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 *Петраша Євгенія Ігоровича*

академічної групи *125-19ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

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

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доцент Сафаров О. О.	94	відмінно	
розділів:				
спеціальний	ст. викл. Войцех С. І.	92	відмінно	
економічний	доцент Пілова Д. П.	85	добре	

Рецензент		94	відмінно	

Нормоконтролер	ст. викл. Тимофєєв Д. С.			

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 ***Петрашу Євгенію Ігоровичу*** **академічної групи** ***125-19ск-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

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

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

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Стан питання. Аналіз нормативно-правової бази. Постановка задачі	20.05.2022
Розділ 2	Обстеження об'єкту інформаційної діяльності, аналіз інформаційних потоків на підприємстві, розробка та технічна реалізація політики безпеки	12.06.2022
Розділ 3	Визначення економічно-технічної доцільності політики безпеки, розрахунки витрат впровадження політики безпеки	14.06.2022

Завдання видано _____ **Сафаров О.О.**
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 15.04.2022

Дата подання до екзаменаційної комісії: 15.06.2022

Прийнято до виконання _____ **Петраш Є.І.**
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 72 с., 6 рис., 20 табл., 4 додатки, 12 джерел.

Об`єкт дослідження: інформаційно-телекомунікаційна система ТОВ «FixUp».

Мета роботи: підвищення рівня захисту інформації в інформаційно-телекомунікаційній системі товариства з обмеженою відповідальністю «FixUp».

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі наведено такі теоретичні відомості, як стан питання, аналіз нормативно-правової бази захисту інформації виконана постановка задачі кваліфікаційної роботи. В завершенні розділу було сформульовано висновки щодо результатів аналізу нормативно-правової бази та задач, які потрібно вирішити при виконанні кваліфікаційної роботи.

У спеціальній частині наведено загальні відомості щодо об'єкту інформаційної діяльності, обстежено об'єкт інформаційної діяльності, фізичне середовище, обчислювальну систему та інформаційне середовище. Було проаналізовано актуальні для підприємства загрози інформаційної безпеки, побудована модель порушника, модель загроз та визначено методи, засоби захисту інформації на об'єкті інформаційної діяльності та було проведено висновки щодо виконаної роботи.

В економічному розділі визначено економічну доцільність розробки та впровадження рекомендацій для проведення ідентифікації інформаційних активів. Проведено розрахунок капітальних (фіксованих) витрат, поточних (експлуатаційних) витрат, загального збитку від атаки на ІТС та загального ефекту від впровадження рекомендацій.

Практичне значення роботи полягає у дослідженні та підвищенні рівня захищеності інформації в інформаційно-телекомунікаційній системі товариства з обмеженою відповідальністю «FixUp».

ІНФОРМАЦІЙНА БЕЗПЕКА, ІДЕНТИФІКАЦІЯ, ІНФОРМАЦІЙНИЙ АКТИВ, КІБЕРБЕЗПЕКА, РЕЄСТР ІНФОРМАЦІЙНИХ АКТИВІВ.

ABSTRACT

Explanatory note: 72 pages, 6 figures, 20 tables, 4 appendices, 12 sources.

Object of research: information and telecommunication system of LLC "FixUp".

Purpose: to increase the level of information protection in the information and telecommunication system of the limited liability company "FixUp".

Development methods: observation, comparison, analysis, description.

The first section provides such theoretical information as the state of the issue, analysis of the regulatory framework for information protection, the task of qualification work. At the end of the section, conclusions were formulated on the results of the analysis of the regulatory framework and the tasks to be solved during the qualification work.

The special section provides general information about the object of information activities, examines the object of information activities, the physical environment, computer system and information environment. The information security threats relevant to the enterprise were analyzed, the model of the violator, the threat model were built and the methods, means of information protection at the object of information activity were determined and conclusions were drawn about the work done.

The economic section identifies the economic feasibility of developing and implementing recommendations for the identification of information assets. The calculation of capital (fixed) costs, current (operational) costs, total damage from the attack on ITS and the overall effect of the implementation of recommendations.

The practical significance of the work is to study and increase the level of information security in the information and telecommunications system of the limited liability company "FixUp".

INFORMATION SECURITY, IDENTIFICATION, INFORMATION ASSET, CYBER SECURITY, REGISTER OF INFORMATION ASSETS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ІЗоД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КЗ – контрольована зона;

КС – комп'ютерна система;

НД ТЗІ – нормативний документ в галузі технічного захисту інформації;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ТОВ – товариство з обмеженою відповідальністю;

ЗМІСТ

ВСТУП

Компанії стають все більш залежними від інформаційних систем, що робить їх уразливими для витоку даних внаслідок кібератак і комп'ютерних вірусів, а також втрати даних через внутрішні ризики: людського фактору або збоїв у роботі носіїв інформації. В середньому, витік даних з успішністю в 93% займає менше одної хвили.

Наслідки втрати даних можуть бути катастрофічними для бізнесу. Якщо великі організації зазнають величезних збитків, малі підприємства можуть поплатитися своїм існуванням: приблизно 60% з них закриються протягом півроку після втрати даних.

Не варто забувати і про величезний удар по репутації компанії, який істотно позначиться на лояльності клієнтів. Інформаційна безпека і захист інформації мають бути спрямовані на запобігання ризикам, а не на ліквідацію їх наслідків.

Досі головною причиною втрати даних є збій у роботі жорсткого диска. Щотижня тільки в США виходить з ладу приблизно 140 тис. жорстких дисків. Водночас 41% малих підприємств не мають відповідних фахівців у штаті, а 58% компаній не підготовлені до втрати даних і не мають чіткої стратегії. Не варто забувати і про людський фактор: за даними Лабораторії Касперського, неуважність співробітників і кіберзлочинність є небезпечними для бізнесу. У свою чергу, головною зовнішньою загрозою для діяльності компанії є кіберзлочинність.

Незважаючи на значний супротив, її активність продовжує наростати. Механізм поширення кіберзагроз змінився, еволюціонував від використання простих фішингових атак, спаму і завантажувальних дисків до більш складних і комплексних технологій - DDoS-атак і вірусів-здирників. Це означає, що фахівці з інформаційної безпеки повинні не тільки відповідати на виклики індустрії, яка постійно змінюється, але й попереджати і відбивати всі загрози, нав'язані кібер-злочинцями.

Актуальність роботи обумовлена необхідністю підвищення рівня інформаційної захищеності інформаційно-телекомунікаційній системи ТОВ «FixUp» за для запобігання витоку даних та захисту від кібератак.

Об`єктом дослідження є інформаційно-телекомунікаційна система ТОВ «FixUp».

Мета кваліфікаційної роботи підвищення рівню захисту інформації в інформаційно-телекомунікаційній системі ТОВ «FixUp».

Для досягнення поставленої мети треба взяти до уваги наступні завдання:

- Провести обстеження об’єкту захисту інформації;
- Провести обстеження обчислювальної системи;
- Провести обстеження інформаційного середовища;
- Провести аналіз можливих загроз інформації;
- Розробити модель порушника;
- Розробити модель загроз інформаційної безпеки;
- Розробити рекомендації щодо підвищення рівня інформаційної безпеки інформаційно-телекомунікаційній системі ТОВ «FixUp»

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Шлях України у розбудові власної кібербезпеки потребує докорінних і невідкладних змін. Це не лише позиція лідерів вітчизняного кіберзахисту. Необхідність змін підтверджена атаками на об'єкти критичної інфраструктури, багатьма іншими інцидентами, які створили Україні сумнівну репутацію одного з головних кіберполігонів.

Законодавча база – важлива складова у забезпеченні інформаційної безпеки та кібербезпеки держави, однак, ураховуючи основні недоліки чинного законодавства у безпековій сфері, його пасивний характер, декларування теоретичних аспектів забезпечення ІБ, безпеки кіберпростору та протидії кіберзлочинності на рівні доктрин, указів, рішень тощо, потрібно розробити механізм практичного провадження захисту інформації в кіберпросторі. Тобто задається «напрям», якого необхідно дотримуватися за відсутності правового, фінансового та кадрового забезпечення і без жодної відповідальності посадових осіб.

Безпека інформаційного і кіберпростору, запровадження диджиталізації процесів управління, гарантування безпеки й сталого функціонування національної критичної інфраструктури, інформаційних систем (ІС) повинні стати не тільки складовими державної політики у сфері розвитку кіберпростору та становлення інформаційного суспільства в Україні, а також включення цих чинників у сферу політичних пріоритетів держави.

Протягом останніх років все ширше використання перспективних ІТ-технологій зумовило не лише численні переваги, а й цілу низку проблем. Зокрема, істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційній безпеці, таких як нові форми кібератак. Гарантування стабільного максимально ефективного функціонування та

розвитку будь-якого підприємства є основним завданням забезпечення безпеки його економічної інформації.

Найціннішою економічною інформацією є облікова інформація, яка характеризує всі аспекти підприємницької діяльності. Сьогодні більшість суб'єктів підприємницької діяльності використовують комп'ютеризовану форму ведення бухгалтерського обліку, яка передбачає використання спеціалізованого програмного забезпечення та технічних засобів. При цьому в комп'ютерних системах зберігаються і обробляються великі обсяги облікової інформації, тому будь-який збій може привести до надмірних витрат, зниженню доходів, втрати активів тощо. Тому головним пріоритетом захисту облікової інформації на підприємстві є розроблення заходів, спрямованих на збереження інформації, що міститься у комп'ютерних базах підприємства.

У зв'язку з тим, що останнім часом збільшується кількість незаконних фінансових операцій, крадіжок та шахрайства в мережі Інтернет, несанкціонованого використання чи модифікації програмного забезпечення, під час оцінки надійності систем інформаційної безпеки мають бути змінені пріоритети від забезпечення традиційної інформаційної безпеки до кібербезпеки. Питання кібербезпеки зачіпає інтереси не лише державних інституцій, а і приватного сектору та громадянського суспільства. При цьому низький рівень взаємодії органів державної влади, неурядових організацій та приватного сектору, а також відсутність системних нормативних документів, які описують загрози Україні в кіберпросторі, є наслідком відсутності цілісного обговорення питань кібербезпеки.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Основу нормативно-правового забезпечення інформаційної безпеки складають формування та підтримка його нормативно-правової бази як юридичного засобу досягнення реальної упорядкованості системи інформаційної безпеки.

Нормативна база являє собою організаційно-функціональний образ системи інформаційної безпеки, виражений юридичною мовою і який відповідає її цільовому призначенню.

При цьому правові норми забезпечують моделювання як самої системи національної безпеки, так і її підсистем, нормування та формалізацію їх функціональних, організаційних та інформаційних структур, а також самі виконують інформаційну функцію.

Нормативно-правове забезпечення інформаційної безпеки визначається як процес створення і підтримки в необхідних межах конструктивних організаційно-функціональних характеристик системи інформаційної безпеки за допомогою впорядковуючого впливу нормативно-правових засобів.

Система нормативно-правового забезпечення інформаційної безпеки являє собою сукупність законів і підзаконних нормативних актів, які створюють нормативно правове поле для функціонування системи національної безпеки і виконання нею свого призначення.

При розробці рекомендацій щодо підвищення рівня інформаційної безпеки потрібно покладатися на наступні нормативні документи:

- Закон Україні «Про інформацію»
- Закон Україні «Про захист інформації»
- Закон Україні «Про захист інформації в інформаційно-телекомунікаційних системах»
- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»
- НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»
- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»
- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

- НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»
- НД ТЗІ 3.6-001-2000 «Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.»
- ДСТУ 3396.1-96 «Захист інформації. Технічний захист. інформації. Порядок проведення робіт»

1.3 Постановка задачі

Так як на підприємстві ТОВ «FixUp» обробляється інформація з обмеженим доступом, було прийнято рішення щодо підвищення рівня захищеності інформації в його інформаційно телекомунікаційній системі.

Для досягнення поставленої мети необхідно виконати наступні завдання:

- Провести обстеження об’єкту захисту інформації;
- Провести обстеження обчислювальної системи;
- Провести обстеження інформаційного середовища;
- Провести аналіз можливих загроз інформації;
- Розробити модель порушника;
- Розробити модель загроз інформаційної безпеки;
- Розробити рекомендації щодо підвищення рівня інформаційної безпеки інформаційно-телекомунікаційній системі ТОВ «FixUp»

1.4 Висновки

У даному розділі розглянуто стан питання щодо безпеки інформаційного та кіберпростору, здійснено опис стану загроз інформаційної безпеки, наведено та проаналізовано нормативно-правову базу у сфері захисту інформації та поставлено задачі для досягнення поставленої мети

щодо підвищення рівня інформаційної безпеки інформаційно-телекомунікаційної системи ТОВ «FixUp»

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про ОІД

ТОВ «FixUp» – сервісний центр, основний напрям якого є ремонт та технічне обслуговування комп'ютерної і мобільної техніки, додатковим напрямом ТОВ «FixUp» є Інтернет-магазин з продажу запчастин для ремонту комп'ютерної та мобільної техніки; аксесуарів для мобільних пристроїв (планшетів, телефонів тощо).

ТОВ «FixUp» засновано у 2016 році.

2.2 Обстеження ОІД

2.2.1 Обстеження фізичного середовища

Офіс компанії знаходиться за адресою проспект Дмитра Яворницького, 111, Дніпро, Дніпропетровська область, 49000.

Графік роботи офісу з 10:00 до 18:00, з понеділка по суботу, неділя вихідний.

ОІД знаходиться на другому поверсі офісної будівлі, яка має 2 поверхи.

До ОІД примикають сусідні офісні приміщення, які знаходяться на першому поверсі та за західною і південною внутрішньою стіною приміщення ОІД, інші стіни – зовнішні та ні до чого не примикають.

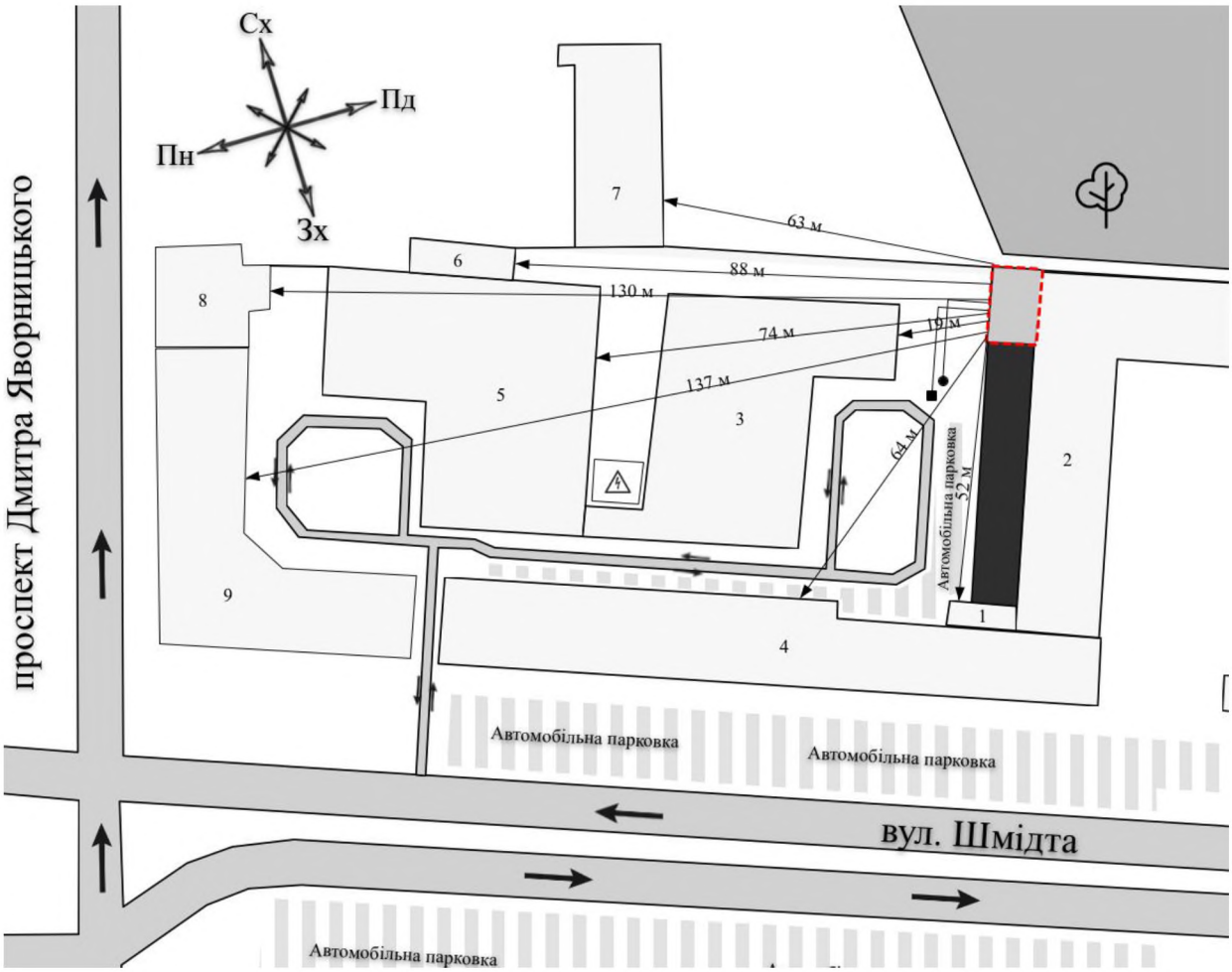
Вхід до ОІД можливий тільки з однієї сторони – з вулиці, сходами, які безпосередньо ведуть на другий поверх будівлі до вхідних дверей ОІД.

Границя контрольованої зони обмежена стінами приміщення в якому знаходиться ОІД.

ОІД має 4 вікна, перше вікно розташовано з північної сторони, останні три вікна розташовані зі східної сторони та мають залізні грати із зовнішньої сторони приміщення з розміром осередку 15 см на 30 см, діаметр арматури 15мм.

Охорону ОІД забезпечує охоронна служба «Гуард». Охоронця на об'єкті немає.

На ситуаційному плані (Рисунок 2.1) відображено розташування ОІД на місцевості.



Умовні позначення:

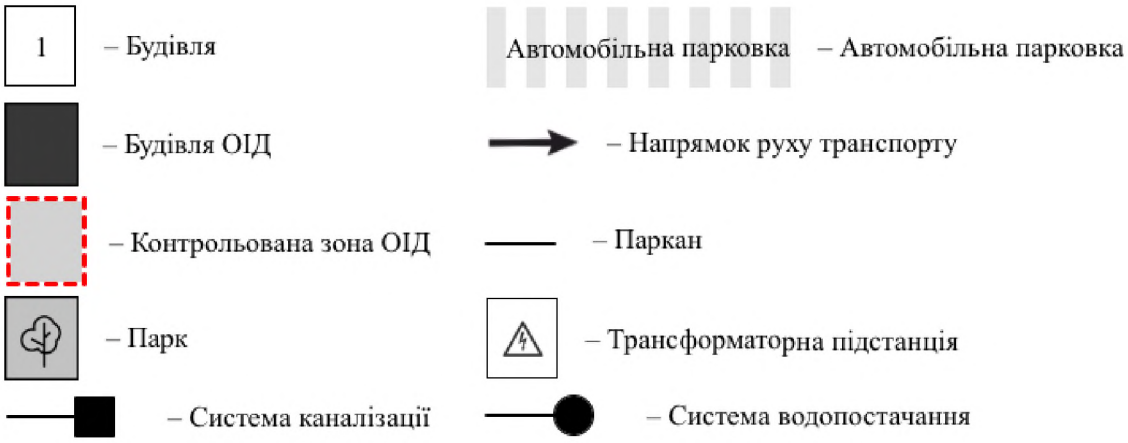


Рисунок 2.1 – Ситуаційний план

Таблиця 2.1 – Характеристика будівель та споруд

№	Найменування	Адреса	Кількість поверхів	Відстань до ОІД, м
1	Нежила технічна будівля	проспект Дмитра Яворницького, 111	1	52
2	Малі торгівельні приміщення	Шмідта, 2Б	1	–
3	Офісні приміщення	проспект Дмитра Яворницького, 111	1	19
4	Нежилий будинок з магазинами	Шмідта, 3	3	64
5	Торгівельний центр «Berlin»	проспект Дмитра Яворницького, 111	4	74
6	Господарський корпус	–	1	88
7	Багатоквартирний житловий будинок	проспект Дмитра Яворницького, 109	5	63
8	Нежилий будинок з магазинами	проспект Дмитра Яворницького, 109а	3	130
9	Нежилий будинок з магазинами	проспект Дмитра Яворницького, 111а	3	137

Системи опалення, водопостачання та каналізації – централізовані та підключені через підвальне приміщення будівлі в якій знаходиться ОІД.

Система електропостачання – централізована, трансформаторна підстанція розташована за 75 метрів від будівлі, в якій знаходиться ОІД.

Електропостачання надходить до будівлі підземними комунікаціями та заходить в підвальне приміщення в якій знаходиться ОІД.

Система мережі Інтернет – централізована, від Інтернет-провайдеру «DTS». Кабель надходить до офісу з розподільного щитка який знаходиться на першому поверсі.

Схема генерального плану ОІД наведена на рисунку 2.2.

Загальна площа усіх приміщень ОІД становить 53,94 м². Розміри – 9,30 м на 5,80 м. Висота стелі – 3 м, матеріал – залізобетонні плити;

Товщина несучих стін – 50 см, матеріал – шлакоблок;

Товщина перегородок – 20 см, матеріал – цегла;

Товщина підлоги – 30 см, матеріал – залізобетонні плити.

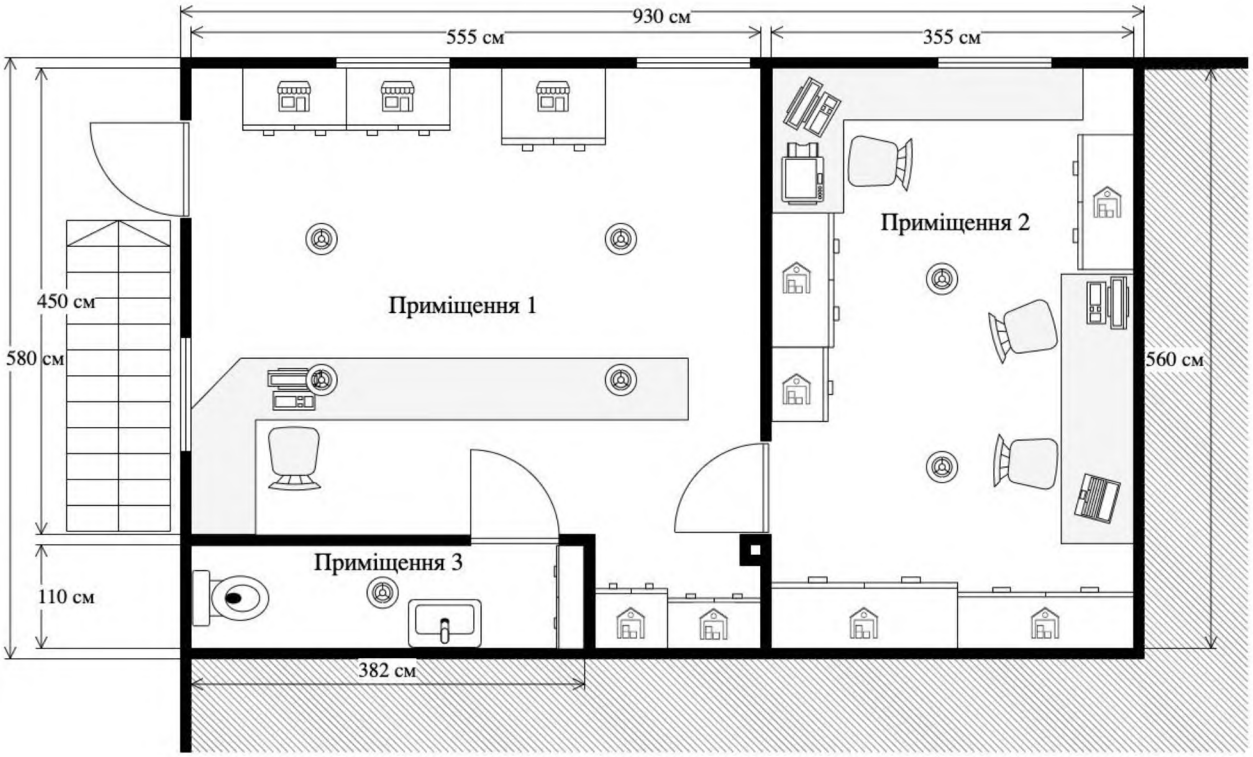
Вхідні двері розміром 110 см на 210 см, матеріал – металеві, товщина двері – 90 мм, двері з врізаним замком під ключ.

Міжкімнатні двері розміром 90 см на 210 см, матеріал – ДСП, товщина двері 60 мм, двері з врізаним замком під ключ.

Всі чотири вікна відчиняються всередину приміщення, матеріал – ПВХ, склопакет однокамерний (два скла), розмір кожного вікна – 110 см на 140 см.

Сектор видимості вікон – будівля №3, будівля №5 (північна сторона); парк (східна сторона).

На вікні з північної сторони встановлені горизонтальні жалюзі, які частіше знаходяться у відкритому положенні.



Умовні позначення:

Рисунок 2.2 – Генеральний план. Загальний

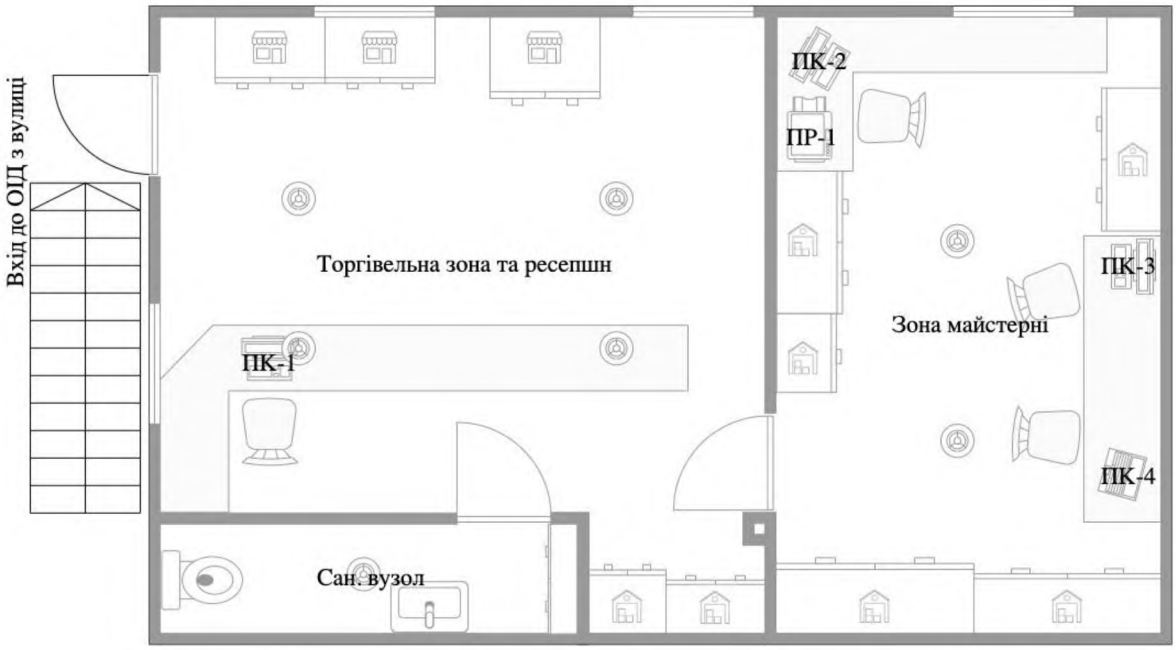
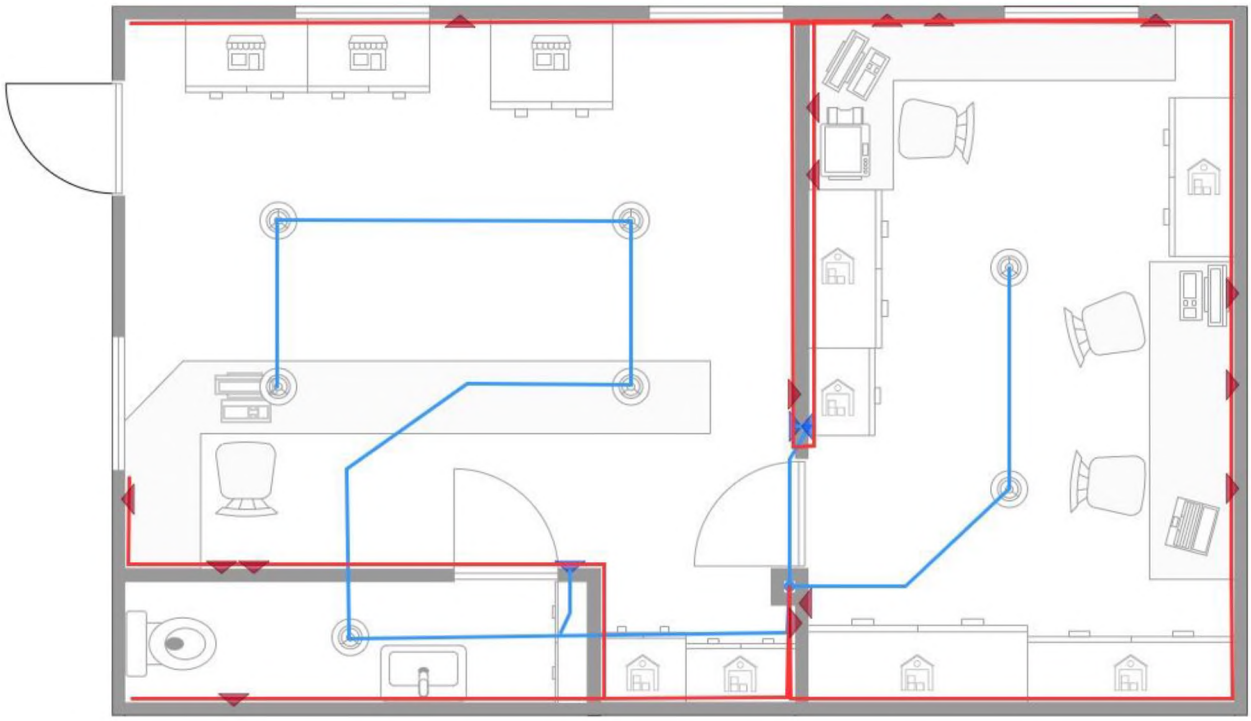


Рисунок 2.3 – Генеральний план. Опис приміщень



Умовні позначення:

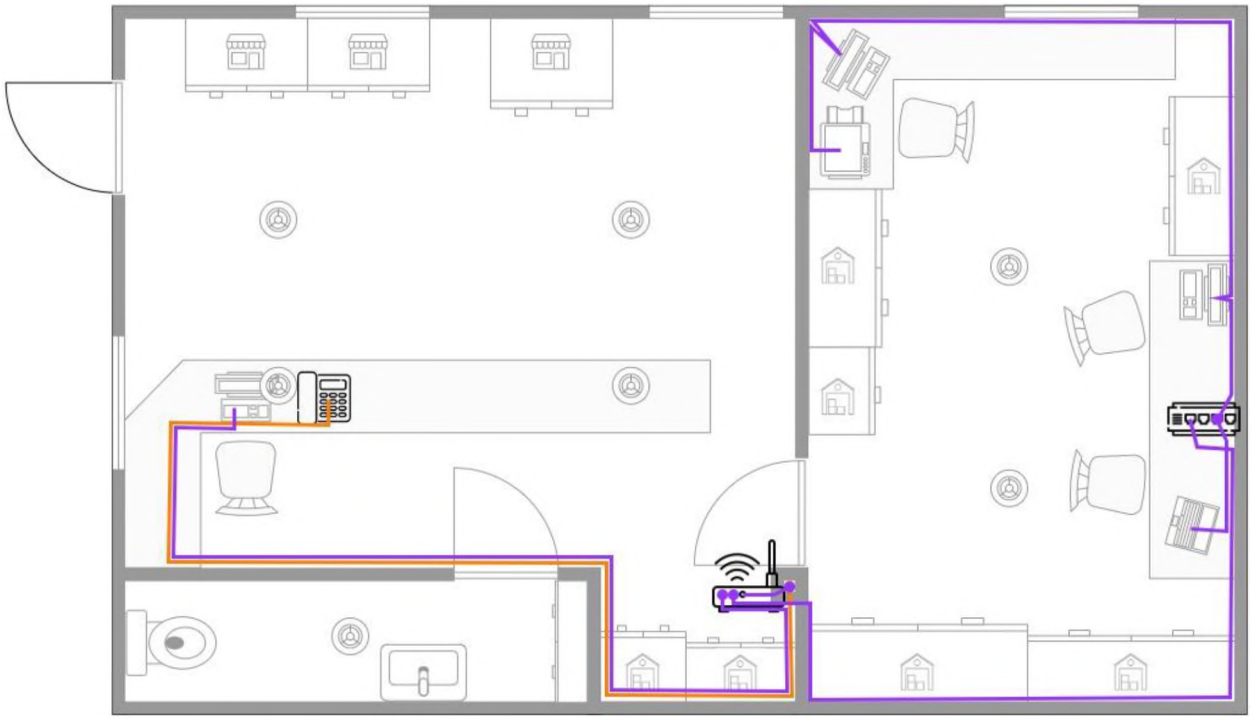
– Лінія системи електропостачання

– Лінія системи освітлення

– Розетка 220В

– Вимикач світла

Рисунок 2.4 – Генеральний план. Лінії систем електропостачання та освітлення



Умовні позначення:

– Лінія телефонного зв'язку

– Лінія комп'ютерної мережі

– Комутатор

– WiFi роутер

– Стаціонарний телефон

Рисунок 2.5 – Генеральний план. Лінії систем телефонної та комп’ютерної мереж

2.2.2 Обстеження обчислювальної системи

ІТС ОІД являє собою мережу типу «зірка», побудована з використанням одного маршрутизатору з функцією Wi-Fi та одного комутатору.

Являє собою багатомашинний багатокористувацький комплекс, задача якого – обробка як конфіденційної інформації з обмеженим доступом, так і відкритої інформації. Також цей комплекс має необмежений доступ мережі до Інтернет, який забезпечує Інтернет-провайдер «DTS».

ІТС відноситься до третього класу АС.

Обчислювальна система складається з чотирьох ПК, з яких три ПК – стаціонарні та один ПК – портативний і одного принтеру (принтер-ксерокс-сканер).

На рисунку 2.6 представлена структурна схема ІТС.

В таблиці 2.2 наведено мережеве обладнання.

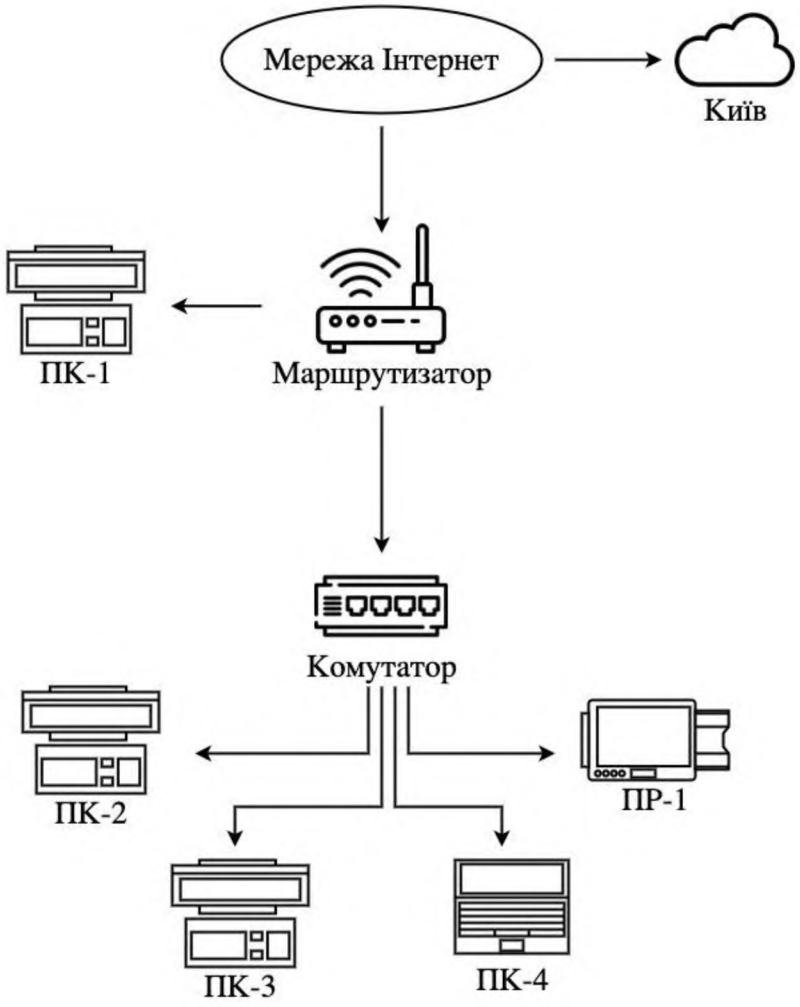


Рисунок 2.6 – Схема ІТС

Таблиця 2.2 – Мережеве обладнання

№	Назва	Модель	Специфікація
1	Маршрутизатор	TP-LINK Archer A8	4 порти LAN; Wi-Fi-; 1.9Гбіт/с
2	Комутатор	TP-LINK TL-SG108-M2	8 портів LAN; 2.5Гбіт/с

Інформація щодо основних та додаткових технічних засобів, які використовуються на ОІД, наведено в таблицях 2.3 та 2.4.

Таблиця 2.3 – Основні технічні засоби

Ім’я	Ім’я в ІС	Специфікація	Серійний номер	Користувач
ПК-1	Manager1-PC	Монітор ASUS VA24EHE, на столі, 1.5м до границі КЗ	41NP030691	Менеджер
		Клавіатура Defender HM-710, на столі, 1.5м до границі КЗ	KB0942665-34	
		Миша Genius NS-120, на столі, 1.5м до границі КЗ	12964WA5442SE	
		Системный блок ASUS D500MAES, під столом, 1.5м до границі КЗ	X550CC-X0420H	
ПК-2	Master1-PC	Монітор Samsung SyncMaster 2343BW, на столі, менше 1м до	GR356FE360844FE	Майстер з ремонту

		границі КЗ		

Продовження таблиці 2.3 – Основні технічні засоби

Ім’я	Ім’я в ІС	Специфікація	Серійний номер	Користувач
		Монітор Samsung SyncMaster 940N, на столі, менше 1м до границі КЗ	GT18H4UR300158E	
		Клавіатура A4Tech KV-300H, на столі, менше 1м до границі КЗ	RM1702K300H0	
		Миша A4Tech G9-500FS, на столі, менше 1м до границі КЗ	UE1812012407	
		Системний блок іншої конфігурації, під столом, менше 1м до границі КЗ	–	
ПК-3	Master2-PC	Монітор Samsung SyncMaster 2343BW, на столі, менше 1м до границі КЗ	GR238FG547224FD	Майстер з ремонту
		Монітор Samsung SyncMaster 940N, на столі, менше 1м до границі КЗ	GT22H4UD605352E	

		Клавіатура Logitech G213 Prodigy, на	1841SCK08A18	

Продовження таблиці 2.3 – Основні технічні засоби

Ім’я	Ім’я в ІС	Специфікація	Серійний номер	Користувач
		столі, менше 1м до границі КЗ		
		Миша Logitech M170, на столі	1738LZX30UWA8	
		Системний блок іншої конфігурації, під столом, менше 1м до границі КЗ	–	
ПК-4	Buhgalter 1-PC	Ноутбук Lenovo ThinkPad E14, на столі, менше 1м до границі КЗ	PF-0QQJQM	Бухгалтер
ПР-1	HP-M428dw	МФУ HP LaserJet Pro M428dw, на столі, 2м до границі КЗ	VNB4F85NF2	–
Мар-шру-ти-за-тор	TL-ArcherA8	4 порти LAN; Wi-Fi-; 1.9Гбіт/с, закріплений на стіні, 1м до границі КЗ	2167481000585V1.0	–
Ко-му-та-тор	TL-SG108	8 портів LAN; 2.5Гбіт/с, закріплений на стіні, менше 1м до	5467351000234A	–

		границі КЗ		

Таблиця 2.4 – Допоміжні технічні засоби

Ім’я	Специфікація	Серійний номер	Користувач
Світлоідодна лампа 1-7 (7 шт.)	VIS-30-E27, в стелі	–	–
IP-відеокамера спостереження з Wi-Fi 1-3 (3 шт.)	TP-LINK Tapco C200, на стіні, 1.5м до границі КЗ (1), менше 1м до границі КЗ (2-3)	NSC20KH2-K25, NSC20HS-FK3, NS7D4KHF-3F5	–
Настільні лампи 1-7 (7 шт.)	На столі	–	–
Інфрачервона паяльна станція	ACHI IR6500, на столі, менше 1м до границі КЗ	ND3894YF762K	Майстер з ремонту
Термо-воздушна паяльна станція 1	Lukey 852D, на столі, менше 1м до границі КЗ	84ND9B3534	Майстер з ремонту
Термо-воздушна паяльна станція 2	Lukey 852D, на столі, 1м до границі КЗ	34NV9FG432	Майстер з ремонту
Лабораторний блок живлення 1	Zhaoxin RXN 305D, на столі, менше 1м до границі КЗ	ENK23KR3-30V	Майстер з ремонту
Лабораторний блок живлення 2	Zhaoxin RXN 305D, на столі, 1м до границі КЗ	EDK42KR3-30V	Майстер з ремонту

Продовження таблиці 2.4 – Допоміжні технічні засоби

Ім’я	Специфікація	Серійний номер	Користувач
Лабораторний блок живлення 3	Zhaoxin RXN 305D, на столі, 1.5м до границі КЗ	EBK212R3-30V	Майстер з ремонту
Осцилограф	Hantek DSO5102P, на столі, менше 1м до границі КЗ	JF2387F3F	Майстер з ремонту
Мультиметр 1-4 (4 шт.)	UNI-T UT33C, в столі, менше 1м до границі КЗ	MUT33432LF, MUT3343245, MUT33432N4, MUT33432B1	Майстер з ремонту
Програматор мікросхем	TL866 Universal programmer, в столі, 1.5м до границі КЗ	F312MR-866	Майстер з ремонту
Тачскрин-дисплей сепаратор	RUNTOP, на столі, менше 1м до границі КЗ	–	Майстер з ремонту
RLC-тестер	В столі, менше 1м до границі КЗ	–	Майстер з ремонту
Ультразвукова ванна	В стелажі, 2м до границі КЗ	–	Майстер з ремонту
Принтер-тестер для картриджів 1	Samsung ML-1660, на столі, менше 1м до границі КЗ	SML12FJ4G4	Майстер з ремонту

Продовження таблиці 2.4 – Допоміжні технічні засоби

Ім’я	Специфікація	Серійний номер	Користувач
Принтер-тестер для картриджів	Samsung CJX-1000, в стелажі, 2м до границі КЗ	SCJXS892KG6	Майстер з ремонту
Програматор мультиконтролерів	В столі, менше 1м до границі КЗ	–	Майстер з ремонту
Мікроскоп	МБС-10, на столі, менше 1м до границі КЗ	–	Майстер з ремонту
Програматор мобільних телефонів	OCTOPLUS, Medusa PRO, в стелажі, 3м до границі КЗ	–	Майстер з ремонту
Програматор флеш-пам’яті	TNM5000, в стелажі, 2м до границі КЗ	JFK32MRF453	Майстер з ремонту

Таблиця 2.5 – Характеристика комп’ютерів

Ім’я	Ім’я в ІС	Характеристики
ПК-1	Manager1-PC	Процесор: Intel Pentium G4620
		Оперативна пам’ять: DDR3 4 ГБ
		Накопичувач: HDD 1 ТБ
		Відео карта: Інтегроване відео
		Материнська плата: H270
ПК-2	Master1-PC	Процесор: AMD Ryzen 7
		Оперативна пам’ять: DDR3 8 ГБ
		Накопичувач: SSD 250 ГБ, HDD 1 ТБ
		Відео карта: Nvidia GTX 650
		Материнська плата: Gigabyte G1 Sniper Z-97

Продовження таблиці 2.5 – Характеристика комп'ютерів

Ім'я	Ім'я в ІС	Характеристики
ПК-3	Master2-PC	Процесор: AMD Ryzen 7
		Оперативна пам'ять: DDR3 16 ГБ
		Накопичувач: SSD 250 ГБ, HDD 2 ТБ
		Відео карта: Nvidia GTX 650
		Материнська плата: Gigabyte G1 Sniper Z-97
ПК-4	Buhgalter1-PC	Процесор: Intel Core i5-10210U
		Оперативна пам'ять: DDR4 8 ГБ
		Накопичувач: M.2 SSD 120 ГБ, HDD 500 ГБ
		Відео карта: Інтегроване відео
		Материнська плата: Lenovo

Таблиця 2.6 – Програмне забезпечення

Ім'я	Тип ПЗ	Встановлено	Тип ліцензії	Термін дії ліцензії
Windows 10 Home	Системне	ПК-1, ПК-4	Корпоративна	Необмежений
Ubuntu 21.04 LTC	Системне	ПК-2	Free	–
Windows 10 Pro	Системне	ПК-3	Корпоративна	Необмежений
Windows 7 Ultimate	Системне	ПК-3	Корпоративна	Необмежений
Драйвери	Системне	ПК-1 – ПК-4	–	–
CRM	Прикладне	ПК-1 – ПК-4	Корпоративна	1 рік (підписка)
ERP	Прикладне	ПК-1 – ПК-4	Корпоративна	1 рік (підписка)

Продовження таблиці 2.6 – Програмне забезпечення

Ім’я	Тип ПЗ	Встановлено	Тип ліцензії	Термін дії ліцензії
M.E. Doc	Прикладне	ПК-4	Корпоративна	1 рік (підписка)
1С: Каса	Прикладне	ПК-1, ПК-4	Корпоративна	Необмежений
1С: Бухгалтерія	Прикладне	ПК-4	Корпоративна	Необмежений
Google Chrome	Прикладне	ПК-1 – ПК-4	Free	–
Пакет програм MS Office (Word, Excel, Outlook)	Прикладне	ПК-1 – ПК-4	Корпоративна	1 рік (підписка)
7-Zip	Прикладне	ПК-1 – ПК-4	GNU	–
TeamViewer	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
Notepad++	Прикладне	ПК-2, ПК-3	Volume license	–
Proteus	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
Visual Analyser	Прикладне	ПК-2, ПК-3	Free	–
Sprint-Layout	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
SP Flash Tool	Прикладне	ПК-2, ПК-3	Free	–
QFIL	Прикладне	ПК-2, ПК-3	Free	–
Odin	Прикладне	ПК-2, ПК-3	GNU	–
ASUS Flash Tool	Прикладне	ПК-2, ПК-3	Free	–

Продовження таблиці 2.6 – Програмне забезпечення

Ім’я	Тип ПЗ	Встановлено	Тип ліцензії	Термін дії ліцензії
XiaoMiFlash	Прикладне	ПК-2, ПК-3	GNU	–
Aida 64	Прикладне	ПК-2, ПК-3	GNU	–
Memtest	Прикладне	ПК-2, ПК-3	Free	–
Recuva	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
Victoria	Прикладне	ПК-2, ПК-3	Free	–
Driver Pack	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
3uTools	Прикладне	ПК-2, ПК-3	GNU	–
iTunes	Прикладне	ПК-2, ПК-3	GNU	–

Всі пристрої ІТС з’єднані між собою за допомогою крученої пари.

Кручена пара надходить до ОІД з першого поверху та потрапляє до маршрутизатору.

Далі від маршрутизатора підключений комп’ютер ПК-1 та комутатор, до комутатору підключені комп’ютери ПК-2, ПК-3, ПК-4 та принтер ПР-1.

Можливість друку на принтері ПР-1 здійснюється за допомогою локальної мережі. До принтеру ПР-1 мають доступ всі комп’ютери локальної мережі.

2.2.3 Обстеження інформаційного середовища

На ОІД циркулює відкрита інформація та інформація з обмеженим доступом (конфіденційна). Конфіденційна інформація має можливість поширювання зі згоди відповідної за неї особи, у визначеному нею порядку та в інших випадках, які не порушують політику компанії.

Інформація на ОІД зберігається в паперовому та електронному виді. Паперова інформація зберігається в ящику стола бухгалтера, який закритий на ключ. Електронна інформація зберігається на комп’ютері бухгалтера ПК-4.

Після закінчення терміну дії документа він видаляється з комп'ютера (якщо електронний) або знищується шредером для паперів (якщо паперовий).

До комп'ютеру бухгалтера ПК-4 має доступ тільки бухгалтер, авторизуючись під обліковим записом "User" та паролем, який знає тільки бухгалтер.

На ОІД циркулює інформація таких типів:

- Організаційно-розпорядча;
- Бухгалтерська звітність;
- Фінансова звітність;
- Про вартість послуг та товарів;
- Про закупочну вартість товарів та комплектуючих;
- Про закази товарів;
- Про реалізацію товарів;
- Про активні ремонти;
- Про виконані ремонти;
- Про співробітників;

В таблиці 2.7 наведена більш детальна характеристика інформації, що циркулює на ОІД

Таблиця 2.7 – Характеристика інформації, що циркулює на ОІД

№	Інформація	Режим доступу	Правовий режим	Вимоги до захисту		
				К	Ц	Д
1	Організаційно-розпорядча	ІЗоД	Конфіденційна інформація	К2	Ц3	Д2
2	Бухгалтерська	ІЗоД	Комерційна таємниця	К3	Ц4	Д4
3	Фінансова	Відкрита	–	К1	Ц4	Д3
4	Про закази товарів	ІЗоД	Комерційна таємниця	К2	Ц4	Д3

Продовження таблиці 2.7 – Характеристика інформації, що циркулює на ОІД

№	Інформація	Режим доступу	Правовий режим	Вимоги до захисту		
				К	Ц	Д
5	Про вартість послуг та ремонту	Відкрита	–	К1	Ц4	Д2
6	Про активні та виконані ремонти	ІЗоД	Конфіденційна інформація	К3	Ц4	Д3
6	Про клієнтів	ІЗоД	Конфіденційна інформація	К3	Ц4	Д2
7	Про співробітників	ІЗоД	Конфіденційна інформація	К4	Ц4	Д2

Конфіденційність – це така інформація, яка не може бути отримана користувачем який не проходив авторизацію.

Цілісність – це відсутність можливості будь якої модифікації інформації користувачем який не проходив авторизацію.

Цілісність інформації це дуже важливий аспект в інформаційній безпеці, який забезпечує запобігання несанкціонованих змін в інформації та/або її руйнування.

Доступність полягає в тому, що користувач який пройшов авторизацію може використовувати інформацію відповідно до встановлених політикою безпеки правил, не очікуючи довше прийнятого інтервалу часу.

Рівні конфіденційності інформації:

- К-1 – рівень, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

- К-2 – рівень, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- К-3 – рівень, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- К-4 – рівень, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;
- К-5 – критичний рівень, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності інформації:

- Ц-1 – рівень, при якому можна знехтувати втратою цілісності інформації;
- Ц-2 – рівень, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;
- Ц-3 – рівень, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;
- Ц-4 – рівень, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;
- Ц-5 – критичний рівень, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності інформації:

- Д-1 – рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;
- Д-2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;
- Д-3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

- Д-4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;
- Д-5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Організаційно-розпорядча інформація зберігається, створюється та редагується на комп'ютері менеджера ПК-1 та комп'ютері бухгалтера ПК-4.
За потребою поширюється серед майстрів з ремонту за допомогою локальної мережі або корпоративної електронної пошти.
Види зберігання: паперовий, електронний.

Бухгалтерська звітність зберігається, створюється та редагується на комп'ютері бухгалтера ПК-4.
За потребою поширюється до комп'ютера менеджера ПК-1 за допомогою локальної мережі або корпоративної електронної пошти та до головного офісу в Київ корпоративною електронною поштою.
Види зберігання: паперовий, електронний.

Фінансова звітність зберігається, створюється та редагується на комп'ютері бухгалтера ПК-4.
За потребою поширюється до комп'ютера менеджера ПК-1 за допомогою локальної мережі або корпоративної електронної пошти та до головного офісу в Київ корпоративною електронною поштою.
Види зберігання: паперовий, електронний.

Інформація про співробітників зберігається, створюється та редагується на комп'ютері бухгалтера ПК-4.
За потребою поширюється до комп'ютера менеджера ПК-1 за допомогою локальної мережі або корпоративної електронної пошти та до головного офісу в Київ корпоративною електронною поштою.
Види зберігання: паперовий, електронний.

Інформація про клієнтів зберігається, створюється та редагується на комп'ютері менеджера ПК-1.

За потребою поширюється до комп'ютера бухгалтера ПК-4 за допомогою локальної мережі або корпоративної електронної пошти.

Види зберігання: паперовий, електронний.

Інформація про вартість послуг та вартість товарів зберігається, створюється та редагується на комп'ютері менеджера ПК-1.

За потребою поширюється до комп'ютера бухгалтера ПК-4 за допомогою локальної мережі або корпоративної електронної пошти.

Види зберігання: електронний.

Інформація про ремонтні роботи зберігається, створюється та редагується на комп'ютері менеджера ПК-1, та поширюється до комп'ютерів майстрів з ремонту ПК-2 та ПК-3 за допомогою локальної мережі.

Види зберігання: електронний.

В таблиці 2.8 наведено матрицю розмежування доступу до інформації що циркулює на ОІД.

Таблиця 2.8 – Матриця розмежування доступу до інформації що циркулює на ОІД

№	Ім'я	Менеджер	Майстер 1	Майстер 2	Бухгалтер
1	Організаційно-розпорядча	RWD	R	R	RWD
2	Бухгалтерська	R	–	–	RWD
3	Фінансова	R	–	–	RWD
4	Про закази товарів	RWD			–
5	Про вартість послуг та ремонту	RWD	–	–	R
6	Про активні та виконані ремонти	RWD	RW	RW	–
6	Про клієнтів	RWD	–	–	R
7	Про співробітників	R	–	–	RWD

Умовні скорочення:

R – читання; W – запис; D – видалення;

2.3 Аналіз загроз інформації

2.3.1 Модель порушника

Модель порушника – абстрактний формалізований або неформалізований опис порушника, в якій порушник це користувач, що здійснює несанкціонований доступ до інформації.

Якщо існує інформаційна система, у якій циркулює інформація з обмеженим доступом та конфіденційні дані, то знайдеться особа (порушник), метою якої буде ознайомлення з інформацією, її модифікація чи знищення.

Для того, щоб розробити комплекс заходів по забезпеченню захищеності інформаційних ресурсів, необхідно побудувати модель можливого порушника. Ця модель може бути побудована з урахування різних критеріїв.

Модель порушника розробляється для того, щоб отримати відповіді на наступні питання:

- Від кого захищати інформацію?
- Яка мета порушника?
- Якими знаннями володіє порушник?
- Які повноваження в системі має потенційний порушник?
- Якими методами і засобами користується порушник?
- Яка обізнаність порушника щодо об’єкта інформаційної діяльності і системи охорони?

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей.

Порушників прийнято поділяти на зовнішніх і внутрішніх.

До внутрішніх належать співробітники, користувачі інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і

приміщення (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки).

Зовнішні порушники – це сторонні особи, які знаходяться поза контрольованою зоною підприємства або не авторизовані для використання даної комп'ютерної системи. Це означає, що вони не мають в системі облікового запису і згідно системної політики безпеки взагалі не можуть працювати в даній системі.

Приклад зовнішніх порушників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; кваліфіковані хакери; особи, яких найняли конкуренти для отримання необхідної інформації тощо.

Таблиця 2.9 – Категорії порушників

Позначення	Визначення	Рівень загроз
Внутрішні порушники:		
ПВ1	Менеджер	2
ПВ2	Майстер з ремонту	3
ПВ3	Бухгалтер	4
ПВ4	Покупці/клієнти	2
ПВ5	Технічний персонал	3
ПВ6	Персонал, що обслуговує технічні засоби	4
Зовнішні порушники:		
ПЗ1	Хакери	3
ПЗ2	Комунальні служби	2
ПЗ3	Конкуренти інших підприємства	3
ПЗ4	Сторонні особи	2

Класифікація порушників за мотивом порушень.

Зловмисники можуть порушувати інформаційну безпеку з різних причин.

Порушення можна розбити на дві групи – навмисні та ненавмисні.

Особи, які ненавмисно наносять збитків інформаційним ресурсам, порушуючи конфіденційність, цілісність або доступність інформації, не складають плану дій, не мають мети та спеціальних методів та засобів реалізації запланованого порушення. Ненавмисні порушення частіше всього здійснюються в результаті недостатньої кваліфікації, неуважності персоналу.

Порушники, які наносять збитків інформаційним ресурсам навмисно, мають певну мету, готують план реалізації атаки на інформаційний ресурс. Навмисні порушення інформаційної безпеки здійснюються для нанесення збитків організації (матеріальних чи моральних), для власного збагачення за рахунок отриманої інформації, а також для нейтралізації конкурентів.

Таблиця 2.10 – Специфікація моделі порушника за мотивом здійснення порушень

Позначення	Мотив	Рівень загроз
М1	Помилка	1
М2	Неуважність	1
М3	Корисливі цілі	3
М4	Конкурентність (ПЗЗ)	4

Класифікація порушників інформаційної безпеки за рівнем знань про автоматизовані системи.

Кожен порушник має певний рівень кваліфікації та поінформованості відносно організації функціонування лабораторії зовнішніх та внутрішніх мереж інформаційного комп'ютерного комплексу. В залежності від рівня знань, якими володіє порушник, може бути нанесений певний рівень збитків інформаційним ресурсам організації.

В класифікації враховуються знання можливого порушника та його практичні навички у роботі з комп'ютерними системами та інформаційними технологіями.

Таблиця 2.11 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Кваліфікаційні ознаки	Рівень загроз
К1	Низький рівень кваліфікації, базові навички працювати з технічними засобами ІТС	1
К2	Середній рівень кваліфікації, володіє практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Високий рівень кваліфікації, володіє практичними навичками у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає всю структуру, функції, недоліки та механізми захисту інформації в ІТС	4

Класифікація порушників за рівнем можливостей, які надані їм засобами автоматизованої системи та обчислювальної техніки.

Внутрішніх порушників можна класифікувати за наданим рівнем повноважень у системі. Адже чим більше повноважень, там більше можливостей доступу до інформації з обмеженим доступом.

Таблиця 2.12 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Можливості	Рівень загроз

З1	Підслуховування, підглядання	1

Продовження таблиці 2.12 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Можливості	Рівень загроз
З2	Використання пасивних технічних засобів перехвату інформації	2
З3	Використання недоліків системи або інших способів обману системи	3
З4	Використання хакерського спеціалізованого ПЗ або інші технічні засоби впливу на ІТС для модифікації або крадіжки інформації	4

Класифікація порушника за місцем дії.

Ця класифікація проводиться для визначення розташування порушника відносно організації під час здійснення спроби несанкціонованого доступу до інформаційного ресурсу.

Таблиця 2.13 – Специфікація моделі порушника за місцем дії

Позначення	Можливості	Рівень загроз
Д1	За межами ОІД	1
Д2	В приміщенні (торгова зона та ресепшн)	2
Д3	В приміщенні (зона майстерні)	4

Таблиця 2.14 – Специфікація моделі порушника за часом дії

Позначення	Можливості	Рівень загроз
Ч1	Під час бездіяльності ІТС з метою відновлення або ремонту	1

Ч2	Під час призупинки ІТС з метою відновлення або ремонту	2

Продовження таблиці 2.14 – Специфікація моделі порушника за часом дії

Позначення	Можливості	Рівень загроз
Ч3	Під час функціонування ІТС	3
Ч4	У всіх випадках водночас	4

Таблиця 2.15 – Модель внутрішнього порушника

Посада	Мотив	Квалі-фікація	Можли-вості	Місце дії	Час дії	Категорія порушника	Сума загроз
Менеджер	М2	К2	З3	Д2	Ч3	ПВ1	13
Майстер з ремонту	М1	К1	З3	Д3	Ч3	ПВ2	18
Бухгалтер	М1	К2	З3	Д3	Ч3	ПВ3	20
Покупці/ клієнти	М3	К1	З1	Д2	Ч3	ПВ4	17
Технічний персонал	М4	К3	З3	Д3	Ч4	ПВ5	19
Персонал, що обслуговує технічні засоби	М4	К4	З3	Д3	Ч4	ПВ6	20

Таблиця 2.16 – Модель зовнішнього порушника

Посада	Мотив	Квалі-фікація	Можли-вості	Місце дії	Час дії	Категорія порушника	Сума загроз
Хакери	М3	К3	З4	Д1	Ч3	ПЗ1	17
Комунальні	М1	К1	З1	Д3	Ч3	ПЗ2	11

служби							

Продовження таблиці 2.16 – Модель зовнішнього порушника

Посада	Мотив	Квалі-фікація	Можли-вості	Місце дії	Час дії	Категорія порушника	Сума загроз
Конкуренти інших підприємства	М4	К4	З2	Д2	Ч3	ПЗ3	18
Сторонні особи	М3	К1	З1	Д2	Ч3	ПЗ4	12

2.3.2 Модель загроз

Загрози інформаційної безпеки можуть залежати від багатьох факторів, наприклад від таких факторів як персонал, програмні засоби або апаратні засоби фізичного середовища.

Згідно НД ТЗІ 1.1-003-99 побудована модель загроз являє собою абстрактний опис засобів і методів можливих загроз.

Модель загроз визначає різні класифікації і типи загроз та вказує на які властивості інформації будуть спрямовані загрози, визначає способи по втіленню загроз і так далі.

Таблиця 2.17 – Перелік загроз з визначенням порушень властивостей інформації та ІТС

№	Загрози	Властивості		
		К	Ц	Д
Загрози об’єктивної природи				
1.1	Стихійні явища (пожежа, аварія)		+	+
1.2	Збої або відмови електроживлення			+
1.3	Збої або відмови обчислювальної техніки			+

1.4	Збої або відмови носіїв інформації		+	+
1.5	Збої або відмови програмного забезпечення		+	+

Продовження таблиці 2.17 – Перелік загроз з визначенням порушень властивостей інформації та ІТС

№	Загрози	Властивості		
		К	Ц	Д
Загрози суб'єктивної природи				
2.1	Несанкціоноване підключення до технічних засобів та каналів зв'язку	+		
2.2	Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів, підслуховування	+		
2.3	Перехоплення інформації за рахунок ПЕМВ від технічних засобів	+		
2.4	Хакерські атаки через мережу Інтернет	+	+	
2.5	Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу	+		
Порушення нормальних режимів роботи				
2.2.1	Зараження системи комп'ютерними вірусами	+	+	+
2.2.2	Втрата або розголошення засобів розмежування доступу, носіїв інформації, резервних копій	+	+	+
2.2.3	Несанкціоноване внесення змін у технічні засоби, програмне забезпечення тощо		+	+
2.2.4	Використання стороннього програмного забезпечення		+	+
2.2.5	Пошкодження носіїв інформації	+	+	+
2.2.6	Вхід у систему недопущених осіб		+	+
Помилки персоналу				

2.3.1	Помилки при інсталяції програмного забезпечення або сторонніх програм		+	+

Продовження таблиці 2.17 – Перелік загроз з визначенням порушень властивостей інформації та ІТС

№	Загрози	Властивості		
		К	Ц	Д
2.3.2	Помилки при експлуатації програмного забезпечення або технічних засобів	+	+	+
2.3.3	Помилки при введенні даних		+	+

2.4 Визначення методів та засобів захисту

2.4.1 Профіль захищеності

Досліджувана АС є інформаційно-телекомунікаційною системою, яка включає в себе фізичне та інформаційне середовища.

Побудована модель загроз наглядно демонструє, що найбільшу вразливість в АС є загрози доступності, бо через специфіку роботи підприємства такі загрози можуть призвести до інколи репутаційних та частіше матеріальних збитків підприємства.

Також велику роль грає вразливість в АС через загрозу цілісності інформації також через специфіку роботи підприємства. Такі загрози можуть призвести до репутаційних та серйозних матеріальних збитків підприємства.

Відповідно, АС належить до класу «3» (розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності). Відміна «3» класу від попереднього класу – необхідність передачі інформації через незахищене середовище або через вузли які реалізують різну політику безпеки.

Відповідно до методичного забезпечення для АС, яка має «3» клас, було вибрано наступний профіль захищеності інформації:

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

Опис кожної реалізованої послуги критеріїв безпеки наведено нижче.

КД-2 Базова довірча конфіденційність. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ надає користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначати конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КА-2 Базова адміністративна конфіденційність. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта.

КО-1 Повторне використання об’єктів. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта будуть скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, стане недосяжною.

КВ-2 Базова конфіденційність при обміні. КЗЗ забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається. Запити на призначення або зміну рівня захищеності обробляються КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

ЦД-1. Мінімальна довірча цілісність. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта.

ЦА-2. Базова адміністративна цілісність. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

ЦО-1. Обмежений відкат. Існують автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-2: Базова цілісність при обміні. КЗЗ визначає множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується механізмами, які використовуються і спроможність користувачів і/або процесів керувати рівнем захищеності.

ДР-1. Квоти. Політика використання ресурсів, що реалізується КЗЗ визначає множину об'єктів КС, до яких вона відноситься.

ДВ-1. Ручне відновлення. КЗЗ визначає множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки.

НР-2. Захищений журнал. КЗЗ визначає перелік подій, що реєструються.

НИ-2. Одиночна ідентифікація і автентифікація. КЗЗ автентифікує користувача із використанням захищеного механізму.

НК-1. Однонаправлений достовірний канал. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-2. Розподіл обов'язків адміністраторів. КЗЗ не визначає ролі адміністратора і звичайного користувача і притаманні їм функції.

НЦ-2. КЗЗ з гарантованою цілісністю. КЗЗ не підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.

НТ-2. Самотестування при старті. КЗЗ не описує властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ при старті.

НВ-1: Автентифікація вузла. Підтвердження ідентичності виконується на підставі затвердженого протоколу автентифікації.

2.5 Політика безпеки

Під політикою безпеки інформації розуміють набір законів, правил, обмежень, рекомендацій та інших заходів, які регламентують порядок обробки інформації на підприємстві і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретніше і формальніше стають правила.

В ІТС на обраному підприємстві циркулює значна кількість інформації з обмеженим доступом, яка обов’язково потребує захисту від певних загроз.

Тому при підвищенні рівня захисту інформації обов’язково треба приділити увагу на організаційні заходи щодо правильного та гарантованого забезпечення функціонування політики безпеки інформації на підприємстві.

2.6 Організаційні заходи забезпечення політики безпеки

Проаналізувавши можливі загрози та вразливості в інформаційно-телекомунікаційній системі ТОВ «FixUp» маємо наступні пропозиції:

- Політика антивірусного захисту;
- Політика користування електронною поштою;
- Політика безпеки паролів користувачів;

2.6.1 Політика антивірусного захисту

Мета політики це створення вимог, які повинні дотримуватися всіма комп'ютерами в ІТС, щоб гарантувати ефективний захист від вірусів.

Створення умов постійної підтримки корпоративних вимог. Підтримка антивірусного програмного забезпечення є необхідною для корпоративного вузла. Завантажувати і підтримувати поточну версію.

Завантажувати і встановлювати свіжі модифікації антивірусного програмного забезпечення, як тільки вони стають доступними;

Ніколи не відкривати будь-які файли або макрокоманди, що торкаються електронної пошти від невідомого, підозрілого або ненадійного джерела. Треба негайно перемістити ці повідомлення в папку «Видалене» шляхом видалення листа, потім остаточно видалити лист за допомогою спорожнення папки «Видалені листи»;

Видаляти папку «Спам», ланцюг та іншу електронну пошту, яка не має атрибутів підприємства відповідно до політики безпеки;

Ніколи не завантажувати файли від невідомих або підозрілих джерел;

Уникати прямого дискового доступу (читання/запис), за винятком того, що відповідає необхідним діловим вимогам;

Перед використанням завжди сканувати диск/переносний носій/тощо від невідомого джерела або клієнтів на предмет вірусів;

Регулярно дублювати критичні дані і системні конфігурації, та зберігати їх в безпечному місці (видалене сховище, хмарне сховище);

Якщо лабораторна перевірка встановлює конфлікт з антивірусним програмним забезпеченням, треба запустити сторонню антивірусну утиліту, яка буде гарантувати незабрудненість комп'ютера. Після лабораторної перевірки дозволяється використовувати антивірусне програмне забезпечення. Під час блокування антивірусного програмного забезпечення ні в якому разі не можна завантажувати будь-які додатки, які могли б перенести вірус.

2.6.2 Політика користування електронною поштою

Листи можуть легко опинитися під контролем зловмисників, тому треба зобов'язати всіх співробітників дотримуватися цієї політики, щоб гарантувати ефективний захист від витоку інформації.

Ввімкнути шифрування листів на транспортному рівні, яке забезпечить безпеку повідомлення в процесі передачі через Інтернет. Даний метод схожий на вкладення листа в конверт, тобто можна побачити звідки та куди направляється повідомлення, проте його зміст можна побачити тільки після відкриття так званого «конверта».

Зробити фільтрування повідомлень за типом вкладення або дозволяти відправлення тільки від перевірених джерел. Багато організацій, щоб забезпечити захист пошти своїх користувачів, перевіряють повідомлення на наявність шкідливих програм і вірусів, перш ніж вони поширяться через мережу.

Всім співробітникам підключити багатофакторну автентифікацію. Ідентифікація особистості здійснюється за допомогою одноразового ключа, який відправляється в SMS-повідомленні. Багатофакторна автентифікація забезпечує захист пошти та є важливою частиною процесу входу в електронну скриньку або в мережу.

2.6.3 Політика безпеки паролів користувачів

Заборонити користувачам повторюваність паролів. Тобто, заборонити створювати новий пароль, який буде схожий на попередній.

Паролі користувачів повинні бути унікальними, та не повторюватись.

Встановити максимальний термін дії пароля до 12 місяців.

Якщо є ризик, що пароль було скомпрометовано – треба негайно змінити пароль на новий з усіма вимогами безпеки.

Заборонити використання простих паролів, таких як 12345678, ZAQWERTY, які містять особисту інформацію, дату народження, та іншу відкриту інформацію.

Встановити наступні вимоги щодо складності пароля:

пароль не повинен містити в собі будь які частини імені користувача;

пароль повинен мати довжину не менше 8 символів;

пароль повинен містити в собі наступні символи: A-Z, a-z, 0-9, !#%$.

2.7 Висновки

В ході виконання спеціального розділу наведено загальні відомості про ОІД, проведено повне обстеження від інформаційного середовища до обчислювальної системи. Виконано аналіз загроз інформаційної безпеки, побудовано модель порушника та модель загроз. Визначені методи та засоби захисту інформації, рекомендовані основні організаційні заходи щодо забезпечення політики безпеки.

Для запобігання загроз наведено рекомендації щодо впровадження політики антивірусного захисту, політики користування електронною поштою та політики безпеки паролів користувачів.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є визначення економічної доцільності розробки засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації. Для досягнення цієї мети необхідно здійснити розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту; показників економічної ефективності розробки та впровадження запропонованих рішень.

3.1 Розрахунок (фіксованих) капітальних витрат

До капітальних витрат належать витрати на розробку заходів із забезпечення інформаційної безпеки, а також витрати на придбання матеріальних та нематеріальних активів.

3.1.1 Визначення трудомісткості розробки засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації

Трудомісткість розробки визначається тривалістю кожної робочої операції:

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{p} + t_{\text{д}}, \text{годин} \qquad (3.1)$$

де:

$t_{\text{тз}}$ – тривалість складання технічного завдання на розробку засобів захисту інформації в гетерогенних мережах, $t_{тз}=6$;

$t_{\text{в}}$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_{в}=48$;

$t_{\text{а}}$ – тривалість аналізу існуючих загроз безпеки інформації, $t_{а}=24$;

$t_р$ – тривалість розробки засобів захисту інформації в гетерогенних мережах, $t_м$=*32*;

$t_д$ – тривалість підготовки технічної документації, $t_д$=*6*.

Отже,

$$t = 6 + 48 + 24 + 32 + 6 = 116 \text{ годин} \quad (3.2)$$

3.1.2 Розрахунок витрат на розробку засобів захисту інформації в гетерогенних мережах

Витрати на розробку заходів безпеки $К_{пз}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу $З_{мч}$:

$$З_{зп} = t * З_{пр} = 116 * 130 = 15080 \text{ грн} \quad (3.3)$$

$$К_{пз} = З_{зп} + З_{мч} = 15080 + 740{,}08 = 15820{,}08 \text{ грн} \quad (3.4)$$

де :

t – загальна тривалість операцій, годин;

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

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t * С_{мч} = 116 * 6{,}38 = 740{,}08 \text{ грн} \quad (3.5)$$

де:

t – трудомісткість операцій із побудови ефективної системи доступу персоналу, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р * t_{нал} * С_е + \frac{Ф_{зал} * Н_а}{F_р} + \frac{К_{лпз} * Н_{апз}}{F_р} \text{ грн} \quad (3.6)$$

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 на 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 (за 40-годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.11,808+1,3541+0,8125

$$С_{мч} = 0{,}5 * 5 * 1{,}68 + \frac{6600 * 0{,}4}{1920} + \frac{5150 * 0{,}3}{1920} = 6{,}38 \text{ грн} \qquad (3.7)$$

Відповідно до поставлених задач в контексті розробки засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації необхідне придбання наступних матеріальних активів:

Таблиця 3.1 – Вартість матеріальних активів для розробки засобів захисту інформації в гетерогенних мережах

Матеріальний актив	Кількість	Ціна, грн.	Вартість, грн.
Антивірус ESET Smart Security Premium (на 1 рік)	4	1152	4608
Разом:			4608

Заплановані витрати на налагодження системи інформаційної безпеки в розмірі 2500 грн. ($К_н$=2500 грн.)

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} \quad (3.8)$$

де:

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

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

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

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

Отже, капітальні (фіксовані) витрати на розробку засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі складуть:

$$К = 15820{,}08 + 4608 + 2500 = 22928{,}08 \text{ грн} \quad (3.9)$$

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак} \text{ грн} \quad (3.10)$$

де:

$С_{в}$ - вартість відновлення й модернізації системи;

$С_{к}$ - витрати на керування системою в цілому;

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

$С_а$ – Річний фонд амортизаційних відрахувань, визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ).

При розробці засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації витрати на відновлення й модернізації системи не матимуть місце.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос} \text{ грн} \quad (3.11)$$

Таблиця 3.2. Групи основних засобів та інших необоротних активів і мінімально допустимі строки їх амортизації

Групи	Мінімально допустимі строки корисного використання років
Група 4 – машини та обладнання З них: Електронно-обчислювальні машини, інші машини для автоматичного оброблення інформації, пов'язані з ними засоби зчитування або друку інформації, пов'язані з ними комп'ютерні програми (крім програм, витрати на придбання яких визнаються роялті, та/або програм, які визнаються нематеріальним активом), інші інформаційні системи, комутатори, маршрутизатори, модулі, модеми, джерела безперебійного живлення, та засоби їх підключення до телекомунікаційних мереж, телефони (в тому числі стільникові), мікрофони і рації, вартість яких перевищує 2500 гривень.	5 2

Таблиця 3.3. Строки амортизації нематеріальних активів

Групи	Строк дії права користування
Група 5 – авторське право та суміжні з ним права (право на комп'ютерні програми, програми для електронно-обчислювальних машин, компіляції даних (бази даних)), крім тих, витрати на придбання яких визнаються роялті;	Відповідно до правовстановлюючого документа, але не менш ніж 2 роки

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

$$С_з = З_{осн} + З_{дод} \text{ грн} \quad (3.12)$$

Річні амортизаційні відрахування матеріальних активів, які відповідно до чинного законодавства України підлягають амортизації, визначатимуться, виходячи зі строку корисного використання 5 років. Сума амортизаційних відрахувань визначається за прямолінійним методом нарахування амортизації. Таким чином, річні амортизаційні відрахування складуть:

$$С_а = 4608 \text{ грн} \quad (3.13)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати. Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 15080 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо реалізації засобів захисту інформації в гетерогенних мережах потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (15080 * 12 + 15080 * 12 * 0{,}1) * 0{,}25 = 49764 \text{ грн} \quad (3.14)$$

Ставка ЄСВ для всіх категорій платників з 01.01.2022 р. складає 22%. (мінімальний ЄСВ 1430,00 грн.)

$$С_{єв} = 49764 * 0,22 = 10948,08 \quad (3.15)$$

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

$$С_{ел} = Р * F_р * Ц_е \text{ грн} \quad (3.16)$$

де:

Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,5 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,5 * 1920 * 1,68 = 1612,80 \text{ грн} \quad (3.17)$$

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

$$С_{тос} = 22928,08 * 0,02 = 458,56 \text{ грн} \quad (3.18)$$

Таким чином, витрати на керування системою інформаційної безпеки ($С_к$) становлять:

$$С_к = 4608 + 49764 + 10948,08 + 1612,80 + 458,56 = 67391,44 \text{ грн} \quad (3.19)$$

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

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 67391{,}44 \text{ грн} \quad (3.20)$$

3.2 Оцінка можливого збитку

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 6 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 20000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 10000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 3 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 580 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 3;

N – середнє число атак на рік, 7.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \quad (3.21)$$

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:

$$П_П = \frac{\sum З_с}{F} * t_n = \frac{10000 * 6}{176} * 6 = 2045{,}45 \text{ грн} \quad (3.22)$$

де:

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.23)$$

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 $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви} = \frac{10000 * 6}{176} * 6 = 2045{,}45 \textbf{ грн} \quad (3.24)$$

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

$$П_{пв} = \frac{\sum З_о}{F} * t_в = \frac{20000 * 2}{176} * 3 = 681{,}82 \text{ грн} \quad (3.25)$$

Витрати на заміни встаткування або запасних частин можуть скласти 3400 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 2045{,}45 + 681{,}82 + 3400 = 6127{,}27 \text{ грн} \quad (3.26)$$

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

$$V = \frac{О}{Fг} \cdot (t_П + t_В + t_{ВИ}) \quad (3.27)$$

$$V = \frac{580000}{2080} * (6 + 3 + 6) = 4182{,}70 \text{ грн} \quad (3.28)$$

де:

$F_г$ – річний фонд часу роботи (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 681{,}82 + 6127{,}27 + 4182{,}70 = 10991{,}79 \text{ грн} \quad (3.29)$$

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

$$\text{В} = \Sigma_{\text{I}}\Sigma_{\text{N}}U = \Sigma_3\Sigma_7 10991{,}79 = 230827{,}59 \text{ грн} \quad (3.30)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B * R - C \text{ грн} \quad (3.31)$$

де:

В – загальний збиток від атаки у разі перехоплення інформації, 230827,59 грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці;

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

Загальний ефект від впровадження системи інформаційної безпеки за становитиме:

$$E = 230827{,}59 * 0{,}4 - 67391{,}44 = 24939{,}60 \text{ грн} \quad (3.32)$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

За методикою сукупної вартості володіння (ТСО) визначають такі показники економічної ефективності системи інформаційної безпеки як Коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K} \text{ частки одиниці} \quad (3.33)$$

де:

Е – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI складе:

$$\text{ROSI} = \frac{24939,60}{22928,08} = 1,09 \text{ частки одиниці} \quad (3.34)$$

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

$$ROSI > (N_{\text{деп}} - N_{\text{інф}})/100 \quad (3.35)$$

де:

$N_{деп}$ – річна депозитна ставка, (10,75 %);

$N_{інф}$ – річний рівень інфляції, (10 %).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,09 > (10 - 10,75)/100 = 1,09 > 0,0075 \quad (3.36)$$

Отже, запропоновані засоби захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації можна вважати економічно доцільними.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки. Відповідно термін окупності розробки засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет складе:

$$T_o = \frac{К}{Е} = \frac{1}{ROSI} = \frac{1}{1,09} = 0,92 \text{ року (11 місяців)} \quad (3.37)$$

3.4 Висновок

Запропоновані засоби захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації можна вважати економічно доцільними, оскільки значення коефіцієнту повернення інвестицій ROSI, що складає 1,09 при величині економічного ефекту 24939,60 грн. Отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів. Термін окупності при цьому складатиме 0,92 року (приблизно 11 місяців). Капітальні витрати на засоби захисту інформації складуть в 22928,08 грн., а щорічні експлуатаційні витрати складатимуть 67391,44 грн.

ВИСНОВКИ

У першому розділі розглянуто стан питання щодо безпеки інформаційного та кіберпростору, здійснено опис стану загроз інформаційної безпеки, наведено та проаналізовано нормативно-правову базу у сфері захисту інформації та поставлені задачі для досягнення поставленої мети щодо підвищення рівня інформаційної безпеки інформаційно-телекомунікаційної системи ТОВ «FixUp».

У спеціальному розділі наведено загальні відомості про ОІД, проведено обстеження об'єкту захисту інформації, обчислювальної системи та інформаційного середовища. Проведено аналіз можливих загроз інформаційної безпеки на підприємстві, розроблена модель порушника та модель загроз безпеки інформації. В кінці розділу для запобігання загроз наведено рекомендації щодо підвищення рівню інформаційної безпеки завдяки впровадженню політики антивірусного захисту, політики користування електронною поштою та політики безпеки паролів користувачів.

В економічному розділі проведено розрахунки збитку від реалізації загрози, визначено економічну доцільність та витрати на засоби забезпечення інформаційної безпеки підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 кібербезпека / Упоряд.: О.В. Герасіна, Д.С. Тимофеєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП» 2020.
2. Методичні рекомендації до економічної частини дипломного проекту зі спеціальності 125 кібербезпека / Упоряд.: Д.П. Пілова – Дніпро: НТУ «ДП» 2019.
3. Закон Україні «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України-1992-No48. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12
4. Закон Україні «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No80-VI // Відомості Верховної Ради України-1994-No80. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр
5. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
6. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
7. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. [Чинний від 04.12.2000] – К.: ДСТСЗІ СБУ, 2000-No53 (Нормативний документ системи технічного захисту інформації)
8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. [Чинний від

28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)

9. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
10. НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. [Чинний від 20.12.2000] – К.: ДСТСЗІ СБУ, 2000-No60 (Нормативний документ системи технічного захисту інформації)
11. ДСТУ 3396.1-96 Захист інформації. Технічний захист. інформації. Порядок проведення робіт
12. Work.ua [Електронний ресурс] Режим доступу до ресурсу: https://work.ua

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	4	
6	А4	Спеціальна частина	38	
7	А4	Економічний розділ	13	
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	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Петраш_ЄІ_125_19ск_1_ПЗ.docx
2. Петраш_ЄІ_125_19ск_1_ПЗ.pdf
3. Петраш_ЄІ_125_19ск_1_ПЗ.pdf.p7s
4. Петраш_ЄІ_125_19ск_1_Презентація.pptx

ДОДАТОК В. Відгук керівника економічного розділу

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

Керівник розділу _____ доц. Пілова Д.П.
(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19ск-1

Петраша Євгенія Ігоровича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "FixUp"

Кваліфікаційна робота виконана у відповідності до завдання в повному обсязі і представлена пояснювальною запискою та презентацією.

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 72 сторінках з додатками.

Об'єкт дослідження – інформаційно-телекомунікаційна система ТОВ «FixUp».

Мета кваліфікаційної роботи – підвищення рівня захисту інформації в інформаційно-телекомунікаційній системі ТОВ «FixUp».

Тема безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека».

Актуальність обраної теми обумовлена підвищенням вимог до рівня інформаційної безпеки в інформаційно-телекомунікаційній системі ТОВ «FixUp» в сучасних умовах.

Для досягнення поставленої мети детально проаналізовано стан питання та існуюча нормативно-правова база і сформульовано перелік задач, що потребують свого вирішення в кваліфікаційній роботі.

В спеціальній частині кваліфікаційної роботи проведено обстеження об'єкта інформаційної діяльності, фізичного середовища, обчислювальної системи та інформаційного середовища. Виявлено актуальні для підприємства загрози інформаційній безпеці, побудовані модель порушника і модель загроз та запропоновано методи і засоби протидії.

В економічному розділі визначено економічну доцільність запропонованих рекомендацій та загальний економічний ефект від їх впровадження.

Оформлення матеріалів пояснювальної записки до кваліфікаційної роботи виконано з дотриманням нормативних вимог.

Протягом дипломування Пєтраш Є.І. проявив себе організованим, достатньо підготовленим та обізнаним фахівцем з питань кібербезпеки, здатним самостійно та системно проводити дослідження і приймати обґрунтовані рішення, має певний досвід практичної роботи.

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

В цілому кваліфікаційна робота заслуговує оцінки «відмінно» (92 бали), а її автор Пєтраш Є.І. присвоєння відповідної кваліфікації.

Керівник кваліфікаційної роботи,
к.т.н., доцент _____ О.О. Сафаров

Керівник спец. розділу,
старший викладач _____ С.І. Войцех