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 *Бакуна Дениса Вікторовича*
академічної групи *125-18-2*
спеціальності *125 Кібербезпека*
спеціалізації[1]
за освітньо-професійною програмою *Кібербезпека*

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

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст.викл. Кручінін О.В.		Добре	
економічний	к.е.н., доц. Пілова Д.П.	60	Задовільно	

Рецензент				

Нормоконтролер	ст.викл. Тимофєєв Д.С.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Бакуну Денису Віктровичу* **академічної групи** *125-18-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*
спеціалізації _____
за освітньо-професійною програмою *Кібербезпека*

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

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

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Надання загальної відомості про підприємство. Обстеження ІТС та постановка задачі	15.05.2022
Розділ 2	Розробка моделі загроз та моделі порушника. Вибір профілю захищеності. Впровадження проектних рішень для захисту інформації	25.05.2022
Розділ 3	Економічна доцільність впровадження проектних рішень	06.06.2022

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____
Дата подання до екзаменаційної комісії: 16.06.2022р.
Прийнято до виконання

_____ Бакун Д.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 77с., 7 рис., 23 табл., 6 додатка, 24 джерела.

Об’єкт розробки: інформаційно-телекомунікаційна система ТОВ «Soft Solution»

Предмет розробки: комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «Soft Solution»

Мета роботи: досягнення необхідного рівня захищеності інформації, яка обробляється в ІТС

Методи розробки: спостереження, порівняння, аналіз, опис.

Перший розділ надає загальний опис підприємства, його організаційну структуру, було проведено обстеження ІТС, а також проаналізовано обчислювальну систему підприємства.

В спеціальній частині було розроблено модель порушника, модель загроз, було обрано профіль захищеності та впровадження проектних рішень для досягнення необхідного рівня захищеності інформації в ІТС.

В економічному розділі було розраховано капітальні та поточні витрати, проведено оцінку можливого збитку та виконано аналіз економічної доцільності запропонованих рішень.

Практичне значення кваліфікаційної роботи полягає у створені комплексу захисту інформації для ТОВ «Soft Solution»

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНОФРМАЦІЇ, ЗАХИСТ ІНОФРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, ПРОФІЛЬ ЗАХИЩЕНОСТІ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ.

ABSTRACT

Explanatory note: 77 pages, 7 figures, 23 tables, 6 appendices, 24 sources.

Object of development: information and telecommunication system of Soft Solution LLC

Subject of development: complex information protection system of information and telecommunication system of LLC "Soft Solution"

Purpose: to achieve the required level of security of information processed in the ITS

Development methods: observation, comparison, analysis, description.

The first section provides a general description of the enterprise, its organizational structure, ITS survey was conducted, as well as analyzed the computer system of the enterprise.

In the special part the model of the violator, the model of threats will be developed, the profile of protection and implementation of design decisions for achievement of necessary level of protection of the information in ITS has been chosen.

In the economic section, capital and current costs were calculated, an assessment of possible damage and an analysis of the economic feasibility of the proposed solutions.

The practical significance of the qualification work is to create a complex of information protection for LLC "Soft Solution"

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, INFORMATION PROTECTION, OBJECT OF INFORMATION ACTIVITY, INFRINGEMENT MODEL, THREAT MODEL, PROFILE PROTECTION, PROFILE PROTECTION, ECONIMIC EXPEDIENCY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ОІД – об’єкт інформаційної діяльності

КЗ – контрольована зона

ПКП – приймально-контрольний прилад

КСЗІ – комплексна система захисту інформації

НД ТЗІ – нормативний документ технічного захисту інформації

ІТС – інформаційно-телекомунікаційна система

ІзОД – інформація з обмеженим доступом

АС – автоматизована система

ТЗ – технічне завдання

ПЗ – програмне забезпечення

ЗУ – закон України

ТЗІ – технічний захист інформації

ОС – обчислювальна система

ЕП – електронний підпис

ЗМІСТ

ВСТУП

В сучасному соціумі інформація є одним з найважливіших активів, кожного дня окремі і люди і цілі підприємства та установи створюють величезну кількість конфіденційної інформації.

На хвилі підвищення кількості важливої і конфіденційної інформації підвищилась і кількість спроб вкрасти або знищити важливу інформацію.

Більшість людей і підприємств малого бізнесу нехтуються правилами безпеки, через це популярність різного роду політик безпеки неупинно росте.

Сьогодні кожен може стати жертвою хакерів, на великі підприємства проводяться масові атаки різними методами, наприклад за допомогою хакерських атак на сервери, фізичні спроби проникнення у інфраструктуру компаніях, викрадення носіїв інформації тощо.

У таких умовах сучасне та прогресивне підприємство котре хоче захистити себе від різного роду небезпек повинно міркувати про безпеку у самих різних напрямках – хакінг, вразливості ПЗ, недостатньо кваліфіковані робітники, які своїми діями можуть привести до величезних збитків. Також не можна забувати про старі загрози, такі як катастрофи, збої обладнання, тощо.

Щоб уникнути завеликих збитків компанії використовують комплексні системи захисту інформації — сукупність організаційних і інженерних заходів, програмно- апаратних засобів, які забезпечують захист інформації в ІТС. Адже гарантований захист інформації, вдосконалення впроваджених технологій, постійний аналіз існуючих системи безпеки і сучасних технологічних змін забезпечує розвиток компаній та закріплення їх позицій на світовому ринку.

1.СТАН ПИТАННЯ. ПОТСАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство ТОВ «Soft Solution»

Підприємство «SoftSolutions» підприємство в сфері інформаційних і телекомунікаційних технологій, основна діяльність якого полягає в створенні веб-сайтів «під ключ», охоплюючи всі етапи життєвого циклу розробки програмного забезпечення, починаючи від концептуального проектування і закінчуючи бета-тестуванням і аналітикою.

Компанія працює на ринку надання послуг зі створення програмного забезпечення з січня 2019 року і орендує офіс на третьому поверсі в бізнес-центрі за адресою м.Дніпро, вул. Воскресенська, 20.

Таблиця 1.1 - Штат підприємства «SoftSolutions»

№	Посада	Кількість працівників на посаді	Стаж на підприємстві
1	Директор	1	3
2	HR-менеджер	1	1
3	Тімлід	1	2
4	Розробник	4	1
5	Сайлз-менеджер	1	1
6	Офіс-менеджер	1	2

В обов’язки директора входить повне вирішення всіх податкових і економічних питань компанії, взаємодія з сайлз-менеджером і тімлідами, часткова взаємодія з клієнтами при необхідності. Окрім цього, директор виконує функціонал бухгалтера.

HR-менеджер займаються підбором та прийомом на роботу персоналу.

Тімліди відповідають за вірну роботу команд розробників, включаючи строки проектів, правки, тощо.

Сайлз-менеджер менеджер відповідає за пошук клієнтів і всі взаємодії з ними. Деякі взаємодії проходять при участі тімлідів.

Офіс-менеджер — широкопрофільний співробітник, який відповідає за доставку продуктів в офіс, замовлення і доставку меблів, техніки, тощо. Окрім цього виконує обов'язки локального системного адміністратора.

Розробники – безпосередньо створюють веб-сайти, роблять їх тестування , проводять аналітику тощо.

Організаційна структура підприємства зображена на рисунку 1.1

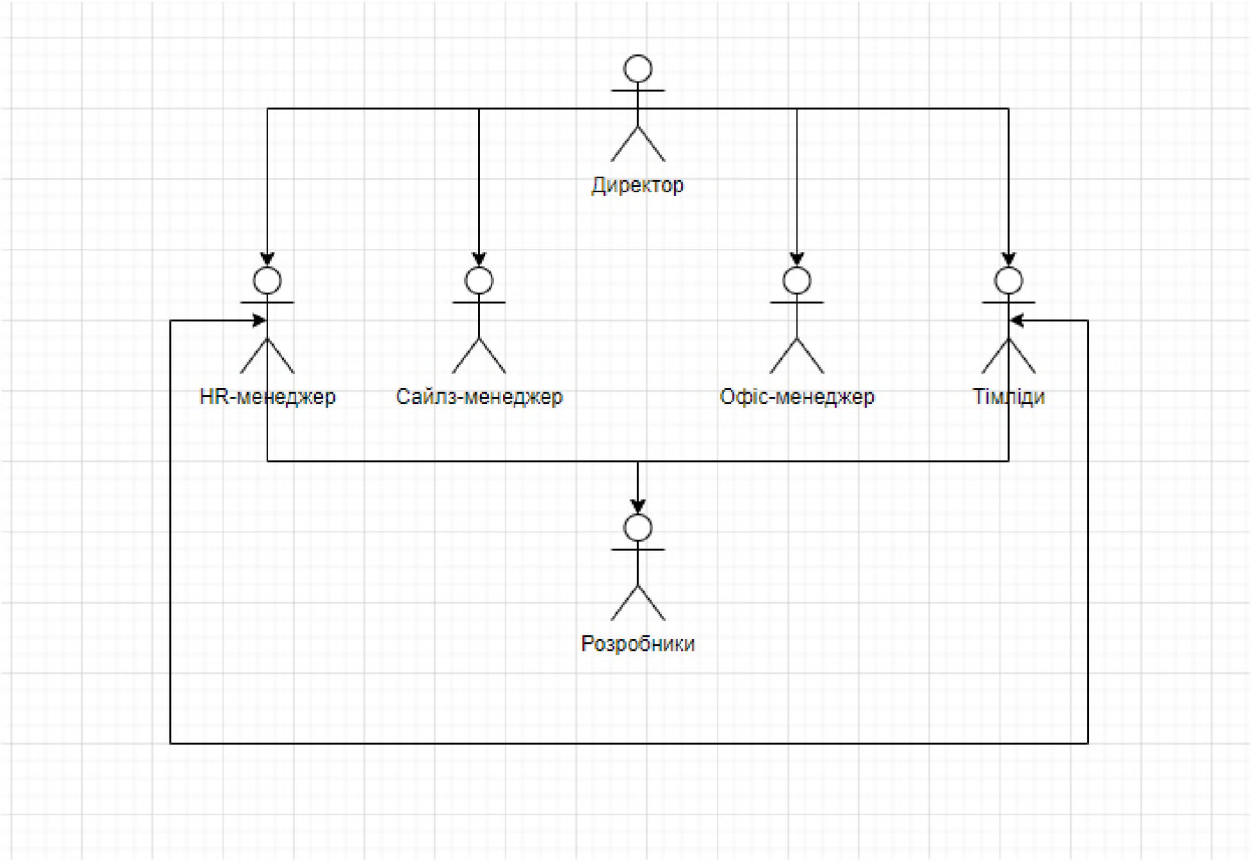

Рисунок 1.1 — Організаційна структура підприємства

1.2 Обгрунтування необхідності створення КСЗІ

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» розглядається забезпечення захисту інформації в системі. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Також згідно з Законом України «Про інформацію», де описані види інформації і визначено, що інформації про фізичну особу та інформації з обмеженим доступом повинен надаватися обов'язковий захист, а така інформація циркулює на підприємстві, тому керівництвом було вирішено створити комплексну систему захисту інформації

Згідно з НД ТЗІ 3.7-003-05 було встановлено порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційної системі.

1.3 Обстеження середовища функціонування

Ситуаційний план

Приміщення компанії, є об'єктом інформаційної діяльності (ОІД). Об'єкт інформаційної діяльності розташований на 3 поверсі бізнес-центру за адресою м. Дніпро, вул. Вознесенська, 20.

Контрольована зона (далі КЗ) обмежена зовнішніми стінами будівлі з усіх сторін, знизу - підлогою, під якою розташоване підвальне приміщення, фітнес-центр, студія краси та інші офіси та магазини, а зверху - стелею.

Стіни будинку зроблені із цеглини з залізобетонним перекриттям та утеплювача.

Територія позаду будинку огороджена невисоким парканом із шлагбаумом, асфальтована, наявні ділянки із кущами, є місця для паркування авто, які вказані на рис.1.2

Рисунок 1.2 —Ситуаційний план

До даного будинку підключені наступні комунікації:

- електропостачання - від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля кімнати охорони;
- каналізація та водопостачання - підключені до міських магістралей та заходять до підвального приміщення даного будинку;
- система опалення - централізована, труби стояку йдуть з 0 поверху до приміщень на 1 поверсі, а потім до офісів вище.

Схема заземлення зображена на Ситуаційному плані рис.1.2 Заземлення іде від трансформаторної підстанції до розподільного щита. Безпосередньо в офісі заземлення немає.

КЗ розташована в офісному будинку, комунікації, а саме труби системи опалення, лінія електропостачання та лінія комп'ютерної мережі виходять за межі КЗ. Інформація про навколишні будинки та споруди приведена у табл.1.2

Таблиця 1.2 - Характеристика будівель та споруд.

	Найменування	К-ть поверхів	Адреса	Відстань до ОІД, м
	Житловий будинок	4	Мечнікова, 1	28
	Адміністративна будівля	4	Мечнікова, 6	21
	Трансформаторна підстанція ТП-102	1	Біля адміністративної будівлі №4	17
	Адміністративна будівля	5	Проспект Дмитра Яворницького, 75а	22
	Житловий будинок	5	Воскресенська, 18	20
	Ремонтована будівля	5	Воскресенська, 18	7
	Адміністративна будівля	2	Воскресенська, 16	12

Таблиця 1.3 – Дані про вулиці відносно ОІД

Назва	Опис
вул. Мечнікова	Відносно ОІД вулиця розташована на заході. Автомобільний трафік становить 80 - 120 машин на годину.

Продовження таблиці 1.3 - Дані про вулиці відносно ОІД

Назва	Опис
вул. Воскресенська	Відносно ОІД вулиця розташована на сході. Автомобільний трафік становить 180 - 230 машин на годину.
вул. Челюскіна	Відносно ОІД вулиця розташована на півдні. Автомобільний трафік становить 70 - 100 машин на годину.

- площа ОІД: 68м^2;
- висота стелі — 2.89м. Поверх — 3-ій;
- стеля (матеріал бетон, товщина — 0,5м.), підлога (матеріал бетон+металеві конструкції+деревина, товщина 1.5м.), стіни (матеріал цегла+гіпсокартон, товщина 0,6м);
- вікно (кількість — 6 шт, матеріал пластик (ПВХ)), розміри: 2.5м х 1,1м. Вікна виходять на двір. Сектор прямої видимості — це адміністративні будівлі та вулиці Воскресенська та Мечнікова;
- лінія електропостачання іде до поверхового щитка у підвалі, а звідти — до основного електрощита;
- сигналізація підключена до ПКП біля входу в будівлю;
- лінія комп'ютерної мережі — оптичний кабель: Wi-Fi роутер підключений до мережевого обладнання провайдеру;
- система опалення — горизонтальна.

Генеральний план

Рисунок 1.3— Генеральний план

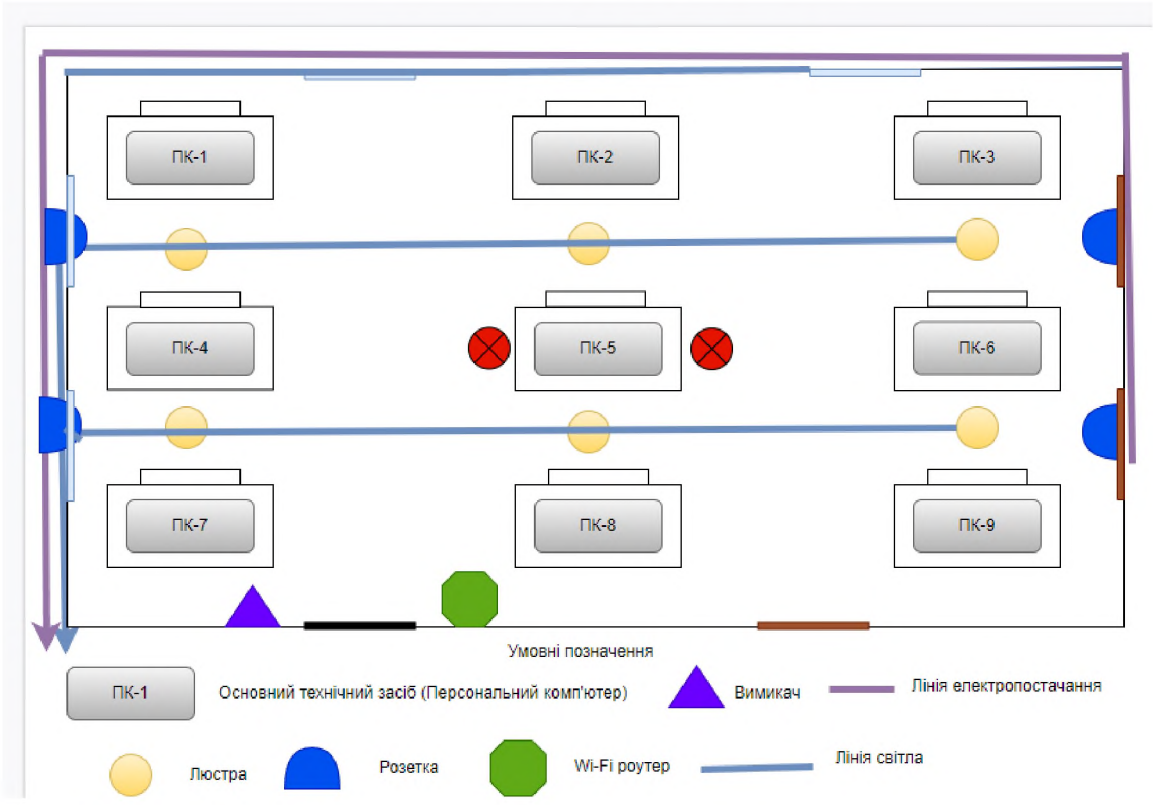

Рисунок 1.4 —Схема систем електропостачання та освітлення

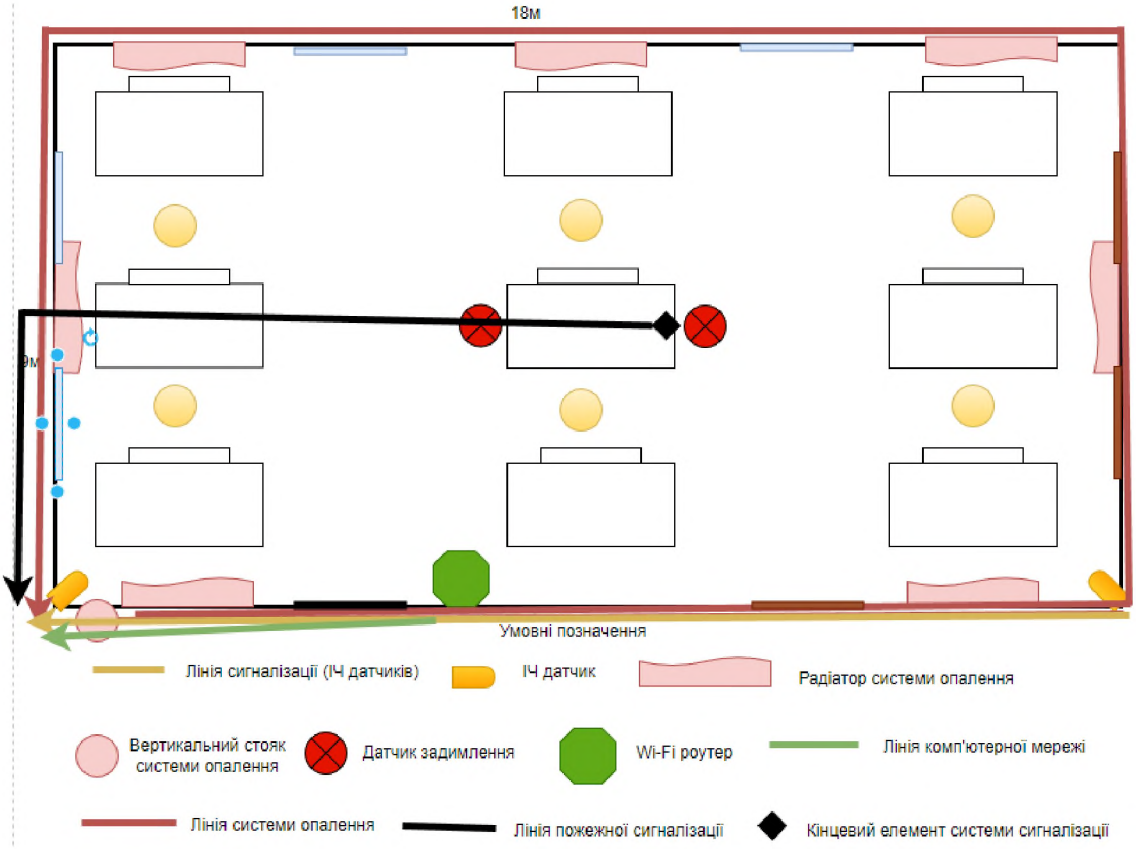

Рисунок 1.5 —Схеми ліній комп'ютерної мережі, системи сигналізації та системи опалення

Режим КЗ забезпечується таким чином:

- у робочий час забезпечується співробітниками саме нашого підприємства. Тобто якщо прийшов відвідувач ми його зустрічаємо, проводжуємо до офісу, и потім так саме ведемо до виходу ;
- у неробочий час забезпечується силами охорони з використанням засобів відеоспостереження, решіток на вікнах, вхідними металопластиковими дверями, які закриваються на ключ. Також застосовується автономна сигналізація приміщень всього будинку, яка підключена до приймально-контрольного пристрою, який знаходяться біля чергових ПКП. Чергові мають тривожну кнопку, яка застосовується для виклику наряду представників охоронної організації. Сигналізація КЗ входить до составу системи

сигналізації усієї будівлі.

Комунікаційні системи КЗ вказані у табл.1.4. Вони також відображені на генеральному плані (Рисунки 1.3-1.5).

Таблиця 1.4 – Характеристики технічних систем

Вид системи	Характеристика
Система електропостачання	від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля входу до приміщення.
Система опалення	Централізована, труби стояку йдуть з 0 поверху до КЗ, а потім до офісів вище.
Система каналізації	Підключені до міських магістралей та заходять до підвального приміщення даного будинку
Система водопостачання	
Телефонна лінія та Інтернет	Підключені до Інтернет-провайдера «Укртелеком» . Кабель локальної мережі являє собою неекранована вита пара
Система сигналізації	Складається з інфрачервоних датчиків, датчиків задимлення, системи відеоспостереження. Керується службою безпеки власника будівлі.

Перелік основних та допоміжних технічних засобів приведено в ДОДАТКУ Ґ.

1.4 Обчислювальна система

Опис програмного забезпечення та його локалізація на комп'ютерах підприємства «SoftSolutions»

Таблиця 1.5 - Програмне забезпечення в інформаційній системі підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	На яких ПК встановлено
1	Windows	Системне	Commercial	Операційна система	Безстроковий	PC1..PC9

Продовження таблиці 1.5 - Програмне забезпечення в інформаційній системі підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	На яких ПК встановлено
2	Microsoft Word 2020	Прикладне	Commercial	Редактор тексту	Безстроковий	PC1..PC9
3	Microsoft Excel 2020	Прикладне	Commercial	Редактор таблиць	Безстроковий	PC1..PC9
4	Adobe Photoshop 2020	Прикладне	Commercial	Графічний редактор	Безстроковий	PC3..PC7
5	Unity	Прикладне	Commercial	Ігровий двигун	Безстроковий	PC3..PC7
6	Visual Studio 2022	Прикладне	Commercial	Інтегроване середовище розробки	Безстроковий	PC3..PC7
7	PyCharm 2022	Прикладне	Commercial	Інтегроване середовище розробки	Безстроковий	PC3..PC7
8	1С Бухгалтерія (8.3)	Прикладне	Commercial	Бухгалтерська програма для автоматизованого обліку	Безстроковий	PC1,PC2 PC8,PC9
9	iFin 1.2	Прикладне	Commercial	Програма для звітності	Безстроковий	PC1,PC2, PC8,PC9
10	Avira free antivirus 13.1	Прикладне	Commercial	Антивірус	Безстроковий	PC1..PC9

Продовження таблиці 1.5 - Програмне забезпечення в інформаційній системі підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Темрін дії	На яких ПК встановлено
11	Zoom	Прикладне	Commercial	Програма онлайн зв'язку	Безстроковий	PC1,PC2, PC8,PC9

Система складається з 9 персональних комп'ютерів, 2 принтерів, 1 комутатора, 1 роутера.

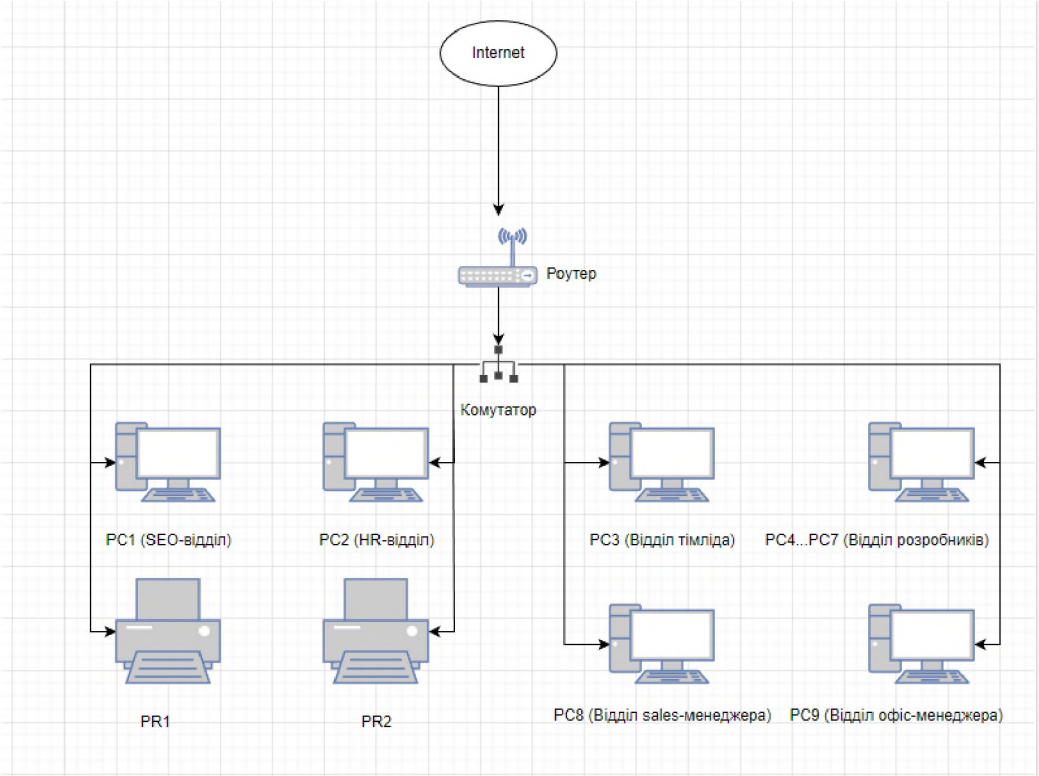

Рисунок 1.6 — Структурна схема обчислювальної системи підприємства

Кабель інтернету проведений до офісу оптоволоконним кабелем. Кручена пара підключена до маршрутизатора (локальна мережа (LAN)), до якого прямим

підключенням під'єднаний до комутатора. PC1...PC9 з'єднуються прямим підключенням з комутатором (Кручена пара). Іпринтери PR 1, PR 2 під'єднані до комутатора прямим підключенням. Принтери підключені локально до PC1, PC2, відповідно. PC1 комп'ютер SEO-відділу, PC2 комп'ютер HR-відділу, PC3 комп'ютер тімліду, P C 4 … P C 7 комп'ютери розробників . PC8 sales-менеджера, PC9 комп'ютер офіс-менеджера.

Інформація, що циркулює в ІТС це персональна інформація про клієнтів та працівників підприємства, фінансова та бухгалтерська звітність, та інформація

про роботу компанії (продукти, проекти...), відкрита інформація (реклама). Класифікація цієї інформації наведена в таблиці 1.6.

Характеристика складу ОС приведено у ДОДАТКУ Д.

Таблиця 1.6 — Класифікація інформації, яка циркулює на ІТС

№	Вид інформації	Режим доступу	Правовий режим	Вид представ-лення в ІТС	Вимоги до захисту		
					К	Ц	Д
1	Інформація про клієнтів (персональна)	ІзОД	Конфіден-ційна інформація	Паперовий Електрон-ний	3	2	3
2	Інформація про працівників (персональна)	ІзОД	Конфіден-ційна інформація	Паперовий Електрон-ний	4	4	4
3	Продукти роботи підприємства	ІзОД	Конфіден-ційна інформація	Паперовий Електрон-ний	4	5	4
4	Бухгалтерська звітність, договори	ІзОД	Конфіден-ційна інформація	Паперовий Електрон-ний	4	5	4

Продовження таблиці 1.6 - Класифікація інформації, яка циркулює на ІТС

№	Вид інформації	Режим доступу	Правовий режим	Вид представ-лення в ІТС	К	Ц	Д
5	Фінансова звітність (банківські рахунки, виручка)	ІзОД	Службова інформація	Електрон-ний	3	4	4
6	Реклама	Відкрита інформа-ція	Відкрита інформація	Електрон-ний	1	2	3

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 е 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 зазнае незначних збитків у разі втрати доступності інформації;

– Д3 - рівень доступності інформації, при якому організація зазнае 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.

Всі ресурси обробляються працівниками підприємства - 1 sales-менеджер, 1 офіс-менеджер, 4 розробника, 1 тімлід, 1 HR, 1 SEO.

Вся текстова документація зберігається у сейфі SEO, до якого доступ має тільки SEO. Електронна інформація записується та зберігається на жорстких дисках 4тб, які лежать на 3 різних полках та зачиняються на ключ . Резервування всієї інформації виконується кожен день на ці диски, а також в хмарне сховище Terabox.

Інформація про клієнтів (персональна) менеджер домовляється з клієнтом про проект (замовлення), після чого вносить його в систему замовлень (CRM, ERP, Printoffice24) та передає інформацію до SEO, вона може бути роздрукована. Зберігається на полицях в закритому сейфі.

Інформація про працівників (персональна) обробляється SEO,офіс-менеджером та HR-менеджером може бути роздрукована. Зберігається на полицях в закритому сейфі.

Продукти роботи підприємства - вхідні та вихідні документи (правки, розрахунки, аналітика...), матеріали про проекти, дизайнерські рішення та розробки - при роботі над проектом, тімлід та розробники постійно зберігають результати на певному етапі і передають на перевірку офіс-менеджеру та SEO. Після внесення всіх правок, готовий проект передається замовнику.

Реклама —підприємство активно рекламує свої послуги в соціальних мережах та на просторах інтернету. Цим займається sales-менеджер.

Клієнти самі звертаються до компанії (реклама) або менеджери самі знаходять потенційних клієнтів (спеціальні платформи, аналіз та опрацювання нових компаній та підприємств); клієнт звертається до компанії з своїм проектом/ідеєю до менеджера компанії з яким ведуться переговори з приводу проекту (мета, ціль, розвиток, потенціал та прибуток) та його можливостей. Клієнта вносять в програми (CRM, ERP, Printoffice24). Всю допоміжну інформацію по проекту та свої персональні данні клієнти пересилають на корпоративну пошту. Після ознайомленням з проектом SEO, його приймає в роботу тімлід, розробляється план робіт та визначаються терміни (період вивчення ринку, період створення моделі проекту, корективи, графічна робота, корективи, побудова фінальної моделі та виведення результатів на ринок). З клієнтом також зв'язуються SEO та sales-менеджер та створюють договір, після якого клієнт вносить повну оплату проекту (під час проекту можуть виникати додаткові витрати, про які інформують клієнтів). Менеджери працюють над проектом, використовуючи певне ПЗ.При кожному етапі відтворення проекту, SEO та тімлід вносять корективи. Для конкретного проекту створюють свої терміни для кожного етапу, під час яких з клієнтом підтримується зв'язок (інформується по виконанню певного етапу та його результатів) через sales-менеджера (Zoom). Клієнти також можуть вносити свої корективи. Для коректівів проекту на кожній стадії він може друкуватися принтерами, які локально

підключені до кожного SEO та HR. Після завершення проекту SEO тримає зв'язок із клієнтом для підтвердження результатів та у ролі допомоги для правильного просування проекту у ринок.

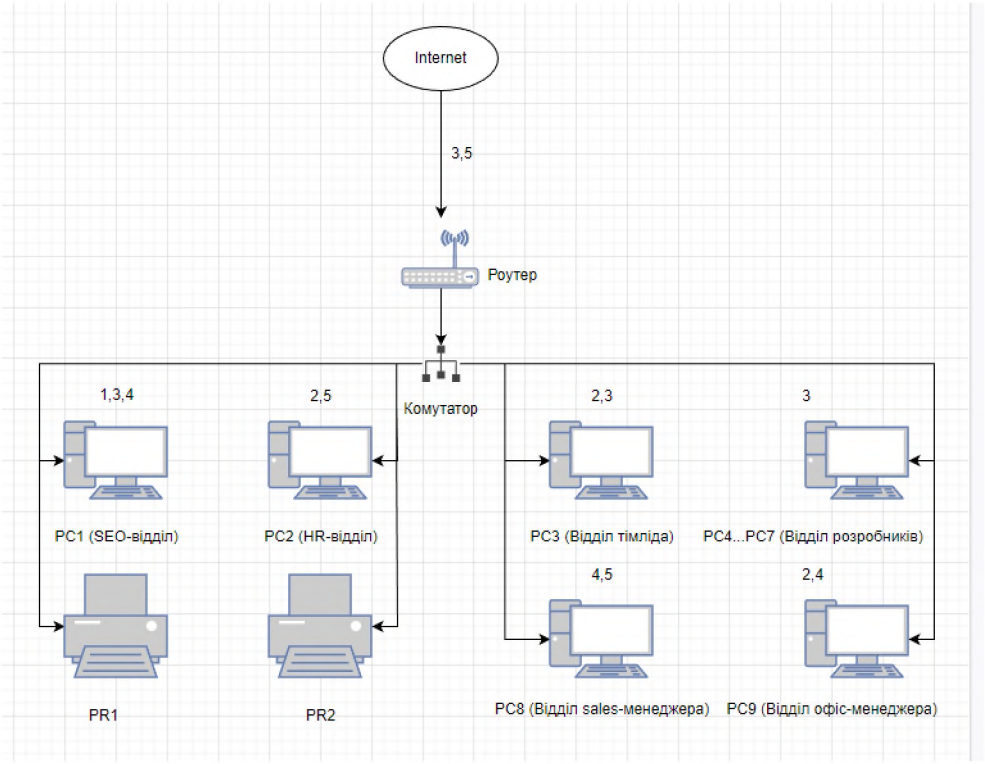

Рисунок 1.7 — Схема інформаційних потоків

Інформаційні потоки:

1. Обробка інформації про клієнтів
2. Обробка інформація про працівників
3. Обробка продуктів роботи підприємства
4. Обробка договорів
5. Обробка рекламних даних

Таблиця 1.7 – Середовище користувачів

№	Посада	Роль в системі	Кількість працівників на посаді	Рівень кваліфікації	Стаж на підприємстві
1	SEO	Адміністратор	1	Високий	3
2	HR-менеджер	Користувач	1	Середній	1
3	Тімлід	Користувач	1	Високий	2
4	Розробник	Користувач	4	Середній, Високий	1
5	Сайлз-менеджер	Користувач	1	Високий	2
6	Офіс-менеджер	Адміністратор	1	Високий	2

Таблиця 1.8 — Матриця розмежувань доступу

Користувач		SEO	Sales-менеджер	Офіс-менеджер	HR	Тімлід	Розробник
Інформація	Інформація про клієнтів	R, W, M, D, C, T	R, W, C, T, D	R, W, C, T, M, D	-	R	R

Продовження таблиці 1.8 - Матриця розмежувань доступу

	Інформація про працівників	R, W, M, D, C, T	-	R, W, C, T, M, D	R, W, M, D, C, T	R, M	R
	Продукти роботи підприємства	R, W, M, D, C, T	R	R	-	W, R, C, T, D, M,	R, W, M, C, T
	Обробка договорів	R, W, M, D C, T	R, M,C	R, M, W, D	R,W,M,C	-	-
	Реклама	R, W, M, D, C, T	R, W, C, T, D	R, M, D, C	R, W, C	-	-
Повноваження встановлювати ПЗ		+	-	+	-	+	+
Ресурси		PC1	PC8	PC9	PC2	PC3	PC4…PC7

R — Читання;

W — запис;

M — модифікація;

D — видалення;

C — створення нових файлів;

T — перенесення.

1.5 Постановка задачі

Так як на підприємстві ТОВ «SoftSolutions» обробляється інформація з обмеженим доступом, було прийнято рішення про створення КСЗІ, а для цього необхідно виконати:

- проаналізувати модель загроз;
- проаналізувати модель порушника;
- обрати профіль захищеності;
- запропонувати організаційні та програмно-апаратні засоби захисту інформації для реалізації послуг безпеки профіля захищеності

1.5 Висновки до першої частини

Розглянуто актуальність теми маркетингу і технологій, а також захисту інформації з розвитком технологій.

Розглянуті загальні відомості про підприємство «SoftSolutions», виконано обстеження ситуаційного та генерального плану, обчислювальної та інформаційної системи, організаційної структури підприємства. Об ґрунтовано необхідність створення КСЗІ на підприємстві «SoftSolutions» та виконано постановку задачі.

2.СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель порушника

До зовнішніх порушників відносяться особи, які знаходяться за поза підприємством. Це можуть бути конкуруючі підприємства та крадії або персонал з обслуговування приміщення, особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД, наприклад, прибиральники, електрики тощо.

До внутрішніх порушників відносяться особи, що мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних, користувачі АС, персонал, який безпосередньо пов'язаний із забезпеченням функціонування ІТС.

В таблиці 2.1 наведені категорії порушників, що використовуються при створенні моделі. Модель порушника наведена зі специфікаціями за різними показниками:

- за мотивами здійснення порушень;
- за рівнем кваліфікації та обізнаності щодо ІТС;
- за показником можливостей використання засобів ІТС для реалізації загроз;
- за часом та місцем дії.

Профіль порушника визначає сукупність цих характеристик.

Таблиця 2.1

Рейтингова оцінка	Опис
1	незначний
2	нижчий за середній
3	середній
4	вищий за середній
5	значний

Спираючись на отримані результати аналізу характеристик обробляємої інформації, категорій порушників, що мають потенційну можливість порушення конфіденційності та цілісності інформації, вважаються найбільш

небезпечними, доступності - менш небезпечними, а спостережності - найменш небезпечними.

Таблиця 2.2 - Категорії порушнишв. Внутрішні по відношенню до ІТС.

Позначення	Визначення категорії	Рівень загроз
ПВО	Директор	4
ПВ1	HR-менеджер	1
ПВ2	Розробник	3
ПВ3	Тімліди	3
ПВ4	Офіс-менеджер	5
ПВ5	Сайл-менеджер	2

Таблиця 2.3 - Категорії порушнишв. Зовнішнішні по відношенню до ІТС

Позначення	Визначення категорії	Рівень загроз
П30	Агенти та конкуренти	4
П31	Вахтери, сантехнік, електрик, прибиральниці	3

Таблиця 2.4 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність(ненавмисне порушення	1

М2	Самоствердження	2
М3	Корисний інтерес	4

Таблиця 2.5 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Рівень кваліфікації	Рівень загроз
К1	Володіє низьким рівнем знань; може використовувати ІС на рівні користувача	1
К2	Володіє середнім рівнем знань, має впевнені навики використання ІС та їх обслуговування	3
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІС	5

Таблиця 2.6 - Специфікація моделі порушника за показником можливостей

Позначення	Характеристика можливостей порушника	Рівень загроз
30	Може підслуховувати розмови у приміщеннях	1

	та читати документи на чужих робочих місцях	

Продовження таблиці 2.6 - Специфікація моделі порушника за показником можливостей

Позначення	Характеристика можливостей порушника	Рівень загроз
31	Використовує пасивні технічні засоби перехвату без можливості модифікації інформації та компонентів ІС.	2
32	Використовує лише штатні засоби та недоліки системи захисту інформації для її подолання (несанкціоновані дії з використанням дозволених та доступних засобів), а також компактні носії інформації, які можливо приховано пронести повз пост охорони офісу.	4
33	Використовує просунуті технічні	5

	засоби активного впливу з метою модифікації інформації та компонентів ІС, дезорганізації систем обробки інформації.	

Таблиця 2.7 - Специфікація моделі порушника за часом дії

Позначення	Час дії	Рівень загроз
Ч1	Під час бездіяльності компонентів системи (неробочий час)	3
Ч2	Під час функціонування системи	5
ЧЗ	Під час обслуговування компонентів, їх ремонту	4

Таблиця 2.8 - Специфікація моделі порушника за місцем дії

Позначення	Час дії	Рівень загроз
Д1	Ззовні приміщень офісу; всередині приміщень, але без доступу до технічних засобів ІТС.	2
Д2	З робочих місць	3

	користувачів ІТС.	

Продовження таблиці 2.8 - Специфікація моделі порушника за місцем дії

Позначення	Час дії	Рівень загроз
Д3	З доступом у зону зберігання баз даних, архівів, тощо	4

Профілі порушників всіх категорій наведено у таблиці 2.14, у колонці «Сума загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.9 - Профілі порушників

Позначення	Визначення категорії	Характер дій порушника					Ефективний рівень загроз
		Мотив порушення	Кваліфікація	Можливості	Час дії	Місце Дії	
1	Директор	М1-М3	К3	З0-З2	Ч1-Ч3	Д1-Д3	26
2	HR-менеджер	М1-М2	К2	З0,З2	Ч1-Ч2	Д1-Д2	18
3	Розробник	М1-М3	К3	З0-З2	Ч1-Ч2	Д1-Д2	24

Продовження таблиці 2.9 - Профілі порушників

4	Тімлід	М1-М3	К3	30-32	Ч1-Ч2	Д1-Д3	25
5	Сайл-менеджер	М1-М2	К2	30-32	Ч1-Ч2	Д1-Д2	19
6	Офіс-менеджер	М1-М3	К3	30-32	Ч1-Ч3	Д1-Д3	27
7	Агенти та конкуренти	М3	К3	30-33	Ч2	Д1	25
8	Вахтери,сантехнік, електрик, прибиральниці	М1-М2	К1	30	Ч1-Ч3	Д1-Д3	16

Дослідженні в роботі категорії порушників безпеки інформації, засвідчують, що теоритично найбільш велику небезпеку будуть становити:

Офіс-менеджер(він же системний адмін) і директор, оскільки вони мають безпосередній доступ до системи ІТС та працюють з її компонентами, та мають достатню компетенцію і мотиви.

2.2 Модель загроз

За результатами впливу на інформацію та систему її обробки, загрози поділяються на чотири класи:

Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.

Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

Порушення доступності інформації (Д) - часткова або повна втрата працездатності

системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

Втрата спостережності (керованості системою) (С) - порушення процедур ідентифікації та автентифікації адміністраторів або процесів і надання їм повноважень, втрата контролю за їх діяльністю, можливість відмови від отримання або пересилання повідомлень.

Потенційно загрози можуть завдати шкоди обробляємої інформації, працівникам, кліентам, технічним засобам і процесам. Загрози також можна поділити на:

навмисні (Н);

випадкові (В);

природні (П).

Потрібно ідентифікувати як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

Таблиця 2.10 – Модель загроз

№ з/п	Вид загрози	Вразливість	Можливий механізм реалізації	Джерело загрози	Наслідки	Ймовірність
1	Катастрофа		Пожежа, повінь, землетрус, техногенні аварії	Зовнішнє середовище	Ц, Д	Середня
2	Хакінг	Недоліки механізмів автентифікації та авторизації	Виконання несанкціонованих дій на пристрої коритсувача	Зовнішній порушник	К, Ц	Середня

Продовження таблиці 2.10 – Модель загроз

№ з/п	Вид загрози	Вразливість	Можливий механізм реалізації	Джерело загрози	Наслідки	Ймовірність
3	Крадіжка носія з ІзОД	Недбалість самих працівників або недбале зберігання носія (під час перерви на обід не зачинили двері до офісу)	Проникнення до офісу у не робочий час або під час огляду кандидата на роботу офісу	Зовнішній або внутрішній порушник	К, Д	Середня
4	Вірусне зараження	Не оновлене ПО, не має правил підключання незареєстрованих накопичувачів	Скачування не ліцензійних програм, помилки під час конфігурації, використання та	Зовнішній або внутрішній порушник	Ц,Д	Висока

			підключення засобів захисті			

Продовження таблиці 2.10 – Модель загроз

№ з/п	Вид загрози	Вразливість	Можливий механізм реалізації	Джерело загрози	Наслідки	Ймовірність
5	Незаконне отримання конфіденційних даних	Недостатньо навчений персонал	Соціальна інженерія	Зовнішній порушник	К	Низька
6	Відмова в обслуговуванні		Виведення з ладу/пошкодження/перехід в нештатний режим роботи обчислювальної системи	Зовнішній або внутрішній порушник	Д,Ц	Низька
7	Зловживання можлив	Неправильний розподіл прав, відсутній	Порушення правил, встановлен	Внутрішній порушник	К,Ц,Д,С	Середня

	остями адміністраторів	журнал подій	их ролями користувачів			

Продовження таблиці 2.10 – Модель загроз

№ з/п	Вид загрози	Вразливість	Можливий механізм реалізації	Джерело загрози	Наслідки	Ймовірність
8	Використання системи в корисних цілях	Порушення правил розмежування доступу	Копіювання коду проекту	Внутрішній порушник	К,Ц,С	Висока
9	Вивід з ладу обладнання	Збої електроживлення	Перепад набруги	Система електропостачання	Д,Ц	Висока
10	Перехоплення інформації(візуальне)	Відкриті вікна, не зачинені двері	Підглядування за роботою через недбалість працівників	Зовнішній порушник	К	Середня
11	Недолік охоронної або пожежн	Погане технічне обладнання або	Не працюють датчики руху або	Технічне обладнання	Д,К,Ц	Низька

	ої	неправильно встановлена система сигналізації	датчики диму			

Якщо ідентифіковані загрози використають відповідні до них вразливості інформаційної безпеки, негативними наслідками для підприємства стануть порушення конфіденційності інформації, її цілісність та доступність. Подібні інциденти негативно вплинуть на ресурси підприємства та на всю роботу.

2.3 Профіль захищеності

Проаналізувавши основні характеристики ІТС об'єкту кваліфікаційної роботи, та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-004-99

«Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

АС підприємства — АС «3» класу. Тобто, це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Для даної АС «3» класу обрано наступний профіль захищеності:

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

Цей профіль являє собою прелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ, щоб задовольняти певні вимоги щодо захищеності інформації, яка оброблюється в даній АС.

Таблиця 2.11 - Профіль захищеності

№	Послуга	Назва
1	КД-2	Базова довірч а конфі денцій ність
2	КО-1	Повторне використання об'єктів
3	КВ-1	Мінімальна конфіденційність при обміні
4	ЦД-1	Мінімальна довірча цілісність

5	ЦО-1	Обмежений бекап
6	ЦВ-1	Мінімальна цілісність при обміні
7	ДР-1	Квоти
8	ДВ-1	Ручне відновлення

Продовження таблиці 2.11 - Профіль захищеності

9	НР-2	Захищений журнал
10	НИ-2	Одиночна ідентифікація і автентифікація
11	НК-1	Однонаправлений достовірний канал
12	НО-2	Розподіл обов'язків адміністраторів
13	НЦ-2	КЗЗ з гарантованою цілісністю
14	НТ-2	Самотестування при старті
15	НВ-1	Автентифікація вузла

КД-2 - Базова довірча конфіденційність – Реалізовано

Користувач, домену якого належить об’єкт(процес) може вказати, які групи користувачів і які конкретні користувачі мають право одержувати інформацію від об’єкта, тобто КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта

КО-1 - Повторне використання об'єктів – Реалізовано

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, не залишається і скасовуються попередні права доступу до об’єкта.

КВ-1 - Мінімальна конфіденційність при обміні – Частково реалізовано

Реалізовано з допомогою протоколів FTP, HTTPS,POP3,SMTP.

ЦД-1 - Мінімальна довірча цілісність – Реалізовано

КЗЗ надаю можливість користувачу для кожного об’єкта, що належить його домену, визначати користувачів або групи користувачів, які мають право

модифікувати об’єкт.(Наприклад коди проектів, дизайнерські рішення сайтів тощо)

ЦО-1 - Обмежений бекап – Частоково реалізовано

Користувач або процес має можливість відкатити або відмінити дії над об’єктом до певного моменту, наприклад за допомогою горячих клавіш, резервним копіюванням даних. Якщо трапився збой в програмному забезпеченні, то система має автоматично відкатити ПЗ до попереднього стану. Якщо таке трапилось система повинна фіксувати це в журнал подій, але не робить тому, що журнал подій не реалізован.

ЦВ-1 - Мінімальна цілісність при обміні – Частково реалізовано

За допомогою протоколів TLS,SSL.

ДР-1 – Квоти – Не реалізовано

Не має обмежень на обсяг ресурсів які, виділяються користувачу , а також відсутній облік та контроль зовнішніх носіїв.

ДВ-1 – Ручне відновлення – Реалізовано

Коли перестає працювати КС чи її перестають обслуговувати КЗЗ переводить КС до стану очікування із якого її повернути до нормальної роботи може тільки адміністратор.

НР-2 - Захищений журнал – Не реалізовано

Відсутній облік та контроль зовнішніх носіїв. Журнал подій не включен.

НИ-2 - Одиночна ідентифікація і автентифікація – Реалізовано

Вхід здійснюється з використанням логіну та паролю.

НК-1 - Однонаправлений достовірний канал – Реалізовано

Зв’язок з використанням каналу ініціює саме користувач, тобто при включеня системи проводить користувач і вводить пароль тільки з клавіатури.

НО-2 – Розподіл обов’язків адміністраторів – Не реалізовано

Політика розподілу обов’язків, повинна визначати мінімум дві адміністративні ролі: адміністратор безпеки та іншого. У нас на підприємстві є тільки системний адміністратор , а адміністратора безпеки немає зовсім.

НЦ-2 - КЗЗ з гарантованою цілісністю – Частокво реалізовано

Політика цілісності КЗЗ визначає склад КЗЗ і механізми контролю цілісності компонентів. В системі є вбудовані механізми захисту Windows defender. А також є антивірусний комплекс, але який не має експертного висновку.

НТ-2 - Самотестування при старті – Реалізовано

Антивірусний комплекс при старті роботи перевіряє систему.

НВ-1 – Автентифікація вузла – Реалізовано

За допомогою протоколів TCP/IP і HTTPS.

В результаті аналізу КС було виявлено:

реалізовані послуги: КД-2, КО-1, ЦД-1, ДВ-1, НИ-2, НК-1, НВ-1, НТ-2;

частково реалізовані послуги: КВ-1, ЦО-1, ЦВ-1, НЦ-2;

нереалізовані полсуги: ДР-1, НР-2, НО-2;

2.4 Впровадження проектних рішень для захисту інформації

Після аналізу моделі порушника та моделі загроз, а також після обрання і аналізу профілю захищеності, виявлено загрози ,що мають високий рівень реалізації на підприємстві «SoftSolutions». До таких загроз належать збої електроживлення, несанкціоноване копіювання на зовнішні носії, інсталяція стороннього ПЗ, ненавмисні помилки співробітників, хакерські дії на вразливості ПЗ, перегляд ІзОД на екранах моніторів. Щоб досягти максимального рівня захищеності на підприємстві необхідно впровадити організаційні та програмно-апаратні засоби захисту інформації для реалізації функцій КЗЗ.

2.4.1 Організаційні рішення

Так як у нас не реалізована НО-2 і не має адміністратора безпеки та через відсутність чіткого контролю за встановленням ПЗ працівниками, можливе використання ПЗ в власних цілях або занесення вірусу до комп'ютерної системи. Для того щоб зменшити ризики потрібно ввести постійні перевірки знань, та тести

для підвищення кваліфікації, які будуть стосуватися всього персоналу, включаючи керівництво, а також потрібно ввести нову посаду – адміністратор безпеки. Також треба ввести правило «DownloadRestrictions», щоб заборонити користувачам завантажувати підозрілі файли, такі як шкідливі програми та заражені файли. Обмеження спрацьовують, коли користувач намагається завантажити файл за посиланням або натискає файл правою кнопкою миші і вибирає команду Зберегти посилання як.; ввести «білий список» сайтів в Інтернеті, які будуть відкритими для персоналу, інші заблокувати, також цей «білий список» буде живим і постійно розширювитася; удосконалювати роботу з підбору та розстановки кадрів, а також заходи контролю за персоналом. Під час інсталяції мають бути задіяні механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення.

Також, оскільки є можливість переглядати інформацію з екранів моніторів, оскільки прилеглі будівлі розташовані близько або із застосування спеціальної техніки(дронів) , потрібно таким чином, щоб з сусідніх будівель неможливо було бачити екран монітора або поставити перегородки біля кожного столу. Це унеможливить перегляданння інформації з сусідньої будівлі або за територією комплексу при наявності спеціальної техніки. Також треба поставити кодовий замок на двери, щоб якась постороння людина не могла просто взяти і увійти до кімнати, також це допоможе коли працівника забули закрити двері на ключ.

Для запобіганню крадіжок необхідно здійснити заходи для охорони території офісу та усі дані, документі, пристрої накопичення інформації зберігати у сейфі і необхідно створити приміщення для зберігання цих речей та закривати його, а доступ надати лише уповноваженим особам.

Ще треба ввести засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного

лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);

Через відсутність контролю за останніми версіями ПЗ можливі хакерські атаки на його вразливості. Було виявлено, що встановлено iFin версія 1.2 і не оновлено до останньої версії. Також розглядалось можливість впровадження Комп'ютерна програма «Українська бухгалтерська система УБС» замість iFin та 1С бухгалтерія. Звісно УБС має велику кількість переваг перед 1С і iFin, має експертний висновок, а також вже вбудовану КЗЗ, але було прийнято рішення залишити iFin тому, що вона відносно УБС має дуже низьку ціну і зараз підприємство не має можливості купити таку коштовну програму, але у майбутньому, коли підприємство буде розширюватися, перехід на УБС буде можливим . Отже потрібно ввести чіткий контроль за своєчасним оновлення ПЗ — підключити функцію автоматичного оновлення в певний час, щоб ПЗ не мало можливості оновлюватися в неробочі години та під час обслуговування системи, а також перевіряти ці оновлення та більш чіткого контролю виконанням цієї функції системним адміністратором.

2.4.2 Програмно-апаратні засоби

КВ-1 була частково реалізована за допомогою протоколів, щоб повністю реалізувати цю функцію, треба також додатково шифрувати дані, які у підприємстві зберігаються на зовнішніх носіях. Це допоможе у випадку, якщо ці зовнішні носії вкрадуть. Шифрування виконується у ПЗ VeraCrypt.

ЦВ-1 була частково реалізована також за допомогою протоколів, щоб повністю реалізувати цю функцію, потрібно також забезпечити захист об'єктів від модифікації, а саме впровадити у систему щоб, перед передачею ІзОД файли які будуть передаватися підписувались ЕП. Сертифікат електронного ключа береться у акредитованому центрі сертифікації ключів і сам сертифікат буде

зберігається на флешці і на комп'ютері SEO. Підписання файлів здійснюється за допомогою порталу Дія.

Через відсутність обліку та контролю зовнішніх носіїв інформації, протоколювання роботи зі змінними носіями можливе несанкціоноване копіювання на зовнішні носії, наприклад кодів проектів, або зараження вірусом. Отже щоб реалізувати ДР-1 та НР-2 потрібно заборонити підключати до робочого комп'ютера будь-які зовнішні накопичувачі інформації (USB Flash, SD-карти, телефони/смартфони) без підтвердження таких дій з SEO. Також можна впровадити систему контроль знімних носіїв і пристроїв (Ivanti Device Control) - це дозволить контролювати і управляти процесом використання знімних носіїв і зовнішніх пристроїв будь-яких типів на робочих станціях користувачів. Як найпростіший приклад таких політик можна привести дозвіл на підключення до комп'ютера корпоративних накопичувачів і повна заборона на підключення та використання будь-яких інших носіїв(буде можливість реєструвати свої накопичувачи, але їх потрібно буде перевіряти антивірусом і записувати результати перевірки в спеціальний журнал), якщо користувач все ж таки підключе незареєстрований свій носій на нього буде накладен штраф. Щоб була можливість реєструвати події також треба ввімкнути журнал подій для того щоб система мала можливість реєструвати всі події зв'язані із відкатом ПЗ, авторизацією користувачів тощо і це також допоможе повністю реалізувати ЦО-1.

Вибор робився із двох систем контролю знімних носіїв – це саме Ivanti device control і McAfee device control.

Mcafee захищає корпоративні дані, через такі носії інформації як USB-накопичувачі, MP3-плеєри, компакт-диски (CD) та цифрові відеодиски (DVD), в той час як Ivanti дає контроль та керування всіма пристроями введення/виводу через всі порти, включаючи USB, Firewire, WIFI, Bluetooth тощо. Також Ivanti використовує запатентовану технологію двостороннього тіньового копіювання інформації, яка записується/читається з дискет, CD/DVD дисків або інших знімних пристроїв, а також засоби для аудиту всіх подій, незалежно від того, був

доступний або не дозволений. На розсуд адміністратора може зберігатися або повна копія документа, що копіюється/переглядається, або тільки його назва, а McAfee в свою чергу лише надає інформацію про пристрій який був підключен і позначку в часі. Саме головне, що Ivanti надає можливість вирішити проблему витоку конфіденційної інформації внаслідок несанкціонованого використання в корпоративній мережі змінних незареєстрованих носіїв тому був обран саме Ivanti device control.

На підприємстві встановлена антивірусна програма Avira free antivirus версії 13.1.21.0, але щоб повністю реалізувати НЦ-2 краще встановити антивірусну програму, яка затверджена експертним висновком – Програмний продукт антивірусного захисту інформації McAfee Mvision Protect Plus for Endpoint який відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі "Державна експертиза за критеріями технічного захисту інформації комплексу засобів захисту антивірусного програмного забезпечення. Експертний висновок № 1151 Дійсний з 27.08.2020 до 27.08.2023. Цей антивірус був обраний не тому, що він має якійсь великі переваги ніж наприклад програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows (EEA)версії 7.x виробництва компанії «ESET» (Словаччина), а тому що у Eset експертний висновок закінчується 12.07.2022, а це вже незабаром. Також розглядався варіант із Zillya. Що стосується функціональності, обидві антивірусні програми пропонують сканування на віруси, подрібнювач файлів, брандмауер і безліч функцій для підвищення продуктивності вашого пристрою. Однак McAfee був обран головним чином тому, що він постійно показує кращі результати в антивірусних тестах і тестах на антивірусне програмне забезпечення. Антивіруси AVG, ZoneAlarm чи Norton не розглядалися тому, що не мають експертного висновку.

Збої електроживлення можливі через перепади напруги. На ОІД немає безперебійного джерела живлення, але в той же час є два принтери та 9 ПК, через які може статися падіння напруги в електромережі. Це стає можливим оскільки робота принтерів і комп’ютерів не контролюється — вони всі можуть працювати

одночасно, а також у персоналу впродовж робочого часу немає фіксованих правил, за якими вони зберігають проекти/документи в певний проміжок часу протягом дня. Отже, потрібно ввести для даної системи джерело безперебійного живлення — APC Smart-UPS

Таблиця 2.12 – Технічні характеристика ДБЖ

Технічна характеристка	APC Smart-UPC	Power Walker	Powercom
Габарити	171x215x439мм	190x328x399мм	428x635x84мм
Тип архітектури	Лінійно-інтерактивні	Безперервної дії (on-line)	Лінійно-інтерактивні
Потужність	1800ВТ	1800ВТ	1800ВТ
Напруга	12В	12В	12В
Вхідна напруга під час роботи	280В	300В	500В
Ємність	50	50	50
Час заряду батареї	3 години	6 години	4 годин

Для APC

$$T = \frac{C*U}{P*N} = \frac{50*12}{280*9} = 0.23 = 14 \text{ хвилин}$$

Для Power Walker

T=13 хвилин

Для Powercom

T=8 хвилин

Час автономної роботи розраховано за наступною формулою

Де T – час роботи від ДБЖ

C – ємність

U – напруга

P – потужність

N – кількість ПК.

Тобто у нас буде 14 хвилин при максимальному навантажені усіх засобів системи, щоб завершити всі необхідні процеси і зробити сейви проектів, а також користувач повинен за цей час має завершити роботу комп'ютера.

Джерело APC було вибрано тому, що воно має відносно не великий цінник і добре підходе саме для невеличкого підприємства, він маленький має достатній час автономної роботи, якщо його зрівнювати з іншими аналогами в цій ціновій категорії наприклад з Power Walker, то Power Walker теж забезпечує достатній час автономної роботи, але виходячи з відгуків він дуже гучний і може завадити працювати, а також має довгий час заряду батареї, а наприклад Powercom має великі габарити порівняно з APC і для збільшення автономної роботи потребує додаткові витрати на батарейні блоки.

Також треба ввести в ПЗ, в якому відбувається створення/модифікація проектів, функцію автоматичного зберігання через певний проміжок часу, щоб не було випадків коли розробник забув зробити сейви, і наприклад вимкнув комп'ютер, щоб не довелося проект робити з нуля.

2.6 Висновки до спеціальної частини

Ігнорування загроз та вразливостей інформаційно-телекомунікаційної системи може призвести до значних фінансових втрат та витоку інформації. Тому в другому розділі детально досліджено безпеку інформації на ІТС.

В ході виконання другого розділу розроблено модель порушника та модель загроз. Також обрано стандартний профіль захищеності, який використовується на підприємстві. Виявлено найбільш актуальні загрози, запропоновані організаційні та програмні рішення для досягнення максимального рівня захищеності на підприємстві «SoftSolutions».

Із організаційних рішень було впроваджено: правило «DownloadRestrictions»,

було запропоновано розгорнути столи, монітори і поставити перегородки для того, щоб унеможливити перегляд інформації через вікна, також вирішили створити приміщення для зберігання цінних речей і створити виділений сервер для архівації даних. Із програмно-апаратних рішень було впроваджено: шифрування даних за допомогою ПЗ VeraCrypt, впровадити систему контроль знімних носіїв і пристроїв (Ivanti Device Control), також підписувати файли ІзОД з допомогою ЕП, вирішили змінити антивірусну програму на яку має експертний висновок, обгрунтували не зміну, а оновлення програми бухгалтерської звітності і обгрунтували вибір джерела безперебійного живлення.

3.ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Економічне обгрунтування доцільності впровадження проектних рішень

Для економічного обгрунтування доцільності розробки проектних рішень інформації ТОВ «Soft Solution» потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів, які будуть отримані після розрахунків.

Економічна доцільність визначається:

- розрахунками капітальних витрат, що потребує розроблені проектні рішення;
- розрахунками експлуатаційних витрат;
- розрахунками річного економічного ефекту від розробки інформаційної політики безпеки.

3.1.1 Розрахунок суми витрат на розробку проектних рішень

Спочатку розраховується трудомісткість розробки проектних рішень, для цього потрібно скласти час, який знадобиться для кожної робочої операції:

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

- tmз - тривалість складання ТЗ на розробку проектних рішень = 50 годин;
- tв - тривалість розробки концепції безпеки інформації у організації = 30 годин;
- ta - тривалість процесу аналізу ризиків = 36 годин;
- tак - тривалість визначення вимог заходів, методів та засобів захисту = 18 годин;
- tозб - тривалість виробу основних рішень з забезпечення БІ = 56 годин;
- tовр - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 120 години;
- tд - тривалість документального оформлення проектних рішень = 20 годин.

$$t = 50 + 30 + 36 + 18 + 56 + 120 + 20 = 330 \text{ годин.}$$

3.1.2 Розрахунок суми витрат на реалізацію проектних рішень.

Сума витрат на розробку політики безпеки {Kpn) складається з витрат на:

- Заробітну плату спеціаліста з кібербезпеки — Ззп, грн;
- Вартості витрат машинного часу, що необхідний для розробки проектних рішень — Змч.

$$Kpn = Ззп + Змч = 27411 \text{ грн}$$

Заробітна плата спеціаліста складається з основної та додаткової заробітної плати, соціальних виплат та визначається за формулою:

$$Ззп = t * Зіб = 24750{,}00 \text{ грн}$$

де t — загальна тривалість розробки проектних рішень = 330 годин;

Зіб — середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями = 12000 / 160 = 75, грн/годину

Вартість машинного часу для розробки проектних рішень на ІТК визначається за формулою:

$$Змч = t * Смч = 2661 \text{ грн}$$

де t — трудомістшсть підготовки документації на ІТК =4 години;

Смч — вартість 1 години машинного часу ПК, грн./година (5,6 грн).

Відповідно до розроблених рекомендацій, планується використання ліцензійних програмних засобів, як вже встановлених, так і нових.

Розрахована вартість розробки проектних рішень Kpn ь складовою одноразових капітальних витрат разом з витратами на придбання програмних засобів, яш рекомендовані для використання.

Отже фіксована сума капітальних витрат на розробку проектних рішень складае:

$$К = Kpn + Кзпз + Knз + Каз + Кнавч + Кн = 61411 \text{ грн.}$$

де *Кпр* — вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх спеціалістів, тис. грн;

Кзпз — вартість закупівель ліцензійного основного і додаткового програмного забезпечення (ПЗ), тис. грн;

Крп — вартість розробки політики безпеки інформації, тис. грн;

Каз — вартість закупівли апаратного забезпечення та допоміжних матеріалів,

Кнавч вартість витрати на навчання технічних фахівців і обслуговуючого персоналу = 5600 грн;

Лв — витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

3.2 Оцінка можливого збитку

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

Необхідні вихідні дані для розрахунку:

tn — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 1 година;

tв — час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

tви — час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі 2 години;

Зо — заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 5500 грн./міс.;

Зс — заробітна плата співробітнишв атакованого вузла або сегмента корпоративної мережі, 11000 грн./міс.;

Чо — чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

Чс — чисельність співробітнишв атакованого вузла або сегмента корпоративної мережі, 7 осіб.;

О — обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2 млн грн. у рік;

Пзч — вартість заміни устаткування або запасних частин, грн; І — число атакованих сегментів корпоративної мережі, 1;

N — середне число атак на рік, 10.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U=Пп +Пв +V=11740,4,$$

де Пп — оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пв — 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:

$$П_п = \frac{\sum Зс}{F} * t_n,$$

$$Пп = ((11000 *7)/176)*3 = 1312,5 грн,$$

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

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

$$Пви = ((11000 *7)/176)*4 = 1750 грн,$$

Витрати на заміни устаткування або запасних частин можуть скласти 3200

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

$$Пв = 1312,5 + 1750 + 125 = 1875 \text{ грн.}$$

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

$$В = 1 * 14 * 13764,4 = 192700 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

$$ROSI = E / K, \text{ еастки одиниці}$$

де — Е загальний ефект від впровадження системи інформаційної безпеки грн.; К — капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$57226 / 60423,5 = 0,95$$

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

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,95 > (23 — 14)/100 = 0,95 > 0,09$$

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

$$Т = 1/0,95 = 1.05 \text{ років.}$$

Висновки

Розробка проектних рішень безпеки для ТОВ «Soft Solution» є економічно доцільною, оскільки коефіцієнт повернення інвестицій ROSI складає 0,95, що означає отримання 0,95 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів.

ВИСНОВКИ

На сьогоднішній день захист інформації це головна мета для підприємств усіх галузей розвитку, адже безпека інформації - це безпека підприємства загалом, яка відповідає не тільки за безпеку інформації на цифрових носіяї чи пристроях, а й усього що стосується приватної інформації про клієнтів, працівників, діла компанії та щодо комерційних таємниць.

Комплексні системи захисту інформації — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації у підприємстві. Згідно з законодавством України, інформація з обмеженим доступом повинна в обов'язковому порядку бути захищена за усіма нормами.

В цій кваліфікаційній роботі показано користь вирішення питання безпеки інформації підприємстві на прикладі підприємства «SoftSolutions».

В першому розділі надані загальні відомості та детально описано організаційну структуру підприємства, а також надано схеми, які допоможуть створити чіткий план дій для забезпечення безпеки підприємства. Обґрунтовано причини створення КСЗІ. В акті обстеження детально розглянуто ситуаційний та генеральний плани, також було проведено аналіз обчислювальної системи на підприємстві.

Згідно з даними першого розділу, в спеціальній частині розроблено модель порушника, модель загроз та обрано профіль захищеності. Проаналізувавши ці дані, проведено впровадження організаційних та програмно-апаратних рішень для захисту інформації.

В економічному розділі провели основні розрахунки, результатом яких стало підтвердження економічної доцільності запропонованих проектних рішень.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Статистика кібератак на підприємства [Електронний ресурс]. - Режим доступу https://techexpert.ua/cyber-attacks-number-statistics/

2. Статистика кібератак на малі підприємства за 2021 рік [Електронний ресурс]. - Режим доступу https://www.fundera.com/resources/small-business-cyber-security-statistics#

3. Інформація щодо IT компаній, які ведуть бізнес на території України [Електронний ресурс]. - Режим доступу https://jobs.dou.ua/ratings/

4. Закон України «Про інформацію» від 02.10.1992 No 2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація “інформації в законодавстві України”.

5. Закон України “Про захист персональних даних” від 01.06.2010 No 2297-VI// Відомості Верховної Ради України. - 2010. - No 5. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2297-17.

6. Закон України “Про доступ до публічної інформації” від 13.01.2011 No 2939- VI // Відомості Верховної Ради Україии. - 2011. - No 32. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2939-17.

7. Закон Україии “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. -

8. 1994. - No 80. [Електронний ресурс]. - Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

9. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id doc=66911.

10. ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id doc=66912.

11. НД ТЗІ 3.7-003 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. -[Чинний від 08.11.2005] - К. ДССЗЗІ, 2005. - No125 - (Нормативний документ системи технічного захисту інформації).

12. НД ТЗІ 1.4-001 - 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).

13. НД ТЗІ 2.5-004 - 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).

14. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).

15. НД ТЗІ 1.6-005 - Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної темниці. - [Чинний від 15.04.2013] - К. : ДССЗЗІ, 2013. - No125 - (Нормативний документ системи технічного захисту інформації).

16. Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive- zavdannya-sogodennya/.

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

18. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека / О.В. Герасіна, Д.С.Тимофеев, О.В. Кручинін, Ю.А.МілінчукДніпро: НТУ “ДП”, 2020. 47 с.

19. НД ТЗІ 2.5-004 - 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).

20. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).

21. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2-004-99. — Київ: ДСТСЗІ СБ України, 1999. — 55 с.

22. Інформація щодо середньої заробітної плати спеціаліста з кібербезпеки. [Електронний ресурс]. - Режим доступу https://ua.trud.com/ua/salary/2/67683.html

23. Актуальні ціни на електроенергію [Електронний ресурс]. - Режим доступу https://yasno.com.ua/b2c-tariffs

24. Середня заробітна плата спеціаліста з кібербезпеки [Електронний ресурс]. - Режим доступу https://ua.trud.com/ua/salary/2/67682.html

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	18	
6	А4	Спеціальна частина	20	
7	А4	Економічний розділ	6	
8	А4	Висновки	1	
9	А4	Перелік використаних джерел	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Ґ	7	
14	А4	Додаток Д	5	
15	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Пояснювальна_записка_Бакун.doc
2. Пояснювальна_записка_Бакун.pdf
3. Презентація_Бакун.pptx

ДОДАТОК В. Відгуки керівників розділу

Відгук керівника економічного розділу

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 60б. («Задовільно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Ґ . Основні і допоміжні технічні засоби

Таблиця - Основні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
1	PC1	Системний блок	Комп'ютер ARTLINE Business X22v06	X22v06PC1	Під столом
2	PC2	Системний блок	Комп'ютер ARTLINE Business B55v06Win	B55v06WinPC2	Під столом
3	PC3	Системний блок	Комп'ютер ARTLINE Program B29v25	B29v25PC3	Під столом
4	PC4	Системний блок	Комп'ютер ARTLINE Program B29v25	B29v25PC4	Під столом
5	PC5	Системний блок	Комп'ютер ARTLINE Program B29v25	B29v25PC5	Під столом
6	PC6	Системний блок	Комп'ютер ARTLINE Program B29v25	B29v25PC6	Під столом

Продовження таблиці - Основні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
7	PC7	Системний блок	Комп'ютер ARTLINE Program B29v25	B29v25PC7	Під столом
8	PC8	Системний блок	Комп'ютер ARTLINE Business B55v06Win	B55v06WinPC8	Під столом
9	PC9	Системний блок	Комп'ютер ARTLINE Business B55v06Win	B55v06WinPC9	Під столом
10	PC1	Монітор	ASUS VZ279HEW FullHD 1920x1080	UM.WV7EE.001	На столі
11	PC2	Монітор	Acer V225Qbi FullHD 1920x1080	VZ279HE-PC2	На столі
12	PC3	Монітор	Acer V227Qbi FullHD 1920x1080	VZ279HE-WPC3	На столі
13	PC4	Монітор	Acer V227Qbi FullHD	VZ279HE-WPC4	На столі

			1920x1080		

Продовження таблиці - Основні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
14	PC5	Монітор	Acer V227Qbi FullHD 1920x1080	VZ279HE-WPC5	На столі
15	PC6	Монітор	Acer V227Qbi FullHD 1920x1080	VZ279HE-WPC6	На столі
16	PC7	Монітор	Acer V227Qbi FullHD 1920x1080	VZ279HE-WPC7	На столі
17	PC8	Монітор	Acer V225Qbi FullHD 1920x1080	VZ279HE-PC8	На столі
18	PC9	Монітор	Acer V225Qbi FullHD 1920x1080	VZ279HE-PC9	На столі
19	PC1	Клавіатура дротова	Logitech K120 USB (мембранна)	920-002643	На столі (на висувній полиці)
20	PC2	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC2	На столі (на висувній полиці)

Продовження таблиці - Основні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
21	PC3	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC3	На столі (на висувній полиці)
22	PC4	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC4	На столі (на висувній полиці)
23	PC5	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC5	На столі (на висувній полиці)
24	PC6	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC6	На столі (на висувній полиці)
25	PC7	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC7	На столі (на висувній полиці)
26	PC8	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC8	На столі (на висувній полиці)
27	PC9	Клавіатура дротова	2E KS 101 Slim (мембранна)	KS101WBPC9	На столі (на висувній полиці)
28	PR1	БФП кольорового друку	Epson L3101	C11CG88402PR1	На столі директора

Продовження таблиці - Основні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
29	PR2	БФП кольорового друку	Epson L3101	C11CG88402PR2	На столі HR-менеджера
30	K1	Комутатор	TP-Link TL-SG1016PE	TL-SG1016PEK1	На полиці справа від входу
31	M1	Роутер	Keenetic Ultra 1810	K434NU45198	На стелі біля входу

Таблиця - Допоміжні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
1	PC1	Миша дротова	ASUS ROG Sica	90MP00B1-B0UA01PC1	На столі (на висувній полиці)
2	PC2	Миша дротова	2E MF107	MF107UBPC2	На столі (на висувній полиці)
3	PC3	Миша дротова	ASUS ROG Sica	90MP00B1-B0UA01PC3	На столі (на висувній полиці)
4	PC4	Миша дротова	ASUS ROG Sica	90MP00B1-B0UA01PC4	На столі (на висувній полиці)

Продовження таблиці - Допоміжні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
5	PC5	Миша дротова	ASUS ROG Sica	90MP00B1-B0UA01PC5	На столі (на висувній полиці)
6	PC6	Миша дротова	ASUS ROG Sica	90MP00B1-B0UA01PC6	На столі (на висувній полиці)
7	PC7	Миша дротова	ASUS ROG Sica	90MP00B1-B0UA01PC7	На столі (на висувній полиці)
8	PC8	Миша дротова	2E MF107	MF107UBPC8	На столі (на висувній полиці)
9	PC9	Миша дротова	2E MF107	MF107UBPC9	На столі (на висувній полиці)
10	PC1	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC1	На столі (біля монітору)
11	PC2	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC2	На столі (біля монітору)
12	PC3	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC3	На столі (біля монітору)
13	PC4	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC4	На столі (біля монітору)

Продовження таблиці - Допоміжні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
14	PC5	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC5	На столі (біля монітору)
15	PC6	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC6	На столі (біля монітору)
16	PC7	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC7	На столі (біля монітору)
17	PC8	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC8	На столі (біля монітору)
18	PC9	Гарнітура дротова	HyperX Cloud Stinger	HX-HSCSC2-PC9	На столі (біля монітору)

Продовження таблиці - Допоміжні технічні засоби

№	Назва	Складова	Марка	Серійний номер	Розміщення
19		Датчик диму	Ajax FireProtect Plus	14567212	На стелі (лівіше ніж PC5)
20		Датчик диму	Ajax FireProtect Plus	14567213	На стелі (правіше ніж PC5)
21		ІЧ-датчик руху	Ajax MotionProtect	12255510	На стелі (в куті зліва кімнати)
22		ІЧ-датчик руху	Ajax MotionProtect	12255511	На стелі (в куті справа кімнати)

ДОДАТОК Д. Таблиця - Характеристика складу ОС

№	Назва	Складова	Серійний номер
1	PC1	Процесор AMD 8-core Ryzen 7 5700G	13463111
2	PC1	Відеокарта Sapphire Radeon RX 6700	13463112
3	PC1	Материнська плата ASUS ROG Strix B450	13463113
4	PC1	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	13463114
5	PC1	Накопичувачі 240GB SSD 2TB HDD	13463115 13463116
6	PC1	Блок живлення Gigabyte P850GM	13463117
7	PC2	Процесор Intel 4-Core i3-10100	12411110
8	PC2	Відеокарта Asus GeForce GTX 1050 Ti	12411111
9	PC2	Материнська плата Asus Prime H510M-K	12411112

Продовження таблиці - Характеристика складу ОС

№	Назва	Складова	Серійний номер
10	PC2	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	12411113
11	PC2	Накопичувачі 240GB SSD 2TB HDD	12411114 12411115
12	PC2	Блок живлення Gigabyte P850GM	12411116
13	PC3	Процесор intel 6-Core i5-10400	12134560
14	PC3	Відеокарта MSI GeForce RTX2060	12134561
15	PC3	Материнська плата Asus Prime H510M-K	12134562
16	PC3	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	12134563
17	PC3	Накопичувачі 240GB SSD 2TB HDD	12134564 12134565
18	PC3	Блок живлення Gigabyte P850GM	12134566
19	PC4	Процесор intel 6-Core i5-0400	53214560

Продовження таблиці - Характеристика складу ОС

№	Назва	Складова	Серійний номер
20	PC4	Відеокарта MSI GeForce RTX2060	53214561
21	PC4	Материнська плата Asus Prime H510M-K	53214562
22	PC4	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	53214563
23	PC4	Накопичувачі 240GB SSD 2TB HDD	53214564 53214565
24	PC4	Блок живлення Gigabyte P850GM	53214566
25	PC5	Процесор intel 6-Core i5-0400	65412340
26	PC5	Відеокарта MSI GeForce RTX2060	65412341
27	PC5	Материнська плата Asus Prime H510M-K	65412342
28	PC5	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	65412343
29	PC5	Накопичувачі 240GB SSD 2TB HDD	65412344 65412345
30	PC5	Блок живлення Gigabyte P850GM	65412346

Продовження таблиці - Характеристика складу ОС

№	Назва	Складова	Серійний номер
31	PC6	Процесор intel 6-Core i5-0400	54180870
32	PC6	Відеокарта MSI GeForce RTX2060	54180871
33	PC6	Материнська плата Asus Prime H510M-K	54180872
34	PC6	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	54180873
35	PC6	Накопичувачі 240GB SSD 2TB HDD	54180874 54180875
36	PC6	Блок живлення Gigabyte P850GM	54180876
37	PC7	Процесор intel 6-Core i5-0400	86186420
38	PC7	Відеокарта MSI GeForce RTX2060	86186421
39	PC7	Материнська плата Asus Prime H510M-K	86186422
40	PC7	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	86186423
41	PC7	Накопичувачі 240GB SSD	86186424 86186425

		2TB HDD	

Продовження таблиці - Характеристика складу ОС

42	PC7	Блок живлення Gigabyte P850GM	86186426
43	PC8	Процесор intel 6-Core i5-0400	98712340
44	PC8	Відеокарта Asus GeForce GTX 1050 Ti	98712341
45	PC8	Материнська плата Asus Prime H510M-K	98712342
46	PC8	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	98712343
47	PC8	Накопичувачі 240GB SSD 2TB HDD	98712344 98712345
48	PC8	Блок живлення Gigabyte P850GM	98712346
49	PC9	Процесор Intel 4-Core i3-10100	74351090
50	PC9	Відеокарта Asus GeForce GTX 1050 Ti	74351091
51	PC9	Материнська плата Asus Prime H510M-K	74351092

Продовження таблиці - Характеристика складу ОС

№	Назва	Складова	Серійний номер
52	PC9	Оперативна пам’ять Kingston Fury 16GB DDR4-3200	74351093
53	PC9	Накопичувачі 240GB SSD 2TB HDD	74351094 74351095
54	PC9	Блок живлення Gigabyte P850GM	74351096

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студента групи 125-18-1
Бакуна Дениса Вікторовича
на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «Soft Solution»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 77 сторінках.

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

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, розробка моделі порушника, визначення актуальних загроз, формування вимог до захисту інформації та розробка проектних рішень їх реалізації.

Запропоновано розділити повноваження адміністраторів, правила доступу до Інтернет та інсталяції програмного забезпечення. Розроблені проектні рішення: з впровадження шифрування, з контролю використання зовнішніх носіїв, з оновлення прикладного програмного забезпечення бухгалтерського обліку; антивірусного захисту та забезпечення резервного електроживлення.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей ІТС та самого ТОВ «Soft Solution».

До недоліків відноситься недостатньо обгрунтована модель загроз та профіль захищеності та деякі проектні рішення.

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

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

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

Кваліфікаційна робота заслуговує оцінки «Добре».

Керівник кваліфікаційної роботи, професор Корнієнко В.І.

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