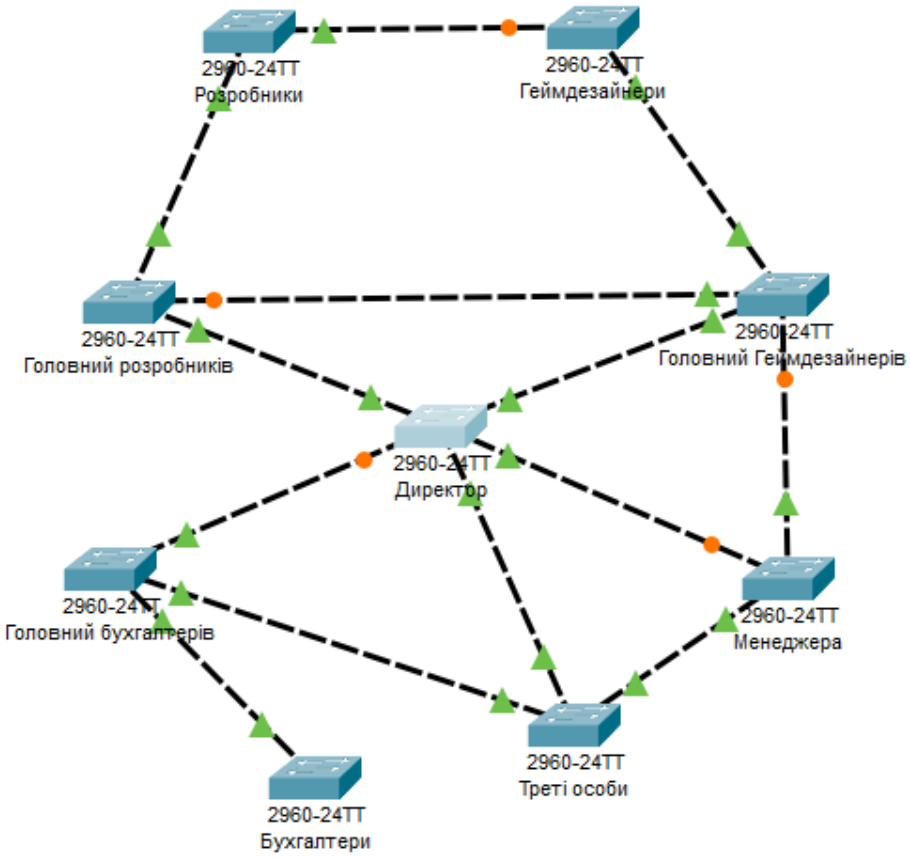


Рисунок 2.1 – Схема комунікації зроблена в Packet Tracer

Оскільки тепер відділи компанії організовані таким чином, що кожен з них має свого головного, який виконує функції представника та комунікатора. Головні відділів є посередниками між директором та членами їхньої команди. Вони збирають важливу інформацію від спеціалістів, що працюють у їхньому відділі, включаючи ідеї, проблеми, пропозиції та звіти про прогрес. Потім вони передають цю інформацію директору для її обговорення та прийняття рішень. Після отримання відповідних інструкцій від директора, лідери відділів

забезпечують їхнє впровадження у своїх командах, пояснюючи деталі та координуючи роботу спеціалістів.

Кожен відділ складається зі спеціалістів, які відповідають за виконання конкретних завдань відповідно до отриманих інструкцій. Їхні функції можуть варіюватись залежно від специфіки відділу, але їх основне завдання — забезпечувати високий рівень професіоналізму, ефективність та якість виконання доручених робіт. Підсумок зведений в таблиці таблиці 2.2.

Таблиця 2.2 – Класифікація корпоративної інформації

Тип інформації	Опис	Вектор
1	2	3
Задачі (технічні/організаційні)	Інформація про поставлені задачі, дедлайни, призначених виконавців.	Від менеджерів до команд розробки
Стан виконання задач	Поточний прогрес, статуси (виконується, завершено, затримка)	Від розробників до менеджерів
Код / програмні дані	Код проєктів, скрипти, конфігураційні файли	Між розробниками, збереження у Git
Особиста інформація і клієнтів і працівників на два окремих пункта	Дані працівників: ПІБ, контакти, графік роботи	Внутрішній облік компанії
Фінансова інформація	Зарплата, бюджети проєктів, витрати, надходження	Бухгалтерія → керівництво, податкові
Технічна інформація про робоче ПЗ та обладнання	Конфігурації обладнання, ліцензії ПЗ, інструкції	Від технічного персоналу до команд

Кінець таблиці 2.2.

1	2	3
Комерційна інформація	Дані про партнерів, угоди, прайси, бізнес-стратегії	Внутрішнє використання, частково зовн.
Внутрішня нормативна документація та корпоративні регламенти	Внутрішня документація, політики, регламенти, внутрішнє листування	Лише для співробітників
Публічна інформація	Презентації, новини компанії, рекламні матеріали, зв’язок із клієнтами	Компанія зовнішній світ

У результаті дослідження було сформовано чітке уявлення про структуру інформаційних потоків у компанії ArcadiaWorks. Встановлено, що обмін даними має ієрархічний характер з активною участю лідерів відділів, які координують комунікацію між командами та керівництвом. Ідентифіковано основні типи інформації, вектори її передачі та канали взаємодії, що дозволяє врахувати особливості внутрішніх процесів при подальшому проєктуванні системи захисту інформації.

2.2 Опис основних недоліків та вразливостей інформаціної безпеки приміщення.

Було проведено аудит безпеки, в результаті якого виявлено цілу низку проблем, що становлять реальну загрозу стабільній роботі та розвитку комерційного приміщення. Аналіз показав, що наявні недоліки охоплюють як технічні аспекти захисту інформації, так і організаційні процеси, які

безпосередньо впливають на безпеку даних, ефективність роботи колективу та загальну надійність бізнесу. Виявлені ризики можуть призвести до серйозних наслідків: втрати важливої інформації, фінансових збитків, репутаційних втрат, порушення робочих процесів і зниження конкурентоспроможності на ринку.

Результати аудиту також показали, що більшість рішень у сфері безпеки та організації роботи раніше приймалися ситуативно та точково. Підходи були спрямовані не на системне усунення першопричин проблем, а переважно на боротьбу з їхніми наслідками. Замість впровадження комплексної політики інформаційної безпеки, будувалася імпровізована реакція на окремі інциденти. Це призводило до накопичення ризиків, хаотичного розвитку внутрішніх процесів і зростання вразливості компанії як до зовнішніх загроз, так і до внутрішніх помилок. Відсутність чіткої стратегії і довгострокового планування у сфері захисту інформації, організації інфраструктури та управління ризиками не дозволяла будувати міцний фундамент для стабільної роботи й розвитку бізнесу.

Тож після проведеного аудити на приміщенні було вийвлено безліч проблем різного типу та рівня загрози.

Критичні недоліки можуть виникати у будь-якій компанії, і вони часто пов'язані з організацією роботи, технічними аспектами або управлінням ресурсами. Нище ми можемо бачити критичні недостатки на приміщенні:

– відсутність чіткої політики паролів створює ризики для інформаційної безпеки приміщення. Використання слабких або повторюваних паролів підвищує ймовірність компрометації облікових записів, а відсутність вимог до їхньої складності та регулярного оновлення збільшує вразливість системи до несанкціонованого доступу;

– повна відсутність систематичного підходу до інформаційної безпеки. (Відсутність політик, процедур і відповідальної особи призводить до хаотичного управління ризиками. Це створює сприятливі умови для витоку даних, внутрішніх інцидентів і зовнішніх атак);

– відсутність системного адміністратора. (Ніхто не відповідає за підтримку серверів, налаштування мережі, безпеку даних та технічну інфраструктуру. Це створює хаос у роботі ІТ-систем і підвищує ризик кібератак, збоїв і втрат даних);

– невпорядкованість каналів комунікації. (Працівники використовують різні месенджери та приватні акаунти без належного захисту. Це створює ризик витоку інформації, втрати завдань і непорозумінь між відділами);

– відсутність системи резервного копіювання даних. (У разі фізичної поломки обладнання, кібератаки або помилки користувача компанія ризикує втратити всю критично важливу інформацію без можливості відновлення);

– відсутність політики інформаційної безпеки. (Працівники не мають інструкцій, як захищати корпоративні дані. Через це зростає ризик випадкової або навмисної втрати або розголошення конфіденційної інформації);

– недостатній контроль за доступом до ресурсів. (Відсутність чітких правил доступу означає, що будь-який співробітник може отримати доступ до фінансових або внутрішніх даних компанії, навіть якщо це не входить у його обов'язки);

– неавторизоване використання особистих пристроїв у роботі. (Смартфони, ноутбуки та інші гаджети працівників можуть не мати антивірусного захисту або оновленого програмного забезпечення, що робить їх "слабким місцем" у безпеці компанії);

– відсутність регулярного оновлення програмного забезпечення (Застаріле ПЗ має відомі вразливості, які легко можуть бути використані для атак. Без оновлень системи стають мішенню для вірусів і хакерів);

– необізнаність співробітників із кібербезпекою. (Працівники можуть стати жертвами фішингових листів або підключати заражені флешки, не усвідомлюючи можливих наслідків);

– фізична незахищеність офісу (відсутність контролю доступу). (Будь-яка стороння особа може потрапити до офісу, отримати доступ до комп’ютерів чи документів, викрасти або пошкодити обладнання).

Значні загрози можуть серйозно впливати на стабільність та розвиток компанії. Нище також ми можемо бачити значні недоліки на приміщенні:

– відсутність чіткої структури комунікацій між підрозділами. (Відсутність єдиного стандарту передачі завдань та звітності призводить до плутанини, втрати інформації та неефективності);

– перевантаження лідерів команд. (Лідери змушені займатися як технічною, так і адміністративною роботою одночасно, що призводить до стресу, вигорання та зниження якості управління);

– недостатня автоматизація бізнес-процесів. (Виконання завдань вручну (наприклад, облік, звітність) уповільнює роботу, підвищує ризик людських помилок і забирає багато часу);

– відсутність культури безпеки серед працівників. (Співробітники не розуміють, чому важливо захищати дані, що збільшує ризик витоків та порушень безпеки);

– відсутність договірних зобов'язань із підрядниками щодо безпеки. (Підрядники можуть неналежно зберігати або передавати дані компанії, що створює ризики витоку інформації);

– використання застарілого обладнання. (Стара техніка має нижчий рівень безпеки і стабільності, що може призводити до частих поломок і збоїв);

– низький рівень шифрування даних. (Передача даних без шифрування дозволяє зловмисникам перехопити важливу інформацію);

– відсутність протоколу реагування на інциденти. (Компанія не має чіткої інструкції, що робити у випадку атаки чи витоку, що призводить до хаосу в кризових ситуаціях);

– відсутність двофакторної автентифікації. (Простий пароль недостатній для захисту облікових записів, особливо в умовах сучасних кіберзагроз);

– відсутність автоматичного блокування робочих станцій при тривалому простої, що може дозволити несанкціонований доступ.

Хоча основні загрози інформаційній безпеці приміщення зосереджені на критичних і значних ризиках, існують також незначні проблеми, які не створюють

серйозної загрози, але можуть впливати на загальну ефективність роботи та рівень захисту даних:

– недостатня організація внутрішньої документації. (Незручне або застаріле зберігання документів ускладнює доступ до інформації, але не створює безпосередньої загрози безпеці);

– відсутність регулярного тестування резервних копій, що може ускладнити їхнє відновлення у разі потреби;

– використання застарілих інструменьів розробки.

Приклад однією з критичних загроз є вразливе розташування мережевого обладнання яке можна бачити на рисунку-2.2. Сервири стоять на підлозі не далеко до вхідних дверей, що підвищує ризик пошкодження (механічного чи через пролиття рідини). Кабелі прокладенні не акуратно є можливість зачепитися, висмикнути або пошкодити, роутер розміщений на відкритій полиці, легко доступний для сторонніх осіб.

Рисунок-2.2 – Небезпечне розташування мережевого обладнання

Всі виявлені проблеми на приміщенні було класифіковано за рівнем їхньої потенційної загрози для безпеки інформації. Зокрема, вони були поділені на три

основні категорії: критичні, значні та незначні. Такий підхід дозволив сформувати структуроване бачення стану інформаційної безпеки приміщення та виокремити пріоритети для реагування. Підсумки проведеного аналізу наведено в узагальненій таблиці 2.3, яка відображає розподіл загроз за рівнем важливості та дозволяє наочно оцінити ступінь ризику для кожної виявленої проблеми.

Таблиця 2.3 – Класифікація проблеми за рівнем загрози

Проблема	Рівень загрози
1	2
Відсутність чіткої політики паролів	Критична
Повна відсутність систематичного підходу до інформаційної безпеки	Критична
Відсутність політики інформаційної безпеки	Критична
Невпорядкованість каналів комунікації	Критична
Немає системного адміністратора	Критична
Відсутність системи резервного копіювання даних	Критична
Недостатній контроль за доступом до ресурсів	Критична
Неавторизоване використання особистих пристроїв у роботі	Критична
Відсутність регулярного оновлення програмного забезпечення	Критична
Необізнаність співробітників із кібербезпекою	Критична
Фізична незахищеність офісу)	Критична
Вразливе розташування мережевого обладнання	Критична

Кінець таблиці 2.3.

1	2
Відсутність чіткої структури комунікацій між підрозділами	Значна
Перевантаження лідерів команд	Значна
Недостатня автоматизація бізнес-процесів	Значна
Відсутність культури безпеки серед працівників	Значна
Відсутність договірних зобов'язань із підрядниками щодо безпеки	Значна
Використання застарілого обладнання	Значна
Низький рівень шифрування даних	Значна
Відсутність протоколу реагування на інциденти	Значна
Відсутність автоматичного блокування робочих станцій при тривалому простої	Значна
Відсутність двофакторної автентифікації	Значна
Недостатня організація внутрішньої документації	Незначна
Відсутність регулярного тестування резервних копій	Незначна
Викорестання застарілих інструментів	Незначна

За результатами проведеного аналізу було ідентифіковано 12 критичних загроз, які потребують негайного усунення для забезпечення стійкості інформаційної системи приміщення. 10 значних загроз, що не є критичними, але можуть суттєво впливати на ефективність бізнес-процесів і загальну захищеність

інформаційної інфраструктури. І 3 незначну недоліки, що має мінімальний вплив на захищеність даних, але може покращити загальну організацію роботи приміщення.

Оцінка загроз за рівнем їх критичності дозволяє визначити першочергові заходи для їхнього усунення та розробити стратегічний план захисту інформаційної системи приміщення. Найнебезпечнішими є загрози, які можуть спричинити серйозні порушення бізнес-процесів, витік інформації або повну втрату даних. Усуваючи ці проблеми насамперед, приміщення може значно зменшити ризики критичних наслідків.

Значні загрози, хоч і не ведуть до негайного руйнування інформаційної інфраструктури, все ж можуть створювати серйозні труднощі у роботі компанії. Важливо розглядати ці ризики у довгостроковій перспективі та поступово впроваджувати відповідні заходи для їхнього зниження.

Незначні загрози мають найменший вплив на безпеку та стабільність роботи приміщення. Хоча їх усунення може покращити організацію бізнес-процесів, вони не є критичними для функціонування системи захисту даних.

Загальна класифікація загроз дозволяє визначити оптимальну стратегію інформаційної безпеки, де ключовий фокус спрямовується на ліквідацію критичних ризиків, а також поступове вдосконалення організаційної структури для довгострокової стабільності роботи.

2.3 Побудова моделі загроз системи захисту інформації комерційного приміщення

На основі виявлених вище недоліків у сфері інформаційної безпеки буде сформована модель загроз, яка дозволить систематизувати потенційні ризики, виявити найуразливіші місця в ІТ-інфраструктурі та розробити відповідні заходи для їхнього усунення чи мінімізації. Такий підхід забезпечить цілісне бачення поточних загроз і стане основою для побудови ефективної системи захисту.

У сучасному цифровому та глобалізованому середовищі малі комерційні приміщення все частіше стикаються з різноманітними загрозами, які можуть вплинути на їхню стабільну діяльність, репутацію та фінансову стійкість. Незважаючи на обмежені ресурси, саме малі бізнеси є привабливою ціллю для зловмисників через недостатній рівень захисту, обмеженість внутрішніх політик безпеки та низький рівень усвідомлення ризиків.

Метою створення моделі загроз є ідентифікація потенційних ризиків, виявлення вразливостей приміщення, а також розробка заходів щодо їхнього запобігання або мінімізації наслідків. Модель базується на аналізі внутрішніх і зовнішніх факторів, що можуть вплинути на приміщення, та враховує як технічні, так і організаційні аспекти безпеки.

Моделі загроз створюватимуться з урахуванням чинних нормативних настанов і рекомендацій у сфері технічного захисту інформації, зокрема НД ТЗІ 1.1-002-99 та НД ТЗІ 1.4-001-2000. Це дозволить забезпечити відповідність вимогам національного законодавства, врахувати типові загрози для об’єктів інформаційної діяльності та закласти основу для побудови ефективної системи захисту інформації, загрози для приміщення поділяються на чотири класи:

– порушення конфіденційності інформації – отримання інформації користувачами або процесами всупереч встановлених правил доступу;

– порушення цілісності інформації – повне або часткове знищення інформації, її викривлення або видозмінення, нав’язування помилкової інформації тощо;

– порушення доступності інформації – абсолютній або часткова втрата працездатності системи, блокування доступу до інформації;

– втрата спостереженості або керованості системи обробки – порушення методів ідентифікації та автентифікації користувачів і процесів, надання їм прав, здійснення контролю за їх діяльністю, відмовлення від одержання або пересилання повідомлень.

За типом основного засобу, який використовується для реалізації загрози, всі джерела загроз поділяються на такі групи:

– людина;

– апаратура;

– програма;

– фізичне середовище.

Основними видами загроз ресурсам комп’ютерних сиситем Приміщення можуть бути:

– зміна умов фізичного середовища (стихійні лиха (землетрус, повінь, ураган), пожежа або інші випадкові події);

– збої та відмови у роботі обладнання та технічних засобів комп’ютерних сиситем;

– наслідки помилок під час проектування та розробки компонентів комп’ютерних сиситем приміщення (технічних засобів, технології обробки інформації, програмних засобів захисту, структур даних тощо);

– помилки під час експлуатації (персоналу, користувачів комп’ютерних сиситем);

– навмисні дії порушників (спроби несанкціонованого доступу).

Умисні (зокрема і пов’язані з діяльністю зареєстрованих користувачів) небезпеки з боку порушників спрямовуються на порушення роботи КС (її окремих складових) або вивидення її з ладу, доступ в систему і отримання можливості несанкціонованого входу до її активів.

Загрози, пов’язані з поведінкою зареєстрованих користовувачів, у свою чергу можуть класифікуватися на випадкові чи умисні. Кожна із небезпек здійснюється з деякою ймовірністю, може порушувати ту чи іншу функціональну властивість захисної системи, має своїм результатом (особливо навмисні ризики) певні втрати (збитки) та джерело походження чи активації.

Перелік можливих загроз інформації, яка опрацьовується в приміщенні та циркулює у відповідних приміщеннях, наводиться в таблицях нище.

Умовні позначення такі:

К – порушення конфіденційності інформації;

Ц – порушення цілісності інформації, програмного забезпечення, системних даних, даних реєстрації;

Д – порушення можливості доступу до інформації, системних даних, даних реєстрації;

С – порушення спостереженості, керованості процесу оброблення інформації.

У процесі забезпечення інформаційної безпеки комерційного приміщення необхідно враховувати не лише цілеспрямовані дії зловмисників, але й випадкові загрози, які можуть виникати незалежно від людського фактору. До таких загроз належать як природні явища (повені, урагани, пожежі тощо), так і наслідки бойових дій, що стали особливо актуальними в умовах воєнного стану в Україні. Ці загрози можуть мати критичний вплив на конфіденційність, цілісність, доступність і спостережуваність інформації.

У таблиці 2.4 подано класифікацію таких загроз за джерелом походження, ймовірністю виникнення, рівнем потенційної шкоди, а також типом наслідків для інформаційної безпеки приміщення.

Таблиця 2.4. Випадкові загрози природного походження

№	Тип та визначення загрози	Джерело загрози	Ймовірність	Рівень шкоди	Наслідки			
					К	Ц	Д	С
	2	3	4	5	6	7	8	9
ЗП1	Переривання зв’язку або інтернету через пошкодження комунікацій	інфраструктура	середня	середній	+		+	+
ЗП2	Повінь, землетрус, ураган	середовище	низька	неприпустимо високий		+	+	+
ЗП3	Вологість, запиленість, зміни температури	середовище	Середня	високой		+	+	+

Також, істотну небезпеку для інформаційної інфраструктури приміщення становлять випадкові загрози техногенного походження. Вони виникають у результаті технічних несправностей, людських помилок, збоїв обладнання чи системного програмного забезпечення, а також аварій на об’єктах інженерної інфраструктури. Вони можуть спричинити порушення в роботі інформаційних систем, втрату або спотворення даних, зниження доступності сервісів. У таблиці 2.4 наведено основні типи техногенних загроз та бойових дій, їхні джерела, ймовірність виникнення, рівень потенційної шкоди та наслідки.

Таблиця 2.5 – Випадкові загрози техногенного походження та бойових дій

№	Тип та визначення загрози	Джерело загрози	Ймовірність	Рівень шкоди	Наслідки			
					К	Ц	Д	С
1	2	3	4	5	6	7	8	9
ВЗТ1	Ураження програмного забезпечення та масивів даних комп’ютерними вірусами	людина, програма	середня	неприпустимо високий	+	+	+	+
ВЗТ2	Недбале зберігання та облік носіїв інформації, систематичне неправильне виконання своїх функцій	людина	висока	неприпустимо високий	+	+	+	+
ВЗТ3	Випадкові помилки користувачів, обслуговуючого персоналу, помилкове конфігурування та адміністрування системи	людина	середня	високий	+	+	+	+
ВЗТ4	Відмови, помилки програмного забезпечення	програми	висока	середній	+	+	+	+
ВЗТ5	Відмови, збої, помилки основної апаратури, носіїв інформації	апаратура	висока	неприпустимо високи	+	+	+	+

Кінець таблиці 2.5.

1	2	3	4	5	6	7	8	9
ВЗТ6	Вразливе розташування мережевого обладнання	людина	висока	високий	+	+	+	
ВЗТ7	Перенавантаження лідерів команди	людина	висока	середній	+	+	+	
ВЗТ8	Ракетний або артилерійський обстріл, вибухова хвиля	військове	середня	високий		+	+	+
ВЗТ9	Пожежа, вибух	середовище	низька	неприпустимо високий		+	+	+
ВЗТ10	Вібрація обладнання	апаратура	низька	середній		+	+	+
ВЗТ11	Небажаний вплив процесів один на одного	апаратура	середня	середній		+	+	+
ВЗТ12	Сторонні електромагнітні випромінювання (електромагнітна сумісність)	апаратура	низька	низький		+	+	+
ВЗТ13	Відключення електроенергії через удари по енергосистемі	інфраструктура	висока	високий			+	+
ВЗТ14	Відмови, збої систем живлення, систем забезпечення нормальних умов роботи апаратури і персоналу	середовище апаратура	середня	високий		+	+	
ВЗТ15	Поломка апаратури	людина, апаратура	низька	високий		+	+	
ВЗТ16	Пошкодження носіїв інформації	людина, апаратура	середня	високий		+	+	
ВЗТ17	Недостатня автоматизація бізнес процесів	людина	середня	середня	+	+		
ВЗТ18	Недостатня організація внутрішньої документації	людина	середня	малий	+			

Серед численних ризиків для інформаційної безпеки особливу увагу слід приділити навмисним загрозам техногенного походження, які здійснюються дистанційно. До них належать дії, спрямовані на втручання в інформаційні системи приміщення через мережу Інтернет або інші канали зв’язку, без фізичного доступу до об'єкта. Такі загрози можуть мати цілеспрямований характер і бути реалізовані зловмисниками як ззовні, так і зсередини — шляхом використання шкідливого програмного забезпечення, віддаленого адміністрування, перехоплення даних, атак типу DDoS тощо. У таблиці 2.6 наведено класифікацію таких загроз за джерелами, засобами реалізації, ймовірністю та наслідками для інформаційної безпеки приміщення.

Таблиця 2.6 – Навмисні загрози техногенного походження дистанційної дії

№	Тип та визначення загрози	Джерело загрози	Ймовірність	Рівень шкоди	Наслідки			
					К	Ц	Д	С
1	2	3	4	5	6	7	8	9
НЗТ1	Використання електромагнітних імпульсів з метою зруйнування інформації, засобів її обробки та збереження	апаратура	низька	неприпустимо високий		+	+	
НЗТ2	Захоплення ресурсів обчислювальної системи потоком неінформативних (хибних) повідомлень	людина, програми	низька	середній			+	+
НЗТ3	Перегляд інформації, відображеної на терміналах, або зафіксованої на паперових носіях	апаратура	низька	високий	+			

Ці загрози виникають у результаті навмисних дій зловмисника, який має фізичний доступ до інформаційних систем або приміщень приміщення. Вони можуть включати підключення сторонніх пристроїв, втручання в апаратне

забезпечення, зчитування або модифікацію інформації. Такі загрози становлять серйозну небезпеку, особливо якщо здійснюються уповноваженим персоналом або під прикриттям. У таблиці 2.7 – Навмисні загрози техногенного походження контактної дії наведено основні типи контактних загроз, їх джерела, ймовірність виникнення, рівень шкоди та очікувані наслідки для інформаційної безпеки.

Таблиця 2.7 – Навмисні загрози техногенного походження контактної дії

№	Тип та визначення загрози	Джерело загрози	Ймовірність	Рівень шкоди	Наслідки			
					К	Ц	Д	С
1	2	3	4	5	6	7	8	9
НТК1	Вербування персоналу	людина	середня	неприпустимо високий	+	+	+	+
НТК2	Несанкціоновані зміни, підміна елементів програм, апаратури	людина, програми	низька	неприпустимо високий	+	+	+	+
НТК3	Використання вад мов програмування, операційних систем, прикладних програм	людина, програми	низька	неприпустимо високий	+	+	+	+
НТК4	Включення до програми програмних закладок типу «троянський кінь», «бомба», фішингових атак тощо	людина, програми	середня	неприпустимо високий	+	+	+	+
НТК5	Дії щодо дезорганізації функціонування системи (зміна режимів роботи пристроїв та програм, саботаж персоналу тощо)	людина	середня	високий		+	+	+

Кінець таблиці 2.7.

1	2	3	4	5	6	7	8	9
НТК6	Перехоплення блоків інформації, які виводяться на комунікаційні порти обладнання	апаратура, програми	низька	середня	+			+
НТК7	Відключення або виведення з ладу підсистем забезпечення функціонування)	людина, програми, апаратура,	середня	високий		+	+	
НТК8	Фізичне зруйнування системи, її компонентів	людина, середовище	низька	неприпустимо високи		+	+	
НТК9	Розкрадання матеріальних носіїв інформації, виробничих відходів	людина	середня	неприпустимо високи	+		+	
НТК10	Провокування до розмов персоналу	людина	середня	високий	+			+
НТК11	Несанкціоноване використання обчислювальних ресурсів	людина, програми	середня	високий		+		+
НТК12	Несанкціоноване використання технічних пристроїв	людина	середня	високий			+	+
НТК13	Читання “сміття” (залишкової інформації з запам’ятовуючих пристроїв)	апаратура, програми, людина	середня	низький	+			
НТК14	Перегляд інформації, виведеної на екран терміналу	людина, програми	середня	високий	+			
НТК15	Перегляд документів на паперових носіях під час друкування	людина	середня	високий	+			
НТК16	Копіювання вихідних документів, інших матеріальних носіїв інформації	апаратура, програми, людина	низька	неприпустимо високий	+			

За результатами аналізу моделі загроз встановлено, що найбільшою вразливістю комерційного приміщення є фактори, пов’язані з людською недбалістю, відсутністю чітких політик безпеки, технічною неготовністю до загроз та активністю зовнішніх зловмисників. В основі більшості ризиків лежить недостатній рівень інформаційної культури, обмеженість фінансових та кадрових ресурсів, а також слабка організаційна структура безпеки.

Приміщення схильне до втрат даних, їх викривлення, несанкціонованого доступу та перебоїв у роботі IT-інфраструктури. Основними проблемами залишаються відсутність контролю за доступом, слабкий рівень резервного копіювання, брак систематичного моніторингу та низький рівень підготовки персоналу.

Для забезпечення базової стійкості до інформаційних загроз доцільним є впровадження мінімально необхідного, але комплексного набору організаційно-технічних заходів. Серед ключових кроків — створення політики інформаційної безпеки, впровадження системи навчання працівників, налагодження процедур логування та резервування, а також регулярна перевірка систем на наявність вразливостей.

Побудова системи інформаційної безпеки має стати стратегічним напрямком діяльності приміщення, що гарантує не лише зменшення ризиків, а й підвищення довіри з боку клієнтів, партнерів та суспільства в цілому.

Завдяки сформованій моделі загроз є можливість наочно оцінити масштаб потенційних ризиків, з якими може зіткнутися інформаційна система приміщення. Такий підхід дозволяє систематизувати загрози за походженням та характером впливу, що, у свою чергу, сприяє більш ефективному плануванню заходів з їхньої нейтралізації чи мінімізації.

- 3 випадкові загрози природного походження;
- 18 випадкових загроз техногенного походження;
- 3 навмисні загрози техногенного походження дистанційної дії;
- 16 навмисних загроз техногенного походження контактної дії.

Проаналізувавши і класифікувавши виявлені загрози в інформаційній системі, ми провели оцінку ймовірності їх виникнення та рівня потенційної шкоди, яку вони можуть завдати. В таблиці 2.8 ми можемо бачити зведений підсумок цієї оцінки.

Таблиця 2.8 – Класифікація загроз за рівнем шкоди та ймовірністю.

Рівень шкоди / Ймовірність	середня	висока	неприпустимо висока
Низька	3	2	8
Середня	3	13	5
Висока	2	2	2

Для кожної комірки, яка відповідає певному поєднанню ймовірності та шкоди, вказано кількість загроз, що підпадають під ці критерії. Таким чином, ми змогли візуалізувати розподіл ризиків за їх серйозністю.

Щоб надати кожній загрозі пріоритет реагування, ми використали кольорове кодування та шрифтове позначення:

– П1 – критичний пріоритет (червоне горизонтальне заштрихування): загрози, які вимагають негайного усунення або запобігання;

– П2 – високий пріоритет (блакитне вертикальне заштрихування): загрози, що становлять суттєву небезпеку і потребують термінових заходів;

– П3 – середній пріоритет (помаранчеві діагональні лінії вниз): загрози, усунення яких важливе, але не є критичним;

– П4 – низький пріоритет (жовті діагональні лінії вгору): загрози з мінімальним впливом, які можна контролювати планово.

В загальному підсумку було виявлено:

– 3 випадкові загрози природного походження;

– 18 випадкових загроз техногенного походження;

– 3 навмисні загрози техногенного походження дистанційної дії;

– 16 навмисних загроз техногенного походження контактної дії.

Далі, згідно з цією класифікацією, ми прив’язали конкретні загрози до відповідних пріоритетів:

– критичний пріоритет (П1), загрози: ВЗТ2, ВЗТ5;

– високий пріоритет (П2), загрози: ВЗТ13, ВЗТ1 ,ВЗТ6, ВЗТ8, НТК1, НТК4 НТК9, ;

– середній пріоритет (П3), загрози: ВЗП3, ВЗТ4, ВЗТ7,ВЗТ14, ВЗТ16, НТК5, НТК7, НТК10, НТК11, НТК12, НТК13, НТК14, НТК15, НЗТ3, ВЗТ15, ВЗП2, ВЗТ9, НТК9, НТК16, ВЗП1,ВЗТ3, ВЗТ11, ВЗТ17, НЗТ1, НТК2, НТК3, НТК8 ВЗТ8,;

– низький пріоритет (П4), загрози: НТК6, НЗТ2, ВЗТ9.

Таким чином, побудована модель дозволяє не лише бачити всі загрози в структурованому вигляді, але й визначити першочерговість заходів безпеки, що є важливим етапом у розробці системи захисту інформації.

В ході проєктування першочергово увага та ресурси будуть приділенні загрозам критичного та високо приорітету. Загрози середнього приорітету будуть розглянуті в другу чергу. Загрози низького пріоритету можуть бути частково проігнорованні або частково усуненні разом із загрозами вищого пріоритету.

2.4 Побудова моделі порушника системи захисту інформації комерційного приміщення

Порушник – це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби, здійснила спробу виконати дії, які призвели або могли призвести до порушення конфіденційності, цілісності та доступності інформації або спостереженості підприємства.

Метою порушника можуть бути:

– несанкціоноване зчитування інформації;

– несанкціонована модифікація інформації;

– несанкціоноване знищення інформації;

– повна або часткова руйнація операційної системи.

Відносні оцінки збитків, які може заподіяти порушник за умов наявності відповідних характеристик, зазначені в графі «Рівень загрози» кожної таблиці, що наведена нижче, і характеризуються такими категоріями:

– мінімальна загроза;

– загроза з незначними наслідками;

– можлива загроза з серйозними наслідками;

– максимальна загроза

Одним із ключових факторів, що впливають на поведінку порушника, є мотив, який спонукає його до здійснення протиправних дій. Мотиви можуть бути як несвідомими (наприклад, безвідповідальність), так і цілеспрямованими (корислива мета, професійний обов'язок тощо). Рівень загрози, що виникає внаслідок дій порушника, значною мірою залежить від характеру його намірів. У таблиці 2.9 наведено класифікацію можливих мотивів порушення з відповідними оцінками рівнів загрози.

Таблиця 2.9 – Мотиви порушень

Позначення	Мотив порушення	Рівень загроз
М 1	Безвідповідальність	1
М 2	Самоствердження	2
М 3	Корислива мета	3
М 4	Професійний обов'язок	4

Порушники можуть суттєво відрізнятися між собою за походженням, посадовими обов'язками, рівнем доступу до інформаційних ресурсів та намірами. Важливо розмежовувати внутрішніх і зовнішніх порушників, оскільки їхні дії можуть мати різну природу та потенційну шкоду. У таблиці 2.10 представлено розподіл

порушників за категоріями та відповідний рівень загрози, що виникає від дій кожної групи.

Таблиця 2.10 – Категорії порушників

Позначення	Визначення категорії	Рівень загроз
Внутрішні порушники		
ВП 1	Технічний персонал	1
ВП 2	Працівники комерційного приміщення	2
ВП 3	Персонал, який обслуговує технічні засоби (інженери тощо)	2
ВП 4	Співробітники служби захисту інформації, керівники різних рівнів	4
Зовнішні порушники		
ПЗ 1	Відвідувачі (запрошені з любого приводу)	1
ПЗ 2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ 3	Хакери	3
ПЗ 4	Агенти конкурентів або іноземних спецслужб «під прикриттям»	4

Ступінь фізичного або логічного доступу до системи чи об’єкта є критичним чинником, що визначає вразливість до загроз. Чим легше доступ, тим вищий ризик реалізації потенційних атак. У таблиці 2.11 подано градацію доступності інформаційної системи для порушника та відповідний рівень загрози, пов'язаний із кожною ситуацією.

Таблиця 2.11 – Доступність

Позначення	Доступність	Рівень загроз
Д 1	Дуже низька: доступ майже неможливий або вимагає спеціальних обставин	1
Д 2	Низька: доступ ускладнений і потребує значних зусиль	2
Д 3	Середня: доступ є, але потребує певних зусиль	3
Д 4	Висока: легкий доступ до системи	4

Рівень знань і технічної підготовки порушника прямо впливає на його здатність обходити системи захисту та завдавати шкоди. Від поверхневого ознайомлення з технікою до глибокого розуміння захисних механізмів — кожен рівень кваліфікації становить різний ступінь загрози. У таблиці 2.12 представлено типові рівні обізнаності та їхній вплив на загальну оцінку загрози.

Таблиця 2.12 – Рівні обізнаності

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
1	2	3
К 1	Порушник володіє малим рівнем знань, але вміє працювати з технічними засобами комерційного приміщення	1
К 2	Порушник володіє середнім рівнем знань і практичними навичками роботи з технічними засобами та їх обслуговування	2
К 3	Порушник володіє високим рівнем знань у програмуванні та обчислювальної техніки, проєктування та експлуатації комерційного приміщення	3

Кінець таблиці 2.12.

1	2	3
К 4	Порушник знає структуру, функції та механізми дії засобів захисту інформації в комерційному приміщенні, їх недоліки та можливості	4

Обставини, за яких може діяти порушник, зокрема час реалізації загрози, також мають істотне значення для оцінки ризику. Деякі дії можуть бути здійснені лише в умовах призупинки роботи системи, тоді як інші — у будь-який момент функціонування. У таблиці 2.13 Специфікація моделі порушника за часом дії подано класифікацію ситуацій за часовим фактором і відповідний рівень загрози.

Таблиця 2.13 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	Під час повної бездіяльності інформаційно-технологічного супроводу з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів інформаційно-технологічного супроводу з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування інформаційно-технологічного супроводу (або компонентів системи)	3
Ч4	Як у процесі функціонування інформаційно-технологічного супроводу, так і під час призупинки компонентів системи	4

Рівень технічного оснащення та практичних умінь порушника визначає його здатність подолати існуючі бар’єри безпеки. Від простого візуального

спостереження до використання активних технічних засобів — кожен тип можливостей має свою характеристику ризику. таблиця 2.13 демонструє класифікацію порушників за таким критерієм і відповідні рівні загроз.

Таблиця 2.14 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів інформаційно-технологічного супроводу	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів інформаційно-технологічного супроводу, дезорганізації систем обробки інформації	4

Розглянуті вище потенційні цілеспрямовані (навмисні) та випадкові загрози є двома основних класами прояву можливих загроз несанкціонований доступ до інформації комерційного приміщення. Оскільки час та місце факту умисної загрози несанкціонований доступ передбачити неможливо, доцільно прогнозувати узагальнену інформаційно-аналітичну модель поведінки

потенційного порушника технічного захисту інформації в найбільш загрозливих ситуаціях, а саме:

– порушники можуть з’явитися в будь-який час та в будь-якому місці периметру безпеки об’єкту електронно-обчислювальної техніки;

– кваліфікація та освіченість порушників технічного захисту інформації можуть бути на рівні розробника даної системи;

– інформація щодо принципів роботи системи, у тому числі і з обмеженим доступом, порушникам технічного захисту інформації відома;

– для досягнення своєї мети порушники технічного захисту інформації вибиратимуть найбільш слабкішу ланку в захисті;

– порушниками технічного захисту інформації можуть бути не тільки сторонні особи, але і санкціоновані користувачі системи;

– порушники можуть діяти в складі спеціалізованого підрозділу.

Для кращого усвідомлення того, як поведе себе зловмисник, формалізуємо типову схему стратегії дій порушника технічного захисту даних в комерційних приміщеннях.

– одержати несанкціонований доступ до інформації з обмеженим доступом;

– видати себе за іншого користувача, щоб скинути з себе відповідальність, або ж використати його повноваження щоб зформувати хибну інформацію, зміни санкціонованої інформації;

– стверджувати, що інформація одержана від деякого санкціонованого користувача, хоча вона сформована самим же порушником технічного захисту інформації;

– несанкціоновано змінити повноваження інших санкціонованих користувачів (розширити або обмежити, вивести або ввести інших осіб і т. ін.);

– несанкціоновано розширити свої повноваження по доступу до - інформація з обмеженим доступом та її обробці;

– приховати факт наявності певної інформації в іншій інформації (таємне зберігання однієї в змісті іншої інформації);

– вивчити - хто, коли і до якої інформації отримує доступ (навіть якщо сама - інформація з обмеженим доступом залишається недоступною);

– модифікувати програмне забезпечення внаслідок вилучення або надання нових функцій.

Подані вище формалізовані моделі стратегії поведінки зловмисника технічного захисту інформації в обчислювальних системах вказують на те, наскільки важливо знати, кого вважати порушником технічного захисту інформації. Для побудови даної моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них вказується в дужках і оцінюється за 4-бальною шкалою. Таким чином було створено модель порушника і зведено підсумок в дві таблиці наведені нище. Часто порушення відбуваються випадково, через необізнаність, недбалість або технічні помилки з боку працівників чи відвідувачів. Такі дії можуть спричинити серйозні наслідки, особливо якщо особа має доступ до критичних ресурсів.

У табиці 2.15 наведено класифікацію потенційних випадкових порушників із зазначенням їхніх характеристик та сумарного рівня загроз.

Таблиця 2.15 – Модель порушника за випадковістю

№	Порушник	Категорія порушника	Мотив	Кваліфікація	Можливості щодо подолання захисту	Можливості за часом дії	Доступність	Сума загроз
1. Внутрішні порушники, за випадковістю								
1	2	3	4	5	6	7	8	9
1.1	Директор	ВП 4	М 1	К 4	З 4	Ч 4	Д 4	21
1.2	Головний розробників	ВП 3	М 1	К 3	З 3	Ч 3	Д 4	17
1.3	Розробники	ВП 3	М 1	К 3	З 2	Ч 3	Д 3	15

Кінець таблиці 2.15.

1	2	3	4	5	6	7	8	9
1.4	Головний геймдезайнерів	ВП 3	М 1	К 2	З 2	Ч 3	Д 3	14
1.5	Головний бухгалтер	ВП 2	М 1	К 2	З 2	Ч 2	Д 3	12
1.6	Менеджери	ВП 2	М 1	К 1	З 2	Ч 2	Д 3	11
1.7	Бухгалтер	ВП 2	М 1	К 2	З 1	Ч 2	Д 2	10
1. Зовнішні порушники за випадковістю								
1.1	Хакер	ПЗ 3	М 3	К 4	З 4	Ч 3	Д 1	18
1.2	Клієнт	ПЗ 1	М 2	К 2	З 2	Ч 3	Д 1	11

Порушники, що діють з корисливою метою, становлять одну з найбільших загроз для інформаційної безпеки приміщення. Їхні дії, як правило, добре сплановані, цілеспрямовані та мотивовані бажанням отримати особисту або комерційну вигоду.

У таблиці 2.16 представлено порушників з розподілом за категоріями, рівнем доступу, мотивацією, технічними можливостями та іншими характеристиками, що впливають на сумарну оцінку рівня загрози.

Таблиця 2.16 – Модель порушника за корисливим інтересом

№	Порушник	Категорія порушника	Мотивація	Кваліфікація	Можливості щодо подолання захисту	Можливості за часом дії	Доступність	Сума загроз
1 Внутрішні порушники, за корисливим інтересом								
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1.1	Директор	ВП 4	М 3	К 2	З 4	Ч 4	Д 4	23

Кінець таблиці 2.16.

1	2	3	4	5	6	7	8	9
1.2	Керівник відділу розробки	ВП 3	М 3	К 4	З 3	Ч 4	Д 4	21
1.3	Керівник відділу геймдезайнерів	ВП 3	М 3	К 3	З 2	Ч 3	Д 3	17
1.4	Розробники	ВП 3	М 3	К 3	З 2	Ч 3	Д 3	17
1.5	Менеджери	ВП 2	М 3	К 2	З 3	Ч 3	Д 3	16
1.6	Головний бухгалтер	ВП 2	М 3	К 2	З 3	Ч 3	Д 3	16
1.7	Бухгалтер	ВП 2	М 3	К 2	З 1	Ч 2	Д 2	12
2 Зовнішні порушники за корисливим інтересом								
1.1	Хакер	ПЗ 4	М 4	К 4	З 4	Ч 4	Д 2	21
1.2	Клієнт	ПЗ 1	М 3	К 2	З 2	Ч 3	Д 2	12

У ході аналізу було розглянуто основні типи порушників, що можуть становити загрозу для інформаційної безпеки комерційного приміщення, зокрема ІТ-компанії, яка займається розробкою комп’ютерних ігор. Модель порушника побудована з урахуванням мотивації, кваліфікації, технічних можливостей, доступності до інформаційних систем і часу реалізації загроз.

Результати аналізу двох основних моделей — за випадковістю та за корисливим інтересом — дозволили виявити найнебезпечніших та найменш небезпечних порушників:

– Найнебезпечнішим порушником виявився директор приміщення, який у моделі за корисливим інтересом має найвищу суму загроз — 23 бали. Це зумовлено високим рівнем доступу до систем, значними технічними можливостями, широкими повноваженнями та потенційною зацікавленістю у навмисних діях.

– Найменшу загрозу становить бухгалтер, який у моделі за випадковістю має найнижчий рівень сумарної загрози — 10 балів. Це пояснюється обмеженим рівнем кваліфікації, низькою мотивацією до порушення та меншою технічною оснащеністю.

Таким чином, ключовими факторами для оцінки загроз від порушників є не лише технічні навички, але й рівень доступу, посадові обов'язки та мотивація. Високий ризик походить не лише від зовнішніх зловмисників (наприклад, хакерів), але й від внутрішніх осіб, які мають повний доступ до критичних ресурсів приміщення.

2.5 Проєктування системи захисту інформації відповідно до визначених вимог.

У попередніх розділах було створено модель загроз із пріорітетами щодо їх усунення. Керуючись цим, побудова системи захисту інформації комерційного приміщення буде проєктуватися таким чином щоб першочергово усунути найбільш пріоритетні загрози, зокрема з урахуванням потенційних порушників, що можуть їх реалізувати та рівнем їх мотивації.

Згідно з створеною моделлю, загрозами із критичним пріорітетом є:

– недбале зберігання та облік носіїв інформації, систематичне неправильне виконання своїх функцій(ВЗТ2);

– відмови, збої, помилки основної апаратури, носіїв інформації(ВЗТ5).

Усунення даних загроз буде включено в комплекс засобів захисту першочергово, оскільки успішна їх експлатація призведе до найбільш тяжки наслідків.

Загрози з високим пріоритетом також становлять суттєву небезпеку для інформаційної системи приміщення, хоча й не є настільки критичними, як ті, що мають пріоритет П1. Їх реалізація може призвести до серйозних порушень

конфіденційності, цілісності або доступності інформації. До таких загроз належать:

– відключення електроенергії через удари по енергосистемі (ВЗТ13);

– ракетний або артилерійський обстріл, вибухова хвиля (ВЗТ8);

– вразливе розташування мережевого обладнання (ВЗТ6);

– ураження програмного забезпечення та масивів даних комп'ютерними вірусами (ВЗТ1);

– вербування персоналу (НТК1);

– включення до програми програмних закладок типу «троянський кінь», «бомба», фішингових атак тощо (НТК4).

У процесі проєктування системи захисту інформації основна увага зосереджена на критичних та високопріоритетних загрозах, оскільки саме вони становлять найбільший ризик для безперервної діяльності приміщення та безпеки даних. Їм буде приділено першочергову увагу як у технічному, так і в організаційному аспектах — через впровадження сучасних рішень, контроль доступу, резервне живлення, політики інформаційної безпеки тощо. Окремі специфічні загрози, які не охоплюються загальними рішеннями або потребують індивідуального підходу, будуть розглянуті додатково в подальших етапах проєкту. Таким чином, підхід до побудови системи захисту буде комплексним, з акцентом на найнебезпечніші фактори, без ігнорування менш критичних, але потенційно ризикованих аспектів.

Разом з цим, більшість інших загроз середнього та низького рівня будуть повністю або частково усунені завдяки цим самим заходам.

Тож як і було вище згадано першочергово ми займемося вирішенням загроз із критичним приірітетом. На момент аналізу інформаційної інфраструктури приміщення було виявлено низку критичних недоліків, що стосуються побудови мережі, її захисту та організації доступу. Зокрема, на приміщенні відсутня сегментована мережева структура, немає ізольованих підмереж для різних відділів, а також не передбачено використання фаєрволів для обмеження та контролю міжмережевої взаємодії. Усі робочі місця підключені без загальної

схеми кабельного розведення, а в окремих зонах доступ до інтернету здійснюється виключно через загальнодоступний Wi-Fi, що створює серйозні ризики компрометації даних та велеки навантаження на мережу що значно зменьшує продуктивність приміщення.

У зв’язку з цим необхідно повністю перепроєктувати мережеву архітектуру, щоб забезпечити належний рівень інформаційної безпеки. Основою майбутньої мережі стане організація окремої корпоративної мережі із сегментуванням, яка передбачає розподіл структури на логічно ізольовані зони: підмережа менеджерів та бухгалтерів, підмережа розробників, підмережа директора та технінч мережа. Кожен із цих сегментів буде ізольований із встановленим режимом доступу що дозволить централізовано контролювати трафік між зонами, обмежувати доступ лише необхідним службам і користувачам, а також вчасно виявляти аномальну активність чи вторгнення. Для уніфікації та зручного адміністрування інфраструктури, ми впровадили єдину політику іменування пристроїв та сервісів. У межах цієї політики використовується глобальний простір імен для фізичного офісу, в якому всі імена обладнання, систем та служб мають стандартний префікс ARES.

Для зручності проєктування та подальшого розгортання інфраструктури було створено візуальну схему мережі в Cisco Packet Tracer. Вона відображає логічну архітектуру приміщення з поділом на сегменти та чіткою маршрутизацією між ними. Це дозволяє швидко ідентифікувати ресурси, їхнє розташування та належність до офісної інфраструктури, а також спрощує навігацію в системах моніторингу, обліку та керування. Також сегмент серверів (позначений зеленою зоною) повністю розміщений у хмарному середовищі Amazon Web Services. Усі компоненти цього сегмента — такі як сервери Arkime, Security Onion, File Server, Backup Camera Server, а також маршрутизатор і комутатор — є віртуальними. Вони об'єднані у відокремлену приватну підмережу (VPC) із захищеним VPN-з'єднанням до фізичної офісної мережі. На рисунку 3.1. Ми наглядно можемо бачити розроблену схему в Cisco Packet Tracer

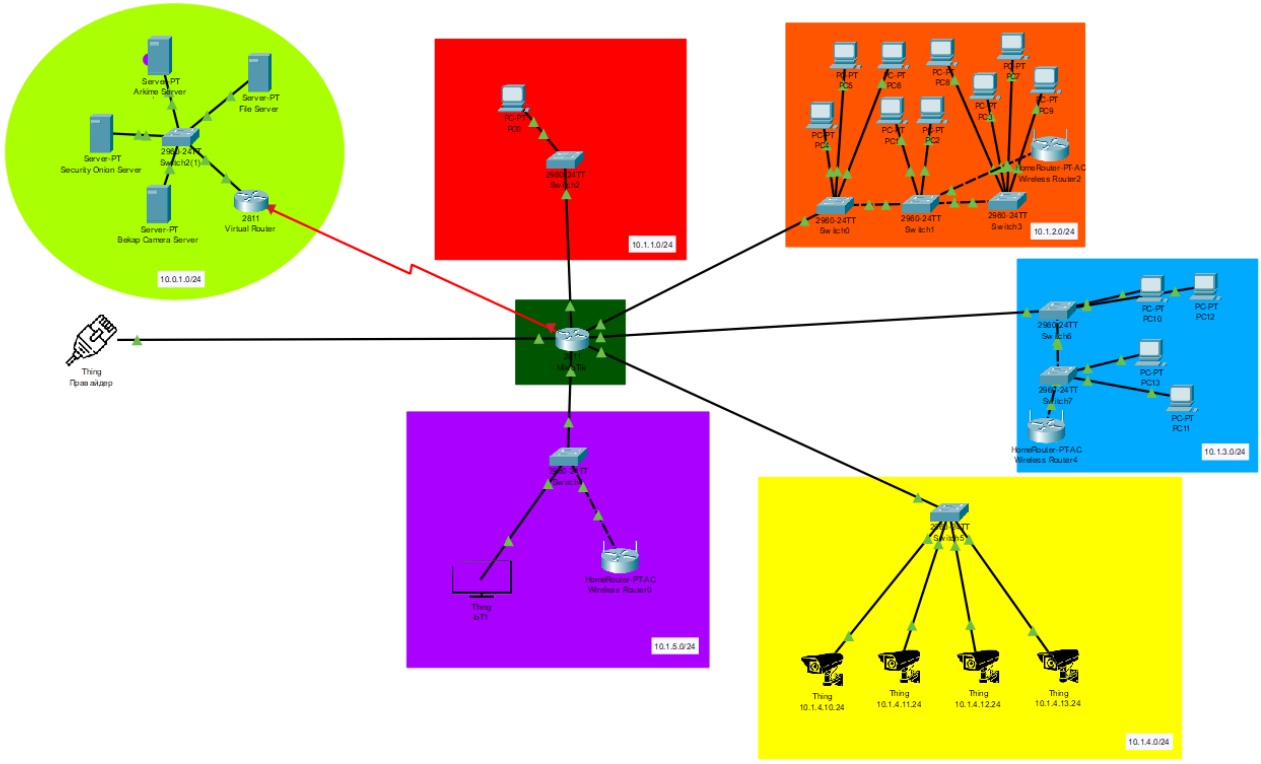


Рисунок 2.3 – Схема мережі розроблена в Cisco Packet Tracer

У центрі знаходиться маршрутизатор MikroTik, який виконує роль центрального маршрутизатора між усіма сегментами. Через нього реалізовано доступ між підмережами згідно з політиками фаєрвола.

Схема не лише дозволяє наочно зрозуміти логіку побудови мережі, а й стане практичним інструментом при реалізації фізичної інфраструктури: від прокладання кабелів до налаштування маршрутизації та безпеки.

Для мінімізації ризиків, пов’язаних із вразливим розташуванням мережевого обладнання, було прийнято рішення реалізувати низку технічних заходів. Насамперед створюється окреме серверне приміщення, яке дозволить ізолювати критичне обладнання від загального офісного простору, забезпечивши контрольований доступ виключно для уповноважених осіб. Це значно знижує ймовірність несанкціонованого втручання чи випадкового пошкодження.

Додатково, для фізичного захисту серверів та іншого мережевого обладнання передбачено використання серверної шафи яку ми можемо бачити на рисунку 2.4. Вибір пав на модель 6U 19" 530x400x300 мм (GWMSN-6U) це бюджетне рішення з базовими функціями, підходить для невеликого обсягу

обладнання та обмеженого бюджету. Вона не лише ускладнить фізичний доступ до техніки, а й сприяє правильній організації кабельної інфраструктури, вентиляції та підтримці порядку в системі.

Рисунок 2.4 – Серверна шафа[36].

Сама шафа буде обладнана наступпними приладами:

MikroTik rb2011il-IN (рисунок 2.5) було прийнято було обрати саме його оскільки він поєднує в собі широкий функціонал, достатню продуктивність і гнучкі можливості налаштування за доступну ціну. Пристрій має 5 портів Fast Ethernet і 5 портів Gigabit Ethernet, підтримує VLAN, фаєрвол, VPN та інші функції, необхідні для побудови безпечної мережі. Завдяки RouterOS він дозволяє реалізувати складну логіку маршрутизації та контроль трафіку, що робить його ефективним і економічним ядром мережевої інфраструктури бізнесу.

Рисунок 2.5 – MikroTik rb2011il-IN [37].

Комутатор Tp-Link PoE, TL-sg1005lp (рисунок 2.6) є доцільним вибором для побудови захищеної мережевої інфраструктури, оскільки забезпечує живлення PoE-пристроїв без потреби у додаткових блоках живлення, що спрощує монтаж і підвищує надійність. Він має достатню кількість портів для офісу (5 портів Gigabit Ethernet), підтримує автоматичне визначення споживання енергії, компактний і доступний за ціною, що робить його оптимальним рішенням для ефективної організації локальної мережі в умовах обмеженого бюджету.

Рисунок 2.6 – Комутатор Tp-Link PoE, TL-sg1005lp [38].

При виборі джерела безперебійного живлення вибір пав на energenie basic 850 va (eg-ups-b850) (рисунок 2.7) так як це є вдалим вибором як джерело безперебійного живлення для системи захисту інформації приміщення, оскільки має достатню потужність для підтримки роботи критичних компонентів (сервер, маршрутизатор, комутатор) під час короткочасних перебоїв з електропостачанням. Пристрій також забезпечує базовий захист від стрибків напруги завдяки функції AVR, є доступним за ціною та простим у встановленні, що робить його оптимальним рішенням за співвідношенням ціна/якість для офісної IT-інфраструктури з помірним навантаженням.

Рисунок 2.7 – Energenie basic 850 va (eg-ups-b850) [39].

Такий підхід забезпечує надійний рівень захисту від як внутрішніх, так і зовнішніх загроз фізичного характеру.

Додатково, усі робочі місця повинні бути оснащені дротовим підключенням до локальної мережі за допомогою Ethernet-кабелів. Це дозволить забезпечити стабільність з’єднання, високі швидкості передачі даних і, головне, значно підвищити рівень захисту порівняно з бездротовими підключеннями, які схильні до перехоплення. Для реалізації цього завдання необхідно здійснити повний кабель-менеджмент — прокладання структурованої кабельної системи з маркуванням, у підлогових коробах, що також спростить подальше обслуговування та масштабування мережі. Додатково, в межах реалізації структурованої кабельної системи кожне приміщення приміщення було оснащене окремими мережевими комутаторами, що забезпечують дротове підключення всіх робочих місць через Ethernet. Це рішення дозволяє гарантувати високу стабільність з’єднання, максимальну пропускну здатність для внутрішньої комунікації та, що найважливіше, — підвищений рівень захисту порівняно з бездротовими технологіями, які залишаються вразливими до перехоплення сигналу.

У відділі розробників, де часто використовуються мобільні пристрої для тестування, а також необхідна гнучкість у підключенні, планується встановлення захищеної Wi-Fi мережі а саме Mikrotik wAP ac (RB-wAPG-5HacT2HnD) (рисунок 2.8) з фільтрацією доступу за MAC-адресами.

Рисунок 2.8 – Mikrotik wAP ac (RB-wAPG-5HacT2HnD) [40].

Окрема гостьова Wi-Fi мережа буде створена у відділі, де розміщуються бухгалтери та менеджери. Гостьова мережа буде повністю ізольована від внутрішніх корпоративних ресурсів, матиме обмежений доступ лише до зовнішнього інтернету та буде функціонувати за окремими правилами безпеки. Такий підхід дозволить надавати інтернет-доступ стороннім особам (наприклад, підрядникам або гостям компанії) без ризику компрометації основної мережі, а також запобігатиме витоку конфіденційної інформації чи впливу на внутрішні системи.

Також у рамках побудови ефективної системи захисту інформації потрібно призначити відповідальну особу (інженер з безпеки) за систематичний моніторинг і технічне обслуговування інформаційного обладнання. Для інженера з безпеки необхідно розробити проєкт посадової інструкції який має включати перелік функціональних обов’язків, вимог до кваліфікації, а також опис зони відповідальності, зокрема:

– здійснення щоденного моніторингу мережевого обладнання, серверів і систем зберігання даних;

– виявлення та усунення технічних збоїв, апаратних і програмних помилок;

– реагування на інциденти інформаційної безпеки згідно з внутрішніми протоколами;

– своєчасне оновлення операційних систем і мережевого програмного забезпечення;

– організація і контроль резервного копіювання критично важливої інформації;

– проведення аудиту дій користувачів для виявлення порушень політики інформаційної бепеки;

– контроль доступу до іт-ресурсів компанії відповідно до ролей і повноважень;

– участь у розробці й впровадженні нових засобів захисту та процедур кібербезпеки;

– підготовка звітності щодо технічного стану іт-інфраструктури та інцидентів безпеки;

– підвищення обізнаності персоналу з питань інформаційної безпеки (за необхідності);

– взаємодія з зовнішніми підрядниками або техпідтримкою щодо обслуговування обладнання.

Не рекомендуєця сумісництво даної посади із іншими технічними посадами компанії зокрема з розробниками, деректором тощо. Так як на даний момен обслуговуванням мережі та контролем за інформаційною системою займалися працівники відділу розробки, які не мали належної кваліфікації в цій сфері. Це призводить до помилок, затримок у реагуванні на проблеми та відволікало розробників від їх основної роботи. Тож призначення такої особи є критично важливим для підтримання сталої роботи системи захисту інформації та оперативного реагування на потенційні загрози, що можуть виникати в ході повсякденної діяльності приміщення. Таким чином, реалізація вищезазначених

заходів не лише усуне наявні загрози, а й створить надійну інфраструктурну основу для подальшої побудови системи захисту інформації, яка відповідатиме вимогам сучасної кібербезпеки для комерційного приміщення.

Запропоновані заходи комплексно захищають компанію від потенційних загроз. Сегментована мережева архітектура із розподілом підмереж ізолює критично важливі відділи та обмежує доступ стороннім особам, що запобігає внутрішнім порушенням. Фізичне захист серверного обладнання, включаючи пломбування шафи та контрольований доступ, не дозволяє несанкціоноване втручання з боку співробітників чи випадкових осіб. Для протидії зовнішнім загрозам впроваджено використання фаєрволів та VPN-з'єднання, що унеможливлює прямі атаки через інтернет та запобігає несанкціонованому доступу хакерів. Аудит логів і моніторинг активності дозволяють оперативно виявляти спроби вторгнень та реагувати на них. Впровадження двофакторної аутентифікації та фільтрації доступу забезпечує захист мережі від фішингових атак та соціальної інженерії. Завдяки комплексному підходу до кіберзахисту, компанія матиме надійну основу для подальшого розвитку, мінімізуючи ризики компрометації інформації та забезпечуючи безперебійну діяльність. Для ефективного реагування на загрози з високим пріоритетом, приміщення має вжити низку послідовних технічних та організаційних заходів, що підвищать стійкість інформаційної інфраструктури до зовнішніх і внутрішніх впливів, мінімізуючи ризики втрати даних, збоїв у роботі або компрометації інформації.

Однією з ключових загроз є відключення електроенергії через удари по енергосистемі (ВЗТ13). У разі втрати живлення, особливо в умовах воєнного стану чи надзвичайних ситуацій, приміщення може втратити доступ до критичних систем. Для усунення цієї загрози передбачається встановлення системи резервного електроживлення, зокрема джерел безперебійного живлення для серверного та мережевого обладнання. Крім того, буде організовано підключення до аварійної лінії живлення, що дозволить підтримувати роботу офісу або хоча б базових комунікацій у кризовій ситуації.

Ще однією потенційно небезпечною загрозою є ракетний остріл, вибухова хвиля, стихійні лиха та техногенні катоастрофи (ВЗТ8, ВЗП1, ВЗП2, ВЗП3). Незважаючи на те, що подібні події є поза сферою контролю приміщення, можливо зменшити їх наслідки шляхом розробки чіткого плану евакуації, який включає основні та запасні шляхи виходу з будівлі, місця збору, а також інструкції дій для всього персоналу. Цей план має бути доведений до кожного співробітника та періодично перевірятися під час навчань.

Загроза вразливого розташування мережевого обладнання (ВЗТ6) вже була усунута в межах заходів, запланованих для критичних загроз. Йдеться про створення окремої серверної кімнати, захищеної фізично та електрично, із правильним кабель-менеджментом та відповідним рівнем доступу.

Загрози ураження вірусами (ВЗТ1) та включення до програмного забезпечення шкідливих елементів, таких як троянські програми, фішинг, логічні бомби тощо (НТК4) потребують комплексного реагування. Прийнято рішення встановити систему моніторингу мережевого трафіку, обравши Arkime та Security Onion як основні інструменти. Arkime дозволяє детально аналізувати мережевий трафік, що дає змогу швидко виявляти потенційні загрози та спроби несанкціонованого доступу. Security Onion, у свою чергу, є комплексним рішенням для аналізу логів, реагування на кіберзагрози та контролю внутрішньої безпеки. Разом ці системи забезпечують деталізований моніторинг активності в мережі, що значно підвищує ефективність реагування на можливі атаки та мінімізує ризики порушення інформаційної безпеки. Запровадження цих рішень гарантує підприємству стабільність і кращий рівень захисту даних.

У випадку вербування персоналу (НТК1) основним методом протидії є підвищення обізнаності та впровадження чітких політик безпеки. Передбачається заборона використання персональних пристроїв, акаунтів, знімних носіїв та зовнішніх хмарних сховищ у межах корпоративного середовища. Також буде організовано навчання персоналу з питань кібергігієни, соціальної інженерії та внутрішньої безпеки, що допоможе зменшити ризик втрати інформації через людський фактор. Менеджер з безпеки контролює виконання правил кіберзахисту

та організовує заходи з підвищення обізнаності співробітників щодо кібергігієни. Він стежить за доступом до систем, аналізує загрози та проводить тренінги, щоб мінімізувати ризики компрометації даних. Ще однією важливою загрозою є розкрадання матеріальних носіїв інформації, включно з виробничими відходами (НТК9). Для її усунення планується встановлення системи відеоспостереження з функцією довготривалого збереження відеоархіву. Важливо, що доступ до камер та архівів відеозаписів обмежується і підлягає логуванню, що унеможливлює несанкціоноване видалення чи перегляд навіть із боку керівного персоналу. Таким чином, захист буде забезпечено навіть у разі порушення з боку посадової особи на зразок директора або системного адміністратора. Буде встановлено чотири камери відеоспостереження моделі Hikvision DS-2CD1123G2-IUF які представленні на рисунку 2.9.

Рисунок 2.9 – Камери Hikvision [41].

Дві камери будуть розміщені в публічній зоні щоб охоплювати головний вхід, вхід в кабінет до деректора та загальний простір, що дозволяє фіксувати пересування гостей, працівників і прибиральниці. Камера в кабінеті менеджерів та бухгалтерів — забезпечує контроль над простором, де можуть оброблятися

конфіденційні документи. І остання камера буде в кабінеті розробників — для фіксації роботи з технікою, захисту обладнання та наглядом за серверною кімнатою. Камери відеоспостереження повині бути розміщені таким чином, щоб забезпечити контроль зон із критично важливим обладнанням, не порушуючи приватність співробітників. Вони не мають захоплювати монітори та клавіатури, що мінімізує ризик витоку даних через відеозаписи, водночас покриваючи всі ділянки, де можливий доступ до мережевої інфраструктури. Це дозволить зберігати баланс між безпекою та конфіденційністю.

Для забезпечення належного рівня фізичної безпеки в офісі приміщення необхідно впровадити систему контролю доступу до приміщень на основі електронних замків і персоналізованих карт доступу. Така система дозволить обмежити переміщення працівників лише тими зонами, які безпосередньо пов’язані з їх службовими обов’язками, а також забезпечить журналювання входів/виходів для подальшого аудиту. Згідно з принципами розмежування доступу працівники відділу розробки повинні мати доступ виключно до кабінету №3, який визначено як їх робочу зону, менеджери та бухгалтери повинні мати доступ лише до кабінету №2, що відповідає їх функціональній зоні. Доступ до серверної кімнати надається виключно відповідальному спеціалісту, який обслуговує IT-інфраструктуру. Це дозволяє не лише обмежити ризики несанкціонованого доступу, але й виключає можливість випадкового або навмисного втручання в роботу критичних елементів системи.

Запропоновано було два варіанти електроних замків. Aqara N100 (рисунок 2.10) він має тип доступу: RFID-картки / PIN-коди / Bluetooth (через телефон). Також є підтримка аварійного відкриття у разі збоїв живлення.

Рисунок 2.10 – Замок Aqara N100 [42]

У якості альтернативного рішення для контролю доступу може бути використано ZKTeco ML10/ID (рисунок 2.11) . Це електронний замок, який підтримує відкривання за допомогою відбитків пальців і RFID-карток, що забезпечує зручний і надійний спосіб ідентифікації. Він не потребує підключення до мережі або додаткового обладнання, що робить його ідеальним варіантом для малих офісів.

Рисунок 2.11 – Замок ZKTeco ML10/ID [43].

Для уніфікації та зручного адміністрування інфраструктури, ми впровадили єдину політику іменування пристроїв та сервісів. У межах цієї політики використовується глобальний простір імен для фізичного офісу, в якому всі імена обладнання, систем та служб мають стандартний префікс ares-. Це дозволяє швидко ідентифікувати ресурси, їхнє розташування та належність до офісної інфраструктури, а також спрощує навігацію в системах моніторингу, обліку та керування.

Отже, запропоновані рішення дозволять знизити ймовірність реалізації загроз високого рівня та зменшити потенційні наслідки для приміщення, забезпечуючи стабільну та безпечну роботу навіть в умовах зовнішнього тиску чи внутрішніх порушень.

Для уніфікації та зручного адміністрування інфраструктури, ми впровадили єдину політику іменування пристроїв та сервісів. У межах цієї політики використовується глобальний простір імен для фізичного офісу, в якому всі імена обладнання, систем та служб мають стандартний префікс ares-. Це дозволяє швидко ідентифікувати ресурси, їхнє розташування та належність до офісної інфраструктури, а також спрощує навігацію в системах моніторингу, обліку та керування.

Ми використаємо таку політику імен для пристроїв буде обраний глобальний простір імен для фізичного офісу і всі назвиобладнання налаштування назви сервісів буде включати дану незву як префікс

2.6. Висновок

У другому розділі було здійснено систематичне проєктування системи захисту інформації для комерційного приміщення. Проаналізовано інформаційні потоки в межах організації, ідентифіковано критичні вузли та канали передачі даних. Побудовані моделі загроз та порушників дозволили визначити потенційні вектори атак та оцінити вразливості інформаційної інфраструктури. На основі

зібраної інформації розроблено архітектуру системи захисту, що включає захищену локальну мережу, систему контролю доступу, резервне копіювання, моніторинг, міжмережеві екрани та інші засоби безпеки. Запропоновані рішення враховують обмежені ресурси приміщення, забезпечуючи при цьому достатній рівень захищеності, масштабованість та простоту у впровадженні

.

3 ОЦІНКА СПРОЄКТОВАНОЇ СИСТЕМИ ЗАХИСТУ, СТВОРЕННЯ НАСТАНОВ ЩОДО ЇЇ ВПРОВАДЖЕННЯ ТА ЕКСПЛУАТАЦІЇ.

3.1 Імплементація спроєктованої системи захисту інформації на приміщенні

На основі рішень, зазначених у попередньому розділі, перейдемо до етапу безпосередньої імплементації та фізичної реалізації, впровадження спроєктованих рішень. Відповідно до поставлених задач кваліфікаційної роботи, перейдемо до впровадження спроєктованих рішень.

Впровадження безпекових рішень буде відбуватися у такій ж послідовності, як вони були описанні у попередньому розділі. Згідно цього, розпочнемо з перебудови мережевої архітектури, кабельменеджменту та організації серверної шафи офісу.

У межах реалізації оновленої інфраструктури приміщення було впроваджено нову архітектуру корпоративної мережі, яка поєднує як фізичні, так і віртуальні компоненти. В її основі — логічний поділ на окремі ізольовані підмережі, зокрема для кабінету менеджерів і бухгалтерії, розробників, директора, технічного сегменту та мережі камер відеоспостереження. Всі підмережі функціонують незалежно одна від одної, без прямого міжмережевого доступу, що реалізовано за допомогою міжмережевих екранів (фаєрволів) та ретельно налаштованих правил маршрутизації. Це дозволяє не лише чітко регламентувати доступ до ресурсів відповідно до ролей і повноважень, але й значно зменшити ризики горизонтального поширення внутрішніх загроз у разі компрометації окремих вузлів.

У хмарному середовищі Amazon Web Services було розгорнуто віртуальну серверну інфраструктуру, на якій встановлено та налаштовано системи Arkime, Security Onion, файловий сервер та інші прикладні сервери, панель керування віртуальними серверами Амазон ми можемо бачити на рисунку 3.1. Рішення приймалося з урахуванням необхідності забезпечення гнучкого масштабування, високої доступності,можливості легкого розгортання нових серверів в

майбутньому а також централізованого моніторингу безпеки у віддаленому середовищі.

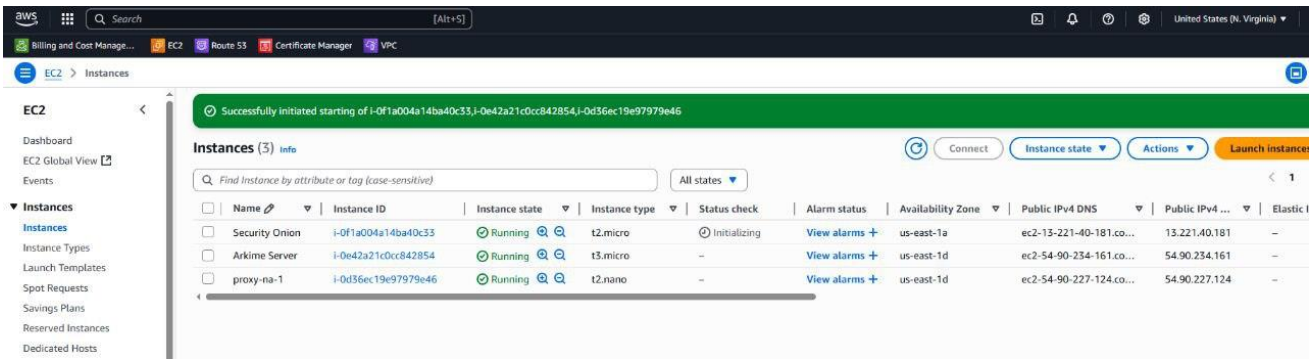
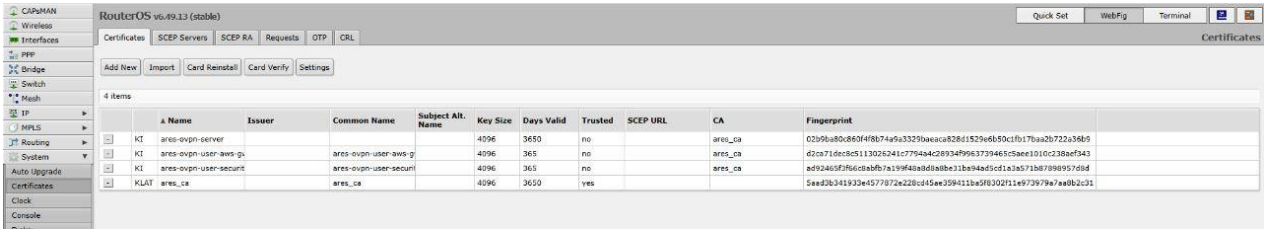


Рисунок 3.1 – Панель керування віртуальними серверами Амазон (сервіс EC2)

Комунікація внутрішньої корпоративної мережі із хмарною приватною мережею відбуватиметься за допомогою протоколу OpenVPN, що дозволить створити єдиний мережевий простір із захищеним шифрованим з'єднанням. У випадку якщо в компанії з'являться нові офіси, вони можуть бути так само легко інтегровані в існуючу віртуальну приватну мережу.

Налаштування віртуальної приватної мережі складається з двох компонентів: сервера та клієнтів. У нашому випадку, сервер буде розміщений безпосередньо на роутері MikroTik, оскільки дане обладнання за замовчуванням має все для реалізації даного функціоналу. Клієнтська частина працюватиме на окремому інстансі в інфраструктурі Amazon Web Services. Для забезпечення високого рівня захищеності з'єднання, аутентифікація відбуватиметься за двома факторами: логіном та паролем, а також за файловим ключем, підписаним сервером. З цією метою на сервері буде створено новий самопідписаний кореневий сертифікат (рисунок 3.2),



Рисунрк 3.2 – Самопідписаний кореневий сертифікат

Для клієнтів VPN буде створена окрема підмережа «10.100.0.0/24», з працюючим DHCP сервером, дивитися на рисунку 3.3.

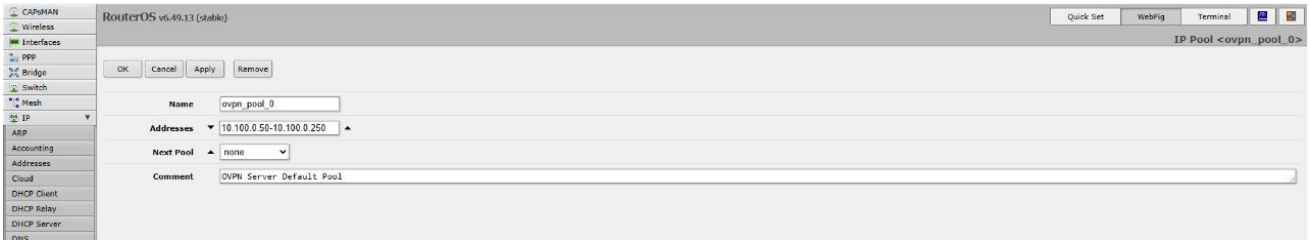


Рисунок 3.3 – Окрема підмережа для клієнтів.

Система Arkime була встановлена як основний засіб захоплення, індексації та аналізу мережевого трафіку. Вона дозволяє здійснювати детальний перегляд пакетів, будувати хронологію мережевої активності, а також виявляти аномальні з'єднання або ознаки потенційного зловмисного трафіку. Для повноцінного функціонування Arkime було налаштовано відповідні мережеві інтерфейси з можливістю пасивного прослуховування трафіку в режимі реального часу дивитися на рисунку 3.4.

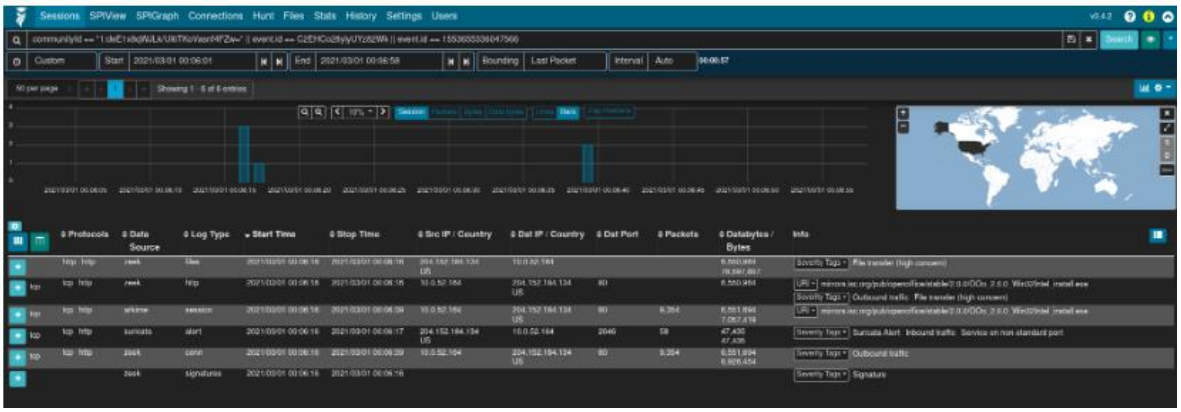


Рисунок 3.4 – Робота Arkime

Паралельно з цим, у тій самій AWS-інфраструктурі було впроваджено систему Security Onion (рисунок 3.5) — комплексне рішення з виявлення вторгнень (IDS), обробки логів і реагування на інциденти інформаційної безпеки. Security Onion інтегрує інструменти, такі як Suricata, Zeek, Wazuh, TheHive та

Kibana, що дозволяє здійснювати повний цикл обробки подій безпеки: від збору логів і мережевого аналізу — до аналітики, візуалізації і триажу інцидентів.

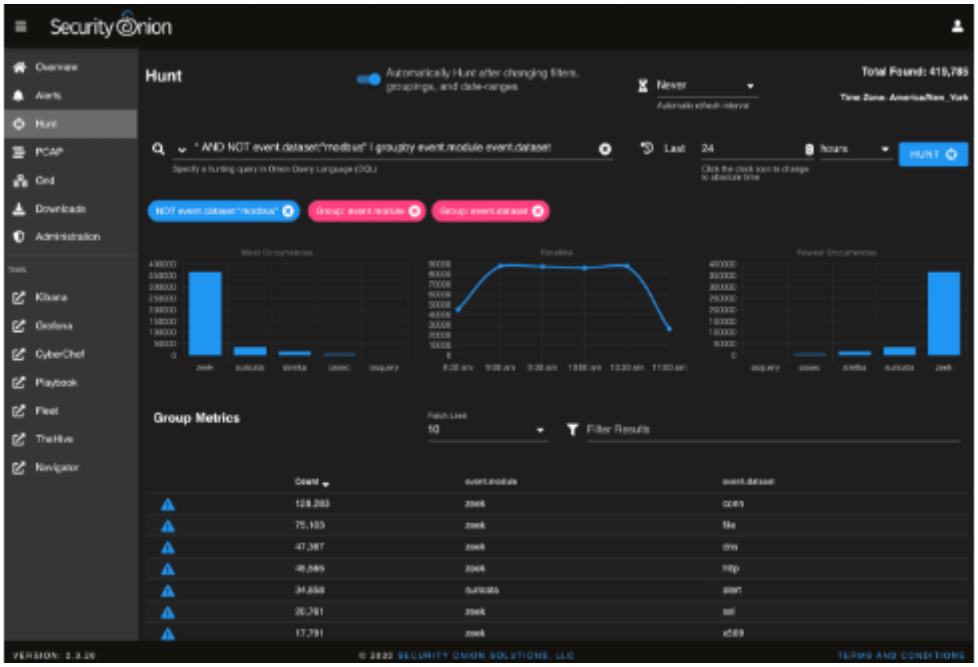


Рисунок 3.5 – Security Onion.

Обидві системи — Arkime і Security Onion — були об'єднані в єдиний захищений середовищем VPN (OpenVPN) доступ, який забезпечує безпечне з'єднання для адміністраторів та аналітиків, що здійснюють моніторинг та керування. VPN-інфраструктура гарантує шифрування всього адміністративного трафіку, обмеження доступу за IP-адресами та реалізацію додаткових заходів автентифікації, що знижує ризик несанкціонованого доступу до критичних систем.

У приміщенні облаштовано серверну кімнату з обмеженим фізичним доступом. Встановлено серверну шафу з необхідним обладнанням: маршрутизатор MikroTik RB2011iL-IN, PoE-комутатор TP-Link TL-SG1005LP та UPS EnerGenie Basic 850 VA. Таке рішення забезпечує надійний фізичний захист та ефективне функціонування інфраструктури навіть у разі перебоїв з електропостачанням. Вже встановлену та обладнану шафу можемо бачити на (рисунок 3.6).

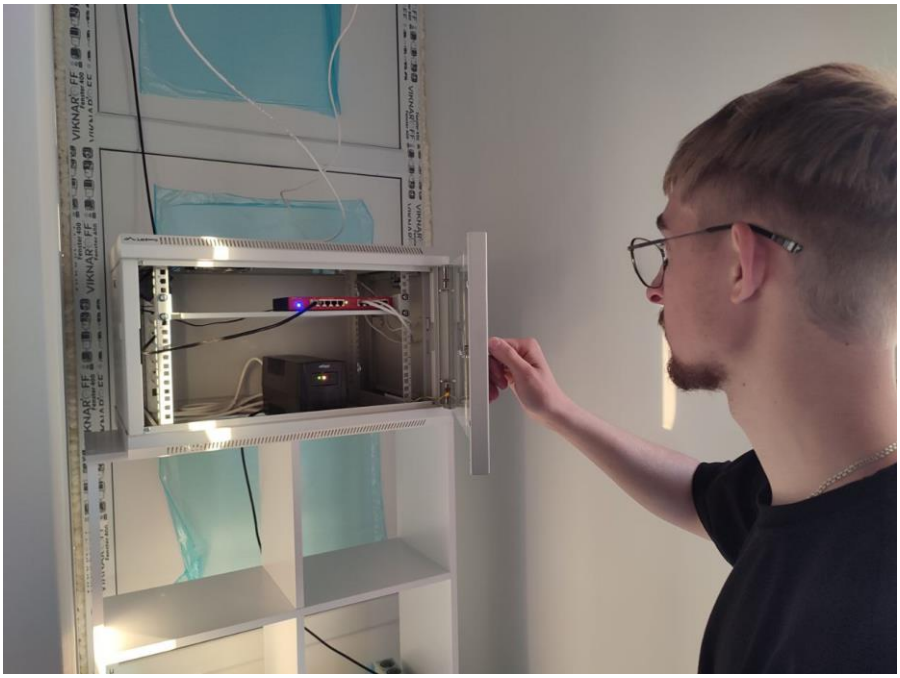


Рисунок 3.6 – Обладнана серверна шафа.

Також, в кожен із кабінетів було встановлено кумутатор TP-Link TL-SF1005D для забезпечення робочих місць підключенням до мережі. В ході імплементації в початкву схему мережі були внесенні коретктиви в тому що у кабінеті розробників було встановлено три комутатора а не один як планувалося. Таке рішеня було прийнято у звязку з тим що на приміщенні були комутатори які підходили нам для виконання поставленої задачі. Наглядно введені зміни ми можемо бачити на рисунку 3.7.

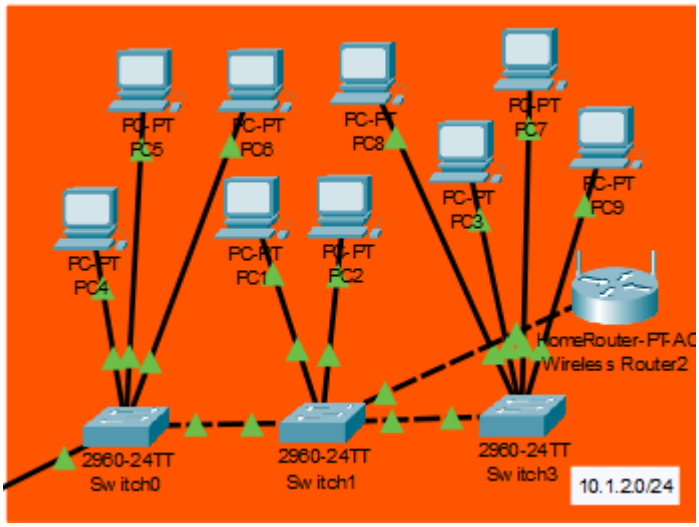


Рисунок 3.7 – Зміни в схемі мережі

Усі робочі місця підключені до локальної мережі через Ethernet. Було виконано структуроване прокладання кабелю з маркуванням і укладанням у підлогові канали. Це забезпечує не лише стабільне з’єднання, але й високий рівень безпеки в порівнянні з бездротовими технологіями.

У відділі розробників встановлено точку доступу MikroTik wAP ac (RB-wAPG-5HacT2HnD) з фільтрацією MAC-адрес. Також створено окрему гостьову мережу на точці доступу яка знаходиться у віділі менеджерів та бухгалтерів, вона буде ізольована від внутрішніх ресурсів, яка надає лише доступ до інтернету для відвідувачів. І третю точку доступу встановлено в публічній зоні і розміщено в технічній мережі так як в подальшому планується використання безпровідних технологій на приміщенні. На рис3.8. можна бачити встановлення точки доступу.

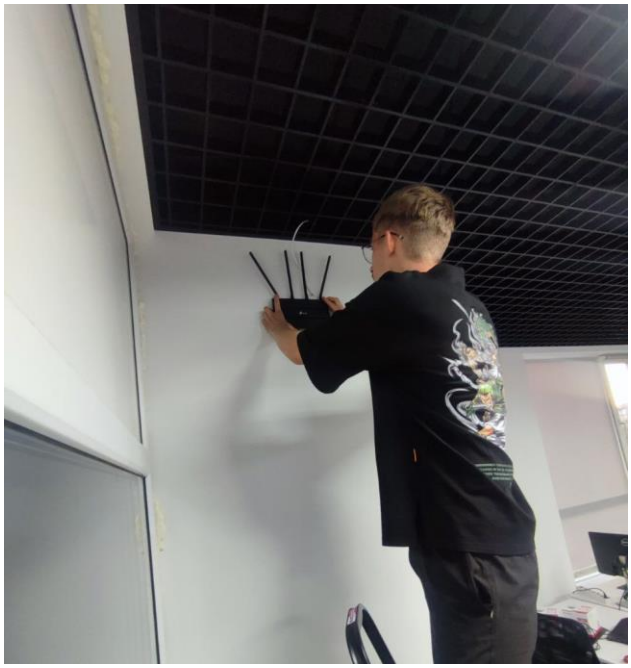


Рисунок 3.8 – Встановлення точки доступу

Було також призначено відповідальну особу — менеджера з безпеки, який відповідає за моніторинг, технічне обслуговування, аудит користувачів, резервне копіювання, оновлення програмного забезпечення та реагування на інциденти. Розроблено та затверджено посадову інструкцію з чітким переліком функціональних обов’язків. Зазначені вище заходи вже впроваджено в рамках

внутрішньої політики інформаційної безпеки, це значно підвищить надійність та стабільність роботи інформаційної інфраструктури.

Для забезпечення безперервної роботи обладнання підключено UPS. Розроблено та доведено до працівників план евакуації у разі надзвичайних ситуацій, з визначенням маршрутів, місць збору та відповідальних осіб.

Встановлено чотири камери Hikvision DS-2CD1123G2-IUF які ми можемо бачити на рис 3.9. Розміщені вони у приміщеннях бухгалтерії, розробників і дві в загальній зоні. Система налаштована так, щоб уникати зйомки моніторів та клавіатур.

Рисунок.3.9 – Камери Hikvision

Відеоархів доступний лише уповноваженим особам, всі дії логуються. У рамках забезпечення безпеки відеоспостереження та захисту конфіденційних даних на приміщенні було реалізовано окрему ізольовану підмережу для камер відеоспостереження. Усі камери фізично та логічно відокремлені від загальної офісної та технічгої мереж, що мінімізує ризики несанкціонованого доступу чи зовнішніх атак.

Мережа камер захищена фаєрволом, який повністю блокує будь-які зовнішні або внутрішні спроби доступу з інших сегментів мережі приміщення.

Доступ до відеопотоків та налаштувань камер здійснюється лише через фаєрвол, виключно з внутрішнього офісу, з попередньо визначеної IP-адреси, яка належить інженеру з безпеки. Доступ захищений багаторівневою автентифікацією, зокрема через VPN-з'єднання та облікові дані з ротацією паролів.

Архіви відеозаписів та резервні копії системи спостереження автоматично зберігаються на окремому виділеному сервері у хмарному середовищі Amazon Web Services. Даний сервер має обмежений доступ — тільки з IP-адреси офісу інженера з безпеки або зі спеціального адміністративного Virtual Private Network. Сервер конфігуровано в режимі «тільки для запису» для процесу копіювання, що унеможливлює несанкціоноване втручання в архівні дані. Для підвищення безпеки використано S3 Bucket з політиками Identity and Access Management, які дозволяють доступ лише визначеним сервісам і обліковим записам.

Крім того, всі дії з доступом до відеосистеми та архівів логуються і регулярно аналізуються з метою виявлення підозрілої активності або спроб порушення політик доступу.

Заключним етапом потрібно впровадити систему контролю доступу на базі електронних замків ZKTeco ML10/ID їх було обрано завдяки їхній автономності, надійності та підтримці кількох способів автентифікації: біометричної (відбиток пальця), карткової (RFID) та механічного ключа. Крім того, вони не потребують постійного з’єднання з мережею чи додаткових контролерів, що суттєво спрощує їх встановлення та експлуатацію. Установка таких замків передбачена на дверях до кабінету розробників, кабінету менеджерів і бугалтерів та кабінету деректора.

Таким чином, було завершено імплементацію спроєктованих рішень. Далі можемо перейти до оцінки затрачених та потенційно необхідних ресурсів, а також створення настанов щодо експлуатації та можливої модернізації системи захисту інформації приміщення.

3.2 Оцінка необхідних ресурсів та вартості впровадження системи захисту інформації приміщення.

Реалізація системи захисту інформації потребує як одноразових капіталовкладень, так і постійних операційних витрат. Далі буде оцінено загальні витрати, включаючи вартість обладнання, програмного забезпечення, хмарної інфраструктури, заробітної плати відповідального фахівця та резервного фонду для покриття потенційних непередбачених витрат. Вартість обладнання наведено в таблиці 3.1:

Таблиця.3.1. – Вартість обладнання

Компонент	Кількість	Ціна за одиницю	Загалом
Маршрутизатор MikroTik RB2011iL-IN	1	4 000	4 000
PoE-комутатор TP-Link TL-SG1005LP	1	1 500 грн	1 500 грн
UPS EnerGenie Basic 850 VA	1	2 500 грн	2 500 грн
Комутатори TP-Link TL-SF1005D	6	Були в наявності	Були в наявності
Точки доступу MikroTik wAP ac	3	3 000 грн	9 000 грн
Камери Hikvision DS-2CD1123G2-IUF	4	3 300 грн	13 200 грн
Серверна шафа	1	4 363 грн	4 363 грн
Електронні замки ZKTeco ML10/ID	3	4 620 грн	13 860 грн

Загальні витрати на обладнання склали: 48 423 грн.

Також при впровадженні мережевої інфраструктури приміщення були здійснені додаткові витрати на закупівлю та монтаж кабельної продукції. Зокрема:

– вартість кабелю (60 метрів): 3 360 грн;

– конектори для з’єднання (120 одиниць): 300 грн.

Загальна вартість придбаного обладнання для впровадження системи захисту інформації на приміщенні склала 52 083 грн. До цієї суми входить закупівля маршрутизаторів, комутаторів, точок доступу, UPS, камер відеоспостереження та електронних замків, необхідних для забезпечення фізичної та мережевої безпеки. Обладнання було підібрано з урахуванням балансу між надійністю, функціональністю та вартістю.

Хмарна інфраструктура, що включає віртуальні сервери, сховища даних та системи моніторингу безпеки, потребує щомісячної оплати. Витрати на Amazon Web Services:

– EC2-інстанси (сервери для Arkime, Security Onion та файлівий сервер) — 3 500 грн/міс.

– сховище S3 для резервного копіювання та відеоархіву — 2 000 грн/міс.

– мережава інфраструктура — 1 500 грн/міс.

Таким чином можемо порахувати що витрати на Amazon Web Services в місяць складатимуть близько 7 000 грн.

Виплата заробітної плати для інженера з безпеки у розмірі 40 000 грн/міс забезпечує необхідний рівень оплати для спеціаліста, який виконує моніторинг, аудит, резервне копіювання, налаштування інфраструктури, реагування на інциденти і тд.

Також будь-яка технічна інфраструктура може зіткнутися з аваріями або потребою в оновленні. Для покриття неочікуваних витрат закладено резервний фонд:

– можливі заміни обладнання, ремонт та оновлення — 20 000 грн/рік;

– додаткове програмне забезпечення та ліцензії — 10 000 грн/рік.

Загальні резервні витрати: 30 000 грн/рік

Враховуючи перелічені статті витрат, загальна вартість впровадження системи захисту інформації становить 52 083 грн одноразово на обладнання та монтаж. Щомісячні операційні витрати, включаючи хмарну інфраструктуру Amazon Web Services та заробітну плату інженера з безпеки, становлять 47 000 грн. Додатково передбачено 30 000 грн на рік на ремонт і неочікувані витрати для забезпечення стабільної роботи системи. Таким чином, загальні витрати у перший рік складають 646 083 грн, з яких основна частина припадає на оплату роботи інженера та підтримку хмарної інфраструктури. Надалі щорічні витрати будуть зменшені до рівня 594 000 грн, оскільки капітальні вкладення в обладнання вже здійснені.

Запропонований бюджет забезпечує стабільну роботу системи безпеки, її підтримку та оновлення, а також гарантує фінансову готовність до можливих технічних несправностей та неочікуваних витрат.

Таким чином, ми обчислили загальну вартість впровадження системи захисту інформації з урахуванням усіх ключових складових: одноразових витрат на обладнання та монтаж, щомісячних витрат на хмарні сервіси та заробітну плату фахівця, а також резервного фонду на випадок неочікуваних витрат. Отримані дані дозволяють точно оцінити фінансове навантаження та ефективно планувати подальші витрати на підтримку та розвиток інформаційної безпеки.

3.3 Створення настанов щодо впровадження та експлуатації системи захисту інформації приміщення.

Ефективна експлуатація системи захисту інформації неможлива без наявності чітко визначених процедур, рекомендацій та регламентів, які мають охоплювати всі аспекти роботи з інформаційною інфраструктурою. Створення настанов щодо впровадження та подальшої експлуатації дозволяє стандартизувати дії персоналу, зменшити ймовірність людських помилок і

забезпечити відповідність політикам безпеки. Нище розглянуто ключові організаційні та технічні заходи, які слід врахувати для підтримки системи в актуальному та працездатному стані, а також запропоновано шляхи її масштабування і вдосконалення.

Наприклад Amazon Web Services: дозволяє вкрай легко додавати нові прикладні сервери у хмарній інфраструктурі наприклад поштові сервери і тд, можна покращувати корпоративне серверне обладнання наприклад замінити мікротік на більш продуктивний роутер за не обхідності регулярно проводити навчальні заходи для працівників розробити процедуру введення в курс діла нових праціників.

Забезпечення захищеності інформаційної інфраструктури — це процес, який потребує постійного вдосконалення та адаптації до нових загроз і технологічних змін. Розглянемо можливі напрями розширення та модернізації системи.

Однією з ключових переваг використання хмарної інфраструктури Amazon Web Services є її гнучкість у розгортанні нових серверів та додаткових сервісів. Це дозволяє підприємству легко масштабувати свою інфраструктуру відповідно до зростаючих потреб. Наприклад, можна додати корпоративний поштовий сервер для централізованого управління електронною поштою, що забезпечить контроль доступу та захист листування. Також є можливість впровадити систему управління документацією, яка дозволить створити захищене сховище з гнучкими правами доступу для працівників. У хмарі можна розміщувати аналітичні сервіси, які допоможуть виявляти загрози інформаційної безпеки через розширені засоби моніторингу та аналізу мережевого трафіку.

Крім цього, можливе покращення корпоративного серверного обладнання. Якщо продуктивності маршрутизатора MikroTik буде недостатньо, його можна замінити на більш потужне рішення, наприклад, обладнання Cisco або Juniper, яке забезпечить кращу продуктивність і розширені можливості безпеки. Впровадження додаткових комутаторів із підтримкою VLAN допоможе більш детально сегментувати мережу, що підвищить рівень контролю доступу.

Локальне сховище можна розширити за рахунок впровадження NAS-систем для резервного копіювання та збереження критичних даних. З часом можна відокремити фаєрвол від роутера з метою підвищення швидкодії та продуктивності.

Окрему увагу слід приділити підвищенню рівня обізнаності співробітників. Регулярне проведення тренінгів з інформаційної безпеки дозволить працівникам краще розуміти загрози та запобігати інцидентам. Для нових працівників варто розробити адаптаційну програму, яка міститиме основні правила роботи з корпоративними системами безпеки, процедури автентифікації та політику доступу до даних. Щоб покращити захист критичних сервісів, необхідно впровадити політику двофакторної автентифікації для доступу до всіх важливих корпоративних ресурсів. Організаційні заходи з безпеки повині мати комплексний та систематичний характер зокрема підготовка та навчання працівників повині проводитись в плановому режепі з дотриманням певного графіку а не бути спорядичними та реактивними.

Також Регулярні аудити безпеки необхідні для виявлення нових вразливостей та загроз, які могли залишитися непоміченими під час попередніх перевірок. Вони дозволяють оцінити стан мережевої інфраструктури, перевірити конфігурацію фаєрволів, правила маршрутизації та політики доступу. Окрему увагу слід приділити аналізу прав користувачів та автентифікації, щоб запобігти несанкціонованому доступу. Періодичні перевірки фізичної безпеки, зокрема доступу до серверної, камер відеоспостереження та електронних замків, допоможуть мінімізувати ризики. Такий системний підхід забезпечує стабільність захисту інформації та адаптацію до нових загроз.

Щоб нові співробітникм швидко адаптувалися, має бути чітка процедура введення в курс справ. Спочатку він проходить ознайомчий брифінг, де дізнається про політики безпеки та правила доступу. Далі отримує інструкції щодо використання корпоративних ресурсів, а також тестується на знання ключових процедур. Під керівництвом наставника він налаштовує необхідні доступи та проходить практичне введення у робочий процес. Також передбачене періодичне

навчання та перевірка знань, що допомагає підтримувати високий рівень обізнаності про інформаційну безпеку.

Приміщення має розробити цілісну політику безпеки, яка об’єднає всі запропоновані заходи в єдиний документ. Вона регламентуватиме правила доступу, використання корпоративної мережі, оновлення програмного забезпечення та механізми автентифікації. У політиці повинні бути визначені процедури реагування на інциденти, аудит безпеки та навчання працівників. Чітке формулювання вимог і відповідальності допоможе мінімізувати ризики та підтримувати високий рівень захисту інформації.

Масштабування інфраструктури також стане необхідним у разі розширення приміщення. Якщо буде відкрито нові офіси, їх можна легко інтегрувати у корпоративну VPN-мережу через OpenVPN, забезпечуючи захищене з’єднання між філіями. Для забезпечення стабільного покриття в нових приміщеннях можна розгорнути додаткові точки доступу Wi-Fi, які підтримуватимуть ізольовані мережі для персоналу та гостей. Розширення системи моніторингу передбачає встановлення додаткових камер відеоспостереження та покращення логічної сегментації відповідних мереж.

Модернізація системи захисту інформаційної інфраструктури є необхідною умовою для її стабільної та безпечної роботи в умовах зростаючих викликів. Впровадження нових технічних рішень, підвищення рівня обізнаності персоналу та удосконалення організаційних заходів дозволяє створити комплексну, динамічну систему, здатну адаптуватися до змін у зовнішньому середовищі. Завдяки використанню гнучких хмарних сервісів і масштабованої мережевої архітектури, приміщення отримує змогу ефективно реагувати на нові потреби бізнесу, забезпечуючи водночас високий рівень захисту критичної інформації.

Підсумовуючи, створення настанов щодо впровадження та експлуатації системи захисту інформації є важливим етапом для забезпечення її стабільної та ефективної роботи. Завдяки впровадженню чітких процедур, сучасних технічних рішень і постійному навчанню персоналу, приміщення здатне не лише підтримувати належний рівень безпеки, а й адаптуватися до нових викликів.

Гнучкість хмарних сервісів, вдосконалення локальної інфраструктури та систематичний підхід до організаційних заходів формують надійну основу для довготривалої та захищеної роботи інформаційної системи.

3.4 Висновок

У цьому розділі було проведено комплексну оцінку практичного впровадження розробленої системи захисту інформації. Початково здійснено технічне обґрунтування обраної архітектури захисту, що включає використання мережевого поділу, хмарної інфраструктури AWS, засобів відеоспостереження, контролю доступу та моніторингу трафіку. Особливу увагу приділено балансуванню між функціональністю та вартістю обладнання, враховуючи специфіку приміщення та його ресурсні обмеження. Вибір технічних рішень був зумовлений потребою в масштабованості, стабільності та доступності ключових сервісів, включаючи SIEM-системи, NAS-сховища, VPN-доступ та централізоване логування. Далі проаналізовано витрати на реалізацію системи — як одноразові, пов’язані з придбанням обладнання, так і щомісячні операційні витрати на обслуговування хмарної інфраструктури та оплату праці спеціаліста з безпеки. Загальна сума витрат у перший рік склала понад 640 тисяч гривень, що свідчить про реалістичне та обґрунтоване бюджетування. Також враховано резервний фонд для покриття аварійних витрат і оновлень. Також сформовано чіткі настанови щодо експлуатації системи: визначено напрями її розширення, модернізації, організаційної підтримки та навчання персоналу. Зокрема, запропоновано процедури впровадження нових серверів у хмарному середовищі, адаптаційні програми для нових працівників, політики двофакторної автентифікації та регулярні аудити. Це дозволяє не лише підтримувати систему у працездатному стані, а й забезпечити її гнучкість та стійкість до нових загроз.

ВИСНОВКИ

У межах цієї кваліфікаційної роботи було здійснено повний цикл проєктування, впровадження та документування системи захисту інформації для комерційного приміщення, яке функціонує в IT-сфері. Робота охоплює як теоретичне обґрунтування, так і практичну реалізацію комплексного рішення, адаптованого до реальних умов бізнесу.

Для досягнення поставленої мети було виконано низку завдань, що логічно структурують процес дослідження:

– проаналізовано предметну область теми, зосереджену на потребах і викликах, які постають перед малими комерційними приміщеннями у сфері IT;

– досліджено типові загрози інформаційній інфраструктурі таких підприємств, а також методи протидії цим загрозам, з урахуванням їхніх обмежених ресурсів;

– вивчено державні нормативні документи України та міжнародні стандарти що визначають вимоги до побудови систем захисту інформації;

– проведено аналіз специфіки інформаційного функціонування малих IT-компаній, зокрема досліджено типові інформаційні потоки на прикладі компанії ArcadiaWorks;

– побудовано модель загроз і модель порушника для обраного приміщення, що дозволило виявити потенційні вразливості та визначити пріоритетні напрями захисту;

– спроєктовано архітектуру системи захисту, яка включає фізичні, мережеві та організаційні засоби безпеки з використанням хмарних технологій;

– впроваджено та апробовано запропоноване рішення з урахуванням реальних технічних і фінансових можливостей приміщення;

– розроблено настанови щодо експлуатації системи, її масштабування, оновлення, навчання персоналу та аудиту безпеки.

У процесі реалізації проєкту було розраховано обсяг витрат на впровадження системи, що склав понад 640 тисяч гривень у перший рік, з

наступним зменшенням до 594 тисяч на рік. Це підтверджує фінансову обґрунтованість запропонованих заходів та їх доцільність для умов бізнесу. Результати роботи засвідчують, що впровадження системи захисту інформації є не лише необхідним, але й цілком реалізованим навіть для невеликих підприємств за умови грамотного підходу до проєктування, ресурсного планування та організації внутрішніх процесів. Отримане рішення забезпечує захист конфіденційної інформації, підвищує рівень цифрової стійкості приміщення, зміцнює довіру клієнтів і партнерів, а також дозволяє відповідати вимогам чинного законодавства у сфері інформаційної безпеки..

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Information Security - CIA TRIAD. Scribd. URL: https://www.scribd.com/document/768825267/Information-Security-CIA-TRIAD (дата звернення: 08.05.2024).

2. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. 26 лютого 2024. С 1-14.

3. Модуль інформаційної безпеки . URL: https://surli.cc/mhrodn (дата звернення: 12.01.2025).

4. Загрози комп'ютерної безпеки . Kievoit . URL: https://www.kievoit.ippo.kubg.edu.ua/kievoit/2013/102/102.html (дата звернення: 12.01.2025).

5. Souppaya M., Scarfone K. Guide до Enterprise Patch Management Planning: Preventive Maintenance for Technology . [Міністерство торгівлі США], 2022. С 1-20.

6. Kotikalapudi S., Montgomery D. Зовнішній міжнародний Traffic Exchange: BGP Security and DDoS Mitigation . [Міністерство торгівлі США], 2020. С 16-25

7. Класифікація загроз безпеці та пошкодження даних у комп'ютерних системах . [Назва сайту невідома] . URL: https://surl.li/hygunv (дата звернення: 15.01.2025).

8. Методи фізичної захисту інформації в інформаційно-комунікаційних система. URL: https://er.nau.edu.ua/items/91a86ac8-7f34-4753-a026-5e81ab3c831e (дата звернення: 15.01.2025).

9. Що таке інформаційна безпека: основні засади та загрози. URL: https://surl.li/puxibe (дата звернення: 17.01.2025).

10. Види заходів протидії загрозам безпеки. Правові основи забезпечення безпеки інформаційних технологій. [Назва сайту]. URL: https://surl.li/yflnnx (дата звернення: 17.01.2025)

11. Основи кібербезпеки. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2? (дата звернення: 20.01.2025).

12. Про захист інформації в інформаційно-комунікаційних системах :

Закон України від 02.12.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 20.01.2025).

13. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 21.01.2025).

14. Стратегія кібербезпеки України (2021 – 2025 роки). URL: https://surl.li/ewmhxu (дата звернення: 25.01.2025).

15. Комплексні системи захисту інформації. URL: https://surl.gd/mvgafe (дата звернення: 25.01.2025).

16. НОРМАТИВНИЙ ДОКУМЕНТ 2.5-004-99. Системи технічного захисту інформації. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 26.01.2025).

17. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910 (дата звернення: 26.01.2025).

18. ДСТУ EN ISO/IEC 27002:2024. Інформаційна безпека, кібербезпека та захист конфіденційності. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=106958 (дата звернення: 26.01.2025).

19. Про національну безпеку України : Закон України. URL: https://protocol.ua/ua/pro_natsionalnu_bezpeku_ukraini_stattya_12/#google_vignette (дата звернення: 26.01.2025).

20. Стратегія для та середнього бізнесу: основи та важливість. URL: https://surl.lt/pzmdpf (дата звернення: 26.01.2025).

21. Про електронну ідентифікацію та електронні довірчі послуги : Закон України. URL: https://surl.li/nwazpj (дата звернення: 26.01.2025).

22. Новини бізнесу. Liga Zakon. URL: https://biz.ligazakon.net/news/page-2 (дата звернення: 26.01.2025)

23. Основні загрози безпеці для нових та зростаючих онлайн-бізнесів. URL: https://surl.li/jedzzw (дата звернення: 26.01.2025)

24. https://protocol.ua/ua/pro_osnovi_natsionalnoi_bezpeki_ukraini_stattya_7/ (дата звернення: 26.01.2025)

25. Гребенюк А. М. Основи управління інформаційною безпекою : навч. посіб. Дніпро : ДДУВС, 2020. 144 с.

26. Чотири українські місцеві медіа зазнали DDoS-атак і фішингу. URL: https://surl.li/fdlbue (дата звернення: 13.02.2025)

27. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 13.02.2025).

28. Держспецзв'язку попередило про нову фішингову атаку на бухгалтерів підприємств. URL: https://surl.li/ujucxw (дата звернення: 13.02.2025).

29. Програміст «Епіцентра» викрав з роботи понад 20 комп'ютерів. dev.ua. URL: https://dev.ua/news/prohrammyst-epitsentra (дата звернення: 13.02.2025).

30. Що таке шкідливе програмне забезпечення? URL: https://surl.li/whhyca (дата звернення: 13.02.2025).

31. В СБУ сказали, яку російську програму-шпигун знайшли у Dragon Capital. URL: https://surl.li/lohprt (дата звернення: 13.02.2025).

32. Інформаційна безпека та види можливих загроз. IT-Biz. URL: https://itbiz.ua/statti-ta-obzori/informacijna-bezpeka-ta-vidi-mozhlivih-zagroz/ (дата звернення: 13.02.2025).

33. Що таке соціальна інженерія. URL: https://surl.li/hsktou (дата звернення: 13.02.2025).

34. Безпека в епоху хаосу: інформаційна оборона для компаній. IT-Solutions. URL: https://it-solutions.ua/blog/bezpeka-v-epohu-haosu-informatsijna-oborona-dlya-kompaniy/ (дата звернення: 13.02.2025).

35. Кібербезпека. Cyber Academy. URL: https://www.cyber.academy/kiberbezpeka (дата звернення: 13.02.2025).

36. Шафа серверна настінна з полицею GEAR 6U 19" 530x400x300 мм.

ipmall.com.ua. URL: https://ipmall.com.ua/product/shafa-serverna-nastinna-z-polytseju-gear-6u-19-530x400x300-mm-chorna (дата звернення: 10.03.2025).

37. Маршрутизатор. Hotline.ua. URL: https://surli.cc/uqzttk (дата звернення: 10.03.2025).

38. Комутатор. Hotline.ua. URL: https://surl.lu/osqxpg (дата звернення: 10.03.2025).

39. ДБЖ EnerGenie EG-UPS-B850. Rozetka. URL: https://hard.rozetka.com.ua/ua/energenie_eg_ups_b850/p10585761/ (дата звернення: 10.03.2025).

40. Точка доступа MikroTik wAP ac (RBwAPG-5HacD2HnD). Mikrotik.ua. URL: https://mikrotik.ua/ru/product/mikrotik-wap-ac-rbwapg-5hacd2hnd (дата звернення: 10.03.2025)

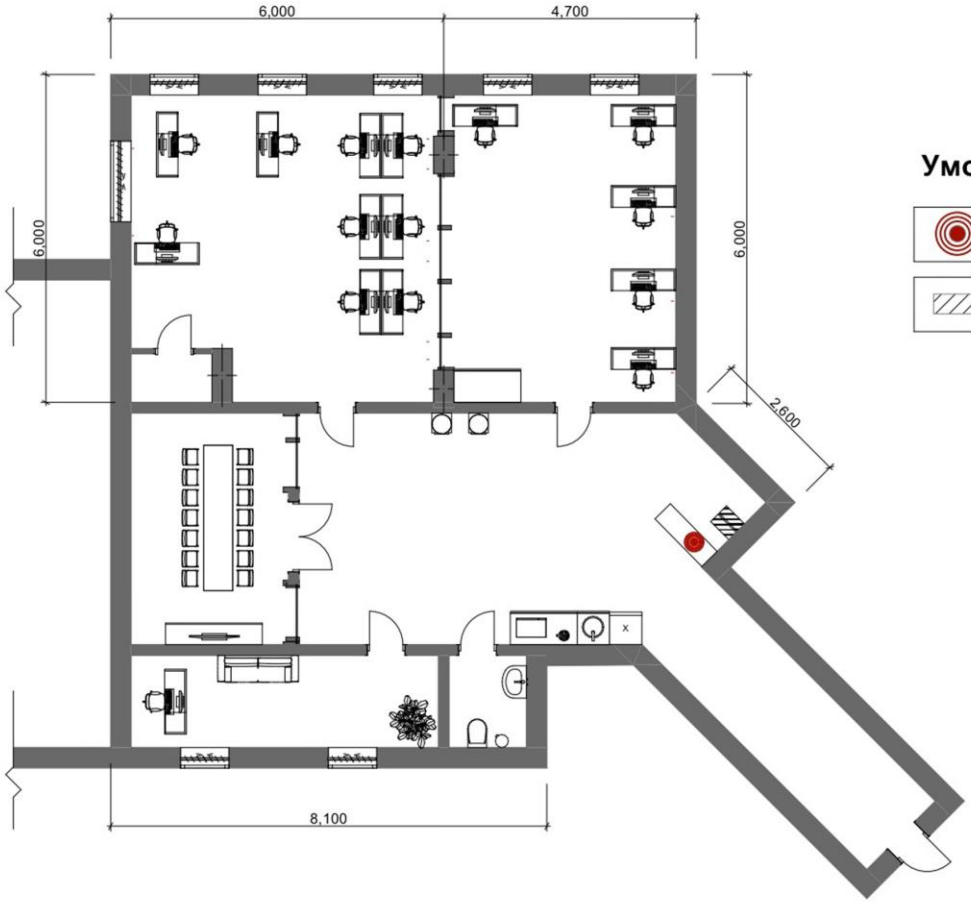
41. IP-камера відеоспостереження HIKVISION DS-2CD1123G2-IUF (2.8 мм). Hotline.ua. URL: https://hotline.ua/ua/dom-ip-kamery-videonablyudeniya/hikvision-ds-cd1123g2-iuf-28-mm/ (дата звернення: 10.03.2025).

42. Біометричний замок Aqara Smart Door Lock N100. Hotline.ua. URL: https://hotline.ua/ua/remont-zamki/aqara-n100-apple-homekit-znms16lm/ (дата звернення: 10.03.2025).

43. Електромеханічний замок (виразний) ZKTeco ML10/ID. Hotline.ua. URL: https://hotline.ua/ua/remont-zamki/zkteco-ml10id/ (дата звернення: 10.03.2025)

ДОДАТОК А

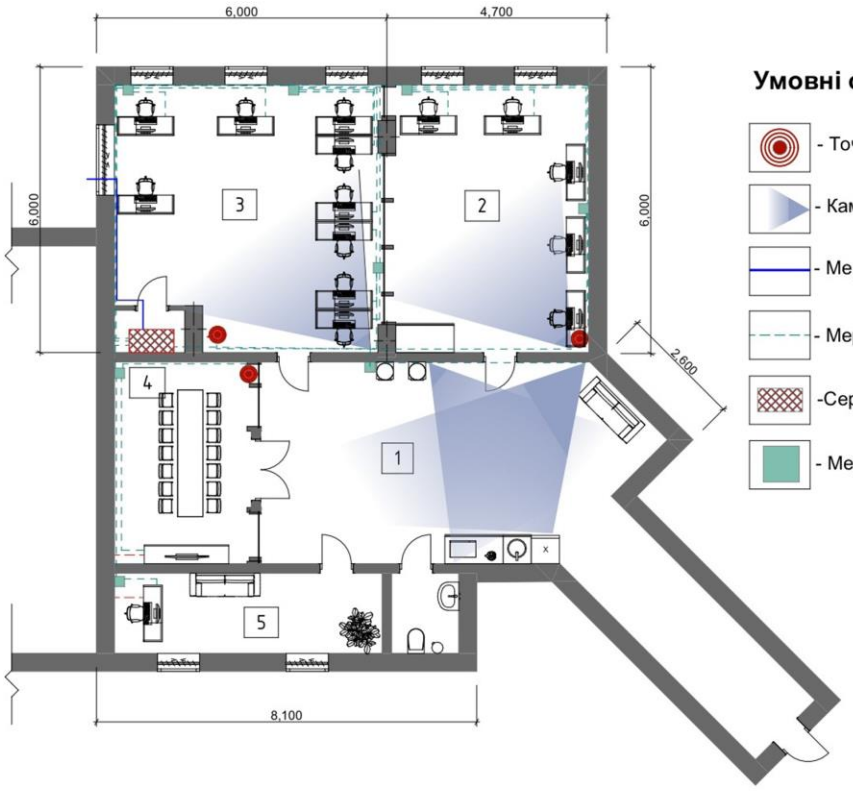
КРБКБ.2102149.21.02.37 Е8



Умовні позначення

- Точка доступу
- Системний блок

					КРБКБ.2102159.21.02.37 Е8			
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту інформації комерційного офісного приміщення План приміщення до впровадження системи захисту	Літера	Маса	Масштаб
Розроб.		Ягловський О.О						
Перевір.		Чешун В.М.				Аркуш 1	Аркушів 3	
Н.контр.						ХНУ, КБ-21-2		
Т. контр.		Мостовий С.В.						
Затв.		Кльоц Ю.П.						



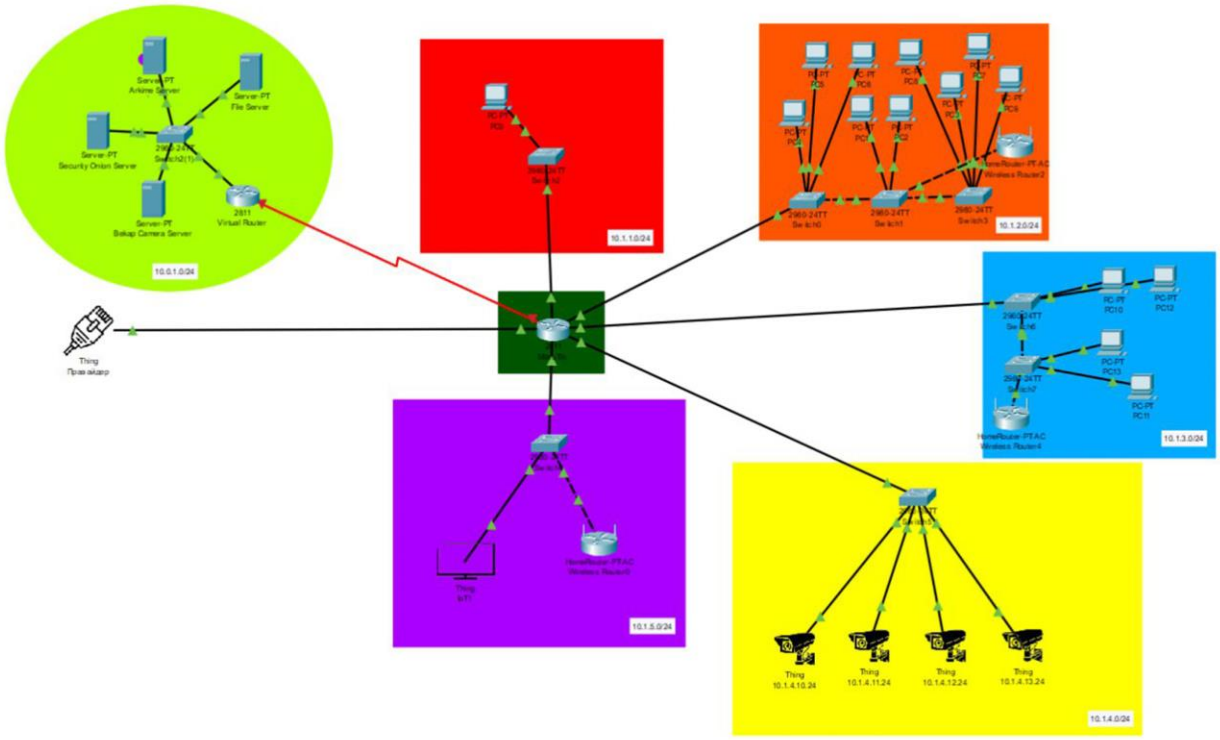
Умовні означення

- Точка доступу
- Камера
- Мережевий кабель від провайдера
- Мережевий кабель
- Серверна
- Мережевий комутатор

Експлікація		
№	Найменування	Площа
1	Публічна зона	46,57
2	Кабінет менеджерів та бухгалтерів	23,52
3	Кабінет розробників	32,08
4	Кабінет для перемовин	13,24
5	Кабінет директора	9,73

					КРБКБ.2102159.21.02.37 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту інформації комерційного офісного приміщення План приміщення після впровадження системи захисту	Літера	Маса / Масштаб
Розроб.		Чигловський О.О.					
Перевір.		Чепуп В.М.				Аркуш 2	Аркушів 3
Н.контр.							
Т. контр.		Мостовий С.В.				ХНУ, КБ-21-2	
Затв.		Кльоц Ю.П.					

КРБКБ.2102149.21.02.37 Е8



					КРБКБ.2102159.21.02.37 Е8			
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту інформації комерційного офісного приміщення Схема розробленої мережі	Літера	Маса	Масштаб
Розроб.		Низовський О.О						
Перевір.		Чепуи В.М.				Аркуш 3	Аркушів 3	
Н.контр.								
Т. контр.		Мостовий С.В.				ХНУ, КБ-21-2		
Затв.		Кльоц Ю.П.						

ДОДАТОК Б

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

XX Міжнародної науково-практичної конференції

«Військова освіта і наука: сьогодення та майбутнє»

29 листопада 2024 року

Київ – 2024

Зміст

Анікін В.А. *(ХмНУ)*
Нігловський О.О. *(ХмНУ)*

СИСТЕМА БЕЗПЕКОВИХ НАСТАНОВ МАЛОГО КОМЕРЦІЙНОГО ОФІСНОГО ПРИМІЩЕННЯ

На сьогодні значна частина малого та середнього бізнесу, зокрема пов'язаного з інформаційними технологіями, розміщують свій штат в малих офісних приміщеннях, де також зосереджена їх інформаційно-комунікаційна мережева комп'ютерна інфраструктура. При цьому часто такі компанії або повністю нехтують базовими правилами кібербезпеки, або не надають їй належної уваги та фінансування, точково та не комплексно закриваючи проблеми по факту їх виникнення. Система захисту інформації є критично важливою для забезпечення конфіденційності, цілісності та доступності даних, що обробляються в офісі. В умовах зростаючих кіберзагроз та витоків інформації, впровадження систем захисту дозволяє захистити комерційну таємницю, персональні дані клієнтів та інші важливі відомості від несанкціонованого доступу та розголошення.

Як правило системи захисту інформації включають сукупність організаційних та інженерно-технічних заходів, спрямованих на захист інформації від розголошення, витоку та несанкціонованого доступу. Сучасні системи захисту використовують різноманітні методи захисту, такі як шифрування, багатофакторну аутентифікацію, системи виявлення атак, тощо. Ключовою характеристикою сучасних систем захисту інформації є те що вони працюють комплексно, запобігаючи широкому спектру загроз, навідміну від неефективних точкових рішень. Зазначені системи також потребують регулярного оновлення, модернізації для протидії новим видам загроз. Окрім технічної складової, важливим аспектом є також адміністративно-організаційний супровід, який регламентує політики та протоколи безпеки компанії.

В роботі пропонується схема програмних, апаратних та мережевих рішень що комплексно вирішують типову безпекову проблематику середньостатистичного комерційного офісного приміщення малої IT-компанії. Вона включає в себе аналіз типових загроз та вразливостей, визначення вимог до безпеки, та створення комплексу рекомендацій для різних рівнів фінансування.

Запропоновано схему безпечного налаштування мережевого обладнання, а також перелік рекомендованих виробників та номенклатури виробів різного цінового діапазону. Особливу увагу було приділено корпоративним мережевим сховищам даних та серверам.

Крім того створено рекомендації щодо розробки організаційно-адміністративних політик та процедур, які регламентують загальні правила інформаційної безпеки та гігієни. Важливим аспектом є також навчання співробітників основам інформаційної безпеки та регулярне проведення тренінгів для підвищення їх обізнаності щодо можливих загроз.

Створені рекомендації було апробовано на 2 різних IT-компаніях, керівництво яких добровільно погодилось на участь у дослідженні. За результатами апробації, впродовж трьох тижнів спостереження було сумарно зафіксовано та вдалось запобігти 7 фішингових атак, 2 спроб отримання віддаленого доступу та 1 спроби отримання доступу до корпоративної системи відеоспостереження, що свідчить про ефективність впроваджених рішень.

ЛІТЕРАТУРА:

1. Calder, Alan, Steve Watkins. "IT governance: an international guide to data security and ISO 27001/ISO 27002." (2024): 1-486.
2. Badotra, Sumit, Amit Sundas. "A systematic review on security of E-commerce systems." International Journal of Applied Science and Engineering 18.2 (2021): 1-19.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Нігловського Олександра Олександровича
Студента ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism) і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення текстових збігів в роботах.

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

04.06.2025
дата

підпис

Протокол аналізу звіту подібності науковим керівником

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

Автор: Нігловський Олександр Олександрович

Співавтор:

Назва: Система захисту інформації комерційного офісного приміщення

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:2%

Коефіцієнт подібності 2:0.1%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-08 17:03:54.0

Після аналізу Звіту подібності констатую наступне:

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

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

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

Обгрунтування:

09.06.2025р.

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 8%**

ID: 244107 Title: Система захисту інформації комерційного офісного приміщення Added in a DB: 2025-06-08 Authors: Нігловський Олександр Олександрович Heads: Чешун В.М. Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	120538	910	722 (1%)	10 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Система захисту інформації комерційного офісного приміщення

Автор: Нігловський Олександр Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник:Віктор ЧЕШУН, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 100%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Віктор ЧЕШУН

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Нігловський Олександр Олександрович

Тема Система захисту інформації комерційного офісного приміщення

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 95.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена система захисту інформації для комерційного приміщення на прикладі IT-компанії ArcadiaWorks. У межах дослідження проаналізовано специфіку інформаційної інфраструктури приміщення, типові інформаційні потоки, а також основні загрози, що можуть призвести до втрати або витоку інформації. Розглянуто державні та міжнародні нормативно-правові акти, які регулюють питання інформаційної безпеки. Проведено аудит існуючих недоліків і вразливостей, побудовано модель загроз та модель порушника, характерні для досліджуваного середовища.

2. Висновок про відповідність кваліфікаційної роботи завданню У роботі повністю виконано поставлені завдання, визначені темою та завданням на кваліфікаційну роботу, як у теоретичній, так і в практичній частинах. Розроблено систему захисту інформації малого комерційного офісного приміщення

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовано актуальність розробки системи захисту інформації для комерційного приміщення в умовах зростаючих кіберзагроз, визначено мету та завдання дослідження, а також окреслено методичну базу. У першому розділі проаналізовано предметну область, вивчено типові загрози інформаційній безпеці малих офісів, а також досліджено чинні державні нормативні документи та міжнародні стандарти. Проведено аналіз специфіки інформаційних потоків у малому IT-бізнесі на прикладі компанії ArcadiaWorks. У другому розділі на основі зібраних даних і внутрішньої структури компанії побудовано модель загроз і модель порушника, здійснено аналіз інформаційної взаємодії між підрозділами, визначено найбільш вразливі компоненти та спроєктовано систему захисту, що охоплює організаційні та технічні заходи. У третьому розділі реалізовано імплементацію системи захисту в експериментальному середовищі, протестовано її функціональні можливості, проведено оцінку ефективності рішень та визначено ресурсні витрати на впровадження. Розроблено настанови щодо подальшої експлуатації системи.

4. Позитивні сторони Робота має високу практичну цінність, оскільки спрямована на проєктування та реалізацію системи захисту інформації комерційного офісного приміщення. Запропонована система враховує актуальні загрози, характерні для малого офісного середовища, зокрема організаційні, технічні та нормативні ризики. Вона побудована на основі аудиту компанії ArcadiaWorks, моделі загроз і моделі порушника.

Рішення відзначається адаптивністю, модульною структурою та придатністю для середовищ з обмеженими ресурсами. Експериментальне впровадження засвідчило стабільну роботу системи, її здатність виявляти та нейтралізувати типові загрози інформаційній безпеці.

5. Негативні сторони роботи Серед недоліків роботи слід зазначити обмежене охоплення фізичних каналів витоку інформації — увагу зосереджено переважно на організаційних та технічних аспектах у цифровому середовищі. Також не всі запропоновані заходи пройшли апробацію в реальному офісі, частину рішень протестовано лише в умовах моделювання.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. Загалом графічна частина виконана на належному рівні, а пояснювальна записка оформлена відповідно до встановлених вимог..

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Говорущенко Тетяна Олександрівна.
Доктор технічних наук, професор, декан факультету інформаційних технологій

« 04 » червня 2025