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

студентки *Марченко Поліни Валентинівни*

академічної групи *125-18-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	професор Корнієнко В. І.			
розділів:				
спеціальний	ст. викл. Кручінін О. В.			
економічний	к. е. н., доц. Пілова Д. П.	94 б.	Відмінно	

Рецензент				

Нормоконтролер				

Дніпро
2022

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

«_____»_____2022 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенці *Марченко Поліні Валентинівні* **академічної групи** *125-18-3*

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс»*

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

Розділ	Зміст	Термін виконання
Розділ 1	*Загальні відомості про підприємство «Сай.Фокс». Обстеження інформаційно-телекомунікаційної системи. Аналіз загроз інформації, що циркулює в ІТС підприємства.*	13.03.2022 – 17.04.2022
Розділ 2	*Розробка політики безпеки інформації. Повторний аналіз загроз після впровадження політики.*	18.05.2022 – 30.05.2022
Розділ 3	*Обґрунтування доцільності витрат на впровадження політики безпеки інформації*	01.06.2022 – 09.06.2022

Завдання видано: Кручінін О. В.

Дата видачі: 13.03.2022р

Дата подання до екзаменаційної комісії:

Прийнято до виконання: Марченко П. В.

РЕФЕРАТ

Пояснювальна записка: 82 с., 9 рис., 26 табл., 4 додатка, 12 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс».

Мета кваліфікаційної роботи: забезпечення необхідного рівня безпеки інформації в інформаційно-телекомунікаційній системі ТОВ «Сай.Фокс».

У першому розділі кваліфікаційної роботи наведено відомості про підприємство (рід діяльності, графік роботи та штат). Виконано огляд середовищ функціонування ІТС: фізичне середовище, обчислювальна система, інформаційне середовище та середовище користувачів. Розроблено модель порушника та модель загроз. Визначено елементи політики безпеки, які необхідно запровадити на підприємстві.

У другому розділі представлено елементи політики безпеки для забезпечення безпеки інформації в ІТС (розмежування доступу, антивірусного захисту, використання мережі Інтернет на підприємстві, передачі документів в електронному вигляді, «чистого» стола/екрану, створення та використання паролів, доступу сторонніх осіб до підприємства). Представлено результати повторний аналіз загроз після введення політик.

У третьому розділі визначено економічну доцільність впровадження створених елементів політики безпеки. Проведено розрахунок капітальних витрат, поточних витрат, оцінки величини збитку при виникненні загроз.

Практична цінність роботи полягаю у адаптації елементів політики безпеки до особливостей інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс».

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, БЕЗПЕКА ІНФОРМАЦІЇ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ВРАЗЛИВОСТІ, ЗАГРОЗА

РЕФЕРАТ

Пояснительная записка: 82 с., 9 рис., 26 табл., 4 приложения, 12 источников.

Объект разработки: политика безопасности информации информационно-телекоммуникационной системы ООО «Сай.Фокс».

Цель квалификационной работы: обеспечение необходимого уровня безопасности информации в информационно-телекоммуникационной системе ООО «Сай.Фокс».

В первом разделе квалификационной работы представлены сведения о предприятии (род деятельности, график работы и штат). Проведен обзор сред функционирования ИТС: физическая среда, вычислительная система, информационная среда и среда пользователей. Разработаны модель нарушителя и модель угроз. Определены элементы политики безопасности, которые необходимо ввести на предприятии.

Во втором разделе представлены элементы политики безопасности для обеспечения безопасности информации в ИТС (разграничение доступа, антивирусной защиты, использование сети Интернет на предприятии, передача документов в электронном виде, «чистого» стола/экрана, создание и использование паролей, доступ сторонних лиц на предприятие). Представлены результаты повторного анализа угроз после введения политик.

В третьей главе определена экономическая целесообразность внедрения созданных элементов политики безопасности. Произведен расчет капитальных затрат, текущих затрат, оценки величины ущерба при возникновении угроз.

Практическая ценность работы состоит в адаптации элементов политики безопасности к особенностям информационно-телекоммуникационной системы ООО «Сай.Фокс».

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ НАРУШНИКА, МОДЕЛЬ УГРОЗ, БЕЗОПАСНОСТЬ ИНФОРМАЦИИ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА, УЯЗВИМОСТИ, УГРОЗА

ABSTRACT

Explanatory note: 82 p., 9 pic., 26 tab, 4 applications, 12 sources.

Object of development: information security policy of the information and telecommunications system of LLC “Cy.Fox”.

The purpose of the qualification work: ensuring the required level of information security in the information and telecommunication system of LLC "Cy.Fox".

In the first chapter of the qualification work provides information about the company (type of activity, work schedule and staff). An overview of ITS operating environments: physical environment, computer system, information environment and user environment. The model of the violator and the model of threats have been developed. It is determined which elements of security policy should be implemented at the enterprise.

In the second chapter, presents security policy elements to ensure the security of information in ITS (differentiation of access, antivirus protection, use of the Internet in the enterprise, electronic transmission of documents, "clean" table/screen, creation and use of passwords, access to third parties). The results of the re-analysis of threats after the introduction of policies are presented.

In the third chapter identifies the economic feasibility of implementing the created elements of security policy. The calculation of capital costs, current costs, estimates of the amount of damage in the event of threats.

The practical value of the work lies in the adaptation of security policy elements to the features of the information and telecommunication system of LLC "Cy.Fox".

SECURITY POLICY, VIOLATION MODEL, MODEL OF THREAT, SECURITY OF INFORMATION, INFORMATION AND TELECOMMUNICATIONS SYSTEM, VULNERABILITIES, THREAT

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

ТОВ – товариство з обмеженою відповідальністю;

ІТС – інформаційно-телекомунікаційна система;

ПБ – політика безпеки;

ТЗ – технічне завдання;

ПЗ – програмне забезпечення;

ІзОД – інформація з обмеженим доступом;

ОІД – об’єкт інформаційної діяльності;

ПК – персональний комп’ютер;

ПЗ – програмне забезпечення;

НД ТЗІ – нормативний документ в галузі технічного захисту інформації;

ІПН – індивідуальний податковий номер;

АС – автоматизована система.

ЗМІСТ

ВСТУП

Сьогодні все більше сфер нашого життя переходить до інформатизації. Здавалося б, немає такої сфери людської діяльності, в якій ми не використовуємо інформації та телекомунікаційні технології. Вони активно використовуються у всіх сферах життя – науковій, фінансовій, транспортній, промисловій, комерційній, торговій та соціальній.

Інформатизація має великий вплив на економіку, а саме її управління, на розвиток та автоматизацію виробництва, більш швидке підвищення продуктивності праці, збільшення збуту та покращення соціально-економічних відносин.

Розвиток та зростання підприємства тісно пов'язане зі зростанням інформатизації. Складність та масштаби інформаційних систем постійно зростають, породжуючи при цьому нові види загроз, вразливостей та ризиків, які мають безпосередній вплив на організацію.

Майже кожна інформаційна система містить інформацію, розкриття якої третім особам може завдати шкоди її власнику, компанії або особі, якої ця інформація стосується. Тому забезпечення безпеки інформації є особливо актуальна на підприємствах.

Безпека інформації – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. [1]

Політика безпеки інформації – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо які регламентують порядок обробки інформації. [1]

Для політики безпеки необхідно провести обстеження інформаційно-телекомунікаційної системи та проаналізувати загрози які є актуальними для підприємства. Після чого можна зрозуміти які політики необхідно розробити для даної організації.

Отже, метою даної кваліфікаційної роботи є розробка рекомендацій щодо вдосконалення політики безпеки для забезпечення захисту від існуючих загроз в інформаційно-телекомунікаційних системах.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство «Сай.Фокс»

У кваліфікаційній роботі розглянуто ТОВ «Сай.Фокс» яке займається брендингом на замовлення. Воно знаходиться за адресою: Дніпропетровська обл., м. Дніпро, вул. Надії Алексєєнко 21. ОІД розташований на четвертому поверсі семиповерхового будинку з адміністративними приміщеннями.

Агентство надає послуги брендингу, а саме організація розробляє унікальні бренди та логотипи, створює візуально-графічні марки, а також підготовлює та запускає рекламу, що швидко та легко запам'ятаються.

Підприємство працює п'ять днів на тиждень згідно з графіком – з понеділка по п'ятницю з 9:00 до 18:00. Обідня перерва з 12:00 до 13:00. Субота та неділя є вихідними.

Ключі від офісу знаходяться у всіх співробітників. Допуск сторонніх осіб в приміщення відбувається лише у робочий час. У підприємства підписаний договір з охоронною фірмою. Охорона території підприємства у неробочий час забезпечується сигналізацією, у разі спрацювання якою до об'єкта виїжджає силова бригада.

Штат складається з 7 працівників:

- директор – 1 особа;
- креативний директор – 1 особа;
- дизайнер – 3 особи;
- бухгалтер – 1 особа;
- SEO-спеціаліст – 1 особа;

1.1 Обстеження ІТС

Під час обстеження ІТС буде розглянуто наступні пункти:

- обстеження фізичного середовища;
- обстеження обчислювальної системи;
- обстеження інформаційного середовища;
- обстеження середовища користувача.

1.1.1 Обстеження фізичного середовища

Об’єкт знаходиться за адресою: Дніпропетровська обл., м. Дніпро, вул. Надії Алексєєнко 21 у семиповерховому будинку. Будівля в якій знаходиться офіс побудована з білої цегли, де перекриття зроблено з залізобетонних плит. Фундамент виконано з залізобетонних забивних паль. Будівля має плоский дах покритий руберойдом. Вікна металопластикові.

Контрольованою зоною даного підприємства є зона обмежена зовнішніми стінами будівлі, в інших сторін – коридором та інші офісні приміщення. На поверхах вище та нижче знаходяться інші офісні приміщення.

Ситуаційний план на якому вказано місце розташування ОІД та усіх навколишніх об’єктів наведено на рис. 1.1.

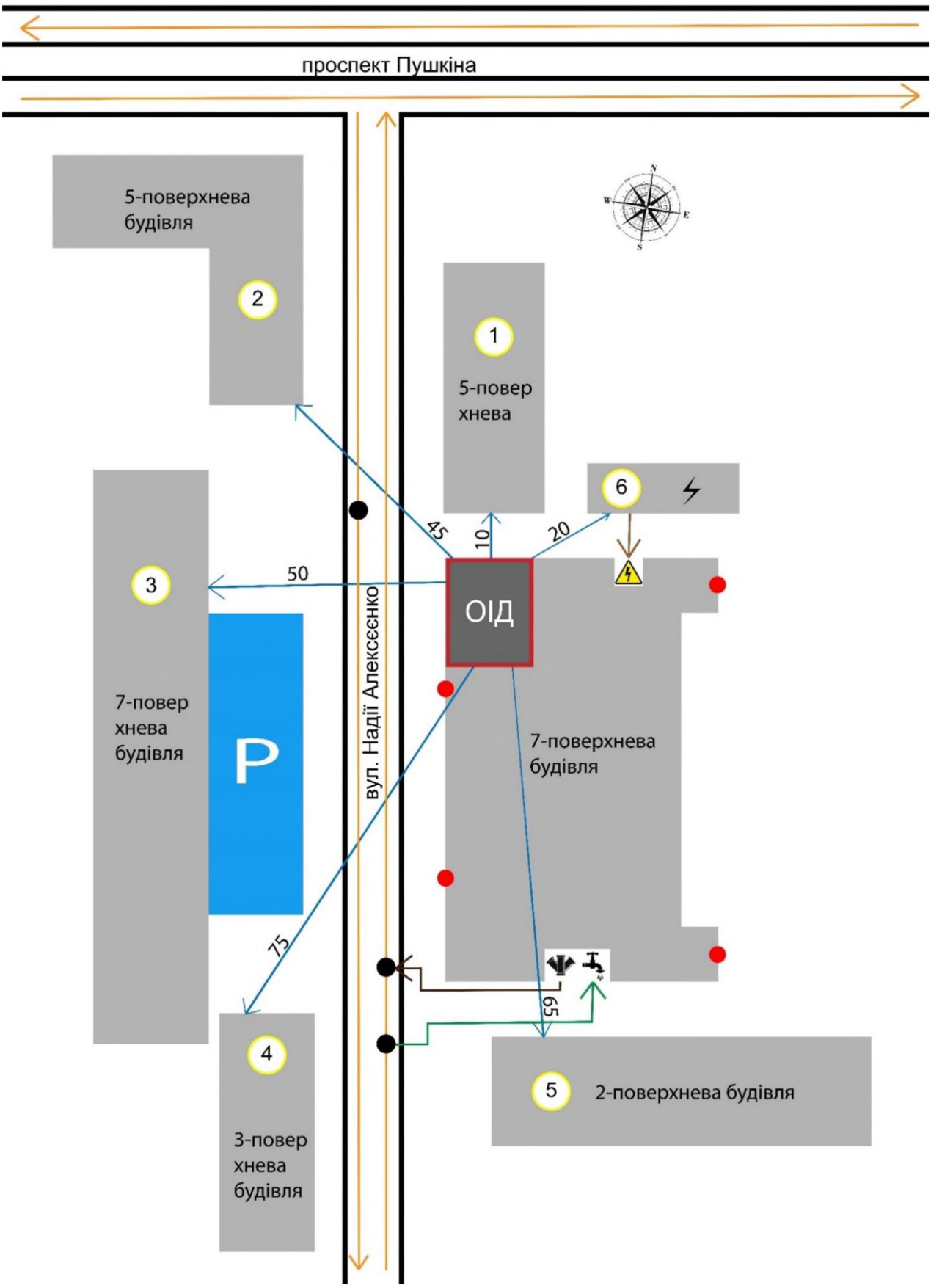


Рисунок 1.1 – Ситуаційний план

Умовні позначення

В табл. 1.1 наведено перелік будівель, розташованих навколо будівлі де розташований ОІД.

Таблиця 1.1 – Будівні, що знаходяться поруч з ОІД.

№	Тип об'єкту	Адреса	Кількість поверхів	Розташування відносно ОІД	Мінімальна відстань до ОІД, м
1	Житловий будинок, дрібні магазини	вул. Надії Алексєєнко, 19	5	Пн	10

Продовження таблиці 1.1

№	Тип об’єкту	Адреса	Кількість поверхів	Розташування відносно ОІД	Мінімальна відстань до ОІД, м
2	Житловий будинок	вул. Надії Алексєєнко, 22	5	Пн-Сх	45
3	Офісна будівля, поштові відділення	вул. Надії Алексєєнко, 30	7	Сх	50
4	Житловий будинок	вул. Надії Алексєєнко, 32	3	Пд-Сх	75
5	Житловий будинок	вул. Надії Алексєєнко, 23	2	Пд	65
6	Трансформаторна підстанція	вул. Надії Алексєєнко, 21	1	Пн-Зх	20

На рис. 1.2 зазначено генеральний план ОІД з розміщенням основних виробничих приміщень підприємства.

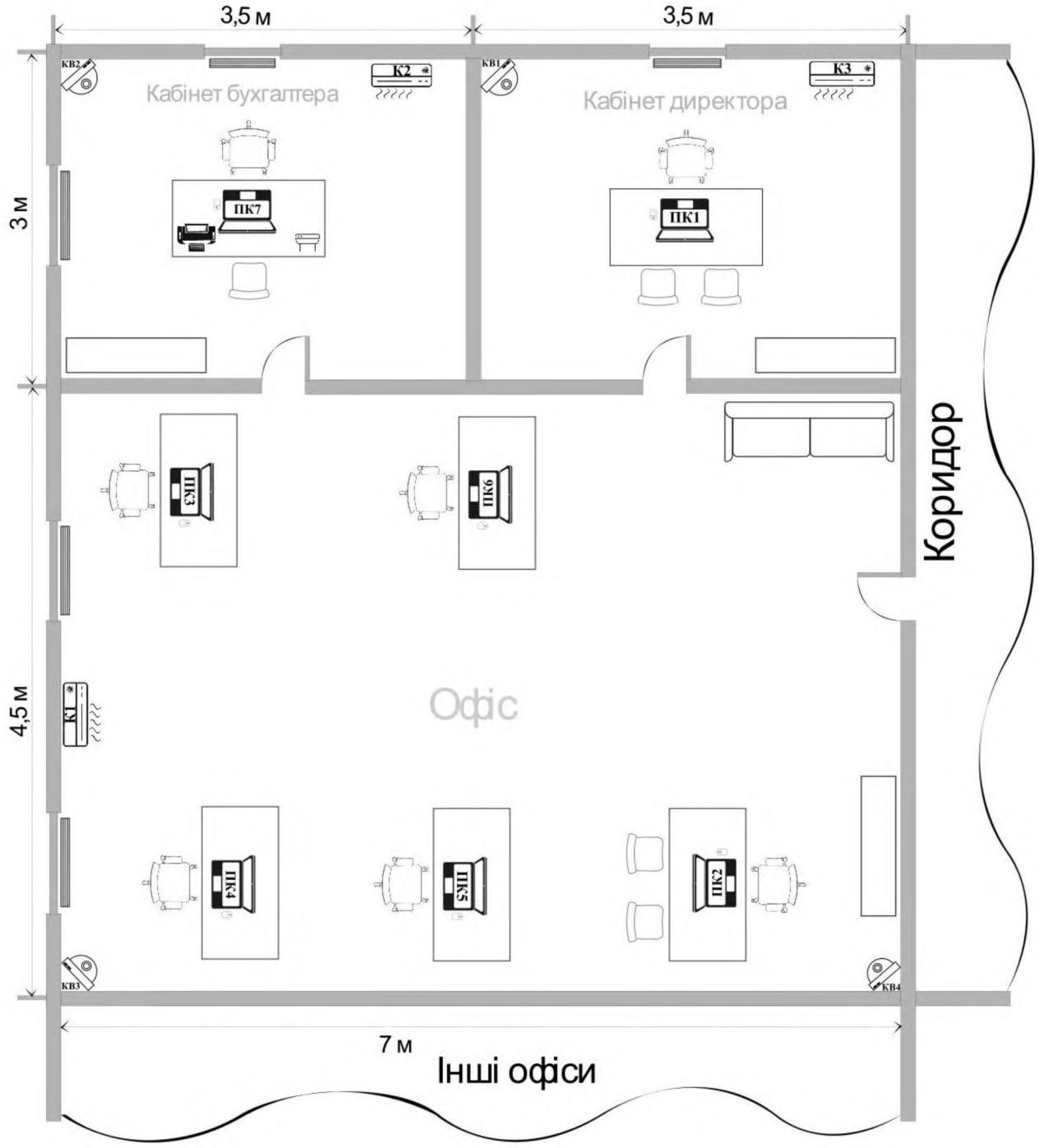


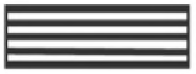
Рисунок 1.2 – Генеральний план ОІД

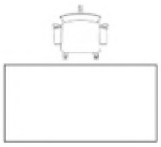
Умовні позначення

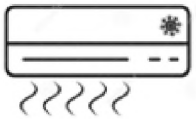

Стіна

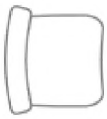

Шафа


Двері


Батарея


Робоче місце


Кондиціонер


Стілець


Принтер


Диван


Роутер


Ноутбук


Камера відеоспостереження


Комп'ютерна миша

Підписані обладнання:

- ПК1 – ноутбук директора;
- ПК 2 – ноутбук креативного директора;
- ПК3 – ноутбук дизайнера;
- ПК4 – ноутбук дизайнера;
- ПК5 – ноутбук дизайнера;
- ПК6 – ноутбук SEO-спеціаліста;
- ПК7 – ноутбук бухгалтера;
- К1 – кондиціонер;
- К2 – кондиціонер;
- К3 – кондиціонер;
- КВ1 – камера відеоспостереження;

- КВ2 – камера відеоспостереження;
- КВ3 – камера відеоспостереження;
- КВ4 – камера відеоспостереження.

На рис. 1.3 зображено схему електропроводки та Інтернету всередині приміщень підприємства.

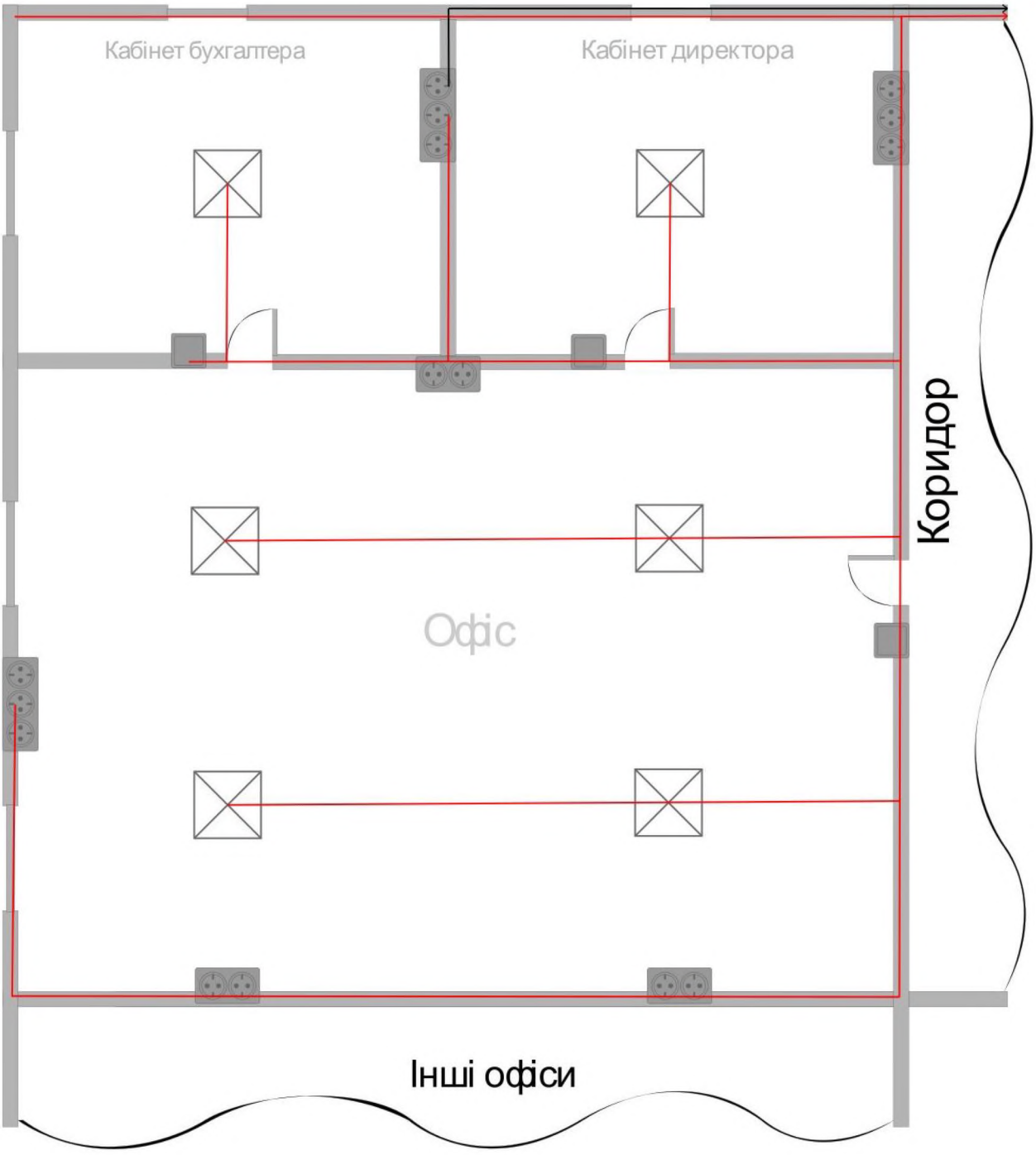
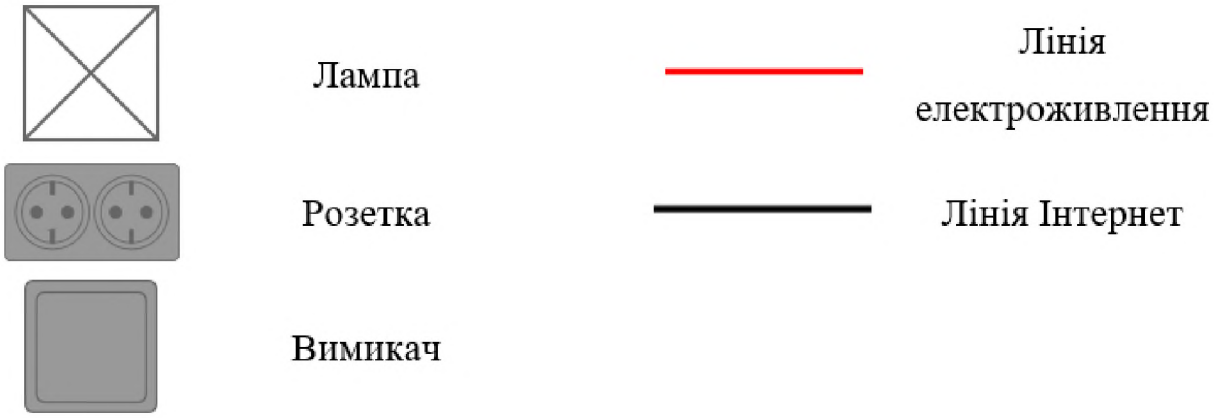


Рисунок 1.3 – Схема електропроводки та Інтернету

Умовні позначення



На рис. 1.4 зображено схему охороно-пожежної сигналізації.

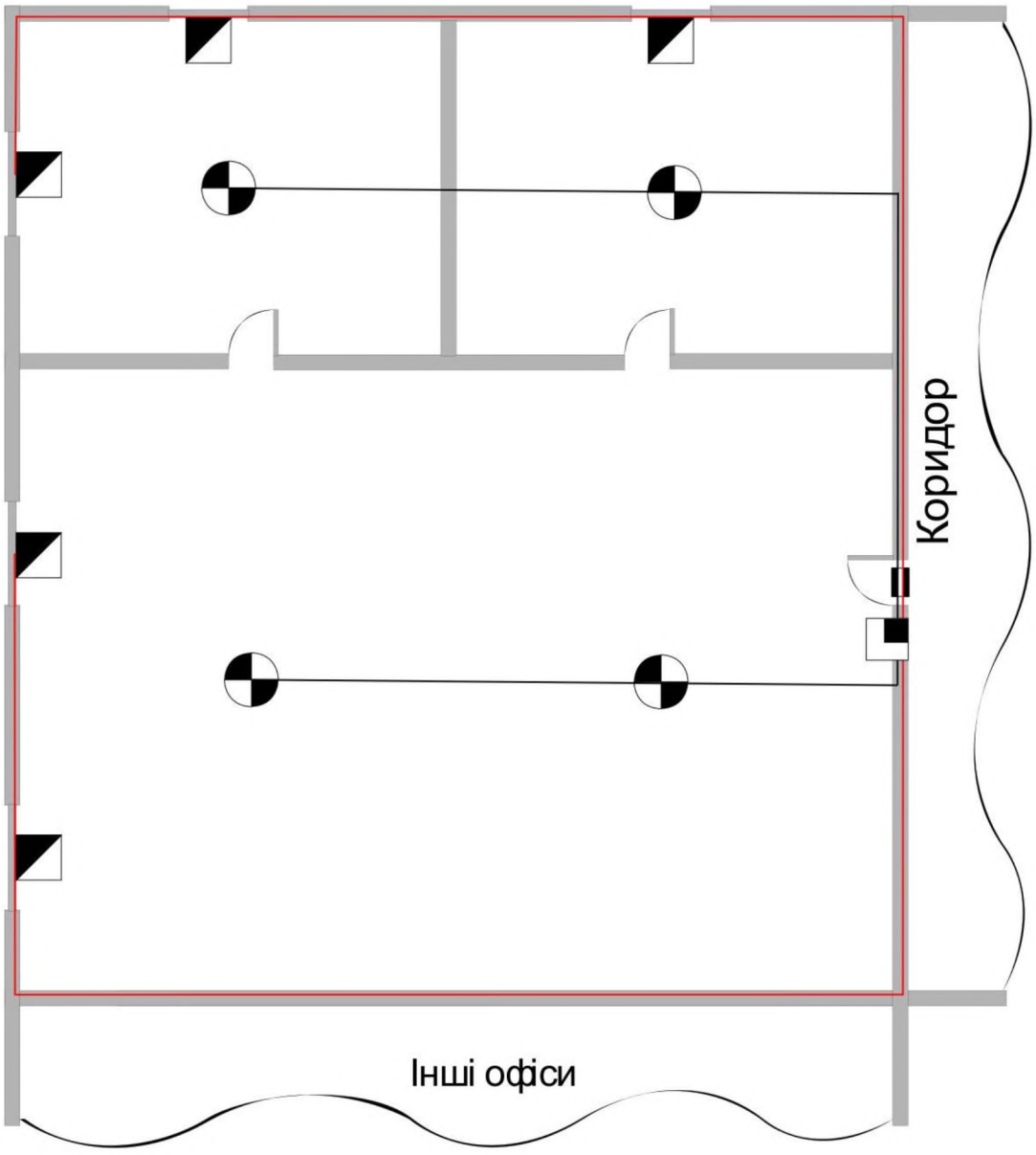


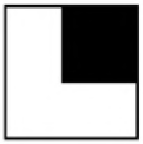
Рисунок 1.4 – Схема охороно-пожежної сигналізації

Умовні позначення

Пожежні сповіщувач

Магнітоконтактний сповіщувач

Датчик розбиття скла



Приймально-контрольований пристрій

Лінія живлення пожежних сповіщувачів

Лінія живлення системи сигналізації

Більш точні фізичні характеристики:

- товщина несучих стін – 400 мм;
- товщина перегородки – 150 мм;
- висота стелі – 3 м;
- стеля – залізобетонна плита – 200 мм;
- підлога – монолітна бетонна стяжка – 100 мм;
- підлога покрита ламінатом – 10 мм;
- вікна вироблені з металопластику з подвійним склопакетом – 5 штук;
- розміри вікон – 3 по 1500 мм * 1500 мм, 2 по 1000 мм * 1500мм;
- двері міжкімнатні вироблені з ламінованого МДФ – 2 штуки;
- розміри внутрішніх дверей – 800 мм * 2000 мм;
- вхідні двері вироблені зі звареної листової сталі, оздоблені електронним кодовим замком, що відкривається за допомоги коду та звичайним ключем;
- розміри вхідних дверей – 900 мм * 2000 мм;
- підключення до мережі Інтернет здійснюється оптоволоконним кабелем та надається компанією «Фрегат»;
- електроенергія до будівлі подається з трансформаторної підстанції, яка розташована за межами ОІД – 220 В;

- система водопостачання та каналізації підключені до міської системи та підведено під землею;
- система опалення підключена до міської мережі опалення, проходить під землею до підвалу, та розмежовується вертикально до інших приміщень;
- спліт-система кондиціонування складається з 3 кондиціонерів та вмикається тільки при необхідності;
- система заземлення – відсутня;
- є охороно-пожежна сигналізація;
- є 4 камери відеоспостереження, які використовуються для контролю поточної ситуації всередині підприємства.

Розміри приміщень:

- загальна площа ОІД – 52 м^2
- кабінет директора – 10,5 м^2;
- кабінет бухгалтера – 10,5 м^2;
- офіс – 31 м^2.

1.2.2 Обстеження обчислювальної системи

Обчислювальна система поєднує в собі технічні пристрої, що знаходяться в межах ОІД. На території підприємства знаходиться 7 персональних комп'ютерів, принтер, Wi-Fi роутер, 4 камери та три кондиціонера. Кожен комп'ютер закріплений за певним співробітником. Усі працівники мають доступ до принтеру через мережу Wi-Fi. У кожного на підприємстві є свій обліковий запис, доступ до якого має лише він.

Кожен з комп'ютерів підключається до мережі Інтернет від Wi-Fi роутера. Підключення моє архітектуру «зірка». На точці доступу Wi-Fi знаходиться простий пароль, який ніколи не змінювався.

Обладнання за допомогою якого обробляється інформація:

- ПК1 – ноутбук директора;

- ПК 2 – ноутбук креативного директора;
- ПК3, ПК4, ПК5 - ноутбуки дизайнерів;
- ПК6 – ноутбук SEO-спеціаліста;
- ПК7 – ноутбук бухгалтера;
- Принтер;
- Wi-Fi роутер;
- Камери відеоспостереження (камера 1, камера 2, камера 3, камера 4).

На рис. 1.5 зображено структурну схему мережі інформаційно-телекомунікаційної системи.

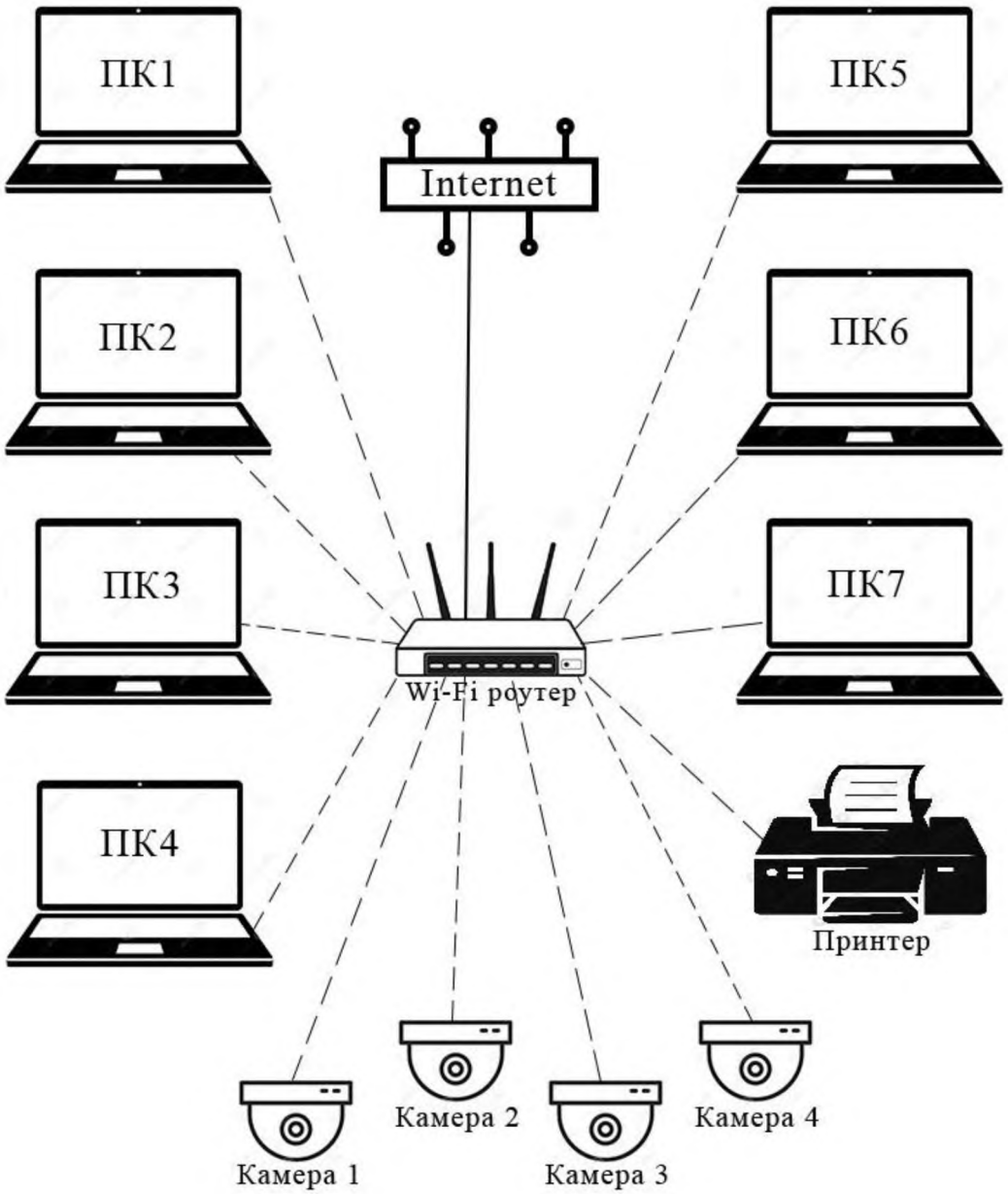


Рисунок 1.5 – Структурна схема мережі ІТС

У табл. 1.2 та табл. 1.3 наведено перелік основних та додаткових технічних засобів підприємства відповідно.

Таблиця 1.2 – Основні технічні засоби підприємства

№	Обладнання	Модель	Кіль-кість	Місце знаходження	Серійний номер
1	Ноутбук	Asus ZenBook 15 UX425EA-KI855	1	Кабінет директора	78V0AN001989
2	Ноутбук	Acer ConceptD 3 Ezel CC314-72G-59ME White (NX.C5HEU.004	1	Офіс, на столі креативного директора	MMZLEEU003 6660741N4201
3	Ноутбук	Acer Spin 5 SP513-55N 13.5QHD (NX.A5PEU.00H	3	Офіс, на столах дизайнерів	ПК3: EMELEE2438 396009IU0038 ПК4: UEKLID3627 396000LI0083 ПК5: MVIPV53530 6791KQI06660
4	Ноутбук	Asus VivoBook Pro 15 K3500PC-L1194W (90NB0UW2-M003E0	1	Кабінет бухгалтера	68E0SBA00086

Продовження таблиці 1.2

№	Обладнання	Модель	Кіль-кість	Місце знаходження	Серійний номер
5	Ноутбук	Asus ZenBook 14 UX425 UX425EA-KI853 Grey	1	Офіс, на столі SEO-спеціаліста	66AB7SA00096
6	Принтер	Canon MAXIFY GX6040 with Wi-Fi	1	Кабінет бухгалтера	MPIV05730
7	Wi-Fi роутер	Asus RT-N12+ Wireless-N300	1	Кабінет бухгалтера	K8IO1P009625
8	Комп'ютерна мишка	Logitech Pebble M350	7	Кабінет директора Кабінет бухгалтера Офіс	1547HS710YU3-1547HS710YU9
9	Камери відеоспостереження	Wi-Fi камера Camhi Cupol	4	Кабінет директора Кабінет бухгалтера Офіс	7759802776-7759802779

Таблиця 1.3 – Додаткові технічні засоби підприємства

№	Обладнання	Модель	Кіль-кість	Місце знаходження	Серійний номер
1	Кондиціонер	Ergo AC 0708 CH	3	Кабінет директора	E1300853820-E1300853822
				Кабінет бухгалтера	
				Офіс	
2	Пожежний сповіщувач	Артон СПД 3.4	4	Кабінет директора	AP13723S7524-AP13723S7527
				Кабінет бухгалтера	
				Офіс	
3	Магнітоконтактний сповіщувач	Covi Security MC-25	1	Офіс	875036669219
4	Датчик розбиття скла	Crow GBD-2	5	Кабінет директора	9A975422-9A975426
				Кабінет бухгалтера	
				Офіс	

На всіх ноутбуках встановлено ліцензійний Windows 10. Опис та характеристики встановленого ПЗ наведено в табл. 1.4.

Таблиця 1.4 – Опис встановленого ПЗ в ІТС

№	Найменування ПЗ	Версія	Ліцензія	Пристрої
1	Windows 10	10.0.19044.1620	Комерційна	Всі ПК
2	Microsoft Office 2019	14026.20246	Комерційна	Всі ПК
3	Google Chrome	101.0.4951.64	Відкрита	Всі ПК
4	Adobe Illustrator 2021	23.3.1	Комерційна	ПК2-ПК5
5	Adobe Photoshop 2021	23.3.1	Комерційна	ПК2-ПК5
6	Avast Premium Security	22.5.6015	Комерційна	Всі ПК
7	WinRaR	5.3.12	Відкрита	Всі ПК
8	Telegram Desktop	3.7.3	Відкрита	Всі ПК
9	Skype	8.62.0.83	Відкрита	Всі ПК
10	CamHi	6.1.2	Відкрита	ПК1

1.2.3 Обстеження інформаційного середовища

В даному розділі проводиться опис інформації, що циркулює в ІТС. На підприємстві циркулює відкрита та конфіденційна інформація з обмеженим доступом. Інформація зберігається в електронному вигляді або на паперовому носії у директора та бухгалтера. У табл. 1.5 наведено перелік інформації, що циркулює на об’єкті, де вказані режим доступу та правовий режим.

Таблиця 1.5 – Інформація, що циркулює на об’єкті

№	Інформація	Режим доступу	Правовий режим	Вид зберігання
1	Розпорядження директора	Відкрита	-	Електронний
2	Інформація про надання послуг,	Відкрита	-	Електронний

	графік роботи, контакти			

Продовження таблиці 1.5

№	Інформація	Режим доступу	Правовий режим	Вид зберігання
3	Договори компанії	З обмеженим доступом	Конфіденційна	Електронний, паперовий
4	Відомості про працівників	З обмеженим доступом	Конфіденційна	Електронний
5	Клієнтська база підприємства	З обмеженим доступом	Конфіденційна	Електронний
6	Технічне завдання дизайнера	З обмеженим доступом	Конфіденційна	Електронний
7	Технічне завдання SEO-спеціаліста	З обмеженим доступом	Конфіденційна	Електронний
8	Документ дизайнера, щодо виконання замовлення	З обмеженим доступом	Конфіденційна	Електронний
9	Документ SEO-спеціаліста, щодо виконання замовлення	З обмеженим доступом	Конфіденційна	Електронний
10	Звіти про виконану роботу	З обмеженим доступом	Конфіденційна	Електронний
11	Щомісячний фінансовий звіт	З обмеженим доступом	Конфіденційна	Електронний, паперовий
12	Щорічний фінансовий звіт	З обмеженим доступом	Конфіденційна	Електронний, паперовий
13	Звіт щодо нарахування зарплати	З обмеженим доступом	Конфіденційна	Електронний, паперовий
14	Відео з камер	З обмеженим	Конфіденційна	Електронний

	відеоспостереження	доступом		

У табл. 1.6 зазначена інформація про рівні конфіденційності, цілісності та доступності інформації.

Згідно з нормативним документом системи технічного захисту інформації «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99» можна визначити що таке конфіденційність, цілісність та доступність інформації. Конфіденційність та цілісність відносяться до властивостей інформації, а доступність – до властивостей ресурсу системи.

Конфіденційність інформації (К) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом. [1]

Цілісність інформації (Ц) — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. [1]

Доступність (Д) — властивість ресурсу системи, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний. [1]

Для класифікації цих рівнів використовуються рівні властивостей, що надані далі.

Рівні конфіденційності:

- **К1** – рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;
- **К2** – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

- **К3** – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- **К4** – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;
- **К5** – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності;

- **Ц1** – рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;
- **Ц2** – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;
- **Ц3** – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;
- **Ц4** – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;
- **Ц5** – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

- **Д1** – рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;
- **Д2** – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;
- **Д3** – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;
- **Д4** – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

- **Д5** – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Таблиця 1.6 – Рівні конфіденційності, цілісності та доступності інформації.

№	Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
1	Розпорядження директора	К1	Ц3	Д3
2	Інформація про надання послуг, графік роботи, контакти	К1	Ц4	Д3
3	Договори компанії	К2	Ц3	Д4
4	Відомості про працівників	К4	Ц3	Д3
5	Клієнтська база підприємства	К4	Ц3	Д3
6	Технічне завдання дизайнера	К3	Ц2	Д2
7	Технічне завдання SEO-спеціаліста	К3	Ц2	Д2
8	Документ дизайнера, щодо виконання замовлення	К3	Ц2	Д3
9	Документ SEO-спеціаліста, щодо виконання замовлення	К3	Ц2	Д3
10	Звіти про виконану роботу	К4	Ц3	Д4
11	Щомісячний фінансовий звіт	К4	Ц3	Д3
12	Щорічний фінансовий звіт	К4	Ц3	Д3
13	Звіт щодо нарахування зарплати	К1	Ц3	Д3

Продовження таблиці 1.6

№	Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
14	Відео з камер відеоспостереження	К4	Ц2	Д2

Технології обробки інформації:

Вся електронна інформація підприємства, створюється та зберігається в хмарному сховищі Google Cloud Використовуються такі сервіси, як Google Документ, Google Таблиця, Google BigQuery. Для передачі інформації та отриманих URL-адреси здійснюється за допомогою месенджера Telegram.

Розпорядження директора (1) завантажуються до Google Cloud, де з ними можуть ознайомитися інші працівники.

Відомості про працівників (4) зберігаються у хмарній базі даних (Google BigQuery). Туди заносяться особисті дані, ІПН, паспортні дані, особовий банківський рахунок, на який працівнику здійснюється нарахування заробітної плати. Звіт щодо нарахування зарплати щомісяця оновлюється. Бухгалтер надає доступ для читання цього документу директору, де звітує про заробітну плату персоналу, надсилаючи отриманий URL-адрес за допомогою в месенджера Telegram.

Кожного місяця бухгалтер формує щомісячний фінансовий звіт (11), використовуючи сервіс Google Таблиця. Отримані фінансові дані за 12 місяців звітності збираються у щорічному фінансовому звіті (12), який створюється наприкінці року. Бухгалтер так само надає доступ директору до читання цих документів.

Коли з’являється новий клієнт, першим чином директор проводить з ним бесіду та підписує договір (3). Після цього клієнт прямує до креативного директора з яким обговорює замовлення та записує особисті дані клієнта (ПІБ та номер телефону), вказує тип виконуваних робіт та усі примітки та тонкощі

замовлення. Всі ці дані креативний директор вносить до клієнтської бази (5) підприємства, яка знаходиться в хмарний базі даних.

Далі креативний директор в залежності від заказу створює технічне завдання для дизайнера (6) або технічне завдання для SEO-спеціаліста (7) в сервісі Google Документ. За готовності ТЗ, він надає доступ до читання дизайнеру або SEO-спеціалісту, відправляючи URL-адреси за допомогою месенджера Telegram.

Після отримання ТЗ, дизайнер або SEO-спеціаліст починає виконувати замовлення. Усю необхідну інформацію щодо замовлення вони заносять у створений документ (8/9). Під час виконання замовлення клієнт може вносити свої коригування та побажання, тому ці документи підлягають редагуванню.

Після виконання замовлення, креативний директор формує звіт про виконані робіти (10), де зазначає графік виконання та графічно ілюструє виконане замовлення. Клієнту надається доступ до цього звіту для ознайомлення. Отримана URL-адреса вноситься до клієнтської бази.

Доступ до відео з камер відеоспостереження має лише директор. Він і встановлює пароль для доступу. Воно транслюється на комп'ютер та телефон директора через програму CamHi. Відеоспостереження використовується на підприємстві для контролю поточної ситуації всередині приміщення, тобто контроль та перевірка роботи працівників (14).

Працівники мають право друкувати інформацію.

На рис. 1.6 зображено схему інформаційних потоків.

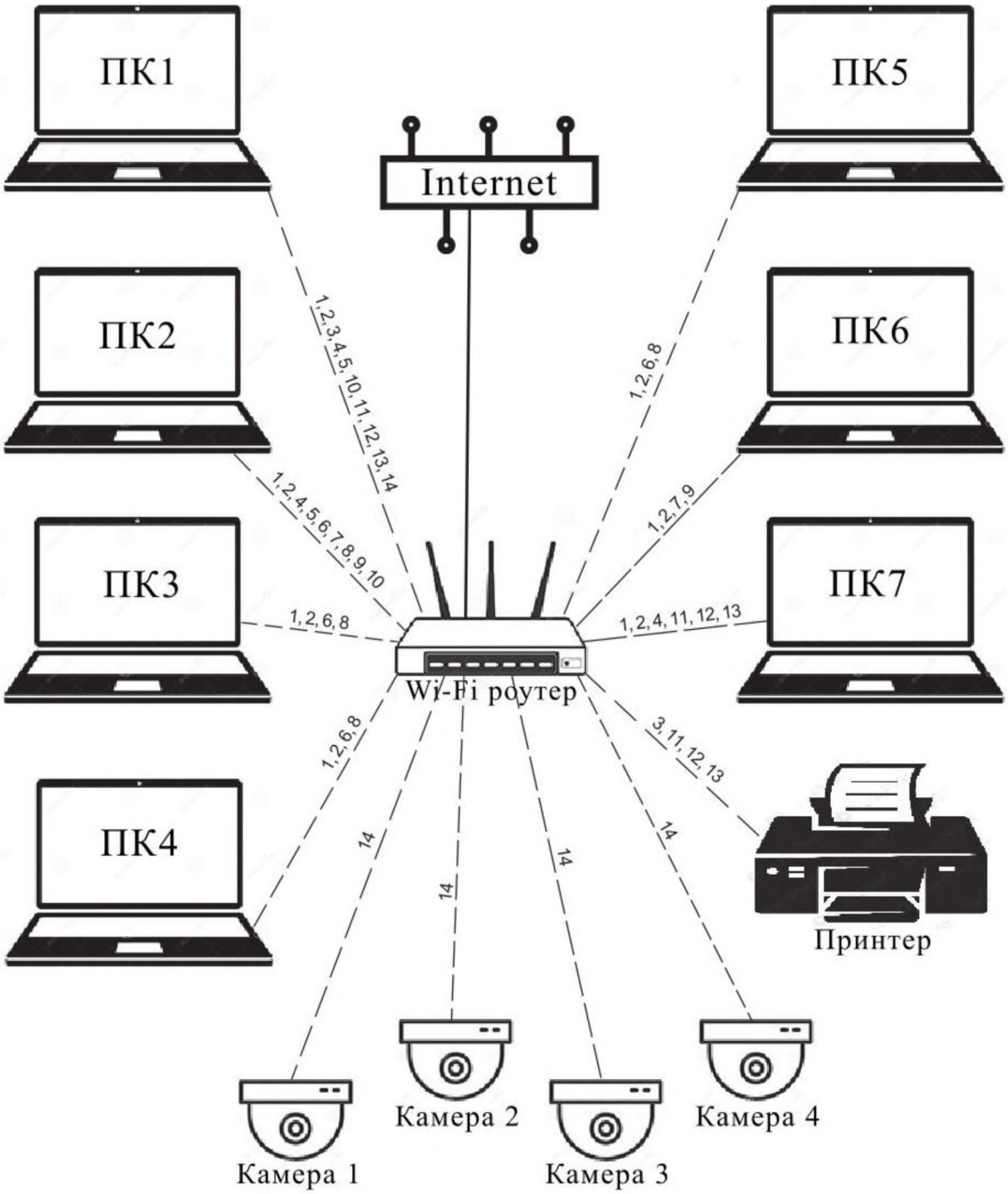


Рисунок 1.6 – Схема інформаційних потоків

1.2.4 Обстеження середовища користувачів

На ОІД працює та знаходитися впродовж робочого дня 7 осіб, які являються працівниками підприємства. А саме це: директор, креативний директор, три дизайнера, SEO-спеціаліст та бухгалтер. В кожного з працівників є свої обов'язки, які зазначені у табл. 1.7.

Таблиця 1.7 – Посадові обов’язки працівників

Посада	Кіль-кість	Обов’язки	Роль в ІТС	Кваліфікація
Директор	1	- організовує ефективну комунікацію на підприємстві; - затверджує та перевіряє відомості, що містять інформацію про заробітну плату працівників; - приймає рішення та підписує договори з замовником; - відстежує позиції компанії на ринку та встановлює цілі.	Користувач 1	Середня
Креативний директор	1	- надає консультації клієнтам; - створює ТЗ (технічне завдання); - відповідає в соцмережах; - формує звіт про виконання замовлення.	Користувач 2, системний адміністратор	Висока
Дизайнер	3	- оформлює замовлень згідно технічного завдання; - займається розробкою дизайну, логотипів.	Користувач 3, користувач 4, користувач 5	Середня

Продовження таблиці 1.7

Посада	Кіль-кість	Обов'язки	Роль в ІТС	Кваліфікація
SEO-спеціаліст	1	- оформлює замовлень згідно технічного завдання; - займається запуском та просуванням реклами.	Користувач 6	Практик
Бухгалтер	1	- веде бухгалтерію та фінансовий облік; - збирає та розраховує баланс підприємства; - розраховує та видає заробітну плату працівникам підприємства.	Користувач 7	Висока

1.3 Аналіз загроз інформації, що циркулює на ОІД

Загроза інформації – будь-яка обставина або подія, які можуть порушити політику безпеки інформації або завдати шкоди автоматизованій системі.

Оновою для проведення аналізу ризиків є опис:

- моделі порушника;
- моделі загроз.

1.3.1 Модель порушника

Модель порушника – абстрактний формалізований та неформалізований опис порушника. [1]

Порушники поділяються на дві категорій: внутрішні та зовнішні. До внутрішніх порушників відносяться авторизовані користувачі ІТС, які мають право доступу до ІзОД. Наприклад, працівники підприємства. Зовнішні порушники – це особи, які знаходяться за межами ІТС, але мають можливість підключення до каналів зв'язку та можуть здійснити злочині дії щодо політики безпеки ІТС. Наприклад, клієнти, відвідувачі, конкуренти тощо.

Згідно документу НД ТЗІ 1.4-001-2000 модель порушника повинна визначати:

- мету;
- рівень можливостей;
- рівень знань;
- за методами та способами;
- місце здійснення дії;
- час здійснення дії.

Більш конкретна інформація щодо класифікації порушника за цими визначеннями наведені у табл. 1.8-1.13.

Таблиця 1.8 – За мотивом

Рівень	Характеристика
1	Отримання необхідної інформації
2	Мати можливість вносити зміни в інформаційні потоки відповідно до своїх намірів, планів та інтересів
3	Нанесення пошкоджень та збитків шляхом знищення матеріальних та інформаційних цінностей

Таблиця 1.9 – За рівнем можливостей

Рівень	Характеристика
1	Запуск фіксованого набору завдань, що реалізують заздалегідь передбачені функції обробки інформації
2	Створення і запуск власних програм з новими функціями обробки інформації

Продовження таблиці 1.9

Рівень	Характеристика
3	Управління функціонуванням ІТС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурації. Її устаткування
4	Здійснює проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення ІТС, аж до включення до складу ІТС власних засобів з новими функціями обробки інформації

Таблиця 1.10 – За рівнем знань

Рівень	Характеристика
1	Володіє інформацією про функціональні особливості ІТС, основні закономірності формування в ній масивні даних та потоків запитів до них, вміє працювати з штатними засобами
2	Володіє середнім рівнем знань та практичними навичками робіт з технічними засобами ІТС та їх обслуговування
3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС
4	Володіє інформацією про структуру, функції та механізми дії засобів захисту

Таблиця 1.11 – За методами та способами

Рівень	Характеристика
1	Використовує виключно агентурні методи одержання інформації
2	Використовує пасивні технічні засоби перехоплення інформаційних потоків

Продовження таблиці 1.11

Рівень	Характеристика
3	Використовує виключно штатні засоби ІТС або недоліки проектування КСЗІ для реалізації несанкціонованого доступу
4	Використовує способи і засоби активного впливу на АС, що змінюють конфігурацію системи

Таблиця 1.12 – За місцем дії

Рівень	Характеристика
1	Без доступу до контрольованої зони організації та технічних засобів
2	Доступ до КЗ, але без доступу до технічних засобів
3	Доступ до робочих місць користувачів АС
4	Доступ до місць накопичення і зберігання даних
5	Доступ до зони управління засобами забезпечення безпеки

Таблиця 1.13 – За часом дії

Рівень	Характеристика
1	У процесі функціонування/У робочий час
2	У період не активності системи/У неробочий час/Під час планових перерв
3	Як у процесі функціонування, так і в період не активності системи

Після проведення аналізу можливих порушників було складено модель внутрішнього та зовнішнього порушника, які наведені у табл. 1.14 та табл. 1.15 відповідно.

Таблиця 1.14 – Модель внутрішнього порушника

Порушник	За метою	За рівнем можли-востей	За рівнем знань	За методами, засобами	За місцем дії	За часом дії	Сума
Директор	1	1	2	1	4	3	12
Креативний директор	1	4	4	4	5	3	21
Дизайнери	1	2	2	2	4	1	12
SEO-спеціаліст	1	2	2	2	4	1	12
Бухгалтер	1	1	2	1	4	3	12

Таблиця 1.15 – Модель зовнішнього порушника

Порушник	За метою	За рівнем можли-востей	За рівнем знань	За методами, засобами	За місцем дії	За часом дії	Сума
Відвідувачі	1	1	1	1	2	1	7
Конкуренти	3	1	2	2	1	1	10
Хакери, злочинці	1	4	4	4	4	1	18

Результат моделі порушника наведено на рис. 1.7.

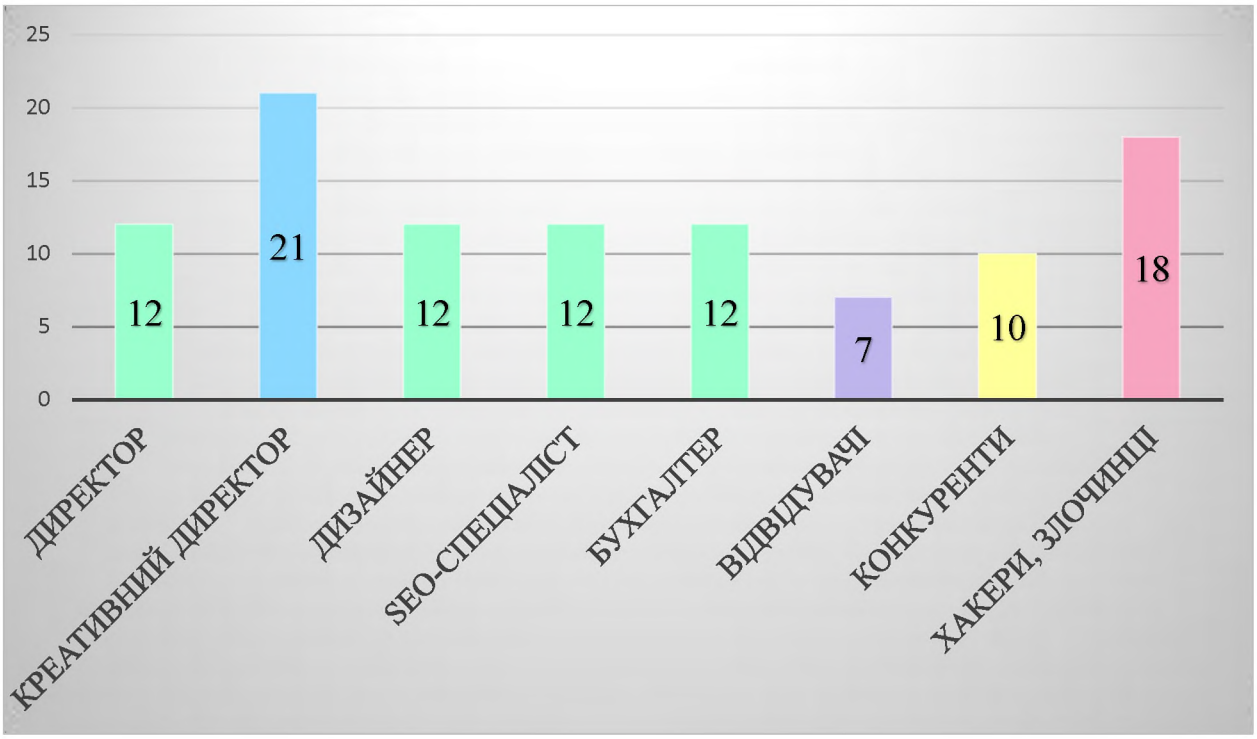


Рисунок 1.7 – Результат моделі порушника

За результатами моделі порушника можна визначити, що найбільшу загрозу для ІТС підприємства становлять працівники креативний директор та хакери/злочинці. Тож ІТС повинна бути більш контрольована, а доступ до конфіденційної інформації повинен бути розділеним.

1.3.2 Модель загроз

Модель загроз – це абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз. [1]

Загрози націлені на порушення конфіденційності, цілісності та доступності інформація. Вони наносять збитки підприємству та його персоналу, клієнтам та технічному обладнанню.

Загрози поділяються на випадкові, навмисні та природні. Також є розподілення на зовнішні та внутрішні.

До випадкових загроз відносяться ненавмисні дії, вчинені працівниками або користувачами через необережність, недбалість чи незнання, збої програмного забезпечення та поламки технічного обладнання.

До навмисних – відносять неправомірний доступ до інформації та поширення вірусних програм авторизованими працівниками, хакерами чи конкурентами.

До природних відносять загрози спричинені стихійними лихами.

У табл. 1.16 наведено перелік загрози, їх вразливості та джерел.

Таблиця 1.16 – Загрози та вразливості

№	Загроза	Вразливість	Джерело
1	Несанкціонований доступ до мережі Wi-Fi	- слабкі паролі Wi-Fi; - нерегулярна зміна паролів на Wi-Fi	Зовнішнє
2	Зараження комп'ютерними вірусами	- несвоєчасне оновлення антивірусного ПЗ; - відсутність контролю за запуском стороннього ПЗ користувачами системи; - відсутність правил, щодо користуванням мережі Інтернет; - відсутність правил, щодо використання месенджера	Внутрішнє
3	Несанкціоноване читання даних на екрані чи паперових документів	- неналежне зберігання документів; - відсутність правил, щодо того в якому виді залишати робоче місце; - слабкі паролі на камери відеоспостереження	Зовнішнє

Продовження таблиці 1.16

№	Загроза	Вразливість	Джерело
4	Несанкціонований доступ до інформації	- відсутність контролю за діями працівників	Внутрішнє
5	Несанкціонований доступ до камер відеоспостереження	- слабкі паролі доступу до камер	Зовнішнє
6	Несанкціонований доступ до технічних засобів	- передача персональних ключів стороннім особам; - розголошення коду	Внутрішнє
7	Збій та/або відмова інтернет мережі	- обриви; - відсутність додаткового провайдеру	Зовнішнє
8	Збій та/або відмова системи електроживлення	- скачки напруги, що можуть вивести з ладу технічні засоби	Зовнішнє

Для одержання ймовірності реалізації загроз використаємо формулу 1.1

$$К_{заг} = \frac{К_1 * К_2 * К_3}{125} \quad (1.1)$$

де, $К_1$ – доступності до об’єкта;

$К_2$ – можливість виконання;

$К_3$ – наслідки/фатальність;

125- максимальний добуток $К_1$, $К_2$, $К_3$.

Коефіцієнти оцінки загроз зазначено у табл. 1.17-1.19.

Таблиця 1.17 – $К_1$ – доступності до об’єкта

Рівень	Характеристика
1	Доступ відсутній
2	Віддалений доступ
3	Доступ до будівлі

Продовження таблиці 1.17

Рівень	Характеристика
4	Доступ до приміщення
5	Доступ до приміщення технічних та програмних засобів

Таблиця 1.18 – $К_2$ – можливість виконання

Рівень	Характеристика
1	Виконання загрози неможливо, або надзвичайно важко реалізувати
2	Для виконання необхідна велика кількість часу та ресурсів
3	Для виконання необхідні певні умови
4	Для виконання необхідні знання та вміння
5	Може виконати будь хто

Таблиця 1.19 – $К_3$ – фатальність наслідків

Рівень	Характеристика
1	Наслідків не буде
2	Наслідки, якими можна знехтувати
3	Наслідки будуть несуттєві
4	Наслідки можуть призвести до витрат
5	Наслідки призведуть до суттєвих витрат, підприємство може втратити репутацію

Результати аналізу загроз наведено у табл. 1.10 та на рис. 1.8.

Таблиця 1.20 – Результати аналізу загроз

№	Загроза	$К_1$	$К_2$	$К_3$	$К_{заг}$
1	Несанкціонований доступ до мережі Wi-Fi	3	4	4	0,38
2	Зараження комп'ютерними вірусами	5	4	4	0,64
3	Несанкціоноване читання даних на екрані чи паперових документів	5	4	3	0,48
4	Несанкціонований доступ до інформації	5	4	5	0,8
5	Несанкціонований доступ до камер відеоспостереження	3	4	4	0,38
6	Несанкціонований доступ до технічних засобів	5	3	4	0,48
7	Збій та/або відмова інтернет мережі	2	1	4	0,06
8	Збій та/або відмова системи електроживлення	2	1	4	0,06

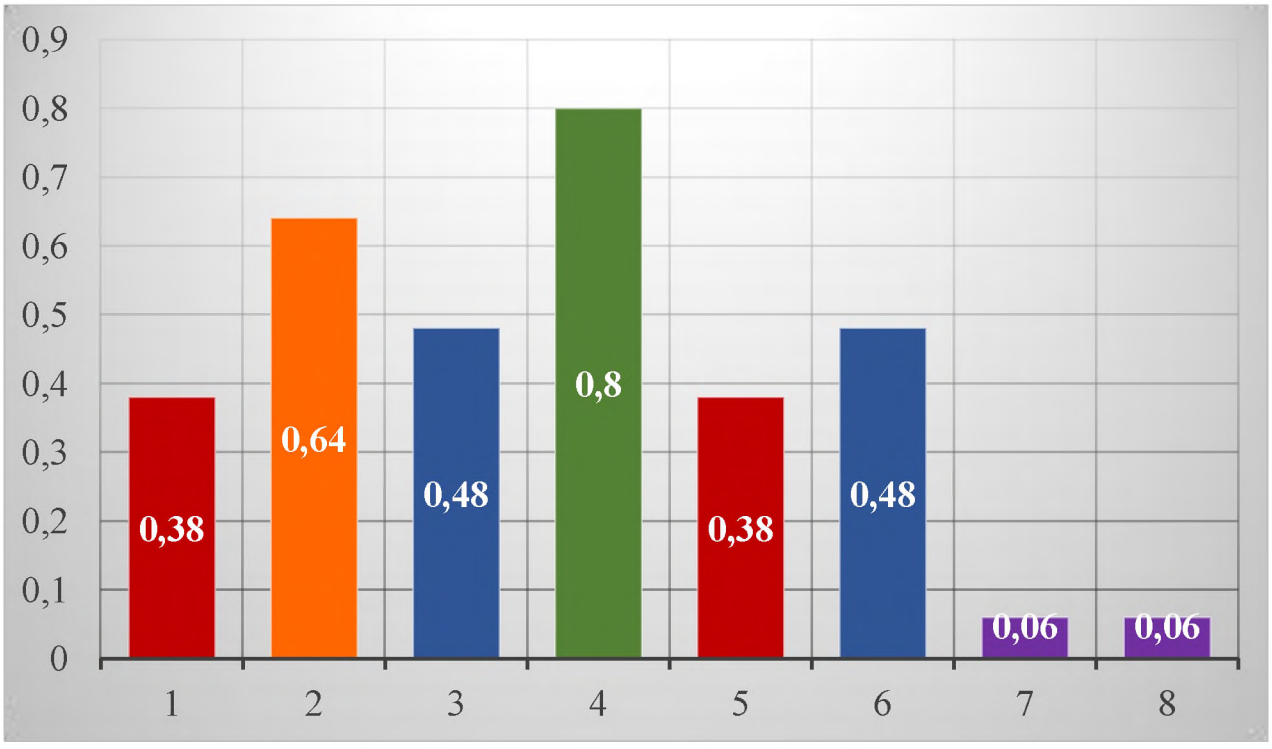


Рисунок 1.8 – Результат аналізу загроз

Нумерація згідно з табл. 1.20.

Проаналізувавши загрози, можна зробити висновки, що можна знехтувати загрозами $К_{заг}$ <= 0,20. До таких загроз відносяться:

- збій та/або відмова інтернету мережі;
- збій та/або відмова системи електропостачання.

1.4 Висновки та постановка задачі

У першому розділі кваліфікаційної роботи будо виконано обстеження ІТС (фізичне середовище, обчислювальна система, інформаційне середовище, середовище користувача), зроблено модель порушника та модель загрози, на основі чого було виведено які політики безпеки необхідно впровадити на підприємство. У спеціальній частину необхідно написати:

- політику розмежування доступу;
- політика антивірусного захисту;
- політика використання мережі Інтернет на підприємстві;
- політика передачі документів в електронному вигляді;
- політика «чистого» стола/екрану;
- політика створення та використання паролів;
- політика доступу сторонніх осіб до підприємства.

В кінці необхідно буде провести повторний аналіз загроз для виявлення результатів впровадження запропонованих політик безпеки.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Розробка політики безпеки інформації

Розробка політики безпеки займає важливе місце у життєдіяльності підприємства. Її відсутність чи недбале ставлення до неї може призвести до тяжких наслідків для підприємства, та навіть до припинення діяльності.

Основними етапами розробки політики безпеки інформації є:

- обстеження інформаційного середовища та інформаційної безпеки підприємства;
- формування плану робіт з розробки політики безпеки інформації;
- розробка політики безпеки інформації підприємства.

Основною метою політики безпеки є:

- мінімізація ризиків інформаційної безпеки;
- встановлення правил, які забезпечать захист інформації, що циркулює в ІТС;
- забезпечення необхідних умов для роботи з конфіденційною інформацією (конфіденційність, цілісність та доступність).

Для забезпечення необхідного рівня дій організації політика безпеки інформації повинна забезпечувати захист:

- автоматизованої системи підприємства;
- приміщення, де розташовані елементи АС;
- інформація, що обробляється та зберігається на АС.

Усі заходи, що представленні в політиці безпеки, направлені на зниження ризиків реалізації загрози ІТС, спираючись на існуючий аналіз ризиків (табл. 1.20).

2.2 Політика розмежування доступу

1) Огляд:

Політика розмежування доступу вставною правила доступу користувачів до інформації, що циркулює на підприємстві.

2) Мета:

Створення регламенту доступу користувачів до ресурсів обчислювальної системи.

3) Область дії:

Розповсюджується на всіх працівників підприємства.

4) Політика безпеки:

Зі згоди директора системний адміністратор (креативним директором) створюється та видається працівнику свої унікальні атрибути доступу. Скомпрометовані, розголошені чи застарілі атрибути повинні бути негайно видалені та змінені на нові.

Атрибути доступу до запису системного адміністратора зберігаються на листі, який схований у конверт в шафі в кабінеті директора, ключ від якої є лише в директора.

У матриці доступу розділяють об’єкти (інформації, що циркулює в ІТС) та суб’єкти (працівники «Сай.Фокс»). Матриця доступу зазначена у табл. 2.1.

Об’єкти доступу:

К1 – директор;

К2 – креативний директор;

К3 – SEO-спеціаліст;

К4 – дизайнер-1;

К5 – дизайнер-2;

К6 – дизайнер-3;

К7 – бухгалтер.

Суб’єкти доступу:

І1 – розпорядження директора;

І2 – інформації про надання послуг, графік роботи, контакти;

І3 – договори компанії;

І4 – Відомості про працівників;

І5 – клієнтська бага;

І6 – технічне завдання дизайнера;

І7 – технічне завдання SEO-спеціаліста;

І8 – документ дизайнера щодо виконання замовлення;

І9 – документ SEO-спеціаліста щодо виконання замовлення;

І10 – Звіти про виконану роботу

І11 – щомісячні фінансові звіти;

І12 – щорічні фінансові звіти;

І13 – звіти про нарахування зарплат;

І14 – відео з камер відеоспостереження.

Операції з файлами:

С – створення;

Ч –читання/перегляд;

Р – редагування;

В – видалення/знищення;

З – зберігання;

Д – друкування.

Таблиця 2.1 – Матриця доступу до інформації

Інформація	Користувач						
	К1	К2	К3	К4	К5	К6	К7
І1	С, Ч, Р, В, З	Ч	Ч	Ч	Ч	Ч	Ч
І2	Ч	С, Ч, Р, В, З	Ч	Ч	Ч	Ч	Ч

Продовження таблиці 2.1

Інформація	Користувач						
	К1	К2	К3	К4	К5	К6	К7
І3	С, Ч, Р, В, З, Д	-	-	-	-	-	-
І4	Ч	С, Ч, Р, В, З	-	-	-	-	Ч
І5	Ч	С, Ч, Р, В, З	-	-	-	-	-
І6	-	С, Ч, Р, В, З	Ч, З	Ч, З	Ч, З	-	-
І7	-	С, Ч, Р, В, З	-	-	-	Ч, З	-
І8	-	Ч	С, Ч, Р, В, З	С, Ч, Р, В, З	С, Ч, Р, В, З	-	-
І9	-	Ч	-	-	-	С, Ч, Р, В, З	-
І10	Ч	С, Ч, Р, В, З	-	-	-	-	-
І11	Ч	-	-	-	-	-	С, Ч, Р, В, З, Д
І12	Ч	-	-	-	-	-	С, Ч, Р, В, З, Д
І13	Ч	-	-	-	-	-	С, Ч, Р, В, З, Д
І14	Ч, В, З	-	-	-	-	-	-

5) Виконання політики безпеки інформації:

При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

6) Порядок та періодичність перегляду:

Політика безпеки переглядається кожен рік директором. У разу виникнення форс-мажорних ситуацій політика може бути переглянута раніше вказаного терміну.

7) Відповідальність:

Системний адміністратор несе відповідальність за невиконання політики безпеки, у разі недотримання рекомендацій щодо розмежування доступу та інша користувачі при порушенні правил.

2.3 Політика антивірусного захисту

1) Огляд:

Дана політика визначає вимоги щодо користуванням антивірусними програмними забезпеченнями для захисту інформаційно-телекомунікаційної системи підприємства ТОВ «Сай.Фокс» від загроз, спричинених розповсюдженням шкідливих ПЗ.

2) Мета політики:

Метою є зменшення ризику зараження ІТС підприємства шкідливими ПЗ.

3) Область дії:

Політика поширюється на всіх працівників, які користуються ноутбуками, та мають доступ до мережі Інтернет.

4) Політика безпеки:

На всіх ноутбуках підприємства мають бути встановлені та налагоджені антивірусні засоби, які повинні оновлюватися на початку робочого дня. Також необхідно проводити щоденне сканування на пошук вірусів. Будь-які дії, що можуть призвести до розповсюдження шкідливих програм у мережах підприємства заборонені.

Рекомендації для уникнення зараження вірусом:

- перед тим, як розпочати роботу необхідно переконатися у тому, що антивірусне ПЗ увімкнене;
- всі файли скачані із мережі Інтернет повинні діагностуватися антивірусом;
- забороняється відкривати та завантажувати інформацію з сайтів, які антивірус вважає підозрілими;
- ніколи не відкривайте вкладене до повідомлень, отриманим від недовірених відправників;
- при підключенні зовнішніх носіїв інформації, їх необхідно сканувати на наявність вірусів.

5) Виконання політики безпеки інформації:

При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

6) Порядок та періодичність перегляду:

Політика безпеки переглядається кожен рік директором. У разу виникнення форс-мажорних ситуацій політика може бути переглянута раніше вказаного терміну.

7) Відповідальність

На працівника, який порушить правила даної політики, може бути накладений штраф аж до звільнення. Ступінь покарання визначається в залежності від серйозності наслідків.

2.4 Політика використання Інтернету на підприємстві

1) Огляд:

Політика описує, правила щодо використання мережі Інтернет працівникам «Сай.Фокс».

2) Мета політики:

Збільшення рівня інформаційної безпеки підприємства за рахунок введення інструкцій та правил використання мережі Інтернет для працівників.

3) Область дії:

Політика стосується всіх працівників, що мають доступ до мережі Інтернет.

4) Політика безпеки:

Дозволяється користуватися мережею для:

- пошук інформації, яка необхідна для виконання замовлення;
- для комунікації з іншими працівниками;
- досліджень та вдосконалення своїх навичок;
- для комунікації з клієнтами.

Забороняється користуватися мережею для:

- використання комп'ютера для особистих цілей;
- передання конфіденційної інформації третім особам;
- скачування невідомих файлів.

5) Виконання політики безпеки інформації:

При прийнятті (зміні) політики безпеки кожен співробітник має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

6) Порядок та періодичність перегляду:

Політика безпеки переглядається раз на рік директором та креативним директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

7) Відповідальність

У разі першого порушення політики, порушник отримує попередження. У рази повторного порушення політики буде накладено штраф. При системному недотримані політики, порушника може чекати звільнення.

2.5 Політика передачі документів в електронному вигляді

1) Огляд:

Найпоширенішим методом передачі інформації на підприємстві «Сай.Фокс» є месенджер, неправильне використання якого може призвести до зараження системи вірусами та втрати інформації. Дана політика дає рекомендації щодо використання месенджера.

2) Мета політики:

Мета політики в тому, щоб мінімізувати загрози безпеки інформації під час користуванням месенджера працівниками для виконання своїх обов'язків.

3) Область дії:

Політика поширюється на всіх працівників, що використовують месенджер.

4) Політика безпеки:

Рекомендації, щодо використання месенджера:

- перед запуском та відкриттям файлів, вони повинні бути просканові антивірусом;
- функція автоматичного завантаження файлів повинна бути виключена;
- приймати та обробляти повідомлення можна лише від надійного відправника;
- у користувачів месенджера повинна бути увімкнення подвійна аутентифікація для додаткового захисту.

5) Виконання політики безпеки інформації:

При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової політики.

6) Порядок та періодичність перегляду:

Політика безпеки переглядається раз на рік директором. У разі виникнення форс-мажорів або необхідності, політика може бути переглянута раніше вказаного терміну.

7) Відповідальність

У разі недотримання та порушення політики, на працівника будуть накладені штрафні санкції, ступінь яких визначається в залежності з наслідками..

2.6 Політика «чистого» стола/екрана

1) Огляд:

Політика чистого стола чи екрану визначає, в якому вигляді працівник повинен залишати своє робоче місце, коли вів залишає його без нагляду та у кінці робочого дня.

2) Мета політики:

Захист інформації на електронних та паперових носіях від несанкціонованого доступу. Надання рекомендацій для працівників у якому вигляді вони повинні залишати свої робочі місця.

3) Область дії:

Ця політика відноситься до всіх працівників підприємства.

4) Політика безпеки:

Працівник має дотримуватися наступних правил:

- персональні комп'ютери та принтер повинні вимикатися після закінчення роботи з ними;
- надруковані документи з важливою або конфіденційною інформацією повинні негайно вилучатися з принтера;
- після закінчення робочого дня працівник підприємства повинен залишати своє робоче місце у чистоті та ховати всі документи, що зберігаються на робочому місці до шафи;

- забороняється доступ та користування ПК працівника сторонніми особами;
- в кінці робочого дня працівник підприємства має забирати з собою усі свої особисті технічні засоби;
- забороняється записувати та залишати на робочому місці паролі, коди та ключі;
- у разі покидання працівника свого робочого місця, він має заблокувати або вимкнути свій ПК.

5) Виконання політики безпеки інформації:

При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

6) Порядок та періодичність перегляду:

Політика безпека повинна переглядатися кожен рік директором або креативним директором. У разі виникнення форс-мажорів або необхідності, до політики можуть бути переглянуті раніше вказаного строку.

7) Відповідальність

У разі першого порушення політики, порушник отримує попередження. У рази повторного порушення політики буде накладено штраф. При системному недотримані політики, порушника може чекати звільнення.

2.7 Політика створення та використання паролів

1) Огляд:

Паролі є важливою складовою забезпечення інформаційної безпеки. Вони використовуються для захисту доступу до Wi-Fi, до камер відеоспостереження та облікових записів. Саме тому необхідно їх якісно підбирати.

2) Мета:

Метою є написання рекомендацій щодо створення надійних паролів, їх захист, збереження та частоту зміни.

3) Область дії:

Розповсюджується на всіх працівників компанії.

4) Політика безпеки:

Паролі для мережі Wi-Fi встановлює системний адміністратор.

Паролі для камер відеоспостереження встановлює директор.

Пароль виданий системним адміністратором працівнику для облікового запису, змінюється користувачем на новий при першому вході.

Паролі повинні генеруватися відповідно політиці паролів підприємства.

- паролі маються бути унікальними та не повторюватися;
- паролі маються бути довжиною не менше ніж 8 символів, але не довше ніж 16 символів;
- пароль повинен включати в себе наступні символи:
  - цифри (0-9);
  - латинські заголовні букви (A-Z);
  - латинські прописні букви (a-z);
  - знаки пунктуальності та інші символи (, ! % * # $ () _ + = {} [] ^ >< / | \ ~ “ ‘).
- пароль не повинен співпадати з ім’ям облікового запису;
- паролі не можна записувати на папері чи зберігати в незашифрованому вигляді;
- не може бути заснований на персональній інформації (прізвище, ім’я, дата народження, дані родичів тощо);
- використовувати службові паролі на інших сайтах в особистих цілях.

Забороняється:

- передавати паролі стороннім особам;
- передавати паролі за допомогою месенджерів, поштових повідомлень та інших способів через Інтернет.

Періодично необхідно змінювати пароль на новий, який має відповідати політиці паролів підприємства. Рекомендовано це робити кожні 3 місяці.

5) Виконання політики безпеки інформації:

При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

6) Порядок та періодичність перегляду:

Політика безпека повинна переглядатися кожен рік директором або креативним директором. У разі виникнення форс-мажорів або необхідності, до політики можуть бути переглянуті раніше вказаного строку.

7) Відповідальність:

За порушення політики полягає дисциплінарне покарання або сплата штрафу у розмірі наслідків.

2.8 Політика доступу сторонніх осіб до приміщення

1) Огляд:

Документ щодо доступу сторонніх осіб до території підприємства, тобто захисту від проникнення до приміщення сторонніх осіб в робочий час організації.

2) Мета політики:

Політика встановлює порядок організації пропускного режиму до підприємства, порядок контролю відвідування, а також встановлює відповідальність за порушення правил.

3) Область дії:

Область дії політики розповсюджується на працівників організації, які запрошують відвідувачів (здебільшого креативний директор). Також вона стосується безпосередньо і самих відвідувачів, які приходять.

4) Політика безпеки:

Доступ на територію підприємства контролюється за допомогою електронного замку з кодом, який знає кожен працівник і який заборонено розповідати стороннім особам. При розголошені PIN повинен бути змінений.

Крім цього в директора, креативного директора та бухгалтера є персональний ключ, який заборонено передавати стороннім особам.

Якщо працівник загубив свій ключ, то він повинен звернутися до директора, щоб йому видали новий ключ. Заборонено самостійно робити копію ключа.

При звільнені працівник повинен здати свій ключ, а PIN для кодового замка повинен бути змінений.

5) Виконання політики інформаційної безпеки:

При прийнятті (зміні) політики безпеки кожен працівник має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової політики. Після ознайомлення з даною політикою користувач має підписатися у спеціальному журналі з техніки безпеки.

6) Порядок та періодичність перегляду:

Політика безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика може бути переглянута раніше вказаного терміну.

7) Відповідальність:

У разі порушення безпеки політики підприємства, відповідальність за наслідки дій відвідувача несе співробітники, що порушили політику безпеки, Відповідальність за порушення вираховується в залежності від критичності наслідків: від сплати штрафу до звільнення.

2.9 Аналіз загроз після впровадження політики безпеки

Проведемо повторний аналіз загроз, але вже після впровадження в дію політики безпеки. Таким чином ми зможемо перевірити ефективність запропонованої політики.

Результати записані у табл. 2.2, та рис. 2.1.

Таблиця 2.2 – Результат повторного аналізу загроз

№	Загроза	$К_1$	$К_2$	$К_3$	$К_{заг}$
1	Несанкціонований доступ до мережі Wi-Fi	3	2	4	0,19
2	Зараження комп'ютерними вірусами	5	1	4	0,16
3	Несанкціоноване читання даних на екрані чи паперових документів	5	1	3	0,12
4	Несанкціонований доступ інформації	5	1	5	0,2
5	Несанкціонований доступ до камер відеоспостереження	3	2	4	0,19
6	Несанкціонований доступ до технічних засобів	5	1	4	0,16
7	Збій та/або відмова інтернет мережі	2	1	4	0,06
8	Збій та/або відмова системи електроживлення	2	1	4	0,06

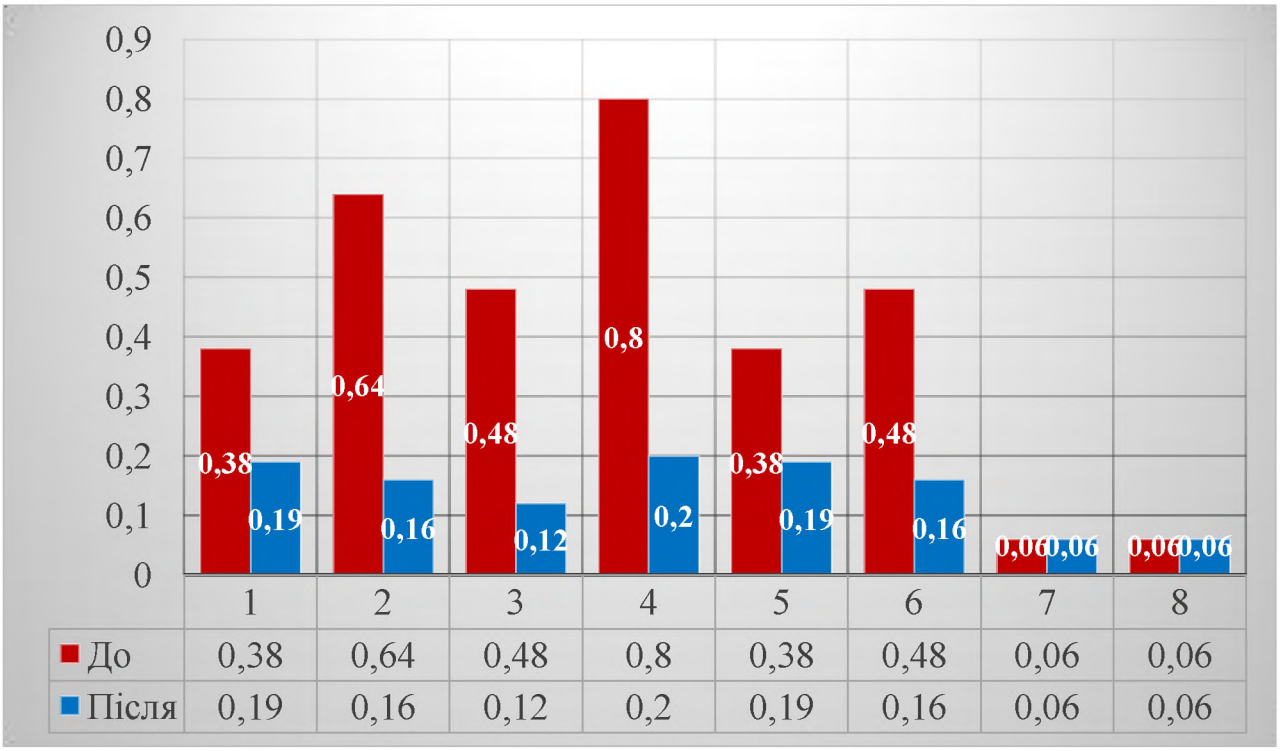


Рисунок 2.1 – Результат повторного аналізу загроз

Дані згідно з табл. 1.20 та табл. 2.2.

2.10 Висновки

У другому розділі було розроблено політику щодо розмежування доступу, антивірусного захисту, використання мережі Інтернет на підприємстві, передачі документів в електронному вигляді, «чистого стола/екрану», створення та використання паролів, доступу сторонніх осіб до підприємства. В кінці було проведено повторний аналіз загроз після впровадження запропонованих політик безпеки, який показує зниження рівня загроз до необхідного рівня.

3 ЕКОНОМІЧНА ЧАСТИНА

3.1 Мета техніко-економічного обґрунтування дипломного проекту

Метою виконання економічного розділу є техніко-економічне обґрунтування політики безпеки інформації на ТОВ «Сай.Фокс», тобто визначення витрат на їх впровадження.

Для визначення витрат на розробку політики безпеки інформації необхідно:

- визначити розмір капітальних витрат;
- визначити розмір експлуатаційних витрат;
- визначити обсяги відвернених втрат;
- розрахувати коефіцієнт повернення інвестицій та термін окупності.

На основі цих розрахунків можна буде визначити наскільки доцільним, прибутковим або збитковим є запропоновані політики.

3.2 Визначення витрат на розробку політики безпеки

3.2.1 Розрахунок капітальних (фіксованих) витрат

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

За методикою Gartner Group до капітальних варто віднести наступні витрати:

- вартість розробки проекту інформаційної безпеки, тобто розробки політики безпеки інформації;
- витрати на залучення зовнішніх консультантів;
- вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

- вартість створення основного й додаткового програмного забезпечення (ПЗ);
- витрати на первісні закупівлі апаратного забезпечення;
- витрати на інтеграцію системи інформаційної безпеки у вже існуючу корпоративну систему;
- витрати на навчання технічних фахівців і обслуговуючого персоналу. [11]

Капітальні (фіксовані) витрати розраховуються за формулою:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н} \quad (3.1)$$

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

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

$К_{рп}$ – вартість розробки політики безпеки інформації, грн.

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, грн.

$К_{навч}$ – вартість на навчання фахівців і персоналу, грн.

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

Для визначення витрат на розробку політики безпеки інформації необхідно:

- визначити трудомісткість розробки;
- розрахувати витрати на розробку.

Трудомісткість розробки політики безпеки визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документів.

Трудомісткість розраховується за формулою:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин} \quad (3.2)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_в$ – тривалість розробки концепції безпеки інформації у організації;

$t_а$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ – тривалість документального оформлення політики безпеки.

Значення показників наведено у табл. 3.1.

Таблиця 3.1 – Часові показники трудомісткості розробки політики безпеки.

Показник	Значення, год
$t_{тз}$	21
$t_в$	21
$t_а$	15
$t_{вз}$	11
$t_{озб}$	17
$t_{овр}$	13
$t_д$	17

Згідно формули:

$$t = 21 + 21 + 15 + 11 + 17 + 13 + 17 = 115 \text{ годин} \qquad (3.2)$$

Таким чином:

$$t = 115 \text{ год.}$$

Наступним кроком є розрахунок витрат на створення політики безпеки інформації ($К_{рп}$), яка складається з витрат на заробітну плату спеціаліста з інформаційної безпеки ($З_{зп}$) і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації ($З_{мч}$). Вони розраховуються за формулою:

$$К_{рп} = З_{зп} + З_{мч}, \text{ грн} \quad (3.3)$$

У свою чергу, витрати на заробітну плату спеціаліста ІБ розраховуються за формулою:

$$З_{зп} = t * З_{іб}, \text{ грн} \quad (3.4)$$

де, t – загальна тривалість розробки політики безпеки, годин;

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

Середня заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями складає 79 грн/годину, виходячи із заробітної плати 15000 грн/міс.

Тому виходить що:

$$З_{зп} = 115 * 132 = 9085, \text{ грн} \quad (3.4)$$

Вартість машинного часу для розробки ПБ на ПК визначається за формулою:

$$З_{мч} = t * С_{мч}, \text{ грн} \quad (3.5)$$

де, t – трудомісткість розробки політики безпеки інформації на ПК, годин.

$С_{мч}$ – вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р * t_{нал} * С_{е} + \frac{Ф_{зал} * Н_{а}}{F_{р}} + \frac{К_{ппз} * Н_{апз}}{F_{р}}, \text{ грн} \quad (3.6)$$

де, Р – встановлена потужність ПК, кВт:

$С_е$ – тариф на електричну енергію, грн/кВт*година;

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

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

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

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

$F_р$ – річний фонд робочого часу.

Значення для визначення вартості 1 години машинного часу ПК зазначено в табл. 3.2.

Таблиці 3.2 – Значення для формули $С_{мч}$

Показник	Значення
Р	0,6
$С_е$	1,68 кВт
$Ф_{зал}$	3600 грн
$Н_а$	0,5
$Н_{апз}$	2400
$К_{лпз}$	0,3
$F_р$	2160

Згідно формулі:

$$С_{мч} = 0,6 * 5 * 1,68 + \frac{3600*0,5}{2160} + \frac{2400*0,3}{2160} = 6,2, \text{ грн} \qquad (3.6)$$

Таким чином:

$$С_{мч} = 6,2, \text{ грн} \qquad (3.6)$$

$$З_{мч} = 115 * 6,2 = 713, \text{ грн} \qquad (3.5)$$

Отже, витрати на створення ПБ становить:

$$К_{рп} = 9085 + 713 = 9798, \text{ грн} \quad (3.3)$$

В результаті розрахунків, вартість розробки ПБ становить 9798 грн

Таким чином, наразі можна розрахувати капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки. Показники занесені до табл. 3.3.

Таблиця 3.3 – Показники

Показник	Значення, грн
$К_{зпз}$	6000
$К_{рп}$	9798
$К_{навч}$	1000

$$К = 6000 + 9798 + 1000 = 11398, \text{ грн} \quad (3.1)$$

Тож, вартість капітальних витрат дорівнює 11398 грн.

3.2.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені у грошовій формі.[11]

Формула річних потомних виплат:

$$С = С_в + С_к + С_{ак}, \text{ грн} \quad (3.7)$$

де, $С_в$ – витрати на модернізацію системи інформаційної безпеки;

$С_к$ – витрати на керування системою інформаційної безпеки;

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

Витрати на керування системою інформаційної безпеки розраховується за формулою:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{єл} + С_о + С_{тос}, \text{ грн} \quad (3.8)$$

$С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів;

$С_а$ – річний фонд амортизаційних відрахувань;

$С_з$ – річний фонд заробітної плати інженерно-технічного персоналу;

$С_е$ – вартість електроенергії;

$С_о$ – витрати на залучення сторонніх організацій;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс.

Річний фонд амортизаційних відрахувань складає 25% від капітальних витрат:

$$С_а = 11398 * 0,25 = 2849,5, \text{ грн}$$

Річний фонд заробітної плати інженерно-технічного персоналу розраховується по формулі:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.9)$$

де $З_{осн}$ та $З_{дод}$ – є основною та додатковою заробітною платою відповідно, грн/рік.

Основна заробітна плата визначається, виходячи з місячного посадового осаду, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата спеціалісті з інформаційної безпеки на місяць складає 15000 грн/міс та 180000 грн/рік. Додаткова заробітна плата – 1500 грн/міс та 18000 грн/рік. Виконання робіт щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,1 ставки. Отже:

$$С_з = (180000 + 18000) * 0,1 = 19800, грн \quad (3.9)$$

Ставка ЄСВ для всіх категорій платників з 01.012022 складає 22%.

$$С_{єв} = 19800 * 0,22 = 4356, грн$$

Вартість електроенергії розраховується за формулою:

$$С_{ел} = P * F_p * Ц_е, грн \quad (3.10)$$

де, Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки;

$Ц_е$ – тариф на електроенергію, грн/кВт*годин.

$$С_{ел} = 0,6 * 7 * 2160 * 1,64 = 14878,08, грн \quad (3.10)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2%.

$$С_{тос} = 11398 * 0,02 = 227,96, грн$$

Можна розрахувати витрати на керування системи інформаційної безпеки:

$$С_к = 2849,5 + 19800 + 4356 + 14878,08 + 227,96 = 42211,54, грн$$

Маючи всі необхідні дані можемо розрахувати річні експлуатаційні витрати:

$$С = 42211,54 + 2279,6 = 44491,14, грн \quad (3.7)$$

Таким чином;

$$С = 44491,14, грн$$

3.3 Оцінка збитків у разі виникнення загроз

3.3.1 Оцінка величини збитку

Ця оцінка проводиться для визначення обсягів матеріальних збитків, виходячи з ймовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Заробітна плата працівників підприємства зазначена в табл. 3.4.

Таблиця 3.4 – Заробітна плата працівників підприємства.

Посада	Розмір заробітної плати в місяць, грн
Директор	20000
Креативний директор	17000
SEO-спеціаліст	15000
Дизайнер 1	15000
Дизайнер 2	15000
Дизайнер 3	15000
Бухгалтер	12000

Загальна сума заробітних плат працівників підприємства становить 76000 грн.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 5 годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 година;

$t_{ви}$ – час повторного введення загубленої інформації працівниками атакованого вузла або сегмента корпоративної мережі, 1 годину;

$З_о$ – заробітна плата обслуговуючого персоналу, 17000 грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 76000 грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу, 1 особа;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі,7 осіб;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, 700000 грн у рік;

$П_{зч}$ – вартість зміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів корпоративної мережі, 1;

N – середнє число атак на рік7.

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

$$U = П_п + П_в + V \quad (3.11)$$

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;

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

Витрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі розраховується за формулою:

$$П_п = \frac{\sum Зс}{F} * t_п \quad (3.12)$$

де, F – місячний фонд робочого часу (при 45-и годинному робочому тижні становить 198 годин)

$$П_п = \frac{76000*7}{198} * 5 = 13434{,}34 \quad (3.12)$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають такі складові;

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.13)$$

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 розраховуються за формулою:

$$П_{ви} = \frac{\sum Зс}{F} * t_{ви} \quad (3.14)$$

$$П_{ви} = \frac{76000*7}{198} * 1 = 2686,87 \quad (3.14)$$

Витрати для відновлення вузла або сегмента корпоративної мережі розраховується за формуло:

$$П_{пв} = \frac{\sum Зо}{F} * t_в \quad (3.15)$$

$$П_{пв} = \frac{17000*1}{198} * 2 = 171,17 \quad (3.15)$$

Отже упущена вигода дорівнює;

$$П_в = 2686,87 + 171,71 = 2858,58 \quad (3.13)$$

Витрати на зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента розраховується за формулою:

$$V = \frac{О}{F_г} * (t_п + t_в + t_{ви}) \quad (3.16)$$

де, $F_г$ – річних фонд часу роботи організації, 1800 годин.

$$V = \frac{700000}{1800} * (5 + 2 + 1) = 3111,1 \quad (3.16)$$

Упущена вигода від простою дорівнює:

$$U = 13434{,}34 + 2858{,}58 + 3111{,}1 = 19404{,}02, \text{ грн} \quad (3.11)$$

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

$$B = \sum i \sum n\, U \quad (3.17)$$

$$B = 1 * 7 * 19404{,}02 = 135828{,}14, \text{ грн} \quad (3.17)$$

Отже загальний збиток від атаки на вузол або сегмент корпоративної мережі організації дорівнює 135828,14

3.3.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B * R - C \quad (3.18)$$

де, В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

$$E = 135828{,}14 * 0{,}46 - 44491{,}14 = 17989{,}80 \text{ грн} \quad (3.18)$$

Таким чином, загальний ефект віл впровадження системи інформаційної безпеки становить:

$$E = 17989{,}8 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності системи захисту інформації, здійснюється на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО) – використовується, коли 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;
- термін окупності капітальних інвестицій (T_o) – показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки.[11]

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих витрат від атаки на сегмент або вузол корпоративної мережі, а отже

$$ROSI = \frac{E}{K} \tag{3.19}$$

де, Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Таким чином,

$$ROSI = \frac{17989,8}{11398} = 1,58, \text{ частки одиниці} \tag{3.19}$$

Термін окупності капітальних інвестицій (T_o) розраховується за формулою:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} \tag{3.20}$$

$$T_o = \frac{1}{1,58} = 0,6, \text{ років} \tag{3.20}$$

Таким чином, капітальні інвестиції окупляться за 6 місяців.

3.5 Висновки

В цьому розділі було визначено доцільність впровадження основних елементів політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс». Для було проведено наступні розрахунки:

1. Капітальні витрати на впровадження на експлуатацію політики безпеки інформації становить 11398 грн.
2. Повна вартість річних експлуатаційних витрат становить 44491,14 грн.
3. Загальний збиток від атаки становить 135828,14 грн.
4. Загальний ефект від впровадження системи інформаційної безпеки становить 17989,8 грн.
5. Термін окупності капітальних інвестицій становить 6 місяців.

Отже запропонований підхід щодо політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс» може вважатися економічно доцільним.

ВИСНОВКИ

Об’єкт розробки кваліфікаційної роботи є інформаційно-телекомунікаційна системи ТОВ «Сай.Фокс».

В першому розділі кваліфікаційної роботи було проведено обстеження ІТС, а саме обстежено фізичне середовище, обчислювальну систему, інформаційне середовище та середовище користувача. Також було проведено аналіз загроз, побудовано модель порушника та модель загроз, та визначено які елементи політики необхідно ввести.

У другому розділі було розроблено елементи політики безпеки інформації, а саме: розмежування доступу, антивірусного захисту, використання мережі Інтернет на підприємстві, передачі документів в електронному вигляді, «чистого» стола/екрану, створення та використання паролів, доступу сторонніх осіб до підприємства. В кінці проведено повторний аналіз загроз, після впровадження запропонованих елементів політики безпеки, який показує зниження рівня ризиків.

В третьому розділі кваліфікаційної роботи було визначено доцільність впровадження основних елементів політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс». Для цього було розраховано капітальні витрати на впровадження та експлуатацію політики безпеки інформації, загальний збиток у разі виникнення загроз, загальний ефект від впровадження системи інформаційної безпеки та термін окупності. Тим самим, можна вважати що запропонований підхід щодо політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс» є економічно доцільним.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», 1999 URL:https://tzi.ua/assets/files/1.1_003_99.pdf

2. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», 2012 URL:https://tzi.com.ua/downloads/1.4-001-2000.pdf

3. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, 1999 URL:https://tzi.com.ua/downloads/1.1-002-99.pdf

4. Закон України «Про інформацію» URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» URL:https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

6. Види інформаційних загроз та методи боротьби з ними, 2012 URL:https://www.dokwork.ru/2012/01/blog-post.html

7. Загрози інформаційної безпеки URL:http://www.security.ase.md/publ/ru/pubru91/

8. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» 2012 URL:https://tzi.com.ua/downloads/2.5-005%20-99.pdf

9. Комплексні системи захисту інформації: проектування, впровадження, супровід, Вадим Гребенніков,2013 URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/10070

10. Розробка політики інформаційної безпеки URL: http://www.rusnauka.com/20_AND_2014/Informatica/4_174328.doc.htm

11. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.

12. 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. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Розділ 1. Стан питання. Постановка задачі	35	
6	А4	Розділ 2. Спеціальна частина	15	
7	А4	Розділ 3. Економічна частина	14	
8	А4	Висновок	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника кваліфікаційної роботи	2	
13	А4	Додаток Г. Відгук керівника економічного розділу	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Марченко_ПВ_125-18-3_ПЗ.docx
2. Марченко_ПВ_125-18-3_ПЗ.pdf
3. Марченко_ПВ_125-18-3_ПЗ.pdf.p7s
4. Марченко_ПВ_125-18-3.pptx

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-18-3

Марченко Поліни Валентинівни

на тему: «Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сай.Фокс»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 82 сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІТС ТОВ «Сай.Фокс».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІТС, виявлення актуальних загроз, розробка елементів політики безпеки.

Запропоновано матрицю розмежування доступу, розроблені положення політики безпеки щодо: розмежування доступу, антивірусного захисту, використання мережі Інтернет, передачі документів в електронному вигляді, «чистого» стола/екрану, створення та використання паролів, доступу сторонніх осіб до підприємства.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих політик до особливостей ТОВ «Сай.Фокс».

До недоліків відноситься недостатньо обґрунтовані методика аналізу загроз та модель порушника.

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

За час дипломування Марченко П.В. проявила 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 «добре».

Керівник кваліфікаційної роботи, професор **Корнієнко В.І.**

Керівник спец. розділу, ст. викладач **Кручінін О.В.**

ДОДАТОК Г. Відгук керівника економічної частини

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 94 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)