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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Мінченко Микити Владиславовича*

академічної групи *125-18-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи підприємтсва ТОВ "Рейтранс"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Сафаров О.О.	98	відмінно	
розділів:				
спеціальний	к.т.н., доц. Сафаров О.О.	98	відмінно	
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	

Рецензент				

Нормоконтролер	ст.в. Тимофєєв Д.С.	90	відмінно	

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Мінченко М.В.* **академічної групи** *125-18-3*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи підприємтсва ТОВ "Рейтранс"*

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

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Провести огляд внутрішнього та зовнішнього середовища об'єкта, розглянути обчислювальну систему та інформаційне середовище.	14.04.2022
Розділ 2	Розробити моделі порушника та загроз, запропонувати методи та засоби захисту, проаналізувати ризики після впровадження програмно – технічних та організаційних рішень	07.05.2022
Розділ 3	Виконати техніко-економічне обґрунтування доцільності запровадження запропонованих заходів захисту інформації	02.06.2022

Завдання видано _____ Сафаров О.О
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: 20.01.2022
Дата подання до екзаменаційної комісії: 15.06.2022

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

РЕФЕРАТ

Пояснювальна записка: 89 с., 11 рис., 21 табл., 5 додатків, 14 джерел.

Об'єкт розробки: інформаційно-телекомунікаційна система ТОВ «Рейтранс».

Предмет розробки: елементи політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Рейтранс»

Мета кваліфікаційної роботи: підвищення загального рівня інформаційної безпеки у інформаційно- телекомунікаційній системі.

У першому розділі розглянуті загальні відомості про організацію, наведена причина створення КСЗІ та політики безпеки інформації, проаналізована нормативно-правова база у сфері захисту інформації, виконано обстеження об'єкту інформаційної діяльності (ОІД), де циркулює інформація з обмеженим доступом (ІзОД), аналіз відомостей про підприємство та особливості обробки інформації, яка циркулює в компанії.

У другому розділі виходячи з даних першого розділу, проаналізовано потенційні загрози та вразливості, розроблені моделі порушника та модель загроз. Згідно отриманих даних сформовані основні елементи політики безпеки інформації для інформаційно-телекомунікаційної системи (ІТС) за для мінімізації втрат ресурсів компанії.

В економічній частині здійснені розрахунки капітальних витрат на внесення основних елементів політики безпеки інформації та визначена доцільність їх впровадження.

Практична значимість роботи полягає у підвищенні рівня інформації безпеки, для мінімізації потенційних витрат при загрозах інформації, з врахуванням властивості її обробки в ОІД.

МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, ГЕНЕРАЛЬНИЙ ПЛАН, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНІ ПОТОКИ, ВРАЗЛИВОСТІ, ЗАХИСТ ІНФОРМАЦІЇ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.

ABSTRACT

Explanatory note: 89 p., 11 pictures, 21 tables, 5 applications, 14 sources.

Object of development: information and telecommunication system LLC «Raytrans».

Subject of development: elements of the information security policy of the information and telecommunication system LLC «Raytrans».

The purpose of the qualification work: increasing the overall level of information security in the information and telecommunication system.

The first section considers the general information about the organization, gives the reason for the creation information security policy, the relevance of creation and analyzes the legal framework in the field of information protection, performed a survey of the object of information activities, which circulates information with limited access, analysis of information about the company and the features of processing information circulating in the company.

In the second section, based on the data of the first section, potential threats and vulnerabilities are analyzed, violator models and threat models are developed. According to the data obtained, the main elements of the information security policy for the information and telecommunications system are formed to minimize the loss of company resources.

In the economic part, the main calculations of capital expenditures for the introduction of the main elements of information security policy to determine the feasibility of their implementation.

The practical significance of the work is to increase the level of information security to minimize the potential costs of information threats, taking into account the nature of its processing in the information and telecommunication system.

THREAT MODEL, INFORMATION SECURITY POLICY, GENERAL PLAN, VULNERABILITIES, INFORMATION SECURITY, RISK ASSESSMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ТОВ - товариство з обмеженою відповідальністю;

ТТН - товарно-транспортна накладна;

НД ТЗІ – нормативний документ технічного захисту інформації;

АС - автоматизована система;

КЗ – контрольована зона;

ДТЗС - допоміжні технічні засоби і системи;

ІзОД - інформація з обмеженим доступом;

ІТС - інформаційно-телекомунікаційна система;

КСЗІ - комплексна система захисту інформації;

НСД - несанкціонований доступ;

ОІД - об’єкт інформаційної діяльності;

ТКВІ – технічні канали витоку інформації;

ПБ - політика безпеки;

ПЗ - програмне забезпечення;

ПК - персональний комп’ютер;

АЗ – апаратне забезпечення;

USB - Universal Serial Bus;

CD - Compact Disc

ЗМІСТ

ВСТУП

Ми живемо у часи розвитку інформації та інформаційних технологій. У сучасному світі інформація є одним з найважливіших ресурсів. Інформаційні процеси відбуваються у матеріальному світі, живій природі та людському суспільстві. Ці процеси вивчаються багатьма науковими дисциплінами. Зараз людина навряд чи змогла б уявити своє життя без комп'ютера, телевізора, телефону, Інтернету. Всі перераховані вище предмети та інструменти служать цілям зберігання та передачі інформації.

Інформаційні технології є найважливішою складовою процесу використання інформаційних ресурсів у суспільстві. Впровадження інформаційних технології є однією з головних революційних змін, що відбуваються сьогодні у різних сферах та особливо у галузі бізнесу . Вони стали незамінним засобом взаємодії всіх суб'єктів ринку, інструментом ведення бізнесу, що застосовується для здійснення більшості бізнес-процесів компаній.

Сучасні організації активно використовують інформаційні технології, зокрема можливості Інтернету, що допомагає їм:

- створювати стратегічну перевагу у бізнесі;
- забезпечити мобільний доступ до інформації про організацію.

Глобальний зв'язок та системи управління доставляють споживачеві інформацію про пропозиції, якість та ціни і дозволяють здійснювати угоди та замовлення протягом 24 годин на добу в будь-якому місці, де є доступ до мережі.

Безсумнівно, організаціям вигідно використовувати інформаційні технології при здійсненні своєї діяльності, оскільки вони сприяють розвитку діяльності, поширенню інформації про організацію, а внаслідок чого підвищується популярність фірми, збільшується кількість замовлень.

Зі зростанням впливу технологій постає також питання безпеки інформації.

З підвищенням впливу компаній на ринку з'являються конкуренти, впроваджується нове програмне забезпечення, обладнання та технологічні рішення. З цим зростає шанс перехоплення конфіденційної інформації, її знищення або модифікація.

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

В цій роботі буде розглянуто підприємство “Рейтранс”, його фізична та інформаційна структура, обґрунтування необхідності створення КСЗІ для інформаційно – технологічної системи підприємства.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про організацію ТОВ “Рейтранс”

Підприємство “Рейтранс” – траснпортно – логістична компанія яка надає послуги з перевезення, сортування, зберігання вантажів та їх митного оформлення. Організація працює з 2015 року. Компанія має власний автопарк, що складається із вантажних автомобілів: Iveco (до 1,5 т); Volkswagen Crafter (до 5 т); Renault Master (до 7 т); тягачі марки MAN (до 20 т), а також залучений транспорт за договором експедицій.

Офіс компанії знаходитися на 2 поверсі (5-ти поверхова будівля) за адресою - місто Дніпро, вулиця В’ячеслава Липинского 9. Робочі часи підприємства - з понеділка по п’ятницю з 9:00 – 18:00.

За формою власності ТОВ “Рейтранс” – комерційна організація, що була зареєстрована 30.04.2015 як товариство з обмеженою відповідальністю.

Рисунок 1.1 – схема організаційної структури підприємства “ Рейтранс ”

Штат працівників (26) та службові обов’язки:

- Директор – Організація, координація та контроль роботи підприємства; Організація ефективної взаємодії структурних підрозділів підприємства; стратегічне планування розвитку підприємства та реалізація цих планів; участь у формуванні бюджету та контроль його виконання; забезпечення ефективного документообігу та своєчасного руху інформації у компанії.
- Керівник відділу маркетингу - розробка маркетингової стратегії підприємства; аналіз ефективності рекламних засобів; підрахунок коштів на проведення рекламної компанії; консультація, ведення переговорів та при необхідності проведення зустрічей з потенційними клієнтами.
- Спеціалісти з маркетингу(2) – допомагає керівнику відділу маркетингу проводити маркетинговий аналіз.
- Керівник відділу логістики та перевезень – стежить за технічним станом автопарку фірми; контролює процес ремонту та тестування придатності автотранспорту; виробляє всі необхідні документи для експлуатації вантажного транспорту; укладення договору транспортних послуг згідно з вимогами клієнта.
- Експедитори(3) - повинен організувати маршрут, який вибрав клієнт, а також забезпечити перевезення вантажу саме тим транспортним засобом, який необхідний для такого транспортування. Основними обов’язком експедитора є пошук та залучення експедиційного транспорту, якщо увесь транспорт фірми зайнятий.
- Диспетчери(3) – тримає зв'язок з водієм на всіх етапах перевозки вантажу; контролює процес завантаження і відвантаження; інформує водія о усіх можливих перешкодах на шляху до точки розвантаження; постійно тримає зв'язок з клієнтом для переказу інформації щодо розташування авто.
- Митний брокер(2) – забезпечує декларування товарів митному органу; надає документи, необхідні для здійснення митного оформлення та контролю, у тому числі митну декларацію; пред'являє товари митному

органу; митний брокер присутній на всіх етапах митного оформлення товару, а також сприяє працівникам митниці у проведенні такого оформлення; завжди присутній під час огляду вантажу є обов'язковою; у разі потреби за дорученням замовника здійснює сплату всіх митних платежів та зборів.

- Водії автотранспорту(9) – безпечне перевезення вантажу із точки А в точку Б; оформлення дорожніх листів; перевірка технічного стану перед виїздом та підтвердження його своїм підписом; контроль процесу завантаження товару в автомобіль; контроль температури в кузові та температури товару; контроль розвантажувального процесу автомобіля; виписати маршрутний лист - CMR або ТТН; дати необхідні екземпляри вантажоодержувачу; здати необхідні екземпляри на склад замовнику; здати потрібні екземпляри на фірму.
- Головний бухгалтер - керівництво веденням бухгалтерського обліку та складанням звітності на підприємстві; забезпечення складання розрахунків із зарплати, нарахувань та перерахувань податків та зборів до бюджетів різних рівнів, платежів до банківських установ; контроль за своєчасним та правильним оформленням бухгалтерської документації; Розподіл та виплата заробітної платні співробітникам.
- Бухгалтер – допомагає головному бухгалтеру у ведені бухгалтерського обліку підприємства; надання методичної допомоги працівникам підрозділів підприємства з питань бухгалтерського обліку, контролю та звітності; Виставлення рахунків та акт виконаних робіт для контрагентів; відправка документації почтою.
- Системний адміністратор - ремонт використовуваної техніки; забезпечення безперебійної роботи всіх ПК та усунення несправностей; допомога штатним співробітникам, які працюють з ПК та офісною технікою, електронною поштою тощо. у разі виникнення труднощів; оновлення та закупівля потрібної техніки та їх комплектуючих; забезпечення нормальної роботи операційних систем і набір робочих програм (ОС Windows, MS

Office і т.п.); встановлення та налаштування ПЗ для коректної роботи; своєчасне оновлення необхідного ПЗ; забезпечення інформаційної безпеки та захисту від хакерських атак та від спаму; створення резервних копій даних, видалення та їх відновлення у разі потреби; мережеве налаштування; налаштування мережного обладнання; забезпечення працездатності; забезпечення безпеки мережі; розширення мережі; створення та видалення облікових записів; форматування/редагування облікових записів;

Програміст 1С - Автоматизація діяльності компанії на базі 1С «Підприємство»; налаштування та адміністрування стандартних та нетипових конфігурацій на базі 1С; розробка конфігурацій під завдання підприємства; складання інструкцій та технічної документації до створюваного програмного продукту; підтримка та консультація користувачів.

1.2 Аналіз нормативно – правової бази у сфері захисту інформації

Під поняттям нормативно-правового забезпечення слід розуміти сукупність правових норм, що визначають порядок створення, правовий статус і функціонування захищених інформаційно-комунікаційних систем і мереж, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Розробка КСЗІ ґрунтується у відповідності до вимог чинного законодавства України та на основі нормативно-правових документів, серед яких можна виділити:

- Закон України "Про інформацію»;
- Закон України "Про захист інформації в автоматизованих системах";
- НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);
- НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію

Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

- НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р.№ 53);
- НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).;
- ДСТУ ISO/IEC 27001:2015 - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)- На заміну ДСТУ ISO/IEC 27001:2010
- НД ТЗІ 3.7-003-05 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»
- ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).
- стандарти ДСТУ ISO/IEC, що основані на міжнародних стандартах і відповідно до вимог, що висуваються до захисту інформації на підприємстві;
- НД ТЗІ 1.6-005-2013 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

1.3 Обґрунтування необхідності створення КЗСІ

Згідно з НД ТЗІ 3.7-003-05 - Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

На підприємстві наявна інформації, яка підлягає автоматизованій обробці та потребує захисту і забезпечення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів, розглянутих у підрозділі 1.2.

На підставі проведеного аналізу власником інформації, яким виступає директор, прийняте рішення щодо створення КСЗІ та видано наказ «Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на ТОВ “Рейтранс” (ДОДАТОК Б).

1.4 Обстеження ОІД

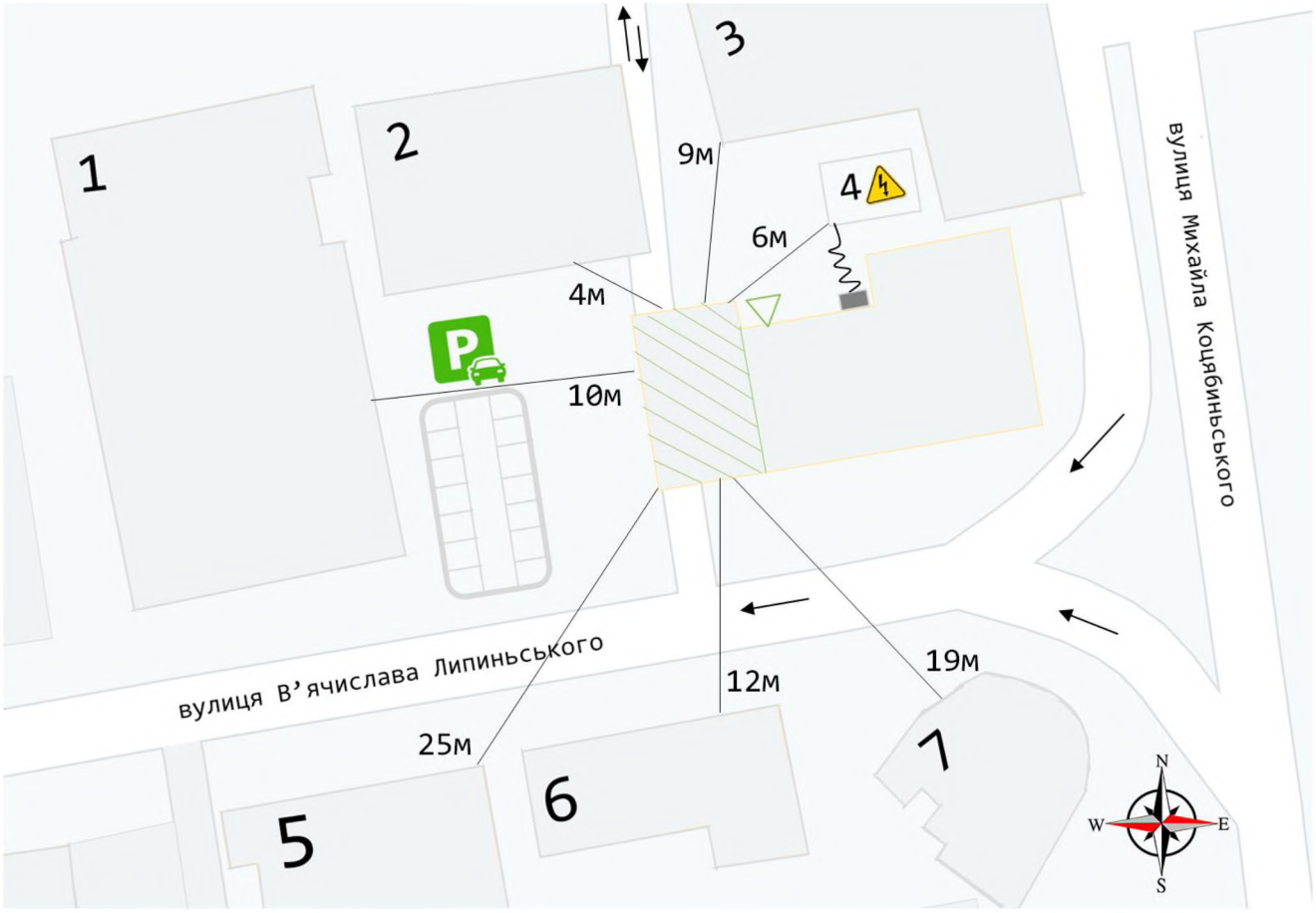
1.4.1 Ситуаційний план

Об’єктом інформаційної діяльності (далі ОІД) є приміщення та коридори офісу. ТОВ “Рейтранс” має офіс на 2 поверсі 5–ти поверхової будівлі яка розташована за адресою - місто Дніпро, вулиця В’ячеслава Липинского 9.

Схема ситуаційного плану та умовні позначення наведенні на рисунку 1.2.

Територія будівлі – відкрита; не огороджена парканом чи огорожею. Вхід до приміщення знаходиться у внутрішньому дворі на який виходять вікна офісу. Вхідні двері (металеві 60мм) оснащені магнітною стрічкою для ініціалізацій перепусток (вхід/вихід). Відеоспостереження – зовнішнє та внутрішнє цілодобове. Охоронний пункт на першому поверсі біля вхідних дверей, проводить верифікацію осіб які входять до будівлі та цілодобово веде моніторинг камер відеоспостереження.

Територія навколо – асфальтована. З західної сторони є паркувальний майданчик. З південної та східної сторін до будівлі прилягає дорога з односторім рухом транспорту, а на півночі з двостороннім.



УМОВНІ ПОЗНАЧЕННЯ

- Будівля
- Межа КЗ
- Територія ОІД
- Напрям руху транспорту
- Парковка
- 1 - Номер будівлі
- Трансформаторна підстанція
- Щиток
- Вхід до ОІД
- Лінія зв'язку щиту з транс. підстанцією

Рисунок 1.2 – схема ситуаційного плану ОІД

У таблиці 1.1 наведена характеристика прилеглих споруд.

Цілодобовий доступ в офіс мають лише директор компанії та охорона будівлі. Для решти працівників доступ відкривається виключно у робочі дні о 6

годині ранку та діє до 21 години вечора. Якщо комусь із співробітників треба потрапити до офісу в інший час – він має проінформувати директора та пояснити мету свого візиту.

Прибирання офісу проводиться у неділю з 10-11 години. Черговий охоронець який має ключі від усіх кімнат в будинку відкриває прибиральниці кімнату. Прибиральниця – найманий співробітник підприємства.

Таблиця 1.1 – Характеристика прилеглих споруд

Найменування	Кіл-ть поверхів	Адреса	Відстань до КЗ, м
Офісний будинок(місце ОІД)	5	Вул. В'ячеслава Липиньського 9	0
Торгівельний центр	6	Вул. В'ячеслава Липиньського 7Б	10
Відділення поліцій	3	Вул. В'ячеслава Липиньського 7	4
Житловий будинок	5	Вул. Михайла Коцюбинського 5	9
Трансформа-торна підстанція №17	1	Вул. В'ячеслава Липиньського 10	6
Житловий будинок	5	Вул. В'ячеслава Липиньського 14	25
Житловий будинок	3	Вул. В'ячеслава Липиньського 18	12
Магазин тканин	1	Вул. Михайла Коцюбинського 10	19

До будинку в якому знаходиться ОІД підключені такі комунікації:

Таблиця 1.2 - Системи комунікації

Електропостачання	Підключено до трансформаторної підстанції, яка має сторонніх споживачів і знаходиться за межами КЗ
Система опалення	Підключена до міської мережі опалення, знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Система каналізації	Підключена до міської мережі, яка знаходиться за межами КЗ
Система водопостачання	Підключена до міського водоканалу, яка знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Заземлення	Всі прилади, комп'ютери заземлені на спільний контур заземлення, який є замкнутий і виходить за межі КЗ
Система вентиляції	Приточно-витяжна
Internet	Кабельне підключення, що виходить за межі ОІД

Усі комунікацій виходять за межі контрольованої зони (КЗ).

Будівля обладнана системами електроживлення, опалення, водопостачання та каналізації, автоматичною пожежною сигналізацією.

Живлення систем освітлення, водопостачання та опалення здійснюється через підключення до міських комунальних мереж. Система пожежної сигналізації підключена на центральний пульт.

Схема підключення комунікацій та умовні позначення наведенні на рисунку 1.3

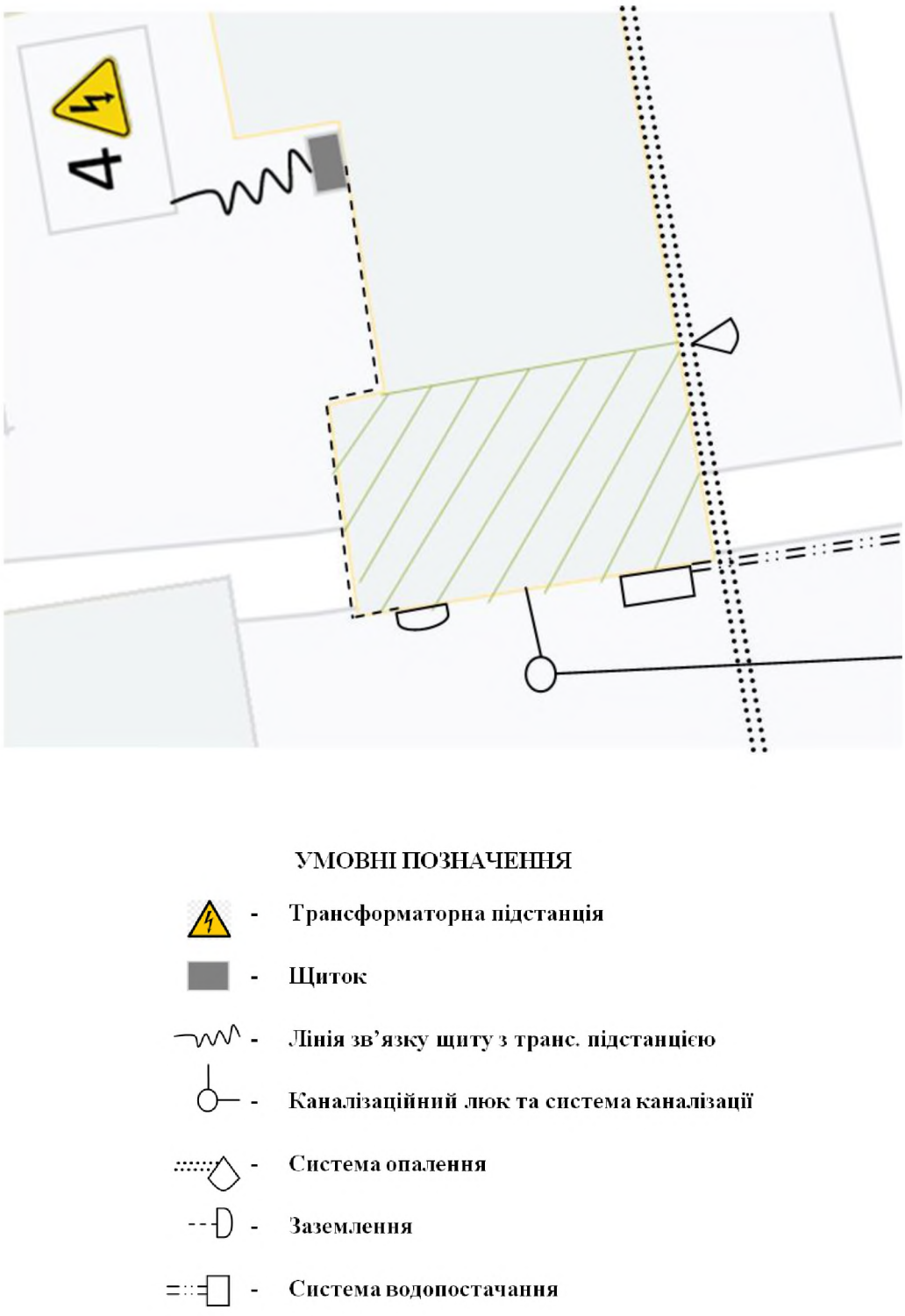


Рисунок 1.3 – Ситуаційний план. Схема комунікацій.

1.4.2 Генеральний план

ОІД це офіс який знаходиться на 2 поверсі 5ти поверхової будівлі.

Площина ОІД – 175,4 м^2 ;

До складу ОІД входять: кімната директора, кімната працівників відділу маркетингу, кімната бухгалтерів, логістичний відділ, кімната працівників тех. відділу, серверна, санвузол, коридор.

Генеральний план зображено на рисунку 1.4

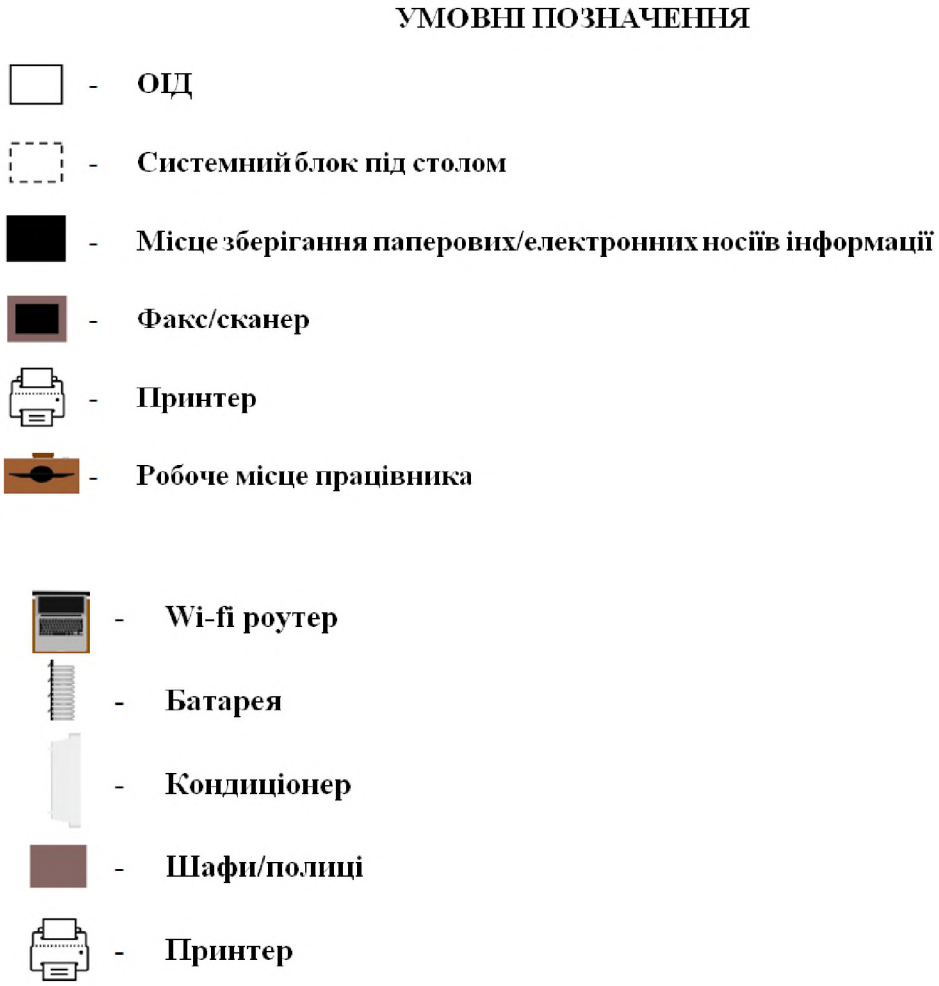


Рисунок 1.4 – Генеральний план

Характеристика складових ОІД:

– висота стель – 410 м;
– перекриття – 450 мм;
– стінні перегородки – 100 мм;
– стіни зовнішні з цегли – 450 мм.

Вікна: двостулковий метало-пластиковий склопакети у всіх приміщеннях розміром 1300х1210 мм. Віконні отвори обладнані регульованими пристроями типу: ролетні жалюзі. Звичайні жалюзі та завіси на вікнах відсутні.

Двері в приміщення металеві 2800х800. Дверні петлі захищені анти зрізами. Захисна металева внутрішня розсувна решітка на двері при вході до ОІД. На території ОІД встановлено 8 дерев'яних дверей, які замикаються на ключ. Висота – 2.1м. Ширина -1м. Ключ виготовлений із металу.

Для визначення засобів ТЗІ та їх місць знаходження слід врахувати характерні особливості ОІД: 2 поверх; в металевій шафі яка розташована в кімнаті директора , та має дві окремі полиці кожна з котрих замикається ключем (ключ знаходиться у директора) зберігаються паперові та електроні (2 окремі диски 1ТБ) носії інформації; усі прилеглі будівлі мають вихід на вікна ОІД.

Система електроживлення – централізована, виходить за межі ОІД до етажного розподільчого щитку, який з'єднаний головним щитком на 1 поверсі який підключений до трансформаторної підстанцій. Трансформаторна підстанція має сторонніх споживачів.

Лінія комп'ютерної мережі – вита пара, Wi-Fi роутер підключений до мережевого обладнання провайдеру. Провайдер – Lifecell. Схема електроживлення та освітлення надана на рисунку 1.5

Система водопостачання – централізована. Підключена до міського водоканалу, який знаходиться за межами КЗ. Система каналізації – підключена до міської системи каналізації. Схема водопостачання надана на рисунку 1.6

Система опалення – централізована. Підключена до систем теплопостачання, які знаходяться за межами ОІД. Труби системи опалення проходять через всі поверхи будівлі. На ОІД встановлено 11 радіаторів вертикального з'єднання. Схема опалення надана на рисунку 1.7

Система вентиляції – Проточно-витяжна, виходить за межі ОІД. Шахти вентиляції проходять через всі поверхи будівлі. Система вентиляції надана на рисунку 1.7

Система кондиціювання – виходить за межі КЗ і ОІД. На території встановлено 2 пристрої Mitsubishi Electric MSZ-DM35VA / MUZ-DM35VA (Потужність охолодження 3,5 кВ. Потужність нагріву 4,2 кВ). Система кондиціювання надана на рисунку 1.7

Система сигналізації – централізована, з виходом на пульт сигналізації який виходить за межі ОІД. При спрацьовані датчиків, сигнал з панелі сигналізації направляється на пульт охорони. Охорона знаходиться на 1 поверсі. Система охоронної сигналізації - Tiras Orion-4T3.2, система пожежної безпеки – датчики диму АРТОН ASD-10. На всіх вікнах (13 штук) розташованих та території ОІД встановлені датчики на відкриття вікна, рівня освітленості, температури і руху - Philio PST02-C – Z. На стінах усіх кімнат – датчик руху Right Hausen HN-061051 – інфрачервоний датчик з кутом виявлення -180 градусів. На вхідні двері – магнітоконтактний накладний SATEL B-3 A (відстань елементів при замиканні контактів – 38 мм, при розмиканні – 42 мм;). Такий самий датчик встановлено в металевій шафі в кімнаті директора де в паперових та електронних носіях зберігається інформація. Світло-звукова сигналізація August SIREN black знаходиться з зовнішньої сторони вхідної двері. Датчики диму знаходять у всіх приміщеннях і коридорах КЗ. Схема розміщення усіх датчиків та приладів сигналізації надана на рисунку 1.8.

Внутрішні камери відеоспостереження (GV-136-IP-H-COF40-30 4MP) розташовані в усіх кімнатах ОІД. Камери працюють в режимі он-лайн, спостерігати за камерами можна через спеціальний мобільний додаток, інформація за осатаній місяць зберігається в хмарі. Відеоспостереження цілодобове. Схема розміщення камер відеоспостереження надана на рисунку 1.8.

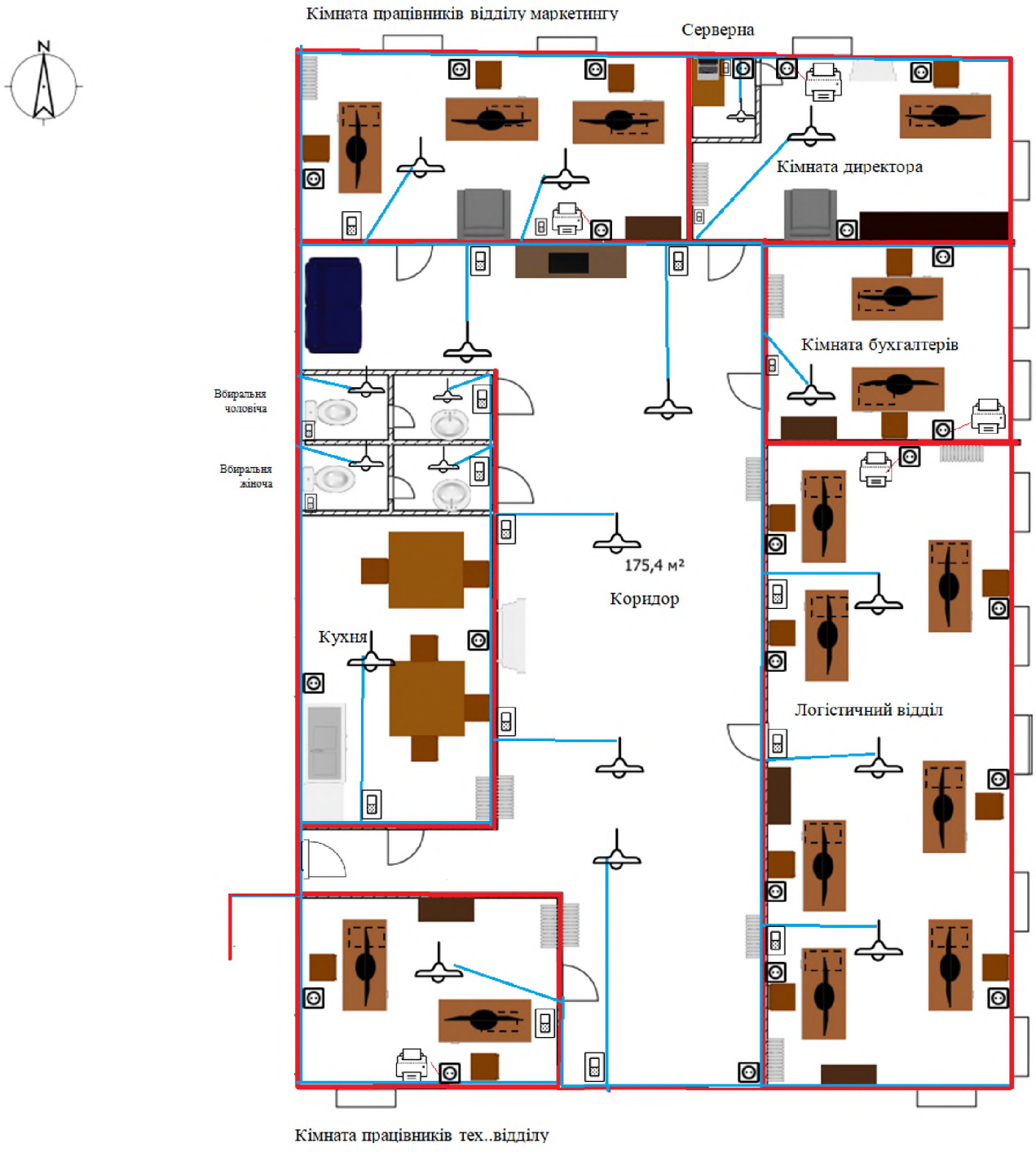


Рисунок 1.5 – Схема електроживлення і освітлення.

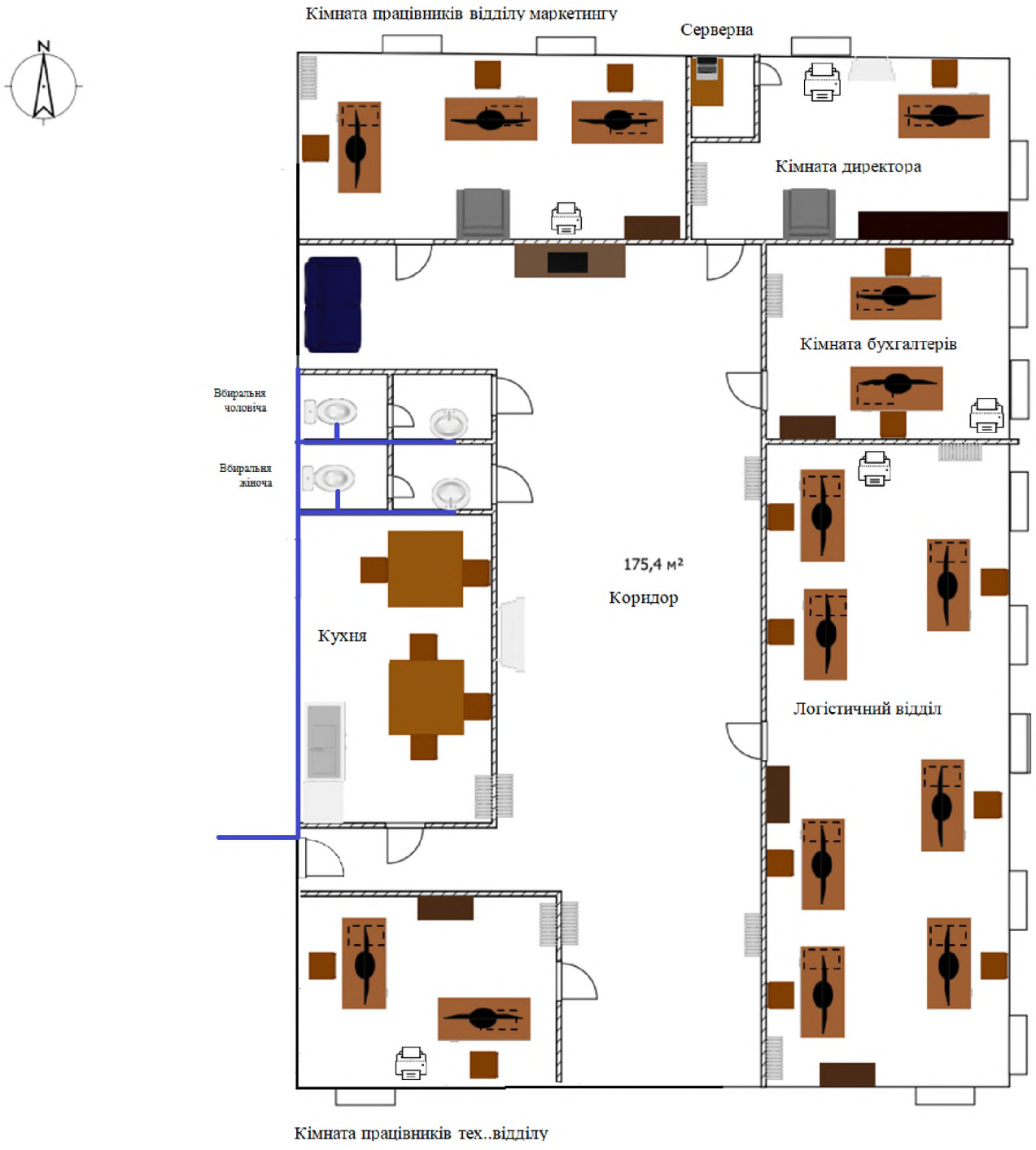


Рисунок 1.6 – Схема водопостачання.

Рисунок 1.7 – Схема опалення,вентиляції, кондиціювання.

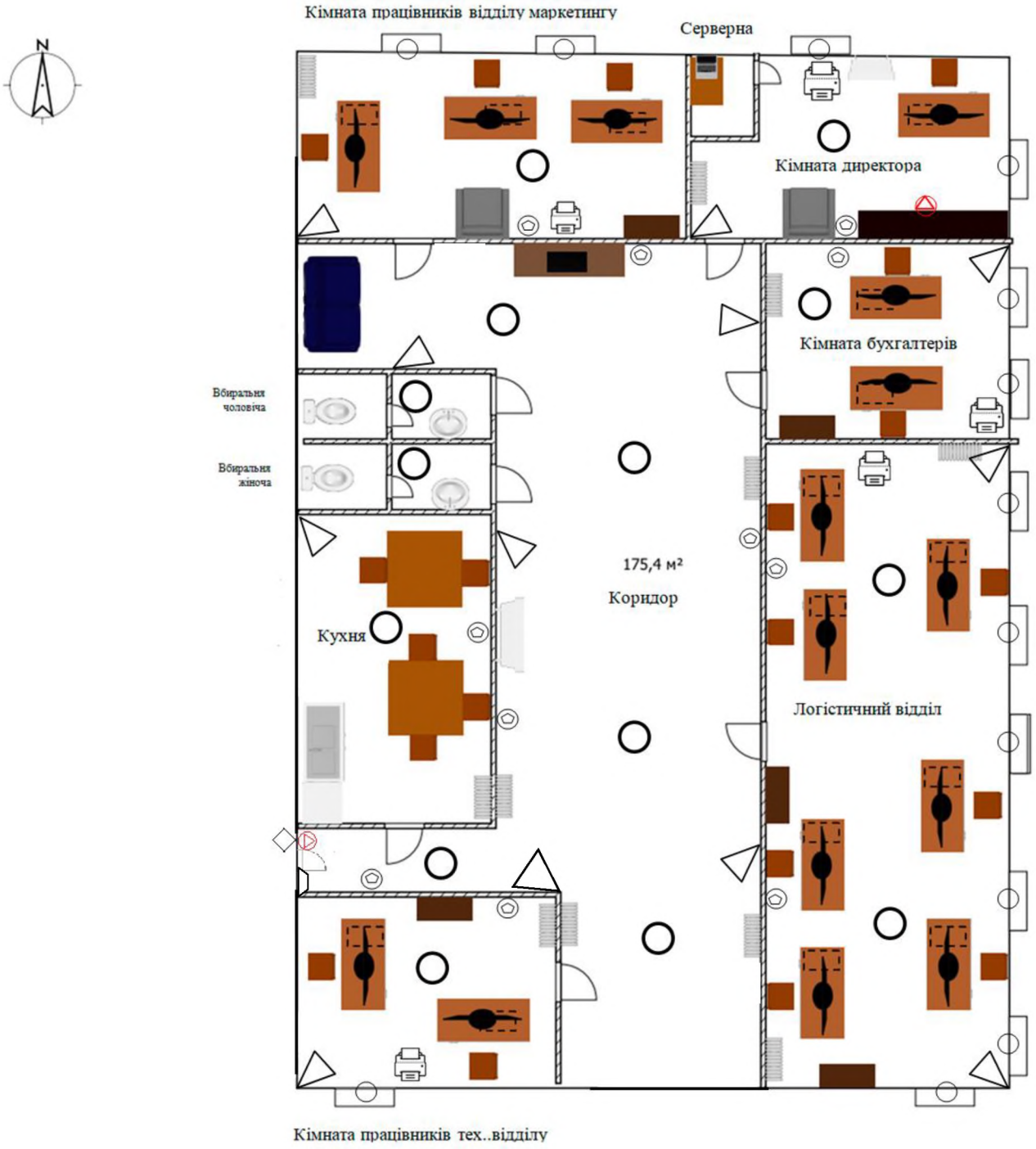


Рисунок 1.8 – Схема розміщення датчиків, приладів сигналізації та камер відеоспостереження.

УМОВНІ ПОЗНАЧЕННЯ

- Лінія систем електропостачання
- Лінія систем освітлення
- Лінія систем кондиціювання
- Лінія систем опалення
- Лінія систем водопостачання
- Шахта вентиляції
- Вентиляція
- Напрям руху повітря
- Освітлення
- Вимикач світла
- Розетка
- Датчик диму
- Датчик відкриття/розбиття скла
- Інфрачервоний датчик руху
- Магнітоконтактний датчик на двері/двері шафи
- Світло-звукова сигналізація
- Камера відеоспостереження
- ПКП Tiras Orion-4T3.2

1.4.3 Обстеження обчислювальної системи

Інформаційно – телекомунікаційна система ОІД представляє собою мережу типу ”Passive star”, яка налічує один комутатор. ІТС можна кваліфікувати як багатомашинний багатокористувацький комплекс, який в свою чергу має доступ до мережі Інтернет, та в якому циркулює інформація різних ступенів обмеження доступу. Комплекси з такими характеристиками відносяться до класу АС 3.
Структурна схема ІТС підприємства представлена на рисунку 1.9.

Інформація про ОТЗ та ДТЗС які використовуються на підприємстві наведена в таблиці 1.3 Та 1.4 відповідно

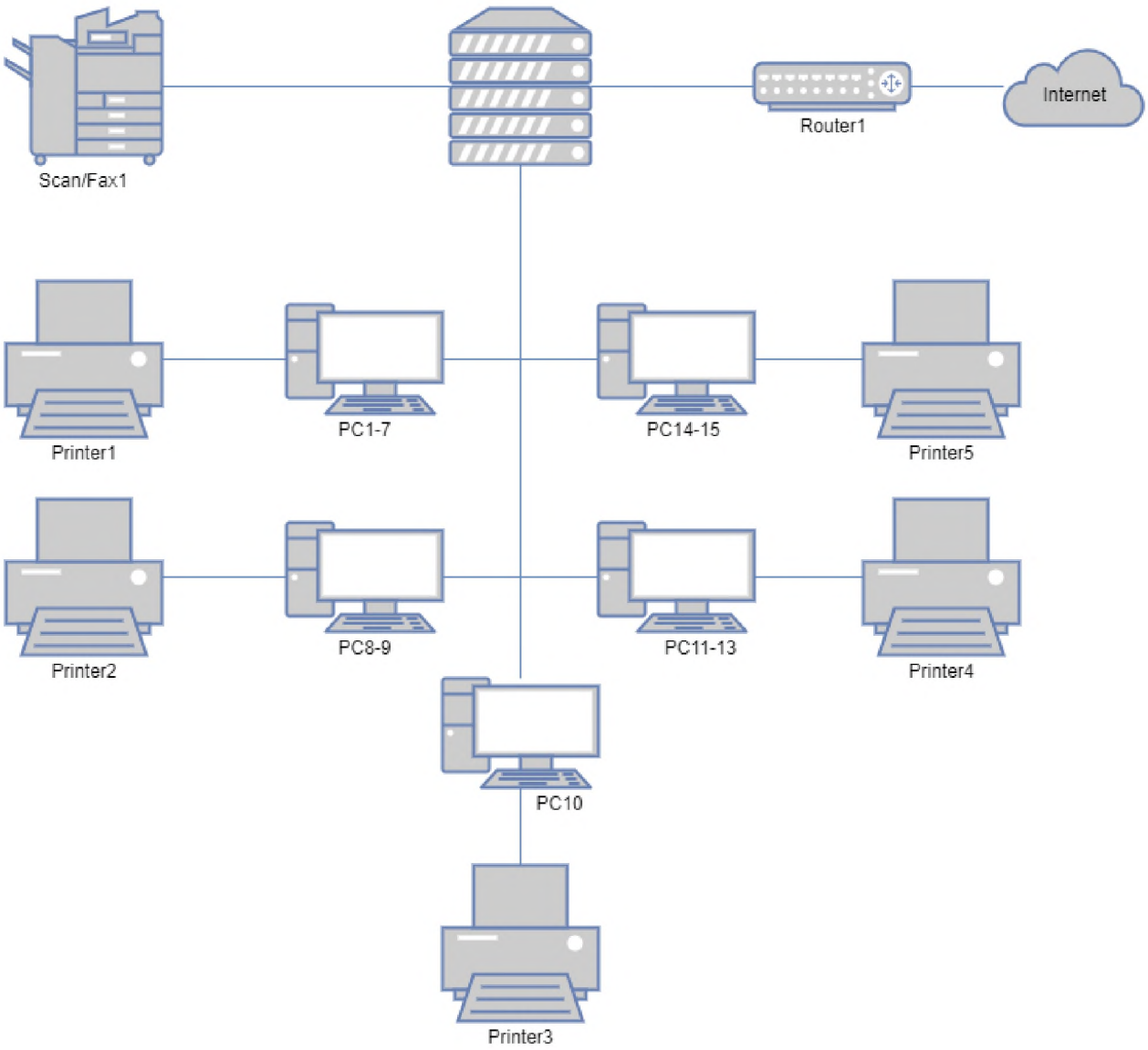


Рисунок 1.9 – Структурна схема ІТС

Таблиця 1.3 – ОТЗ на підприємстві

Ім’я в системі	Тип	Марка	Модель	Розміщення	Серійний номер	Відстань до границі КЗ, м
PC1	Комп’ютер	ASUS	S500MCR	На столі	x865FegZA8	2
PC2	Комп’ютер	ASUS	S500MCR	На столі	eu8Yx999TD	2
PC3	Комп’ютер	ASUS	S500MCR	На столі	2B4hFx3mX7	2
PC4	Комп’ютер	ASUS	S500MCR	На столі	7E4uACj	5
PC5	Комп’ютер	ASUS	S500MCR	На столі	D8KVbrh94	5
PC6	Комп’ютер	ASUS	S500MCR	На столі	sVnSJ4n492	5
PC7	Комп’ютер	ASUS	S500MCR	На столі	b9cP778LNg	5
PC8	Комп’ютер	ASUS	U500MA-R5300G00	На столі	5d4HN77Vny	2
PC9	Комп’ютер	ASUS	U500MA-R5300G00	На столі	c7VF6f7pA6	2
PC10	Комп’ютер	ASUS	U500MA-R5300G00	На столі	dC8yb3B5P7	3
PC11	Комп’ютер	ASUS	U500MA-R5300G00	На столі	s4mb47P7BB	7
PC12	Комп’ютер	ASUS	U500MA-R5300G00	На столі	e28vJ93DzL	7
PC13	Комп’ютер	ASUS	U500MA-R5300G00	На столі	33x53BbYvP	7
PC14	Комп’ютер	ASUS	G15CE-71170F0360	На столі	DN562vscA7	1
PC15	Комп’ютер	ASUS	G15CE-71170F0360	На столі	Ry8NdyU274	1
Printer1	Принтер	Canon	i-SENSYS X 1238p	На підлозі	KA223Bc7xe	1

Продовження таблиці 1.3 - ОТЗ на підприємстві

Ім'я в системі	Тип	Марка	Модель	Розміщення	Серійний номер	Відстань до границі КЗ, м
Printer2	Принтер	Canon	i-SENSYS X 1238p	На підлозі	8t3ND22Gez	3
Printer3	Принтер	Canon	i-SENSYS X 1238p	На підлозі	sP3b4a5EZ7	4
Printer4	Принтер	Canon	i-SENSYS X 1238p	На підлозі	iJ29GHa3z4	2
Printer5	Принтер	Canon	i-SENSYS X 1238p	На підлозі	2s2McgGM98	1
Scanner/Fax1	Сканер/Факс	ECOSYS	M5521cdn	На столі	47uxFA9dS3	3
Сервер	Сервер	Cisco	UCS C220	На підлозі	EVV86a	1
Wi-Fi роутер	Wi-Fi роутер	Xiaomi	ALOT ROUTER AC2350	На стіні	sMpG5766zT	
Клавіатура 15)	Клавіатура	A4TECH	KV-300H	На столі	kuTHf42D27	-
Комп. миша (15)	Комп'ютерна миша	Logitech	B100 USB Black	На столі	3jV8F9Zb3b	-

Таблиця 1.4 – ДТЗС на підприємстві

Назва	Модель	Розміщення	Серійний номер
Сітлодіодні лампи(35)	T8 9W 220V 600mm	На стелі	Sd7u8G82Ld
Датчики диму(14)	АРТОН ASD-10	На стелі	ic3RCfT942
ІЧ датчик(12)	Right Hausen HN-061051	На стелі	6tuJPE2i77

Обчислювальна система формується з 15 ПЕОМ (PC1-13 мають ОС – Microsoft Windows 10, PC14-15 – Linux Ubuntu 21.10), 5 принтерів та 1 факса/сканера та мережевого обладнання.

Мережеве обладнання:

- Сервер Cisco UCS C220
- Wi-Fi роутер XIAOMI MI ALOT ROUTER AC2350 (DVB4248GL)

Усього на підприємстві є 3 види комп'ютерів: U500MA-R5300G00, S500MC, G15CE-71170F0360.

Характеристика персональних комп'ютерів розташованих в логістичному відділі ASUS S500MCR (Ім'я в системі PC1-7):

- CPU: Intel Core i3-10105
- RAM: Kingston Fury DDR4-2666 4096MB
- HDD: Western Digital AV 500ГБ
- GPU: GEFORCE GT730 2048MB GIGABYTE
- Материнська плата: Asus PRIME H310M-K R2.0

Характеристика персональних комп'ютерів розташованих в кімнаті директора, бухгалтерії та відділі маркетингу ASUS U500MA-R5300G00 (Ім'я в системі PC8-13):

- CPU: AMD RYZEN 5 5600G
- RAM: DDR4-2666 8Gb PC4-21300 HyperX Fury Black
- HDD: Seagate BarraCuda HDD 2TB 7200rpm
- GPU: GeForce GTX 1650 OC 4GB GDDR6
- Материнська плата: Asus PRIME H610M-A D4

Характеристика персональних комп'ютерів розташованих в кімнаті працівників тех.. відділу ASUS G15CE-71170F0360 (Ім'я в системі PC14-15):

- CPU: Intel Core i7-11700F
- RAM: HYPERX Fury Black DDR4 2666MHz 16GB
- SSD: Samsung 870 QVO 1TB
- GPU: nVidia GeForce RTX 3080
- Материнська плата: MSI X470

Сервер (PC16) :

- CPU: INTEL Xeon E5-2620 V4 8C/16T/2.1GHz
- RAM: Kingston Fury DDR5-5600 32768MB PC5-44800 64GB
- HDD: Seagate SkyHawk Surveillance 4 TB

В таблиці 1.5 наведене програмне забезпечення яке встановлене на всіх ПК які використовуються на підприємстві ТОВ “Рейтранс”.

Таблиця 1.5 – Програмне забезпечення встановлене на ПК ОІД

Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
Windows 10(версія 1909)	Системне	Commercial	Операційна система	Безсетроково	PC1-13
Linux Ubuntu (версія 21.10)	Системне	Freeware	Операційна система	Безсетроково	PC14-15
MS Word 2019	Прикладне	Commercial	Створення та редагування текстових документів	Безсетроково	PC1-15
CRM(версія 3.1)	Прикладне	Shareware	Комунікація з клієнтами, автоматизація продажів	До 08.2024	PC7-11
MS Exel 2019	Прикладне	Commercial	Створення та редагування даних поданих у вигляді таблиць.	Безсетроково	PC1-15
Adobe Photoshop (версія 2021г.)	Прикладне	Commercial	Багатофункціональний графічний редактор	Безсетроково	PC1-15
Norton (версія 22.2.10)	Спеціалізо-ване	Commercial	Антивірус-на програма	Безсетроково	PC1-15
M.E.DOC (версія 13.08.037)	Прикладне	Commercial	Подання звітності в контролю- ючі органи в електронно-му вигляді	Безсетроково	PC8-9
1С. Бухгалтерія (версія 3.01.10.229)	Прикладне	Commercial	Бухгалтерська програма для автоматизо-ваного обліку	Безсетроково	PC8-10

Продовження таблиці 1.5 - Програмне забезпечення встановлене на ПК ОІД

Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
1С. Підприємство TMS Логістика (версія 2.03.11)	Прикладне	Commercial	Програма для автоматизації процесів на логістичному підприємстві	Безсетроково	РС1-15
ERP (версія 3.6.7)	Прикладне	Shareware	Планування ресурсів підприємства	До 10.2022	РС7-11

1.4.4 Обстеження інформаційного середовища

На підприємстві циркулює інформація з відкритим доступом до неї та з обмеженим. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Паперові документи зберігаються в кабінеті директора в металевій шафі. Ключ знаходиться у директора. Після втрати своєї актуальності документи знищуються. Обчислення та місце зберігання пристроїв які містять інформацію в електронному вигляді на підприємстві не відстежується.

Роль адміністратора мережі відведена системному адміністратору. До складу працівників служби безпеки входять охоронці які спостерігають за відеокамерами та слідкують за тим хто заходить до будівлі. Роль адміністратора служби безпеки на підприємстві не передбачена.

Всі працівники мають доступ до комп'ютерів авторизуються під власними обліковими записами, обмеження доступу до робочого місяця забезпечується паролем (кожен співробітник має свій унікальний пароль).

В ІТС підприємства оброблюється наступна інформація:

- інформація про контрагентів (персональна, договори співпраці)

- інформація про працівників (персональна, трудові договори)
- інформація про актуальні та виконанні замовлення
- фінансова звітність (банківські рахунки, виручка)
- інформація про бухгалтерські звіти
- інформація про ресурси підприємства
- інформація про технічний стан автомобілів
- реклама

Класифікація інформацій яка циркулює в ІТС підприємства наведена в таблиці 1.6.

Таблиця 1.6 – Класифікація інформації яка циркулює на ІТС

Вид інформацій	Режим доступу	Правовий режим	Вид зберігання в ІТС	Вимоги до захисту		
				К	Ц	Д
Інформація про контрагентів (персональна, договори співпраці)	ІЗоД	Конфіденційна інформація	Паперовий Електронний	3	2	2
Інформація про працівників (персональна, трудові договори)	ІЗоД	Конфіденційна інформація	Паперовий Електронний	4	4	2
Інформація про актуальні та виконанні замовлення	ІЗоД	Конфіденційна інформація	Паперовий Електронний	4	4	3
Фінансова звітність (банківські рахунки, виручка)	ІЗоД	Службова інформація	Електронний	3	4	4
Інформація про технічний стан авто.	ІЗоД	Службова інформація	Електронний	2	3	3

Продовження таблиці 1.6 - Класифікація інформації яка циркулює на ІТС

Вид інформацій	Режим доступу	Правовий режим	Вид зберігання в ІТС	Вимоги до захисту		
				К	Ц	Д
Інформація про ресурси підприємства	ІЗоД	Конфіденційна інформація	Електронний	3	4	3
Реклама	Відкрита інформація	Відкрита інформація	Електронний	1	2	3

Рівні конфіденційності:

- К1 - рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;
- К2 - рівень конфіденційності інформації, при якому компанія зазнає незначних збитків уразі розкриття інформації особам, що не мають допуску до неї;
- К3 - рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- К4 - рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;
- К5 - критичний рівень конфіденційності інформації, що може призвести до краха компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

- ЦІ - рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;
- Ц2 - рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;
- Ц3 - рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

- Ц4 - рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;
- Ц5 - критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

- Д1 - рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;
- Д2 - рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;
- Д3 - рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;
- Д4 - рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;
- Д5 - критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Всі інформаційні ресурси обробляються співробітниками підприємства – 6 працівників логістичного відділу, 2 бухгалтери, 2 спеціаліста з маркетингу, 2 працівника технічного відділу, 2 керівника відділів та директор.

Вся текстова інформація зберігається в кабінеті директора (окрема металева шафа, зачинена на ключ). Електронна інформація записується та зберігається на 2 окремих полицях шафи, у вигляді 1ТБ дисків. Копіювання інформації виконується кожен день на ці диски і на хмарне сховище.

Інформація про контрагентів (персональна, договори співпраці) – після обробки заявки клієнта на перевезення вантажу та створення договору надання транспортно-експедиційних послуг керівник логістичного відділу вносить клієнта в систему замовлень (1С. Підприємство TMS Логістика). Дані відображаються у експедитора який буде виконувати замовлення та у бухгалтера для перевірки. Зберігається переважно в електронному вигляді, але може бути роздрукована на всіх етапах.

Інформація про працівників (персональна, трудові договори) – обробляється керівниками відділів, бухгалтерами та директором. Роздруковані копій зберігаються в кабінеті директора.

Інформація про актуальні та виконанні замовлення – заявки на перевезення, акти виконаних робіт, транспортні листи, товаро – транспортні накладні, митні документи опрацьовуються переважно експедиторами, диспетчерами та митними брокерами. Митні брокери працюють за межами офісу та мають доступ до інформації лише яка зберігається в хмарному сховищі (Google Disk). Узгоджена з керівником логістичного відділу фінальна версія документів друкуються та віддається директору на зберігання, у разі потреби переглянути їх можна в електронному вигляді.

Бухгалтерська та фінансова звітність обробляється бухгалтерами (1С. Бухгалтерія, MS Exel) та перевіряється керівниками відділів. Бухгалтера зберігають звітність про оплату праці в електронному та паперовому вигляді.

Ресурси підприємства такі як: паливо для автомобілів, дрібні та розхідні автозапчастини, літні на зимові покришки, а також інформація про технічний стан автомобілів – відображується в програмі ERP, редагується керівником логістичного відділу, директором, бухгалтерами та зберігається виключно в електронному вигляді.

Реклама – фірма рекламує свої послуги на різних тематичних сайтах в мережі Інтернет.

Замовники звертаються до компанії самі (реклама), або маркетологи самі знаходять потенційних клієнтів (робота зі спеціальними платформами, обробка та аналіз даних підприємств які користувались аналогічними послугами); клієнт звертається до фірми зі своєю заявкою на перевезення до керівника логістичного відділу з яким ведуться переговори про з приводу перевезення (вага, об'єм, пункт перетину кордону, транзит, температурний режим вантажу та ін.). Узгодивши всі деталі клієнта вносять в програми клієнта вносять в програми (1С,ERP,CRM). Свої реквізити, юридичну адресу, та іншу допоміжну інформацію клієнти присилають на корпоративну почту. Після ознайомлення з заявкою керівником

відділу, його приймає в роботу експедитор – ведеться пошук автомобіля згодне з вимогами клієнта, визначається термін розвантаження. Якщо перевезення міжнародне з митним брокером обговорюються деталі перетину кордону. Перед завантаженням вантажу в автомобіль клієнт підписую сформований бухгалтерією договір (1С. Бухгалтерія, M.E.Doc). Диспетчер інформує клієнта про місцезнаходження, стан вантажу на кожному етапі перевезення від завантаження і до розвантаження. Оплата виконується клієнтом після огляду товару у місці розвантаження та надання усієї документації – підписаний акт виконаних робіт, підписаний договір, товаро – транспортна накладна або CMR (ТТН або CMR заповнюється водієм).

Схема інформаційних потоків зображена на рис 1.10

В таблиці 1. Наведена матриця розмежування доступу до інформації згідно з посадами співробітників ТОВ “Рейтранс”.

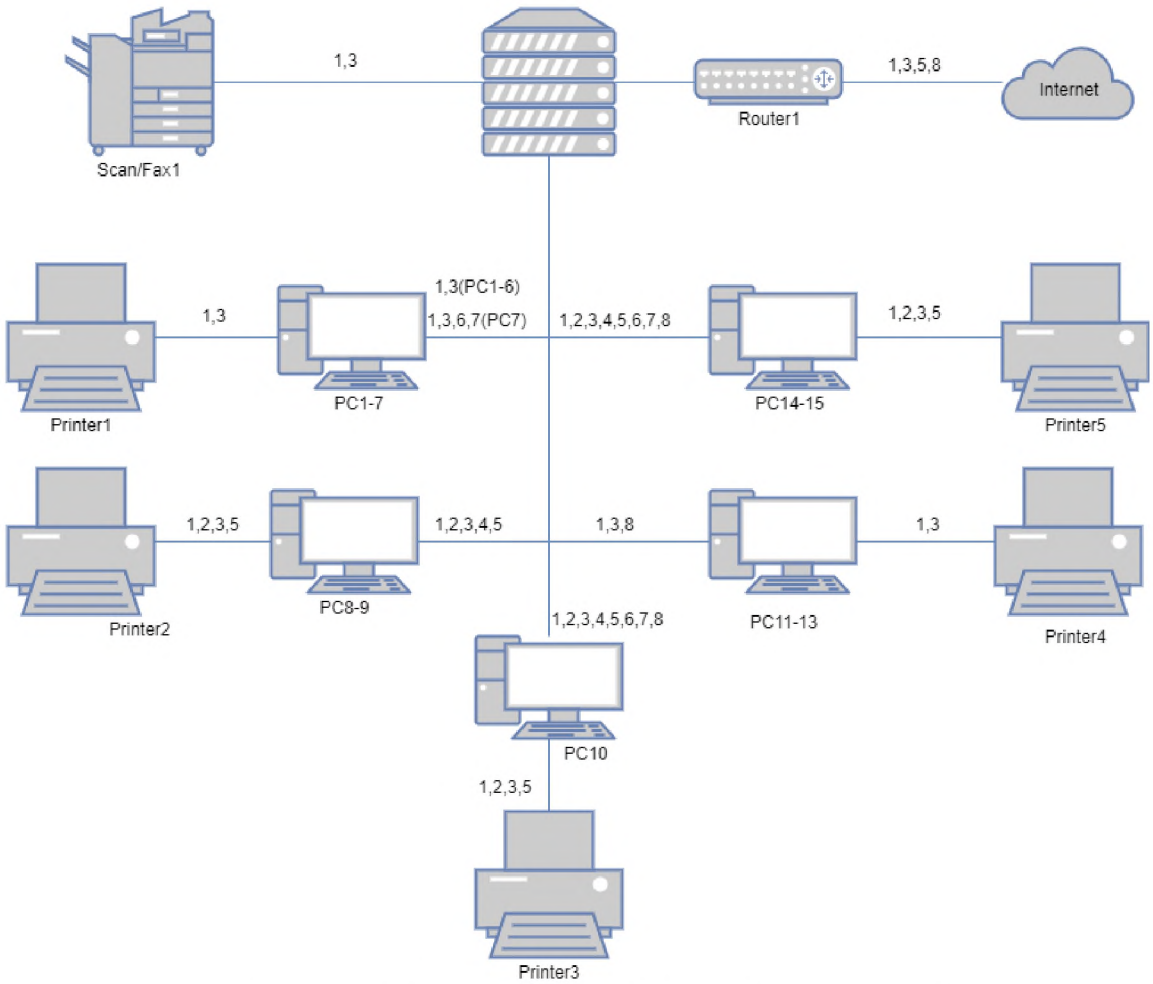


Рисунок 1.10 – Схема інформаційних потоків.

Інформаційні потоки:

- Обробка інформації про контрагентів (1)
- Обробка інформації про працівників (2)
- Обробка інформації про актуальні та виконанні замовлення (3)
- Обробка фінансової звітності (4)
- Обробка бухгалтерської звітності (5)
- Обробка інформації про ресурси підприємства (6)
- Обробка інформації інформація про технічний стан автомобілів (7)
- Обробка рекламних даних (8)

Таблиця 1.7 – Матриця розмежування доступу

	Д	КВЛ	КВМ	ПЛВ	ПМВ	ГБ	Б	СА	П1 С
Інформація про контрагентів	R,W,D, C,M,T	R,W,D, C,M,T	R,W,D, C,M,T	R,W, C,T	R,W, C,T	R,W,C, M,T	R,W,C, T	R	R
Інформація про працівників	R	R	R	-	-	R,W,D, C,M,T	R,W,C M,T	R	R
Інформація про актуальні та виконанні замовлення	R,W,D, C,M,T	R,W,D, C,M,T	R,W,C	R,W,D C,M	R,W,C	R,W,T	R,W,T	R	R
Фінансова звітність	R,W,D, C,M,T	R,W,D, C,M,T	R	-	-	R,W,D, C,M,T	R,W,C T,M	R	R
Бухгалтерська звітність	R,W,D, C,M,T	R,W,C, M,T	R	-	-	R,W,D, C,M,T	R,W,C T,M	R	R
Інформація про ресурси підприємства	R,W,D, C,M,T	R,W,C, M,T	R	R	-	R,W,M	R,W,M	R	R
Інформація про технічний стан автомобілів	R,W,D, C,M,T	R,W,D, C,M,T	R	R	-	R	R	R	R
Рекламні данні	R,W,D, C,M,T	R,W,D, C,M,T	R,W,D, C,M,T	R	R,W, C,M	R	R	R	R
Повноваження інсталювання ПЗ	+	-	-	-	-	-	-	+	+
Ресурси	РС10	РС7	РС11	РС1-6	РС12-13	РС8	РС9	РС 14	РС1 5

Умовні скорочення

Д – директор;

КВЛ – керівник логістичного відділу;

КМВ – керівник маркетингового відділу;

ПЛВ – працівник логістичного відділу;

ПМВ – працівник маркетингового відділу;

ГБ – головний бухгалтер;

Б – бухгалтер;

СА – системний адміністратор;

П1С – програміст 1С;

R – читання;

W – запис;

D – видалення;

С – створення нових файлів;

М – модифікація;

Т – перенесення;

1.5 Постановка задачі

Так як в інформаційному середовищі підприємства ТОВ “Рейтранс” циркулює інформація з обмеженим доступом, директором Бердніков С.В. було прийнято рішення про створення КЗСІ ,для цього потрібно:

- проаналізувати модель порушника;
- проаналізувати модель загроз;
- обрати методи та засоби захисту інформації;
- проаналізувати можливі ризики та загрози після впровадження КЗСІ.

1.6 Висновок до першої частини

У першому розділі кваліфікаційної роботи були розглянуті:

- загальні відомості про підприємство ТОВ “Рейтранс”.
- ситуаційний план
- генеральний план
- середовище обчислювальної системи

- інформаційне середовище

Виконаний аналіз нормативно – правової бази, що регулює відносини у сфері захисту інформації в Україні. Обґрунтована необхідність створення комплексної системи захисту інформації на підприємстві ТОВ “Рейтранс”. та виконано постановку задачі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Визначення моделі можливого порушника

Модель порушника інформаційної безпеки – це набір припущень про одного або кількох можливих порушників інформаційної безпеки, їх кваліфікацію, їх технічні та матеріальні засоби тощо. Правильно розроблена модель порушника є гарантією побудови адекватної системи забезпечення інформаційної безпеки. Спираючись на побудовану модель, можна будувати адекватну систему інформаційного захисту.

Найчастіше будується неформальна модель порушника, що відображає причини і мотиви дій, його можливості, цілі, їх пріоритетність для порушника, основні шляхи досягнення поставлених цілей: способи реалізації вихідних від нього загроз, місце і характер дії, можлива тактика і т.д. Для досягнення поставленої мети порушник повинен докласти певних зусиль і витратити деякі ресурси. Визначивши основні причини порушень, є можливим вплинути на них або необхідним чином скоригувати вимоги до системи захисту від даного типу загроз. Під час аналізу порушень захисту необхідно приділяти увагу суб'єкту (особистості) порушника. Усунення причин або мотивів, що спонукали до порушення, може допомогти уникнути повторення подібного випадку.

Потенційними порушниками є:

- особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв’язку або інших складових мережі передачі даних;
- користувачі автоматизованої системи;
- співробітники, які безпосередньо пов'язані з забезпеченням функціонування ІТС;
- особи, яким непередбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД.

Порушники бувають внутрішніми та зовнішніми.

Внутрішні порушники - порушники, які мають права доступу в контрольовану зону (територію) та (або) повноваження з автоматизованого доступу до інформаційних ресурсів та компонентів систем та мереж.

Категорії осіб, які можуть бути внутрішніми порушниками:

- Співробітники підприємства;
- Системний адміністратор.

Зовнішні порушники – особи, які не мають права доступу до інформаційної системи, її окремих компонентів та реалізують загрози безпеці інформації з-за кордонів інформаційної системи.

Зовнішнім порушником може бути особа з наступних категорії персоналу:

- Технічний персонал;
- Відвідувачі офісу;
- Стороні особи, що знаходяться за межами КЗ.

Для розробки моделі порушника буде використана система таблиць (Таблиці 2.1 – 2.6). Побудована модель повинна враховувати категорії, ознаки та характеристики можливих порушників для більш точного їх аналізу, при цьому рівень загрози вказується в окремому стовпчику і оцінюється за 5-ти бальною шкалою.

Таблиця 2.1 – Специфікація моделі порушника за мотивами здійснення порушень.

Позначення	Мотив порушення	Ефективний рівень загрози
M1	Безвідповідальність/недбалість.	5
M2	Самоствердження.	2
M3	Корислива цілеспрямованість.	4

Рівні кваліфікації порушників, які можуть загрожувати ІТС підприємства наведені в таблиці 2.2

Таблиця 2.2 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС.

Позначення	Основні кваліфікаційні ознаки порушника	Ефективний рівень загрози
К1	Володіє низьким рівнем знань та інформацією щодо функціонування ІТС, але вміє працювати з технічними засобами системи.	1
К2	Має середній рівень знань та практичних навичок роботи з технічними засобами ІТС та їх експлуатацією,	3
К3	Володіє базовими знаннями щодо функціонування обчислювальної техніки, ПЗ та практичними навичками роботи засобів які використані в ІТС.	4
К4	Володіє знаннями про функціонування засобів/механізмів захисту, що реалізовані в ІТС, їх недоліки та можливості.	5

Можливості використання засобів та методів подолання системи захисту наведені в таблиці 2.3.

Часові інтервали, під час яких порушник може нанести збиток інформаційній системі наведено в таблиці 2.4.

Таблиця 2.3 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту.

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
З1	Може спостерігати за об’єктом ззовні, підслуховувати розмови співробітників або поглянути у документи на робочих місцях	1
З2	Використовує лише штатні засоби, можливі недоліки системи для подолання системи захисту(несанкціовані дії з використанням дозволених засобів). Може використовувати переносні механічні носії інформації, які можуть бути пронесенні крізь охорону для копіювання даних.	2
З3	Має можливість використання повного функціоналу елементів захисту ІТС (конфігурує ПЗ), є авторизованим користувачем.	5

Продовження таблиці 2.3 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту.

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
З4	Використовує технічні засоби активного впливу для модифікації елементів ІТС, порушення нормальної роботи системи обчислення інформації, не є авторизованим користувачем.	4

Таблиця 2.4 – Специфікація моделі порушника за часом дії.

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
Ч1	Під час повної бездіяльності компонентів ІТС.	1
Ч2	Під час функціонування ІТС(або компонентів системи)	4
Ч3	Під час перерв роботи компонентів ІТС з метою обслуговування, модернізації обладнання або ремонту.	2
Ч4	Як у процесі функціонування, так і під час призупинки компонентів ІТС.	5

Припустимі місця виконання порушниками загроз ІТС підприємства наведені в таблиці 2.5

Таблиця 2.5 – Специфікація моделі порушника за місцем дії.

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
Д1	Усереднені приміщення, але без доступу до технічних засобів ІТС.	1
Д2	З робочих місць користувачів ІТС.	3
Д3	З доступом у зону управління засобами забезпечення безпеки ІТС.	5

Таблиця 2.6 – Категорія порушників окреслених у моделі.

Позначення	Визначення категорії	Ефективний рівень загрози
Внутрішні по відношенню до ІТС		
ПВ1	Користувачі ІТС.	3

Продовження таблиці 2.6 - Категорія порушників окреслених у моделі.

Позначення	Визначення категорії	Ефективний рівень загрози
ПВ2	Адміністратори системи, працівники служби безпеки.	4
ПВ3	Співробітники служби захисту установи, та керівники різних рівнів	5
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі офісу, запрошені з будь-якого приводу.	1
ПЗ2	Представники з технічно – експлуатаційних питань(енергопостачання, водопостачання, газопостачання, прибирання прилеглої території та ін.)	3
ПЗ3	Хакери	4
ПЗ4	Представники конкуруючих організацій	5

У стовпці “Ефективний рівень загрози” приведених вище таблиць наведено ранжування можливих збитків, які може спричинити порушник маючи наступні характеристики. Згідно до НДТЗІ 1.4-001-2000 рівень збитків характеризується таким чином:

1 – незначний або відсутній;

2 – нижчий за середній;

3 - середній;

4 – вищий за середній;

5 - значний(високий).

На основі таблиць 2.1 – 2.6 була побудована модель внутрішнього порушника – таблиця 2.7, та модель зовнішнього порушника – таблиця 2.8.

Таблиця 2.7 – Модель внутрішнього порушника.

Посада	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Категорія поршника	Сумарний рівень загрози
Д	М2	К3	З3	Ч2	Д3	ПВ1	23
КВЛ	М3	К4	З3	Ч4	Д3	ПВ1	27
КМВ	М3	К3	З2	Ч2	Д2	ПВ1	20
ПЛВ	М1	К2	З2	Ч2	Д2	ПВ1	20
ПМВ	М1	К1	З2	Ч2	Д2	ПВ1	18
ГБ	М1	К2	З2	Ч2	Д2	ПВ1	20
Б	М1	К1	З2	Ч2	Д2	ПВ1	18
СА	М3	К4	З3	Ч4	Д3	ПВ2	28
П1С	М1	К3	З2	Ч2	Д2	ПВ1	21

Таблиця 2.8 – Модель зовнішнього порушника.

Посада	Мот-ив	Квалі-фікація	Можли-вості	Час дії	Місце дії	Категорія поршни-ка	Сумарний рівень загрози
Персонал будівлі	М3	К2	З2	Ч3	Д2	ПЗ1	16
Прибиральниця	М1	К1	З1	Ч1	Д2	ПЗ1	12
Конкуренти	М3	К3	З4	Ч2	Д2	ПЗ4	24
Хакери	М3	К3	З4	Ч4	Д1	ПЗ3	22
Представники комунальних структур	М1	К2	З2	Ч1	Д2	ПЗ2	17
Відвідувачі офісу	М3	К1	З1	Ч2	Д2	ПЗ1	15

Розглянувши побудовані моделі порушників можна виділити наступне:

По – перше, проаналізувавши характеристики внутрішніх та зовнішніх порушників можна зазначити що саме внутрішні мають більший рівень загрози, адже вони мають доступ до цінних даних та діють переважно в межах КЗ.

По – друге, конкуруючи організації в комерційній сфері завжди зацікавлені у володінні даними про контрагентів, підрядників і стратегії розвитку фірми для розуміння стратегії та принципів роботи підприємства. Звідси робимо висновки, що серед зовнішніх порушників слід виділити конкурентів, які в свою чергу можуть залучити хакерів.

Таким чином, потенційними порушниками можуть бути:

- Керівник логістичного відділу
- Системний адміністратор
- Конкуренти
- Хакери

Тому організація роботи цих працівників має бути найбільш контрольованою.

2.2 Аналіз можливих загроз

Загрози безпеки інформаційних систем класифікуються за декількома ознаками (рис 2.1)

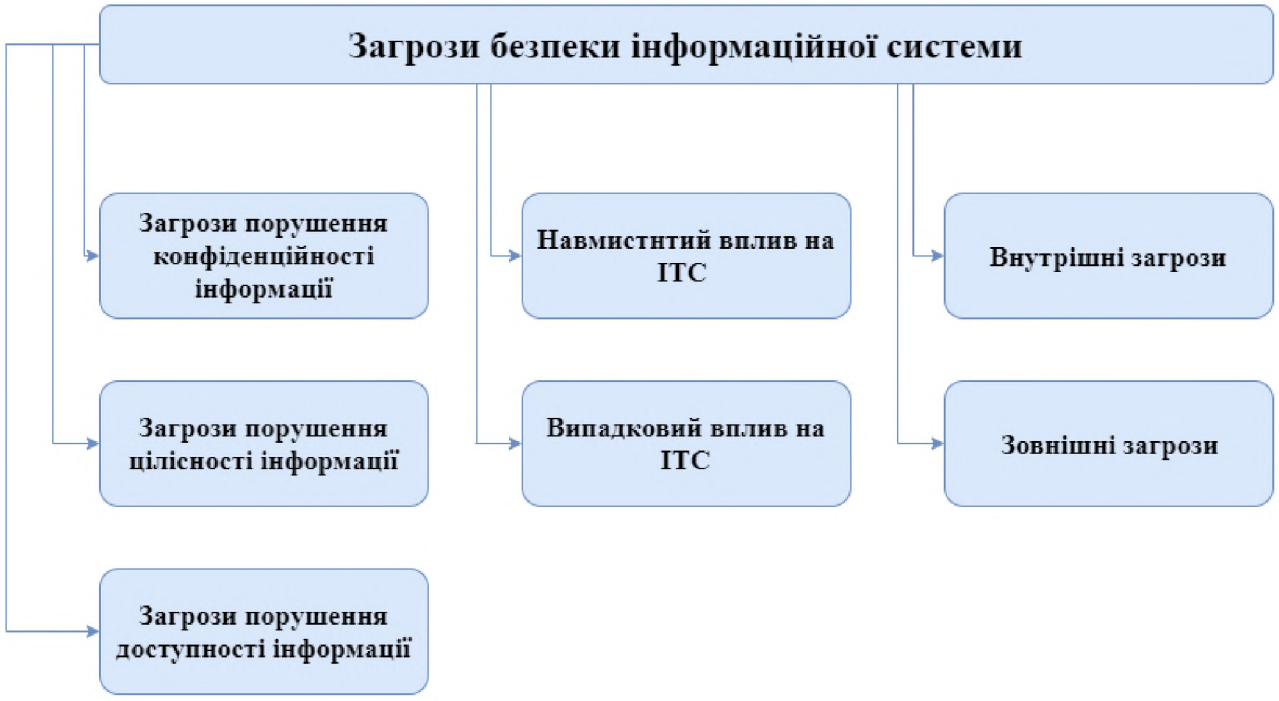


Рисунок 2.1 – Класифікація загроз безпеки інформаційних систем

Загрози порушення конфіденційності (К) спрямовані на отримання (розкрадання) конфіденційної інформації. У разі реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступу. Несанкціонований доступ до інформації, що зберігається в інформаційній системі або передається по каналах (мережах) передачі даних, копіювання цієї інформації є порушенням конфіденційності інформації.

Загрози порушення цілісності (Ц) інформації, що зберігається в інформаційній системі або передається через мережу передачі даних, спрямовані на зміну або спотворення даних, що призводить до порушення якості або повного знищення інформації. Цілісність інформації може бути порушена навмисно зловмисником, а також внаслідок об'єктивних впливів із боку середовища, що оточує систему (перешкоди). Ця загроза є особливо актуальною для систем передачі інформації – комп'ютерних мереж та систем телекомунікацій. Умисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яку виконують авторизовані користувачі з обґрунтованою метою.

Загрози порушення доступності (Д) системи спрямовані створення таких ситуацій, коли певні дії або знижують працездатність інформаційної системи, або блокують доступом до деяких її ресурсів.

Причини випадкових впливів на ІТС:

- аварійні ситуації через стихійні лиха та відключення електроенергії;
- - помилки у програмному забезпеченні;
- помилки у роботі обслуговуючого персоналу та користувачів;
- перешкоди у лінії зв'язку через вплив довкілля, або внаслідок великого навантаження на систему (велика кількість запитів за якийсь проміжок часу).

Навмисні впливи пов'язані з цілеспрямованими діями зловмисника, якою може виступити будь-яка зацікавлена особа (конкурент, відвідувач, персонал тощо). Події зловмисника можуть бути зумовлені різними мотивами: невдоволенням співробітника своєю кар'єрою, матеріальним інтересом, цікавістю, конкуренцією, прагненням самоствердитись за всяку ціну тощо. Поділяються на антропогенні та техногенні.

Внутрішні загрози ініціюються персоналом об'єкта, на якому встановлено систему, що містить конфіденційну інформацію. Причинами виникнення таких загроз може послужити нездоровий клімат у колективі або незадоволеність

виконуваної роботи деяких співробітників, які можуть розпочати дії з видачі інформації особам, зацікавленим у її отриманні.

Також має місце так званий "людський фактор", коли людина не навмисне, помилково, робить дії, що призводять до розголошення конфіденційної інформації або до порушення доступності інформаційної системи. Велику частку конфіденційної інформації зловмисник (конкурент) може отримати за недотримання працівниками-користувачами комп'ютерних мереж елементарних правил захисту інформації. Це може виявитися, наприклад, в примітивності паролів або в тому, що складний пароль користувач зберігає на паперовому носії на видному місці або записує в текстовий файл на жорсткому диску та ін. Витік конфіденційної інформації може відбуватися при використанні незахищених каналів зв'язку, наприклад, телефонного з'єднання.

Під зовнішніми загрозами безпеці розуміються загрози, створені сторонніми особами та які виходять із зовнішнього середовища, такі як:

- атаки із зовнішньої мережі (Інтернет), спрямовані на спотворення, знищення, розкрадання інформації або, що призводять до відмови в обслуговуванні інформаційних систем підприємства;
- розповсюдження шкідливого програмного забезпечення;
- перехоплення інформації з використанням радіоприймальних пристроїв;
- небажані розсилки (спам);

Враховуючи класифікацію загроз безпеки ІТС була побудована модель загроз підприємства “Рейтранс”, яка наведена в таблиці 2.9

Таблиця 2.9 – Модель загроз ІТС.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
1. Навмисні загрози (антропогенні та техногенні)								
1.1	Несанкціонований доступ до ІзОД сторонніх людей внаслідок фізичного проникнення на об'єкт	Зовнішнє	- Відсутність пильності охоронної служби - Малоефективна система охорони	Низька	К	2	3	5
					Ц	3	4	7
					Д	2	3	5
1.2	Порушення конфіденційності або цілісності інформації внаслідок навмисних дії авторизованого користувача	Внутрішнє	- Відсутність резервних копії інформації в паперовому чи електронному вигляді - Людський фактор(помилка при підборі персоналу)	Середня	К	2	4	6
					Ц	2	4	6
1.3	Навмисне відключення системи від мережі електропостачання	Внутрішнє	- Малоефективна система охорони - Недостатній контроль за приміщенням	Низька	К	1	2	3
					Ц	2	4	6
					Д	2	4	6

Продовження таблиці 2.9 - Модель загроз ІТС.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
1.4	Занесення до системи комп'ютерних вірусів/шкідливих програм	Зовнішнє Внутрішнє	- Відсутність якісного антивірусного ПЗ	Висока	К	4	4	8
					Ц	4	4	8
					Д	4	4	8
1.5	Використання зовнішніх, механічних носіїв інформації	Внутрішнє	- Недостатній контроль за системою	Середня	К	4	4	8
					Ц	4	4	8
					Д	4	4	8
1.6	Відправка файлів які місять інформацію стороннім особам	Внутрішнє	- Недостатній контроль за співробітниками	Висока	К	3	3	6
					Ц	1	3	4
					Д	1	3	4
1.7	Перехоплення даних по технічним каналам витоку інформації	Зовнішнє	- Старе приміщення - Відсутність контролю за мережами функціювання будівлі	Середня	К	2	4	6
					Ц	3	3	6
					Д	3	4	7

Продовження таблиці 2.9 - Модель загроз ІТС.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
1.8	Підслуховування	Внутрішнє	- Людський фактор	Низька	К	3	3	6
					Ц	1	1	2
					Д	1	1	2
1.9	Одержання повноважень інших користувачів(дирек-тора, системного адміністратора)	Внутрішнє	- Неефективна система аунтифікації - Необізнаність персоналу	Середня	К	3	3	6
					Ц	2	3	5
					Д	2	3	5
1.10	Перевищення службових обов’язків	Внутрішнє	- Людський фактор	Висока	К	4	4	8
					Ц	3	3	7
					Д	3	3	7
2. Випадкові загрози								
2.1	Розголошення інформації	Зовнішнє	- Людський фактор	Середня	К	3	1	4
					Ц	1	1	2
					Д	1	1	2
2.2	Порушення інформації через ненавмисні дій користувачів	Внутрішнє	- Відсутність резервних копії інформації в паперовому чи електронному вигляді	Середня	Ц	2	2	4
					Д	2	2	4

Продовження таблиці 2.9 - Модель загроз ІТС.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
2.3	Підслуховування	Внутрішнє	- Людський фактор	Середня	К	4	3	7
					Ц	1	1	2
					Д	1	1	2
2.4	Відкриття фішингових листів користуючись корпоративною почтою	Зовнішнє	- Необізнаність персоналу - Відсутність якісного антивірусного ПЗ	Середня	К	2	4	6
					Ц	2	4	6
					Д	2	4	6
2.5	Помилки персоналу	Внутрішнє	- Необізнаність персоналу	Середня	К	1	1	2
					Ц	2	2	4
					Д	2	2	4
2.6	Збої в роботі технічних засобів	Внутрішнє	- Впровадження нового ПЗ	Низька	К	1	2	3
					Ц	2	3	5
					Д	2	3	5
2.7	Використання застарілого ПЗ	Внутрішнє	- Застаріла операційна система	Низька	К	2	3	5
					Ц	1	1	2
					Д	2	3	5
2.8	Випадкове одержання повноважень інших користувачів(дирек-тора, системного адміністратора)	Внутрішнє	- Необізнаність персоналу	Низька	К	2	3	5
					Ц	2	3	5
					Д	2	3	5

Продовження таблиці 2.9 - Модель загроз ІТС.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
3. Стихійні (впливи природних факторів)								
3.1	Пожежа	Зовнішнє	- Наявність легкозаймистих матеріалів - Несвоєчасна перевірка обладнання приміщення	Середня	Ц	2	5	7
					Д	2	5	7
3.2	Затоплення	Зовнішнє	- Старе приміщення	Низька	Ц	2	5	7
					Д	2	5	7
3.3	Землетрус	Зовнішнє	- Старе приміщення	Низька	Ц	2	5	7
					Д	2	5	7
3.4	Віялові відключення електроенергії	Зовнішнє	- Несвоєчасна перевірка обладнання приміщення - Відсутність автономних пристроїв живлення	Висока	Ц	3	5	8
					Д	3	5	8

Рівні ризиків та збитків:

- Низький. Оцінюється в 1 бал. Призводить до незначних збитків ;
- Середній. Оцінюється в 3 бали. Призводить до збитків середніх розмірів;
- Високий. Оцінюється в 5 балів. Призводить до значних збитків.

Найбільш актуальними загрозами для підприємства ТОВ “Рейтранс” є:

- Віялові відключення електроенергії.
- Відкриття фішингових листів;
- Перехоплення даних по технічним каналам витоку інформації;
- Використання зовнішніх, механічних носіїв інформації;
- Перевищення службових обов’язків;
- Занесення до системи комп’ютерних вірусів/шкідливих програм.

В подальшому для розробки заходів безпеки, до урахування будемо брати наведені вище загрози.

2.3 Профіль захищеності

Згідно до НД ТЗІ 2.5-005 -99 [6] – “ Опис профілю складається з трьох частин: буквеночислового ідентифікатора, знака рівності і переліку рівнів послуг, взятого в фігурні дужки. Ідентифікатор у свою чергу включає: позначення класу АС (1, 2 або 3), буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д), номер профілю і необов’язкове буквене позначення версії. Всі частини ідентифікатора відділяються один від одного крапкою.”

АС – організаційно – технічна система, що включає в собі персонал, оброблювальну інформацію, ОС та фізичне середовище. Беручи до уваги характеристики існуючої ІТС та згідно вимог та властивостей інформації, відповідно до НД ТЗІ 2.5-005 -99 для даної ОС вибрано наступний профіль захищеності, призначений для АС 3 класу з підвищеними вимогами до конфіденційності, цілісності, доступності оброблювальної 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}

Опис вимог до профілю захищеності ІТС наведено у таблиці 2.10

Таблиця 2.10 – Вимоги до профілю захищеності ІТС.

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
	Повторне використання об’єктів	КО-1 (повторне використання об’єктів)
	Конфіденційність при обмінні	КВ-1 (базова конфіденційність при обмінні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обмінні	ЦВ-1 (мінімальна цілісність при обмінні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Достовірний канал	НК-1 (одно направлений достовірний канал)
	Розподіл обов’язків	НО-2 (поділ обов’язків між адміністратором і користувачами)
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування з запитом	НТ-2 (Самотестування при старті)
	Автентифікація вузла	НВ-1 (автентифікація вузла)

Опис кожного критерія обраного профіля:

КД-2. Базова довірча конфіденційність:

- 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.

КО-1. Повторне використання об'єктів:

- 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 доданого 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.

КВ-1. Мінімальна конфіденційність при обміні:

- політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейс них 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.

ЦД-1.Мінімальна довірча цілісність:

- політика довірчої цілісності, 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 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.

ЦО-1. Обмежений відкат:

- 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.

ЦВ-1. Мінімальна цілісність при обміні:

- політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейс них 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.

ДР-1. Квоти:

- 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.

ДВ-1. Ручне відновлення:

- 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.

НР-2. Захищений журнал:

- 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.

НИ-2. Одиночна ідентифікація і автентифікація:

- 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 автентифікувати цього користувача з використанням захищеного механізму;
- КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Одно направлений достовірний канал:

- 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.

НО-2. Розподіл обов'язків адміністраторів:

- 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 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.

НЦ-2. КЗЗ з гарантованою цілісністю:

- 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.

НТ-2.Самотестування при старті:

- 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.

НВ-1. Автентифікація вузла:

- 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.

2.4 Визначення методів та засобів захисту

Створення КЗСІ включає в себе заходи, що направлені на аналіз можливих ризиків та їх зниження, а також на зниження реалізації загроз через вразливості в інформаційно – телекомунікаційній системі. Проаналізувавши моделі порушника та моделі загроз виявлено загрози, що мають високий рівень реалізації на підприємстві “Рейтранс”. До переліку таких загроз належать збої електроживлення, перевищення службових обов’язків, відкриття фішингових листів, перехоплення даних по технічним каналам витоку інформації, використання зовнішніх, механічних носіїв інформації, занесення до системи

комп'ютерних вірусів/шкідливих програм. Зниження ризиків цих загроз є першочерговим.

Збої електроживлення можливі через віялові відключення та перепади напруги. На ОІД немає безперебійного джерела живлення, але в той же час є 15 комп'ютерів, 5 принтерів та 1 факс, через які може статися падіння напруги. Серверна частина системи також є вразливою до перепадів напруги так як підключена напряму до мережі та в якому невідмінно від комп'ютерів в блоку живлення не передбачено захисту від перепадів напруги. Результати роботи персоналу зберігаються на сервері та в хмарному сховищі наприкінці робочого дня, отже при виведені із строю одного з ПК або серверу на початку або в середині робочої доби, документи можуть бути втрачені. Таким чином потрібно ввести для даної системи джерело безперебійного живлення - Challenger HomeLine 1500T12 і під'єднати до нього сервер, а також - ввести в ПЗ в якому відбувається редакція/створення файлів функцію автоматичного зберігання з частотою в 30 хв. Також ввести правило постійного мануального збереження даних для персоналу.

Зазвичай для фішингу використовуються електронні листи або реклама, а також підроблені сайти, що імітують ресурси, вже знайомі відвідувачам. Наприклад, шахраї можуть надіслати вам листа, що імітує лист з вашого банку з проханням підтвердити номер вашого рахунку. В нашому випадку відкриття листів або посилань може призвести до втрати великих об'ємів важливої для підприємства інформації. Фішинг є доволі простим засобом незаконного заволодіння інформацію, але з часом люди стають все більш грамотні та рідко потрапляють на підозрілі ресурси. Найпростішим методом виключення даної загрози буде проведення курсів базової комп'ютерної грамотності для тих співробітників які відчувають невпевненість при використанні комп'ютера.

Через відсутність контролю за діями системного адміністратора, який фактично є адміністратором мережі, та адміністратором безпеки можливі несанкціовані дії з його боку. Тому є доцільним, з метою забезпечення контролю його дії розділити ролі адміністраторів мережі, безпеки з мінімізацією функції

так, щоб включати тільки ті функції, які необхідні для виконання обов'язків на даній посаді, та передати роль адміністратора безпеки довіреному персоналу (директору, або керівнику відділу маркетингу, обидва володіють потрібним рівнем знань та навичок для виконання даної ролі). Наказ на суміщення відповідальності надан в ДОДАТКУ В .

Через відсутність чіткого контролю за встановленням ПЗ працівниками,можливе використання ПЗ в власних цілях або занесення вірусу до комп'ютерної системи. Для того щоб зменшити ризик потрібно ввести постійні перевірки знань, та тести для підвищення кваліфікації, які будуть стосуватися всього персоналу, включаючи керівництво. Також ввести правило «DownloadForbid», щоб заборонити користувачам завантажувати підозрілі файли, такі як шкідливі програми та заражені файли. При цьому можна заборонити завантажувати всі файли або тільки ті, які Google (безпечний перегляд) визначає як небезпечні. При спробі завантажити такий файл користувачеві буде показано попередження, яке неможна буде обійти; ввести «білий список» сайтів в Інтернеті, які будуть відкритими для персоналу, інші – заборонити. На підприємстві встановлено антивірус Norton (версія 22.2.10), для визначення доцільності використання саме цієї програми були проведені тести існуючого та пропонованих антивірусних програм. Порівняльний аналіз наведено в таблиці 2.11

Таблиця 2.11 – Порівняльний аналіз антивірусних програм.

	Антивірус		
Характеристика	Avast Antivirus 21.6.2474 (Paid)	McAfee (Paid)	Norton 22.2.10 (Paid)
швидкість реакції на загрозу	5	5	4
робота поведінкового блокатора	4	4	4
можливість лікування активних заражень	5	4	4
обсяг хибних спрацьовувань	5	3	4
наявність підтримки архіваторів	5	4	5
виявлення активності руткітів	5	3	4
блокування підозрілих ресурсів	5	5	5
блокування реклами в браузерах	5	3	5
Сума	39	31	35

Критерій оцінювання:

- 1 – Немає в наявності
- 2 – Є в наявності, але не відповідає вимогам
- 3 – Задовольняє вимогам (низький рівень)
- 4 – Задовольняє вимогам (середній рівень)
- 5 – Задовольняє вимогам (високий рівень)

Після проведених тестів можна відзначити, що найкраще із завданням впоралася платна версія браузерного антивірусу Avast Antivirus 21.6.2474.

Програма McAfee та встановлений Norton показали себе досить непогано і між собою за показниками сильно не відрізняються, у McAfee було більше помилкових спрацьовувань, а Norton у свою чергу міг виявити загрозу з невеликим запізненням. Щодо цих двох програм – платна версія Avast Antivirus виглядає у рази краще. Таким краще встановити Avast Antivirus 21.6.2474 виробництва компанії AVAST Software s.r.o. (Чеська республіка). Ця програма відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний комплекс антивірусного захисту «Avast Business Antivirus» версії 21», «Технічні вимоги щодо захисту інформації від несанкціонованого доступу».

Через відсутність обліку та контролю зовнішніх/механічних носіїв інформації, було прийнято рішення о впровадженні Політики використання/механічних носіїв інформації на підприємстві:

- забороняється підключати до робочого комп'ютера будь-які носії інформації (USB, Flash, CD, телефони/смартфони) без дозволу директора;
- усі накопичувачі інформації повинні бути записані в перелік інвентаризаційної відомості;
- заборонено передавати носії інформації іншим користувачам ІТС для будь – яких цілей;
- інформація на зареєстрованих флеш накопичувачах та ЖМД повинна зберігатися в зашифрованому вигляді;
- повинні зберігатися в зачиненому сейфі;
- відповідальність за зберігання флеш накопичувачів та ЖМД цілком покладається на директора.

При обстеженні офісного приміщення та побудові генерального плану були визначено декілька технічних каналів витоку інформації за якими порушник може отримати інформацію. Можливі ТКВІ та засоби їх реалізації наведені в таблиці 2.12

Таблиця 2.12 Реалізація ТКВІ на ОІД

№	Технічний канал витоку інформації	Процес перехоплення	Реалізація ТКВІ на ОІД
1	Візуально - оптичний	Підглянути інформацію на комп'ютері	Для реалізації є багато варіантів, бо вікна в офісі розташовані в усіх кімнатах. ОІД розташовано в значний близькості до інших будівель(25м макс.) та підглянути інформацію на екрані буде досить легко.
2	Повітряно - акустичний	Підслухати розмову	Підслухати розмову можливо через стіни кімнат,систему вентиляції, або за допомогою ненаправленого мікрофону.
3	Оптико-Електронний	Підслухати розмову за допомогою опромінення лазерним променем вібруючих в акустичному просторі поверхонь (найчастіше вікна)	Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється по амплітуді і фазі (згідно із законом вібрації поверхні) і приймається приймачем оптичного (лазерного) випромінювання, при демодуляції якого виділяється мовна інформація.

Таким чином можна визначити же найуразливішими містами ОІД є вікна, стіни і система вентиляції. Ролети встановлені на всіх вікнах, але частіше за все у часи функціонування підприємства є відкритими. Отже можна легко підглянути інформацію з прилеглих споруд враховуючи маленьку відстань до ОІД. Потрібно ввести правило яке забезпечую закриття ролетів в робочий час на вікнах. Це унеможливить перегляданння інформації на моніторах з сусідніх будівель, або зчитування вібрації з поверхні.

Для захисту акустичної (мовної) інформації використовуються пасивні та активні методи та засоби. Пасивні методи захисту акустичної (мовної) інформації спрямовані на:

- ослаблення акустичних (мовних) сигналів на межі контрольованої зони до величин, що забезпечують неможливість їх виділення засобом розвідки на тлі природних шумів;
- послаблення інформаційних електричних сигналів у сполучних лініях ДТЗС, що мають у своєму складі електроакустичні перетворювачі, що володіють мікрофонним ефектом, до величин, що забезпечують неможливість їх виділення засобом розвідки на тлі природних шумів;
- виключення (ослаблення) проходження сигналів високочастотного нав'язування у допоміжні технічні засоби, що мають у своєму складі електроакустичні перетворювачі, що володіють мікрофонним ефектом;
- виявлення випромінювань акустичних закладок і побічних електромагнітних випромінювань диктофонів в режимі запису;
- виявлення несанкціонованих підключень к телефонним лініям зв'язку.

Активні методи захисту акустичної інформації спрямовані на:

- створення маскуючих акустичних та вібраційних перешкод;
- електромагнітне виключення диктофонів в режимі запису;
- ультразвукове виключення диктофонів у режимі запису;
- створення маскуючих електромагнітних перешкод в лініях електроживлення ДТЗС

Звукоізоляція приміщень спрямована на локалізацію джерел акустичних сигналів і проводиться з метою виключення перехоплення акустичної інформації по прямому акустичному (через щілини, вікна, двері, технологічні отвори, вентиляційні канали і т.д.) і вібраційному (водо-, тепло- та газопостачання, каналізації і т.д.) каналам.

Для підвищення звукоізоляції в приміщеннях застосовують акустичні екрани, що встановлюються на шляху поширення звуку на найбільш небезпечних (з точки зору розвідки) напрямках. Дія акустичних екранів засноване на відображенні звукових хвиль і освіті за екраном звукових тіней. Розміри ефективних екранів перевищують більш ніж у 2-3 рази довжину хвилі.

Для зменшення ризиків витоку мовної інформації на підприємстві було прийнято рішення провести звукоізоляцію окремих стін в кімнатах директора та бухгалтерії. Придбання детектору випромінювання (1~1999 В/м, 0,01~99,99 μt) Benetech GM3120 та періодичні огляди офісу, вентиляції на наявність пасивних мікрофонів також зменшать ризик розкриття інформації стороннім особам.

2.5 Аналіз ризиків після впровадження програмно – технічних та організаційних рішень

Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-технічних та організаційних рішень надано в таблиці 2.13.

Таблиця 2.13 - Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
1. Навмисні загрози (антропогенні та техногенні)								
1.1	Несанкціонований доступ до ІзОД сторонніх людей внаслідок фізичного проникнення на об'єкт	Зовнішнє	- Відсутність пильності охоронної служби - Малоефективна система охорони	Низька	К	2	3	5
					Ц	3	2	5
					Д	2	3	5
1.2	Порушення конфіденційності або цілісності інформації внаслідок навмисних дії авторизованого користувача	Внутрішнє	- Відсутність резервних копії інформації в паперовому чи електронному вигляді - Людський фактор(помилка при підборі персоналу)	Низька	К	2	2	4
					Ц	2	2	4
1.3	Навмисне відключення системи від мережі електропостачання	Внутрішнє	- Малоефективна система охорони - Недостатній контроль за приміщенням	Низька	К	1	2	3
					Ц	2	1	3
					Д	2	1	3

Продовження таблиці 2.13 - Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
1.4	Занесення до системи комп'ютерних вірусів/шкідливих програм	Зовнішнє Внутрішнє	- Відсутність якісного антивірусного ПЗ	Низька	К	2	2	4
					Ц	2	2	4
					Д	2	2	4
1.5	Використання зовнішніх, механічних носіїв інформації	Внутрішнє	- Недостатній контроль за системою	Низька	К	1	1	2
					Ц	1	1	2
					Д	1	1	2
1.6	Відправка файлів які місять інформацію стороннім особам	Внутрішнє	- Недостатній контроль за співробітниками	Низька	К	1	2	3
					Ц	1	3	4
					Д	1	3	4
1.7	Перехоплення даних по технічним каналам витоку інформації	Зовнішнє	- Старе приміщення - Відсутність контролю за мережами функціювання будівлі	Середня	К	1	2	3
					Ц	1	2	3
					Д	1	2	3

Продовження таблиці 2.13 - Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
1.8	Підслуховування	Внутрішнє	- Людський фактор	Низька	К	1	1	2
					Ц	1	1	2
					Д	1	1	2
1.9	Одержання повноважень інших користувачів(дирек-тора, системного адміністратора)	Внутрішнє	- Неефективна система аунтифікації - Необізнаність персоналу	Середня	К	2	2	3
					Ц	1	2	3
					Д	1	2	3
1.10	Перевищення службових обов’язків	Внутрішнє	- Людський фактор	Середня	К	2	1	3
					Ц	2	1	3
					Д	2	1	3
2. Випадкові загрози								
2.1	Розголошення інформації	Зовнішнє	- Людський фактор	Середня	К	3	1	4
					Ц	1	1	2
					Д	1	1	2
2.2	Порушення інформації через ненавмисні дій користувачів	Внутрішнє	- Відсутність резервних копії інформації в паперовому чи електронному вигляді	Низька	Ц	1	2	3
					Д	1	2	3

Продовження таблиці 2.13 - Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
2.3	Підслуховування	Внутрішнє	- Людський фактор	Низька	К	1	1	2
					Ц	1	1	2
					Д	1	1	2
2.4	Відкриття фішингових листів користуючись корпоративною почтою	Зовнішнє	- Необізнаність персоналу - Відсутність якісного антивірусного ПЗ	Низька	К	1	1	2
					Ц	1	1	2
					Д	1	1	2
2.5	Помилки персоналу	Внутрішнє	- Необізнаність персоналу	Низька	К	1	1	2
					Ц	1	1	2
					Д	1	1	2
2.6	Збої в роботі технічних засобів	Внутрішнє	- Впровадження нового ПЗ	Низька	К	1	2	3
					Ц	2	3	5
					Д	2	3	5
2.7	Використання застарілого ПЗ	Внутрішнє	- Застаріла операційна система	Низька	К	2	3	5
					Ц	1	1	2
					Д	2	3	5
2.8	Випадкове одержання повноважень інших користувачів(дирек-тора, системного адміністратора)	Внутрішнє	- Необізнаність персоналу	Низька	К	1	1	2
					Ц	1	1	2
					Д	1	1	2

Продовження таблиці 2.13 - Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень.

№	Загрози	Джерело загрози	Вразливість	Ймовір-ність	Порушення	Рівень		Сума загроз
						Ризиків	Збитків	
3. Стихійні (впливи природних факторів)								
3.1	Пожежа	Зовнішнє	- Наявність легкозаймистих матеріалів - Несвоєчасна перевірка обладнання приміщення	Середня	Ц	2	5	7
					Д	2	5	7
3.2	Затоплення	Зовнішнє	- Старе приміщення	Низька	Ц	2	5	7
					Д	2	5	7
3.3	Землетрус	Зовнішнє	- Старе приміщення	Низька	Ц	2	5	7
					Д	2	5	7
3.4	Віялові відключення електроенергії	Зовнішнє	- Несвоєчасна перевірка обладнання приміщення - Відсутність автономних пристроїв живлення	Висока	Ц	1	2	3
					Д	1	2	3

Рівні ризиків та збитків:

- Низький. Оцінюється в 1 бал. Призводить до незначних збитків ;
- Середній. Оцінюється в 3 бали. Призводить до збитків середніх розмірів;
- Високий. Оцінюється в 5 балів. Призводить до значних збитків.

Порівнюючи з таблицею 2.9 - Модель загроз ІТС, можемо зробити висновок, що зменшилась ймовірність та рівень ризиків/загроз майже у всіх можливих пунктах. Особливо знизилась вірогідність реалізації загроз на які були направлені програмно – організаційні рішення, наприклад:

- Віялові відключення електроенергії (Ризики(було –Ц3,Д5 зараз – Ц1,Д2) (Збитки(було –Ц5,Д5 зараз – Ц2,Д2)
- Відкриття фішингових листів (К2,Ц2,Д2 – К1,Ц1,Д1) (К4,Ц4,Д4 – К1,Ц1,Д1)
- Перехоплення даних по технічним каналам витоку інформації (К2,Ц3,Д3 – К1,Ц1,Д1) (К4,Ц3,Д4 – К2,Ц2,Д2)
- Використання зовнішніх, механічних носіїв інформації (К4,Ц4,Д4 – К1,Ц1,Д1) (К4,Ц4,Д4 – К1,Ц1,Д1)
- Перевищення службових обов'язків (К4,Ц3,Д3 – К2,Ц2,Д2) (К4,Ц3,Д3 – К1,Ц1,Д1)
- Занесення до системи комп'ютерних вірусів/шкідливих програм (К4,Ц4,Д4 – К2,Ц2,Д2) (К4,Ц4,Д4 – К2,Ц2,Д2).

2.6 Висновки до другої частини

Ігнорування загроз та вразливостей ІТС може призвести до значних фінансових втрат та витоку інформації ТОВ "Рейтранс". В ході виконання другого розділу розроблено модель порушника та модель загроз. Також обрано стандартний профіль захищеності, який використовується на підприємстві. Виявлено найбільш актуальні загрози, запропоновані організаційні та програмні рішення для їх мінімізації для підприємства «Рейтранс»: запропоновано джерело безперебійного живлення та детектор поля, правило «DownloadForbid», та правило «білого списку», змінено програму антивірусного захисту, введено правило, яке забезпечує закриття в денний час ролетів на вікнах.

Проведено аналіз та порівняння загроз до та після реалізації запропонованих рішень, а саме їх ймовірності та збитків, після впровадження проектних рішень.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою обґрунтування витрат на розробку комплексної системи захисту інформації ТОВ “Рейтранс” є розрахунок капітальних та експлуатаційних витрат, оцінка величини можливого збитку від атаки, визначення та аналіз показників економічної ефективності.

3.1 Розрахунок капітальних (фіксованих) витрат

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

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

$$t= t_{тз}+t_{в}+t_{а}+t_{вз}+t_{озб}+t_{овр}+t_{д}, \text{ год.}, \quad (3.1.1.1)$$

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

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

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

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

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

$t_{овр}$ - тривалість організації виконання відновлюваних робіт і забезпечення неперервного функціонування організації;

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

Згідно формули 3.1.1.1, трудомісткість розробки політики безпеки інформації дорівнює:

$$t= 10+12+15+9+16+17+8=87 \text{ год.}$$

3.1.2 Розрахунок витрат на створення політики безпеки інформації

Розрахунок витрат на створення політики безпеки:

$$К_{рп}=З_{зп}+З_{мч} \quad (3.1.2.1)$$

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

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

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення політики безпеки.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою:

$$З_{зп}= t * З_{іб} \text{ грн.}, \quad (3.1.2.2)$$

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

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

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 150 грн/ годину.

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби та визначається за формулою 3.1.2.2 :

$$З_{зп} = 87 * 150 = 13050 \text{ грн.}$$

$$З_{мч}= t*С_{мч} \text{ грн.}, \quad (3.1.2.3)$$

де t – трудомісткість розробки політики на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн,} \quad (3.1.2.4)$$

Де Р – встановлена потужність ПЕС, кВт;

$t_{нал}$ – кількість задіяних робочих станцій при написані політики;

$С_е$- тариф на електроенергію, грн./кВт*година;

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

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

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

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

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$=1920).

$$С_{мч}=0,7*2*1,51+((6879*0,3)/1920)+((1958*0,1)/1920)=3,29 \text{грн.}$$

$$З_{мч}= 87*3,29 = 286,23 \text{ грн.}$$

$К_{рп}$= 13050 + 286,23 = 13336,23 грн.

Капітальні (фіксовані) витрати на створення політики безпеки інформації:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н} \quad (3.1.2.5)$$

де: $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення консультантів. Зовнішні консультанти не наймались, тому даний коефіцієнт не враховуємо

$К_{зпз}$ – вартість закупівель ліцензійного і основного і додаткового ПЗ. (Було обрано комплект Windows 10, ERP, CRM, Avast 21.6.2474 – 16 шт. (16*2000=32000 грн);

$К_{рп}$ – вартість розробки політики безпеки інформації – 13336,23 грн;

$К_{аз}$ - вартість закупівлі апаратного забезпечення та допоміжних матеріалів (Було обрано: «джерело безперебійного живлення - Challenger HomeLine 1500T12» - 3457 грн), «Детектору випромінювання (1~1999 В/м, 0,01~99,99 μt) Benetech GM3120» - 915 грн), «Панель з акустичного поролону Ecosound Tetras Black 50X50CM, 70MM, колір чорний» - 30шт (30*121 =3630 грн));

$К_{н}$ - витрати на встановлення обладнання та налагодження системи інформаційної безпеки – 1500 грн;

$К_{навч}$ – витрати на навчання технічних фахівців в обслуговуючого персоналу, 2500 грн;

К = 32000+13336,23+8002+1500+2500=57338,23 грн.

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – поточні витрати на обслуговування об’єкта проектування за визначений період.

Річні поточні витрати на функціонування системи інформаційної безпеки:

$$С=С_{в} +С_{к}+С_{ак}, \text{ грн.} \quad (3.2.1)$$

де: $С_{в}$ - це витрати на оновлення системи;

$С_{в}$ = 1340 грн.

$С_{ак}$ - витрати викликані активністю користувачів системи ІБ.

$С_{ак}$ = 2220 грн.

$С_{к}$ - вартість на керування системою в цілому, рахується за формулою:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос} \quad (3.2.2)$$

де: $С_н$ – це витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації.

$С_н$=2500грн.

Річний фонд амортизаційних відрахувань становить:

$$С_а = С_{а1} + С_{а2}, \text{ грн} \quad (3.2.3)$$

де: $С_{а1}$ - це річний фонд амортизаційних відрахувань ПЗ

$С_{а2}$ - це річний фонд амортизаційних відрахувань АЗ (апаратного забезпечення)

$$С_{а1/2} = \frac{Ф_п}{Т}, \text{ грн} \quad (3.2.4)$$

де: $Ф_п$ – первісна вартість придбаного ПЗ/АЗ

Т – мінімальний срок корисного використання (2 роки для ПЗ, 5 - АЗ)

$$С_{а1} = 32000/2 = 16000 \text{ грн};$$

$$С_{а2} = 8002/5 = 1600{,}40 \text{ грн};$$

$$С_а = 16000 + 1600{,}40 = 17600{,}40 \text{ грн.}$$

$С_з$- це річний фонд заробітної плати інженерно-технічного персоналу, котрий обслуговує систему ІБ, вираховується за формулою:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.2.5)$$

Де основна заробітна плата ($З_{осн}$) визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата ($З_{дод}$) в розмірі 8-10% від основної заробітної плати. Основна заробітна плата спеціаліста з інформаційної безпеки 15318грн./місяць.

Виконання робіт вимагає залучення спеціаліста з інформаційної безпеки на 0,25 ставки.

$$С_з = (15318*12 + 15318*12*0{,}1)*0{,}25 = 50549{,}40 \text{ грн.}$$

В 2022 році ЄСВ є 22% від фонду заробітної плати і становить:

$$С_{єв} = 50549{,}40*0{,}22 = 11120{,}87 \text{ грн.}$$

$С_{ел}$ - це вартість електроенергії, що споживається апаратурою системи ІБ протягом року, вираховується за формулою:

$$С_{ел} = Р * F_р * Ц_е, \text{ грн} \quad (3.2.6)$$

де: Р- встановлена потужність апаратури інформаційної безпеки.

Р = 0.7 кВт.

$F_р$- це річний фонд робочого часу системи інформаційної безпеки.

$F_р$ = 1920 год.

$Ц_е$ – це тариф на електроенергію, 1,51грн/кВт годин.

$С_{ел}$ = 0.7*1920*1,51= 2029,44 грн;

$С_{тос}$ – це витрати на технічне та організаційне адміністрування та сервіс системи ІБ визначаються за даними організації. Або 1% від суми капітальних інвестицій – $С_{тос}$ = 573,38 грн.

$С_о$ – це витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговування персоналу.

$С_о$ = 0 грн.

$С_к$ = 2500+17600,40+50549,40+ 2029,44+11120,87+573,38= 84373,49 грн.

Отже, річні поточні витрати на функціонування системи інформаційної безпеки становлять:

С = 84373,49+1340+2220 =87933.49 грн.

3.3 Оцінка можливого збитку від атаки

3.3.1 Оцінка величини збитку

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

$$U = П_п + П_в + V, \text{ грн.} \quad (3.3.1.1)$$

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:

$$П_п = \frac{\sum З_с}{F} * t_п = \frac{591310}{170} * 4 = 13913{,}18 \text{ грн.} \quad (3.3.1.2)$$

де: $\sum З_с$ = заробітна платня співробітників, грн/міс;

F – місячний фонд робочого часу, год.;

$t_п$ – час простою.

В таблиці 3.1 наведені виплати на заробітну платню співробітників з урахуванням ЄСВ.

Таблиця 3.1 – Виплати на заробітну платню співробітників.

Посада	Кількість співробітників	Місячна заробітна платня, грн. 1 особа	ЄСВ, грн.	Витрати на заробітну платню з урахуванням ЄСВ, грн.
Директор	1	30000	6600	36600
Керівник логістичного відділу	1	24000	5280	29280
Керівник відділу маркетингу	1	24000	5280	29280
Спеціаліст з маркетингу	2	14000	3080	17080
Експедитор	3	15000	3300	18330
Диспетчер	3	12000	3960	15960
Водій	9	20000	4400	24400
Митний брокер	2	14000	3080	17080

Продовження таблиці 3.1 - Виплати на заробітну платню співробітників.

Посада	Кількість співробітників	Місячна заробітна платня, грн. 1 особа	ЄСВ, грн.	Витрати на заробітну платню з урахуванням ЄСВ, грн.
Головний бухгалтер	1	24000	5280	27280
Бухгалтер	1	18000	3960	21960
Системний адміністратор	1	25000	5500	30500
Програміст 1С	1	21000	4620	25620
Всього				591310

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

$$П_в = П_{ви} + П_{пв} + П_{зп'}, \text{ грн.} \quad (3.3.1.3)$$

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

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

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

$П_{зп} = 0$ грн.

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

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви} = \frac{591310}{170} * 3 = 10434{,}88 \text{ грн.} \quad (3.3.1.4)$$

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

$$П_{ви} = \frac{\sum З_с}{F} * t_в = \frac{30500}{170} * 3 = 538{,}23 \text{ грн.} \quad (3.3.1.5)$$

Таким чином, витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 10434{,}88 + 538{,}23 = 10973{,}11 \text{ грн.} \quad (3.3.1.6)$$

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

$$V = \frac{О}{Fр} * (t_в + t_{ви} + t_п) = \frac{70000000}{1920} * (4+3+3) = 364583{,}33 \text{ грн.} \quad (3.3.1.7)$$

де: $F_г$ – це річний фонд часу роботи компанії, 1920 годин;

О- це обсяг продажів атакованого вузла або сегмента мережі, 70000000 грн.

Тепер ми можемо розрахувати упущену вигоду від атаки на ІТС організації:

$$U = 13913{,}18 + 10973{,}11 + 364583{,}33 = 389469{,}62 \text{ грн;}$$

Загальний збиток від атаки на сегмент корпоративної мережі організації:

$$В = \sum i * \sum n * U = 389469{,}62 * 2 * 1 = 778939{,}24 \text{ грн.} \quad (3.3.1.8)$$

3.3.2 Оцінка можливого збитку від атаки

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

$$Е = В * R - С = (778939{,}24 * 0{,}5) - 87933.49 = 301536{,}13 \text{ грн.} \quad (3.3.2.1)$$

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

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

С – щорічні витрати на експлуатацію всіх заходів, грн.

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень

додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

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

$$ROSI = \frac{E}{K} = \frac{301536,13}{57338,23} = 5,26 \quad (3.4.1)$$

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:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{57338,23}{301536,13} = 0,19 \quad (3.4.2)$$

Виходячи зі зроблених розрахунків T_0=0.19, а це приблизно становить 2 місяця.

3.5 Висновок

В економічному розділі була визначена економічна ефективність впровадження програмно – технічних та організаційних в ТОВ “Рейтранс”. Було розраховано капітальні витрати, які склали 57338,23 грн. Провели оцінювання можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі, де визначили, що загальний збиток від атаки на сегмент корпоративної мережі організації складає 778939,24 грн. Визначений термін окупності капітальних інвестицій становить 2 місяці. Таким чином можна вважати, що впровадження комплексної системи захисту інформації на підприємство є економічно доцільним рішенням, яке ефективно захистить інформаційні активи від негативних зовнішніх та внутрішніх впливів.

ВИСНОВКИ

Для будь-якої сучасної компанії інформація стає одним з головних ресурсів, збереження і правильне розпорядження яким має ключове значення для розвитку бізнесу і зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.

Під інформаційною безпекою підприємства або компанії розуміють комплекс заходів організаційного та технічного характеру, спрямованих на збереження і захист інформації та її ключових елементів, а також, яке використовуються для роботи з інформацією, її зберігання і передачі. Згідно з законодавством України, інформація з обмеженим доступом підлягає обов'язковому захисту, вимоги до якого встановлені законом.

В кваліфікаційній роботі була, проаналізована нормативно-правова база, що регулює відносини в інформаційній сфері. Проведено обстеження ТОВ "Рейтранс" та обґрунтовано створення комплексної системи захисту інформації, виконана постановка задачі.

В рамках другого розділу було розроблено модель порушника, модель загроз та проведено оцінку ризиків інформації, що можуть призвести до завдання збитків ТОВ "Рейтранс". Згідно з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових інформаційно-телекомунікаційної системи підприємства.

В економічному розділі, отримали данні щодо підтвердження економічної доцільності запропонованих проектних рішень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Створення комплексних систем захисту інформації [Електронний ресурс] Режим доступу https://tzi.com.ua/stvorennya-kompleksnix-sistem-zaxistu-nformacz.html

2. НД ТЗІ 3.7-003 -2005 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – [Чинний від 08.11.2005]- К. : ДССЗЗІ, 2005. - №125 - (Нормативний документ системи технічного захисту інформації).

3. Кіберзлочини в Україні: як бізнесу захиститися від хакерських атак [Електронний ресурс] – Режим доступу https://hub.kyivstar.ua/news/kiberzlochini-v-ukrayini-yak-biznesu-zahistitisya-vid-hakersikih-atak/.

4. Бізнес під загрозою кібератаки. Як захистити компанію? [Електронний ресурс] – Режим доступу https://biz.ligazakon.net/news/208297_bznes-pd-zagrozoyu-kberataki-yak-zakhistiti-kompanyu.

5. НД ТЗІ 1.1-002-99 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

6. НД ТЗІ 2.5-005-99 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

7. НД ТЗІ 1.4-001-2000 - Типове положення про службу захисту інформації в автоматизованій системі. [Чинний від 04.12.2000]- К. : ДСТСЗІ СБУ, 2005. - №53 - (Нормативний документ системи технічного захисту інформації).

8. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

9. НД ТЗІ 2.5-004-99 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

10. НД ТЗІ 3.7-001-99 - Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).

11. Information Security [Електронний ресурс] Режим доступу http://lib.itsec.ru/articles2/ Inf_security/infosec-torg

12. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Изд-во «ДиаСофт», 2011. – 693с.

13. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 124 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі.	33	
6	А4	Спеціальна частина	35	
7	А4	Економічний розділ	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	ДОДАТОК А	1	
11	А4	ДОДАТОК Б	1	
12	А4	ДОДАТОК В	1	
13	А4	ДОДАТОК Г	1	
14	А4	ДОДАТОК Ґ	1	

ДОДАТОК Б. Наказ на створення КСЗІ

Товариство з обмеженою відповідальністю “Рейтранс”.

НАКАЗ

«___»_____ Дніпро №_____

Про створення КСЗІ
у товаристві з обмеженою відповідальністю
“Рейтранс”.

З метою виконання вимог законів України «Про захист інформації в інформаційно – телекомунікаційних системах», «Про захист персональних даних», Положення про технічний захист інформації в Україні, затверджений від 27.09.1999 1229/99, Правил забезпечення захисту інформації в інформаційно – телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006373,

НАКАЗУЮ:

1.Провести обстеження складових інформаційно – телекомунікаційної системи Товариства з обмеженою відповідальністю “Рейтранс”. (далі-підприємство).

2.Створити комплексну систему захисту інформації підприємства.

3.Затвердити політики безпеки інформації інформаційно - телекомунікаційної Системи підприємства.

4.Відповідальність за виконання наказу покладаю на себе.

Директор товариства Бердніков С.В_____

ДОДАТОК В. Наказ на суміщення відповідальності

Товариство з обмеженою відповідальністю “Рейтранс”.

НАКАЗ

«___»_____ Дніпро №_____

Про створення КСЗІ
у товаристві з обмеженою відповідальністю
“Рейтранс”.

ДОРУЧИТИ:

Назарець Кирилу Владиславовичу, керівнику відділу маркетингу, без увільнення його від основної роботи обумовленої трудовим договором, виконання додаткової роботи на умовах суміщення за посадою адміністратора безпеки зі щомісячною доплатою в розмірі 40 % посадового окладу, з дати підписання наказу.

Директор товариства Бердніков С.В_____

ДОДАТОК Г. Відгук керівників розділів

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. (« відмінно »).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Ґ. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:

на тему створення комплексної системи захисту інформації

інформаційно-телекомунікаційної системи підприємства ТОВ "Рейтранс"

ст. гр. 125-18-3 Мінченко Микити Владиславовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 89 сторінках та містить 11 рисунків, 21 таблицю, 14 джерел та 5 додатків.

Метою кваліфікаційної роботи є підвищити рівень захисту інформації в Інформаційно – телекомунікаційній системі ТОВ «Рейтранс».

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

В кваліфікаційній роботі було проаналізовано стан інформаційної захищеності на підприємстві, нормативно-правова база, що регулює відносини в інформаційній сфері. Проведено обстеження ТОВ «Рейтранс» та обґрунтовано створення комплексної системи захисту інформації.

В рамках другого розділу було розроблено модель порушника, модель загроз та проведено оцінку ризиків інформації, що можуть призвести до завдання збитків ТОВ «Рейтранс». Згідно з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових інформаційно-телекомунікаційної системи підприємства.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності властивостей інформації з обмеженим доступом в інформаційно-телекомунікаційній системі ТОВ «Рейтранс».

До недоліків кваліфікаційної роботи потрібно віднести незначні відхилення від стандартів оформлення.

За час дипломування Мінченко М.В. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійної програми «Кібербезпека».

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

Кваліфікаційна робота заслуговує на оцінку «__відмінно__».

Керівник кваліфікаційної роботи

доц. Сафаров.О.О