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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Глушана Ростислава Сергійовича*

академічної групи *125-16-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційної системи товариства з обмеженою відповідальністю «СІМЛІ ЄЙР»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н. проф. Корнієнко В.І.			
розділів:				
спеціальний	ас. Мілінчук Ю.А			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст.в. Тимофєєв Д.С.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Глушану Ростиславу Сергійовичу*** **академічної групи** ***125-16-3***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему *Комплексна система захисту інформації інформаційної системи товариства з обмеженою відповідальністю «СІМЛІ ЄЙР»*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження ОІД, аналіз інформаційної системи підприємства, модель загроз, модель порушника.	29.04.2020
Розділ 2	Оцінка існуючого стану захисту, проектні рішення, реалізація проектних рішень, аналіз загроз після впровадження комплексу заходів.	22.05.2020
Розділ 3	Розрахунок економічної доцільності впровадження комплексу заходів.	29.05.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 12 рис., 16 табл., 4 додатка, 22 джерел.

Об’єкт дослідження: інформаційна система товариства з обмеженою відповідальністю «СІМЛІ ЄЙР».

Мета роботи: розробка рекомендацій щодо захисту ресурсів інформаційної системи товариства з обмеженою відповідальністю «СІМЛІ ЄЙР»

У спеціальній частині дана характеристика: безпеки інформації на підприємстві «СІМЛІ ЄЙР»; у роботі досліджено: вразливості інформації, яка обробляється на підприємстві; проведено аналіз: загроз для оброблювальної інформації; запропоновано: впровадження рекомендацій (розробка вимог з інформаційної безпеки, впровадження дизель-електростанції, а також технологій інтернет-еквайринг та DLP). В економічному розділі визначено: ефективність впровадження рекомендацій до КСЗІ.

Практичне значення роботи полягає у дослідженні та поліпшені комплексної системи інформації, що циркулює на ТОВ «СІМЛІ ЄЙР».

Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані для поліпшення та удосконалення систем безпеки.

КЛЮЧОВІ СЛОВА: ЗАГРОЗИ ВЛАСТИВОСТЕЙ ІНФОРМАЦІЇ, РІВНІ РІЗИКІВ ТА ЗБИТКІВ, КОНФЕДЕНЦІЙНІСТЬ ІНФОРМАЦІЇ.

РЕФЕРАТ

Пояснительная записка: 76 с., 12 рис., 16 табл., 4 приложения, 22 источников.

Объект исследования: информационная система общества с ограниченной ответственностью «СИМПЛИ ЭЙР».

Цель работы: разработка рекомендаций по защите ресурсов информационной системы общества с ограниченной ответственностью «СИМПЛИ ЭЙР»

В специальной части дана характеристика: безопасности информации на предприятии «СИМЛИ ЭЙР»; в работе исследованы: уязвимости информации, обрабатываемой на предприятии; проведен анализ: угроз для обрабатывающей информации; предложено: внедрение рекомендаций (разработка требований по информационной безопасности, внедрение дизель-электростанции, а также технологий интернет-эквайринг и DLP). В экономическом разделе определены: эффективность внедрения рекомендаций к КСЗИ.

Практическое значение работы состоит в исследовании и улучшенные комплексной системы информации, циркулирующей на ООО «СИМПЛИ ЭЙР».

Результаты проведенных в квалификационной работе исследований могут быть использованы для улучшения и усовершенствования систем безопасности.

КЛЮЧЕВЫЕ СЛОВА: УГРОЗЫ СВОЙСТВ ИНФОРМАЦИИ, УРОВЕНЬ РИСКИ И УБЫТКИ, КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ.

ABSTRACT

Explanatory note: 76 pages, 12 figures, 16 tables, 4 appendices, 22 sources.

Object of research: information system of SIMLY AIR Limited Liability Company.

Purpose: development of recommendations for the protection of resources of the information system of the limited liability company "SIMLY AIR"

In the special part the characteristic is given: information security at the SIMLY AIR enterprise; the paper investigates: vulnerabilities of information processed at the enterprise; analysis of: threats to processing information; proposed: implementation of recommendations (development of information security requirements, implementation of a diesel power plant, as well as Internet acquiring and DLP technologies). The economic section defines: the effectiveness of the implementation of recommendations to the CCIS.

The practical significance of the work lies in the study and improvement of a comprehensive information system circulating at SIMLY AIR LLC.

The results of research conducted in the qualification work can be used to improve and enhance security systems.

KEY WORDS: THREATS TO THE PROPERTIES OF INFORMATION, LEVELS OF RISKS AND LOSSES, CONFIDENTIALITY OF INFORMATION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

КСЗІ – комплексна система захисту інформації;

МПС – міжнародна платіжна система;

DLP – Data Leak Prevention (запобігання витоку інформації);

ТО – технічне обслуговування;

КСІБ – комп'ютерної системи інформаційної безпеки;

КЗ – контрольована зона;

ОІД – об’єкт інформаційної діяльності;

ІТС – інформаційна-телекомунікаційна система;

ІОД – інформація з обмеженим доступом;

ІБ – інформаційна безпека;

НД ТЗІ – нормативний документ технічного захисту інформації.

ЗМІСТ

ВСТУП

В сучасні дні інформація – це найцінніший бізнес-актив будь-якої компанії. Тому необхідно захищати цей актив від чого або кого небудь.

Інфраструктура підприємств розвивається швидше, ніж засоби її захисту, що залишає великий простір для діяльності як цікавих дослідників, так і зловмисників. Кожен співробітник повинен дотримуватись вимогам внутрішнім документам підприємства, регулюючих доступ, використання та розголошення Конфіденційної інформації.

Надійний захист інформації, що циркулює на підприємстві неможливо забезпечити не аналізуючи обладнання та захист підприємства на можливі загрози та вразливості. Не впроваджуючи нових систем та технологій захисту інформації буде все частіше викрадення цієї інформації.

Комплексна система захисту інформації — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів та інше;

Актуальність теми даного кваліфікаційного проекту визначається:

- збільшенням інформаційних та технічних вразливостей підприємства;
- рівнем розвитку та сучасними темпами методів забезпечення захисту інформації, які в значній мірі відстають від рівня розвитку сучасних інформаційних технологій.

Метою дослідження є аналіз систем безпеки підприємства та обґрунтування вибору профілю захищеності конфіденційної інформації, що циркулює на ТОВ «СІМЛІ ЄЙР».

Для досягнення поставленої мети у кваліфікаційній роботі необхідно вирішити наступні завдання:

- розгорнуто проаналізувати систему безпеки підприємства;
- дослідити ОІД з точки зору безпеки;
- виконати аналіз вразливостей інформації з обмеженим доступом;
- побудувати модель порушника;
- розробити аналіз загроз для оброблювальної інформації на ТОВ «СІМЛІ ЄЙР»;
- розробити вимоги з інформаційної безпеки;
- рекомендації про використання комплексної системи захисту інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Загальні відомості про організацію (підприємство) замовника робіт ТОВ «СІМЛІ ЄЙР».

Повна юридична назва: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСЮ СІМЛІ ЄЙР.

Форма власності: товариство з обмеженою відповідальністю.

Напрям діяльності: діяльність в області комп'ютерного програмування, діяльність інформаційно-довідних служб та консультативні послуги у сфері комп'ютерних технологій.

Організаційна структура: організаційна структура підприємства зазначеного вище складається з:

- директора;
- менеджеру проекту;
- керівника відділу дзвінків та електронних листів;
- керівника відділу офіційних справ;
- супервайзерів;
- агентів;
- робітників IT – відділу;
- HR – менеджерів;
- Тренера.

Обов'язки менеджер проекту - організаційні питання та умови договору з замовниками. Керівники відділів – підготовка звітів по людино-годинах за місяць. Супервайзери – слідкування в реальному часі за роботою агентів та допомога у вирішенні форс-мажорних ситуацій. Агенти – вирішення проблем клієнтів. Робітники IT-відділу – підтримка обладнання та забезпечення безпеки інформації. HR-менеджери – підбір персоналу. Тренер – навчання нових агентів.

В офісі, впродовж робочого дня, знаходяться наступні працівники:

- HR-менеджери;

- Робітники IT-відділу;
- Прибиральниця;
- Супервайзер;
- Керівники відділів;
- Від 40 до 50 агентів.

Розглянемо організаційну структуру підприємства на рисунку 1.1.

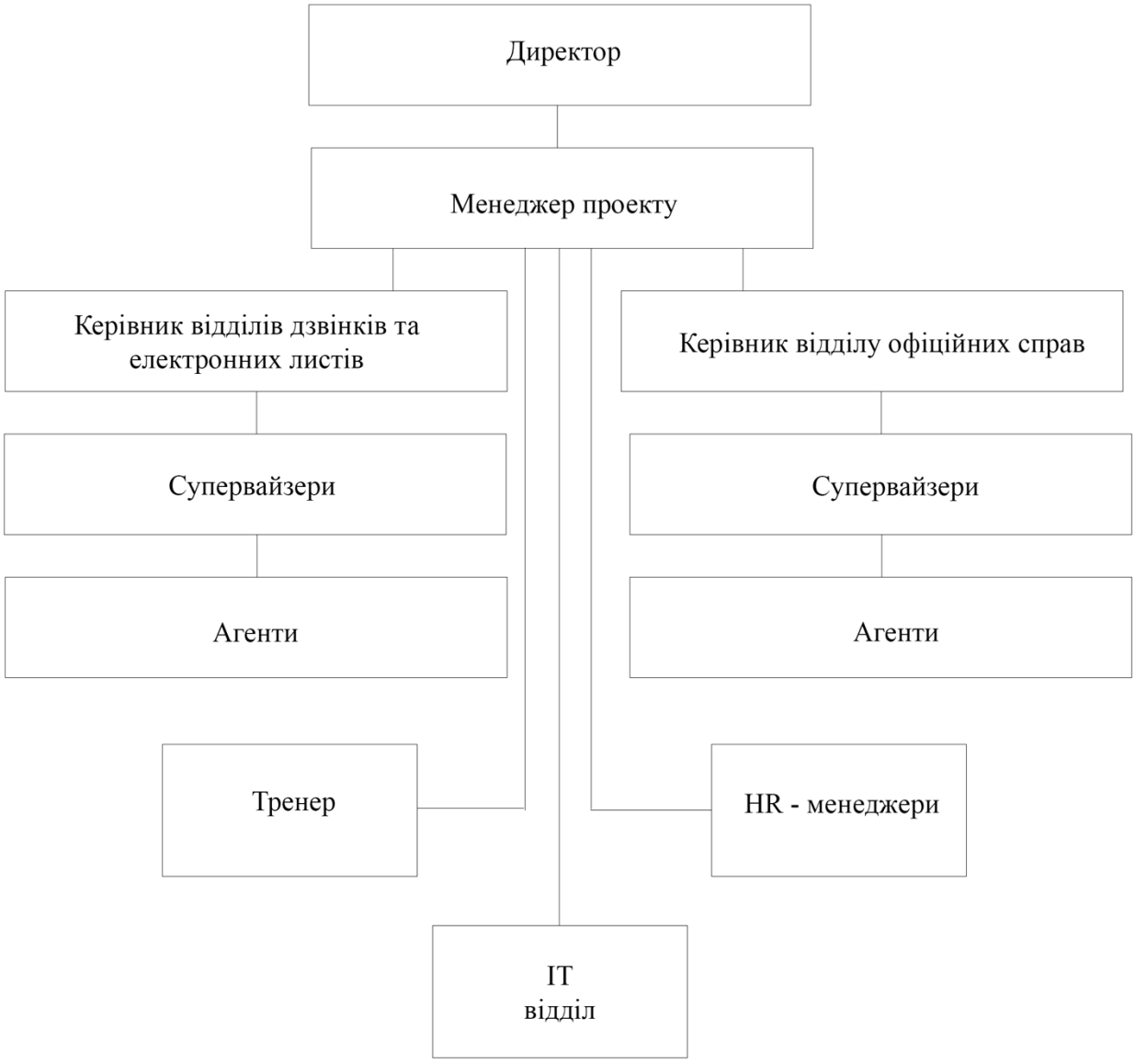

Рисунок 1.1 – Схема організаційної структури ТОВ «СІМЛІ ЄЙР»

На підприємстві ТОВ «СІМЛІ ЄЙР» циркулює відкрита (розклад польотів, кількість доступних місць на борту) інформація з обмеженим доступом, а саме конфіденційна, що містить в собі персональні дані як клієнтів так і співробітників.

1.2. Обґрунтування необхідності створення КСЗІ.

Відповідно до законодавства України і нормативних документів Закону України «Про захист інформації» обов'язковому захисту підлягає інформація з обмеженим доступом та інформація, що містить персональні дані громадян.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;
- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

Для створення комплексної системи захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством. У 2006 році 29 березня Постановою Кабінету Міністрів України №373, були затверджені «Правила забезпечення захисту

інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», в яких визначається, що - (пт. 16) для забезпечення захисту інформації в системі створюється КСЗІ, яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;
- несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;
- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від витоку технічними каналами забезпечується в системі у тому випадку, коли в ній обробляється інформація, що становить державну таємницю чи рішення власника або розпорядником інформації щодо необхідності такого захисту. Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах. Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації. Існує також нормативний документ, «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» НД ТЗІ 3.7-003, який визначає, (пт.5.3) процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в інформаційно-телекомунікаційній системі (ІТС) згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;
- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та інше;
- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Рішення щодо необхідності вжиття заходів захисту від різноманітних впливів на інформацію приймається власником інформації.

1.3. Обстеження ОІД.

1.3.1 Ситуаційний план ОІД.

Об’єкт знаходиться за адресою вул. Гагаріна 37, м. Дніпро, Дніпровська обл., 49000; в семиповерховій будівлі. Контрольована зона (КЗ) обмежується стінами будівлі. У робочий час працівники мають відкритий доступ до приміщення через відбиток пальця. Режим КЗ забезпечується системою контролю доступом, відеоспостереженням, персоналом будівлі.

Перед будівлею знаходиться проїжджа частина, ліворуч та праворуч знаходяться приватні будинки.

ОІД знаходиться на третьому поверсі будівлі у опенспейс офісі.

Характеристика прилеглих споруд та доріг наведені в таблицях 1.1 та 1.2.

Таблиця 1.1 – Характеристика прилеглих споруд

№ п/п	Найменування	Кількість поверхів	Адреса	Відстань до ОІД
1	Приватний будинок №1	1	Гагаріна 35	20 м
2	Приватний будинок №2	2	Гагаріна 31	80 м
3	Приватний будинок №3	1	Баха 1	45 м

Таблиця 1.2 – Характеристика прилеглих доріг

№ п/п	Найменування	Ширина	Інтенсивність руху	Відстань	Паркування
1	Пішохідна зона	3м	У денний час інтенсивний	30 м	-
2	Широкополосна проїздна дорога	11м	У денний час інтенсивний рух	10 м	-

При проведені робіт використовувалася схема ОІД разом з його оточенням з географічної карти. Вона була використана, щоб отримати детальне розташування будівель, зелених насаджень та інших об’єктів навколо ОІД та вимірювання точних відстаней до них. Схема с ситуаційним планом наведена на рисунку 1.2.

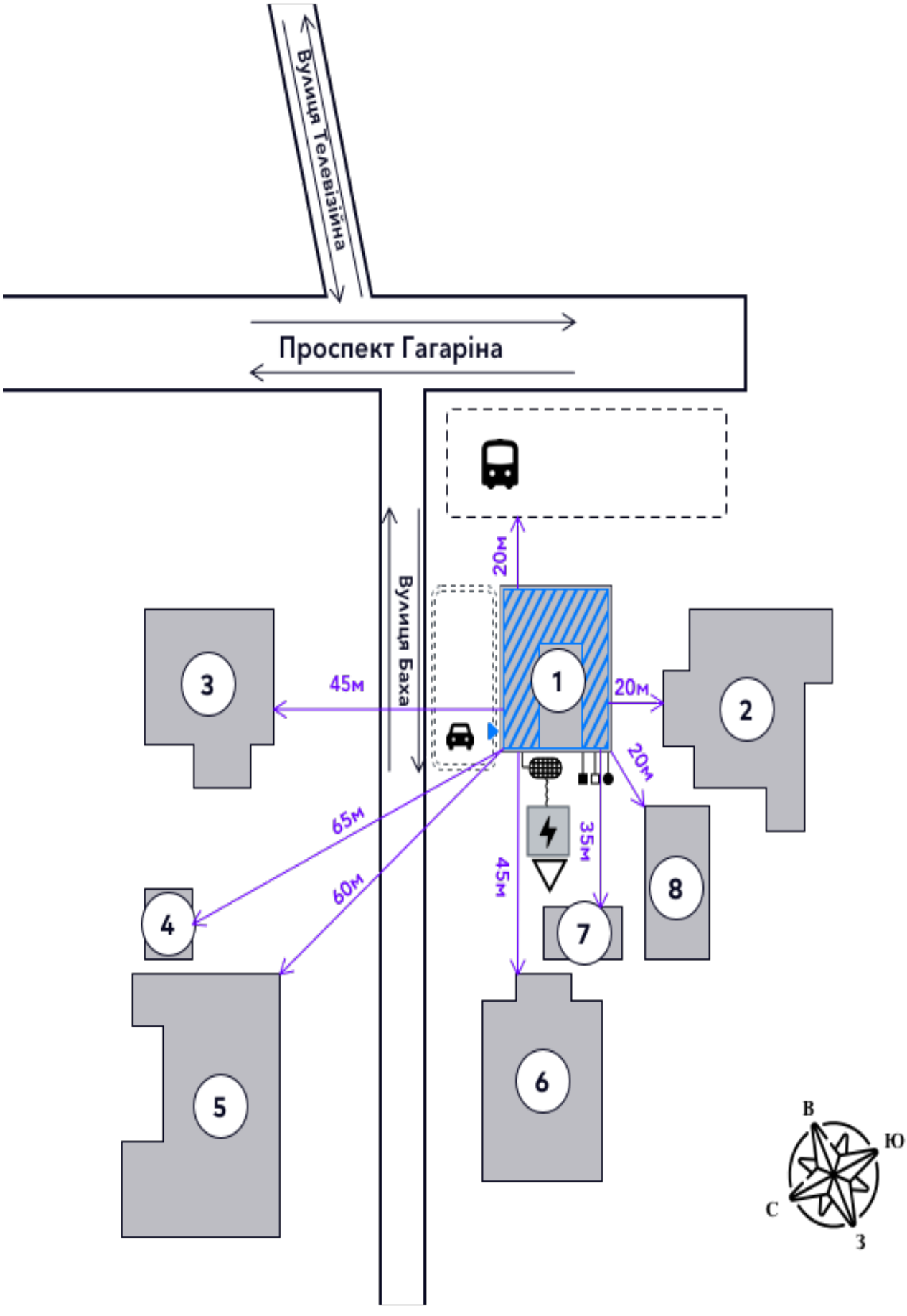

Рисунок 1.2 – Схема ситуаційного плану ОІД

Рисунок 1.3 – Умовні позначення

Уся територія будівлі офісу охороняється засобами охоронної сигналізації, яка встановлена на всіх дверях та вікнах. Усі дані з детекторів охоронної сигналізації в автоматичному режимі відправляються на пульт охорони, що знаходиться у будівлі офісу на нульовому поверсі.

1.3.2 Генеральний план.

Стіни зроблені з газо-бетонних блоків (500x200x500 мм). Фундамент — стовпчастий, дах — покритий руберойдом з грубозернистим посипанням з лицьового боку, територія навколо будівлі покрита асфальтом, будівля має панорамні тоновані вікна.

Зовнішні стіни офісу — газо-бетонні. Товщина зовнішніх стін — 500 мм.

Внутрішні несучі стіни газо-бетонні, товщина — 260 мм. Перегородки зведені за допомогою металоконструкцій та гіпсокартону, загальною товщиною — 70 мм.

Вхідні двері – армоване скло висотою 2 м та шириною 2 м. Вхідні двері до ОІД броньовані з висотою 2 м та шириною 1,5 м.

Приміщення мають висоту 3 м (від підлоги до стелі).

Підлога – плитка, стеля – газо-бетонні плити.

Системи каналізації та водопостачання підключені до міської системи каналізації.

Система опалення автономна.

Система електропостачання підключена до трансформаторної, що знаходиться за межами КЗ і підтримує ще інших споживачів.

Також на підприємстві є джерело безперебійного живлення, яке знаходиться в підвалі будівлі офісу та підтримує короткий час живлення на ОІД.

Інтернет проведено за допомоги оптоволоконного кабелю від декількох провайдерів: «Київстар», «ДТС», «АртемЛайфІнет».

З конвертера виходить вита пара та приєднана до світчів, що утворюють в офісі локальну мережу (використовуючи технологію VLAN).

Комунікація проведена за допомогою комутативних кабелів (патч-кордів).

Встановлена система бездротової охоронної (AJAX) та проводної пожежної сигналізації. Вся інформація передається на обладнання охорони будівлі та до адміністраторів відділу, що працюють в ОІД.

Останній ремонт в приміщеннях ОІД проводився у 05.02.2017р.

На таблиці 1.3 наведена інформація про системи комунікацій, та життєзабезпечення.

Таблиця 1.3 – Системи комунікацій, та життєзабезпечення

Система комунікацій	Спосіб підключення
Система опалення	Підключено до міської мережі опалення, знаходиться за межами КЗ.
Електроживлення	Підключено до трансформаторної підстанції, котра обслуговує сторонніх споживачів і виходить за межі КЗ.
Система водопостачання	Підключено до міського водоканалу, котрий виходить за межі КЗ.
Система каналізації	Підключена до міської мережі каналізації, котра виходить за межі КЗ.
Заземлення	Всі прилади заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ.
Система вентиляції	Приточно-витяжна
Протипожежна сигналізація	Всі прилади, комп’ютери заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ.
Кабелі комп’ютерної мережі	Всі прилади, комп’ютери заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ.

Схема генерального плану ОІД, схема вентиляції та схема освітлення наведена на рисунках 1.4-1.6.

Рисунок 1.4 – Схема генерального плану ОІД

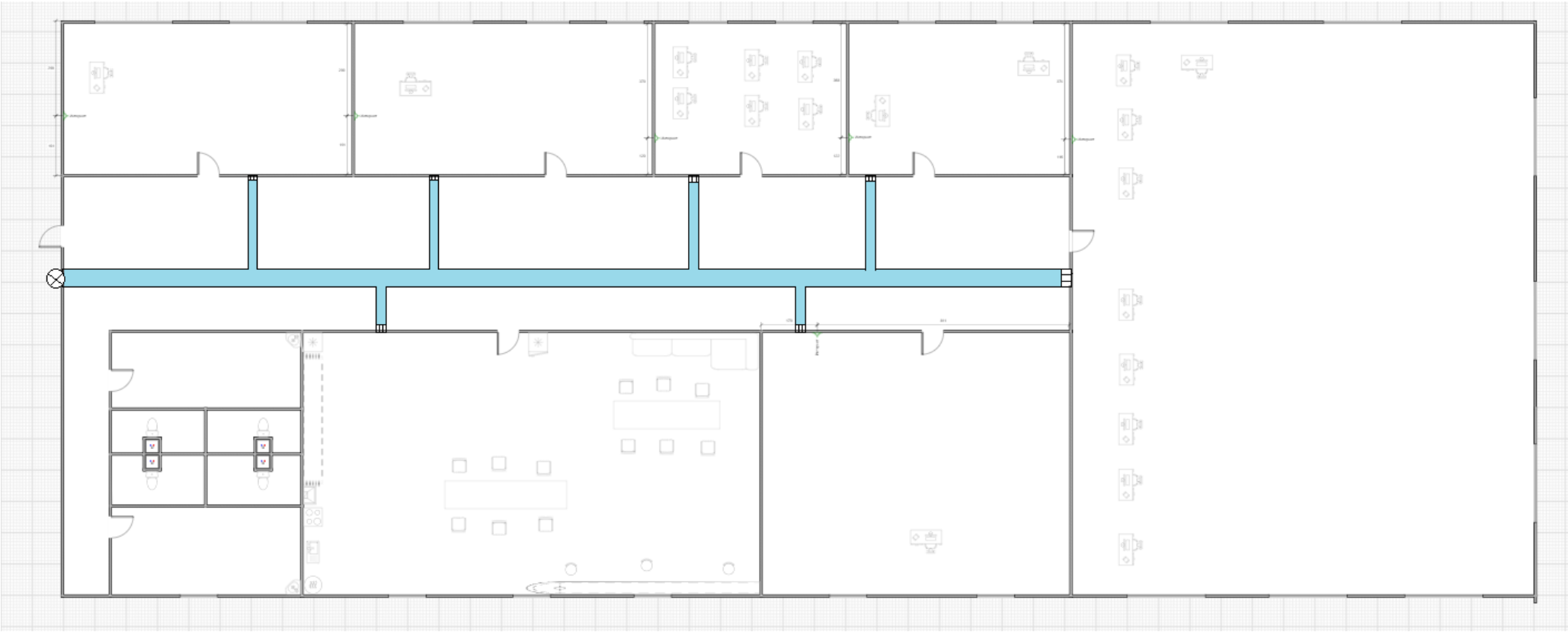

Рисунок 1.5 - Схема вентиляції на ОІД

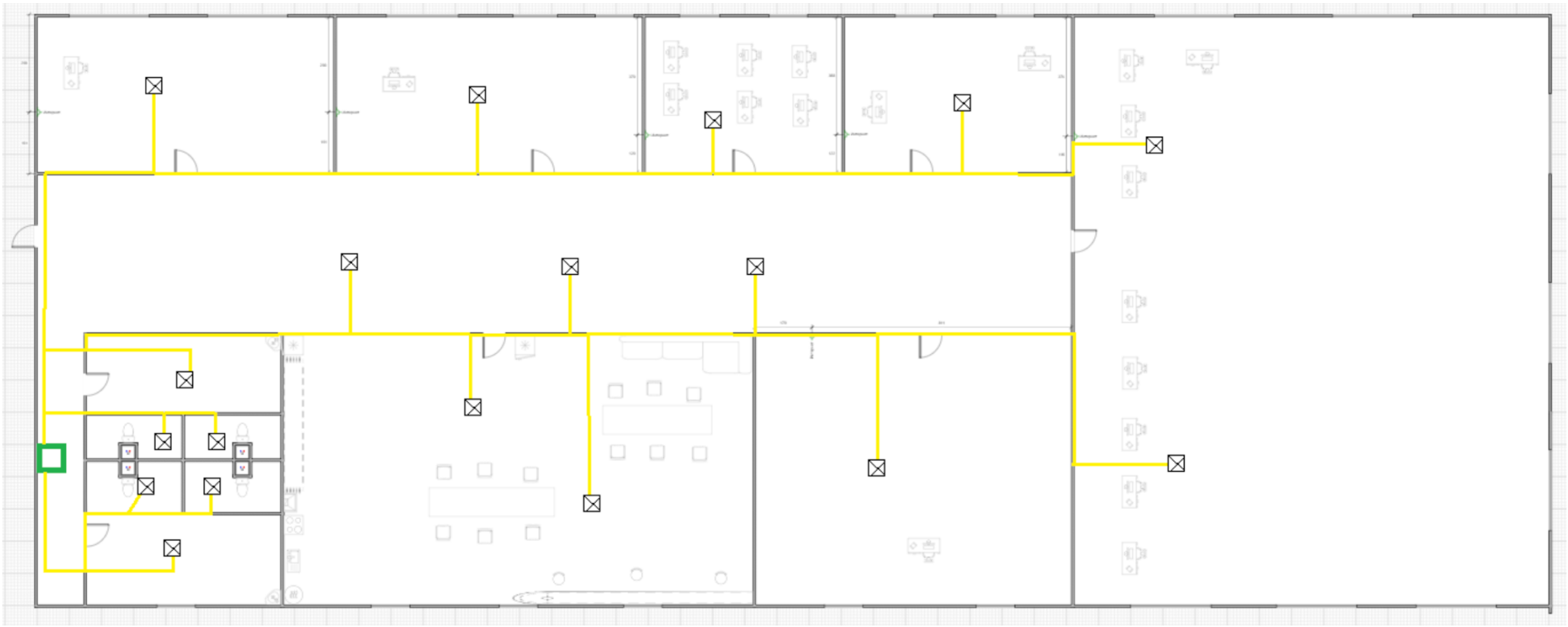

Рисунок 1.6 – Схема освітлення на ОІД

Рисунок 1.7 – Умовні позначення до схем генерального плану

ІТС ОІД являє собою мережу типу «пасивна зірка», побудовану з використанням одного маршрутизатору, одного комутатору. Являє собою багатомашинний багатокористувацький комплекс, який обробляє інформацію однієї категорії конфіденційності, а також має доступ до мережі Інтернет.

Виходячи з наведеного вище, ІТС відноситься до третього класу.

АС 3 класу - розподілений багатомашинний, багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Обчислювальна система у складі:

1. Сто два ПЕОМ з ОС Microsoft Windows 10 Pro;
2. Мережеве обладнання:
    - Один маршрутизатор Mikrotik;
    - Один світч (некерований) Cisco SX550X-52;

Інформація про основні технічні засоби, які використовуються на підприємстві наведено в таблиці 1.4.

Таблиця 1.4 – Основні технічні засоби на підприємстві

№	Тип	Серійний та інвентаризаційний номери	Розташування	Відстань до ДТЗС	Кількість
1	Персональний комп’ютер	DP130H4, 645786101 - 203	Опенспейс офіс, на столі	2 м	102
2	Монітор	LG2220, 645786876 - 978	Опенспейс офіс, на столі	2 м	102
3	Клавіатура	HKR3746, 645786876 - 1080	Опенспейс офіс, на столі	2 м	102

Продовження таблиці 1.4 – Основні технічні засоби на підприємстві

№	Тип	Серійний та ін-вентаризаційний номери	Розташування	Відстань до ДТЗС	Кількість
4	Комп'ютерна миша	6574G21, 6457861080 - 1200	Опенспейс офіс, на столі	2 м	23
6	Гарнітура	JBR40UC, 8771654800 - 006	Опенспейс офіс, на столі	2 м	23
7	Принтер	677567576	Опенспейс офіс, на столі	3 м	1

Характеристика персональних комп'ютерів (ім'я в системі NIP 8-110):

- Процесор Intel Core i5 3470;
- RAM 8 ГБ;
- SSD 128 ГБ;
- Системний блок «DP130H4» (645786101 – 203).

Також наглядно в таблиці 1.5 перераховане програмне забезпечення згідно з інвентаризації станом на 31.12.2019 р, встановлене на всіх ПК, які використовують співробітники ТОВ «СІМЛІ ЄЙР».

Таблиця 1.5 – Програмне забезпечення на ПК ОІД

Тип	Найменування	Описання	Ліцензія	Термін дії	Встановлено на
Системне	Операційна система Microsoft Windows 10 Pro 1909 (білд 18363.476)		Пропріє-тарна, OLP	-	ПК1 — ПК102
	Драйвери		Пропріє-тарна	-	ПК1 — ПК102
Прикладне	Libre Office	Пакет офісних програм	GPL	-	ПК1 — ПК102
Прикладне	Google Chrome	Веб-браузер	GNU GPL, GNU LGPL	-	ПК1 — ПК102
	ESET Smart Security 12.1.21.0	Антивірус	Пропріє-тарна	3 місяці	ПК1 — ПК102
Спеціалізоване	COMNICA 12.2	Клієнтське ПЗ для можливості робити дзвінки	Пропріє-тарна	6 місяців	ПК1 — ПК102

1.4 Аналіз загроз інформації, що циркулює на ОІД.

1.4.1 Інформація, яка циркулює на ОІД.

На розглядаємому підприємстві ТОВ «СІМЛІ ЄЙР» циркулює наступна інформація:

- Організаційно-розпорядча – інформація про співбесіди;
- Інформація про співробітників – це інформація (персональні дані) про працівників, документи, тощо;
- Інформація про клієнтів – інформація про клієнтів авіакомпанії (персональні дані), а саме:
  - прізвище та ім’я;
  - інформація про документі, які необхідні для подорожей;
  - інформація про платіжні картки.

В таблиці 1.6 наведена характеристика до інформації, що обробляється на підприємстві.

Таблиця 1.6 – Характеристика інформації на ТОВ «СІМЛІ ЄЙР»

№	Інформація	Режим доступу	Правовий режим	Місце зберігання
1	Організаційно-розпорядча	З обмеженим доступом	Конфіденційна інформація	Персональний комп’ютер кадрового працівника

Продовження таблиці 1.6 – Характеристика інформації на ТОВ «СІМЛІ ЄЙР»

№	Інформація	Режим доступу	Правовий режим	Місце зберігання
2	Інформація про працівників	З обмеженим доступом	Конфіденційна інформація	Персональні комп'ютери кадрових працівників
3	Інформація про клієнтів (персональна)	З обмеженим доступом	Конфіденційна інформація	-
4	Фінансова звітність	З обмеженим доступом	Конфіденційна інформація	Персональний комп'ютер бухгалтера

1.4.2 Побудова моделі порушника.

Модель порушника – набір припущень про одне або декілька можливих порушників інформаційної безпеки, їх матеріальних та технічних засобів та тому подібне. Припускається, що в своєму рівні порушник – фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Для побудови моделі порушника використовується інформація, що була отримана від служб безпеки та аналітичних груп, дані про існуючі засоби доступу інформації та обробки про можливі способи перехвату даних на стадіях їх передачі. Обробка та зберігання, про обстановку в колективі та об'єкті захисту, відомості про конкурентів і ситуації на ринку інформаційної безпека та тому подібне.

Тому порушника можна назвати особою, яка з помилки, по незнанню чи свідомо здійснює спробу виконання заборонених операцій і використовує для цього різні можливості, засоби і методи.

Практичні уміння та навички можуть бути використані за умовою знаходження у конкретних місцях об’єкта, звідки можна реалізувати загрозу.

В такому разі, необхідно визначити категорію осіб, до якої може належати порушник, а не тільки рівень знань, його кваліфікацію та підготовленість до реалізації своїх планів. Необхідно приділяти увагу суб’єкту порушника при аналізу порушень захисту, щоб на далі мінімізувати можливість повторення подібних випадків.

Якщо розподілити всіх співробітників по їх можливостях щодо доступу до інформаційних ресурсів та і по можливим втратам від дій співробітників, по потенційним збиткам від кожної категорії користувачів.

Кожний користувач може нанести більші або менші збитки шляхом доступу до конкретних елементів системи обробки інформації.

Спираючись на вищевказане, необхідно оцінити реально оперативні технічні можливості зловмисника для впливу на систему захисту. Під технічними можливостями мається на увазі перелік різноманітних технічних засобів, якими може розпоряджатися зловмисник під час здійснення дій, які направлені проти системи інформаційного захисту.

Таблиця 1.7 – Модель внутрішнього порушника

Посада	Мотиви	Специфікація за рівнем кваліфікації і тощо	Можливості	Модель за часом дії	Місце дії	Сума загроз
HR-менеджер	М2	К2	З3	Ч3	Д4	14
Агенти	М2	К2	З3	Ч3	Д2	12
Робітники IT-відділу	М3	К4	З4	Ч4	Д4	19
Прибиральниця	М3	К0	З3	Ч4	Д2	12

Таблиця 1.8 – Модель зовнішнього порушника

Посада	Мотиви	Специфікація за рівнем кваліфікації і тощо	Можливості	Модель за часом дії	Місце дії	Сума загроз
Представники сторонніх організацій	М3	К1	31	Ч4	Д2	11
Охорона	М3	К1	З1	Ч4	Д2	11
Хакери	М3	К4	34	Ч3	Д1	15

Специфікація моделі порушника за мотивами здійснення порушень:

- М1 – Безвідповідальність.
- М2 – Самоствердження.
- М3 – Корисливий мотив.

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС:

- К0 – Не знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами си-ми.
- К1 – Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами си-ми.
- К2 – Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування.
- К4 – Знає структуру, функції й механізми дії засобів захисту, їх недоліки.

Специфікація моделі порушника за місцем дії:

- Д1 – Без доступу на контрольовану територію організації.
- Д2 – З контрольованої території без доступу у будинки та споруди.
- Д3 – Усередині приміщень, але без доступу до технічних засобів АС.
- Д4 – З робочих місць користувачів АС.

Специфікація моделі порушника за часом дії:

- Ч2 – Під час бездіяльності компонентів системи (в неробочий час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.).
- Ч3 – Під час функціонування АС (або компонентів системи).
- Ч4 – Як у процесі функціонування АС, так і під час зупинки компонентів системи.

З наведених таблиць 1.7 - 1.8 можна визначити, що найбільшу загрозу становлять системні адміністратори завдяки найбільшого доступу до інформації, також агенти, які мають доступ до персональних даних клієнтів. Так як обробляється багато персональних даних (банківські реквізити та інше) ОІД може заінтересувати зовнішніх порушників, а не тільки внутрішніх.

1.4.3 Виявлення актуальних загроз.

Джерело загрозі – потенційні антропогенні, техногенні та стихійні носії загрози безпеки.

Атака – можливі наслідки реалізації загрози при взаємодії джерела загрози через наявні вразливості. Насамперед пара «джерело-вразливість», реалізуюча загрозу, яка приводить до збитків.

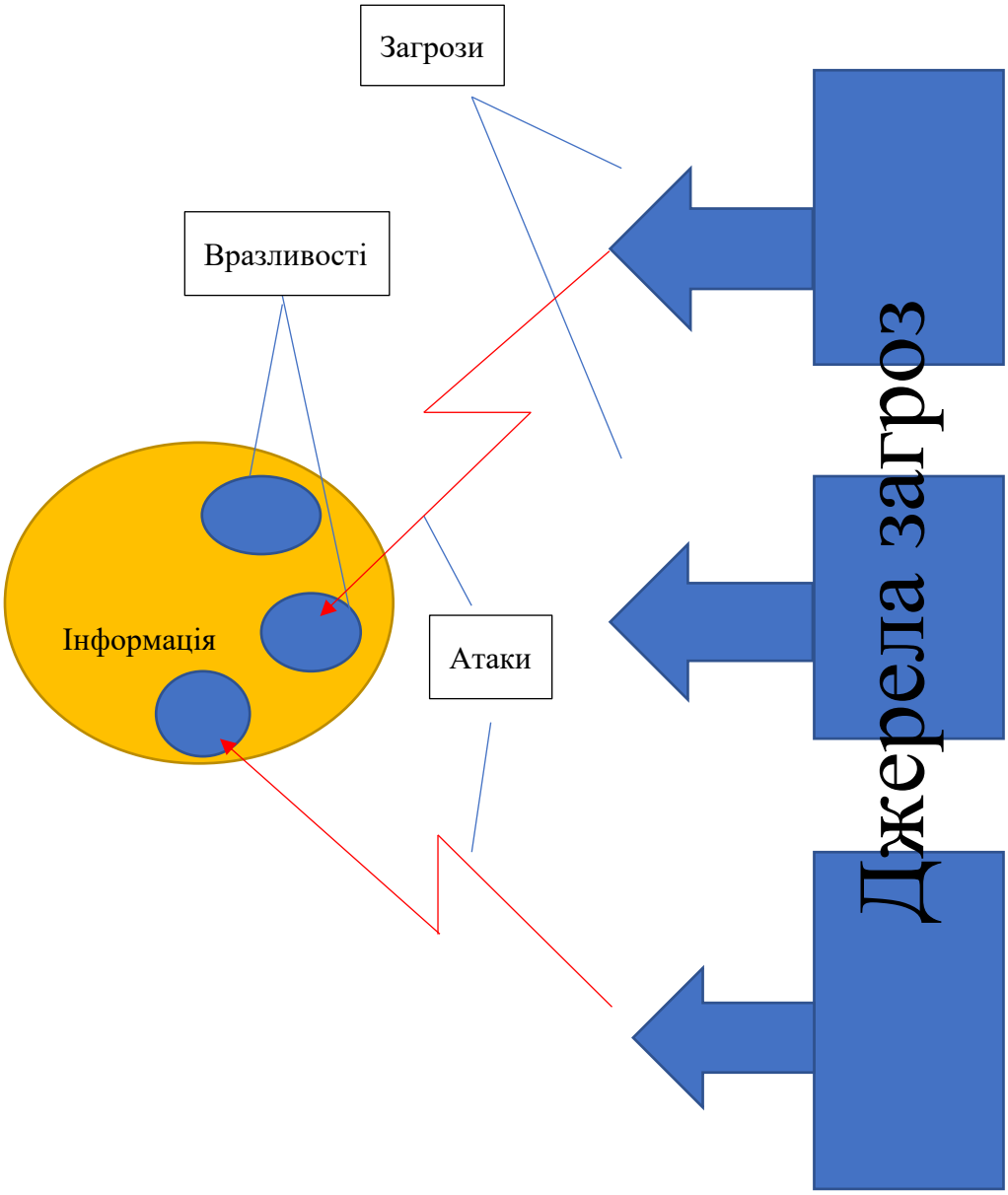

Рисунок 1.8 Схематичне зображення загроз

Припустимо, людина пішохід переходить проїзджу частину в неустановленому місці. Одного разу він потрапляє під автомобіль, що причиняє йому збиток, при якому він втрачає працездатність. Проаналізуємо даний випадок

Наслідки даного випадку – збитки, які сталися в результаті нещасного випадку. Загрозою виступає автомобіль, який збив пішохода. Вразливістю став пішохід, який переходив дорожнє полотно в неустановленому місці. Джерелом загрози є якась сила, яка не дала можливість водію запобігти наїзду на людину.

Можна зробити висновок, що з інформацією також не набагато складніше. Загроз безпеки інформації не так і багато.

Загроза – небезпечність спричинення збитків, можна спостерігати жорстку прояву технічних проблем з юридичною категорією, якою являється «збиток».

Таблиця 1.9 - Загрози з визначенням порушень властивостей інформації ІТС

№	Загрози	Властивості		
		К	Ц	Д
1.1	Стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події	-	+	+
1.2	Втрата електроживлення	-	+	+
1.3	Втрата або пошкодження комунікаційних каналів	-	+	+
1.4	Перенавантаження системи	-	-	+
1.5	Збої та відмови обчислювальної техніки, програмного забезпечення	-	+	+
2.1	Несанкціоноване підключення до технічних засобів	+	-	+
2.2	Хакерські атаки через глобальну мережу Інтернет	+	+	-
2.3	Зараження системи комп’ютерними вірусами	+	+	+
2.4	Втрата або розголошення інформації з носіїв інформації, резервних копій	+	+	+
2.5	Модифікація технічніх засобів або програмного забезпечення	-	+	+
2.6	Використання стороннього програмного забезпечення	+	+	+
2.7	Вхід у систему недопущених осіб	+	+	+
2.8	Пошкодження носіїв інформації	-	+	+
2.9	Помилки при експлуатації ПЗ	+	+	+
2.10	Помилки при експлуатації технічних засобів	-	+	+
2.11	Недбале зберігання та облік документів, носіїв інформації	+	+	+
2.12	Розголошення інформації персоналом ІТС	+	-	-

Таблиця 1.10 – Модель загроз з визначенням рівня ризиків та збитків

№	Механізм реалізації	Рівень		Сума загроз
		Ризиків	Збитків	
1. Загрози конфіденційності інформації				
1.1	Ненавмисне ознайомлення з ІОД під час співбесід персоналу ІТС зі сторонніми особами	2	2	4
1.2	Втрата носіїв ІОД з причини безвідповідального ставлення до виконання обов'язків	1	3	4
1.3	Викрадення носіїв ІОД з метою несанкціонованого ознайомлення сторонніх осіб	1	3	4
1.4	Копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб	3	3	6
1.5	Безпосередній доступ до ІОД будь-яким способом сторонніх осіб	1	3	4
1.6	Перегляд інформації на екранах моніторів, робочих місцях; підслуховування	2	3	5
2.Загрози цілісності інформації				
2.1	Помилки (ненавмисні) користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях	3	3	6
2.2	Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях	2	3	5
2.4	Навмисне пошкодження носіїв інформації користувачами ІТС, яке призвело до модифікації або спотворення інформації	1	2	3
2.5	Помилки (ненавмисні) адміністраторів ІТС при налагодженні засобів захисту та системного ПЗ, в наслідок яких стала можливою модифікація ІОД	1	3	4
3.Загрози доступності				
3.1	Помилки (ненавмисні) користувачів ІТС, які призвели до знищення інформаціїабо втрати доступу до неї	2	2	4

Продовження таблиця 1.10 – Модель загроз з визначенням рівня ризиків та збитків

№	Механізм реалізації	Рівень		Сума загроз
		Ризиків	Збитків	
3. Загрози доступності				
3.2	Втрата електропостачання, яке призвело до знищення інформації або втрати доступу	2	3	5
3.4	Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації	2	2	4
3.5	Навмисне пошкодження парольних носіїв персоналом ІТС, яке призвело до втрати доступу до інформації	2	2	4

Рівні ризиків та загроз:

- Низький – реалізація загрози надає незначних збитків (1 бал).
- Середній –реалізація загрози надає помірних збитків (3 бали);
- Високий – реалізація загрози надає великих збитків (4 бали);

Модель загроз з розрахунком сумарного рівня ризиків та збитків:

- Сума загрози конфіденційності – 27;
- Сума загрози цілісності – 18;
- Сума загрози доступності – 16;

Антропогенними джерелами загроз в безпеці інформації виступають суб'єкти, дії яких можуть бути кваліфіковані, як умисні або випадкові. Ця група найбільш поширена і представляє інтерес з точки зору організації захисту, так як дії суб'єкта не завжди можна оцінити, спрогнозувати і вжити адекватних заходів. Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться:

- потенційні злочинці та хакери;
- несумлінні партнери;
- представники наглядових організацій і аварійних служб;
- представники силових структур.

Внутрішні суб'єкти, як правило, представляють собою висококваліфіковани х фахівців в області розробки і експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою вирішуваних завдань, структурою та основними функціями і принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться:

- основний персонал (користувачі, агенти, розробники);
- представники служби захисту інформації;
- допоміжний персонал (прибиральники, охорона);
- технічний персонал.

Техногенні джерела загроз – це джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки. Даний клас джерел загроз в безпеці інформації є особливо актуальним в сучасних умовах, тому що зростання числа техногенних катастроф, викликаних фізичним і моральним старінням технічного парку використовуваного обладнання, а також відсутністю матеріальних коштів на його оновлення. Технічні засоби, які є джерелами потенційних загроз безпеки інформації так само можуть бути зовнішніми:

- засоби зв'язку;
- мережі інженерних комунікації (водопостачання, каналізації);
- транспорт.

Внутрішні джерела загроз:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- допоміжні засоби (охорони, сигналізації, телефонії);
- інші технічні засоби, що застосовуються в установі.

1.5 Постановка задач

В наслідок того, що на підприємстві циркулює конфіденційна інформація про клієнтів авіакомпанії, яка містить в собі банківські та персональні дані необхідно зберегти конфіденційність, цілісність та доступність інформації.

В наслідок цього у кваліфікаційній роботі потрібно вирішити задачі:

- зробити оцінку існуючого стану захищеності на підприємстві ТОВ «СІМЛІ ЄЙР»;
- проаналізувати ситуаційний та генеральний плани ОІД;
- розробити вимоги з інформаційної безпеки для підприємства ТОВ «СІМЛІ ЄЙР»;
- скласти рекомендації для підвищення інформаційної безпеки;
- проаналізувати актуальні загрози після впровадження рекомендацій;

1.6 Висновки

Всі підприємства схильні до вразливостей, проти яких важко організовувати оперативну, рентабельну та продуктивну протидію.

З кожним роком інфраструктура поступово поповнюється все новими пристроями, які пов'язані з іншими пристроями і системами. Конфіденційна інформація, яка циркулює на підприємствах вимагає спеціального підходу та розробки ефективної системи захисту.

В першому розділі кваліфікаційної роботи зроблений детальний аналіз підприємства ТОВ «СІМЛІ ЄЙР». В ході аналізу були отримані наступні результати:

– виконаний детальний аналіз споруди. Розглянуті ситуаційний план, генеральний план. Проаналізоване програмне забезпечення, яке використовується;
– виконана класифікація інформації, що циркулює на ОІД;
– проаналізовані всі можливі вразливості;
– проаналізовані загрози для оброблюваної інформації на ТОВ «СІМЛІ ЄЙР»;
– розроблена модель порушника.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка існуючого стану захищеності

Спираючись на таблицю 1.10, яка була побудована після проведення аналізу ризиків та обстеження ОІД ТОВ «СІМЛІ ЄЙР» було виявлено, що найбільший ризик складають декілька загроз, а саме:

- копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб;
- перегляд інформації на екранах моніторів, робочих станцій та підслуховування;
- модифікація або спотворення інформації на жорстких дисках.
- втрата електропостачання, яке призвело до знищення інформації або втрати доступу

На підприємстві використовується антивірусний захист від компанії ESET під назвою Smart Security, який відновлюється в автоматичному режимі та сканує всі ПК на наявність заражених файлів. Дане програмне забезпечення має технології глибокого аналізу коду і дослідження елементів, які дозволяють простежити поведінку і створити родові виявлення. Вони використовуються для оцінки потенційно підозрілого коду, знайденого на диску або в пам'яті запущеного процесу. Родові виявлення можуть визначити конкретні відомі зразки шкідливих програм, нові варіанти відомих сімейств шкідливих програм або навіть раніше невидимі або невідомі загрози, які містять певні елементи, що вказують на шкідливу поведінку.

Агенти, які приймають дзвінки мають можливості до викрадення персональних даних, а також банківських даних, до яких входить:

- номер карти;
- CVV код.

Це відбувається, коли працівник Контактного центру запрошує ці дані у дзвінку для сплати товару (авіаквиток або багаж, місце), називаючи кодове слово, яке розпізнається ПЗ під назвою COMNICA 12.2. Після того, як дане ПЗ виявляє це слово - запис дзвінка припиняється.

Також завдяки тому, що на об’єкті дослідження використовується декілька провайдерів інтернету, при збою роботи одного з постачальників інтернету є можливість не припиняти роботу всього контактного центру, а продовжувати працювати та вирішувати проблеми клієнтів авіакомпанії. З моделлю побудови мережі можна ознайомитись на рис 2.0.

На підприємстві використовується система безперебійного живлення, яка підтримує роботу на протязі 2 годин.

Для входу працівників до робочого ПЗ використовуються унікальні логін та пароль. Використовується наступна політика паролів:

- Мінімальна довжина паролю – 8 символів;
- Використовувати мінімум 3 (три) перші групи складності з наведених нижче 4 (чотирьох): символи верхнього регістру (великі літери), символи нижнього регістру (маленькі літери), цифри (0, 1, 2, 3, 4, 5 та ін.), символи не з алфавіту (№, %, !, #, * та інше).
- Новий пароль (послідовність символів) повинен відрізнятись від попередніх раніше використаних чотирьох паролів.
- Для запам’ятовування паролів необхідно застосовувати асоціації.
- Під час вибору паролів заборонено: використовувати у якості пароля будь-яку особисту інформацію (дані облікового запису; прізвище, ім’я, по батькові – як свої так і родичів; дату та місце народження; клички домашніх улюбленців та ін.);).

Для входу до ОІД використовується система біометричної автентифікації (відбиток пальців) на технології Match-in-Sensor має архітектуру, замкнуту на самому чіпі (system-on-a-chip або SoC). Зчитування відбитка пальця і вся подальша обробка біометричних даних здійснюється безпосередньо в ІС-

датчику. В такій архітектурі шаблони відвідуваності зашифровані і підписані за допомогою датчика, а вся інформація зберігається в приватній флеш-пам'яті.

На рисунку 2.1 показана схема біометричної автентифікації.

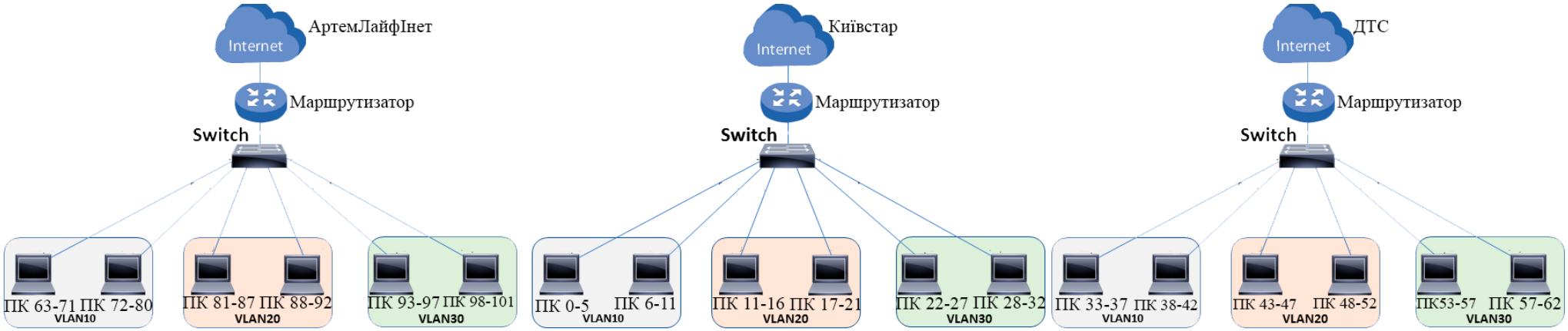

Рисунок 2.0 Модель побудови мережі на підприємстві

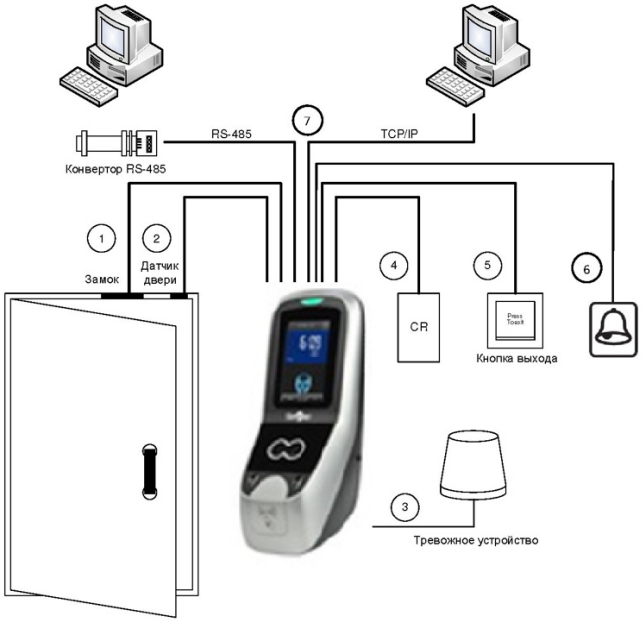

Рисунок 2.1 – Схема біометричної автентифікації

Також на підприємстві ТОВ «СІМЛІ ЄЙР» використовується стандартний функціональний профіль захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.1 = { КД – 2, КО – 1, КВ – 1,

ЦД – 1, ЦО – 1, ЦВ – 1,

ДР – 1, ДВ – 1,

НР – 2, НИ – 2, НК – 1, НО – 2, НЦ – 2, НТ – 2, НВ – 1 }

Критерії:

Довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Базова довірча конфіденційність (КД – 2). Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Повторне використання об'єктів. Послуга дозволяє забезпечити коректність повторного використання розділених об'єктів, гарантуючи, що в разі, якщо розділений об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Повторне використання об'єктів (КО – 1). Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Конфіденційність при обміні. Послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна конфіденційність при обміні (КВ – 1). Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Довірча цілісність. Послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна довірча цілісність (ЦД – 1). Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відносить

користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Відкат. Послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Обмежений відкат (ЦО – 1). Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Цілісність при обміні. Послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна цілісність при обміні (ЦВ – 1). Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання. Використання ресурсів. Послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування

доступністю послуг КС.

Квоти (ДР – 1). Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Відновлення після збоїв. Послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

Ручне відновлення (ДВ – 1). Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

Реєстрація. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Захищений журнал (НР – 2). Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу

і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Одиночна ідентифікація і автентифікація (НИ – 2). Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

Достовірний канал. Послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Одно направлений достовірний канал (НК – 1). Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Розподіл обов'язків. Послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Розподіл обов'язків адміністраторів (НО – 2). Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного

користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Цілісність комплексу засобів захисту. Послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

КЗЗ з гарантованою цілісністю (НЦ – 2). Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи. Самотестування при старті (НТ – 2). Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ. Ідентифікація і автентифікація при обміні. Послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація вузла (НВ – 1). Політика ідентифікації і автентифікація при

обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.2 Проектні рішення

2.2.1 Розробка вимог з інформаційної безпеки

Для підприємства ТОВ «СІМЛІ ЄЙР» необхідно ввести наступні вимоги з інформаційної безпеки, які під час роботи забороняють:

- користуватись мобільними пристроями зв’язку (телефон, смартфон тощо) в операційному залі;
- підключати до робочого комп’ютера будь-які зовнішні накопичувачі інформації (USB Flash, SD-карти, телефони/смартфони тощо) без письмового погодження з Директором по ІТ системам;
- фотографувати/записувати на відео/записувати на паперові носії інформацію, що відображається на екрані робочого комп’ютера;
- приносити та користуватись будь-якою звукозаписуючою апаратурою;
- приносити та підключати до робочих комп’ютерів та/або локальної комп’ютерної мережі будь-яке стороннє обладнання/пристрої без письмового погодження з Директором по ІТ системам;
- використовувати для входу в інформаційні системи Компанії облікові дані іншого співробітника;
- ремонтувати робочий комп’ютер, вносити зміни у склад його апаратних та програмних засобів (завантажувати інтерфейс керування системним ПЗ BIOS, вносити зміни або знищувати системні/конфігураційні файли операційної системи/мережевих пристроїв, самостійно встановлювати

програмне забезпечення, самостійно підключати або відключати периферійне обладнання, порушувати цілісність корпусу робочого комп'ютера (крім випадків обумовлених виконанням посадових/договірних обов'язків);

- залишати на робочому місці робочі записи/чернетки після закінчення робочого часу (в електронному вигляді - видаляти, в паперовому - знищувати у пристроях утилізації паперу);
- залишати ввімкненим робочий комп'ютер по закінченню робочого часу, за винятком випадків коли його подальша робота викликана технологічними вимогами;
- намагатись та/або вчиняти дії щодо отримання несанкціонованого доступу до робочих комп'ютерів, мережевого та серверного обладнання Компанії, а також втручатись в роботу системи антивірусного захисту;
- використовувати мережеві та обчислювальні ресурси Компанії для створення, передачі або розповсюдження недоречних або образливих матеріалів, таких як коментарі з приводу раси, статі, фізичних особливостей, інвалідності, віку, сексуальної орієнтації, порнографії, релігійних переконань, політичних переконань чи національного походження;
- використовувати Інтернет для обміну інформацією розважального характеру, зокрема відвідувати файл обмінні сервіси, соціальні мережі, сайти знайомств, чати, відео-/аудіо-ресурси та ін.
- використовувати загальнодоступні та/або безкоштовні поштові системи/сервіси для здійснення службового листування без письмового погодження з Директором по ІТ системам;
- відправляти повідомлення електронною поштою, особам, які не мають відношення до інформації, що пересилається (спам в електронній пошті);
- поширювати електронні повідомлення, що містять підозрілі вкладення, посилання на сторонні ресурси. Намагатись переглянути вкладення підозрілих електронних повідомлень;

– завантажувати з мережі Інтернет зберігати та/або використовувати на робочому комп'ютері програмне забезпечення та/або інформацію, що не має відношення до виконання посадових обов’язків.

– використовувати мережеві та обчислювальні ресурси Компанії для отримання або спроби отримання несанкціонованого доступу, участі у мережевих атаках та будь-яких деструктивних діях по відношенню до будь-якої мережі через Інтернет.

2.2.2 Впровадження дизельного генератора до системи безперебійного живлення.

Також для підприємства ТОВ «СІМЛІ ЄЙР» критичним питанням є безперебійна подача електроенергії, а будь-які відхилення в електропостачанні може призвести до порушенню наладженої роботи. Зникнення електричної напруги буває досить тяжко відновити коректну роботу серверу. На ОІД встановлена система безперебійного живлення, яка не забезпечує достатньої автономної роботи (так як було вказано раніше дві години). Прикладом цього є ситуація, яка відбулася з 31 грудня 2019 на 1 січня 2020 року. Через перевантаженість постачальника електроенергії було відключено постачання на 24 годину. На підприємстві знаходиться велика кількість комп’ютерних систем та електричних приладів, які є важливими компонентами для коректної роботи контактного центру. Через цю ситуацію необхідно впровадити до системи безперебійного живлення дизельний генератор номінальною потужністю близько 100 кВт.

Перевагами генератора на дизельному паливі являються:

– висока економічність (дозволяє заощадити до 40% палива зрівнюючи з іншими видами палива генераторів);
– надійність - розраховані на інтенсивну і тривалу експлуатацію і при цьому мають тривалий термін служби;
– великий потенціал потужності - навіть при повному знеструмленні підприємства є можливість повноцінної роботи всієї інфраструктури і

наявного обладнання, що гарантує нормальний режим функціонування компанії в цілому.

При використанні генератора в комерційних цілях не менш важливими є такі його характеристики, як величина ККД, вартість палива, а також довговічність. За даними показниками з агрегатами, що функціонують на дизельному паливі, навряд чи може конкурувати хоч один з нині існуючих типів генераторів. Виняток можуть тільки складати газові електростанції, які характеризуються низькою вартістю палива. Для впровадження було вибрано дизель-електростанція JCB G140QS потужністю 112,2 кВт (637 683,19 грн). Розташування залишається на нульовому поверсі (підвал). Технічні характеристики даного генератора приведені в таблиці 2.1.

Таблиця 2.1– Технічні характеристики генератора

Максимальна потужність	112,2кВт
Номінальна потужність	101кВт
Напруга	380В
Коефіцієнт потужності	0.8
Тип запуску	Електростартер
Вид палива	Дизельне паливо
Виконання	Захищений
Тип двигуна/модель	JCB TCAG S2
Кількість циліндрів	4
Переваги	Регулювання напруги, захист по рівню масла
Система охолодження	Рідинне
Оберти двигуна	1500 об/хв
Витрати палива	29.6 л/год
Об’єм паливного бака	285 л
Додаткові опції	Підключення АВР

Продовження таблиці 2.1– Технічні характеристики генератора

Рівень шуму	66 дБ
Регулювання обертів	Механічне
Довжина	2850 мм
Ширина	1140 мм
Висота	1830 мм
Вага	1720 кг

2.2.3 Впровадження технології інтернет-еквайринг

Інтернет-еквайринг (англ. «Internet acquiring») – технологія, що дозволяє приймати до оплати банківські карти через Інтернет. Головна відмінність від торгового і мобільного еквайрингу полягає у відсутності терміналу для фізичного зчитування даних карти. Виходячи с цього, використовувати інтернет-еквайринг можуть всі користувачі, навіть власники віртуальних банківських карт і електронних гаманців, у яких відсутні фізичні носії у вигляді пластикових карт.

У загальному випадку процес оплати складається з наступних етапів:

– Після оформлення замовлення клієнт через електронний лист переадресовується на платіжну форму, де вводить дані своєї банківської карти-номер, термін дії, ім'я та прізвище власника, код CVV2 / CVC2;
– Система передає дані карти і суму замовлення платіжним постачальнику (найбільш поширені платіжні агрегатори);
– Використовуючи введені дані карти, платіжний постачальник відправляє запит авторизації в банк-еквайрер. Зазвичай платіжний агрегатор укладає договори з декількома банками-еквайрами, що дозволяє підвищити надійність системи і в ряді випадків знизити комісію;
– Банк-еквайрер пересилає запит авторизації в міжнародну платіжну систему (далі МПС), що випустила карту, наприклад VISA, MasterCard, UnionPay;

- МПС передає запит авторизації в банк-емітент (банк, що випустив карту клієнта), який виробляє процедуру фрод-моніторингу і перевіряє, активна чи карта;
- Якщо до карти підключена технологія 3-D Secure, відбувається процедура перевірки:
  1. Перенаправлення клієнта на сторінку введення 3DS-пароля
  2. Відправка 3DS-пароля (найчастіше в SMS-повідомленні)
  3. Введення клієнтом 3DS-пароля
  4. Верифікація банком введеного 3DS-пароля

Якщо перевірка пройшла успішно, банк-емітент відправляє підтвердження МПС:

- МПС повертає відповідь банку-еквайреру;
- Банк-еквайрер повертає відповідь платіжним постачальнику;
- Платіжний постачальник відправляє в банк-еквайрер запит на списання суми замовлення з картки клієнта;
- Банк-еквайрер пересилає в МПС запит на списання суми замовлення з картки клієнта;
- МПС передає запит банку-емітенту.
- Банк-емітент перевіряє залишок коштів на рахунку клієнта, і, якщо коштів достатньо, робить переклад і пересилає підтвердження операції МПС.
- МПС передає підтвердження операції банку-еквайреру;
- Банк-еквайрер передає підтвердження платіжним постачальнику;
- Платіжний постачальник сповіщає про успішну оплату.

Спрощена схема проведення сплати за допомогою технології інтренет-еквайринг представлена на рисунку 2.3.

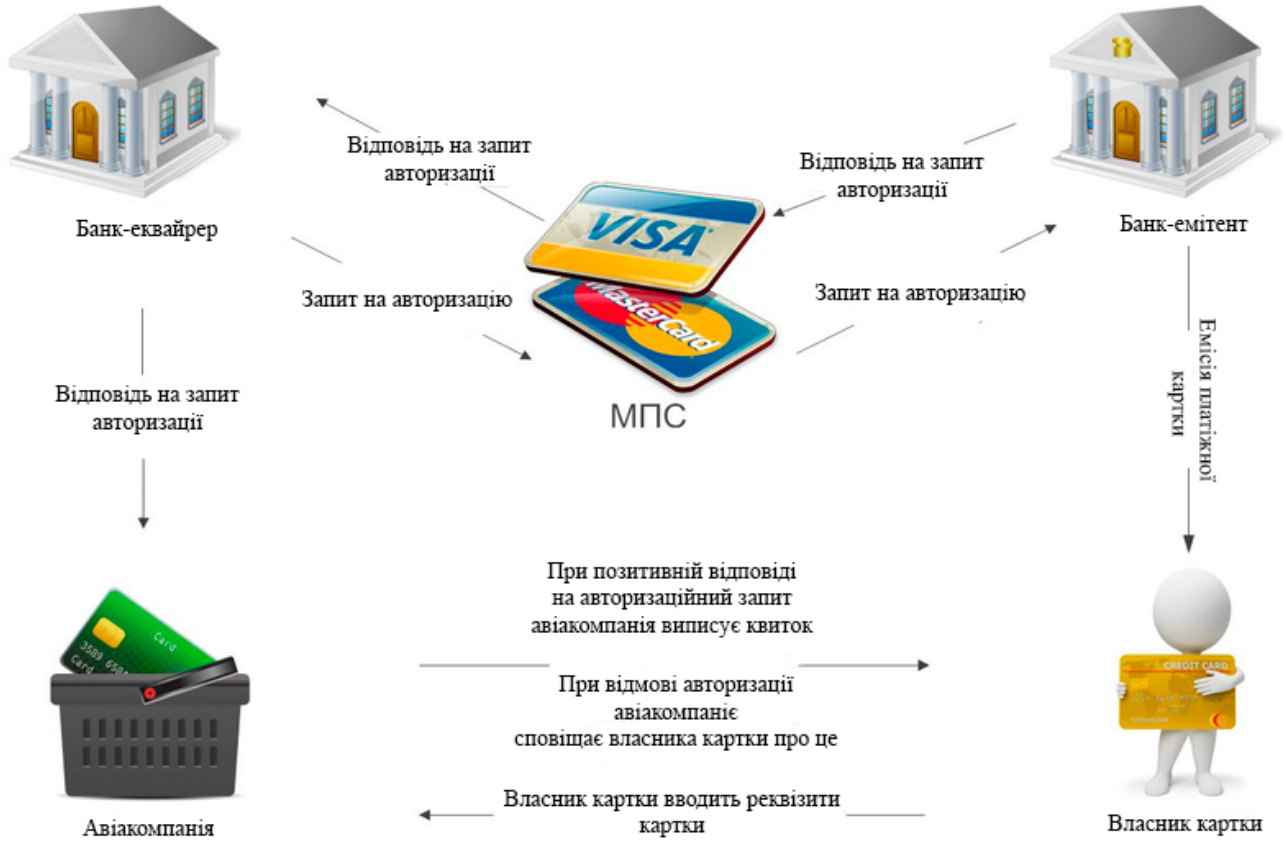

Рисунок 2.3 – Спрощена схема сплати при технології інтернет-еквайринг

2.2.4 Впровадження технології DLP

Технологія DLP (Data Leak Prevention) запобігає витоку конфіденційної інформації з інформаційної системи. DLP-системи будуються на аналізі потоків даних, які перетинають периметр інформаційної системи. Якщо була знайдена після аналізу потоків конфіденційна інформація - спрацьовує активна компонента системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Зазвичай DLP-система працює за наступним алгоритмом:

– перехоплення інформації (система фіксує файл - отриманий, відправлений, відкритий і тому подібне);

– аналіз інформації (система визначає, куди направляється документ і по налаштованим мітках визначає характер інформації в ньому, розуміє, що це за документ);

– блокування або повідомлення про інцидент (система визначає, наскільки операція над документом є легітимною (обробка по налаштованим політикам).

Досить часто співробітники викликають витік конфіденційної інформації не навмисно - причинами є неуважність, халатність чи некомпетентність. Однак випадки викрадення файлів з метою подальшого продажу конкурентам, помсти або відкриття власної компанії на основі унікальної інформації також є досить поширеними.

Звичайно, гарантувати абсолютний захист від наслідків діяльності працівників не може жодна DLP-система, але вона дозволяє значно мінімізувати ризики і наслідки людських помилок, а також забезпечують дотримання положень про захист конфіденційних даних.

Прикладом масштабного витоку конфіденційної інформації у сфері авіаперевезень може бути ситуація, яка склалась с авіакомпанією British Airways у 2019 році. Сумарно інцидент торкнувся близько 500 000 клієнтів даної авіакомпанії. Управління Комісара з інформації Великобританії (ICO) зобов'язало British Airways виплатити рекордний штраф в розмірі 183 000 000 фунтів за витік даних користувачів. У повідомленні ICO говорилось, що через неналежні заходи щодо забезпечення безпеки компрометації піддалися імена і адреси клієнтів авіакомпанії, а також їх облікові дані, дані платіжних карт і деталі бронювань.

Виходячи с цього, впровадження технології DLP є необхідністю для мінімізування ризиків витоку інформації. Так як на підприємстві ТОВ «СІМЛІ ЄЙР» встановлений антивірусний захист від компанії ESET, було обрано для впровадження ESET DLP SAFETICA.

SAFETICA зберігає важливі дані в компанії. Також контролює особисті пристрої співробітників, тому в захищеній корпоративному середовищі передача даних з цих пристроїв неможлива. Співробітники не можуть передати важливу інформацію конкурентам або використовувати її для власних потреб. Захищає важливі дані навіть в разі їх втрати. Весь диск або вибрані файли залишаються зашифрованими і нечитабельними для сторонніх осіб, дозволяє контролювати

використання принтера, додатків, а також обмежувати надмірне використання Інтернет-мережі. Створює звітність щодо всіх операцій з файлами, довгострокових тенденцій, короткострокових коливань активності, всіх веб-сайтів, електронної пошта і веб-пошти, а також миттєвого обміну повідомленнями, принтерами, активності екрану і відстеження натискання клавіш на клавіатурі.

SAFETICA складається з трьох модулів, які доповнюють один одного. Компонент «Аудитор» відстежує нелегітимні дії користувачів, а модуль «Супервайзер» запобігає небажану активність за рахунок заборони запуску певних програм, обмежень на відвідування веб-сайтів і тому подібне. Нарешті, модуль «DLP» захищає від витоку конфіденційної інформації і працює в автоматичному режимі на основі призначених для користувача правил. Рішення базується на клієнт-серверній архітектурі. На робочих станціях разом з клієнтською частиною програмного забезпечення функціонує завантажувальний агент, який виконує завдання по установці, оновленню і управління. Для адміністрування, налаштування і відображення зібраної інформації використовується клієнт або веб-консоль WebSafetica. Відомості, отримані з окремих терміналів, і настройки для всіх компонентів SAFETICA зберігаються в базі даних на сервері.

2.3 Аналіз ризиків після впровадження комплексу захисту

Розглянемо таблицю 2.2, в якій показано як змінилися показники ризиків після впровадження всіх запропонованих технологій, вимог з інформаційної безпеки та поліпшення системи безперебійного живлення.

Таблиця 2.2 – Модель загроз з визначенням рівня ризиків та збитків після впровадження рекомендацій

№	Механізм реалізації	Рівень		Сума загроз
		Ризиків	Збитків	
1. Загрози конфіденційності інформації				
1.1	Ненавмисне ознайомлення з ІОД під час співбесід персоналу ІТС зі сторонніми особами	2	2	4

Продовження таблиці 2.2 – Модель загроз з визначенням рівня ризиків та збитків після впровадження рекомендацій

№	Механізм реалізації	Рівень		Сума загроз
		Ризиків	Збитків	
1. Загрози конфіденційності інформації				
1.2	Втрата носіїв ІОД з причини безвідповідального ставлення до виконання обв'язків	1	3	4
1.3	Викрадення носіїв ІОД з метою несанкціонованого ознайомлення сторонніх осіб	1	2	3
1.4	Копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб	2	2	4
1.5	Безпосередній доступ до ІОД будь-яким способом сторонніх осіб	1	3	4
1.6	Перегляд інформації на екранах моніторів, робочих місцях; підслуховування	2	1	3
2. Загрози цілісності інформації				
2.1	Помилки (ненавмисні) користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях	1	2	3
2.2	Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях	1	2	3
2.4	Навмисне пошкодження носіїв інформації користувачами ІТС, яке призвело до модифікації або спотворення інформації	1	2	3
2.5	Помилки (ненавмисні) адміністраторів ІТС при налагодженні засобів захисту та системного ПЗ, в наслідок яких стала можливою модифікація ІОД	1	3	4
3. Загрози доступності				
3.1	Помилки (ненавмисні) користувачів ІТС, які призвели до знищення інформаціїабо втрати доступу до неї	2	2	4

Продовження таблиці 2.2 – Модель загроз з визначенням рівня ризиків та збитків після впровадження рекомендацій

№	Механізм реалізації	Рівень		Сума загроз
		Ризиків	Збитків	
3.Загрози конфіденційності інформації				
3.2	Втрата електропостачання серверу, яке призвело до знищення інформації або втрати доступу	2	2	3
3.4	Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації	2	2	4
3.5	Навмисне пошкодження парольних носіїв персоналом ІТС, яке призвело до втрати доступу до інформації	2	2	4

Спираючись на таблицю 2.2, можна спостерігати, що рівень ризику загроз зменшився відносно того, що було до впровадження рекомендацій. Після прийняття рекомендацій сума загроз складає:

- копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб (3 бали);
- перегляд інформації на екранах моніторів, робочих станцій та підслуховування (3 бали);
- втрата електропостачання серверу, яке призвело до знищення інформації або втрати доступу (3 бали);
- модифікація або спотворення інформації на жорстких дисках (3 бали).

Завдяки впровадженню технології інтернет-еквайрингу ми спостерігаємо, що зменшився ризик загрози «перегляд інформації на екранах моніторів, робочих станцій та підслуховування», так як у цьому випадку на екрані монітора не відображаються банківські дані клієнтів авіакомпанії.

Впровадження вимог з інформаційної безпеки та DLP технології вплинуло за зменшення рівня ризику загроз «копіювання ІОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб» та «модифікація або спотворення

інформації на жорстких дисках». Так як DLP дозволяє контролювати пересування файлів, які містять конфіденційну інформацію, та створює звіти по пересуванню, тобто можна побачити, хто з персоналу обробляв ці файли та що було зроблено з ними.

Поліпшення системи безперебійного живлення призвело до зменшення ризику загрози «втрата електропостачання серверу, яке призвело до знищення інформації або втрати доступу».

2.4 Висновки до спеціальної частини

Загрози інформації можуть заподіяти велику шкоду як обладнанню, яке належить підприємству ТОВ «СІМЛІ ЄЙР», так і клієнтам авіакомпанії. В спеціальній частині кваліфікаційної роботи було наведено оцінку існуючого захисту ОІД, розроблено вимоги з інформаційної безпеки, а також запропоновано методи запобігання витоку інформації, а саме:

- впровадження технології інтернет-еквайрингу;
- поліпшення системи безперебійного живлення;
- впровадження технології DLP.

Також проаналізовано функціональний профіль захисту, який використовується на підприємстві ТОВ «СІМЛІ ЄЙР».

РОЗДІЛ 3 ВИЗНАЧЕННЯ ВИТРАТ НА ПРОЕКТУВАННЯ ТА ЕКСПЛУАТАЦІЮ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Компанія ТОВ «СІМЛІ ЄЙР» – провідний аутсорсинговий постачальник послуг у сфері авіаперевезень. Підприємство з мільйонним оборотом займає одне з лідируючих положень в Україні, яке працює з авіакомпаніями та агентствами. ТОВ «СІМЛІ ЄЙР» співпрацювало з такими авіакомпаніями та агентствами:

- WizzAir;
- Ukraine International Airline;
- Cheap O` Air.

Річні прибутки підприємства – 2 240 000 млн. грн. Дане підприємство веде свою діяльність з 2007 року. Чисельність співробітників складає сто двадцять чотири особи, IT-відділ складається з 4 осіб; охорона – 3 особи ; директор – 1 особа; HR-менеджери – 4 особи; тренер – 1 особа; менеджер проекту, керівники відділів, агенти – 111 осіб.

Метою цього розділу є обґрунтування економічної доцільності вдосконалення захисту інформації на підприємстві.

3.1 Визначення витрат на впровадження нововведень

3.1.1 Визначення трудомісткості розробки та розрахунок витрат на створення вимог з інформаційної безпеки

Трудомісткість створення вимог з інформаційної безпеки визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації за умови роботи одного робітника:

$$t = t_{\text{тз}} + t_{\text{â}} + t_{\text{à}} + t_{\text{пр}} + t_{\text{опр}} + t_{\text{ä}} = 6 + 2 + 4{,}5 + 4{,}3 + 12 + 9{,}1 = 37{,}9 \text{ людино} - \text{годин} \quad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку вимог;

$t_{â}$ – тривалість вивчення технічного завдання, літературних джерел;

$t_{à}$ – тривалість розробки вимог;

$t_{\text{пр}}$ – тривалість реалізації вимог;

$t_{\text{опр}}$– тривалість опрацювання та ознайомлення співробітників з вимогами;

$t_{ä}$ – тривалість підготовки технічної документації на персональному комп'ютері;

Витрати на створення вимог з інформаційної безпеки $К_{\text{рв}}$ складаються з витрат на заробітну плату на спеціаліста з інформаційної безпеки $З_{\text{зп}}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на персональному комп'ютері $З_{\text{мч}}$:

$$К_{\text{рв}} = З_{\text{зп}} + З_{\text{мч}} = 4184{,}16 + 2609{,}03 = 6793{,}19 \text{ грн} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{\text{зп}} = t \cdot З_{\text{іб}} = 37{,}9 \cdot 110{,}4 = 4184{,}16 \text{ грн} \quad (3.3)$$

де *t* – загальна тривалість створення програмного забезпечення, годин;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки у Дніпропетровській області з нарахуваннями, грн/годину.

Вартість машинного часу для розробки вимог на персональному комп'ютері визначається за формулою:

$$З_{\text{мч}} = t \cdot С_{\text{мч}} = 37{,}9 \cdot 68{,}84 = 2609{,}03 \text{ грн} \quad (3.4)$$

де *t* – трудомісткість розробки вимог з інформаційної безпеки на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу персональному комп'ютері, грн./година.

Вартість 1 години машинного часу персонального комп’ютера визначається за формулою:

$$C_{\text{мч}} = P \cdot t \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p} = 0{,}8 \cdot 37{,}9 \cdot 2{,}13 + \frac{16000 \cdot 0{,}5}{2002} + \frac{2300 \cdot 0{,}24}{2002} = 64{,}58 +$$

$$3{,}99 + 0{,}27 = 68{,}84 \text{ грн/год} \qquad (3.5)$$

де P – встановлена потужність персонального комп’ютера, кВт;

C_e – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$– залишкова вартість персонального комп’ютера на кінець року, грн.;

H_a – річна норма амортизації на персональному комп’ютері, частки одиниці;

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

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

F_p – річний фонд робочого часу (за 40 – годинного робочого тижня F_p = 2002 год).

Таким чином, капітальні витрати на розробку та впровадження вимог з інформаційної безпеки складають 6793,19 грн.

3.1.2 Визначення та розрахунок витрат на придбання та монтаж дизель-електростанції

Капітальні витрати - грошові видатки, пов'язані з вкладеннями в основний капітал чи в приріст виробничих запасів.

Вартість витрат на впровадження дизель-електростанції визначено формулою:

$$К_е = К_{пр} + К_м = 637683{,}19 + 12500 = 650183{,}19 \text{ грн.} \qquad (3.6)$$

де $К_е$ – вартість витрат на придбання та встановлення дизель-електростанції;

$К_{пр}$ – вартість придбання;

$К_м$ – вартість монтажу.

На даний момент вартість обраної моделі дизель-електростанції JCB G140QS потужністю 112,2 кВт становить 637 683,19 грн. Її монтаж становить 12 500 грн.

Таким чином, витрати на встановлення дизель-електростанції складають 650183,19 грн.

3.1.3 Визначення та розрахунок витрат на впровадження технології інтернет-еквайрингу

Витрати на впровадження технології інтернет-еквайрингу визначаються за формулою:

$$К_{ie} = З_{зп} + З_{мч} + К_{пз} = 1600{,}8 + 998{,}18 + 2800 = 5458{,}98 \text{ грн} \quad (3.7)$$

де $К_{ie}$- вартість впровадження технології;

$К_{пз}$ – вартість придбання ліцензійного ПЗ.

Трудомісткість впровадження технології інтернет-еквайрингу наведена в таблиці 3.1.

Таблиця 3.1 - Трудомісткість впровадження технології інтернет-еквайрингу

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год – осіб з податками	Сума, грн
Встановлення ПЗ	1	110,4	110,4
Налаштування ПЗ	1,5		165,6
Навчання персоналу	12		1324,8
Всього			1600,8

Вартість машинного часу впровадження інтернет-еквайрингу на персональному комп’ютері визначається за формулою:

$$З_{мч} = t \cdot С_{мч} = 14{,}5 \cdot 68{,}84 = 998{,}18 \text{ грн} \quad (3.8)$$

де t – трудомісткість розробки вимог з інформаційної безпеки на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу персональному комп'ютері, грн./година.

Вартість 1 години машинного часу персонального комп'ютера розрахована в розділі 3.1.1 за формулою (3.4) та становить 68,84 грн

Таким чином, впровадження технології інтернет-еквайрингу коштуватиме підприємству ТОВ «СІМЛІ ЄЙР» 5458,98 грн.

3.1.4 Визначення та розрахунок витрат на впровадження технології DLP

Витрати на впровадження технології DLP визначаються за формулою:

$$К_{пу} = З_{зп} + З_{мч} + К_{пз} = 2208{,}0 + 1376{,}8 + 1325 = 4909{,}8 \text{ грн} \quad (3.9)$$

де $К_{пу}$- вартість впровадження технології;

$К_{пз}$ – вартість придбання ліцензійного ПЗ.

Трудомісткість впровадження технології DLP наведена в таблиці 3.2.

Таблиця 3.2 - Трудомісткість впровадження технології DLP

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год – осіб з податками	Сума, грн
Встановлення ПЗ	2	110,4	220,8
Налаштування ПЗ	6		662,4
Навчання персоналу	12		1324,8
Всього			2208,0

Вартість машинного часу впровадження інтернет-еквайрингу на персональному комп'ютері визначається за формулою:

$$З_{мч} = t \cdot С_{мч} = 20 \cdot 68{,}84 = 1376{,}8 \text{ грн} \quad (3.10)$$

де t – трудомісткість розробки вимог з інформаційної безпеки на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу персональному комп’ютері, грн./година.

Вартість 1 години машинного часу персонального комп’ютера розрахована в розділі 3.1.1 за формулою (3.4) та становить 68,84 грн

Таким чином, впровадження технології DLP коштуватиме підприємству ТОВ «СІМЛІ ЄЙР» 4909,8 грн.

Таким чином, сукупні капітальні витрати складають:

$$K = K_{\text{пу}} + K_{\text{ie}} + K_{e} + K_{\text{рв}} = 4909{,}8 + 5458{,}98 + 650183{,}19 + 6793{,}19 = 667345{,}16 \text{ грн} \quad (3.11)$$

3.2 Розрахунок поточних (експлуатаційних) витрат

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

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

1. вартість Upgrade – відновлення й модернізації системи ($С_в$);
2. витрати на керування системою в цілому ($С_к$);
3. витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ – "активність користувача").

Під "витратами на керування системою" маються на увазі витрати, пов'язані з керуванням і адмініструванням серверів та інших компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

1. навчання адміністративного персоналу й кінцевих користувачів;
2. амортизаційні відрахування від вартості обладнання та програмного забезпечення;
3. заробітна плата обслуговуючого персоналу;
4. аутсорсинг (тобто залучення сторонніх організацій для виконання деяких видів обслуговування);
5. навчальні курси й сертифікація обслуговуючого персоналу;

6. технічне й організаційне адміністрування й сервіс.

3.2.1 Розрахунок поточних витрат на вимоги з інформаційної безпеки

У зв’язку зі швидким розвитком інформаційної інфраструктури та технологій необхідно підтримувати актуальність розроблених вимог інформаційної безпеки. Для цього потрібно кожні пів року розглядати документ та якщо необхідно вносити корективи до нього.

Таблиця 3.2 - Трудомісткість розгляду вимог на можливість внесення необхідних коректівів

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год – осіб з податками	Сума, грн
Аналіз тенденцій	1	110,4	110,4
Розгляд існуючого документу	0,5		55,2
Можливе внесення коректівів	1	110,4	110,4
Всього			276,0

Поточні затрати на підтримання актуальності вимог з інформаційної безпеки становлять 276,0 грн.

3.2.2 Розрахунок поточних витрат при експлуатації дизель-електростанції

Ймовірне використання дизель-електростанції складає 120 год, оптова закупівля дизельного палива – 22 грн/л. В таблиці 3.3 наведені поточні витрати при експлуатації.

Таблиця 3.3 – Поточні витрати при експлуатації дизель-електростанції

Склад витрат	Сума, грн
Проведення технічного обслуговування	2250
Витрати палива	78 144
Амортизаційні відрахування	31 884,16
Всього	112 278,16

Амортизаційні відрахування розраховані за прямолінійним методом нарахування за умов, що залишкова вартість становитиме 0 грн, а строк корисного використання складе 20 років за формулою:

$$А = \frac{В_п - В_з}{T} = \frac{637\,683{,}19 - 0}{20} = 31\,884{,}16 \text{ грн} \quad (3.12)$$

де А – сума річних амортизаційних відрахувань;

$В_п$ – вартість дизель-електростанції;

$В_з$ – залишкова вартість;

T – строк корисного використання.

Спираючись на дані наведені в таблиці 3.3 можна побачити, що сумарні експлуатаційні витрати складають 112 278,16 грн.

3.2.3 Розрахунок поточних витрат при використанні технології інтернет-еквайрингу

Поточні (експлуатаційні) витрати використання технології інтернет-еквайрингу розраховуються за формулою:

$$С_п = С_л + С_о + С_н = 2800 + 0 + 768 = 3568 \text{ грн} \quad (3.13)$$

де $С_п$ – поточні витрати;

$С_л$ – витрати на продовження ліцензії;

$С_о$ – витрати на оновлення ПЗ;

$С_н$ – витрати на навчання нового персоналу користуванню програмним забезпеченням;

Для розрахування витрат на навчання нового персоналу користуванню програмним забезпеченням використовується формула:

$$С_н = t_в \cdot З_п = 12 \cdot 64 = 768 \text{ грн} \quad (3.14)$$

де $t_в$ – час витрачений на навчання нового персоналу;

$З_п$ – погодинна оплата тренера.

В середньому на навчання приходять шість нових співробітників кожного місяця. Вони навчаються групою, тому на їх навчання витрачається одна година. За рік проходить навчання 72 персони. Виходячи з цього час витрачений на навчання ($t_в$) складає 12 годин на рік.

Поточні (експлуатаційні) витрати використання технології інтернет-еквайрингу становлять 3568 грн.

3.2.4 Розрахунок поточних витрат при використанні технології DLP

Поточні (експлуатаційні) витрати використання технології DLP можна розрахувати за формулою:

$$С_п = С_л + С_о = 1325 + 358{,}38 = 1683{,}48 \text{ грн} \quad (3.15)$$

де $С_п$ – поточні витрати;

$С_л$ – витрати на продовження ліцензії;

$С_о$ – витрати на оновлення ПЗ;

Для розрахування витрат на оновлення ПЗ використовується формула:

$$С_о = З_{зп} + З_{мч} = 220{,}8 + 137{,}68 = 358{,}38 \text{ грн} \quad (3.16)$$

За умови, що трудомісткість оновлення складає 2 години.

Поточні (експлуатаційні) витрати використання технології DLP становлять 1683,48 грн.

Таким чином сукупна величина поточних витрат складає:

$$C = \sum C_{п} = 276 + 112278{,}16 + 3568 + 1683{,}48 = 117805{,}64 \text{ грн} \quad (3.17)$$

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

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки та можливих економічних втрат. Дана величина відображає частину прибутку, яка могла бути втрачена.

3.3.1 Оцінка величин збитків

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

1. порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
2. порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
3. порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
4. порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Можна виділити й деякі універсальні форми нанесення збитку, наприклад, порушення конфіденційності, доступності, цілісності або автентичності ресурсу можна характеризувати як компрометацію ресурсу, тобто втрату довіри до нього

користувачів (це може мати прямий збиток, зв'язаний, наприклад, з переустановленням програмного забезпечення або проведенням розслідування).

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

Необхідні вихідні дані для розрахунку:

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

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

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

$З_о$ – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

Заробітна плата не повинна бути нижче мінімальної заробітної плати на 01 січня поточного року. Ставка єдиного соціального внеску 22% и більше згідно класу професійного ризику підприємства, на якому проводиться захист інформації.

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та програмних інженерів), осіб.;

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

О – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

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

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число можливих атак на рік.

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

$$U = П_п + П_в + V = 12150 + 16650{,}4 + 4602{,}73 = 33\,403{,}13 \text{ грн.} \quad (3.18)$$

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), грн;

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

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

$$П_п = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_п = \frac{\sum 15120 \cdot 18}{168} \cdot 7{,}5 = 12\,150 \text{ грн} \quad (3.19)$$

де F – місячний фонд робочого часу (при 40 – а годинному робочому тижні становить 160 – 176 ч).

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

$$П_в = П_{ви} + П_{пв} + П_{зч} = 6480 + 2870{,}4 + 7300 = 16\,650{,}4 \text{ грн.} \quad (3.20)$$

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

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

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

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

$$П_{ви} = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_{ви} = \frac{\sum 15\,120 \cdot 18}{168} \cdot 4 = 6480 \text{ грн.} \quad (3.21)$$

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

$$П_{пв} = \frac{\sum З_о \cdot Ч_о}{F} \cdot t_в = \frac{\sum 18\,547{,}2 \cdot 4}{168} \cdot 6{,}5 = 2870{,}4 \text{ грн} \quad (3.22)$$

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

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) = \frac{2\ 240\ 000}{8760} \cdot (7{,}5 + 6{,}5 + 4) = 4602{,}73 \text{ грн.} \quad (3.23)$$

де $F_г$ – річний фонд часу роботи організації (організація працює цілодобово) становить близько 8760 ч.

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

$$B = \sum\sum U \cdot N \cdot I = \sum\sum 33\ 403{,}13 \cdot 2 \cdot 1 = 66\ 806{,}26 \text{ грн} \quad (3.24)$$

3.4 Загальний ефект від впровадження комплексу заходів

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

$$E = B \cdot R - C = 66\ 806{,}26 \cdot 4 - 117\ 805{,}64 = 149\ 419{,}4 \text{ грн.} \quad (3.25)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

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

C – щорічні витрати на експлуатацію всіх заходів, грн.

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у. спеціальній частині кваліфікаційній роботі, здійснюється на основні визначення та аналізу наступних показників:

– Сукупна вартість володіння (ТСО);

– Коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
– Термін окупності капітальних інвестицій.

Ключовою перевагою показника ТСО є те, що він дозволяє зробити висновки про доцільність реалізації проекту в області інформаційної безпеки на підставі оцінки одних тільки витрат.

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

У цьому випадку необхідно порівняти сукупну вартість володіння, щодо удосконалення системи інформаційної безпеки.

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

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

$$ROSI = \frac{E}{K} = \frac{15806{,}88}{667345{,}16} = 0.02239 \quad (3.26)$$

де E – загальний ефект від впровадження системи інформаційної безпеки;
K – капітальні інвестиції.

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{667355{,}16}{149\,419{,}4} = 4{,}5 \text{ роки} \quad (3.27)$$

Виходячи з формули (3.27) можна побачити, що термін окупності дорівнює 4,5 роки.

3.6 Висновки

Успішно реалізована атака на корпоративну мережу підприємства ТОВ «СІМЛІ ЄЙР» може заподіяти прямі фінансові витрати організації. Економічно проаналізовано весь об’єкт на впровадження системи інформаційної безпеки. У процесі розрахунків був досліджений комплекс захисту на економічну ефективність, який впроваджується в інформаційну систему.

На підставі проведених розрахунків можна зробити наступні висновки:

Визначена та детально розрахована трудомісткість реалізації комплексу захисту;

Досліджені всі можливі фінансові витрати на реалізацію комплексу захисту;

Проаналізована величина збиту після проведених атак на систему;

Розрахована ефективність впровадження систем інформаційної безпеки.

Розрахувавши всі критерії можемо зробити висновок, про те що є ефективно впровадження цієї інформаційної безпеки. Так, як загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе 66 806,26 грн, а після впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки становить 149 419,4 грн.

ВИСНОВКИ

У кваліфікаційній роботі розв’язано завдання щодо поліпшення КСЗІ на підприємстві та удосконалення існуючих систем інформаційної безпеки.

Було виконано:

- детальний аналіз споруди. Розглянуті ситуаційний план, генеральний план.
- проаналізоване програмне забезпечення, яке використовується;
- класифікація інформації, що циркулює на ОІД;
- проаналізовані всі можливі вразливості;
- проаналізовані загрози для оброблюваної інформації на ТОВ «СІМЛІ ЄЙР»;
- розроблена модель порушника;
- наведено оцінку існуючого захисту ОІД;
- розроблено вимоги з інформаційної безпеки, а також запропоновано методи запобігання витоку інформації.

Прораховані такі об’єкти на підприємстві ТОВ «СІМЛІ ЄЙР»:

- трудомісткість реалізації всіх рекомендацій;
- можливі фінансові витрати на реалізацію та впровадження поліпшень КСЗІ;
- Загальний збиток від атак до і після впровадження.

Загальний збиток від атак буде складати 66 806,26 грн, а після впровадження профілю захищеності загальний ефект буде складати 149 419,4 грн, тобто реалізація та поліпшення КСЗІ є економічно ефективне.

ПЕРЕЛІК ПОСИЛАНЬ

1. Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки. Методики виявлення закладних пристроїв. НД ТЗІ 2.7-011-2012 – Київ 2012 р.;
2. Методи і засоби пошуку електронних пристроїв перехоплення інформації [Електронний ресурс] – Режим доступу до ресурсу: http://www.analitika.info/poisk.php?page=1&full=block_article35;
3. Vpn з’єднання [Електронний ресурс] Режим доступу:https://habrahabr.ru/post/164301/;
4. Класифікація загроз в інформаційній безпеці [Електронний ресурс] - Режим доступу: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml;
5. Модель порушника. Мета та принципи розробки [Електронний ресурс] Режим доступу: http://www.rusnauka.com/11_EISN_2010/Informatica/63866.doc.htm;
6. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-1999 – Київ 1999 р. ;
7. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99 – Київ 1999 р. ;
8. Класифікація інформаційних об'єктів [Електронний ресурс] – Режим доступу: http://www.razgovorodele.ru/security1/safety04/inf08.php;
9. Літнарович Р. М. Сучасні технології інформаційної безпеки – Навчальний посібник – Рівне 2011.
10. Про інформацію: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua
11. Про телекомунікації: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

12. Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6/;
13. Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/.
14. Крижанівський В. Б. КОНСПЕКТ ЛЕКЦІЙ з курсу «Безпека інформаційних систем» [Електронний ресурс] / В'ячеслав Борисович Крижанівський. – 2012. – Режим доступу до ресурсу: https://learn.ztu.edu.ua/mod/resource/view.php?id=201
15. Aladdin – защита информации, информационная безопасность, аутентификация [Електронний ресурс] http:// URL http://www.aladdin.ru/
16. Принципи організації захисту інформації в сучасних інформаційно- комунікаційних системах і мережах [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/16_ADEN_2010/Informatica/68642.doc.htm;
17. Перешкоди в мережі електроживлення [Електронний ресурс]. – Режим доступу: http://www.epos.ua/view.php/about_pubs_archive?subaction=showfull&id=1013724 000&archive=&start_from=&ucat=3&;
18. Найбільш поширені проблеми мережі і необхідність використання ИБП для серверного, промислового і іншого устаткування. [Електронний ресурс]. – Режим доступу: http://pcm.ru/support/tech/6812
19. Джерела безперебійного живлення (ДБЖ) [Електронний ресурс]. – Режим доступу: http://www.sven.fi/ua/press/publications/detail.php?id=6925;
20. Лопухин А.А. Джерела безперебійного живлення без секретів [Електронний ресурс]. – Режим доступу: https://www.twirpx.com/file/42131/
21. Основні параметри вибору UPS [Електронний ресурс]. – Режим до- ступу: http://pcm.ru/support/tech/681

22. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	27	
6	А4	2 Розділ	21	
7	А4	3 Розділ	14	
8	А4	Висновки	1	
9	А4	Список літератури	2	
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 Глушан Р.С.docx

2 Пояснювальна записка Глушан Р.С.docx

3 Презентація Глушан Р.С.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

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

В І Д Г У К

на кваліфікаційну роботу бакалавра на тему:
Комплексна система захисту інформації
інформаційної системи ТОВ «СІМЛІ ЄЙР»
студента групи 125-16-3
Глушана Ростислава Сергійовича

Кваліфікаційна робота за спеціальністю 125 «Кібербезпека» студента Глушана Ростислава Сергійовича представлена пояснювальною запискою на 77 сторінок, що містить 16 таб., 12 рис., 4 додатків та 22 джерела.

Метою кваліфікаційної роботи є поліпшення комплексної системи захисту інформації інформаційної системи на підприємстві ТОВ «СІМЛІ ЄЙР».

На сьогоднішній день нагальною постає проблема збільшення інформаційної безпеки підприємства, яка значною мірою залежить від ступеня захищеності інформаційної сфери, тому поліпшення комплексної системи захисту інформації інформаційної системи ТОВ «СІМЛІ ЄЙР» є надзвичайно актуальним.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності бакалавра спеціальності 125 «Кібербезпека», а зміст та структура роботи дозволяють розкрити поставлену тему повністю.

Практична значущість роботи полягає в можливості використання розроблених рекомендацій при розробці комплексної системи захисту інформації на реальному об’єкті інформаційної діяльності.

В ході виконання кваліфікаційної роботи студент Глушан Р.С. проявив самостійність в роботі, працьовитість і володіння теоретичними та практичними знаннями.

Оформлення пояснювальної записки до дипломного проекту виконано з незначними відхиленнями від стандартів.

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

Загалом кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи бакалавра та заслуговує оцінки *“добре/80”*, а Глушан Ростислав Сергійович присвоєння йому кваліфікації бакалавра з спеціальності 125 «Кібербезпека».

Керівник кваліфікаційної роботи
д.т.н. проф. кафедри БІТ В.І. Корнієнко

Керівник спеціальної частини,
асистент кафедри БІТ Ю.А. Мілінчук