Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Дзеркаля Романа Артурович*

академічної групи *125-18-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «ПІНТА ВЕБВАРЕ»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д. ф.-м. н., проф. Кагадій Т.С.	85	добре	
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.	85	добре	
економічний	к.е.н., доц. Пілова Д. П.	85	добре	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.	85	добре	

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2022 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Дзеркалю Р. А.* **академічної групи** *125-18-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «ПІНТА ВЕБВАРЕ»*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Розглянути стан питання. Проаналізувати нормативно-правову базу. Виконати постановку задачі.	30.04.2022
Розділ 2	Виконати обстеження середовища ОІД, аналіз ризиків. Розробити моделі порушника та загроз. Розробити основні елементи КСЗІ.	16.05.2022
Розділ 3	Обґрунтувати економічну доцільність створення КСЗІ.	03.06.2022

Завдання видано _____ Кагадій Т. С.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 10.01.2022

Дата подання до екзаменаційної комісії: 10.06.2022

Прийнято до виконання _____ Дзеркаль Р. А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 43 с., 8 рис., 13 табл., 6 додатків, 13 джерел.

Об’єктом розробки виступає інформаційно-телекомунікаційна система (далі ІТС) ТОВ «ПІНТА ВЕБВАРЕ».

Предметом розробки є комплексна система захисту інформації ІТС ТОВ «ПІНТА ВЕБВАРЕ».

Мета роботи: забезпечення достатнього рівня захисту інформації в ІТС ТОВ «ПІНТА ВЕБВАРЕ».

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі було проаналізовано статистику кіберінцидентів за 2021 рік, проаналізовано нормативно-правову базу забезпечення кібербезпеки, що використовувалася під час виконання кваліфікаційної роботи; сформульована та поставлена задача кваліфікаційної роботи та аргументовано необхідність створення комплексної системи захисту інформації.

У спеціальній частині були надані загальні відомості про підприємство; проаналізоване фізичне, інформаційне середовища та середовище користувачів. За цими даними було сформовано модель порушника, модель загроз та обрано відповідний профіль захищеності. На базі профілю захищеності, моделі загроз та моделі порушника було розроблено комплекс засобів захисту, який включає в себе організаційні (політики безпеки) заходи та програмно-технічні засоби.

У економічному розділі розрахована та доведена доцільність створення КСЗІ; визначено економічна ефективність її створення.

КОМПЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПРОФІЛЬ ЗАХИЩЕННОСТІ, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ

ABSTRACT

Explanatory note: 43 pages, 8 figures, 13 tables, 6 appendices, 13 sources.

The object of development is the information and telecommunication system (hereinafter ITS) of PINTA WEBWARE LLC..

The subject of development is a comprehensive information security system ITS LLC "PINTA WEBWARE".

Purpose: to ensure a sufficient level of information protection in ITS LLC "PINTA WEBWARE".

Development methods: observation, comparison, analysis, description.

The first section analyzed the statistics of cyber incidents for 2021, analyzed the regulatory framework for cybersecurity, which was used during the qualification work; the task of qualification work is formulated and set and the necessity of creation of complex system of information protection is argued.

The special part provided general information about the company; analyzed physical, information environment and user environment. Based on these data, a model of the violator, a threat model was formed and the appropriate security profile was selected. Based on the security profile, threat model and violator model, a set of protection tools was developed, which includes organizational (security policies) measures and software and hardware.

In the economic section the expediency of creation of CIPS is calculated and proved; the economic efficiency of its creation is determined.

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, THREAT MODEL, INFRINGEMENT MODEL, PROTECTION PROFILE, COMPLEX OF PROTECTION MEANS

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

АС – автоматизована система

ВП – внутрішній порушник

ДТЗ – допоміжні технічні засоби

ЗП – зовнішній порушник

ІзОД – інформація з обмеженим доступом

ІТС – інформаційно-телекомунікаційна система

КЗ – контрольована зона

КЗЗ – комплекс засобів захисту

КСЗІ – комплексна система захисту інформації

ОІД – об’єкт інформаційної діяльності

ОС – операційна система

ОТЗ – основні технічні засоби

ПЗ – програмне забезпечення

ТЗ – технічні засоби

Зміст

ВСТУП

Об’єктом розробки виступає інформаційно-телекомунікаційна система (далі ІТС) ТОВ «ПІНТА ВЕБВАРЕ».

Предметом розробки є комплексна система захисту інформації ІТС ТОВ «ПІНТА ВЕБВАРЕ».

Метою кваліфікаційної роботи є забезпечення достатнього рівня захисту інформації в ІТС ТОВ «ПІНТА ВЕБВАРЕ».

Робота є актуальною, тому що побудова та оптимізація КСЗІ являє собою головним питанням безпеки для будь-якого об’єкту інформаційної діяльності, на якому зберігається, оброблюється і передається інформація з обмеженим доступом, що потребує захисту від впливу внутрішніх і зовнішніх загроз природного або антропогенного характеру.

Останніми роками проблема інформаційної безпеки стала набагато актуальнішою, ніж це було два десятиліття тому. Усі ми намагаємося захиститись від потенційного зловмисника усіма можливими способами. Ми витрачаємо багато коштів та часу та зазвичай – великих грошових витрат.

Для будь-якого підприємства, втрата конфіденційних даних може призвести до непоправних, катастрофічних наслідків – сильного удару по іміджу компанії, або, куди гірше, фінансових збитків.

Одним із ефективних засобів боротьби з порушеннями є розробка та запровадження корпоративної комплексної системи захисту інформації (далі КСЗІ). Основна її мета – захист інформації, пов'язаної з організацією. Вона дозволить перекрити способи витоку даних та мінімізувати ризики.

Керівництво має розуміти, що звичайному робітнику компанії немає справи до ризиків компанії. Їм все одно: чи вкрадуть дані хакери компаній конкурентів, чи вимагатимуть із вас гроші за розшифровку заблокованої інформації, що може призвести до її потрапляння у небажані руки. А це означає, що керівник має сам убезпечити свою компанію від небажаних ситуацій. Комплексна система захисту інформації убезпечить всіх співробітників компанії, що можуть навмисно або

ненавмисно знехтувати правилами захисту. Правильне налаштування та технічний супровід автоматизує більшу частину роботи.

Важливий чинник розробки КСЗІ – цільова аудиторія. Звичайні користувачі, які слідуватиму вказівкам не розуміють технічних термінів, тому потрібно включити в документ найважливіше: цілі, методи їх досягнення та відповідальність – матеріали зрозумілі будь-якому співробітнику.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Будь-яка організація володіє інформацією, порушення властивостей якої може спричинити великі збитки її власнику.

За 2021 рік оперативним центром реагування на кіберінциденти Державного центру кіберзахисту (ДЦКЗ) Держспецзв'язку зафіксовано 41 млн підозрілих подій інформаційної безпеки, опрацьовано 160 тис. критичних подій, зареєстровано 147 кіберінцидентів. Відповідно до зібраних статистичних даних, найбільше кіберінцидентів стосувалися: шкідливого програмного коду – 28%, збору інформації зловмисниками – 18%, шахрайства – 6%. [1]. І подібна статистика з кожним роком лише зростає.

Згідно з останніми дослідженнями [2] за перший квартал 2022 року компанії розробки програмного забезпечення по всьому світі зазнали збільшення фішингових атак електронною поштою з березня 2020 року по нині. Незважаючи на це, майже 1 з 5 компаній проводять навчання щодо протидії шахраям для своїх працівників один раз на рік. Ця недостатня поінформованість є значним фактором, що сприяє тому, що соціальна інженерія залишається типом загрози, який, швидше за все, спричинить витік конфіденційної інформації. Згідно з наведеною статистикою за 2021 рік, близько 85% загроз пов'язані з людським фактором.

Однією з найбільших загроз є зараження вірусами-шифрувальниками. У 2020 році [3] одна з гігантів-компаній розробників програмного забезпечення стала жертвою вірусу-шифрувальщика, що стала причиною зупинення сервісів компанії. Однак, за словами голови компанії, кіберінцидент вдалося швидко локалізувати та знешкодити, в іншому випадку – під загрозу потрапила

1.2 Аналіз нормативно-правової бази

Проблемі забезпечення інформаційної та кібербезпеки присвячений широкий перелік документів нормативно-правової бази України. Зокрема, у законі «Про інформацію» наведено вимоги до класифікації інформації; дані

визначення термінам[1] та наведено статті щодо відповідальності за порушення закону.

Вимоги до захисту інформації в інформаційно-телекомунікаційній системі наведені у відповідному законі «Про захист інформації в інформаційно-телекомунікаційних системах» [2] у якому наведені загальні визначенні, режими доступу та відносини між власниками системи тощо. Також наведені умови обробки інформації.

Правові та організаційні основи регулюються Законом «Про основні засади забезпечення кібербезпеки» [3].

Додатково питання створення комплексної система захисту інформації розглядаються в серії нормативно-правових документів ТЗІ. Серед яких:

НД ТЗІ 1.1-003-99 присвячений термінам та визначенням, що використовуються у сфері захисту інформації в ІТС [4].

НД ТЗІ 2.5-004-99 присвячений критеріям оцінки захищеності інформації в ІТС [5].

НД ТЗІ 2.5-005-99 в якому дається класифікація АС та стандартні профілі захищеності [6].

НД ТЗІ 3.7-003-2005 подано порядок проведення робіт із створення КСЗІ в ІТС [7].

НД ТЗІ 1.6-005-2013 описується положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці [8].

Крім того питання захисту інформації регулюються постановами Кабінету міністрів України, один з яких постанова «Про затвердження загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [9].

1.3 Постановка задачі

Відповідно до розглянутої нормативно-правової бази основною задачею кваліфікаційної роботи є створення КСЗІ, що включає в себе обстеження об’єкту інформаційної діяльності (далі ОІД), створення моделей порушника та загроз,

розгляд профілю захищеності, власне розробка комплексу засобів захисту (далі – КЗЗ) та розрахунок економічної доцільності цього комплексу.

Висновок до розділу

У першому розділі було розглянуто статистичні дані щодо динаміки інцидентів з інформації та кібербезпеки в Україні за 2021 рік. Встановлено що робота є актуальною, проаналізовано нормативно-правову базу. Визначено, що одним з шляхів забезпечення захисту інформації відповідно до нормативно правової бази України є створення комплексних систем захисту інформації на вимогу керівництва та виконано постановку задачі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство. Підстави для створення комплексної системи захисту інформації

ТОВ «ПІНТА ВЕБВАРЕ» - це приватне комерційне підприємство, що займається розробкою мобільних та веб-додатків. Організаційна структура підприємства представлена на рис. 2.1.

Основними видами діяльності є:

- 62.01 Комп'ютерне програмування
- 62.02 Консультування з питань інформатизації
- 62.09 Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
- 63.11 Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність
- 63.12 Веб-портали

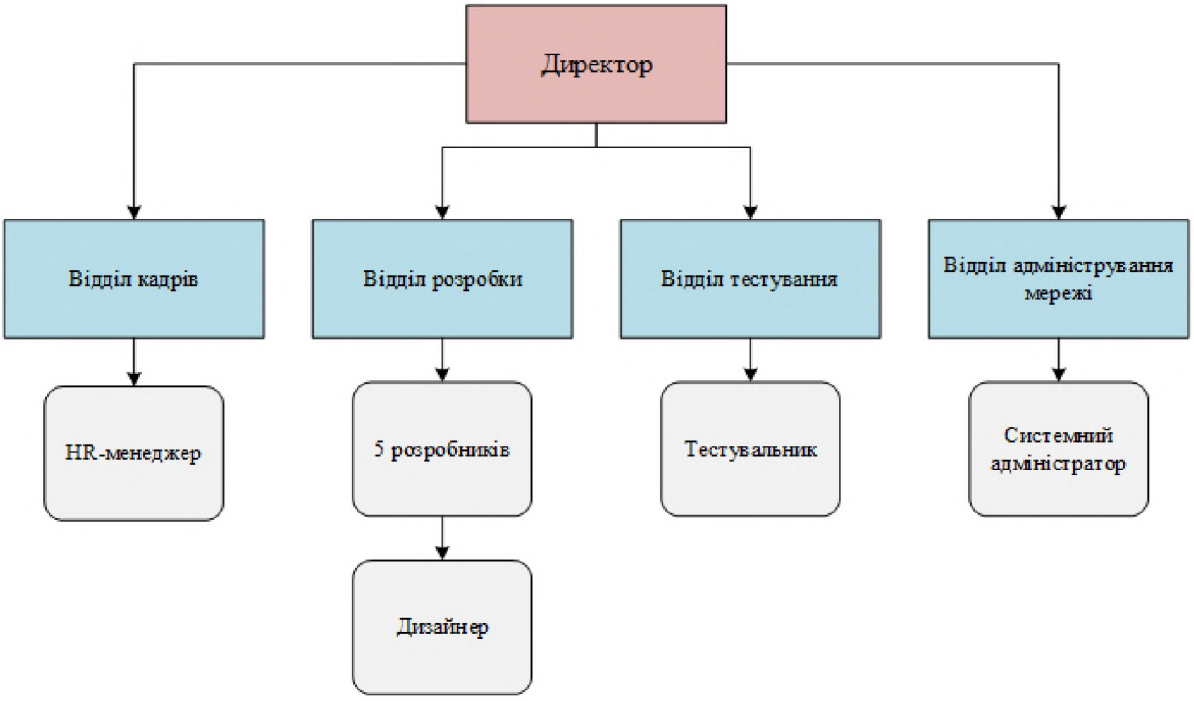


Рисунок 2.1 - Організаційна структура підприємства

Підприємство працює 5 днів на тиждень (з понеділка по п’ятницю) з 09:00 до 18:00 з перервою на обід з 13:00 до 14:00. Усього у компанії 10 робітників.

Відповідно до проведеного категорювання (Додаток Б), ОІД віднесено до четвертої категорії та створення КСЗІ не є обов'язковим, але керівником підприємства прийнято рішення для забезпечення достатнього рівня захисту інформації створити КСЗІ в ІТС і було видано відповідний наказ (Додаток В).

2.2 Обстеження середовищ підприємства

2.2.1 Обстеження фізичного середовища підприємства

Ситуаційний план представлений на рис. 2.2.

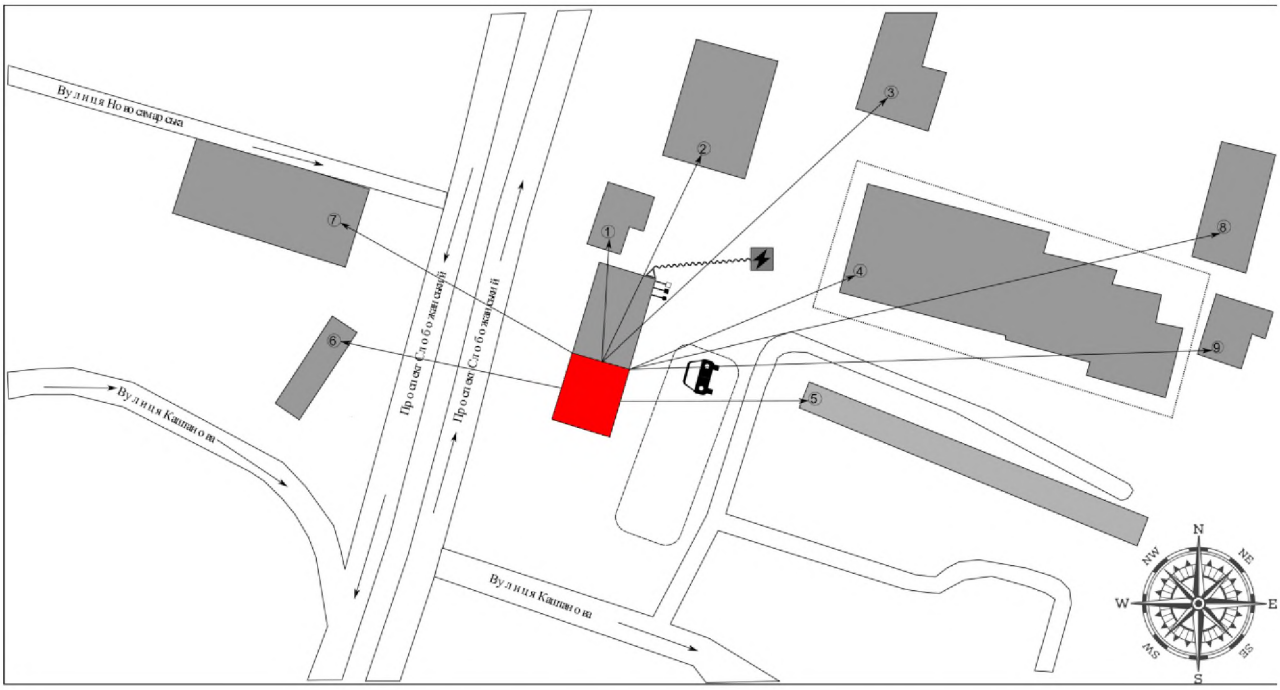
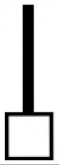
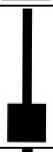
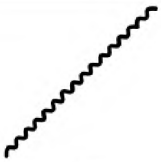
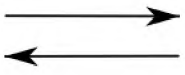


Рисунок 2.2 - Ситуаційний план підприємства

Таблиця умовних позначень

	Паркувальний майданчик		Система опалення
	Контрольована зона		Система водопостачання
	Будівля		Люк системи каналізації

Продовження таблиці умовних позначень

	Трансформаторна підстанція		Лінія зв'язку з трансформаторною підстанцією
	Номер будинку у таблиці		Заземлення
	Напрям руху транспорту		Паркан

Таблиця 2.1 - Характеристика прилеглих будівель

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД, м
1	Продуктовий магазин	1	пр. Слобожанський 34А	36
2	Автосалон	2	пр. Слобожанський 34Б	68
3	Дитяча музична школа	3	пр. Слобожанський 36	109
4	Дитячо-юнацька спортивна школа	1	пр. Слобожанський 36Д	100
5	Гаражі	1	пр. Слобожанський 37	92
6	Ветеринарна клініка	1	пр. Слобожанський 63А	64
7	Меблевий магазин	2	вул. Новосамарська 1	84
8	Житловий будинок	5	пр. Слобожанський 36А	153

Продовження таблиці 2.1 - Характеристика прилеглих будівель

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД, м
9	Житловий будинок	5	пр. Слобожанський 36Б	148

Контрольована зона обмежена стінами ОІД. Знаходиться за адресою проспект Слобожанський, 34. ОІД знаходиться у 5-поверховому житловому будинку, на першому поверсі. Генеральний план підприємства представлено на рис. 2.3. Вхід на ОІД здійснюється через центральні двері. Територія навколо ОІД асфальтована.

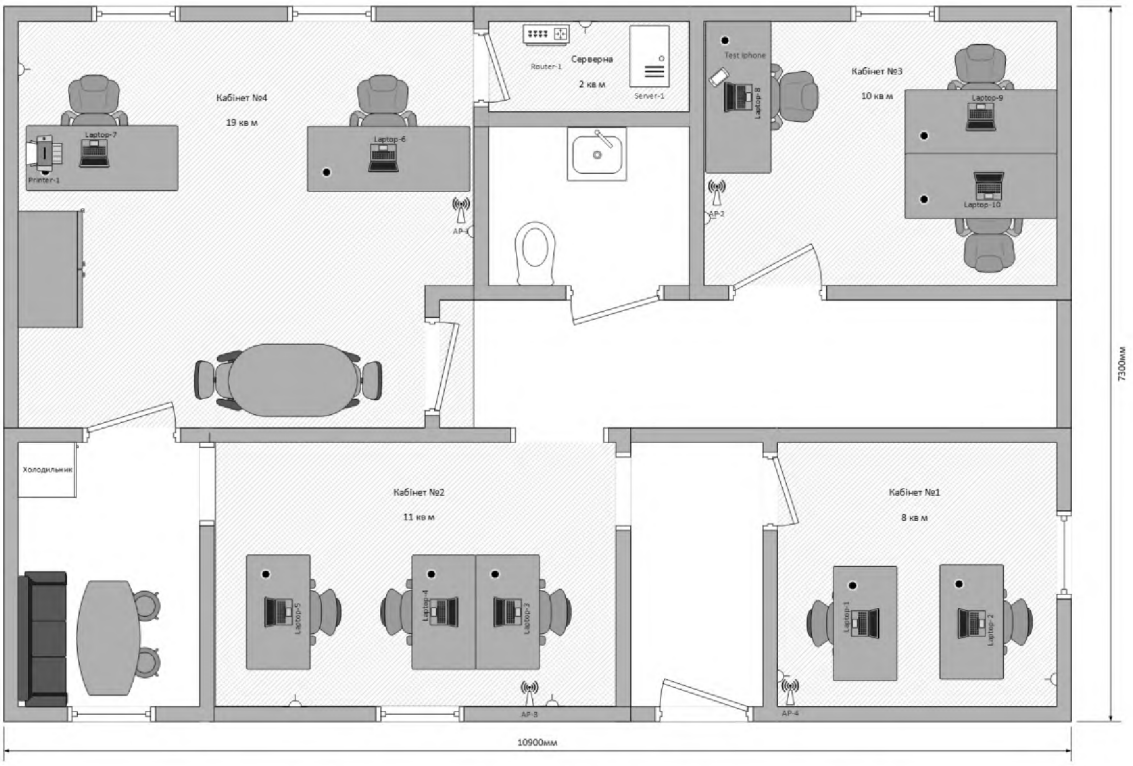


Рисунок 2.3 – Генеральний план підприємства

Стіни зроблені із цегли, товщиною 25 см, окрашені. Висота стелі 2.4 м. Стеля та підлога зроблені із бетону, товщиною 15 см. Стеля вкрита шпаклівкою, а підлога – керамічною плиткою.

Центральні двері – вихід/вихід – металеві, броньовані, типу «Скала». Товщина дверей складає 16 см, ширина 90 см, висота – 2 м. Міжкімнатні двері:

класичні, дерев'яні, виготовлені з ДВП. Ширина дверей 70 см, товщина 8 см, висота – 2м.

У кожній кімнаті встановлені пластикові вікна шириною 100 см, висотою 120см і товщиною 2.4 см. з чотирьох камерним профілем. Зовні встановлені решітки, виготовлені із металевих прутів, товщиною 10мм.

На заході від ОІД пролягає проспект Слобожанський, є підземний перехід. На протилежній стороні проспекту знаходяться ветеринарна клініка та меблевий магазин. На півночі знаходиться автосалон, продуктовий магазин та Дитяча музична школа №10. На сході знаходиться Спеціалізована дитячо-юнацька школа олімпійського резерву №6. На тому ж напрямку знаходяться автостоянка та приватний гаражний комплекс. На півдні пролягає транспортна розв'язка вулиці Каштанова та проспекту Слобожанський.

Системи життєзабезпечення (каналізація, водо-, електро- (рис. 2.4), тепло- (рис. 2.5) постачання) з'єднуються з міськими системами. Труби каналізації, водо- та тепло- постачання знаходяться під землею та виходять за межі контрольованої зони; електропостачання зєднується з трансформаторною підстанцією, що знаходиться біля контрольованої зони, а та у свою чергу – до підстанції району.

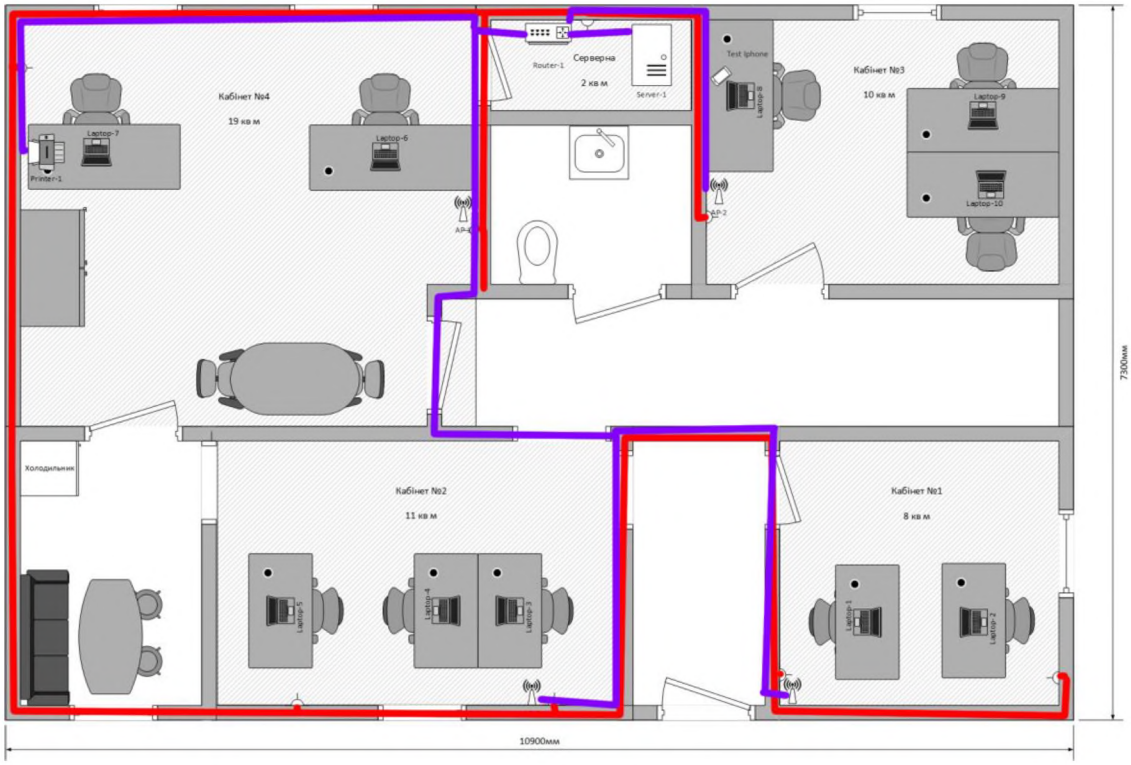


Рисунок 2.4 – Схема системи електроживлення

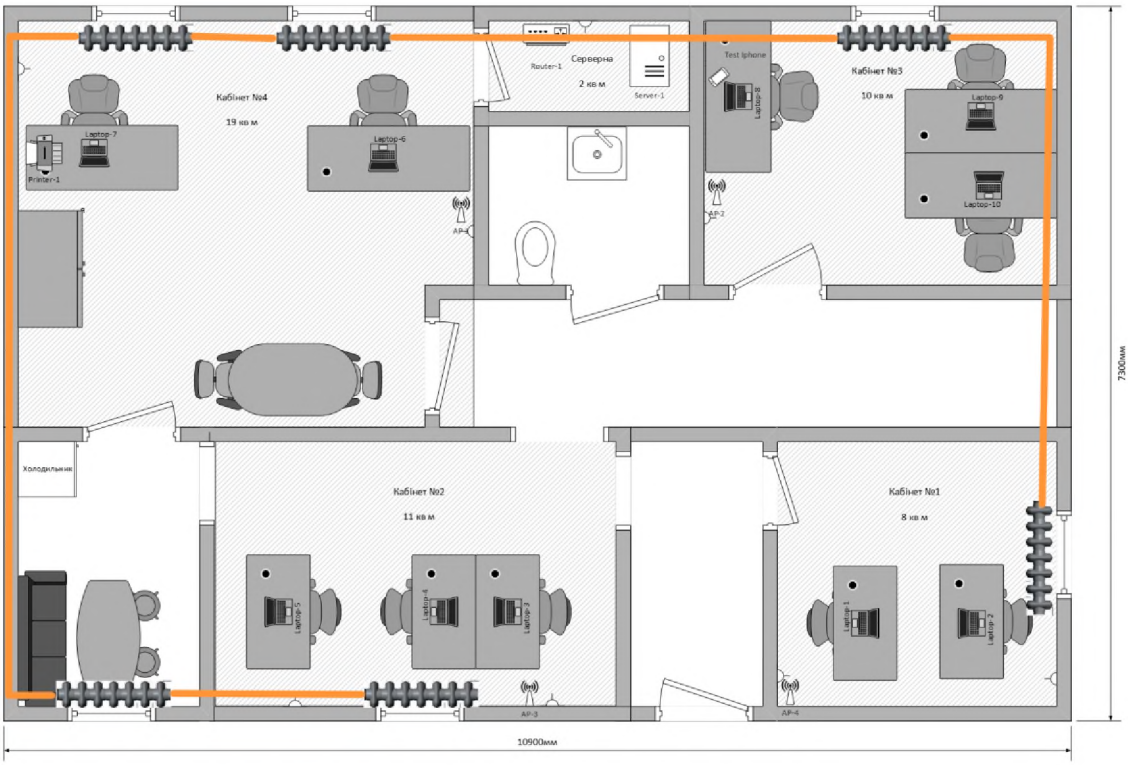


Рисунок 2.5 – Схема системи опалення

У якості освітлення використовуються світлодіодні панелі 36 Вт потужності. Кольорова температура 4000 К. Схема освітлення зображена на рисунку 2.6.

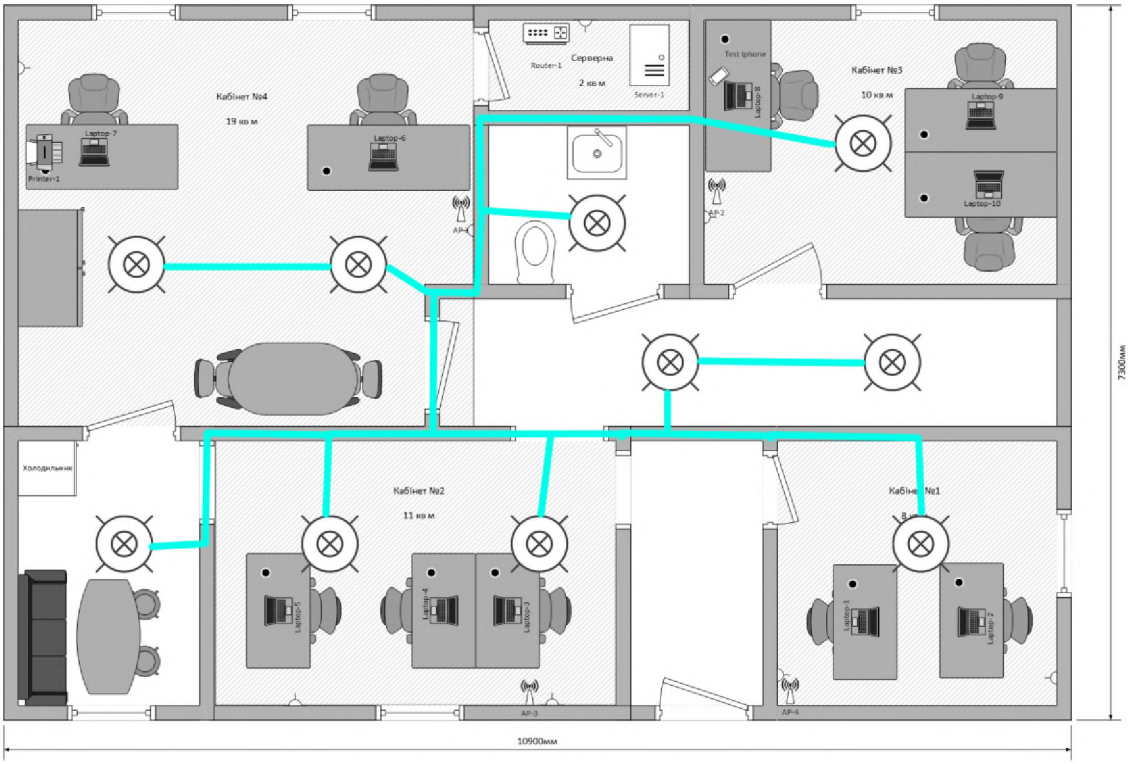


Рисунок 2.6 – Схема системи освітлення

На ОІД діє системи централізованої охорони – встановлені бездротові датчики руху з фотофіксацією, що направлені на вікна та центральні двері; датчики затоплення та диму (рис. 2.7)

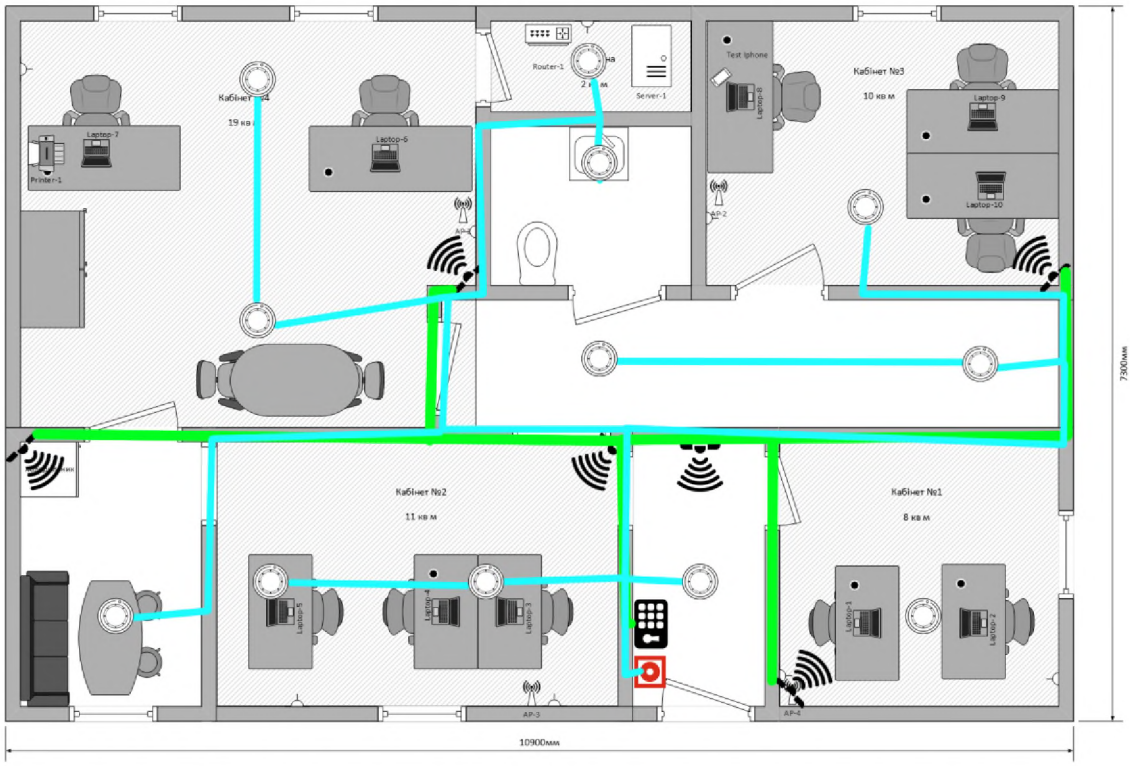


Рисунок 2.7 – Схема системи охорони та пожежної сигналізації

2.2.2 Обстеження обчислювального середовища підприємства

Обчислювальне середовище складається з 10 ноутбуків, що є власністю компанії. На підприємстві є тестовий сервер під управлінням Linux CentOS, на якому розгорнутий веб-сервер Nginx 1.20.2. Сервер призначений для розгортання, тестування та демонстрації для клієнтів додатків, що розробляються. Структурна схема ІТС підприємства зображена на рис. 2.8

Кожний ноутбук під'єднаний до локальної мережі за допомогою технології Wi-Fi 802.11n. Іноді для налаштування маршрутизатору або ретрансляторів використовується вита пара, що знаходиться у системного адміністратора, в інших випадках налаштування проходить через веб-інтерфейс.

Користувачі можуть надсилати документи для друку на принтер. За необхідності, спілкування між сусідніми кабінетами здійснюється через VoIP-програму Skype.

Віддалені сервери для зберігання та обробки розглянутої інформації знаходяться за межами КЗ.

Усе ПЗ регулярно оновлюється, зокрема на сервері та маршрутизаторі, приділяючи особливу увагу оновленням безпеки.

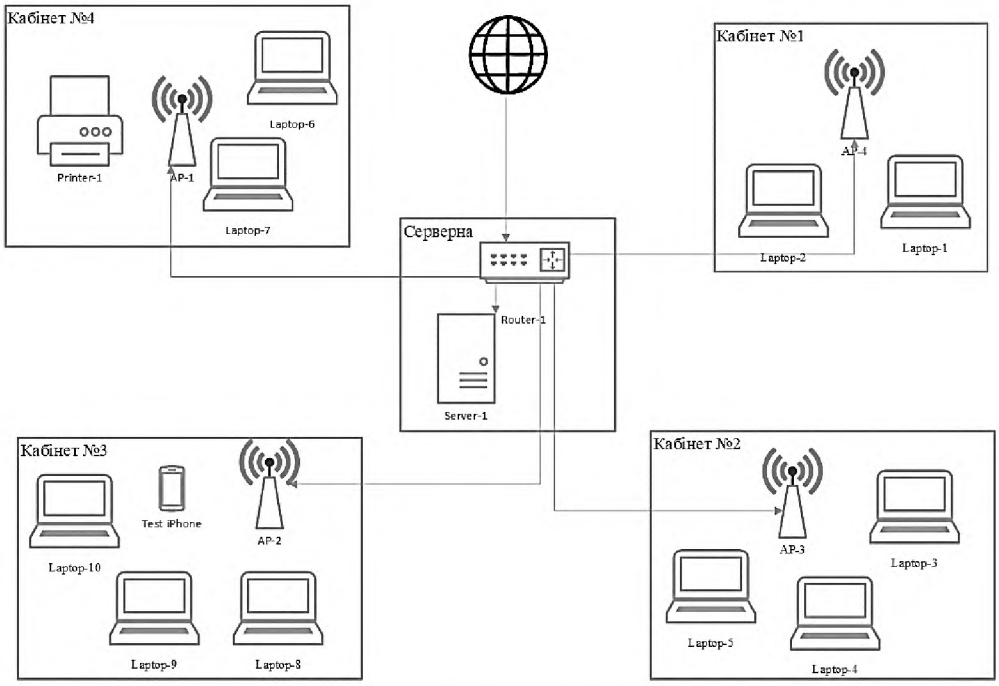


Рисунок 2.8 - Структурна схема ІТС

Таблиця 2.1 - Перелік ОТЗ

№	Позначка	Марка	Модель	Серійний номер	Розміщення	Відстань до границі КЗ, м
1	Laptop-1	HP	Pavilion Power 15	5CD9015 MHC	Кабінет №1, На столі	0.3
2	Laptop-2	Apple	MacBook Air (M1, 2020)	C02DT1P QQ6LC	Кабінет №1, На столі	0.2
3	Laptop-3	Apple	MacBook Air (M1, 2020)	FVFF23G 3Q6L5	Кабінет №2, На столі	0.4

Продовження таблиці 2.1 – Перелік ОТЗ

4	Laptop-4	Acer	Nitro AN515-52	A602082B EF6F	Кабінет №2, На столі	0.4
5	Laptop-5	Apple	MacBook Pro (Mid 2012)	CPWJM4 YMDTY3	Кабінет №2, На столі	0.4
6	Laptop-6	Apple	MacBook Pro (Mid 2012)	C02S81L GG8WN	Кабінет №3, На столі	0.2
7	Laptop-7	Asus	Eee PC 1001 PXD	A30AAS2 93237	Кабінет №3, На столі	1
8	Laptop-8	Asus	Laptop X415EA	AA7393E Q3001	Кабінет №3, На столі	0.2
9	Laptop-9	Asus	Laptop X415EA	LXBWR0 100714	Кабінет №4, На столі	0.2
10	Laptop-10	Asus	ZenBook 14	CNU0113 S08	Кабінет №4, На столі	0.2
11	Server-1	ARTLINE	Business R25v11	F463HS24 4021	Серверна,	0.3

Таблиця 2.2 - Перелік ДТЗ

№	Позначка	Марка	Модель	Серійний інвентаризаційний номер	Розміщення	Відстань до границі КЗ, м
1	Router-1	MikroTik	RB951Ui-2HnD	43CE02B 4E028	У технічному приміщені, на стіні	0.2

Продовження таблиці 2.2 - Перелік ДТЗ

№	Позначка	Марка	Модель	Серійний інвентаризаційний номер	Розміщення	Відстань до границі КЗ, м
2	Printer-1	Epson	L4150	0A19661 A3F	Кабінет №4, на столі	0.3
3	Test iPhone	iPhone	7S	DX3VC0 KEJSKT	Кабінет №3, на столі	0.3
4	AP-1…4	TP-LINK	RE190	220A4S10 02886	У всіх кабінетах, у розетці	0.2

2.2.2.1 Технічні характеристики апаратного забезпечення

Таблиця 3.2.1 – Таблиця технічних характеристик апаратного забезпечення

№	Позначення	Характеристика
1	Laptop-1	Intel Core i5-7300HQ (2.5 - 3.5 ГГц), ОЗУ 8 ГБ HDD 1 ТБ, NVIDIA GeForce GTX 1050
2	Laptop-2, 3	Apple M1 (8 ядер), ОЗУ 8 ГБ SSD 256 ГБ, Apple M1 (8 ядер)
3	Laptop-4	Intel Core i5-8300H (2.3 - 4.0 ГГц), ОЗУ 8 ГБ SSD 256 ГБ, NVIDIA GeForce GTX 1060 + Intel UHD Graphics 630
4	Laptop-5, 6	Intel Core i5-7300HQ (2.5 - 3.1 ГГц), ОЗУ 16 ГБ HDD 500 ГБ, Intel HD Graphics 4000
5	Laptop-7	Intel Atom N455 (1.66 ГГц), ОЗУ 4 ГБ HDD 500 ГБ, Intel HD Graphics 4000
6	Laptop-8, 9	Intel Pentium Gold 7505 (2.0 - 3.5 ГГц), ОЗУ 8 ГБ SSD 256 ГБ, Intel UHD Graphics

Продовження таблиці 4.2.1 – Таблиця технічних характеристик апаратного забезпечення

7	Laptop-10	Intel Core i3-1115G4 (3.0 - 4.1 ГГц), ОЗУ 8 ГБ SSD 256 ГБ, Intel UHD Graphics
8	Server-1	Intel 4-core Xeon E-2224G (3.5-4.7 ГГц), ОЗУ 16 ГБ 2x SSD 256 ТБ, Intel HD Graphics 4000
9	Router-1	AR9344 (600 МГц), ОЗУ 126 МБ HDD 126 МБ, OS RouterOS
10	Test iPhone	Apple A10 Fusion (2.3 ГГц), ОЗУ 3 ГБ NVMe HDD 128 ГБ, PowerVR GT7600
11	AP-1…4	Wi-Fi (802.11b/g/a, Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac)) Потужність 733 Мбіт/сек Швидкість Wi-Fi сигналу 750 Мбіт/сек

Таблиця 2.3 - Програмне забезпечення

№	Вид ПЗ	Назва	Ліцензія	Встановлено на
1	Системне	Windows 10 Corporation LTSC build 1809	Пропрієтарна	Laptop- 7-10
2		Linux Ubuntu 20.04 LTSC	GNU GPL	Laptop-1, 4
3		macOS Monterey v12.3.1	Пропрієтарна	Laptop-2, 3, 5, 6
5		CentOS 8.5 (2111)	GNU GPL	Server-1
6	Прикладне	Intellij IDEA 2022.1.1 build #IU-221.5591.52 (Студентська підписка)	Community edition: Apache License 2.0; Ultimate edition: Trialware	Laptop-1

Продовження таблиці 2.3 - Програмне забезпечення

№	Вид ПЗ	Назва	Ліцензія	Встановлено на
7	Прикладне	PhpStorm 2022.1.1 Build #PS-21.5591.58 (Студентська підписка)	Пропрієтарна	Laptop-4, 5
8		Xcode 13.4 (13F17a)	Суміш пропрієтарної та вільної ліцензій	Laptop-2,3
9		Mozilla Firefox 100.0.2	Потрійна ліцензія MPL / GPL / LGPL	Laptop-1-10
10		Git 2.35.1	GNU GPL v3	Laptop-1-5
11		Skype 8.83.0.409	Власницьке ПЗ, деякі можливості платні	Laptop-1-10

2.2.3 Обстеження інформаційного середовища підприємства

Таблиця 2.4 - Класифікація інформації, що обробляється в АС

№	Інформація	Режим доступу	Правовий режим	Тип представлення
1	Коди програм	ІзОД	Конфіденційна інформація	електронний
2	Дані працівників	ІзОД	Конфіденційна інформація	паперовий
3	База даних клієнтів	ІзОД	Конфіденційна інформація	електронний
4	Портфоліо компанії	відкрита	-	електронний

Продовження таблиці 2.4 - Класифікація інформації, що обробляється в АС

№	Інформація	Режим доступу	Правовий режим	Тип представлення
5	Документи фінансової звітності	відкрита	-	Паперовий, електронний

Технології обробки інформації:

Коди програм зберігаються на віддалених репозиторіях Gitlab/Github. Доступ до них дається після проходження двофакторної автентифікації профілю розробника. Після успішної автентифікації розробник можна клонувати код на робочу станцію, з якої він працює. У процесі розробки код повинен регулярно надсилатися на віддалений репозиторій. Після завершення проекту доступ розробнику до коду закривається.

Дані працівників зберігаються у HR-менеджера. Доступ до них, окрім менеджера, має лише директор компанії. Після звільнення робітника його дані зберігаються 2 роки, після чого знищуються.

База даних клієнтів зберігається та створюється директором компанії.

Портфоліо компанії є відкритим та знаходиться на офіційній веб-сторінці.

Документи фінансової звітності створює директор компанії.

Усі паперові носії інформації зберігаються у шафі з кодовим замком, пароль від якого знають HR-менеджер та директор компанії. Електронна інформація зберігається на віддалених серверах та базах даних.

2.2.4 Обстеження середовища користувачів

Таблиця 2.5 – співробітники компанії

№	Посада	Кількість осіб	Основні обов’язки	Рівень кваліфікації
1	Директор	1	Ведення юридичної документації; співпраця з клієнтами	Високий

Продовження таблиці 2.5 – співробітники компанії

№	Посада	Кількість осіб	Основні обов'язки	Рівень кваліфікації
2	HR-менеджер	1	Оформлення робітників	Високий
3	Розробник	5	Розробка ПЗ	Високий
4	Тестувальник	1	Тестування ПЗ	Середній
5	Системний адміністратор	1	Встановлення, налаштування, оновлення мережі;	Високий
6	Дизайнер	1	Створення макетів майбутнього ПЗ	Середній

2.3 Модель порушника

Відповідно до НД ТЗІ 1.1 003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» модель порушника – це абстрактний формалізований або неформалізований опис порушника.

Порушниками можуть виступати як і особи, що безпосередньо працюють на підприємстві, так і інші особи, що займаються тепло-, електро-, енерго- роботами, працівники конкуруючих компаній тощо.

У свою чергу порушники поділяються на внутрішні та зовнішні. Класифікувати порушників можна на: за рівнем знань про ІТС; за рівнем можливостей; за часом дії; за місцем дії. Нижче представлені таблиці класифікації можливих порушників

Таблиця 2.6 - Категорії порушників

Позначення	Визначення категорії	Рівень загрози
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал, що обслуговує приміщення (прибиральники), в яких розташовані компоненти ІТС	1

Продовження таблиці 2.6 - Категорії порушників

Позначення	Визначення категорії	Рівень загрози
ПВ2	Користувачі (оператори) ІТС	2
ПВ3	Адміністратори ІТС	3
Позначення	Визначення категорії	Рівень загрози
ПВ4	Керівник підприємства	4
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, еплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів	4

Таблиця 2.2 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Таблиця 2.8 Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.9 Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
31	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
32	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
33	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
34	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.10 Специфікація моделі порушника за часом дії

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

Таблиця 2.11 Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Складемо результуючу таблиця імовірних порушників підприємства та їх рівень загроз:

Таблиця 2.12 Модель внутрішнього порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Су ма загроз
Прибиральниця	ПВ1	М1	К1	З1	Ч4	Д1	9
	1	1	1	1	4	1	
Розробник	ПВ2	М1	К2	З1	Ч3	Д2	11
	2	1	2	1	3	2	
Тестувальник	ПВ2	М1	К2	З1	Ч3	Д2	11
	2	1	2	1	3	2	
Системний адміністратор	ПВ3	М3	К4	З3	Ч2	Д4	19
	3	3	4	3	2	4	
Директор	ПВ4	М2	К4	З2	Ч4	Д4	20
	4	2	4	2	4	4	

Таблиця 2.13 Модель зовнішнього порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Су ма загроз
Кандидат на посаду розробника	ПЗ1	М2	К2	З3	Ч4	Д1	13
	1	2	2	3	4	1	
Електрик	ПЗ2	М1	К1	З1	Ч1	Д1	7
	2	1	1	1	1	1	
Хакери	ПЗ3	М3	К3	З4	Ч3	Д1	17
	3	3	3	4	3	1	
Агент конкурентів	ПЗ4	М4	К3	З2	Ч4	Д2	19
	4	4	3	2	4	2	

Виходячи з результатів можна зробити висновок, що найбільшу загрозу для підприємства, з точки зору внутрішнього порушника, становить директор підприємства та системний адміністратор. З точки зору зовнішнього порушника – агент конкурентів.

2.4 Модель загроз

Відповідно до НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»:

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Модель загроз – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Було виконано аналіз загроз в ІТС та за результатами аналізу виділено суттєві загрози. Результати представлені в таблиці 2.9.

Таблиця 2.9 – Таблиця суттєвих загроз

№	Потенційні загрози для інформації в ІТС	Ризики для		
		К	Ц	Д
Загрози об'єктивної природи				
1.1	Стихійні явища		+	+
1.2	Відсутність електропостачання		+	+
1.3	Відмова/збій обчислювальної техніки		+	+
1.4	Відмова/збій програмного забезпечення	+	+	+
1.5	Пошкодження паперової документації	+	+	+
1.6	Відмова доступу до інтернету		+	+
Загрози суб'єктивної природи				
2.1	Втрата паролів			+
2.2	Розголошення ІзОД	+		
2.3	Відсутність резервного копіювання		+	+
2.4	Несанкціоноване підключення до ТЗ	+		
2.5	Хакерські атаки	+	+	

Продовження таблиці 2.9 – Таблиця суттєвих загроз

2.6	Пошкодження носіїв інформації		+	+
2.7	Вхід у систему недопущених осіб	+	+	+
2.8	Зараження комп'ютерними вірусами		+	+

Рівні ризиків та збитків:

- Високий – великі збитки (3 бали)
- Середній – помірні збитки (2 бали)
- Низький – незначні збитки (1 бал)

Було виконано оцінку ризиків. Результати представлені в таблиці 2.10

Ризики розраховувались за формулою: Рза ∗ Рзб, де

За- рівень загрози, зб – рівень збитку

Таблиця 2.10 – Таблиця оцінки ризиків

№	Джерело загрози	Вразливість	Рівень		Рівень ризику
			Загрози	Збитки	
1	Співробітники компанії	Розголошення ІзОД	3	3	9
2	Шкідливе ПЗ	Відсутність антивірусного ПЗ	1	2	2
3	Прослуховування каналу зв'язку за межами КЗ	Використання незахищеного каналу зв'язку	2	2	4
4	Агент компанії конкурента	Низька кваліфікація HR-відділу	3	3	9

Виходячи з таблиці, можна зробити висновок, що найбільші ризики пов'язані з співробітниками компанії та імовірними агентами конкурентів. У всі часи людський фактор був найбільшою вразливістю будь-якої системи.

2.5 Профіль захищеності

Відповідно до розглянутої АС та згідно НД ТЗІ 2.5-005-99, її можна віднести до класу «3» - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Функціонування підприємства залежить від конфіденційності та цілісності кодів програм. Виходячи з цього АС має підвищені вимоги до конфіденційності, цілісності та доступності.

Стандартний функціональний профіль захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації:

3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 2.11 Послуги профілю захищенності

Послуга	Назва	Опис
КД-2	Довірча конфіденційність	Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів.
КО-1	Повторне використання	Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.
КВ-1	Конфіденційність при обміні	Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Продовження таблиці 2.11 Послуги профілю захищенності

Послуга	Назва	Опис
ЦД-1	Довірча цілісність	Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.
ЦО-1	Відкат	Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути захищений об'єкт до попереднього стану.
ЦВ-1	Цілісність при обміні	Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.
ДР-1	Використання ресурсів	Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів.
ДВ-1	Відновлення після збоїв	Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування.
НР-2	Реєстрація	Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжуються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Продовження таблиці 2.11 Послуги профілю захищенності

Послуга	Назва	Опис
НИ-2	Ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС.
НК-1	Достовірний канал	Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ.
НО-2	Розподіл обов'язків	Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування.
НЦ-2	Цілісність КЗЗ	Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.
НТ-2	Самотестування	Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС.
НВ-1	Автентифікація при обміні	Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію.

КД-2. Базова довірча конфіденційність: Реалізовано за допомогою вбудованих можливостей операційних системи сімейства Linux, Windows та MacOS. В Linux та MacOS реалізується за допомогою вбудованої утиліти chmod. В ОС Windows реалізується з використанням налаштувань властивостей файлу. Розповсюджується на усі файли та процеси операційних систем.

КО-1. Повторне використання об'єктів. Реалізовано за допомогою вбудованих можливостей операційних системи сімейства Linux, Windows та MacOS. Якщо користувач спробує отримати доступ до об’єкту КС, який в той момент часу зайнятий іншими користувачем, то йому буде надіслано повідомлення «Об’єкт зайнятий іншим процесом».

КВ-1. Мінімальна конфіденційність при обміні. Не реалізовано.

ЦД-1. Мінімальна довірча цілісність. Реалізовано за допомогою вбудованих можливостей операційних системи сімейства Linux, Windows та MacOS. В Linux та MacOS реалізується за допомогою вбудованої утиліти chmod. В ОС Windows реалізується з використанням налаштувань властивостей файлу. Розповсюджується на усі файли та процеси операційних систем.

ЦО-1. Обмежений відкат. Реалізовано за рахунок вбудованих можливостей відновлення в усіх ОС. В ОС Windows реалізується за допомогою сервісу «Резервне копіювання та відновлення», у якому обирається цільовий диск (включаючи вибір папок) для резервування. В ОС Linux та MacOS використовується

ДВ-1. Ручне відновлення. В Windows реалізовано за допомогою сервісу «Відновлення», в якому обирається файл резервного копіювання. В Linux реалізується за допомогою завантаження операційної системи у Recovery режимі. MacOS використовує сервіс Time Machine.

НР-2. Зовнішній аналіз. Реалізовано усіма наявними ОС. Реєстрація подій ведеться системним журналом подій.

НИ-2. Одиночна ідентифікація і автентифікація. Реалізовано за рахунок токенів та/або виданого системним адміністратором паролю (одноразовий).

НК-1. Однонаправлений достовірний канал. Реалізовано.

НО-2. Розподіл обов'язків адміністраторів. Реалізовано можливостями операційних систем. В ОС Windows реалізується за допомогою групових політик. В ОС Linux та MacOS реалізується за допомогою сервісу chmod, створенням та налаштуванням group та other груп.

НЦ-2. КЗЗ з гарантованою цілісністю. Реалізовано.

НТ-2. Самотестування при старті. Реалізовано автоматичне самотествування на всіх представлених операційних системах за замовчуванням без участі користувача. У випадку проблеми користувач має бути проінформований про проблему.

НВ-1. Автентифікація вузла. Реалізовано усіма наявнимим ОС з використанням автентифікації за токеном та/або виданим системним адміністратором паролем.

2.6 Розробка комплексу засобів захисту

Відповідно до обраного профілю захищеності, було запропоновано наступний організаційний, програмно-технічний комплекс захисту з метою надання достатнього рівня захисту інформації з обмеженим доступом з урахуванням загроз, що були подані у таблиці 2.9 та 2.10:

1. Ввести посаду адміністратора безпеки;
2. Встановити КЗЗ «Гриф-Мережа» версії 3, виробництва ТОВ «Інститут комп'ютерних технологій», що відповідає вимогам нормативних документів системи технічного захисту інформації в Україні, в обсязі функцій, зазначених у документі «Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу «Гриф-Мережа» версія 3. Технічне завдання UA .21541987.00019-01 90 01». Експертний висновок №1034. Дійсний з 24.10.2019 до 24.10.2022;
3. Запровадити політики безпеки:
    1. Політика «Резервного копіювання коду»
    2. Політика «Парольного захисту користувачів»

2.6.1 Політика «Резервного копіювання вихідного коду»

Мета: встановити вимоги на проведення резервного копіювання коду, для запобігання втраті інформації при збоях обладнання та/або програмного забезпечення для написання.

Області дії: Політика розповсюджується на всіх робітників компанії, що займаються безпосередньо розробкою програмного забезпечення.

Відповідальність: будь-який співробітник, який порушив цю політику, може бути притягнутий до дисциплінарної відповідальності. У разі неодноразового порушення – до звільнення.

Зміст політики безпеки:

1. Програмні засоби
   - Резервування відбувається за допомогою системи контролю версій Git.
2. Сервери резервування
   - Серверами резервування мають виступати віддалені сервери-репозитроії.
   - Сервер-репозиторій може бути розгорнутий системним адміністратором на власний розсуд або за наказом директора компанії як в межах КЗ (на тестовому сервері), так і за допомогою хмарних рішень. За умови забезпечення доступності та конфіденційності.
   - Основним представником віддалених серверів-репозиторій є сервіс Gitlab.
3. Безпека резервування
   - Для безпечного резервування має використовуватися access_token користувача, що видається системним адміністратором під час створення облікового запису.
   - Резервування здійснюється з використанням SSH-ключа.

- Для генерації SSH-ключів слід використовувати вбудовану в наявних ОС утиліту ssh-keygen. Довжина ключа повинна бути не меншою 4096 біт.

4. Періодичність
   - 1 раз на годину, та 1 запит на злиття у кінці робочого дня.

2.6.2 Політика «Парольного захисту користувачів»

Паролі - один із найважливіших аспектів інформаційної безпеки, оскільки погано підібраний пароль підвищує потенційний ризик несанкціонованого доступу до інформаційної системи компанії.

Мета: встановити вимоги щодо створення, оновлення, використання паролів користувачами.

Область дії: ця політика стосується кожного співробітника, який має або відповідає за доступ до конфіденційної інформації всіх рівнів (або будь-яка форма доступу, яка підтримує або вимагає пароля) на будь-якій системі, обладнанні, що має доступ до інформації з обмеженим доступом

Відповідальність: будь-який співробітник, який порушив цю політику, може бути притягнутий до дисциплінарної відповідальності. У разі неодноразового порушення – до звільнення.

Зміст політики безпеки:

1. Оновлення паролю
   - Оновлення паролі відбувається, у першу чергу, при підозрі його компрометації.
   - В інших випадках – не рідше 1 разу на місяць.
2. Вимоги до створення та використання паролів
   - Кожний користувач має використовувати один пароль на один обліковий запис (робочі сервіси, обліковий запис в ОС тощо).
   - Заборонено передавати паролі третім особам, включаючи співробітників, керівника підприємства, родичам тощо.

– Довжина паролю повинна бути не менша 8 символів з використанням великих та маленьких літер латиниці, цифр та спец символів (0-9, !@#$%^&*()_+|~-=\`{}[[ ]]:«;'<>?,./).

3. Зберігання паролів

– Для зберігання паролів використовуються менеджери паролів (KeePass, 1Password)

– Браузери використовувати у інкогніто режимі, зокрема, не використовувати функцію «Запам'ятати мене».

2.6.3 Антивірусний захист

Одним із основних методів захисту є антивірусний захист. Для забезпечення безпеки на усіх ноутбуках, було запропоновано програмний продукт антивірусного захисту ESET Endpoint Antivirus для для усіх Windows (EEA) з системою централізованого керування ESET Remote Administrator, виробництва компанії ESET (Словаччина). Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows (EEA) версії 7.х з системою централізованого керування антивірусним захистом корпоративних мереж ESET Security Management Center версії 7.х. Технічні вимоги за критеріями технічного захисту інформації». Експертний висновок №995 Дійсний з 12.07.2019 до 12.07.2022. Також було проведено порівняльну характеристику даного засобу антивірусного захисту з іншим антивірусним програмним забезпеченням. Результати аналізу наведені в таблиці 2.12

Таблиця 2.12 – Порівняльна таблиця антивірусного ПЗ

	ESET Endpoint Antivirus	McAfee	BitDefender	Norton AntiVirus
Пробний період	+	+	-	-
Захист у	+	+	+	+

реальному часі				
VPN	+	-	+	+

Продовження таблиці 2.12 – Порівняльна таблиця антивірусного ПЗ

	ESET Endpoint Antivirus	McAfee	BitDefender	Norton AntiVirus
Видалення шкідливого ПЗ	+	+	+	+
Сканування вразливостей	+	-	+	-
Брандмауер	+	+	+	+

Висновок до розділу

У другому розділі було проведено обстеження підприємства, розглянуто та створено моделі порушника та загроз. На основі отриманих даних було вибрано профіль захищеності, що у свою чергу став основою для розробки та запровадження комплексну систему захисту інформації підприємства.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

У цьому розділі кваліфікаційної роботи метою є техніко- економічне обґрунтування доцільності запровадження КСЗІ. У свою чергу воно складається з розрахунку капітальних витрат, визначення трудомісткості розробки КСЗІ

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні витрати – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

3.1.1 Визначення трудомісткості розробки КСЗІ

Трудомісткість розробки КСЗІ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = tmз + tв + ta + tвз + tозб + tовр + tд, \text{ годин, де}$$

$tmз$ - тривалість складання технічного завдання на розробку політики безпеки інформації;

$tв$ - тривалість розробки концепції безпеки інформації у організації;

ta - тривалість процесу аналізу ризиків;

$tвз$ - тривалість визначення вимог до заходів, методів та засобів захист

$tозб$ - тривалість вибору основних рішень з забезпечення безпеки інформації;

$tовр$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$tд$ - тривалість документального оформлення політики безпеки.

$$t = 36 + 12 + 48 + 48 + 48 + 6 + 6 = 204$$

3.1.2 Розрахунок витрат на створення КСЗІ

Витрати на розробку КСЗІ $К_{рп}$ включають у себе заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу $З_{мч}$, що необхідний для розробки.

$$К_{рп} = З_{зп} + З_{мч} = 23872{,}08 + 912{,}83 = 24784{,}91$$

У свою чергу,

$З_{зп} = t * З_{іб} = 204 * 117{,}02 = 23872{,}08$, де

t – це загальна тривалість розробки КСЗІ, години

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину

$З_{мч} = t * С_{мч} = 94 * 9{,}71 = 912{,}83$, де

t – це трудомісткість розробки КСЗІ, години

$С_{мч}$ – це вартість 1 години машинного часу, грн./година, розраховується за формулою

$$С_{мч} = P * t_{нал} * C_e + \frac{Ф_{зал} * Н_а}{F_p} + \frac{К_{лпз} * Н_{апз}}{F_p}$$ грн/год, де

P – встановлена потужність ПК, кВт

$t_{нал}$ – кількість ПК, шт

C_e – тариф на електричну енергію, грн/кВ*тодина

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.

$Н_а$ – річна норма амортизації на ПК, частки одиниці

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.

ПЗ купується у компанії Jetbrains на офіційному сайті, а саме під ліцензією «All Product Pack» вартістю 19015 грн. Оновлення ліцензії відбувається кожен рік.

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці

F_p – річний фонд робочого часу (за 40-годинного робочого тижня $F_p = 1920$)

$$С_{мч} = 0{,}15 * 10 * 2{,}1 * \frac{13750*0{,}3}{1920} + \frac{19015*0{,}3}{1920} = 9{,}71 \text{ грн}$$

Вартість ноутбуку 22000 грн, строк служби 36 місяців

Накопичена амортизація: $\frac{(22000*36)}{(8*12)} = 8250$ грн

Залишкова вартість: $22000 - 8250 = 13750$

Таблиця 3.1 – Таблиця закупівлі апаратного забезпечення та допоміжних матеріалів

Найменування	**Кіл-ть, шт**	**Ціна, грн**
Маршрутизатор MikroTik RB951Ui-2HnD	1	1839

Продовження таблиці 3.1 – Таблиця закупівлі апаратного забезпечення та допоміжних матеріалів

Найменування	**Кіл-ть, шт**	**Ціна, грн**
Офісний сейф металевий	1	4100
Разом		5939

Таким чином, капітальні (фіксовані) витрати на проектування складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ де}$$

$К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість розробки КСЗІ, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. гри;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

$$К = 6700 + 19015 + 24784{,}91 + 5939 + 6700 = 63138{,}91 \text{ грн}$$

3.2 Розрахунок поточних витрат

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки розраховуються за формулою:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн}$$

$С_{в}$ – відновлення й модернізацію системи інформаційної безпеки;

$С_к$ – витрати на керування системою інформаційної безпеки;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки.

$$С_к = С_н + С_а + С_{а2} + С_з + С_{єв} + С_е + С_{ел} + С_о + С_{тос} \text{ грн}$$

Витрати на відновлення й модернізацію системи інформаційної безпеки ($С_в$) становить 6500 грн.

Витрати на навчання адміністративного персоналу и кінцевих користувачів на підприємстві відсутні.

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу – відсутні.

Річні амортизаційні відрахування матеріальних активів, що підлягають амортизації, визначатимуться, виходячи зі строку корисного використання 5 років. Таким чином, річні амортизаційні відрахування складуть:

$$С_а = \frac{1839+4100}{5} = 1187{,}8 \text{ грн}$$

Річні амортизаційні відрахування ПЗ, що підлягають амортизації, визначатимуться, виходячи зі строку корисного використання 2 роки. Таким чином, річні амортизаційні відрахування складуть:

$$С_{а2} = \frac{19015}{2} = 9507{,}5$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), розраховується за формулою:

$$С_з = З_{осн} + З_{дот}$$

$С_{осн}$ - основна заробітна плата. Визначається, виходячи з місячного посадового окладу.

$З_{дот}$ - додаткова заробітна плата - в розмірі 8-10% від основної заробітної плати

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 20000 грн. Додаткова заробітна плата - 10% від основної заробітної плати. Виконання роботи по реалізації КСЗІ погребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (20000 * 12 + 20000 * 12 * 0,1) * 0,25 = 66000 \text{ грн}$$

Ставка нарахування єдиного внеску з 01.01.2021 становить 22%.

$$С_{єв} = 66000 * 0,22 = 14520 \text{ грн}$$

Вартість електроенергії', що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = P * F_p * Ц_е, \text{ де}$$

P - встановлена потужність апаратури інформаційної безпеки, кВт;

F_p- річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$- тариф на електроенергію, грн/кВт-годин. Отже,

$С_{ел} = 0,15 * 1920 * 2,1 = 604,8$ грн

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються у відсотках від вартості капітальних витрат 3%.

$$С_{тос} = 63138,91 * 0,03 = 1894,17 \text{ грн}$$

Отже, $С_к = 1187,8 + 9507,5 + 66000 + 14520 + 604,8 + 1894,17 = 93714,27$ грн.

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) – відсутні.

Таким чином, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки становлять:

$$С = 6500 + 93714,27 = 100214,27 \text{ грн}$$

3.3 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. Фактично, ця величина відображає ту частину прибутку, що могла бути втрачена.

3.3.1 Оцінка величина збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки. Необхідні вихідні дані для розрахунку:

$t_п$ — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 годин;

$t_в$ — час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 1 година;

$t_{ви}$ — час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 5 годин;

$З_о$ — заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 22000 грн на місяць;

$З_с$ - заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15000 грн на місяць;

$Ч_о$ - чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 осіба;

$Ч_с$ - чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 10 осіб.;

О - обсяг прибутків атакованого вузла або сегмента корпоративної мережі, 500 тис. грн. у рік;

$П_{зч}$ - вартість заміни встаткування або запасних частин, 3000 грн;

I – число атакованих вузлів або сегментів корпоративної мережі; 2

N - середнє число атак на рік. 5

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \text{ де}$$

$П_п$ - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ - вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V - втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с}{F} * t_п = \frac{15000*10}{176} * 2 = 1704{,}54 \text{ грн, де}$$

F - місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ де}$$

$П_{ви}$ - витрати на повторне уведення інформації, грн;

$П_{пв}$ - витрати на відновлення вузла або сегмента корпоративної мережі, грн.

$П_{зч}$ - вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви} = \frac{15000*10}{176} * 5 = 4261{,}36 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} * t_в = \frac{22000}{176} * 1 = 125 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{F_г} * (t_п + t_в + t_{ви}) = \frac{500000}{2080} * (2 + 1 + 5) = 1923{,}08 \text{ грн}$$

Fг - річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Вартість заміни устаткування або запасних частин може становити близько 3000 грн.

Вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.):

$$П_в = 4261,36 + 125 + 3000 = 7386,36 \text{ грн}$$

$$U = 1704,54 + 7386,36 + 1923,08 = 11013,98 \text{ грн}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_2 \sum_5 11013,98 = 110139,8 \text{ грн}$$

3.3.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$E = B * R - C$, де

В - загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. гри;

R - очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці.

С - щорічні витрати на експлуатацію системи інформаційної безпеки, тис. гри.

$$E = 110139,8 * 0.5 - 90706,77 = 459992,23 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

а) сукупна вартість володіння (ТСО);

б) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

в) термін окупності капітальних інвестицій T_o.

Показник сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже

$$ROSI = \frac{E}{K}, \text{ частка одиниці, де}$$

Е - загальний ефект від впровадження системи інформаційної безпеки, тис. гри;

К - капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. гри.

$$ROSI = \frac{459992,23}{63138,91} = 7,28, \text{ частки одиниці}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$ROSI > \frac{N_{\text{деп}} - N_{\text{інф}}}{100}$, де

$N_{\text{деп}}$- річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 6%;

$N_{\text{інф}}$- річний рівень інфляції, 5,5%.

$$7,28 > \frac{6 - 5,5}{100} = 7,28 > 0,005$$

Виходячи з розрахунків розробка та впровадження КСЗІ є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{7{,}28} = 0{,}13 \text{ роки (1.5 місяці)}$$

Висновок до розділу

У третій частині були проведені розрахунки з економічної доцільності розробки та впровадження КСЗІ на підприємстві. Капітальні витрати складають 63138,91 грн. Щорічні експлуатаційні витрати - 100214,27 грн. ROSI становить 7,28, а величина ефекту 459992,23 грн. Цей коефіцієнт перевищує величину річної депозитної ставки з урахуванням інфляції, і можна вважати впровадження КСЗІ економічно доцільним. Термін окупності капітальних інвестицій становить 0,13 роки (1.5 місяці).

ВИСНОВКИ

У першому розділі кваліфікаційної роботи проаналізована статистика кіберінцидентів в Україні за 2021 рік. Розглянуто нормативно-правову базу та поставлено задачу на створення КСЗІ на підприємстві.

У спец розділі проведено обстеження середовища, розроблено моделі порушника, в якому найбільшу загрозу становлять директор компанії та агент компанії конкурента, та загроз, проведена оцінка збитків та вразливостей. Було вибрано профіль захищеності, запропоновано комплекс засобів захисту.

В економічному розділі проведено розрахунок економічної доцільності розробки та впровадження КСЗІ. Капітальні витрати складають 63138,91 грн. Експлуатаційні витрати - 90706,77 грн/рік. Розрахований ROSI-коефіцієнт дорівнює 0,74. Термін окупності капітальних інвестицій становить 1,4 роки.

На вимогу керівництва компанії, її назва та місцерозташування були змінені без суттєвих змін, що не вплинуло на результати роботи.

ПЕРЕЛІК ДЖЕРЕЛ

1. Статистика кіберінцидентів за 2021 рік в Україні. [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://glavcom.ua/country/incidents/fahivci-rozpovili-chim-bavilisya-hakeri-u-2021-813090.html
2. Статистика кіберінцидентів за перший квартал 2022 ріку у світі [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
3. Хакерська атака вірусом-шифрувальщиком на компанію SoftServe у 2020 році [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://ain.ua/ru/2020/09/03/softserve-xaknuli-2/
4. Закон України «Про захист інформації в інформаційно-комунікаційних системах» [Електронний ресурс]. – 1994. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
5. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Textv
6. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/1.1_003_99.pdf
7. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-004-99.pdf
8. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-005%20-99.pdf

9. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7-003-2005.pdf
10. НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категорювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.6-005-2013.pdf
11. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
12. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упорядн. Д. П. Пілова. - Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.
13. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін , Ю.А. Мілінчук - Дніпро: НТУ «ДП», 2020. -47 с

Додаток А. Відомості матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	2	
2	А4	Список умовних позначень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	3	
6	А4	Спеціальна частина	25	
7	А4	Економічний розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

Додаток Б. Акт категорювання

Гриф обмеження доступу

Прим. № ___

ЗАТВЕРДЖУЮ

Керівник установи-власника (розпорядника,

користувача) об'єкта

Директор Гайдамашко О. М.
(посада, підпис, ініціали, прізвище)

01.03.2022

М. П.

АКТ

Категорювання ТОВ «ПІНТА ВЕБВАРЕ»
(найменування об'єкта категоріювання)

1. Підстава для категорювання _____наказ про створення КСЗІ_____
(рішення про створення КСЗІ, закінчення терміну дії акта категорювання,
_____
зміна ознаки, за якою була встановлена категорія об'єкта, тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категорювання)

2. Вид категорювання:_____первинне_____
(первинне, чергове, позачергове)
_____
(у разі чергового або позачергового категорювання вказується категорія, що була встановлена до цього категорювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється _____обробка інформації технічними засобами_____

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті_____конфіденційна інформація_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія: IV категорія, до якої відносяться об'єкти, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці.

Голова комісії Гайдамашко О М.

Члени комісії Любченко В. В.

Додаток В. Наказ на створення КСЗІ

ТОВАРИВСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНСТЮ
«ПІНТА ВЕБВАРЕ»
(ТОВ «ПІНТА ВЕБВАРЕ»)

НАКАЗ №5

м. Дніпро 01.03.2022

Про організацію робіт зі створення комплексної системи захисту інформації в автоматизованій системі (далі - АС) класу ”3” підприємства

Відповідно до вимог Закону України "Про захист інформації в інформаційно-телекомунікаційних системах". Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 року № 1229/99 та Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, для забезпечення технічного захисту інформації (ТЗІ) при обробці інформації з обмеженим доступом, що не становить державної таємниці.

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації (далі КСЗІ) в АС класу "3” призначеній для обробки інформації з обмеженим доступом, що не становить державної таємниці;
2. Відповідальним за створення КСЗІ та впровадження заходів із захисту інформації призначити системного адміністратора Лимаренко В. І.
3. Контроль за виконанням залишаю за собою.

Директор Гайдамашко О. М.

Додаток Г. Перелік матеріалів на оптичному носії

Дзеркаль_РА_125_18_2_ПЗ.docx

Дзеркаль_РА_125_18_2_ПЗ.pdf

Дзеркаль_РА_125_18_2_ДМ.pptx

Дзеркаль_РА_125_18_2_ПЗ.pdf.p7s

Додаток Д. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 85 б. («добре»).

Керівник економічного розділу _____ доц. Пілова Д. П.

(підпис) (ініціали, прізвище)

Додаток Е. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125-18-2

Дзеркаля Романа Артуровича

на тему: «Комплексна система захисту інформації інформаційно телекомунікаційної системи ТОВ «ПІНТА ВЕБВАРЕ»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 43 сторінках.

Метою кваліфікаційної роботи є забезпечення достатнього рівня захисту інформації в ІТС ТОВ «ПІНТА ВЕБВАРЕ».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз автоматизованих засобів збору інформації; обстеження фізичного, інформаційного середовищ та середовища користувачів; проведено аналіз імовірних загроз та вразливостей; обрано профіль захищеності.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності захисту інформації на підприємстві, за рахунок розробки та запровадження програмно-технічних та організаційних засобів.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Дзеркаль Р. А. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки 85 «добре».

Керівник кваліфікаційної роботи **Кагадій Т. С.**

Керівник спец. розділу **Тимофєєв Д. С.**