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 *Чиркова Микити Володимировича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційної системи товариства з обмеженою відповідальністю "Лан-Тайм"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Горєв В.М.			
розділів:				
спеціальний	ст. викл. Святошенко В.О.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
20

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Чиркова М.В.*** **академічної групи** ***125-17-2***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

на тему ***Комплексна система захисту інформації інформаційної системи товариства з обмеженою відповідальністю "Лан-Тайм"***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.21 № 317-С

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Необхідні умови для створення КСЗІ. Постановка задачі	10.05.2021-25.05.2021
Розділ 2	Обстеження об'єкта інформаційної діяльності, аналіз інформаційних потоків на підприємстві, розробка та технічна реалізація політики безпеки	26.05.2021-02.06.2021
Розділ 3	Визначення економічно-технічної доцільності політики безпеки, розрахунки витрат впровадження політики безпеки	03.06.2021-04.06.2021

Завдання видано _____ Святошенко В.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 07.05.2021

Дата подання до екзаменаційної комісії: 18.06.2021

Прийнято до виконання _____ Чирков М.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 72 ст., 5 рис., 11 табл., 4 додатка, 7 джерел.

Об’єкт дослідження: інформаційне поле комерційної структури «Лан-Тайм»

Мета: визначення необхідності реалізації комплексу систем захисту інформації для підприємства, аналіз інформаційного поля компанії і розробка механізмів захисту в сфері інформаційної безпеки організації, розрахунок витрат на реалізацію проекту.

Методи розробки: спостереження, обстеження, аналіз, опис та розрахунки.

Перший розділ являє собою обстеження діяльності підприємства, наведено загальні відомості про об’єкт інформаційної діяльності, категоріювання інформаційно-телекомунікаційної системи, дослідження нормативно-правової бази компанії, та її простеження інформаційного простору і встановлення необхідності реалізації КСЗІ на даному підприємстві.

Другий розділ обґрунтовує технічну частину даної роботи. Створення актів та документів пов'язаних із аналізом інформаційного поля компанії, розробка КСЗІ.

Третій розділ представляю собою економічну частину діяльності підприємства, розраховано доцільність використання розробленої КСЗІ, та економічну ефективність впровадження її елементів в інформаційно-телекомунікаційну систему на об’єкті інформаційної діяльності а також розрахунок економічної ефективності, впровадження системи контролю виконання політики інформаційної безпеки, прорахунок поточних та капітальних витрат

ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, НОРМАТИВНО-ПРАВОВА БАЗА, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ

Реферат

Пояснительная записка: 72 в., 5 рис., 11 табл., 4 приложения, 7 источников.

Объект исследования: информационное поле коммерческой структуры «Лан-Тайм»

Цель: определение необходимости реализации комплекса систем защиты информации на предприятии, анализ информационного поля компании і разработка механизмов защиты в сфере информационной безопасности организации, расчет затрат на реализацию проекта.

Методы разработки: наблюдение, обследование, анализ, описание и расчеты.

Первый раздел представляет собой обследование деятельности предприятия, приведены общие сведения об объекте информационной деятельности, категорирование информационно-телекоммуникационной системы, исследования нормативно-правовой базы компании, и ее проследить информационного пространства і установления необходимости реализации КСЗИ на данном предприятии.

Второй раздел обосновывает техническую часть данной работы. Создание актов и документов связанных с анализом информационного поля компании, разработка КСЗИ.

Третий раздел представляю собой экономическую часть деятельности предприятия, рассчитаны целесообразность использования разработанной КСЗИ, и экономическую эффективность внедрения ее элементов в информационно-телекоммуникационную систему на объекте информационной деятельности, а также расчет экономической эффективности, внедрение системы контроля исполнения политики информационной безопасности, просчет текущих и капитальных расходов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ, НОРМАТИВНО-ПРАВОВА БАЗА, ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

ABSTRACT

Explanatory note: 72 articles, 5 figures, 11 tables, 4 appendices, 7 sources.

Object of research: information field of the commercial structure "Lan-Time"

Purpose: to determine the need for a set of information security systems for the company, analysis of the information field of the company and the development of protection mechanisms in the field of information security of the organization, calculation of project costs.

Development methods: observation, survey, analysis, description and calculations.

The first section is a survey of the enterprise, provides general information about the object of information activities, categorization of information and telecommunications system, study of the regulatory framework of the company, and its tracing of the information space and the need to implement KSZI at the company.

The second section substantiates the technical part of this work. Creation of acts and documents related to the analysis of the company's information field, development of KSZI.

The third section is the economic part of the enterprise, calculated the feasibility of using the developed KSZI, and the economic efficiency of its elements in the information and telecommunications system at the object of information activities and the calculation of economic efficiency, implementation of information security policy, calculation of current and capital costs

INFORMATION SECURITY, COMPLEX OF MEANS OF PROTECTION, REGULATORY LEGAL FRAMEWORK, TECHNICAL MEANS OF PROTECTION

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІТС – Інформаційно-телекомунікаційна система

КСЗІ - Комплексні системи захисту інформації

ОІД - об’єкт інформаційної діяльності

ДТЗС - Допоміжні технічні засоби та системи

ІЗоД - Інформація з обмеженим доступом

ПЕМВН – побічні електромагнітні випромінювання та наводки

КС – комп’ютерна система

КЗЗ – комплекс засобів захисту

ІС – інформаційна система

ІБ – інформаційної безпеки

ЗМІСТ

ВСТУП

У теперішній час задача убезпечити достатній рівень безпеки інформації на підприємстві являється однією із найважливіших. Оскільки галузь інформаційних технологій найбільш стрімко розвивається, більша кількість підприємств починає використовувати, або вже давно використовує ІТС, тому з'являється велика кількість, як спеціалістів у даній сфері, так і з ними, зловмисників.

Вдосконалення комплексної системи безпеки інформації необхідне на сьогоднішній день, так як воно приносить вигоду як підприємству так і його клієнтам. Оскільки будь яка втрата, або модифікація інформації може призвести до великих фінансових та репутаційних втрат як у клієнта так і у компанії.

Зараз більшість держав має органи, які займаються питаннями безпеки інформації. Данні структури розробляють стандарти, закони та правила, які покращують життєдіяльність підприємств, суспільства та інших галузей які впливають на різні чинники життєздатності держави та її ресурсів.

У наступних розділах буде розглянуто організацію «Лан-Тайм», та її життєдіяльність з точки зору підприємства, встановлено необхідність реалізації КСЗІ для ІТС даної компанії, виконано розрахунки на реалізацію КСЗІ виходячи із обстеження підприємства та зроблено висновки стосовно даної роботи.

У роботі було частково змінено інформацію, проте змінені дані на достовірність роботи не впливають.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство

Підприємство «Лан-Тайм» займається логістичною діяльністю по перевозці товарів. Підприємство працює з перевізниками та клієнтами. Організація почала свою власну діяльність у 2017 році. За 4 роки введення власної діяльності компанія працює із 150 великими клієнтами. Головний офіс знаходиться у м. Дніпро, вулиця Січових стрільців, 9д.

Працівники являють собою ресурс для продуктивності будь-якої компанії і реалізації її життєдіяльності. Нижче буде надано таблицю, про загальний обсяг працівників даного підприємства.

Таблиця 1.1 – Штат працівників підприємства

Посада	Кількість працівників	Рівень кваліфікації
Директор	1	Високо кваліфіковані робітники
Менеджер	1	Високо кваліфіковані робітники
Оператор	2	Кваліфіковані працівники
Агенти	10	Кваліфіковані працівники
Бек супорт	1	Кваліфіковані працівники
Бухгалтер	1	Високо кваліфіковані робітники
Менеджер по претензіям	1	Високо кваліфіковані робітники

Проте будь яка компанія потребує переліку документів, які затверджені державним законодавством, котрі впливають та керують діяльністю компанії.

У наступному підрозділі буде обстежено нормативно-правову базу підприємства, проведено аналіз нормативних документів і виходячи із пунктів, зроблено висновки стосовно необхідності КСЗІ для даної організації.

1.2 Нормативно-правова база підприємства

Згідно із ДСТУ 2732:2004 «Діловодство і архівна справа. Терміни та визначення»

«Нормативно-правова база – це обґрунтування, на державному рівні діяльності будь-якого підприємства, незалежно від форми власності, сфери діяльності та масштабу. Діяльність всіх організацій / підприємств / установ завжди спирається на законодавство країни і нормативні акти, які регулюють діяльність в певній сфері»

Із вищеописаного терміну, можна сказати, що нормативно-правова база з точки зору організації являю собою перелік нормативно-правових документів, які керують комерційними чинниками компанії.

Обсяг та перелік документів залежить від діяльності компанії, її сфери галузі та нормативної поведінки в залежності від встановлених державних законів.

Для дослідження діяльності організації було оглянуто перелік документі, які складають нормативно-правову базу організації. Були переглянуті такі документи:

1) Трудовий договір.
2) Договір медичного страхування
3) Договір про нерозголошення комерційної таємниці підприємства

1.3 Акт обстеження

Акт обстеження представляю собою документ аналітичного характеру, де описана інформація про ІТС підприємства, формально, документ можна розподілити на декілька етапів:

1) Обстеження фізичних об’єктів
2) Аналіз програм та апаратного забезпечення ІТС
3) Дослідження захищеності ІТС

Характеристика об’єктів, які розташовані разом із ІТС

ОІД є приміщення товариства з обмеженою відповідальністю (ТОВ) «Лан-Тайм». Область діяльності – логістичні послуги та пошук нових клієнтів та перевізників.

ОІД знаходиться за адресою: Україна, м. Дніпро, вулиця Січових стрільців, 9д, офіс 3. Будівля в якій знаходиться ОІД має шість поверхів, побудована із цегли та залізобетонних конструкцій. Прикладається ситуаційний план ОІД (рисунок 1.1)

Навколо будівлі, де знаходиться ОІД, розміщені такі об’єкти: на північ знаходиться двох поверховий жилий будинок, на схід двох поверховий офісний будинок, на південно-східному та східному напрямку знаходяться два двох поверхових жилих будинків, на західному напрямку знаходиться трьох поверхова жила будівля та на північно-західному напрямку знаходиться двох поверхова жила споруда. Характеристика усіх будівель та споруд наведена у таблиці 1.2

На території ІТС проходять такі лінії систем комунікації: опалення, водопостачання, електропостачання, лінії мережі «Internet», пожежної сигналізації. Вхід до будівлі здійснюється через двері з магнітним та кодовим замком, вхід до офісу здійснюється через залізні двері з двома замками, магнітним та сувальдним замком. У всіх працівників є магнітний ключ, який відкриває двері офісу. Ключі від сувальдного замка є тільки у операторів та директора з менеджером, магнітний замок не відчиняє двері за 15 хвилин перед початком та кінцем робочого дня усім крім директора з менеджером та операторів.

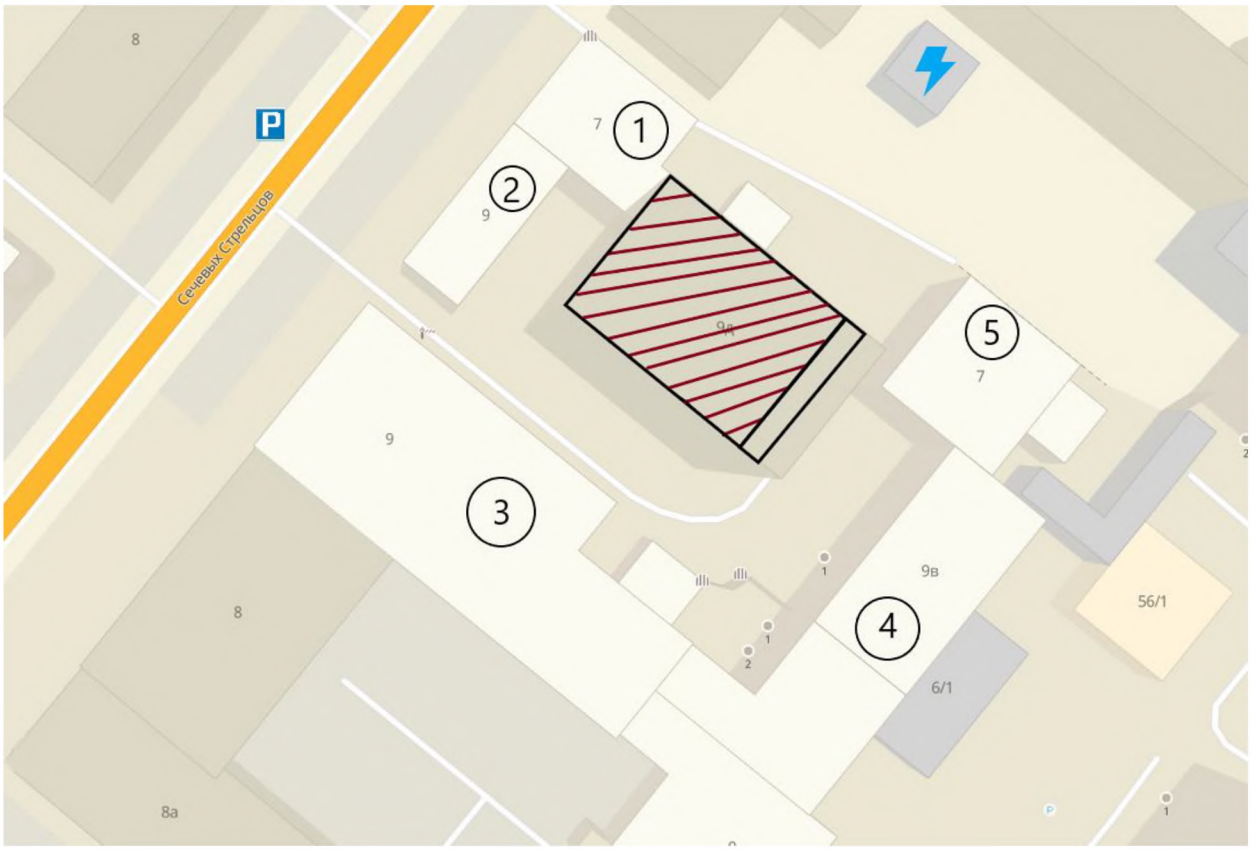


Рисунок. 1.1 – Структура ІТС


- Територія ОІД


-Місце парковки


-Мережа КЗ


-Будівля


-розподільний щит

Умовні позначення

Таблиця 1.2 - Характеристика будівель навколо ОІД

Найменування	Кількість поверхів	Адреса	Відстань від ОІД, м.
жилий будинок	2	Вул. Січових стрільців, 7	5
офісний будинок	2	Вул. Січових стрільців, 7	5
жилий будинок	2	Вул. Січових стрільців, 9в	10
жилий будинок	2	Вул. Січових стрільців, 9	15
жилий будинок	3	Вул. Січових стрільців, 9	10
жилий будинок	2	Вул. Січових стрільців, 9	7,5
Гараж	1	Вул. Січових стрільців, 7	5

Опис фізичного середовища ОІД

ОІД, що обстежується, знаходиться на третьому поверсі, стіни ОІД зроблені із цегли та гіпсокартону, товщина стін 30см. Підлога та стелі залізобетонні конструкції приблизно 12-15 см. На вході в ОІД стоїть металеві двері товщиною 80мм. з магнітним та сувальдним замком. На території ОІД розміщено 9 дерев'яних дверей товщиною 30мм. з засувним механізмом та 10 віконних отворів, товщиною 25мм. Вікна вироблені із склопакети, пластику та металу.

На ОІД з північної, східної, південної та західної сторони є віконні отвори. Вище та нижче поверхом знаходяться сусідні офісні приміщення. Вони мають стіни товщиною 30 см, підлога та стеля залізобетонні конструкції товщиною 12-15 см. Приміщення мають один вхід, нижче знаходиться деревинні двері товщиною 35мм. з циліндровим замком, вище приміщення має металеві двері товщиною 70мм. з кодовим замком. На ОІД є такі лінії систем комунікацій: електропостачання,

освітлення (рисунок 1.2), опалення та вентиляції (рисунок 1.3), водопостачання, лінії мережі «Internet», пожежної сигналізації (рисунок 1.4). Розетки мають паралельне з'єднання та підключаються до електричної щитової в офісі.

На ОІД використовуються ноутбуки, маршрутизатор, принтер (повний список ресурсів приведено в таблиці 1.3) Використовується система пожежної сигналізації та камер відеоспостереження. (список приведений в таблиці 1.4) Повна характеристика складу ІТС (приведена в таблиці 1.5) також на ОІД використовуються системні, прикладні та спеціальні програмі забезпечення (детальний опис яких наведено в таблиці 1.6)

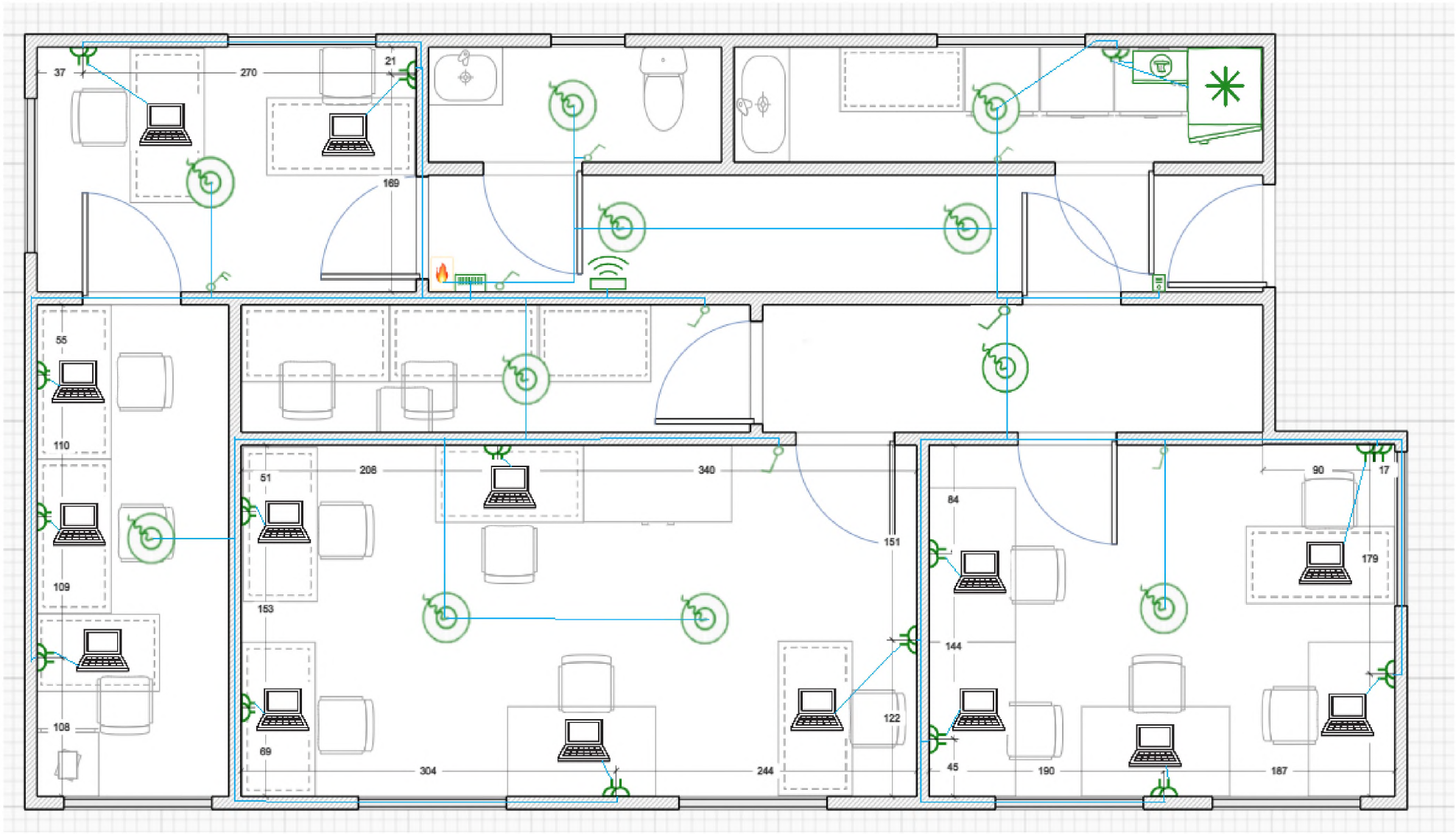
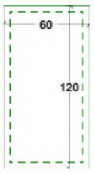


Рисунок 1.2 - План освітлення та електропостачання

- Двері

- Вікна

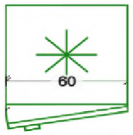


-Стіл

- Шкаф

- тумба

- Мікрохвильова піч



- Холодильник

- Раковина

- Туалет

- кухонний підлоговіий шкаф

- Стіл

- Розетка

- Ноутбук

-Щиток пожежної безпеки

- Вмикач

-Домофон

-Електрощиток

-Зпарений вмикач

-Wi-Fi роутер

- Лампа

- лінії єлектропостачання

УМОВНІ ПОЗНАЧЕННЯ

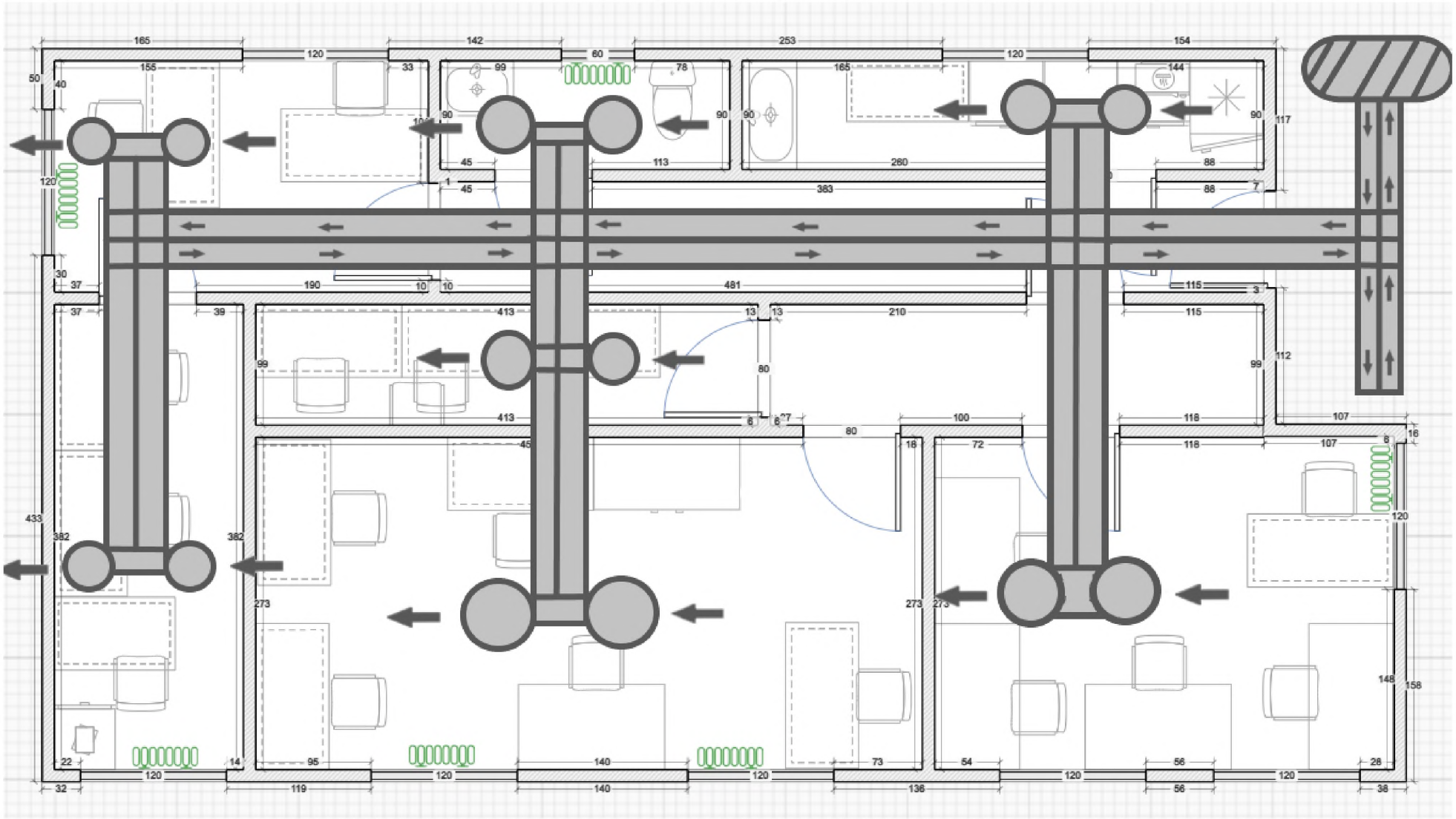


Рисунок 1.3 - План опалення та вентиляції

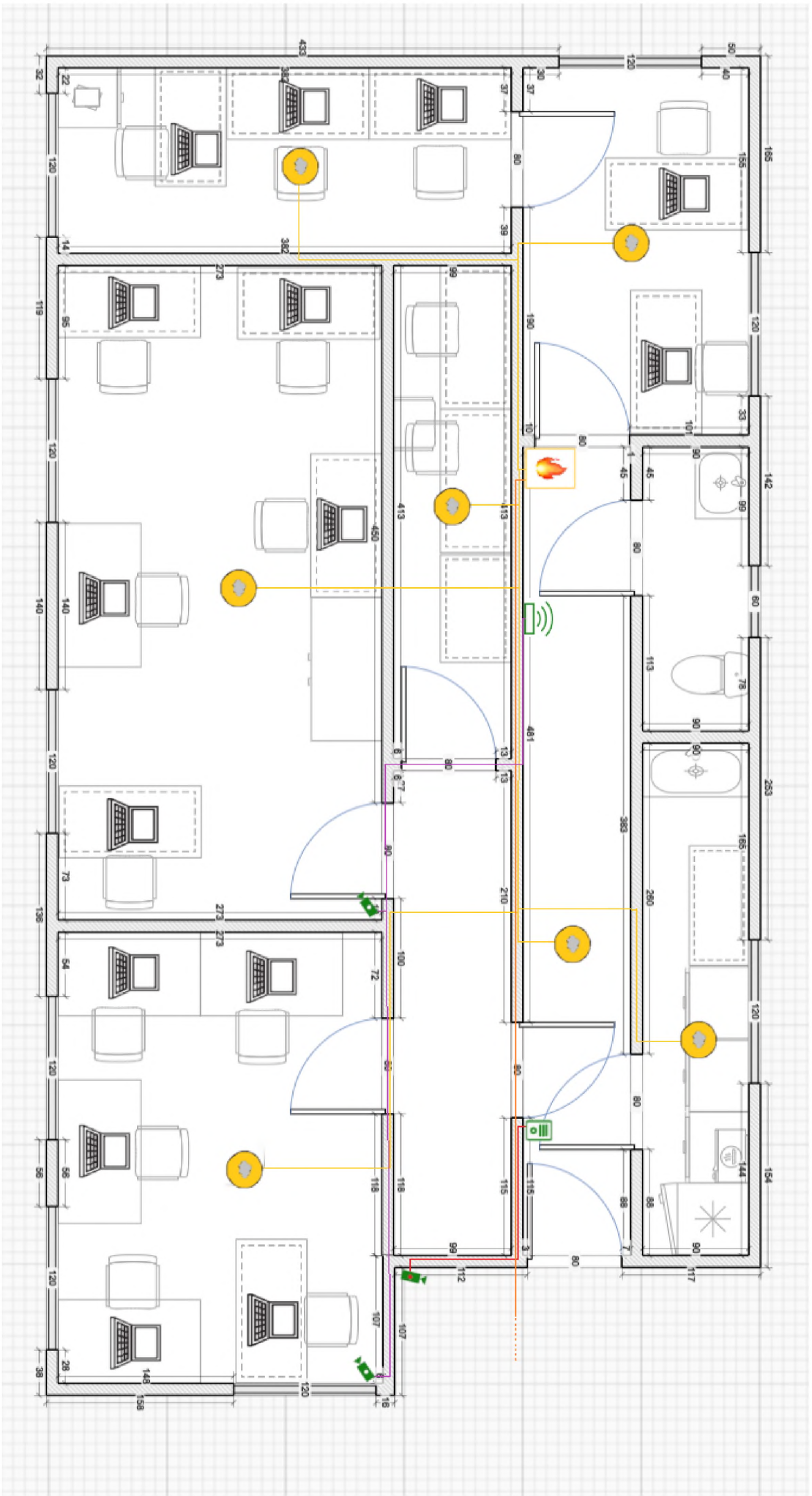
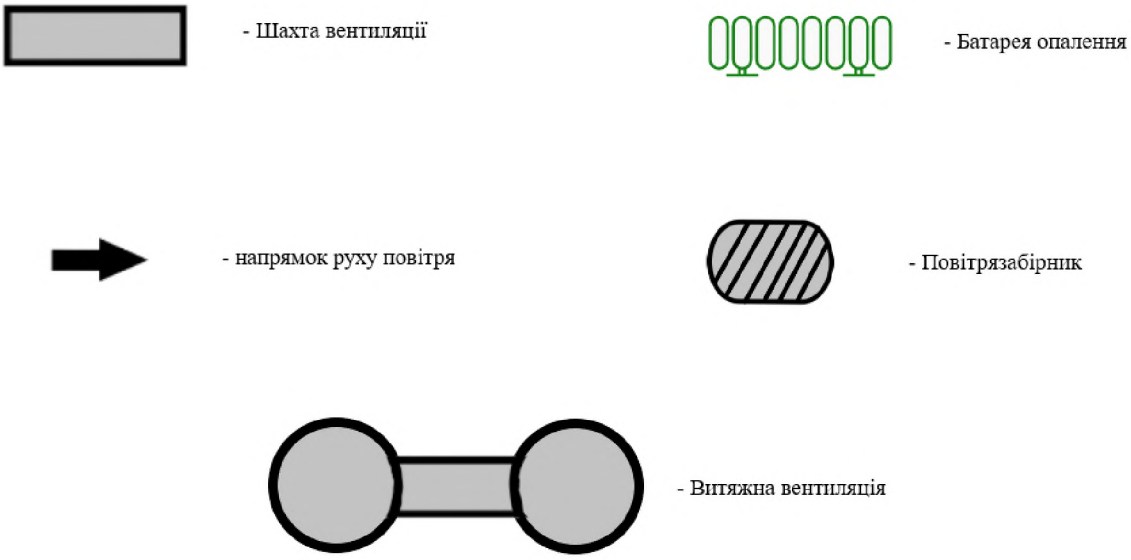
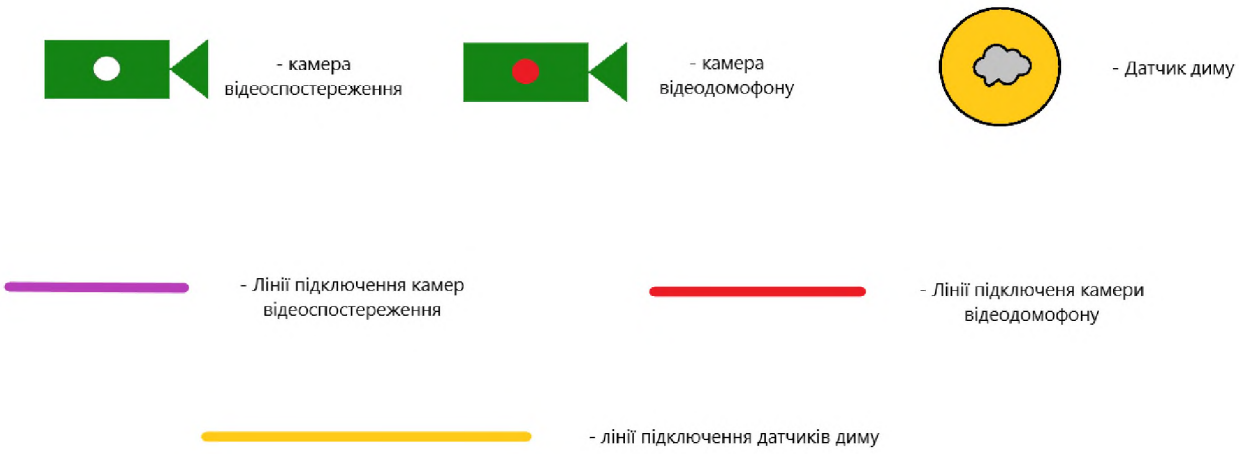


Рисунок 1.4 - План протипожежної системи та системи відеоспостереження



Умовні позначення вентиляції та системи опалення



Умовні позначення плану протипожежної системи та системи відеоспостереження

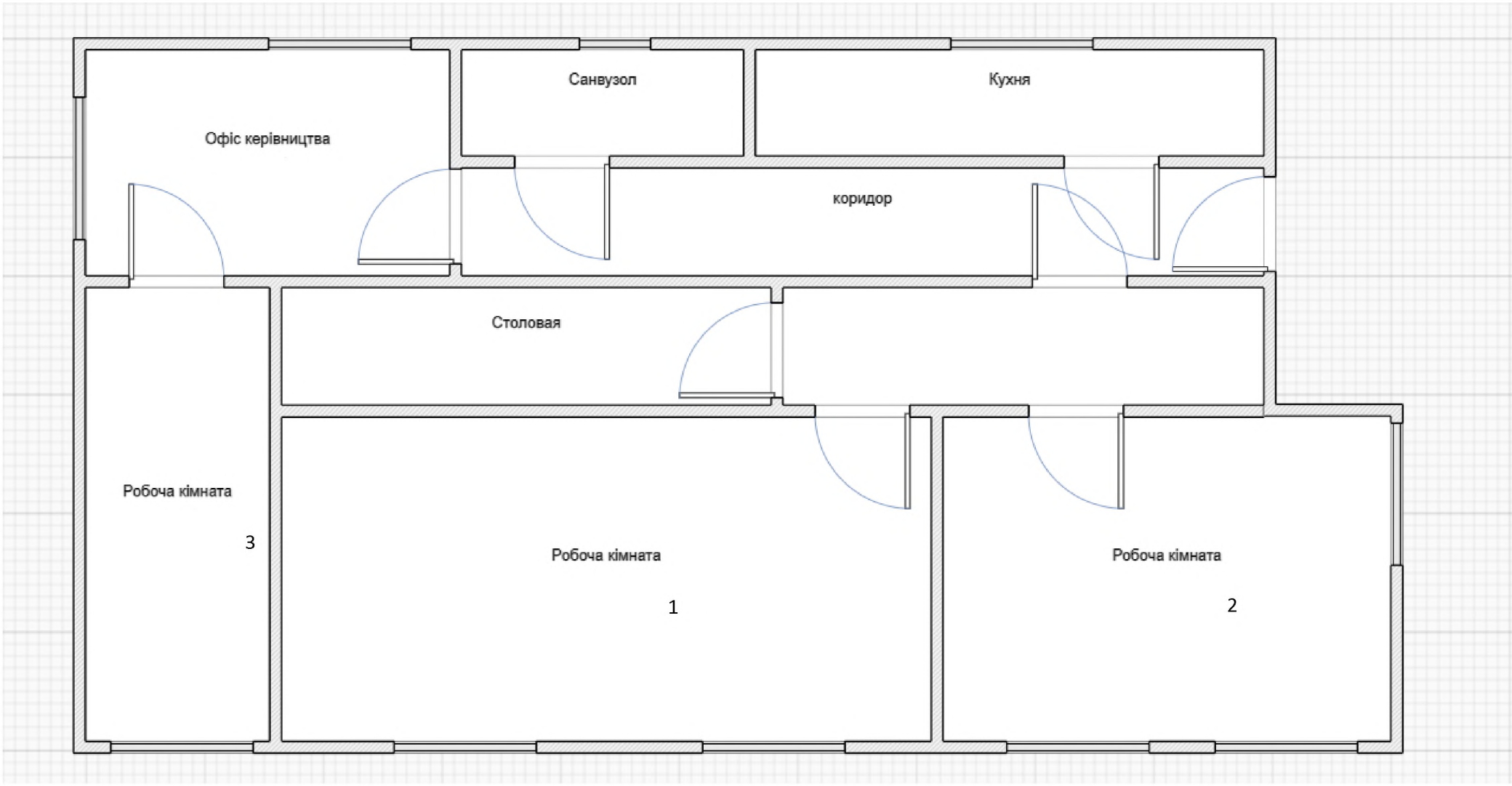


Рисунок 1.5 - Найменування кімнат

Таблиця 1.3 – Інвентаризаційна відомість апаратного забезпечення ІТС

Назва	Марка	Модель	Серійний номер	Розміщення (рисунок 1.5)	Відстань до границі ОІД, м
Ноутбук	HP	255 G8 (32P18EA)	295419	Робоча кімната 2 на столі	0,5
Ноутбук	HP	255 G8 (32P18EA)	141969	Робоча кімната 2 на столі	0,5
Ноутбук	HP	255 G8 (32P18EA)	456876	Робоча кімната 2 на столі	0,5
Ноутбук	HP	255 G8 (32P18EA)	789676	Робоча кімната 2 на столі	1,5
Ноутбук	HP	255 G8 (32P18EA)	453196	Робоча кімната 1 на столі	0,5
Ноутбук	HP	250 G7 (1L3L8EA)	456453	Робоча кімната 1 на столі	0,5
Ноутбук	HP	250 G7 (1L3L8EA)	156456	Робоча кімната 1 на столі	0,5
Ноутбук	HP	250 G7 (1L3L8EA)	34456	Робоча кімната 1 на столі	1,5
Ноутбук	HP	250 G7 (1L3L8EA)	545646	Робоча кімната 3 на столі	0,5
Ноутбук	HP	250 G7 (1L3L8EA)	546456	Робоча кімната 3	0,5
Ноутбук	HP	250 G7 (1L3L8EA)	456456	Робоча кімната 3 на столі	0,5
Ноутбук	HP	250 G8 (2X7K9EA)	4564318	Офіс керівництва на столі	0,5
Ноутбук	HP	250 G8 (2X7K9EA)	8797456	Офіс керівництва на столі	0,5
Ноутбук	HP	250 G8 (2X7K9EA)	7897852	Робоча кімната 1 на столі	2,5

Продовження таблиці 1.3 – Інвентаризаційна відомість апаратного забезпечення ІТС

Ноутбук	HP	250 G8 (2X7K9EA)	564687	Робоча кімната 2 на столі	0,5
Гарнітура дротова	Sven	AP-151MV	416549	Робоча кімната 2 на столі	1,5
Гарнітура дротова	Sven	AP-151MV	645678	Робоча кімната 2 на столі	0,5
Гарнітура дротова	Sven	AP-151MV	786543	Робоча кімната 2 на столі	0,5
Гарнітура дротова	Sven	AP-151MV	789645	Офіс керівництва на столі	0,5
Гарнітура дротова	Sven	AP-151MV	976876	Офіс керівництва на столі	0,5
Гарнітура дротова	Sven	AP-151MV	456456	Робоча кімната 1 на столі	0,5
Гарнітура дротова	Sven	AP-151MV	423489	Робоча кімната 1 на столі	1,5
Гарнітура дротова	Sven	AP-151MV	896548	Робоча кімната 3 на столі	0,5
Гарнітура дротова	Sven	AP-151MV	789467	Робоча кімната 3 на столі	0,5
Гарнітура дротова	Sven	AP-151MV	546896	Робоча кімната 3 на столі	0,5
Wi-Fi роутер	Xiaomi	Mi AloT Router AC2350	164986	Коридор	3
Ксерокс	Canon	Pixma G2411	189413	Робоча кімната 3 на столі	0,5

Таблиця 1,4 – Інвентаризаційна відомість ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Датчик диму	Артон	СПД-3.4	475678	Робоча кімната 3 на стелі
Датчик диму	Артон	СПД-3.4	765789	Робоча кімната 2 на стелі
Датчик диму	Артон	СПД-3.4	459785	Робоча кімната 1 на стелі
Датчик диму	Артон	СПД-3.4	645689	Коридор на стелі
Датчик диму	Артон	СПД-3.4	954613	Офіс керівництва на стелі
Датчик диму	Артон	СПД-3.4	137487	Кухня на стелі
Датчик диму	Артон	СПД-3.4	785642	Столова на селі
Камера відеоспостереження	AHD	CDM-223S-IR	165482	Перед дверима до офісу у кутку зверху
Камера відеоспостереження	IMOU	IPC-K42P	064493	Куток кімнати 1 на стелі
Камера відеоспостереження	IMOU	IPC-K42P	782068	Куток кімнати 2 на стелі
Периферійний блок	Артон	-	162784	Коридор на стелі

Таблиця 1.5 – Характеристика складу ІТС

Назва	Назва в ІТС	Характеристика	Серійний номер	Відповідальний
Робоча станція	Lap#1	Экран 15.6” (1920x1080) Full HD, матовый / Intel Core i3-1005G1 (1.2 - 3.4 ГГц) / RAM 8 ГБ / SSD 512 ГБ / nVidia GeForce MX110, 2 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.78 кг / черный	295419	Агент
Робоча станція	Lap#2	Экран 15.6” (1920x1080) Full HD, матовый / Intel Core i3-1005G1 (1.2 - 3.4 ГГц) / RAM 8 ГБ / SSD 512 ГБ / nVidia GeForce MX110, 2 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.78 кг / черный	141969	Агент
Робоча станція	Lap#3	Экран 15.6” (1920x1080) Full HD, матовый / Intel Core i3-1005G1 (1.2 - 3.4 ГГц) / RAM 8 ГБ / SSD 512 ГБ / nVidia GeForce MX110, 2 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.78 кг / черный	456876	Агент
Робоча станція	Lap#4	Экран 15.6” (1920x1080) Full HD, матовый / Intel Core i3-1005G1 (1.2 - 3.4 ГГц) / RAM 8 ГБ / SSD 512 ГБ / nVidia GeForce MX110, 2 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.78 кг / черный	789676	Менеджер по претензіям
Робоча станція	Lap#5	Экран 15.6” (1920x1080) Full HD, матовый / Intel Core i3-1005G1 (1.2 - 3.4 ГГц) / RAM 8 ГБ / SSD 512 ГБ / nVidia GeForce MX110, 2 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.78 кг / черный	453196	Агент

Продовження таблиці 1.5 – Характеристика складу ІТС

Робоча станція	Lap#6	Экран 15.6” (1920x1080) Full HD, матовый / Intel Core i3-1005G1 (1.2 - 3.4 ГГц) / RAM 8 ГБ / SSD 512 ГБ / nVidia GeForce MX110, 2 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.78 кг / черный	456453	Агент
Робоча станція	Lap#7	Экран 15.6” SVA (1920x1080) Full HD, матовый / Intel Core i7-1165G7 (2.8 - 4.7 ГГц) / RAM 16 ГБ / SSD 512 ГБ / Intel Iris Xe Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / Windows 10 Pro 64bit / 1.74 кг / серый	156456	Директор
Робоча станція	Lap#8	Экран 15.6” SVA (1920x1080) Full HD, матовый / Intel Core i7-1165G7 (2.8 - 4.7 ГГц) / RAM 16 ГБ / SSD 512 ГБ / Intel Iris Xe Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / Windows 10 Pro 64bit / 1.74 кг / серый	34456	Оператор
Робоча станція	Lap#9	Экран 15.6” SVA (1920x1080) Full HD, матовый / Intel Core i7-1165G7 (2.8 - 4.7 ГГц) / RAM 16 ГБ / SSD 512 ГБ / Intel Iris Xe Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / Windows 10 Pro 64bit / 1.74 кг / серый	545646	Оператор
Робоча станція	Lap#10	Экран 15.6” SVA (1920x1080) Full HD, матовый / Intel Core i7-1165G7 (2.8 - 4.7 ГГц) / RAM 16 ГБ / SSD 512 ГБ / Intel Iris Xe Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / Windows 10 Pro 64bit / 1.74 кг / серый	546456	Бек супорт
Робоча станція	Lap#11	Экран 15.6” IPS (1920x1080) Full HD, матовый / AMD Athlon Silver 3050U (2.3 - 3.2 ГГц) / RAM 8 ГБ / SSD 256 ГБ / AMD Radeon Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.74 кг / черный	456456	Агент

Продовження таблиці 1.5 – Характеристика складу ІТС

Робоча станція	Lap#12	Экран 15.6” IPS (1920x1080) Full HD, матовый / AMD Athlon Silver 3050U (2.3 - 3.2 ГГц) / RAM 8 ГБ / SSD 256 ГБ / AMD Radeon Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.74 кг / черный	4564318	Агент
Робоча станція	Lap#13	Экран 15.6” IPS (1920x1080) Full HD, матовый / AMD Athlon Silver 3050U (2.3 - 3.2 ГГц) / RAM 8 ГБ / SSD 256 ГБ / AMD Radeon Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.74 кг / черный	8797456	Агент
Робоча станція	Lap#14	Экран 15.6” IPS (1920x1080) Full HD, матовый / AMD Athlon Silver 3050U (2.3 - 3.2 ГГц) / RAM 8 ГБ / SSD 256 ГБ / AMD Radeon Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.74 кг / черный	7897852	Агент
Робоча станція	Lap#15	Экран 15.6” IPS (1920x1080) Full HD, матовый / AMD Athlon Silver 3050U (2.3 - 3.2 ГГц) / RAM 8 ГБ / SSD 256 ГБ / AMD Radeon Graphics / без ОД / LAN / Wi-Fi / Bluetooth / веб-камера / DOS / 1.74 кг / черный	564687	Агент
Wi-Fi роутер	WiFi#1	Интерфейсы 3 порта LAN 10/100/1000 Мбит/с 1 порт WAN 10/100/1000 Мбит/с WAN-порт Ethernet Скорость Wi-Fi 2183 Мбит/с	164986	Бек супорт
Ксерокс	Ксерокс	Максимальное разрешение печати 1200x4800 dpi Количество цветов 4	189413	Бухгалтер

Таблиця 1.6 – Інвентаризаційна відомість програмного забезпечення ІТС

Назва	Тип	Опис	Тип ліцензії	Встановлено
Windows 10 Версія 20H2	Системне	Операційна система для персональних комп'ютерів та робочих станцій	Commercial	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15
Microsoft outlook (версія 18)	Прикладне	Програми для роботи в комп'ютерній мережі	Commercial	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15
Google Chrome (версія 80.2.4120)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15
WinRar (версія 5.90)	Системне	Архіватор файлів	Shareware	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15
Microsoft Word 2010	Прикладне	Програма для створення, редагування текстових файлів	Commercial	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15

Продовження таблиці 1.6 – Інвентаризаційна відомість програмного забезпечення ІТС

Viber (версія 15.4.0.6)	Прикладне	Програма для Інтернет дзвінків та повідомлень	Freeware	Lap#7, Lap#8, Lap#9, Lap#10
Foxit PDF Reader (версія 10.1.4.37651)	Прикладне	Програма для створення, редагування текстових файлів	Commercial	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15
SoftCall (версія 10.06.12)	Прикладне	Програма для телефонних дзвінків	Commercial	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15
Magic Jack (версія 21.06.17)	Прикладне	Програма для телефонних дзвінків	Commercial	Lap#7, Lap#8, Lap#9, Lap#10
Google Drive (версія 2.21.201.08.32)	Прикладне	Програма для зберігання інформації у хмарному сховищі	Freeware	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15
ESET SMART SECURITY PREMIUM (версія 14.2.10.0 Final)	Системне	Антивірусна програма	Commercial	Lap#1, Lap#2, Lap#3, Lap#4, Lap#5, Lap#6, Lap#7, Lap#8, Lap#9, Lap#10, Lap#11, Lap#12, Lap#13, Lap#14, Lap# 15

Опис структурної системи

Структурна схема являє собою локальну систему з виходом в Internet. Усі працівники мають вихід до Інтернету. В центрі системи знаходиться комутатор(його роботу виконує WI-FI роутер). До нього під'єднані інші комп'ютери, така структура називається «пасивною зіркою». Також ксерокс приєднується до будь я кого ноутбуку.

Опис інформаційних потоків

На ОІД обробляється така інформація, як:

1) Інформація про перевізників
2) Інформація про клієнтів компанії
3) Бухгалтерські звіти компанії
4) Інформація про вантажі, які перевозяться

Вищеописані інформаційні потоки описані в таблиці 1.7. Дана інформація обробляться такими працівниками компанії, як Директор, бухгалтер, два оператори, бек супорт, та десять агентів. (таблиця 1.8)

Інформація про перевізників отримується з відкритих ресурсів, та за допомогою дзвінків. Ця інформація зберігається в спеціальному програмному продукту CRM, яка зберігається на сервері компанії. Усі працівники компанії мають доступ до редагування, копіювання та запису даної інформації.

Інформація про клієнтів компанії зберігається на он-лайн дошках Excel операторами. Доступ до даної інформації мають оператори, бек супорт та директор. Вони мають право редагувати, копіювати та записувати цю інформацію. Більше всього з цією інформацією працюють оператори, вони знаходять інформацію через відкриті ресурси, та за допомогою баз даних інших клієнтів.

Бухгалтерські звіти компанії формуються бухгалтером та зберігаються на он-лайн дошках Excel, доступ до яких мають тільки менеджер директор та бухгалтер. Всі вони мають право редагувати, копіювати та записувати цю інформацію.

Інформація про грузи, які перевозяться зберігається на он-лайн дошках Excel, програмі CRM та Microsoft Outlook. До он-лайн дощок Excel мають доступ усі працівники, але право редагувати інформацію мають тільки оператори та директор. В програмі Microsoft Outlook оператори отримують інформацію про тип вантажів, та їх

унікальні номери, як тільки оператори отримують дану інформації вони відправляють її бек супорту, який створює документацію для перевезення. У програмі CRM зберігається інформація про тип вантажу, місце відправлення та отримання вантажу.

Таблиця 1.7 – Інформація, яка циркулює на ОІД

Вид інформації	Режим доступу	Правовий режим	Вид представлений в ІТС	Вимоги до захисту		
				К	Ц	Д
Інформація про перевізників	Відкрита	-	Текстова	К1	Ц1	Д5
Інформація про клієнтів компанії	Обмежений доступ	Конференційна	Текстова	К2	Ц4	Д5
Інформація про вантажі	Тимчасово Обмежений доступ	Конференційна	Текстова, графічна	К3	Ц2	Д5
Бухгалтерські звіти	Обмежений доступ	Службова	Текстова, графічна, числова	К3	Ц3	Д3

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;

К5 - критичний рівень конфіденційності інформації, що може призвести до крахукомпанії 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 не значних збитків у разі втрати цілісності інформації;

Ц3 - рівень цілісності інформації, при якому організація зазнає відчутних збитківу 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 втратоюдоступності інформації;

Д2 рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

Д4 - рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

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

Опис середовища користувачів

До персоналу підприємства входять: Директор підприємства, два оператори, 10 агентів, менеджер по претензіям, менеджер, бухгалтер та бек супорт.

Директор займається закупівлею обладнання та програмного забезпечення, працює з клієнтами у випадках непередбачених обставин. Перевіряє якість роботи.

Оператори займаються пошуком клієнтів, отримання від них заказів на перевезення, інформування клієнтів о статусі перевезення, формування он-лайн дощок заказів для агентів, формуванням бази даних про клієнтів.

Агенти займаються пошуком перевізників, перевірки їх ліцензій та страхових документів, підбором для перевізників вантажів, підтримують зв'язок з перевізником

під час перевезення та оновленням інформації про статус доставки, отриманням документації про успішну доставку та її перевірки.

Бек супорт перевіряю перевізників у системі TMS, відправлення договору про взаємно працю, якщо він не підписаний перевізником, складає документацію про перевезення та підтвердження оплати, перевіркою документації про отримання вантажу, та виставлення рахунків клієнту. Оновлює інформацію про перевезення у системі TMS. Контролює діяльність агентів та операторів, та перевіряє їх роботу на випадки допущених помилок, та виправляє їх.

Бухгалтер контролює усі платежі, веде їх базу даних, та займається перевіркою невиплачених рахунків клієнтів.

Менеджер по претензіям займається роботою із страховими компаніями та клієнтами у разі пошкодження вантажу, отримую документ про успішну доставку у разі неможливості отримання їх агентами, або операторами у клієнтів.

Менеджер займається справами забезпечення персоналу необхідними ресурсами, контролю персоналу та їх роботи, допомагає в роботі директору та операторам.

До опису додається таблиця матриці розмежування доступу до інформації, КСЗІ та ресурсів

Таблиця 1.8 матриці розмежування доступу до інформації, КСЗІ та ресурсів

Користувач	Кількість працівників	Рівень кваліфікації	Інформація				Повноваження керувати КСЗІ	Ресурси
			Інформація про перевізників	Інформація про клієнтів компанії	Бухгалтерські звіти компанії	Інформація про вантажі, які перевозяться		
Директор	1	Високо кваліфіковані робітники	R,C,M,P,W,D,S	R,C,M,P,W,D,S	R,C,M,P,W,D,S	R,C,M,P,W,D,S	+	Lap#7
Менеджер	1	Високо кваліфіковані робітники	R,C,M,P,W,D,S	R,C,M,P,W,D,S	R,C,M,P,W,D,S	R,C,M,P,W,D,S	+	Lap#7
Оператор	2	Кваліфіковані працівники	R,C,M,P,W,D,S	R,C,M,P,W,D,S	-	R,C,M,P,W,D,S	-	Lap#8, Lap#9
Агент	10	Кваліфіковані працівники	R,C,M,P,W,D,S	R	-	R, S	-	Lap#1 - Lap#3, Lap#5, Lap#6, Lap#11 - Lap# 15
Бек супорт	1	Кваліфіковані працівники	R,C,M,P,W,D,S	R,C,M,P,W,D,S	-	R,C,M,P,W,D,S	-	Lap#10

Бухгалтер	1	Високо кваліфіковані робітники	-	R,C,P,S	R,C,M,P, W,D,S	-	-	Ксерокс
Менеджер по претензіям	1	Високо кваліфіковані робітники	R,C,M,P,W ,D,S	R,C,M,P, W,D,S	-	R,C,M,P,W ,D,S	-	Lap#4

Умовні позначення:

R	–	читання	W	–	запис (створення)
C	–	копіювання	D	–	видалення
M	–	модифікація	S	–	зберігання
P	–	друкування			

1.4 Висновок

Отже, можна сказати, що дана компанія має перелік нормативних документів, які становлять НПБ для даного підприємства. З точки зору безпеки інформації, у даних документах містяться такі види даних, як:

1) Персональні дані працівників компанії
2) Інформація про діяльність підприємства;
3) Підрозділи інформації підприємства, що становлять комерційну таємницю;
4) Договори з клієнтами підприємства, бази даних клієнтів.

Згідно із 9 статті Законів України «Про захист інформації в ІТС»:

«Відповідальність за забезпечення захисту інформації в системі покладається на власника система.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.»

Виходячи із вищеописаного терміну можна сказати, що встановлення питання про реалізацію КСЗІ затверджено на законодавчому рівні і стосується всіх видів підприємств комерційного або державного плану. Оскільки в НПБ були присутні документи в яких може міститися ІЗоД, то для даного типу організації необхідно проаналізувати ІТС даної структури, створити акти обстеження і загроз, вразливостей, моделі порушника та виходячи із даних документів розробити КСЗІ для даної компанії.

Також у даному розділі було детально обстежено ІТС з точки зору безпеки інформації та досліджено організаційні, програмно-апаратні аспекти в сфері ІБ даної компанії.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель загроз і порушника

Згідно із НД-ТЗІ 1.1-003-95 «Термінологія в галузі захисту інформації комп'ютерних систем від несанкціонованого доступу»:

«Модель загроз (model of threats) — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз, таблиця 2.3.

Модель порушника (user violator model) — абстрактний формалізований або неформалізований опис порушника», таблиця 2.1.

Тобто, виходячи із даної термінології можна сказати що виходячи із акту обстеження виконуються роботи пов'язані із розслідуванням можливих інформаційних дір, які можуть привести до порушення конфіденційності, цілісності або доступності інформації та інших її властивостей. Далі буде проведено процедури, пов'язані з виявленням негативних факторів впливу на ІТС.

Таблиця 2.1 – Категорія порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ3	М3	К2	З2	Ч1	Д3	16
	3	2	2	3	3	3	
	ПЗ5	М4	К2	З4	Ч1	Д3	19
	4	3	2	4	3	3	
Менеджер	ПВ3	М3	К2	З2	Ч1	Д3	16
	3	2	2	3	3	3	
	ПЗ5	М4	К2	З4	Ч1	Д3	19
	4	3	2	4	3	3	

Продовження таблиці 2.1 – Категорія порушників

Бухгалтер	ПВ1	М1	К1	З1	Ч4	Д3	10
	1	1	2	1	4	3	
	П35	М4	К3	З2	Ч4	Д3	21
	4	3	4	3	4	3	
Менеджер по претензіям	ПВ1	М1	К1	З1	Ч4	Д3	10
	1	1	2	1	4	3	
	П35	М4	К2	З4	Ч1	Д3	19
	4	3	2	4	3	3	
Агент	ПВ1	М2	К2	З1	Ч1	Д3	12
	1	2	2	1	3	3	
	П35	М4	К3	З2	Ч1	Д3	20
	4	3	4	3	3	3	
Оператор	П35	М4	К3	З2	Ч1	Д3	20
	4	3	4	3	3	3	
	П35	М4	К2	З4	Ч1	Д3	19
	4	3	2	4	3	3	
Бек супорт	ПВ1	М1	К1	З1	Ч4	Д3	10
	1	1	2	1	4	3	
	ПВ3	М3	К2	З2	Ч1	Д3	16
	3	2	2	3	3	3	

Таблиця 2.2 - Модель внутрішнього порушника політики безпеки інформації

Категорія порушника «ПВ»	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ2	М2	К3	З1	Ч4	Д4	17
Менеджер	ПВ2	М2	К3	З1	Ч4	Д4	17
Оператор	ПВ3	М3	К2	З2	Ч1	Д3	16
Бухгалтер	ПВ	М2	К2	З1	Ч1	Д3	12
Бек супорт	ПВ1	М2	К2	З1	Ч1	Д3	12
Менеджер по претензіям	ПВ1	М1	К2	З1	Ч4	Д3	10
Агент	ПВ1	М1	К1	З1	Ч1	Д2	9

Визначено, що найбільшу загрозу представляю співробітник ІТС, який виконує роль Директора та Менеджера. Дії осіб на даній посаді мають відстежуватися, оскільки вона є основним потенційним порушником ІБ на ІТС даного підприємства.

Модель загроз

Таблиця 2.3 - Перелік загроз з визначенням порушень властивостей інформації та ІТС

Загроза	Вразливість	Збиток	Ризики властивостей інформації
Загрози, пов'язанні з внутрішніми діями працівників			
Викрадення або знищення інформації	Недбале зберігання та облік документів, носіїв інформації, баз даних	Середній	К,Ц, Д
Несанкціоновані дії або помилки систем них адміністраторів	Несанкціоновані або помилкові дії адміністраторів (неправильне встановлення або оновлення ПЗ, ОС, систем сигналізації, неправомірне відключення засобів захисту ІТС)	Високий	К,Ц, Д

Помилки користувачів	Помилки користувачів (встановлення та запуск піратського, шкідливого ПЗ, самостійне оновлення системи, використання Інтернету в інших	Середній	К,Ц
Загрози, пов'язані з зовнішніми діями сторонніх людей			
Викрадення інформації	Несанкціоноване копіювання інформації на сторонні носії людьми, що не с працівниками підприємства через недбалість самих робітників	Середній	К
Промисловий шпіонаж	Неправильний підбір співробітників. Викрадення інформації, працюючи на підприємство конкурента.	Середній	К
Перехоплення інформації (ПЕМВН)	Витік з переймання ПЕМВН, які створюються технічними засобами	Середній	К
Хакінг	Виконання несанкціонованих дій на кінцевому пристроєві клієнта	Високий	К,Ц
Перехоплення інформації (візуально - оптичне)	Несанкціонований перегляд інформації за рахунок візуально - оптичного каналу через недбалість працівника	Низький	К
Загрози, пов'язані з внутрішніми технічними проблемами			
Недолік охоронної сигналізації	Не якісне технічне обладнання або не правильно встановлена система охоронної сигналізації	Високий	Ц,Д
Недолік пожежної сигналізації	Не якісне технічне обладнання або не правильно встановлена система пожежної сигналізації	Високий	К,Ц,Д

Збої в каналах зв'язку	Перевищення порогу допустимого навантаження на канали зв'язку або ж розрахункові ресурси системи	Середній	Ц,Д
Зношення технічного обладнання	Збої та відмови системи електроживлення, часті скачки напруги	Низький	Ц,Д
Зношення носіїв інформації, серверу	Збої або пошкодження носіїв інформації, серверної частини підприємства	Високий	Ц
Загрози природного походження			
Катастрофа	Пожежа, повінь, землетрус, техногенні аварії	Високий	Ц,Д

Висновки дослідження моделі загроз і порушника

Порушення конфіденційності інформації (інформації про продукт виготовлення компанії, про клієнтів та бухгалтерські звіти) сторонніми людьми за рахунок несанкціонованого копіювання на сторонні носії. Причина - відсутність режиму КЗ на території підприємства або недбалість працівників. Можливі наслідки - виток інформації, незначні фінансові втрати, шкода репутації підприємства та клієнтів.

Порушення конфіденційності інформації сторонніми людьми за рахунок витоку її з ПЕМВН, які створюються технічними засобами. Причина - відсутність пасивних та активних засобів захисту від ПЕМВН. Можливі наслідки - виток інформації, незначні фінансові втрати, шкода репутації підприємства та клієнтів.

Порушення конфіденційності та цілісності інформації (інформаціїї про продукт виготовлення компанії) співробітниками за рахунок людського фактору (встановлення та запуск піратського, шкідливого ПЗ, самостійне оновлення системи, використання Інтернету в інших цілях). Причина - недостатній контроль дій користувачів керівництвом. Можливі наслідки - виток інформації, фінансові втрати.

Порушення цілісності інформації на технічному обладнанні через поломку носіїв інформації або серверу. Причина - відсутність резервного копіювання. Можливі наслідки часткова/повна втрата інформації, великі фінансові втрати.

Порушення конфіденційності, цілісності та доступності інформації керівництвом за рахунок несанкціонованих або помилкових дій в ІТС (неправильне встановлення або оновлення ПЗ/систем сигналізації). Причина - корисливі дії персоналу, відсутність введення протоколів у журналі подій. Можливі наслідки — технічні збої.

З усіх наведених загроз, механізмів їх реалізації, імовірності, спрямованості, рівня шкоди та наслідків, можна зробити висновок, що помилки системних адміністраторів та користувачів, викрадення інформації, зношення носіїв інформації, серверу, перехоплення інформації с найнебезпечнішими та найактуальнішими загрозами для підприємства, що підлягають для негайної побудови нової політики ІБ. У наступних підрозділах буде розроблено КСЗІ і створено політику безпеки виходячи із зафіксованих загроз, уразливостей і порушень навмисного або ненавмисного характеру з боку осіб, які являються або не являються частиною ІТС.

2.2 Розробка КСЗІ

КД-4. Абсолютна довірча конфіденційність. Не реалізовано. ІТС не має достатню кількість ресурсів для розмежування через КЗЗ користувача, захищеного об’єкта і процесу

КД-3. Повна довірча конфіденційність. Частково реалізовано. У КЗЗ даної ІТС присутні апаратні та людські ресурси, які мають змогу визначати користувачу або групі користувачів процеси, які належать до його або їх домену конкретних користувачів або групи користувачів, які мають або не мають права ініціювати процес, але не мають можливості для розмежування через КЗЗ користувача, захищеного об’єкта і процесу.

КА-4, КА-3. Абсолютна, повна адміністративна конфіденційність. Не реалізовано. Дана політика не мас можливості відноситись до всіх об’єктів КС.

КА-2. Базова адміністративна конфіденційність. Реалізовано. КЗЗ даної ІТС мас програмно-апаратні механізми, які здатні надати можливість адміністратору або особі з відповідними повноваженнями через процедури керування доменами

визначати конкретних користувачів або групи користувачів, які мають права ініціювати процеси (Механізм: Система розмежування доступу до IP в ОС)

КО-1. Повторне використання об'єкта. Частково реалізовано. Через систему розмежування доступу облікових записів, користувачам може бути доступна інформація, в залежності від рівня доступу користувача до IP на програмному рівні, але процеси механічного розмежування неможливо реалізувати (наприклад, при завершенні роботи система не мас можливості автоматично форматувати жорсткий диск)

КК-3. Перекриття прихованих каналів. Не реалізовано. КЗЗ даної ІТС не мас достатню кількість програмно-апаратних механізмів, які реалізують процедури ліквідації прихованих каналів.

КК-2. Контроль прихованих каналів. Реалізовано. В системі даної ІТС присутні програмно-апаратні ресурси та механізми, які забезпечують реєстрацію підмножини прихованих каналів (Механізм: Система перевірки завантажених ресурсів і виявлення прихованих каналів (SCDR and DPC))

КВ-4, КВ-3. Абсолютна, повна конфіденційність при обміні. Не реалізовано. КЗЗ даної ІТС не має максимально можливу кількість програмно - апаратних ресурсів для повної взаємодії із об'єктами і інтерфейсними процесами в КС.

КК-2. Базова конфіденційність при обміні. Реалізовано. КЗЗ має достатню кількість програмно - апаратних ресурсів для забезпечення запитів імпортованих та експортованих ресурсів на підставі атрибутів доступу інтерфейсних процесів (Механізми: Віртуальна приватна мережа (VPN), механізми шифрування (PGP))

ЦД-4,3. Абсолютна, повна довірча цілісність. Не реалізовано. КЗЗ даної АС не мас достатню кількість програмно - апаратних ресурсів для повної реалізації даної політики.

ЦД-2. Базова довірча цілісність. Реалізовано. В системі присутні механізми, які займаються даною політику. КЗЗ має можливість розмежовувати користувачів та їх групи які мають право ініціювати процеси.

ЦА-4,3. Абсолютна, повна адміністративна цілісність. Не реалізовано Система не мас достатню кількість програмно-апаратних і людських ресурсів для повної реалізації даної політики.

ЦА-2. Базова адміністративна цілісність. Реалізовано. В системі присутні програмно-апаратні механізми і осіб, які можуть взаємодіяти з даними ресурсами, керувати потоками інформації. КЗЗ має можливість призначати користувача та їх групи і розмежовувати даних осіб на підставах атрибутів доступу. Групи користувачів взаємодіють з потоками інформації в ІТС (Механізм: Програмні продукти запису файлів та їх пересування (Microsoft Office, програми відправки файлів по ОС)

ЦО-2. Повний відкат. Частково реалізовано. ІТС має програмно-апаратні ресурси для регулювання відкату за будь-який проміжок часу, але ІР можуть бути відновлені вибірково.

ЦВ-3. Повна цілісність при обміні. Не реалізовано. Під час імпорту/експорту ІР відсутні механізми КЗЗ які здатні забезпечувати повну реалізацію даної політики.

ЦВ-2. Базова цілісність при обміні. КЗЗ даної АС має програмно-апаратні механізми, які створюють умови імпорту/експорту. Адміністратори або користувачі з відповідними повноваженнями мають можливості створити умови на імпорт/експорт ІР та присвоєння чи зміни рівня захищеності (Механізм: Утиліта перевірки вагової частки завантажених файлів).

ДР-3, ДР-2. Приорітетність використання ресурсів, недопущення перехоплення ресурсів. Не реалізовано. Політика не відноситься до всіх об'єктів в КС.

ДР-1. Квоти. Реалізовано. В КЗЗ присутні програмно-апаратні механізми, які регулюють циркуляцію ІР в КС (Механізм: Програма обліку робочого часу користувачів).

ДС-3. Стійкість без погіршення обслуговування. Не реалізовано. КЗЗ даної АС не має достатню кількість програмно-апаратних ресурсів, для підтримки системи без погіршених умов у результаті відмови одного або декількох компонентів.

ДС-2. Стійкість з погіршенням характеристик обслуговування. Реалізовано. В системі присутні програмно-апаратні ресурси, які підтримують діяльність ІТС у погіршених умовах у результаті відмови одного або множини компонентів (Механізм: Звернений проксі, резервний сервер).

ДЗ-3, ДЗ-2. Заміна будь-якого компонента, обмежена гаряча заміна. Не реалізовано. КЗЗ не має можливості модернізації або заміни будь-якого компонента або конкретної множини компонентів без переривання обслуговування.

ДЗ-1. Модернізація. Реалізовано. КЗЗ даної ІТС має призначену особу з відповідними повноваженнями, яка має право переривати діяльність ІТС з метою виконання ремонтних робіт або модернізації компонентів в АС.

ДВ-3, ДВ-2. Вибіркове, автоматично відновлення. Не реалізовано. КЗЗ не має програмно-апаратних ресурсів для відновлення і приведення до нормального стану КС у автоматичному режимі.

ДВ-1. Ручне відновлення. Реалізовано. У результаті збою КС в АС присутні особи з відповідними повноваженнями, які приводять КС до нормального стану або стану з обмеженими умовами у ручному режимі. У результаті виконання даної процедури КС тимчасово не доступний.

НР-5. Аналіз у реальному часі. Не реалізовано. КЗЗ не має функцій або програмно-апаратних механізмів для реєстрації НСД або інших подій у реальному часі.

НР-4. Детальна реєстрація. Реалізовано. В КЗЗ присутні програмно - апаратні ресурси, які забезпечують захист журналу подій від НСД або іншого негативного впливу на даний продукт. Адміністратори і користувачі з відповідними повноваженнями здатні аналізувати журнал подій використовуючи засоби для перегляду реєстраційних подій (Механізм: Журнал подій ОС, утиліта Anti-Red для журналу подій з системою блокування до редагування або іншого негативного впливу на реєстраційні події).

НИ-3. Множинна ідентифікація та автентифікація. Частково реалізовано. Система має 1 програмно-апаратний механізм для перевірки користувача в ІТС. Необхідність надання додаткових програмно-апаратних механізмів встановлюється власником ІТС (Механізм: ПКП із налаштованим механізмом бази даних паролів, система ідентифікації ОС (даний механізм присутній, але не активний)).

НК-2. Двонаправлений достовірний канал. Не реалізовано. КЗЗ даної АС не надав користувачеві повного керування зв'язком. Зв'язок не може ініціюватися з боку КЗЗ.

НК-1. Однонаправлений достовірний канал. Реалізовано. В системі присутні механізми, які керують даною процедурою з боку користувача (Механізм: Програма передачі файлів ОС, Bluetooth).

НО-3. Розподіл обов'язків на підставі привілеїв. Нереалізовано. Політика розподілу в системі не визначає множину користувачів.

НО-2. Розподіл обов’язав адміністраторів. Частково реалізовано. В системі присутні механізми, які керують діяльністю обов'язків адміністраторів, але активувати дані програмно-апаратні ресурси та призначити відповідних осіб можливо за бажанням власника ІТС. АС мас особу, яка виконує функцію адміністратора системи та адміністратора безпеки.

НЦ-3, НЦ-2. КЗЗ з функціями диспетчера доступу, гарантованою цілісністю. Не реалізовано. КЗЗ не мас достатню кількість програмно-апаратних ресурсів для підтримки власних доменів від зовнішніх впливів, НСД та інших негативних випадків.

НЦ-1. КЗЗ з контролем цілісності. Реалізовано. Система мас програмні ресурси, які спрямовані на оповіщення адміністратора системи і блокування КС від негативного втручання до тих пір, доки адміністратор не приведе ресурс до нормального стану власноруч (Механізми: Система оповіщення ОС, VirusChecker, OSLocker).

НТ-3. Самотестування у реальному часі. не реалізовано. Система не має програмно-апаратних механізмів для тестування КС у реальному часі.

НТ-2. Самотестування при старті. Частково реалізовано. В КЗЗ присутні механізми, які реалізують дану політику, проте активація даної функції можлива за наказом власника ІТС. (Механізм: Антивірусне ПЗ із механізмом потоку вірусів, хробаків та ін. при старті ОС).

НВ-3, НВ-2. Автентифікація з підтвердженням, автентифікація джерела. Не реалізовано. В КЗЗ відсутні механізми захисту, які встановлюють джерело кожного об’єкта, що експортується або імпортується в КС.

НВ-1. Автентифікація вузла. Реалізовано. КЗЗ присутні механізми для реєстрації вузла або вузлів, які імпортують або експортують об’єкти в КС. (Механізм: Wireshark, Nmap).

НА-2. Автентифікація відправника з підтвердженням. Не реалізовано. Система не мас департаментів, відділів або третіх осіб, які можуть однозначно підтвердити відправника завдяки протоколам автентифікації або інших механізмів.

НА-1. Базова автентифікація відправника. В КЗЗ присутній механізм, який фіксує множину властивостей і атрибутів об'єкта що передається користувачем - відправником (Механізм: Програма для створення та використання електронно - цифрового підпису (OpenSSL)).

НП-2. Автентифікація одержувача з підтвердженням. Не реалізовано. Система не мас департаментів, відділів або третіх осіб, які можуть однозначно підтвердити одержувача завдяки протоколам автентифікації або інших механізмів.

НП-1. Базова автентифікація одержувача. КЗЗ наявний механізм, який здатний автентифікувати одержувача. Система визначає множину властивостей і атрибутів об'єкта що отримується користувачем-одержувачем (Механізм: Утиліта для перевірки електронно-цифрового підпису (OpenSSL)).

Рекомендаційними вирішеннями окрім реалізації КСЗІ з боку програмно - апаратних галузей буде налаштування організаційних аспектів, які налаштують циркуляцію інформації в ІТС. Наступним шляхом буде створено політики, які дозволять забезпечити порядок та послідовність інформаційних потоків в ІТС і мінімізують негативний вплив на ІТС.

2.3 Розробка політики безпеки

Згідно із НД-ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації комп'ютерних систем від несанкціонованого доступу»:

«Політика безпеки інформації (information security policy) — сукупність законів, правил, обмежень, рекомендацій, інструкції тощо, які регламентують порядок обробки інформації».

Тобто, можна сказати що політика безпеки представляю собою перелік нормативних документів, правил законів які забезпечують поведінку потоків інформації в ІТС. Нижче буде наведено декілька політик різнопланового характеру які встановлять стандарти для циркуляції інформації в АС.

Політика шифрування

Останній статус оновлення: оновлено травень 2021 року.

Метою цієї політики є надання вказівок, які обмежують використання шифрування для тих алгоритмів, які отримали істотне та публічне дослідження і було доведено, що вони ефективно працюють. Крім того, ця політика створює напрямок

для забезпечення і дотримання федеральних норм та надання законних повноважень щодо розповсюдження і використання технологій шифрування.

Сфера застосування

Ця політика поширюється на всіх співробітників компанії «Лан-тайм» та їх філій.

Політика

Вимоги до алгоритму

Шифри, що використовуються, повинні відповідати або перевищувати набір, визначений як "AES-сумісний" або ”частково сумісний з AES" відповідно до каталогу шифрів IETF / IRTF або набору, визначеного для використання в Державній службі спеціального зв’язку України. НД-ТЗІ, ДСТУ або будь-які замінені документи відповідно до дати впровадження. Для симетричного шифрування настійно рекомендується використовувати розширений стандарт шифрування (AES).

Використовувані алгоритми повинні відповідати стандартам, визначеними у Держспецзвязку або будь-якому заміненому документі, відповідно до дати впровадження. Для асиметричного шифрування настійно рекомендується використовувати алгоритми RSA та криптографії Еліптичної кривої (ECC).

Алгоритми підпису Алгоритм довжини ключа

RSA 2048 Потрібно використовувати захищену схему прокладки.

Рекомендується схема прокладки PKCS №7. Потрібне хешування повідомлень. LDWM SHA256 Зверніться до чернетки підписів на основі LDWM.

Вимоги до функції кешу

Загалом, «Лан-тайм» дотримується політики охоронної служби

«ГАРДА» щодо функцій кешу.

Ключова угода та автентифікація

Обмін ключами повинен використовувати один з наступних криптографічних протоколів: Diffie-Hellman, IKE, або Еліптична крива Diffie- Hellman (ECDH).

Кінцеві точки повинні бути аутентифіковані до обміну або виведення ключів сеансу.

Публічні ключі, що використовуються для встановлення довіри, повинні бути аутентифіковані перед використанням. Приклади аутентифікації включають передачу через криптографічно підписане повідомлення або ручну перевірку кешу відкритого ключа.

Усі сервери, що використовуються для аутентифікації (наприклад, RADIUS або TACACS), повинні мати встановлений дійсний сертифікат, підписаний відомим надійним постачальником.

Усі сервери та програми, що використовують SSL або TLS, повинні мати сертифікати, підписані відомим надійним постачальником.

Генерація ключів

Криптографічні ключі повинні бути створені та збережені безпечним чином, що запобігає втраті, крадіжці або компрометації.

Генерування ключів повинно бути посіяне з галузевого стандартного генератора випадкових чисел (RNG).

Дотримання політики Вимірювання відповідності

Охоронна служба «ШЕРИФ» перевірить відповідність цій політиці за допомогою різних методів, включаючи, але не обмежуючись ними, звіти про бізнес-інструменти, внутрішні та зовнішні аудити та зворотній зв'язок з власником політики.

Винятки

Будь-який виняток із політики повинен бути затверджений командою Infosec заздалегідь.

Недотримання

Працівник, який порушив умови цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

Політика зберігання інформації в ITC

Останній статус оновлення: оновлено квітень 2021 року

Опис

Дана політика може бути інструментом імпорту, щоб гарантувати, що всі чутливі / конфіденційні матеріали не видаляться з робочої області кінцевого користувача та блокується, коли елементи не використовуються або с працівник залишає свою робочу станцію. ЦС одна з найкращих стратегій, яку потрібно використовувати при спробі зменшити ризик порушення безпеки на робочому місці. Така політика також може зростити обізнаність працівника щодо захисту конфіденційної інформації.

Призначення

Метою цієї політики е встановлення мінімальних вимог щодо підтримки

«чистоти» де знаходиться ІЗоД, комерційна та конфіденційна інформація про працівників, інтелектуальну власність, клієнтів та постачальників захищені у замкнених місцях та поза сайтом. Дана політика с частиною стандартного базового контролю конфіденційності.

Сфера застосування:

Ця політика поширюється на всіх співробітників «Лан-тайм» та їх філій.

Політика:

- Співробітники зобов'язані забезпечити всю критичну інформацію на твердій копії або в електронний формі, яка захищена в робочій зоні, наприкінці дня та протягом тривалого періоду.

Робочі станції комп'ютерів повинні бути заблоковані, коли робоча область незайнята.

Робочі станції комп'ютерів повинні бути повністю вимкнені наприкінці робочого дня.

Будь-яку критичну інформацію необхідно вийняти з письмового столу та зафіксувати у спеціально відведених місцях, зазначених власником ІТС в кінці робочого дня.

- Файлові шафи, що містять критичну інформацію, слід закрити та заблокувати, коли об'єкт не використовується або коли він не відвідується.

Механізми та засоби, які використовуються для доступу до ІзОД або конфіденційної інформації, не повинні залишатися в полі без нагляду.

Ноутбуки повинні бути або заблоковані замикаючім кабелем, або зафіксовані у шухляді.

Паролі не можуть залишатися на клейких нотатках, розміщених на комп'ютері або під ними, а також не можуть бути записаними у доступних місцях.

Роздруківки, що містять ІЗоД, мають бути негайно вилучені з принтера.

Утилізацію критичних документів слід проводити у спеціально відведених місцях власником ІТС або довіреними особами з відповідними повноваженнями. Дана інформація повинна бути роздрібнена спеціальними механізмами або заблокована у файлових шафах або сейфах.

Білі дошки, що містять критичну інформацію, слід стерти.

Портативні обчислювальні пристрої, такі як ноутбуки та планшети повинно бути заблоковано.

Фіксуйте в ІТС пристрої масового зберігання, такі як накопичувачі CDROM, DVD або USB які можуть містити критичну інформацію. Закріпіть їх у спеціально відведених місцях для їх зберігання (сейфи, шафи тощо)

Усі принтери та факсимільні машини повинні бути очищені від паперів, як тільки вони надруковані. Це допомагає переконатися, що конфіденційні документа не залишаються на лотках для принтера, щоб порушник ІТС не вчинив негативний вплив на ІС підприємства.

Дотримання політики

Вимірювання відповідності

Охоронна служба «ШЕРИФ» перевірить відповідність цій політиці за допомогою різних методів, наприклад фізичним оглядом, відеомоніторингом, звітами про бізнес-інструменти, внутрішніми та зовнішніми ревізіями та відгуками власника політики.

Винятки

Будь-який виняток із політики повинен бути затверджений Охоронною службою «ШЕРИФ» заздалегідь.

Недотримання

Працівник, який спричинив порушення цієї політики, може бути підданий дисциплінарному стягненню аж до припинення роботи.

Також коронно службою «Шериф» було установлено комплект обладнання AJAX StarterKit. До якого входять ИК датчик, датчик відкриття, тривожна кнопка, та централь.

2.4 Висновок

Підводячи підсумки можна сказати, що у даному розділі було детально обстежено ІТС з точки зору безпеки інформації та досліджено організаційні, програмно-апаратні аспекти в сфері ІБ даної компанії. Зазначено дані фактори було за допомогою нормативних документів, затверджених із стандартами Держспецзвязку і розроблено методи боротьби із зафіксованими загрозами та вразливостями.

Проте на реалізацію даних політик, механізмів захисту тощо необхідні ресурси. У наступному розділі буде розглянуто економічні фактори, які впливають на

економічне середовище компанії, розраховано витрати на реалізацію політик безпеки та КСЗІ, їх підтримку і надано рекомендації стосовно мінімізації витрат на реалізацію продуктів з галузі безпеки інформації.

Розділ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Розробка політики безпеки комп'ютерної мережі потребує обґрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічний ефект від впровадження та налагодження систем політики безпеки комп'ютерної мережі.

3.1 Розрахунок (фінансових) капітальних втрат

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

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

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

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д},$$ годин,

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

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

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

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

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

$t_{д}$ – тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=18 годин, $t_{в}$=30 годин, $t_{а}$=17 годин, $t_{вз}$=18 годин, $t_{озб}$=8 годин, $t_{овр}$=8 годин, $t_{д}$=11 годин. Отже,

$$t=18+30+17+18+8+8+11= 110 \text{ годин.}$$

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

Розрахуємо витрати на створення ПБ. Розрахунок проводиться за формулою (3.1):

$$Крп = Ззп + Змч \text{ , грн.,} \qquad (3.1)$$

де $К_{рп}$ - витрати на створення політики безпеки;

$З_{зп}$ - заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ - вартість витрат машинного часу, що необхідні для створення ПБ.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою (3.2):

$$Ззп = t \cdot Зіб, грн, \qquad (3.2)$$

де t - загальна тривалість розробки політики безпеки, годин;

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

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить - 75 грн/год.

Відповідно до формули 3.2 , витрати на заробітну плату спеціаліста ІБ становлять:

$З_{зп}$ = 110 год · 75 грн/год,

$З_{зп}$ = 8250 грн.

У свою чергу, витрати машинного часу визначаються за формулою (3.3):

$$З_{мч}=t \cdot С_{мч} = 110 \cdot 9{,}33 = 1026 \text{ грн.}, \qquad (3.3)$$

де t - трудомісткість розробки політики безпеки інформації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою (3.4):

$$С_{мч} = P \cdot t_{нал} \cdot Се + \frac{Фзал \cdot На}{Fр} + \frac{Клпз \cdot Напз}{Fр} грн \qquad (3.4)$$

де P - 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.

$$С_{мч} = 1{,}6 \cdot 3 \cdot 1{,}68 + \frac{7100 \cdot 0{,}3}{1920} + \frac{1670 \cdot 0{,}2}{1920} = 9{,}33 \text{ грн.}$$

Витрати на створення ПБ становлять:

$К_{рп}$= 9276 грн.

Відповідно до розроблених рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі ТОВ «Лан-Тайм», а також рекомендацій та інструкції

по безпосередній роботі з системою планується використання антивірусу ESET SMART SECURITY PREMIUM, який вже встановлений на комп'ютерах підприємства та потребує лише подовження ліцензії.

Апаратні засоби, які необхідно придбати відповідно до розроблених рекомендацій, а саме AJAX StarterKit буде коштувати 5699грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто 1140 грн.

Таким чином, за формулою (3.5), капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 9276 + 5699 + 1140 = 16115 \text{ грн.} \quad (3.5)$$

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

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

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

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

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

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають за формулою (3.6):

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.} \quad (3.6)$$

$С = 0 + 132633,11 + 0 = 132633,11$ грн.

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

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

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн).

Витрати на керування системою інформаційної безпеки ($С_к$) складають за формулою (3.7):

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \qquad (3.7)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н = 0$ грн.).

Річні амортизаційні відрахування усього купленого обладнання із корисним строком використання 5 років, за прямолінійним методом нарахування амортизації складуть:

$С_а = 5699 / 5 = 1139,8$ грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), знаходиться за формулою (3.8):

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \qquad (3.8)$$

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 8000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$С_з = 8000 \cdot 12 + 8000 \cdot 12 \cdot 0,1 = 105600$ грн.

Ставка ЄСВ для всіх категорій платників з 01.01.2019 р. складає 22%.

$С_{єв} = 105600 \cdot 0,22 = 23232$ грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою (3.9):

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,} \qquad (3.9)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,6 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:

$$С_{ел} = 1,6 \cdot 1920 \cdot 1,68 = 5160,96 \text{ грн.} \qquad (3.9)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% ($С_{тос}$ = 16115·0,01=161 грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються за формулою 3.7 відповідно:

$С_к$ = 0+1139,8 +105600+5160,96+0+161 = 112061,76грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 112061,76грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

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, 2 години;

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

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 3 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (інженерів-програмістів), 9000 грн/міс;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн/міс;

$Ч_о$ – чисельність обслуговуючого персоналу (інженерів-програмістів), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 15 осіб;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 12000 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 12.

Упущена вигода від простою атакованого сегмента корпоративної мережі знаходиться за формулою (3.10):

$$U = П_п + П_в + V, \qquad (3.10)$$

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:

$$П_П = \frac{11000 \cdot 12}{176} \cdot 2 = 1500 \text{ грн.},$$

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

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових і знаходиться за формулою (3.11):

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.11)$$

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 $t_{ви}$:

$$П_{ви} = \frac{11000 \cdot 12}{176} \cdot 3 = 2250 \text{ грн.}$$

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

$$П_{пв} = \frac{9000 \cdot 1}{176} \cdot 1 = 51{,}13 \text{ грн.}$$

$П_в = 2250 + 51{,}13 = 2301{,}13$ грн.

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються за формулою (3.12), виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ}) \qquad (3.12)$$

$$V = \frac{12000000}{2080} \cdot (2 + 1 + 3) = 34615{,}38 \text{ грн.}$$

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

$$U = 1500 + 2301{,}13 + 34615{,}38 = 38416{,}51 \text{ грн.}$$

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

$$B = \Sigma_i \Sigma_n U = \Sigma_1 \Sigma_{12} 38416{,}51 = 460998{,}12 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається за формулою (3.13) з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.}, \qquad (3.13)$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (59%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$E = 460998{,}12 \cdot 0{,}59 - 112061{,}76 = 159927{,}13$грн.

3.3 Визначення та аналіз показників економічної ефективності інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки і знаходиться за формулою (3.14):

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \qquad (3,14)$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{159927.13}{16115} = 9,92 \text{ частки оди-ниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції знаходиться за формулою (3.15):

$$ROSI > (N_{деп} - N_{інф})/100), \qquad (3.15)$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (9 %).

Розрахункове значення коефіцієнта повернення інвестицій:

1,05 > (18 – 9)/100 = 1,05 > 0,09.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки і знаходиться за формулою (3.16):

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1,05} = 0,95 \text{ років} \qquad (3.16)$$

3.4 Висновок

Розробка систем політики безпеки ТОВ «Лан-Тайм» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 16115 грн., експлуатаційні – 112061,76 грн. Величина річного економічного ефекту складає 159927,13 грн. Коефіцієнт повернення інвестицій ROSI складає 9,92 грн/грн.

Висновки

Підводячи підсумки даної роботи можна сказати, що підприємства складають найважливішу інфраструктуру для підтримки економічного рівня будь-якої держави. Дані структури являються посередниками між суспільством і державою, надаючи велику кількість привілей: надання робочих міст, створення продукції, проектів, послуг тощо.

Проте дані організації будуть одними із перших, хто буде являтися жертвою нещасних випадків в сфері ІБ та інцидентів. Задля створення безпечних умов для існування даних компаній, держава повинна залучати органи, які займаються питаннями безпеки інформації.

В свою чергу органи повинні розробляти певні законопроекти, стандарти, правила та інші функції, які будуть забезпечувати безпечні умови для діяльності будь-якої організації.

На прикладі даної структури було розроблено стандарти ІБ підприємства, затверджених спеціалізованим органом з питань захисту інформації та телекомунікації. У роботі було створено нормативні документи і акти, які виявляють слабкі місця даного підприємства і запропоновано міри захисту, які знизять ризики реалізації зафіксованих загроз та вражливостей.

Перелік джерел

1) Нормативний документ СТЗІ. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. НД ТЗІ 1.1-005-07: [Електронний ресурс] – Режим доступу: https://tzi.com.ua/downloads/1.1-005-07.pdf
2) Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1. 1-002-99. — Київ: ДСТСЗІ СБ України, 1999. — 16 с. [Електронний ресурс] – Режим доступу: https://tzi.com.ua/downloads/1.1-002-99.pdf
3) ПОСТАНОВА від 29 березня 2006 р. N 373. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text
4) НД ТЗІ 1.3-001-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» [Електронний ресурс] – Режим доступу: https://tzi.com.ua/downloads/1.1-003-99.pdf
5) ДСТУ 2352-54 «Інформація та документація. Базові поняття. Терміни та визначення.» [Електронний ресурс] – Режим доступу: https://dbn.co.ua/load/normativy/dstu/dstu_b_a_2_4_4_2009/5-1-0-781
6) ДСТУ 2732:2004 «Діловодство і архівна справа. Терміни та визначення» [Електронний ресурс] – Режим доступу: https://vnm.vn.court.gov.ua/userfiles/27_2732-2004.pdf
7) Закон України: Про захист інформації в інформаційно-телекомунікаційних системах дев’ята стаття [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ	31	
6	А4	СПЕЦІАЛЬНА ЧАСТИНА	16	
7	А4	ЕКОНОМІЧНИЙ РОЗДІЛ	18	
8	А4	Висновки	1	
9	А4	Список літератури	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Пояснювальна записка Чирков М.В. docx
2. Пояснювальна записка Чирков М.В. pdf
3. Презентація Чирков М.В. pptx

Додаток В. Відгуки керівників розділу

Відгук керівника економічного розділу

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

Додаток Г. Відгук
на кваліфікаційну роботу бакалавра на тему:
Комплексна система захисту інформації інформаційно-телекомунікаційної системи товариства з обмеженою відповідальністю "Лан-Тайм"
Чиркова Микити Володимировича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 72 сторінках та містить 6 рисунків, 12 таблиць, 7 джерел та 4 додатка.

Мета роботи: визначення необхідності реалізації комплексу систем захисту інформації для підприємства, аналіз інформаційного поля компанії і розробка механізмів захисту в сфері інформаційної безпеки організації, розрахунок витрат на реалізацію проекту.

У кваліфікаційній роботі на прикладі даної структури було розроблено стандарти ІБ підприємства, затверджених спеціалізованим органом з питань захисту інформації та телекомунікації. У роботі було створено нормативні документа і акти, які виявляють слабкі місця даного підприємства і запропоновано міри захисту, які знизять ризики реалізації зафіксованих загроз та вразливостей.

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

За час дипломування Чирков М.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 «_____».

Керівник Корнієнко Валерій Іванов