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

**Інститут електроенергетики**
**Факультет інформаційних технологій**
**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеню бакалавра

**студента** *Чурсиної Марії Кирилівни*

**академічної групи** *125-20-1*

**спеціальності** *125 Кібербезпека*

**спеціалізації**[1]

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

**на тему** *Комплексна система захисту інформації інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Мередіан»*

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | к.т.н., проф. Котух Є.В. | | | |
| розділів: | | | | |
| спеціальний | ст. викл. Кручінін О.В. | | | |
| економічний | к.е.н., доц. Пілова Д.П. | 94 | відмінно | |
| **Рецензент** | | | | |
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**
**2024**

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

«_____»_____20___року

**ЗАВДАННЯ**
**на кваліфікаційну роботу**
**ступеня бакалавра**

**студенту** ***Чурсиній Марії Кирилівні*** **академічної групи** ***125-20-1***
(прізвище ім'я по-батькові) (шифр)

**спеціальності** *125 Кібербезпека*
(код і назва спеціальності)

**на тему** ***Комплексна система захисту інформації інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Мередіан»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Розділ 1 | Обстеження інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Мередіан», аналіз загроз безпеки та обґрунтування профілю захищеності системи | 15.03.2024 |
| Розділ 2 | Аналіз стану послуг безпеки, розробка проектних рішень щодо реалізації вимог безпеки | 10.05.2024 |
| Розділ 3 | Економічне обґрунтування доцільності впровадження запропонованих проектних рішень кваліфікаційної роботи | 11.06.2024 |

**Завдання видано** _____ Євген КОТУХ
(підпис керівника) (ім'я, прізвище)

**Дата видачі: 01.04.2024р.**

**Дата подання до екзаменаційної комісії: 28.06.2024р.**

**Прийнято до виконання** _____ Марія ЧУРСИНА
(підпис студента) (ім'я, прізвище)

# РЕФЕРАТ

Пояснювальна записка: 124 с., 15 рис., 31 табл., 9 додатків, 14 джерел.

Об'єкт розробки: інформаційно-комунікаційна система товариства з обмеженою відповідальністю «Мередіан».

Предмет розробки: комплексна система захисту інформації для інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Мередіан».

Мета кваліфікаційної роботи: забезпечення необхідного рівня захисту інформації в інформаційно-комунікаційній системі товариства з обмеженою відповідальністю «Мередіан».

У першому розділі наведені загальні відомості про підприємство та обґрунтування необхідності створення комплексної системи захисту інформації, виконано обстеження середовищ функціонування підприємства, проаналізовано модель загроз та модель порушника, визначені вимоги до функцій захисту інформації в інформаційно-комунікаційній системі підприємства.

У другому розділі було проведено аналіз стану послуг безпеки, запропоновано проектні рішень щодо реалізації визначеного рівня захисту інформації в інформаційно-комунікаційній системі підприємства.

У третьому розділі виконано обґрунтування економічної доцільності розробки, розраховано капітальні та експлуатаційні витрати на впровадження та обслуговування комплексної системи захисту інформації, визначено річний економічний ефект від впровадження запропонованих рішень.

Практична цінність розробки полягає у забезпечені необхідного рівня захисту інформації в інформаційно-комунікаційній системі товариства з обмеженою відповідальністю «Мередіан» шляхом впровадження комплексної системи захисту інформації.

ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБСТЕЖЕННЯ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, ПОСЛУГИ БЕЗПЕКИ, ПРОФІЛЬ ЗАХИЩЕНОСТІ

# ABSTRACT

Explanatory note: 124 pp., 15 pic., 31 table, 9 app, 14 sources.

Object of study: information and communication system of the limited liability company «Meredian».

Subject of study: comprehensive information protection system of the information and communication system of the limited liability company «Meredian».

The purpose of the qualification work: to ensure the necessary level of information protection in the information and communication system of the limited liability company «Meredian».

The first section provides general information about the enterprise and justifies the need to create a comprehensive information protection system, conducted a survey of the environment of the enterprise, analyzed the threat model and the model of the violator, determined the requirements for the functions of information protection in the information and communication system of the enterprise.

In the second section, an analysis of the state of security services was carried out, design solutions were proposed to implement a certain level of information protection in the information and communication system of the enterprise.

The third section substantiates the economic feasibility of development, calculates capital and operating costs for the implementation and maintenance of an integrated information security system, determines the annual economic effect of the implementation of the proposed solutions.

The practical value of the development is to provide the necessary level of information protection in the information and communication system of the limited liability company «Meredian».

OBJECT OF INFORMATION ACTIVITY, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, SURVEY, THREAT MODEL, INTRUDER MODEL, INFORMATION AND COMMUNICATION SYSTEM, SECURITY SERVICES, SECURITY PROFILE

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

| | | |
|---|---|---|
| АС | – | автоматизована система; |
| БФП | – | багатофункціональний прилад; |
| ДТЗС | – | допоміжні технічні засоби та системи; |
| ЗУ | – | закон України; |
| ІКС | – | інформаційно-комунікаційна система; |
| ІзОД | – | інформація з обмеженим доступом; |
| КЗ | – | контрольована зона; |
| КЗЗ | – | комплексні засоби захисту; |
| КСЗІ | – | комплексна система захисту інформації; |
| КПП | – | контрольовано-пропускний пункт; |
| НД ТЗІ | – | нормативний документ системи технічного захисту інформації; |
| ОІД | – | об’єкт інформаційної діяльності; |
| ОС | – | операційна система; |
| ОТЗ | – | основні технічні засоби; |
| ПЗ | – | програмне забезпечення; |
| ПК | – | персональний комп’ютер; |
| ПКП | – | приймально-контрольний прилад; |
| ТП | – | трансформаторна підстанція; |
| ЦКД | – | цивільний кодекс України. |

ЗМІСТ

с.

# ВСТУП

В наш час актуальним для багатьох підприємств постає задача захисту інформації. Розвиток сучасних технологій веде за собою все більше нових загроз, тому необхідною складовою системи будь-якого підприємства є впровадження необхідного рівня захисту інформації. Відсутність своєчасно впроваджених рішень та методів щодо реалізації безпеки інформації можуть призвести до великих фінансових витрат через виникнення подій порушення властивостей інформації.

Об'єктом розробки є інформаційно-комунікаційна система товариства з обмеженою відповідальністю «Мередіан».

Предметом розробки є комплексна система захисту інформації для інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Мередіан».

Метою роботи є забезпечення необхідного рівня захисту інформації в інформаційно-комунікаційній системі товариства з обмеженою відповідальністю «Мередіан».

Завдання роботи включають:

1. Проведення акту обстеження середовищ функціонування ІКС підприємства;
2. Аналіз загроз інформації в ІКС підприємства;
3. Обґрунтування профілю захищеності;
4. Аналіз стану послуг безпеки;
5. Проектні рішення щодо реалізації послуг безпеки;
6. Обґрунтування економічної доцільності запровадження запропонованих проектних рішень.

Практичне значення роботи полягає у забезпечені необхідного рівня захисту інформації в інформаційно-комунікаційній системі товариства з обмеженою відповідальністю «Мередіан» шляхом впровадження комплексної системи захисту інформації.

# РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

## 1.1 Загальні відомості про підприємство

ТОВ «Мередіан» займається розробкою та проектуванням корпусних меблів. Компанія співпрацює з дизайнерами інтер'єрів, різними компаніями по виробництву меблів та індивідуальними замовниками. Конструкторські проекти можуть включати в себе офісні корпусні меблі, кухонні гарнітури та будь-які спеціалізовані меблі для приміщень. Компанія на ринку з 2019 року, річний оборот – близько 1,1 млн грн.

Організаційна структура даного підприємства відображена на рис. 1.1.

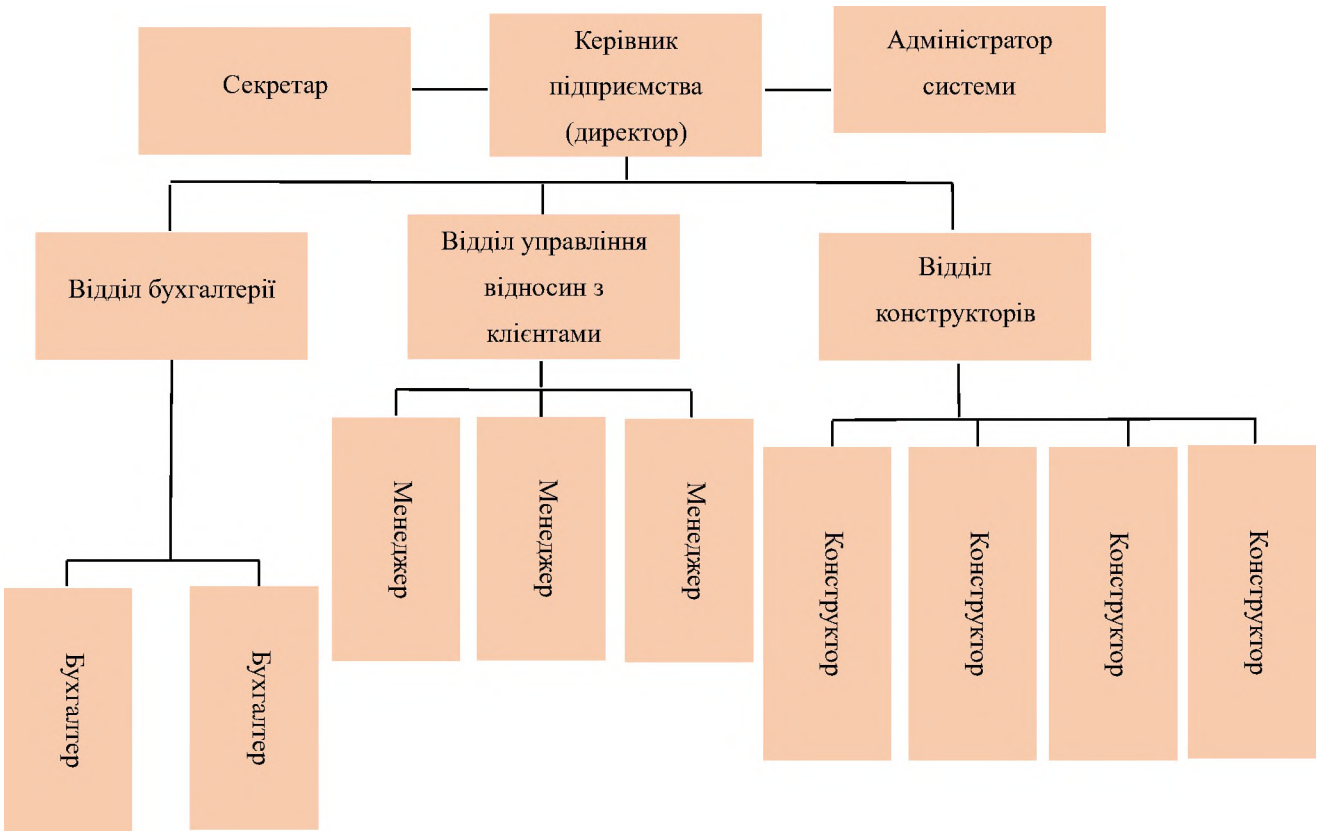


Рисунок 1.1 – Організаційна структура підприємства

Штат працівників підприємства налічує в собі 13 осіб.

Графік роботи підприємства: з понеділка по п'ятницю з 9:00 до 17:00.

## 1.2 Обґрунтування необхідності створення КСЗІ

Для обґрунтування необхідності створення комплексної системи захисту інформації (КСЗІ) виконується аналіз нормативно-правових актів, на підставі яких може встановлюватися обмеження доступу до певних видів інформації або визначається необхідність забезпеченні захисту інформації.

Відповідно до статті 2 ЗУ «Про захист інформації в ІТС» [1]:

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Відповідно до статті 5 ЗУ «Про захист інформації в ІТС»:

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Відповідно до першої частини статті 9 ЗУ «Про захист інформації в ІТС»:

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Відповідно до пункту 1 статті 20 ЗУ «Про Інформацію» [2]:

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Відповідно до статті 21 ЗУ «Про Інформацію»:

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

3. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

Згідно з пунктом 2 статті 4 ЗУ «Про захист персональних даних» [3]:

Володільцем чи розпорядником персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи - підприємці, які обробляють персональні дані відповідно до закону.

Згідно з пунктом 2 статті 5 ЗУ «Про захист персональних даних»:

Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень.

Відповідно до пункту 2 статті 10 ЗУ «Про захист персональних даних»:

Використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

Згідно зі статтею 505 ЦКУ «Поняття комерційної таємниці» [4]:

1. Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

2. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Основною задачею створення КСЗІ є захист інформації, що обробляється в автоматизованій системі (АС). В інформаційно-комунікаційній системи (ІКС) ТОВ «Мередіан» зберігається та обробляється інформація з обмеженим доступом (ІзОД), до якої належать персональні дані працівників та комерційна таємниця, що потребують захисту.

Впровадження КСЗІ забезпечує зниження фінансових витрат підприємства від потенційних загроз для інформації, що обробляється в ІКС. Через надійний захист інформації та своєчасне виявлення загроз зменшується кількість простоїв системи, що підвищує продуктивність роботи та забезпечує високий рівень доступності інформації в системі.

## 1.3 Обстеження середовищ функціонування ІКС

Згідно з НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [5] під час виконання робіт з обстеження середовищ функціонування ІКС розглядається як організаційно-технічна система, яка поєднує:

- фізичне середовище,
- обчислювальну систему,
- середовище користувачів,
- оброблювальну інформацію і технологію її обробки.

### 1.3.1 Фізичне середовище функціонування ІКС

#### 1.3.1.1 Ситуаційний план

Опис ситуаційного плану.

На рисунку Б.1 додатку Б зображено ситуаційний план підприємства. Умовні позначення до ситуаційного плану зображено на рисунку Б.2 додатка Б.

Швейна фабрика «Сучасний край» здає в оренду адміністративну будівлю підприємству, що знаходиться на території цієї фабрики. За договором узгоджено, що орендатори не є конкурентами для цього підприємства.

Об’єкт інформаційної діяльності (ОІД) знаходиться на 3 поверсі 4-х поверхової адміністративної будівлі за адресою вул. Шинна 27Н.

Зона, що охороняється: територія підприємства. Власники підприємства винайняли охоронне агентство, що забезпечує контрольований доступ до території підприємства та основних адміністративних будівель, що розташовані в межах території цього підприємства.

На в'їзді до території встановлені контрольовано-пропускні пункти (далі – КПП) з системою відеоспостереження. Встановленні залізні ворота для в'їзду транспорту, залишаються відчиненими в період робочого дня у будні дні з 9:00 до 18:00. Пропуск робітників на території виконується при пред'явленні пропуску з особистими даними та фотографією власника, запис ведеться у паперовий журнал охороною на КПП. Власники підприємства, на території якого компанія винаймає офісне приміщення, замовили для всього персоналу компанії пропуски. Для сторонніх осіб (відвідувачів) при проходженні КПП на вході до території підприємства створюється тимчасовий пропуск та записуються дані у журнал, за умови заздалегідь інформування співробітників охорони КПП про очікування відвідування цієї особи та пред'явлення документів, що підтверджують його особистість. Після виходу з території підприємства тимчасовий пропуск вилучається.

Пропуск на територію у неробочі години чи вихідні дні обмежений: відбувається лише за окремими списками від керівників при наданні постійного пропуску.

Біля головної дороги вздовж воріт підприємства є зона, де можуть стояти автомобілі, що не охороняється.

На першому поверсі адміністративної будівлі, де розташований ОІД, встановлений КПП. На прохідній пропуск співробітників та відвідувачів здійснюється при пред'явленні оператору КПП постійного та тимчасового пропуску відповідно (біля оператора КПП розміщений механічний роторний турнікет). За прохідною розташовані сходи підйому на верхні поверхи будівлі. На всіх поверхах будівлі встановленні камери відеоспостереження. В сходовому прольоті камери відеоспостереження відсутні.

КЗ обмежена приміщенням, в якій знаходиться ОІД. Режим контрольованої зони (КЗ) забезпечується службою охорони, яка організувала систему допуску персоналу в контрольовану зону. В КЗ можна потрапити лише через вхідні двері, які оснащені електромеханічним замком (вхід – механічний/безконтактний ключ, вихід – вбудована кнопка виходу). Служба охорони видала кожному співробітнику компанії комплект механічний/безконтактний ключів. Біля вхідних дверей встановлений комплект відеодомофону (панель виклику розташована ззовні біля вхідних дверей ОІД, відеопанель – в приміщенні біля робочого місця секретаря).

В робочий час (з понеділка по п'ятницю з 9:00 до 17:00) до КЗ мають право доступу співробітники компанії та відвідувачі. Допуск відвідувачів до КЗ здійснюється наступним чином – перетнувши зону, що охороняється, відвідувач (зі заздалегідь запланованою і затвердженою зустріччю) телефонує у відеодомофон, підтверджує свою особистість, інформує секретаря, який відкриває доступ у контрольовану зону цьому відвідувачу.

В неробочий час доступ до КЗ обмежений. Керівництво компанії заздалегідь створює окремі списки, де зазначено який співробітник, в який день та час має право доступу до КЗ. Зазначимо, допуск до зони, що охороняються, проходить через ті ж самі списки.

Зовнішні стіни будівлі зроблені з залізобетону товщиною 300 мм, внутрішні стіни – цегляні, товщиною 200 мм. Будівля має один вхід – центральний, двері – металеві розміром 2000×800 мм, покриття зовнішнє/внутрішнє – лист металу товщиною 2мм/2мм. Вікна в будівлі встановлені металопластикові з двокамерним склом розміром 1200×800 мм. Висота стелі – 3 м. Дах виготовлений з металочерепиці. Поряд з будівлею впорядкована територія асфальтом.

На рисунку Б.3 додатка Б зображено схему комунікацій ситуаційного плану ОІД. Умовні позначення до схеми комунікації ситуаційного плану ОІД зображено на рисунку Б.4 додатка Б.

Система електроживлення – з'єднана кабельними лініями з трансформаторною підстанцією (ТП), що знаходиться на відстані 5 м від будівлі. Підключення кабелю виконано від ТП на глибині 3 м в щитову на 3-му поверсі через підвальне приміщення, де знаходиться щитова будівлі. До ТП сторонні споживачі не підключені (лише в межах території підприємства).

Система теплопостачання – труби централізованого водопостачання входять до котельної, що знаходиться на відстані 36 м від будівлі, де розташована ОІД. Трубопровід теплопостачання проведені від котельної до підвального приміщення будівлі, де розташована ОІД, під землею. Використовується система двотрубного опалення, труби виготовлені з поліпропілену. Доступ до трубопроводу теплопостачання забезпечується через люки, що прямують від котельної до будівлі.

Система водопостачання – труби централізованого водопостачання проходять через котельну і прямують до підвального приміщення, де розташована ОІД, під землею. Водопостачання до ОІД не доходить. Доступ до трубопроводу водопостачання забезпечується через люки, що прямують від котельної до будівлі.

Система заземлення – система TN-CS. PEN-провідник проведений від ТП до розподільного електричного щитка будівлі, звідти розділений PEN-провідник (PE – захисний провідник, N – нульовий провідник) проводиться до споживача.

Система Інтернет – оптоволоконний кабель провайдера проходить під землею, заходить до комутатора (з вбудованим медіаконвертором) на першому поверсі будівлі, виходить кабель витої пари через стіни на третій поверх і заходить у коммутатор в ОІД.

Система вентиляції – механічна припливно-витяжна вентиляція. Встановлена на кожному поверсі в будівлі, де розміщена ОІД. Системи приточних та витяжних повітропроводів вмонтовані горизонтально, в підвісну стелю. За допомогою приточних та витяжних дифузорів повітря поступає та витягується з приміщення. Ззовні стін будівлі встановлений приточна та витяжна установка.

В таблиці 1.1 наведений опис будівель та споруд, що зображені на ситуаційному плані ІКС.

Таблиця 1.1 – Опис будівель та споруд на ситуаційному плані ІКС

| Найменування | Кількість поверхів | Адреса | Відстань від ОІД, м |
|---|---|---|---|
| 1. Адміністративна будівля | 4 | Вул. Шинна 27Н | 0 |
| 2. Адміністративна будівля | 5 | Вул. Шинна 27С | 11 |
| 3. Промислова споруда | 2 | Вул. Шинна 27А | 22 |
| 4. Виробничий цех | 3 | Вул. Шинна 27К | 14 |
| 5. Складське приміщення | 1 | Вул. Шинна 29 | 41 |
| 6. Складське приміщення | 1 | Вул. Шинна 31А | 62 |
| 7. Виробничий комплекс | 1 | Вул. Шинна 31В | 78 |
| 8. Багатоквартирний будинок | 9 | Вул. Шинна 25 | 69 |
| 9. Квартирний будинок | 5 | Вул. Шинна 23С | 104 |
| 10. СТО | 1 | Вул. Шинна 23А | 65 |
| 11. Багатоквартирний будинок | 9 | Вул. Шинна 35А | 102 |
| 12. Спортивний комплекс | 2 | Вул. Шинна 35В | 82 |
| 13. Медичний центр | 3 | Вул. Шинна 37А | 52 |
| 14. Багатоквартирний будинок | 9 | Вул. Шинна 38А | 48 |
| | | | |

Продовження таблиці 1.1

| Найменування | Кількість поверхів | Адреса | Відстань від ОІД, м |
|---|---|---|---|
| 15. Багатоквартирний будинок | 9 | Вул. Шинна 38В | 36 |
| 16. Багатоквартирний будинок | 9 | Вул. Шинна 38Д | 32 |
| 17. Багатоквартирний будинок | 9 | Вул. Шинна 38Е | 30 |

1.3.1.2 Генеральний план

Опис генерального плану.

На рисунку В.1 додатка В зображено генеральний план ОІД. Умовні позначення до генерального плану зображено на рисунку В.2 додатка В.

Загальна площа ОІД становить 168 м$^2$.

Внутрішні стіни офісу обшиті полівінілхлоридними панелями товщиною 8 мм. Стеля обшита накладними панелями «Армстронг» розміром 600×600×12 мм. Висота стелі 3 м, з навісною стелею – 2,7 м. Підлога покрита лінолеумом.

Вхідні двері виготовлені з МДФ, обшиті сталевим листком товщиною 0,5 мм, розміром 2040×840×940 мм. В стінах вмонтовані металопластикові двокамерні вікна розміром 1200×800 мм, 8 штук. На кожному вікні стоять алюмінієві жалюзі.

З вікон кабінету директора та відділу конструкторів, що виходять на північний-захід, видно вікна іншої адміністративної будівлі, що розташована в 11 м від будівлі ОІД.

На генеральному плані відображені приміщення, в яких знаходяться основні технічні засоби (далі – ОТЗ), допоміжні технічні засоби та системи (далі ДТЗС) та суміжні з ним приміщення.

Відображені місця розташування:

– ОТЗ: персональні комп'ютери (далі – ПК), ноутбуки, багатофункціональні прилади (далі – БФП), сервери, маршрутизатор, комутатор,

– ДТЗС: проектор, система охоронно-пожежної сигналізації, відеодомофон,

– металевої підлогової шафи на ключі та сейфу.

Комбінацію ключа від сейфу знає лише директор. В сейфі зберігаються контракти з партнерами, клієнтами, фінансові звіти, бізнес плани компанії (документи у паперовому вигляді).

Відображені крупні елементи інтер'єру, такі як дерев'яні шафи, ящики, робочі столи, крісла, корзини для сміття.

Документи, представлені у паперовому вигляді, зберігаються у дерев'яних шафах відповідного відділу підприємства. Документація розбита на відповідні папки за профілем документів для збереження.

Всі персональні комп'ютери та ноутбуки розташовані на столах. Усі БФП розташовані на окремих столах. Сервери та комутатор розташовані в металевій підлоговій шафі у кабінеті адміністратора системи. Шафа на ключі, ключ зберігається у адміністратора. Доступ до кабінету адміністратора має лише сам адміністратор та прибиральниця у відповідний період часу (з 18:30 до 19:30 кожного робочого дня).

У Таблиці Г.1 додатку Г наведено перелік основних технічних засобів та мінімальна відстань від об'єкта до межі ОІД. У Таблиці Г.2 додатку Г наведено перелік допоміжних засобів та систем та мінімальна відстань від об'єкта до основних ТЗ (далі ОТЗ).

Елементи та лінії технічних систем в приміщеннях в яких знаходиться ОТЗ вказані на окремих планах.

На рисунку В.3 додатка В зображено лінії системи електропостачання та освітлення генерального плану. Умовні позначення до рисунку ліній системи електропостачання та освітлення генерального плану зображено на рисунку В.4 додатка В.

На рисунку В.5 додатка В зображено комп'ютерну мережу підприємства на генеральному плані. Умовні позначення до рисунку комп'ютерної мережі підприємства на генеральному плані зображено на рисунку В.6 додатка В.

На рисунку В.7 додатка В зображено лінії системи опалення та водопостачання генерального плану. Умовні позначення до рисунку лінії системи опалення та водопостачання генерального плану зображено на рисунку В.8 додатка В.

На рисунку В.9 додатка В зображено систему вентиляції на генеральному плані. Умовні позначення до рисунку системи вентиляції на генеральному плані зображено на рисунку В.10 додатка В.

На рисунку В.11 додатка В зображено лінії системи охоронно-пожежної сигналізації генерального плану. Умовні позначення до рисунку лінії системи охоронно-пожежної сигналізації генерального плану зображено на рисунку В.12 додатка В.

Живлення прямує від щитової будинки на першому поверсі до щитової на поверсі, де знаходиться ОІД. Щитова замикається на ключ, ключ знаходиться у охорони на першому поверсі. В щитовій стоять пакетні автоматичні вимикачі по зонах: на весь поверх, на коридор та санвузол, на кожну кімнату ОІД. У кожній кімнаті ОІД встановлені вимикачі освітлення та зовнішні розетки з замленням.

Кабель Ethernet заходить від комутатора на першому поверсі у охорони до маршрутизатора в ОІД. Від маршрутизатора протянуто кабель витої пари до комутатора. Протягування кабелю витої пари від комутатора до персональних комп'ютерів виконано через стіни з використанням розеток RJ45.

В будівлі встановлена водяна двотрубна система опалення, труби виготовлені з поліпропілену. Перша пара стояків (труба подачі гарячої води та труба відводу) розміщені у відділі бухгалтерії, поруч з місцем секретаря, відповідають за опалення зони кабінету директора та відділу бухгалтерії. Друга пара стояків розміщені у відділі конструкторів, поруч з робочим місцем конструктора, відповідають за опалення зони відділу конструкторів та менеджерів.

Система водопостачання до ОІД не доходить, в стіні вмонтована труба стояку системи водопостачання та системи каналізації.

Системи приточних та витяжних повітропроводів вмонтовані горизонтально, за фальшстелею. За допомогою приточних та витяжних дифузорів повітря поступає та витягується з приміщення. Ззовні стін будівлі встановлений приточна та витяжна установка.

Система охоронно-пожежної сигналізації в ОІД встановлена охоронним підприємством. Ця система складається з: пожежних датчиків, об'ємно інфрачервоних сповіщувачів, токових магнітоконтактних сповіщувачів на вікнах та деяких дверях, точкового ручного сповіщувача та комбінованого світло-звукового сповіщувача. В кабінеті адміністратора розміщений ПКП, всі сповіщувачі з ПКП з'єднані за допомогою кабелів. Клавіатура ПКП розміщена біля вхідних дверей, запрограмована, кожний користувач має свої паролі входу (зняття с охорони).

### 1.3.2 Обчислювальна система

Структурна схема обчислювальної системи підприємства зображена на рисунку 1.2:

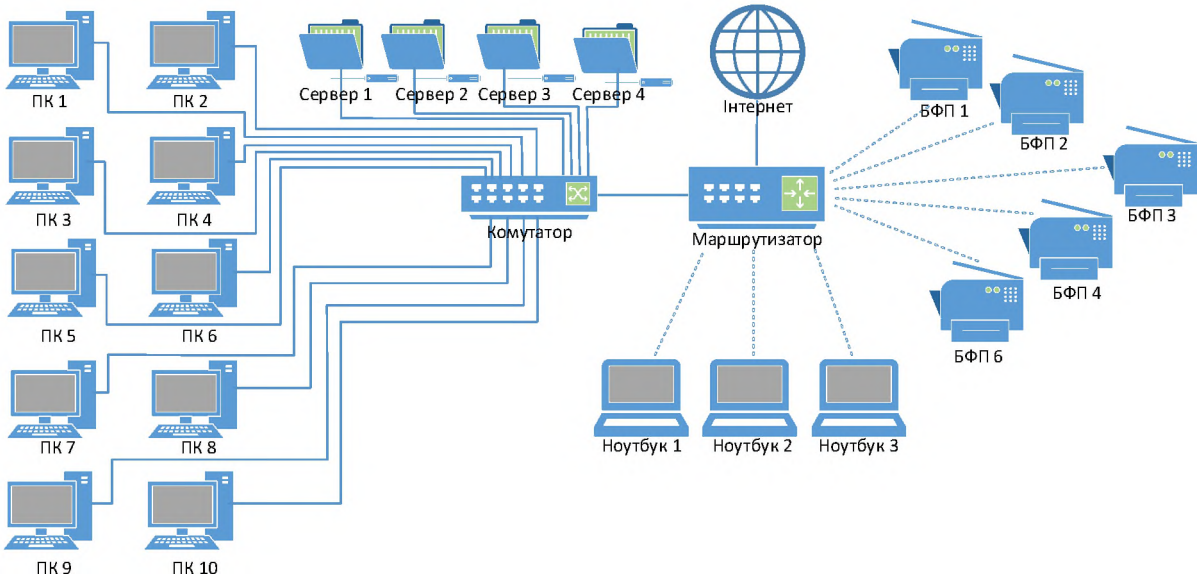


Рисунок 1.2 – Структурна схема ІКС підприємства

Автоматизована система підприємства налічує в собі:

– 10 персональних комп'ютерів (один в кабінеті директора, один в кабінеті адміністратора, чотири в відділі конструкторів, чотири в відділі бухгалтерії);

– 3 ноутбуки (усі в відділ менеджерів);

– 5 БФП (один в кабінеті директора, два у відділі бухгалтерії, один у відділі конструкторів, один у відділі менеджерів);

– 4 сервери (розміщені у кабінеті адміністратора);

– 1 маршрутизатор (розміщений у кабінеті адміністратора);

– 1 комутатор (розміщений у кабінеті адміністратора).

Маршрутизатор є шлюзом між глобальною та локальною мережею. Усі ноутбуки та БФП підключені до локальної мережі бездротовим шляхом (по Wi-Fi). Усі персональні комп'ютери та сервери підключені до локальної мережі кабелями витої пари через комутатор. АС має доступ до мережі Інтернет, провайдер – «Київстар».

За допомогою операційної системи маршрутизатора Mikrotik налаштовані MAC-адреси пристроїв в мережі, врегулюваний доступу до деяких сайтів, виконано відслідковування використаного мережевого трафіку користувачів.

Всі користувачі підключені до домену в мережі компанії. Управління всередині мережі відбувається за допомогою Active Directory, що встановлений на Сервері 3. Також на цьому сервері налаштована функція файлового сховища – створені папки спільного користування для різних груп користувачів з розмежуванням доступу до них.

На Сервері 1 встановлений M.E.Doc Server, доступ до якого виконується через клієнтську версію програми. На сервері встановлена автоматично база даних – Fire Bird, для подання електронної бухгалтерської звітності.

На Сервері 2 встановлений BAF Server, доступ до якого виконується через клієнтську версію програми. Також на сервері встановлена база даних Microsoft SQL Server для роботи BAF-у.

На Сервері 4 – «Back-Up». Адміністратор через віддалений робочий стіл підключається до кожного з серверів, налаштовує функцію автоматичної

архівації даних з цих серверів, зберігаються копії на цьому Сервері 4. Архівні резервні копії бази даних M.E.Doc, BAF та файлів спільного доступу, завантажуються на Сервер 4 кожної суботи, о 1:00, 2:00, 3:00 годині відповідно. Також на цьому сервері зберігаються образи всіх серверів, які адміністратор створює на свій розсуд.

У таблиці Д.1 додатку Д наведена характеристика складу ІКС.

Перелік програмного забезпечення ІКС наведено у таблиці 1.2.

Таблиця 1.2 – Перелік програмного забезпечення ІКС

| Найменування | Тип ПЗ | Тип ліцензії | Де встановлено |
|---|---|---|---|
| 1. Microsoft Windows 11 [10.0.22631.3737], version 23H2 (Updated June 2024) | Системне | Корпоративна ліцензія | ПК 1 – 10<br>Ноутбук 1 - 3 |
| 2. Windows Server [10.0.25398.950], version 23H2 (Updated June 2024) | Системне | Корпоративна ліцензія | Сервер 1 – 4 |
| 3. Microsoft Office 365 Business Standard | Прикладне | Корпоративна ліцензія | ПК 1 – 10<br>Ноутбук 1 - 3 |
| 4. M.E.Doc v.11.02.127 | Прикладне | Корпоративна ліцензія | ПК 2, 8 – 10 |
| 5. DYNALOG Blum v.3643-01 | Прикладне | Безкоштовна | ПК 3 – 6 |
| 6. BAF v. 8.3.19.1529 | Прикладне | Ліцензія на сервер | ПК 1, 2, 8 – 10<br>Ноутбук 1 – 3<br>Сервер 2 |
| 7. BAS. Управління торгівлею | Прикладне | Клієнтська ліцензія на 5 робочих місць | Ноутбук 1 – 3<br>ПК 2 |
| | | | |

Продовження таблиці 1.2

| Найменування | Тип ПЗ | Тип ліцензії | Де встановлено |
|---|---|---|---|
| 8. Antivirus Norton 360 | Прикладне | Клієнтська ліцензія | ПК 1 – 10<br>Ноутбук 1 – 3 |
| 9. Microsoft SQL Server 2022 16.0.1000.6 | Прикладне | Клієнтська ліцензія | Сервер 2<br>ПК 2 |

1.3.3 Інформаційне середовище

В таблиці 1.3 виконано класифікація інформації, що циркулює в ІКС підприємства. Для цього було визначено режим доступу до інформації, її правовий режим, вид представлення в системі та визначено відповідний рівень захищеності властивостей інформації, таких як конфіденційність, цілісність та доступність.

Таблиця 1.3 – Класифікація інформації, яка циркулює в ІКС

| Вид інформації | Режим доступу | Правовий режим | Вид представлення в ІКС | Вимоги до захисту | | |
|---|---|---|---|---|---|---|
| | | | | К | Ц | Д |
| 1. Клієнтська база | ІзОД | Конфіденційна | Текстовий | 4 | 4 | 3 |
| 2. Персональна інформація працівників підприємства | ІзОД | Конфіденційна | Текстовий | 2 | 2 | 3 |
| 3. Конструктор-ська база (креслення, дизайни) | ІзОД | Комерційна таємниця | Текстовий<br>Графічний | 4 | 3 | 4 |

Продовження таблиці 1.3

| Вид інформації | Режим доступу | Правовий режим | Вид представлення в ІКС | Вимоги до захисту | | |
|---|---|---|---|---|---|---|
| | | | | К | Ц | Д |
| 4. Фінансові звіти про прибуток компанії | ІзОД | Конфіденційна | Текстовий | 4 | 5 | 3 |
| 5. Звіти про нарахування заробітної плати | ІзОД | Конфіденційна | Текстовий | 2 | 3 | 2 |
| 6. Контактна інформація підприємства | Відкрита інформа-ції | – | Текстовий | 1 | 1 | 1 |
| 7. Інформація про засоби захисту ІКС підприємства та інформація для авторизації працівників підприємства | ІзОД | Конфіденційна | Текстовий | 5 | 5 | 4 |
| 8. Розклад зустрічей і подій | ІзОД | Комерційна таємниця | Текстовий | 2 | 3 | 2 |
| 9. Контракти з клієнтами | ІзОД | Комерційна таємниця | Текстовий | 4 | 4 | 3 |
| 10. Комерційні пропозиції | ІзОД | Комерційна таємниця | Текстовий | 2 | 2 | 2 |

Для визначення вимог до захисту кожного виду інформації поставимо у відповідність рівень властивості інформації, яким вони задовольняють.

Рівні конфіденційності:

– К1 – рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають доступу до неї, або при якому інформація не є конфіденційною;

– К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

– К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

– Ц1 – рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

– Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

– Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

– Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

– Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

– Д1 – рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

– Д2 – рівень доступності інформації, при якому компанія 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.

Розглянемо технологію обробки кожного виду інформації.

1. Клієнтська база

Інформація представлена у вигляді бази даних, обробляється у програмі BAF. Зберігається база даних клієнтів на сервері 2. Для контрагентів в базі зберігаються такі дані: назва підприємства, ЄДРПО (ІНН для ФОП-ів), юридична та фактична адреса організації, ПІБ власника компанії, контактні дані (номер телефону, адреса електронної пошти, месенджери). Доступ до цієї інформації мають директор підприємства, бухгалтера, менеджери та адміністратор системи. Друк можливий працівникам, що мають доступ до цієї інформації.

2. Персональна інформація працівників підприємства

Інформація вноситься адміністратором системи в домені підприємства при створенні користувачів домену. Заноситься загальна інформація про особу: ФІО, ім'я користувача при вході, посаду, назву організації, назву відділу, адресу місця проживання, номер мобільного телефону. Також адміністратор системи створює користувачів в програмі BAF, заповнювати інформацію про особу може як адміністратор, так і бухгалтер. Доступ до інформації мають директор підприємства, бухгалтера та адміністратор системи. Можливий друг інформації про особу через програмний застосунок BAF.

3. Конструкторська база

Інформація обробляється в програмі DYNALOG Blum. Програма встановлена на персональних комп'ютерах конструкторів (ПК 3-6). В програмі конструктори створюють 3D моделі проектів меблів та креслення з повним розрахунком для подальшого виготовлення. Ця інформація зберігається на Сервері 3 у папці спільного доступу для відділу конструкторів. Доступ до інформації є лише у конструкторів та адміністратора системи. Друк можливий працівникам, що мають доступ до цієї інформації.

4. Фінансові звіти про прибуток компанії

Інформація представлена у вигляді бази даних, обробляється у програмі BAF, інтерфейс «Звіти». Це можуть статистичні звіти при витрати і прибуток компанії, звіти купівлі/продажу. Доступ до цієї інформації мають працівники відділу бухгалтерії, директор підприємства та адміністратор системи. Вносити зміни до інформації можуть працівники відділу бухгалтерії Для подання звітності виконується підвантаження готового звіту у M.E.Doc для подальшої відправки у податкову. Друк можливий працівникам, що мають доступ до цієї інформації.

5. Звіти про нарахування заробітної плати

Інформація представлена у вигляді бази даних, обробляється у програмі BAF, інтерфейс «Заробітна плата і кадри». Доступ до цієї інформації мають лише працівники відділу бухгалтерії, директор підприємства та адміністратор системи. Вносити зміни до інформації можуть працівники відділу бухгалтерії. Для подання звітності виконується підвантаження готового звіту у M.E.Doc для подальшої відправки у податкову. Друк можливий працівникам, що мають доступ до цієї інформації.

6. Контактна інформація підприємства

В Google Maps адміністратор створив профіль компанії, де розміщена основна контактна інформація: назва компанії, профіль діяльності, адреса, графік роботи, контактний номер, адреса електронної пошти. Кожний працівник

компанії має візитну карту, де розміщена контактна інформація підприємства та особисті контакти.

7. Інформація про засоби захисту ІКС підприємства та інформація для авторизації працівників підприємства

Інформація обробляється на Сервері 3 в Active Directory адміністратором. Всі користувачі належать одному домену мережі підприємства. Адміністратор додає користувачів в домен з унікальним логіном та паролем, об'єднує їх у групи, та надає групам користувачів відповідні права та дозволи до ресурсів. Ця інформація зберігається у базі даних домену. З використанням інструменту Групова політика (Group Policy) адміністратор в Active Directory керує правилами для конфігурації комп'ютерів (налаштування брандмауера, встановлення прав доступу до ресурсів на локальному диску, налаштування мережі, моніторинг подій) та для конфігурації користувачів (налаштування прав доступу до робочого столу, налаштування робочого середовища, обмеження можливості встановлення програм користувачами).

8. Розклад зустрічей та подій

Інформацію заповнює секретар в календарі Microsoft Outlook. Відповідному співробітнику компанії приходить сповіщення про подію, місце та час проведення. Змінювати зміст події має право секретар та директор компанії.

9. Контракти з клієнтами

Інформація являє собою договір про надання послуг. Вміст такого юридичного документу:

– назва договору, номер договору, дата укладання договору та сторони договору;

– предмет договору;

– вартість послуг та умови оплати;

– обов'язки сторін;

– терміни дії договору;

– порядок вирішення спорів та форс-мажорних ситуацій;

– підписи.

Директор компанії створює договір та відправляє юристу для перевірки на відповідність. Далі відправляє копію документа другій стороні договору для узгодження. Електронна версія підписаного документу зберігається на сервері 3, доступ має лише директор та адміністратор системи. Договори в паперовому вигляді зберігаються у сейфі в кабінеті директора. Друк можливий працівникам, що мають доступ до цієї інформації.

10. Комерційні пропозиції

Ця інформація може надходити від партнерів або інших комерційних компаній. Надходить на поштовий ящик підприємства, до секретаря. Ці листи секретар може пересилати на поштову адресу директора або менеджерам на подальший розгляд. Також менеджери можуть складати листи з комерційними пропозиціями від компанії. Інформація в листі складається з назви компанії, контактних даних та зміст самої пропозиції. Можливий друк.

Схема інформаційних потоків ІКС підприємства наведена на рис. 1.3.

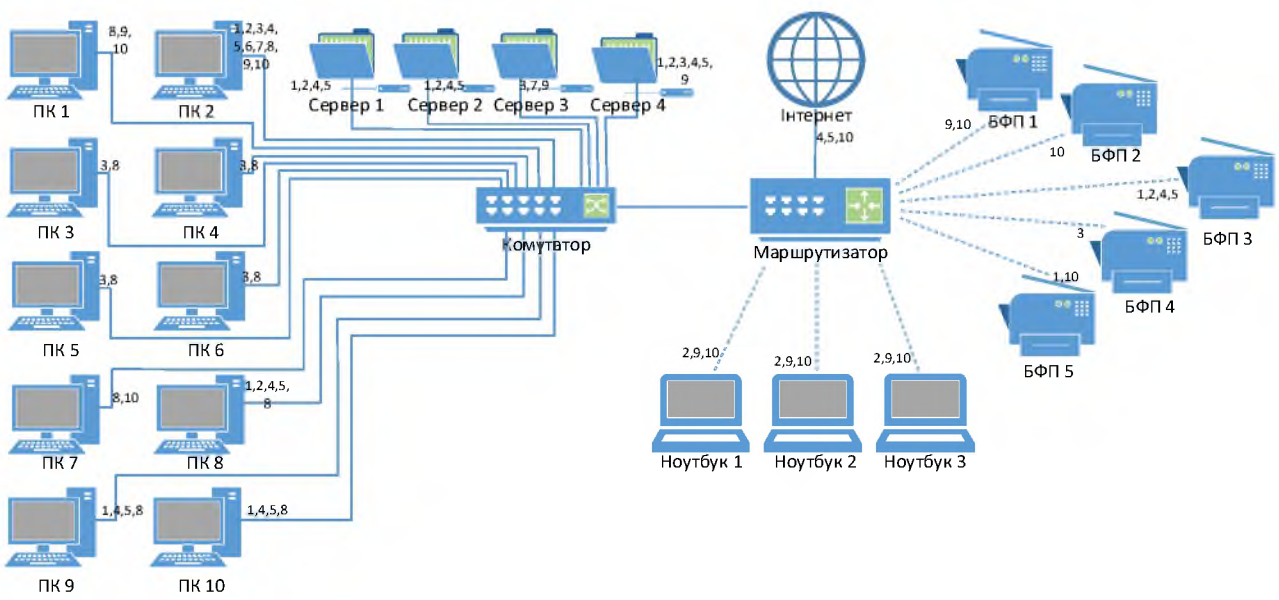


Рисунок 1.3 – Схема інформаційних потоків

1.3.4 Середовище користувачів

Штат працівників налічує в собі 13 осіб. Далі перелічено штат працівників та наведено опис їх службових обов'язків з рівнем кваліфікації та роллю користувача в системі:

Керівник компанії – директор. В його обов'язки входить: управління персоналом, постановка задачі роботи компанії, розробка стратегії розвитку компанії, контроль за фінансовими операціями та бюджетом компанії, зв'язки з партнерами та клієнтами. Рівень кваліфікації – невпевнений користувач комп'ютером. Роль користувача в системі – звичайний користувач.

Секретар. Його задача відповідати на телефонні дзвінки, електронні листи, що надсилаються на пошту підприємства, пересилати електронні листи напряму до відповідних працівників за необхідності. Також секретар займається організацією графіку зустрічей або конференцій директора. Рівень кваліфікації – впевнений користувач: офісні додатки, поштові сервіси. Роль користувача в системі – звичайний користувач.

Адміністратор. Його основна задача – адмініструванням всієї системи компанії: налаштування та керування доступу працівників до певних об'єктів та ресурсів системи, оновлення ПЗ технічних пристроїв, управління мережею, адміністрування серверів, моніторинг та аналіз продуктивності системи. Також адміністратор відповідає за технічну підтримку користувачів. Рівень кваліфікації – впевнений користувач системи Windows. Роль користувача в системі – адміністратор.

Бухгалтери. Займаються веденням бухгалтерського обліку: запис та аналіз фінансових транзакцій компанії, підготовка фінансових, податкових звітів, ведення кадрів. Рівень кваліфікації – впевнений користувач: офісні додатки, поштові сервіси, програма ведення бухгалтерського обліку BAF, програма для ведення та подання бухгалтерської електронної звітності M.E.Doc. Роль користувача в системі – звичайний користувач.

Менеджери. Відповідають за ведення клієнтської бази, керування відносинами з клієнтами, аналіз ринку. Також вони створюють звітність по результатам своєї роботи. Рівень кваліфікації – впевнений користувач: офісні додатки, поштові сервіси, програма ведення бухгалтерського обліку BAF. Роль користувача в системі – звичайний користувач.

Конструктори. Займаються розробкою, проектуванням та модернізацією головної продукції компанії – корпусні меблі. Рівень кваліфікації – впевнений користувач: офісні додатки, програма для проектування корпусних меблів. Роль користувача в системі – звичайний користувач.

Позаштатними працівниками є технічний персонал, що обслуговує будови та приміщення, в яких розташовані компоненти ІКС, такі як:

– прибиральники;

– електрики, сантехники.

В таблиці 1.4 описано матрицю розмежування доступу користувачів системи до інформації.

Таблиця 1.4 – Матриця розмежування доступу

| Користувач | Кількість працівників | Інформація | | | | | | | | | | Ресурси |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
| Адміністратор системи | 1 | ЧЗВ І/Е | ЧЗВ І/Е | ЧЗВ І/Е | ЧЗВ І/Е | ЧЗВ І/Е | ЧЗВ | ЧЗВ | ЧЗВ | ЧЗВ І/Е | - | Всі ресурси |
| Директор | 1 | ЧЗВ І/Е | ЧЗВ І/Е | - | ЧЗВ І/Е | ЧЗВ І/Е | Ч | - | ЧЗВД | ЧЗВД І/Е | ЧВД | ПК 1, Інтернет, БФП 1 |
| Секретар | 1 | - | - | - | - | - | Ч | - | ЧЗВ | - | ЧВД | ПК 7, Інтернет, БФП 2 |
| Конструктор | 4 | - | - | ЧЗВД І/Е | - | - | Ч | - | Ч | - | - | ПК 3-6, Інтернет, БФП 4 |

Продовження таблиці 1.4

| Користувач | Кількість працівників | Інформація | | | | | | | | | | Ресурси |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
| Менеджер | 3 | ЧЗ Д І/Е | - | - | - | - | Ч | - | Ч | - | ЧЗ ВД | Ноутбук 1-3, Інтернет, БФП 5 |
| Бухгалтер | 3 | ЧЗ Д І/Е | ЧЗ В Д І/Е | - | ЧЗ В І/Е | ЧЗ В І/Е | Ч | - | Ч | Ч І/Е | - | ПК 8-10, Інтернет, БФП 3 |

Умовні позначення прав доступу до інформації:

Ч – читання;

З – запис;

В – видалення;

Д – друк;

І/Е – імпорт/експорт на зовнішні носії.

Немає обмеження на використання зовнішніх носіїв. В мережі домену заборонено встановлення та запуск сторонніх програм без втручання адміністратора. Повноваження керувати КЗЗ має лише адміністратор системи.

## 1.4 Аналіз загроз інформації в системі

### 1.4.1 Модель порушника

Згідно з НД ТЗІ 1.1-003 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [6] порушником називають користувача, який здійснює несанкціонований доступ до інформації.

Модель порушника відображає практичні та теоретичні можливості порушника, знання, час і місце події.

Порушників поділяють на дві основні групи: зовнішні та внутрішні, по відношенню до ІКС.

Зовнішніми порушниками є сторонні особи, що знаходяться поза межами контрольованої зони підприємства, та отримують несанкціонований доступ до ІзОД з використанням технічних засобів перехоплення інформації або агентурних методів. Прикладами зовнішніх порушників є відвідувачі, що підслухали конфіденційну розмову, або ж агенти конкурентів, які отримують доступ до інформації із застосуванням методів та засобів активного впливу на технічні засоби.

Внутрішніми порушниками є користувачі системи або обслуговуючий персонал, що мають безпосередній доступ до компонентів ІКС.

Відповідно до НД ТЗІ 1.4-001 «Типове положення про службу захисту інформації в автоматизованій системі» [7] класифікація порушників виконується за наступними ознаками:

– рівень знань про ІКС (в залежності від кваліфікації порушника);

– рівень можливостей (в залежності від методів і засобів, що використовуються);

– час дії (в залежності від активності або пасивності системи);

– місце дії (в залежності від території допуску до засобів системи).

Для визначення рівня загрози порушника використовуємо таблиці 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, в яких виконаний розподіл категорій порушників та його ознак за рівнем загрози від «1» до «4».

Таблиці 1.5 – Категорії порушників, визначених у моделі

| Позначення | Визначення категорії | Рівень загроз |
|---|---|---|
| | Внутрішній по відношенню до ІКС | |
| ПВ1 | Технічний персонал, який обслуговує будови та приміщення, в яких розташовані компоненти ІКС (прибиральники, електрик) | 1 |
| ПВ2 | Служба охорони | 3 |
| | | |

Продовження таблиці 1.5

| | | |
|---|---|---|
| ПВ3 | Обслуговуючий персонал ІКС (Адміністратор системи) | 4 |
| ПВ4 | Користувачі ІКС (Директор, Секретар, Бухгалтери, Конструктори, Менеджери) | 2 |
| | Зовнішні по відношенню до ІКС | |
| ПЗ1 | Відвідувачі (клієнти) | 1 |
| ПЗ2 | Колишні працівники | 2 |
| ПЗ3 | Представники організацій, що взаємодіють з питань технічного забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання і таке інше) | 2 |
| ПЗ4 | Хакери | 3 |
| ПЗ5 | Агенти конкурентів | 4 |

Таблиця 1.6 – Специфікація моделі порушника за мотивами здійснення порушень

| Позначення | Мотив порушення | Рівень загрози |
|---|---|---|
| М1 | Безвідповідальність | 1 |
| М2 | Самоствердження | 2 |
| М3 | Корисливий інтерес | 3 |
| М4 | Професійний обов’язок (ПЗ4) | 4 |

Таблиця 1.7 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІКС

| Позначення | Основні кваліфікаційні ознаки порушника | Рівень загрози |
|---|---|---|
| К1 | Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІКС | 1 |
| К2 | Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІКС та їх обслуговування | 2 |
| | | |

Продовження таблиці 1.7

| Позначення | Основні кваліфікаційні ознаки порушника | Рівень загрози |
|---|---|---|
| К3 | Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІКС | 3 |
| К4 | Знає структуру, функції й механізми дії засобів захисту інформації в ІКС, їх недоліки та можливості | 4 |

Таблиця 1.8 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

| Позначення | Характеристика можливостей порушника | Рівень загрози |
|---|---|---|
| З1 | Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях | 1 |
| З2 | Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІКС | 2 |
| З3 | Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону | 3 |
| З4 | Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІКС, дезорганізації систем обробки інформації | 4 |

Таблиця 1.9 – Специфікація моделі порушника за часом дії

| Позначення | Характеристика можливостей порушника | Рівень загрози |
|---|---|---|
| Ч1 | Під час повної бездіяльності ІКС з метою відновлення та ремонту | 1 |
| Ч2 | Під час призупинки компонентів ІКС з метою технічного обслуговування та модернізації | 2 |
| Ч3 | Під час функціонування ІКС (або компонентів системи) | 3 |
| Ч4 | Як у процесі функціонування ІКС, так і під час призупинки компонентів системи | 4 |

Таблиця 1.10 – Специфікація моделі порушника за місцем дії

| Позначення | Характеристика місця дії порушника | Рівень загрози |
|---|---|---|
| Д1 | Усередині приміщень, але без доступу до технічних засобів ІКС | 1 |
| Д2 | З робочих місць користувачів (операторів) ІКС | 2 |
| Д3 | З доступом у зону зберігання баз даних, архівів тощо | 3 |
| Д4 | З доступом у зону керування засобами забезпечення безпеки ІКС | 4 |

Класифікація порушників ІКС підприємства наведена в таблиці 1.11.

Згідно моделі порушників, серед внутрішніх порушників найбільший рівень загрози мають адміністратор ІКС та представник служби охорони. Серед зовнішніх порушників по відношенню до ІКС найбільшу загрозу представляють хакери та агенти конкурентів.

Таблиця 1.11 – Модель порушників

| Посада | Категорія порушника | Мотив порушника | Рівень обізнаності щодо ІКС | Можливості щодо подолання системи захисту | Можливості за часом дії | Можливості за місцем дії | Сума загроз |
|---|---|---|---|---|---|---|---|
| Внутрішні порушники по відношенню до ІКС | | | | | | | |
| Прибиральник | ПВ1 | М1 | К1 | З1 | Ч3 | Д1 | 8 |
| | 1 | 1 | 1 | 1 | 3 | 1 | |
| Електрик | ПВ1 | М1 | К1 | З1,З2 | Ч1,Ч2 | Д1,Д2 | 9 |
| | 1 | 1 | 1 | 1,2 | 1,2 | 1,2 | |
| Представник служби охорони | ПВ2 | М1,М3 | К2 | З1,З2 | Ч4 | Д4 | 18 |
| | 3 | 1,3 | 2 | 1,2 | 4 | 4 | |
| Адміністратор ІКС | ПВ3 | М2,М3 | К4 | З4 | Ч4 | Д2, Д3,Д4 | 23 |
| | 4 | 2,3 | 4 | 4 | 4 | 2,3,4 | |
| Користувач | ПВ4 | М1,М2,М3 | К2 | З1,З2 | Ч3 | Д2,Д3 | 15 |
| | 2 | 1,2,3 | 2 | 1,2 | 3 | 3,2 | |
| Зовнішні порушники по відношенню до ІКС | | | | | | | |
| Відвідувач (клієнт) | ПЗ1 | М1, М3 | К1 | З1,З2 | Ч3 | Д1 | 11 |
| | 1 | 1,3 | 1 | 1,2 | 3 | 1 | |
| Колишній працівник | ПЗ2 | М3 | К2 | З1,З2,З3 | Ч3 | Д2 | 15 |
| | 2 | 3 | 2 | 1,2,3 | 3 | 2 | |
| Спеціаліст з технічного забезпечення життєдіяльності систем | ПЗ3 | М1 | К2 | З1,З2 | Ч1 | Д1 | 9 |
| | 2 | 1 | 2 | 1,2 | 1 | 1 | |
| Хакер | ПЗ4 | М3 | К3 | З4 | Ч4 | Д3 | 20 |
| | 3 | 3 | 3 | 4 | 4 | 3 | |
| Агент конкурентів | ПЗ5 | М4 | К2,К3 | З2,З3 | Ч3 | Д1,Д2 | 19 |
| | 4 | 4 | 2,3 | 2,3 | 3 | 1,2 | |

### 1.4.2 Модель загроз

Загрозою називають можливу небезпеку (потенційну або реально існуючу) вчинення будь-якого діяння, спрямованого проти об'єкта захисту (інформаційного ресурсу), що завдає шкоди власнику цього об'єкта та виявляється в загрозі спотворення і втрати інформації.

Загроза виникає при взаємодії потенційного джерела загрози з фактором (вразливістю) об'єкта захисту. Усі джерела загроз безпеці інформації можна поділити на такі групи:

– спричинені дією суб'єкта – антропогенні джерела загроз;

– спричинені технічними засобами – техногенні джерела загроз;

– спричинені стихійними лихами.

Антропогенні та техногенні джерела загроз в свою чергу можуть бути як зовнішніми, так і внутрішніми.

Зовнішніми антропогенними джерелами загроз можуть бути випадкові особи або потенційні злочинці, що мають різний рівень кваліфікації. Внутрішніми антропогенними суб'єктами загроз є особи, що мають високий рівень обізнаності у сфері експлуатації технічних засобів, знайомі з основними функціями та принципами роботи засобів захисту інформації. До них відноситься основний, допоміжний та технічний персонал.

Зовнішніми техногенними джерелами загроз є канали зв'язку та системи інженерних комунікацій, а внутрішніми – технічне обладнання та програмне забезпечення.

Стихійними джерелами загроз називають природні катаклізми або такі обставини, що зазвичай неможливо передбачити та запобігти. Такі обставини мають абсолютний і об'єктивний характер, що поширюється на всіх.

При створенні переліку джерел загроз для системи підприємства виконується ранжування загроз за рівнем небезпеки ($К_{оп}$). Оцінка ступеня небезпеки за непрямими показниками, такими як можливість виникнення джерела (К1), готовність джерела (К2) та фатальність (К3). Кожний показник вимірюється аналітичним методом по п'ятибальній шкалі.

Ступінь небезпеки для кожного джерела ($К_{оп\_д}$) визначається як відношення добутків показників, описаних вище, до максимального значення (125).

В таблиці 1.12 наведено перелік джерел загроз для ІКС підприємства та визначений ступінь небезпеки кожної загрози.

Кожному джерелу загрози надано умовне позначення, що складається з умовного позначення групи джерел загроз та його порядкового номеру серед джерел цієї групи.

Таблиця 1.12 – Джерела загроз

| Назва | Позначення | К1 | К2 | К3 | $К_{оп\_д}$ |
|---|---|---|---|---|---|
| І.А. Антропогенні зовнішні | | | | | |
| 1. Відвідувачі (клієнти) | І.А.1 | 1 | 1 | 1 | 0,01 |
| 2. Колишні працівники | І.А.2 | 2 | 2 | 2 | 0,06 |
| 3. Представники організацій, що взаємодіють з питань технічного забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання і таке інше) | І.А.3 | 1 | 1 | 1 | 0,01 |
| 4. Хакери | І.А.4 | 2 | 4 | 4 | 0,26 |
| 5. Агенти конкурентів | І.А.5 | 2 | 5 | 4 | 0,32 |
| І.В Антропогенні внутрішні | | | | | |
| 6. Технічний персонал, який обслуговує будови та приміщення, в яких розташовані компоненти ІКС (прибиральники, електрик) | І.В.1 | 1 | 1 | 2 | 0,01 |
| 7. Служба охорони | І.В.2 | 2 | 1 | 2 | 0,03 |
| 8. Обслуговуючий персонал ІКС (Адміністратор) | І.В.3 | 5 | 4 | 4 | 0,64 |
| 9. Користувачі ІКС (Директор, Секретар, Бухгалтери, Конструктори, Менеджери) | І.В.4 | 3 | 2 | 3 | 0,14 |
| ІІ.А. Техногенні зовнішні | | | | | |
| 10. Канали комп’ютерного зв’язку | ІІ.А.1 | 4 | 2 | 5 | 0,32 |

Продовження таблиці 1.12

| Назва | Позначення | К1 | К2 | К3 | $К_{оп\_д}$ |
|---|---|---|---|---|---|
| 11. Система електропостачання | II.A.2 | 3 | 2 | 4 | 0,19 |
| II.B. Техногенні внутрішні | | | | | |
| 12. Мережеве обладнання | II.B.1 | 4 | 4 | 3 | 0,38 |
| 13. Технічне обладнання | II.B.2 | 3 | 2 | 3 | 0,15 |
| 14. Сервери | II.B.3 | 4 | 2 | 4 | 0,26 |
| 15. Прикладне забезпечення | II.B.4 | 3 | 3 | 3 | 0,21 |
| 16. Системне забезпечення | II.B.5 | 3 | 3 | 4 | 0,29 |
| III.A. Стихійні лиха | | | | | |
| 17. Пожежа | III.A.1 | 3 | 2 | 4 | 0,19 |
| 18. Війна | III.A.2 | 5 | 5 | 5 | 1 |
| 19. Землетруси | III.A.3 | 3 | 2 | 3 | 0,14 |
| 20. Смерчі | III.A.4 | 2 | 2 | 3 | 0,1 |
| 21. Повінь | III.A.5 | 3 | 3 | 4 | 0,29 |

Ті джерела загроз, що мають значення показника ступеня небезпеки менше ніж 0,1 надалі будуть не враховуватися, оскільки вважаються малоймовірними.

Загрози проявляються через чинники (вразливості), що призводять до порушення безпеки інформації на конкретному об’єкті. Кожній загрозі можуть бути співставленні різні вразливості.

Кожна вразливість безпеки має відповідний клас (позначається великою літерою), групу (позначається римською цифрою) та підгрупу (позначається маленькою літерою). В цілому, вразливості безпеки поділяють на три основних класи:

– об’єктивні;

– суб’єктивні;

– випадкові.

Виникнення об’єктивних вразливостей зумовлено особливістю побудови обладнання об’єкту захисту і їх технічних характеристик. Усунення цих вразливостей повністю неможливе, але можна послабити з використанням інженерно-технічних методів протидії загроз безпеки інформації. До об’єктивних вразливостей можна віднести ті, що:

– супутні технічними засобами випромінювання: електромагнітні, електричні, звукові;

– активуються: апаратні та програмні закладки;

– визначаються особливістю елементів: володіють електроакустичними перетвореннями, піддаються впливу електромагнітного поля;

– визначаються особливістю об'єкта, що захищається: місцем розташування об'єкта, організацією каналів обміну інформацією.

Суб'єктивні вразливості залежать від дій співробітників підприємства. Усунення таких вразливостей можливе за допомогою організаційних та програмно-апаратних методів захисту. До суб'єктивних вразливостей можна віднести наступні:

– помилки: під час підготовки та використання програмних засобів, під час управління складних систем, під час експлуатації технічних засобів;

– порушення режиму: охорони та захисту, експлуатації технічних засобів, використання інформації, конфіденційності.

Випадкові вразливості залежать від особливості середовища, що оточує об'єкт захисту, та непередбачуваних обставин. Усунення таких чинників можливе тільки під час проведення комплексу організаційних та інженерно-технічних заходів протидії загрозам інформаційної безпеки. До випадкових вразливостей можна віднести наступні:

– збої та відмови: технічних засобів, програмного забезпечення, електропостачання;

– пошкодження: життєзабезпечувальних комунікацій та огороджувальних конструкцій.

При створенні переліку вразливостей безпеки системи підприємства виконується ранжування загроз за рівнем небезпеки ($К_{оп}$). Оцінка ступеня небезпеки за непрямими показниками, такими як фатальність (К1), доступність використання вразливості джерелом загрози (К2) та кількістю елементів об'єкта, яким характерна ця вразливість (К3).

Ступінь небезпеки для кожної вразливості безпеки ($К_{оп\_в}$) визначається як відношення добутків показників, описаних вище, до максимального значення (125).

В таблицях 1.13, 1.14 та 1.15 наведено перелік об'єктивних, суб'єктивних та випадкових вразливостей безпеки ІКС підприємства відповідно. Для кожної вразливості визначено ступінь небезпеки.

Таблиця 1.13 – Об'єктивні вразливості безпеки

| Назва | | Познач. | К1 | К2 | К3 | $К_{оп\_в}$ |
|---|---|---|---|---|---|---|
| А.І Об'єктивні вразливості, супутні технічними засобами випромінювання | | | | | | |
| Електромагнітні випромінювання кабельних ліній технічних засобів | | А.І.а | 1 | 1 | 1 | 0,01 |
| А.ІІ Об'єктивні вразливості, що активуються | | | | | | |
| Апаратні закладки, що встановлюються у | Мережі електроживлення | А.ІІ.а.1 | 2 | 2 | 4 | 0,13 |
| | У приміщенні | А.ІІ.а.2 | 3 | 3 | 3 | 0,21 |
| | У технічних засобах | А.ІІ.а.3 | 4 | 2 | 3 | 0,19 |
| Програмні закладки | Шкідливі програми | А.ІІ.b.1 | 3 | 3 | 3 | 0,21 |
| | Технологічні виходи з програм | А.ІІ.b.2 | 1 | 2 | 2 | 0,03 |
| | Нелегальні копії ПЗ | А.ІІ.b.3 | 3 | 4 | 2 | 0,19 |
| А.ІІІ Об'єктивні вразливості, які визначаються особливостями елементів | | | | | | |
| Що піддаються впливу електромагнітного поля | Магнітні носії | А.ІІІ.b.1 | 3 | 2 | 3 | 0,14 |
| | Мікросхеми | А.ІІІ.b.2 | 2 | 2 | 3 | 0,1 |
| А.IV Об'єктивні вразливості, які визначаються особливостями об'єкта, що захищається | | | | | | |
| Місцем розташування об'єкта: наявність прямої видимості об'єктів | | А.IV.а | 4 | 1 | 3 | 0,1 |

Таблиця 1.14 - Суб'єктивні вразливості безпеки

| Назва | | Познач. | К1 | К2 | К3 | $К_{оп\_в}$ |
|---|---|---|---|---|---|---|
| В.І Суб'єктивні вразливості: помилки | | | | | | |
| Під час підготовки та використання програмного забезпечення | Інсталяції та завантаження програмного забезпечення | В.І.а.1 | 2 | 2 | 1 | 0,03 |
| | Експлуатації програмного забезпечення | В.І.а.2 | 2 | 2 | 2 | 0,06 |
| | Введення даних | В.І.а.3 | 1 | 2 | 2 | 0,03 |
| Під час експлуатації технічних засобів | Під час увімкнення/вимкнення технічних засобів | В.І.с.1 | 2 | 2 | 2 | 0,06 |
| | Використання засобів обміну інформацією | В.І.с.2 | 2 | 2 | 3 | 0,09 |
| В.ІІ Суб'єктивні вразливості: порушення | | | | | | |
| Режиму охорони та захисту | Доступу на об'єкт | В.ІІ.а.1 | 3 | 2 | 3 | 0,14 |
| | Доступу до технічних засобів | В.ІІ.а.2 | 4 | 2 | 3 | 0,19 |
| Режиму експлуатації технічних засобів | Енергозабезпечення | В.ІІ.b.1 | 1 | 1 | 5 | 0,04 |
| | Життєзабезпечення | В.ІІ.b.2 | 1 | 1 | 5 | 0,04 |
| Режиму використання інформації: зберігання та знищення носіїв інформації | | В.ІІ.с | 4 | 5 | 4 | 0,64 |
| Режиму конфіденційності | Співробітниками в неробочий час | В.ІІ.d.1 | 2 | 3 | 1 | 0,05 |
| | Звільненими співробітниками | В.ІІ.d.2 | 2 | 3 | 1 | 0,05 |
| Режиму безпеки системи: підвищені привілеї | | В.ІІ.е | 4 | 5 | 5 | 0,8 |

Таблиця 1.15 – Випадкові вразливості безпеки

| Назва | | Познач. | К1 | К2 | К3 | $К_{оп\_в}$ |
|---|---|---|---|---|---|---|
| С.І Випадкові вразливості: збої та відмови | | | | | | |
| Відмови та несправності технічних засобів | Що обробляють інформацію | С.І.а.1 | 3 | 2 | 5 | 0,24 |
| | Що зберігають інформацію (внутрішні) | С.І.а.2 | 4 | 2 | 5 | 0,32 |

Продовження таблиці 1.15

| Назва | | Познач. | К1 | К2 | К3 | $К_{оп\ в}$ |
|---|---|---|---|---|---|---|
| | Що забезпечують працездатність засобів обробки інформації | C.I.a.3 | 2 | 2 | 5 | 0,16 |
| Старіння і розмагнічування носіїв інформації | Жорстких дисків | C.I.b.1 | 3 | 2 | 4 | 0,14 |
| | Елементів мікросхем | C.I.b.2 | 3 | 2 | 4 | 0,14 |
| | Кабелів і з'єднувальних ліній | C.I.b.3 | 2 | 2 | 4 | 0,13 |
| Збої програмного забезпечення | Операційних систем і СУБД | C.I.c.1 | 3 | 2 | 3 | 0,14 |
| | Прикладних програм | C.I.c.2 | 2 | 2 | 3 | 0,10 |
| | Антивірусних програм | C.I.c.3 | 3 | 2 | 3 | 0,14 |
| Збої електропостачання: обладнання, що обробляє інформацію | | C.I.d | 3 | 2 | 5 | 0,24 |
| Збої локальної мережі | | C.I.e | 2 | 2 | 5 | 0,16 |
| C.II Випадкові вразливості: пошкодження | | | | | | |
| Пошкодження життєзабезпечувальних комунікацій: електро-, водо-, теплопостачання | | C.II.a | 3 | 2 | 5 | 0,24 |
| Пошкодження огороджувальних конструкцій: корпусів технологічного обладнання (серверна шафа) | | C.II.b | 3 | 2 | 2 | 0,10 |

Перелік загроз ІКС підприємства наведено в таблиці Е.1 додатка Е.

Загрози, що мають значення показника вище за 0,8, позначимо як актуальні загрози для ІКС підприємства. Перелік актуальних загроз для системи визначено у таблиці 1.16.

Таблиця 1.16 – Перелік актуальних загроз

| Загроза | Порушення | | | Коефіцієнт небезпеки |
|---|---|---|---|---|
| | К | Ц | Д | |
| Втрата носіїв інформації, що містять ІзОД | + | - | - | 0,09 |

Продовження таблиці 1.16

| Загроза | Порушення | | | Коефіцієнт небезпеки |
|---|---|---|---|---|
| | К | Ц | Д | |
| Несанкціоноване призначення атрибутів доступу користувачам адміністратором системи | + | + | + | 0,51 |
| Відмова носіїв інформації на сервері | - | + | + | 0,08 |
| Відмова маршрутизатора | - | + | + | 0,09 |

## 1.5 Обґрунтування профілю захищеності

Згідно з НД ТЗІ 2.5-005 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [8] АС підприємства відповідає «3» класу. Обрано стандартний профіль захищеності комп'ютерної системи, що входить до складу АС класу «3» з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності оброблювальної інформації:

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

Загальний опис послуг наведено в НД ТЗІ 2.5-004 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [9].

Відповідно до проаналізованих загроз системи визначено перелік послуг безпеки, що пов'язані з ними:

{НР-2, НО-2, ЦО-2, ДС-1, ДЗ-2}.

Перелік сформованих критеріїв оцінки захищеності інформації в системі надано в таблиці 1.17.

Таблиця 1.17 – Критерії оцінки захищеності інформації в системі

| Критерії | Послуги безпеки | Вимоги до рівнів послуги безпеки |
|---|---|---|
| Конфіденційності | Довірча конфіденційність | КД-2. Базова довірча конфіденційність |
| | Адміністративна конфіденційність | КА-2. Базова адміністративна конфіденційність |
| | Повторне використання об’єктів | КО-1. Повторне використання об’єктів |
| | Конфіденційність при обміні | КВ-2. Базова конфіденційність при обміні |
| Цілісності | Довірча цілісність | ЦД-1. Мінімальна довірча цілісність |
| | Адміністративна цілісність | ЦА-2. Базова адміністративна цілісність |
| | Відкат | ЦО-1. Обмежений відкат |
| | Цілісність при обміні | ЦВ-2. Базова цілісність при обміні |
| Доступності | Використання ресурсів | ДР-1. Квоти |
| | Стійкість до відмов | ДС-1. Стійкість при обмежених відмовах |
| | Гаряча заміна | ДЗ-2. Обмежена гаряча заміна |
| | Відновлення після збоїв | ДВ-1. Ручне відновлення |
| Спостереженості | Реєстрація | НР-2. Захищений журнал |
| | Ідентифікація і аутентифікація | НИ-2. Одиночна ідентифікація і аутентифікація |
| | Достовірний канал | НК-1. Однонаправлений достовірний канал |
| | Розподіл обов’язків | НО-2. Розподіл обов’язків адміністратора |
| | Цілісність комплексу засобів захисту | НЦ-2. КЗЗ з гарантованою цілісністю |
| | Самотестування | НТ-2. Самотестування при старті |
| | Ідентифікація і автентифікація при обміні | НВ-1. Автентифікація вузла |

## 1.6 Висновок

В першому розділі кваліфікаційної роботи було виконано обстеження ОІД:

– загальна інформація про підприємство;

– опис будівлі, де знаходиться ОІД;

– територіальне розміщення компонентів ІКС ОІД, комунікацій, систем життєдіяльності і зв'язку;

– інформація про апаратне та програмне забезпечення в ОІД;

– класифікація інформації в ІКС та інформаційні потоки;

– відомості про користувачів системи та права доступу.

Виконаний аналіз вразливостей системи та джерел загроз, на основі якого виявлено актуальні загрози для системи підприємства. Визначено критерії оцінки захищеності інформації в ІКС.

Необхідно виконати аналіз стану послуг безпеки, за результатами якого надати організаційні, технічні та криптографічні заходи для реалізації цих послуг.

# РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

## 2.1 Аналіз стану послуг безпеки

Профіль захищеності являє собою перелік необхідних рівнів послуг безпеки, які повинен реалізувати комплекс засобів захисту (далі – КЗЗ) обчислювальної системи АС, щоб задовольняти вимоги щодо захищеності оброблювальної інформації в АС.

Для забезпечення вимог щодо захисту інформації виконаємо аналіз рівня реалізації послуг – реалізованих, частково реалізованих та не реалізованих послуг, викладених в таблиці 1.17.

КД-2. Базова довірча конфіденційність. Реалізована

Множина об’єктів. Файлове сховище на жорсткому диску серверу 3: папки спільного користування різних груп користувачів.

Реалізоване розмежування доступу на підставі атрибутів користувача та захищеного об’єкта за допомогою функціоналу системи Windows.

Атрибути доступу користувача: псевдонім користувача, ідентифікатор користувача, ідентифікатор ролі користувача.

Атрибути пасивного об’єкта: найменування об’єкта, ідентифікатор об’єкта, ідентифікатор власника об’єкта, рівень доступу, список керування доступу.

Надається можливість користувачу для захищеного об’єкту, що належить домену, визначити перелік користувачів і/або групи користувачів, що мають право одержувати інформацію від об'єкта: перейти до властивостей безпеки відповідного об’єкту створеного користувачем та надати права доступу до цього об’єкту іншим.

Надається можливість користувачу для процесу, що належить домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес: перейти до властивостей безпеки відповідного процесу та надати права доступу до цього процесу іншим.

Права доступу до кожного захищеного об’єкта встановлюються в момент створення чи ініціалізації за замовчуванням. Атрибути при переносі об’єкта

зберігаються частково (назва об'єкта, розмір, тип, дата створення, атрибути дозволу).

Необхідні умови: НИ-1.

КА-2. Базова адміністративна конфіденційність. Реалізована

Множина об'єктів 1. Файлове сховище на жорсткому диску серверу 3: конструкторська база, контракти з клієнтами.

Множина об'єктів 2. Файлове сховище на жорсткому диску серверів 1 та 2: бази даних M.E.Doc та BAF відповідно.

Множина об'єктів 3. Програмне забезпечення: M.E.Doc, BAF, DYNALOG.

Реалізоване розмежування доступу на підставі атрибутів користувача та захищеного об'єкта: розмежування доступу для користувача або групи користувачів домену до папок на Microsoft Server за допомогою функціоналу Active Directory.

Атрибути доступу користувача: псевдонім користувача, ідентифікатор користувача, ідентифікатор ролі користувача.

Атрибути пасивного об'єкта: найменування об'єкта, ідентифікатор об'єкта, ідентифікатор власника об'єкта, рівень доступу, список керування доступу.

Надається можливість адміністратору для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до домену визначити конкретних користувачів і/або групу користувачів, що мають право одержувати інформацію від об'єкта: за допомогою групової політики домену Active Directory встановити рівень доступу до захищеного об'єкта конкретних користувачів і/або груп користувачів.

Надається можливість адміністратору для кожного процесу шляхом керування належністю користувачів, процесів і об'єктів до домену визначити конкретних користувачів і/або групу користувачів, що мають право ініціювати процес: за допомогою групової політики домену Active Directory встановити рівень доступу до програмного застосунку конкретних користувачів і/або груп користувачів.

Права доступу до кожного захищеного об'єкта встановлюються в момент створення чи ініціалізації за замовчуванням. Атрибути при переносі об'єкта зберігаються частково (назва об'єкта, розмір, тип, дата створення/атрибути дозволу).

Необхідні умови: НО-1, НИ-1.

КО-1. Повторне використання об'єктів. Не реалізовано

Відсутній механізм, який після завершення деякого процесу очищує дані пам'яті, виділеної на даний процес.

Необхідні умови: немає.

КВ-2. Базова конфіденційність при обміні. Частково реалізована

Множина об'єктів 1. Поштові повідомлення.

Інтерфейсний процес 1. Підключення до Інтернет.

Механізм реалізації послуги: забезпечення захищеного з'єднання та передачі даних за протоколом HTTPS (механізм захисту реалізований за допомогою криптографічного протоколу TLS).

Множина об'єктів 2. Файлове сховище на жорсткому диску серверу 3: конструкторська база, фінансові звіти про прибуток компанії, звіти про нарахування заробітної плати, контракти з клієнтами.

Інтерфейсний процес 2. Використання зовнішніх носіїв.

Відсутній механізм реалізації забезпечення конфіденційності інформації при втраті зовнішніх носіїв.

Необхідні умови: НО-1.

ЦД-2. Мінімальна довірча цілісність. Реалізовано.

Множина об'єктів. Файлове сховище на жорсткому диску серверу 3: папки спільного користування різних груп користувачів.

Реалізоване розмежування доступу на підставі атрибутів користувача та захищеного об'єкта за допомогою функціоналу системи Windows.

Атрибути доступу користувача: псевдонім користувача, ідентифікатор користувача, ідентифікатор ролі користувача.

Атрибути пасивного об'єкта: найменування об'єкта, ідентифікатор об'єкта, ідентифікатор власника об'єкта, рівень доступу, список керування доступу.

Надається можливість користувачу для захищеного об'єкту, що належить домену, визначити перелік користувачів і/або групи користувачів, що мають право модифікувати об'єкт: перейти до властивостей безпеки відповідного об'єкту створеного користувачем та надати права на модифікацію цього об'єкту іншим.

Надається можливість користувачу для процесу, що належить домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес: перейти до властивостей безпеки відповідного процесу та надати права доступу до цього процесу іншим.

Права доступу до кожного захищеного об'єкта встановлюються в момент створення чи ініціалізації за замовчуванням. Атрибути при переносі об'єкта зберігаються частково (назва об'єкта, розмір, тип, дата створення, атрибути дозволу).

Необхідні умови: НИ-1.

ЦА-2. Базова адміністративна цілісність. Реалізована

Множина об'єктів 1. Файлове сховище на жорсткому диску серверу 3: конструкторська база, контракти з клієнтами.

Множина об'єктів 2. Файлове сховище на жорсткому диску серверів 1 та 2: бази даних M.E.Doc та BAF відповідно.

Множина об'єктів 3. Програмне забезпечення: M.E.Doc, BAF, DYNALOG.

Реалізоване розмежування доступу на підставі атрибутів доступу процесу (програмного застосунку) та захищеного об'єкта: кожній групі користувачів домену відповідно встановлено перелік програм, дозволених для запуску, з використанням вбудованого функціоналу Windows Server – AppLocker. AppLocker входить до політики безпеки і відповідає за обмеження застосунків.

Атрибути доступу користувача: псевдонім користувача, ідентифікатор користувача, ідентифікатор ролі користувача.

Атрибути пасивного об’єкта: найменування об’єкта, ідентифікатор об’єкта, ідентифікатор власника об’єкта, рівень доступу, список керування доступу.

Надається можливість адміністратору для кожного захищеного об’єкта шляхом керування належністю користувачів, процесів і об’єктів до домену визначити конкретні процеси і/або групи процесів, що мають право модифікувати об’єкт: адміністратор системи налаштовує правила, що встановлюють перелік програм, дозволених для запуску. Відповідно адміністратором створено правило заборони запуску всіх інших програм.

Надається можливість адміністратору для кожного захищеного об’єкта шляхом керування належністю користувачів, процесів і об’єктів до домену визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес: правила, що встановлюють перелік програм, дозволених для запуску, застосовують до відповідних груп користувачів.

ЦА-1. Мінімальна адміністративна цілісність. Реалізована

Реалізоване розмежування доступу на підставі атрибутів користувача та захищеного об’єкта: розмежування доступу для користувача або групи користувачів домену до папок на Microsoft Server за допомогою функціоналу Active Directory.

Атрибути доступу користувача: псевдонім користувача, ідентифікатор користувача, ідентифікатор ролі користувача.

Атрибути пасивного об’єкта: найменування об’єкта, ідентифікатор об’єкта, ідентифікатор власника об’єкта, рівень доступу, список керування доступу.

Надається можливість адміністратору для кожного захищеного об’єкта шляхом керування належністю користувачів, процесів і об’єктів до домену визначити конкретних користувачів і/або групу користувачів, що мають право модифікувати об’єкт: перейти до властивостей безпеки відповідної папки та надати дозволи користувачам і/або групі користувачів.

Права доступу до кожного захищеного об’єкта встановлюються в момент створення чи ініціалізації за замовчуванням. Атрибути при переносі об’єкта

зберігаються частково (назва об’єкта, розмір, тип, дата створення, атрибути дозволу).

Необхідні умови: НО-1, НИ-1.

ЦО-1. Обмежений відкат. Реалізовано

Множина об’єктів: база даних M.E.Doc та BAF, розміщені на сервері 1 та сервері 2 відповідно.

Існує вбудована функція відкату бази даних до попереднього стану: в межах поточної транзакції відмінити незавершені зміни за допомогою команди «ROLLBACK».

ЦО-2. Повний відкат. Реалізовано.

Множина об'єктів: дисковий простір серверів 1, 2 та 3.

Реалізовано автоматизоване резервне копіювання вмісту дискового простору сервері 1, 2 та 3 на сервер 4. Створена подія в домені, яка відповідає за створення архівних копій вмісту серверів та завантаження їх на сервер 4 кожної суботи, о 1:00, 2:00, 3:00 годині відповідно.

Необхідні умови: НИ-1.

ЦВ-2. Базова цілісність при обміні. Не реалізована.

Множина об’єктів: файлове сховище на жорсткому диску серверу 3: конструкторська база, фінансові звіти про прибуток компанії, звіти про нарахування заробітної плати, контракти з клієнтами.

Інтерфейсний процес: використання зовнішніх носіїв.

Відсутній механізм реалізації виявлення порушень цілісності інформації під час імпорту/експорту на зовнішні носії.

Необхідні умови: НО-1.

ДР-1. Квоти. Реалізовано.

Ресурс, на який вводиться обмеження – дисковий простір.

Реалізоване обмеження на використання дискового простору користувачем в домені. На кожного користувача виділено 10 Гб дискового простору на сервері 3, де встановлений домен Active Directory.

ДС-1. Стійкість при обмежених відмовах. Частково реалізовано.

Множина компонентів 1: програмне забезпечення. При виникненні помилки під час експлуатації/запуску програми система повідомляє про помилку (може видати код помилки) та завершити виконання цієї програми. Доступ до всіх інших компонентів КС буде збережений. В Windows 10 реалізована можливість моніторингу стабільності системи.

Множина компонентів 2: апаратне забезпечення – жорсткий диск на серверах. Відмова жорсткого диску на сервері призводить до неможливості функціонування системи (якщо відмовив диск на сервері 3 з доменом Active Directory) та неможливості використання інформації (якщо відмовив диск на сервері 1 та 2). Реалізоване резервне копіювання даних на дисках серверів, але зберігається можливість простою системи на деякий час.

Множина компонентів 3: апаратне забезпечення – маршрутизатор. Відмова маршрутизатора призведе до недоступності даних на серверах та системи в цілому. Доступність КС при такій відмові не збережена.

Необхідні умови: НО-1.

ДЗ-2. Обмежена гаряча заміна. Не реалізовано.

Множина компонентів: апаратне забезпечення – жорсткі диски на серверах.

Не реалізована можливість заміни жорстких дисків на серверах без переривання обслуговування системи.

Необхідні умови: НО-1, ДС-1.

ДВ-1. Ручне відновлення. Частково реалізовано.

Множина типів відмов КС 1: збій операційної системи.

Множина типів відмов КС 2: збій програмного забезпечення – M.E.Doc та BAF.

У разі збоїв операційної системи реалізоване ручне відновлення системи шляхом повторної інсталяції її образу. Адміністратор системи створює образ операційної системи щомісяця.

У разі збоїв програмного забезпечення, а саме програм ведення бухгалтерського обліку та подання електронної звітності BAF та M.E.Doc,

відсутні механізми реалізації ручного відновлення програмних застосунків для повернення КС до нормального функціонування.

Лише адміністратор має повноваження повернути КС до нормального функціонування після переривання обслуговування шляхом ручного відновлення.

Необхідні умови: НО-1.

НР-2. Захищений журнал. Реалізовано.

Журнал реєстрації в домені Active Directory здійснює реєстрацію подій, пов'язаних з безпекою, системою та програмами. Перелік подій, що реєструються:

– аудит успішного входу до домену;

– аудит невдалого входу до домену;

– аудит виходу з системи;

– аудит успішної спроби доступу до об'єкта;

– аудит невдалої спроби доступу до об'єкта;

– аудит зміни дозволів на об'єкт;

– аудит видалення об'єкту;

– аудит створення нового облікового запису користувача домену;

– аудит видалення облікового запису користувача домену;

– аудит виникнення помилки в роботі додатку або системи;

– аудит виникнення попередження про проблеми з апаратним забезпеченням, програмним забезпеченням, драйверами, недостатність пам'яті для роботи додатка.

Журнал реєстрації містить наступну інформацію про подію:

– ідентифікатор події;

– дата та час виникнення події;

– джерело події;

– ідентифікатор типу події;

– тип події: «Інформація», «Попередження», «Помилка», «Аудит успіху», «Аудит невдачі»;

– ім’я користувача, що спричинив подію;

– ім’я комп’ютера, де відбулась подія;

– опис події;

– назва журналу, де збережена подія: «Безпека», «Система», «Програми».

Доступ до перегляду та аналізу журналу реєстрації має лише адміністратор домену.

Необхідні умови: НИ-1.

НИ-2. Одиночна ідентифікація і автентифікація. Реалізовано.

Кожний користувач однозначно ідентифікується КЗЗ. Послуга реалізована шляхом ідентифікація користувача на основі введеного імені користувача для входу (система перевіряє чи існує користувач з таким іменем в домені) та автентифікації користувача по встановленому протоколу на основі даних аутентифікації та введеного паролю.

Протоколом ідентифікації користувача в домені Active Directory є протокол Kerberos. В Active Directory для кожного домену існує Key Distribution Center (KDC), де зберігаються паролі всіх користувачів та комп’ютерів відповідного домену. KDC поділяється на Authentication Service (AS) и Ticket-Granting Service (TGS). При початковій аутентифікації користувач відправляє запит на аутентифікацію до AS шляхом введення ім’я користувача та паролю. AS перевіряє автентичність ім’я користувача та хешу паролю. Якщо автентифікація успішна, то AS видає користувачу квиток початкової аутентифікації Ticket-Granting Ticket (TGT), зашифрований ключем KDC. TGS видається користувачу для доступу до конкретних сервісів (об’єктів) домену.

Необхідна умова: НК-1.

НК-1. Однонаправлений достовірний канал. Реалізовано.

Встановлення достовірного каналу між користувачем та системою під час початкової ідентифікації та аутентифікації реалізований наступними механізмами:

– нічим, окрім клавіатури, неможливо ввести дані;

– при вході в систему чітко встановлено вікно, куди вводити дані.

Зв'язок з використанням даного каналу ініціалізується виключно користувачем.

Необхідні умови: немає.

НО-2. Розподіл обов’язків адміністратора. Не реалізовано.

В системі визначені ролі адміністратора та звичайного користувача з притаманними їм функціями.

Не реалізовано розмежування ролей адміністратора на адміністратора системи та адміністратора безпеки.

Необхідні умови: НИ-1.

НЦ-2. КЗЗ з гарантованою цілісністю. Реалізовано.

Під час запуску система проходить контроль цілісності своїх елементів. Реалізовано за допомогою вбудованої функції в Windows Defender – Безпечне завантаження.

Безпечне завантаження - це стандарт безпеки, розроблений комп'ютерною індустрією, щоб забезпечити завантаження пристрою за допомогою лише програмного забезпечення, якому довіряє виробник обладнання (OEM). Коли комп'ютер запускається, вбудоване програмне забезпечення перевіряє підпис кожного завантажувального програмного забезпечення. Якщо підписи дійсні, комп'ютер завантажується і вбудоване програмне забезпечення забезпечує управління операційною системою і її безпекою.

Необхідні умови: немає.

НТ-2. Самотестування при старті. Реалізовано.

Послуга самотестування комп’ютера при старті в системі реалізується за допомогою програми POST, яку виконує центральний процесор після подачі живлення. POST послідовно перевіряє всі вузли та компоненти комп’ютера. При успішному проходженні POST системний динамік видає один короткий звуковий сигнал.

Необхідні умови: НО-1.

НВ-1. Автентифікація вузла. Реалізовано.

В системі автентифікація вузла реалізована за допомогою системи сертифікатів.

При перевірці наявності оновлень, система Windows встановлює з'єднання з сервером Microsoft за https-протоколом. Наявність в системі довіреного кореневого сертифікату “Microsoft Root Certificate Authority 2011” забезпечує встановлення зашифрованого SSL-з’єднання між клієнтом та сервером Microsoft. Оновлення підписані цифровими підписами Microsoft, що забезпечує їх цілісність та автентичність.

Необхідна умова: немає.

Результат аналізу стану безпеки наведено в таблиці 2.1.

Таблиця 2.1 – Реалізації послуг безпеки

| Критерії | Вимоги до рівнів послуги безпеки | Реалізація послуг безпеки |
|---|---|---|
| Конфіденційності | КД-2. Базова довірча конфіденційність | Реалізовано |
| | КА-2. Базова адміністративна конфіденційність | Реалізовано |
| | КО-1. Повторне використання об’єктів | Не реалізовано |
| | КВ-2. Базова конфіденційність при обміні | Частково реалізовано |
| Цілісності | ЦД-1. Мінімальна довірча цілісність | Реалізовано |
| | ЦА-2. Базова адміністративна цілісність | Реалізовано |
| | ЦО-1. Обмежений відкат | Реалізовано |
| | ЦВ-2. Базова цілісність при обміні | Не реалізовано |
| Доступності | ДР-1. Квоти | Реалізовано |
| | ДС-1. Стійкість при обмежених відмовах | Частково реалізовано |
| | ДЗ-2. Обмежена гаряча заміна | Не реалізовано |
| | ДВ-1. Ручне відновлення | Частково реалізовано |

Продовження таблиці 2.1

| Критерії | Вимоги до рівнів послуги безпеки | Реалізація послуг безпеки |
|---|---|---|
| Спостереженості | НР-2. Захищений журнал | Реалізовано |
| | НИ-2. Одиночна ідентифікація і аутентифікація | Реалізовано |
| | НК-1. Однонаправлений достовірний канал | Реалізовано |
| | НО-2. Розподіл обов'язків адміністратора | Не реалізовано |
| | НЦ-2. КЗЗ з гарантованою цілісністю | Реалізовано |
| | НТ-2. Самотестування при старті | Реалізовано |
| | НВ-1. Автентифікація вузла | Реалізовано |

## 2.2 Проектні рішення щодо реалізації вимог безпеки

### 2.2.1 Елементи політики безпеки

Визначено положення про використання зовнішніх носіїв.

На підприємстві контроль зовнішніх носіїв веде адміністратор системи. Кожний зовнішній носії внесений у реєстр, де вказаний вид зовнішнього носія, його серійний номер, власник носія, місце використання, дата видачі носія, дата повернення носія, статус носія (використовується, втрачений, повернений).

Власникам носіїв заборонено виносити їх за межі КЗ. Кожний зовнішній носії зберігається в шухляді робочого стола користувача.

Заборонено використовувати сторонні носії у службових цілях.

Заборонено використовувати облікові носії у особистих цілях.

Кожні 3 місяці адміністратор проводить низькорівневе форматування (Low Level Format) облікованих носіїв інформації. Очищаються всі дані з носія та таблиця розділів. Для подальшої роботи з носієм інформації адміністратор проводить високорівневе форматування.

Всі обліковані зовнішні носії є зашифрованими. Під час шифрування носіїв задається пароль доступу. Адміністратор виконує шифрування, при видачі зовнішнього носія видається також пароль доступу.

При виявлені пошкодження зовнішні носії знищуються.

Документи, представлені в паперовому вигляді, зберігаються у відповідних місцях, відведених для цього. Користувачі особисто відповідають за ці документи.

Передача роздрукованих версій документів можлива в межах відділу та усього офісу за необхідності.

Визначено положення про використання паролів.

Паролі користувачів домену зберігаються в зашифрованому вигляді.

При створені користувача домену та в програмному застосунку BAF адміністратор надає користувачам тимчасовий пароль, ввімкнена функція «Вимагання встановлення паролю при наступному вході».

Пароль не повинен містити:

– ваші персональні дані (ім'я, прізвище, дату народження);

– комбінації символів, що легко скомпрометувати : «12345», «abc123», «abcdef», «11111», «qwerty», «password» та подібні.

Користувачам заборонено:

– передавати пароль від облікових записів стороннім особам в будь-якому вигляді;

– залишати пароль у відкритому вигляді;

– використовувати один і той самий пароль для різних облікових записів.

Визначено положення про резервне копіювання.

Резервним копіюванням критично важливих файлів, налаштувань програмних застосунків та технічних засобів займається адміністратор системи.

Виконується процедура резервного копіювання наступних об'єктів:

– база даних програмного застосунку M.E.Doc;

– база даних програмного застосунку BAF;

– вміст каталогів спільного доступу користувачів домену;

– журнал реєстрації подій безпеки контролеру домену;

– налаштування маршрутизатора.

Резервні копії баз даних та вмісту каталогів спільного доступу користувачів виконується щотижня, зберігаються 30 днів.

Резервні копії журналу реєстрації подій виконуються кожні 12 годин, зберігаються 7 днів.

Резервна копія налаштувань маршрутизатора виконується після внесення змін конкретних налаштувань, попередня версія видаляється.

Всі резервні копії зберігаються на сервері 4.

Визначено положення про безпеку серверів.

Сервери розміщені у кабінеті адміністратора, в серверній шафі. Серверна шафа закрита на ключ, ключ є лише у адміністратора.

Право на доступу до кімнати та знаходження у ній без нагляду має лише системний адміністратор.

Заборонено перебувати стороннім особам у приміщені, де розташовані сервери.

Фізичний доступ до апаратної частини серверів має лише адміністратор. Доступ надається при проведенні профілактичних робіт, ремонту або заміні комплектуючих.

Логічний доступ до серверів являє собою віддалений доступ під особистим обліковим записом з робочого місця користувача.

Логічний доступ системного адміністратора виконується за локальним обліковим записом для налаштування ролі Active Directory на сервері 3, налаштування домену з підключенням всіх інших серверів до домену.

Логічний доступ системного адміністратора виконується за локальним обліковим записом домену для налаштування всіх облікових записів користувачів та пристроїв з відповідними правами доступу.

Логічний доступ користувачів виконується за локальним обліковим записом домену.

За контроль безпеки серверів відповідає адміністратор домену. Безпека серверів забезпечена за рахунок проведення наступних робіт:

– оновлення програмних засобів та антивірусних баз до останніх версій;

– вчасне усунення несправностей;

– регулярний аналіз журналу реєстрації подій безпеки на наявність подій, що мають критичне значення для безпеки системи;

– дотримання положень про резервне копіювання об’єктів.

Визначена необхідність введення нової ролі в системі – адміністратора безпеки.

Адміністратор системи має надлишкові права доступу до об'єктів ІКС. Необхідно виконати розподіл обов'язків адміністратора системи шляхом виділення облікового запису адміністратора безпеки.

Для забезпечення виділення адміністратора безпеки необхідно залучити спеціаліста з інформаційної безпеки, що буде виконувати обов'язки адміністратора безпеки, та встановити обмеження на права доступу до системи та об'єктів ІКС адміністратора системи.

Згідно з визначеними правами доступу адміністратора системи необхідно виконати заборону на модифікацію журналу реєстрації подій безпеки. Основними обов’язками адміністратора системи є:

– налашутвання служби домену Active Directory;

– підтримка цілісності системи;

– інсталяція необхідного програмного забезпечення;

– створення та налаштування облікових записів з відповідним розмежування доступу;

– виконання резервного копіювання.

Основним обов’язком адміністратора безпеки є контроль за дотриманням правил доступу до ІзОД шляхом:

– контролю встановлених прав доступу;

– управління правилами аудиту подій;

– аналізу зареєстрованих подій.

Однією з найбільш критичних загроз для системи є впровадження правил розмежування доступу до об'єктів адміністратором системи за відсутності контролю над цими подіями. За контролем подій, пов'язаних зі зміною прав доступу до об'єктів системи, відповідає адміністратор безпеки. Впровадження відповідного рівня контролю за цими подіями та швидке реагування на можливу загрозу виконується за рахунок програмного застосунку «Netwrix Auditor».

За допомогою «Netwrix Auditor» адміністратор системи впроваджує аудит за будь-якими критичними змінами, налаштувавши відправку сповіщень зі звітуванням про подію.

Згідно з проведеним аналізом реалізації вимог безпеки було визначено надлишковість матриці розмежування доступ та відсутність необхідних ролей, відображених в таблиці 1.4.

Оновлена матриця розмежування доступу представлена в таблиці 2.2.

Таблиця 2.2 – Оновлена матриця розмежування доступу

| Користувач | Кількість працівників | Інформація | | | | | | | | | | Ресурси |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
| Адміністратор системи | 1 | ЧЗ В I/E | ЧЗ В I/E | ЧЗ В I/E | ЧЗ В I/E | ЧЗ В I/E | ЧЗ В | ЧЗ В | Ч | ЧЗ В I/E | - | Всі ресурси |
| Адміністратор безпеки | 1 | - | - | - | - | - | Ч | ЧЗ В | - | - | - | Сервер 3 |

Продовження таблиці 2.2

| Користувач | Кількість працівників | Інформація | | | | | | | | | | Ресурси |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
| Директор | 1 | Ч | Ч | - | Ч | Ч | Ч | - | ЧЗ ВД | ЧЗ Д I/E | ЧВ Д | ПК 1, Інтернет, БФП 1 |
| Секретар | 1 | - | Ч I/E | - | - | - | Ч | - | ЧЗ, В | - | ЧВ Д | ПК 7, Інтернет, БФП 2 |
| Конструктор | 4 | - | - | ЧЗ В Д I/E | - | - | Ч | - | Ч | - | - | ПК 3-6, Інтернет, БФП 4 |
| Менеджер | 3 | ЧЗ Д I/E | - | - | - | - | Ч | - | Ч | - | ЧЗ ВД | Ноутбук 1-3, Інтернет, БФП 5 |
| Бухгалтер | 3 | ЧЗ Д I/E | ЧЗ В Д I/E | - | ЧЗ В I/E | ЧЗ В I/E | Ч | - | Ч | Ч I/E | - | ПК 8-10, Інтернет, БФП 3 |

2.2.2 Групова політика контролеру домену Active Directory

В домені Active Directory застосована групова політика для керуванням доступу користувачів до об’єктів та ведення аудиту подій.

Опис налаштування групової політики користувачів наведено нижче.

Політика акаунту. Визначається політика паролів, політика використання Kerberos при аутентифікації.

Параметри політики паролів:

– термін дії паролю 90 днів;

– мінімальна довжина паролю 12 символів, максимальна – 24 символи;

– пароль повинен містити: латинські символи верхнього та нижнього регістру, цифри від 0 до 9, спеціальні символи (! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _` { | } ~);

– пароль зберігається в зашифрованому вигляді;

Локальна політика. Визначається політика аудиту, політика використання зовнішніх носіїв, призначення прав доступу, налаштування робочого столу.

До політики аудиту входить:

– аудит успішного/невдалого входу до системи;

– аудит виходу з системи;

– аудит невдалої спроби доступу до об'єкта;

– аудит використання дозволу на об'єкт (читання, запис)

– аудит зміни дозволу доступу до об'єкта;

– аудит зміни паролю користувачем;

– аудит видалення об'єкту;

– аудит створення нового облікового запису користувача домену;

– аудит видалення облікового запису користувача домену;

– аудит виникнення помилки в роботі додатку або системи;

– аудит виникнення попередження про проблеми з апаратним забезпеченням, програмним забезпеченням, драйверами, недостатність пам'яті для роботи додатка;

– аудит змін у політиці безпеки;

– аудит використання зовнішніх пристроїв.

Політика використання зовнішніх носіїв. Кожний облікований носій інформації має свій ідентифікаційний номер. Адміністратор системи через «Диспетчер пристроїв» отримує унікальний ідентифікатор носія. В налаштуваннях групової політики «Обмеження встановлення пристрою» вносить облікові носії у параметр «Дозволити встановлення пристроїв, які відповідають будь-якому з цих ідентифікаторів пристрою». Для заборони на

використання сторонніх носіїв встановлюється параметр «Запобігання встановленню пристроїв, не описаних іншими налаштуваннями політики».

В журналі реєстрації відображено наступні події використання зовнішніх носіїв:

– підключення зовнішнього носія до пристрою;

– вдала спроба копіювання інформації на зовнішній носії;

– невдала спроба копіювання інформації на зовнішній носії;

– видалення інформації з зовнішнього носія;

– запис інформації на зовнішні носії

– відключення зовнішнього носія.

Призначення прав доступу має наступні налаштування:

– резервне копіювання файлів і каталогів: адміністратор;

– відновлення файлів і каталогів: адміністратор;

– виконання задач по обслуговуванні томів: адміністратор;

– доступ до комп'ютеру з мережі: користувачі, адміністратор;

– завершення роботи системи: користувачі, адміністратор;

– завантаження драйверів системи: адміністратор;

– локальний вхід в систему: адміністратор;

– заборона локального входу в систему: користувачі.

Налаштування робочого столу полягає в:

– встановлення параметрів робочого столу, такі як розширення екрану, розмір іконок програм, панелі задач;

– заборона доступу до засобів адміністрування Windows (редактору реєстру, монітору ресурсів, монітору брандмауеру захисника Windows та інші);

– дозвіл на виконання лише тих програм, що внесені до списку дозволених;

– заборона на встановлення програмних застосунків.

### 2.2.3 Залучення RAID-масивів жорстких дисків

Для забезпечення стійкості роботи системи при відмові внутрішніх технічних засобів обробки інформації, жорстких дисків, вирішено забезпечити використання RAID-масивів жорстких дисків на серверах.

На підприємстві працюють чотири сервери:

– на сервері 1 встановлений M.E.Doc Server з базою даних для подання бухгалтерської електронної звітності;

– на сервері 2 встановлений BAF Server з базою даних для ведення торгівлі та бухгалтерської звітності;

– на сервері 3 встановлена служба домену Active Directory підприємства;

– на сервері 4 зберігаються резервні копії файлового сховища всіх серверів.

Використання RAID-масив жорстких дисків виконується для усіх серверів, окрім «Back-Up» серверу 4.

Необхідно обрати, RAID-масиву якого рівня доцільно буде використовувати.

Розглянемо принцип роботи кожного з масивів.

RAID 0. Дані розділяються на блоки та записуються по черзі на кожний диск масиву. Якщо один з дисків масиву вийде з ладу – відновити дані неможливо.

RAID 1. Дані дублюються з диску одного масиву на інший. Відновлення даних при виході з ладу одного з дисків можливе.

RAID 5. Кожний файл розподіляється на блоки, кількість яких дорівнює (n-1) кількості жорстких дисків, записуються почергово на кожний з цих дисків. Розраховується парність блоків цих блоків (операція XOR) та записується на останній жорсткий диск. Така послідовність подій повторюється для кожного рядка файлу. Щоб уникнути того, що парність зберігалася лише на одному жорсткому диску, парність записується на інший диск по циклічному принципу. Якщо один з дисків масиву вийде з ладу, то відновити дані можливо, але зі зменшенням продуктивності роботи масиву.

RAID 6. Кожний файл розподіляється на блоки, кількість яких дорівнює (n-2) кількості жорстких дисків, записуються почергово на кожний з цих дисків. Розраховується парність блоків цих блоків (операція XOR) та записується на один із незадіяних жорстких дисків. Далі розраховується парність тих самих блоків з використанням іншого методу – з урахуванням кодів Ріда – Соломона.

Така послідовність подій повторюється для кожного рядка файлу. Щоб уникнути того, що парність зберігалася лише на одному жорсткому диску, парність записується на інший диск по циклічному принципу. Якщо один з дисків масиву вийде з ладу, то відновити дані можливо, але зі зменшенням продуктивності роботи масиву.

RAID 10. Поєднання масивів системи RAID 0 та RAID 1. Дані розділяються на блоки та записуються по черзі на кожний диск масиву, утворюється RAID 0. Ця пара дисків клонується на іншу пару дисків і отримуємо масив RAID 1.

RAID 01. Поєднання масивів системи RAID 1 та RAID 0. Дані розділені на блоки. Один блок даних записується на два диски (отримаємо RAID 1), а другий блок даних записується на інші два диски. Отримаємо масив RAID 0 з масивів дисків RAID 1.

Порівняльна характеристика типів RAID-масивів наведено в таблиці 2.3. Дані для створення порівняльної таблиці взяті зі статті «Типи RAID-масивів: просте пояснення особливостей, переваг та недоліків» [10].

В результаті аналізу характеристик систем RAID-масивів та принципів їх дії, було вирішено використовувати систему RAID 1 масивів жорстких дисків, оскільки ця система забезпечує достатньо високий рівень продуктивності запису та зчитування даних, потребує залучення мінімально 2 дисків та забезпечує цілісність даних та стійкість всієї системи в разі відмови одного з жорстких дисків.

Для забезпечення роботи масиву жорстких дисків необхідно обрати RAID-контролер для залучення до серверу. Сумісний з серверами HP ProLiant DL380 Gen10 є RAID-контролер HP Smart Array P408i-A SR Sas Modular Controller. Такий контролер забезпечує підключення 8 внутрішніх накопичувачів з SATA інтерфейсом, підтримує рівні RAID 0, 1, 5, 6, 10, 50, 60.

На серверах встановлені жорсткі диски DELL об'ємом в 2TB з підтримкою інтерфейсу SATA. На кожному сервері по дві штуки. Відповідно, для залучення RAID-масиву жорстких дисків на серверах необхідно придбати перелік обладнання, відображеного в таблиці 2.4.

Таблиця 2.3 - Порівняльна характеристика рівнів RAID-масивів

| Рівень | Мінімальна кількість дисків | Максимальна кількість дисків | Продуктивність читання | Продуктивність запису | Надмірність | Використання ємності диска |
|---|---|---|---|---|---|---|
| RAID 0 «Чергування» | 2 | 16 | Висока | Вище середнього | - | 100% |
| RAID 1 «Віддзеркалювання» | 2 | 3 | Вище середнього | Вище середнього | + | 50% |
| RAID 5 «Чергування з розподіленою парністю» | 3 | 16 | Висока | Середня | + | 67-94% |
| RAID 6 «Чергування з подвійною парністю» | 4 | 16 | Висока | Середня | + | 50-88% |
| RAID 01 | 4 | 16 | Вище середнього | Вище середнього | + | 50% |
| RAID 10 | 4 | 16 | Вище середнього | Вище середнього | + | 50% |

Таблиця 2.4 – Перелік обладнання, необхідного для залучення RAID-масиву жорстких дисків

| Тип товару | Найменування товару | Одиниця виміру | Кількість | Ціна за одиницю, грн |
|---|---|---|---|---|
| RAID-контролер | HP Smart Array P408i-A SR Sas Modular Controller | шт | 3 | 8163 |
| Жорсткий диск для серверу | DELL 2TB 7.2K RPM SATA 6GBPS 512N | шт | 6 | 8069 |

2.2.4 Заходи із реалізації послуг безпеки

КО-1. Повторне використання об’єктів

Необхідно реалізувати механізм, що буде після завершення деякого процесу очищує дані пам’яті, виділеної на даний процес.

Для реалізації даної послуги необхідно автоматизувати процес очистки даних виділеної пам’яті після завершення деякого процесу.

В результаті аналізу програмних застосунків, що очищують дані оперативної пам’яті, наведених в таблиці 2.5, було прийняте рішення використовувати Mem Reduct для забезпечення очищення пам’яті, тому що цей продукт налаштувати які саме компоненти пам’яті необхідно очистити та надає змогу виконати це і вручну, і автоматично через встановлений проміжок часу.

Адміністратор системи повинен завантажити утиліту під назвою Mem Reduct, що застосовується для очистки даних оперативної пам'яті. За допомогою вбудованої служби Windows 10 «Планувальник задач» створити задачу: за умови завершення обробки інформації з використанням програмним забезпечення (закриття програми) виконувався запуск програми по очищенню даних оперативної пам’яті.

Таблиця 2.5 – Порівняння характеристика ПЗ для очищення оперативної пам’яті

| Назва | Ліцензія | Підтримка ОС | Методи очищення пам’яті | Основні характеристики |
|---|---|---|---|---|
| CleanMem | Безкоштовне | Windows 10, 8, 7 XP | Автоматичне (кожні 15 хвилин) | Відображається:<br>- об’єм використаної пам’яті системою;<br>- кількість активних процесів. |
| Mem Reduct | Безкоштовне | Windows 11, 10, 8.1, 8, 7 | Ручне та автоматичне | Відображається об’єм використання:<br>- фізичної пам’яті<br>- файлів підкачки<br>- системного кешу<br>Виконує порівняння об’єму пам’яті до та після очищення<br>Можливість налаштувати пам’яті для очищення |
| Memory Cleaner | Безкоштовне | Windows 10, 8.1, 8, 7, XP | Ручне та автоматичне (при перевищені заданого рівня використання пам’яті) | Відображається об’єм використання:<br>- фізичної пам’яті<br>- віртуальної пам’яті<br>Використовуються вбудовані функції Windows для очищення пам’яті |

КВ-2. Базова конфіденційність при обміні

Реалізація даної послуги визначається положеннями про використання зовнішніх носіїв інформації, де вказано, що всі облікові носії інформації є зашифрованими

Реалізація даної послуги визначається положеннями про використання зовнішніх носіїв інформації, де вказано, що всі обліковані носії інформації є зашифрованими.

Характеристика програмних застосунків, що виконують шифрування носіїв інформації, наведених в таблиці 2.6.

Для виконання шифрування облікованих зовнішніх носіїв інформації обрано програмний застосунок VeraCrypt, оскільки лише в цьому застосунку є вбудована можливість перевірки цілісності даних на носії шляхом розрахунку хеш-суми файлів.

Адміністратор системи за допомогою програмного застосунку VeraCrypt забезпечує шифрування зовнішніх носіїв при видачі їх співробітникам підприємства для використання. При втраті зовнішнього носія збережеться конфіденційність ІзОД.

Таблиця 2.6 – Порівняльна характеристика програмних застосунків для шифрування носіїв інформації

| Назва ПЗ | Ліцензія | Функціональні можливості (Шифрування) | Алгоритми шифрування | Використання хешування |
|---|---|---|---|---|
| VeraCrypt | Безкоштовне | - Створення зашифрованих томів<br>- Шифрування розділу<br>- Шифрування цілого диску | - AES-256<br>- Serpent<br>- Twofish | - Генерація ключів<br>- Перевірка цілісності даних на носії |

Продовження таблиці 2.6

| Назва ПЗ | Ліцензія | Функціональні можливості (Шифрування) | Алгоритми шифрування | Використання хешування |
|---|---|---|---|---|
| DiskCryptor | Безкоштовне | - Шифрування розділу диску<br>- Шифрування цілого диску | - AES-256<br>- Serpent<br>- Twofish | Генерація ключів |
| Cryptomator | Безкоштовне | Створення зашифрованих томів на:<br>- локальних дисках<br>- хмарних середовищах | - AES-256 | Перевірка цілісності даних на хмарних середовищах |

ЦВ-2. Базова цілісність при обміні

Реалізація даної послуги визначається положеннями про використання зовнішніх носіїв інформації, де вказано, що всі обліковані носії інформації є зашифрованими. При шифруванні зовнішніх носіїв програмним застосунком VeraCrypt вбудована функція розрахунку хеш-суми файлів, що забезпечує цілісність даних.

ДС-1. Стійкість при обмежених відмовах

Забезпечення доступності системи при відмові жорстких дисків на серверах реалізовано за рахунок впровадження RAID-масивів жорстких дисків.

Для забезпечення доступності системи при відмові маршрутизатора, а саме доступу до даних, що розміщені на серверах, необхідно адміністратору системи підв'язати всі об'єкти локальної мережі підприємства (комп'ютери, ноутбуки, сервери) за статичною IP-адресою до мережі. Таким чином всі об'єкти локальної мережі зможуть обмінюватись інформацією між собою за відмови маршрутизатора, але без доступу до Інтернету.

В такому стані об'єкти локальної мережі можуть працювати, допоки адміністратор не замінить маршрутизатор. Для пришвидшення налаштування

нового маршрутизатора під мережу підприємства, адміністратор системи, відповідно до положення про резервне копіювання, може використовувати резервну копію налаштувань всієї мережі.

ДЗ-2. Обмежена гаряча заміна

Можливість заміни компонентів КС, а саме жорстких дисків на сервері, без переривання обслуговування реалізована завдяки залученню RAID-масивів жорстких дисків.

ДВ-1. Ручне відновлення

У разі збоїв програмного забезпечення, а саме програм ведення бухгалтерського обліку та подання електронної звітності BAF та M.E.Doc, реалізоване ручне відновлення програмних застосунків шляхом їх повторної інсталяції з використанням резервної копії бази даних з відповідними налаштуваннями.

НО-2. Розмежування прав доступу

В відповідності до положення про необхідність введення нової ролі в системі – адміністратора безпеки, наведеному в пункті 2.2.1, в домені Active Directory визначено дві ролі адміністратора – адміністратор системи та адміністратор безпеки.

## 2.3 Висновок

При реалізації запропонованих заходів і наведених положень політики безпеки буде реалізований заданий профіль захищеності ІКС підприємства. Буде забезпечено необхідний рівень захисту інформації, що обробляється в цій системі.

Таблиця 2.7 – Реалізації послуг безпеки при впроваджені запропонованих проектних робіт

| Критерії | Вимоги до рівнів послуги безпеки | Реалізація послуг безпеки |
|---|---|---|
| Конфіденційності | КД-2. Базова довірча конфіденційність | Реалізовано |
| | | |

Продовження таблиці 2.7

| Критерії | Вимоги до рівнів послуги безпеки | Реалізація послуг безпеки |
|---|---|---|
| Конфіденційності | КА-2. Базова адміністративна конфіденційність | Реалізовано |
| | КО-1. Повторне використання об’єктів | Реалізовано |
| | КВ-2. Базова конфіденційність при обміні | Реалізовано |
| Цілісності | ЦД-1. Мінімальна довірча цілісність | Реалізовано |
| | ЦА-2. Базова адміністративна цілісність | Реалізовано |
| | ЦО-1. Обмежений відкат | Реалізовано |
| | ЦВ-2. Базова цілісність при обміні | Реалізован |
| Доступності | ДР-1. Квоти | Реалізовано |
| | ДС-1. Стійкість при обмежених відмовах | Реалізовано |
| | ДЗ-2. Обмежена гаряча заміна | Реалізовано |
| | ДВ-1. Ручне відновлення | Реалізовано |
| Спостереженості | НР-2. Захищений журнал | Реалізовано |
| | НИ-2. Одиночна ідентифікація і аутентифікація | Реалізовано |
| | НК-1. Однонаправлений достовірний канал | Реалізовано |
| | НО-2. Розподіл обов’язків адміністратора | Реалізовано |
| | НЦ-2. КЗЗ з гарантованою цілісністю | Реалізовано |
| | НТ-2. Самотестування при старті | Реалізовано |
| | НВ-1. Автентифікація вузла | Реалізовано |

# РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу є техніко-економічне обґрунтування доцільності запровадження запропонованих в проекті організаційних, технічних та криптографічних рішень щодо впровадження КСЗІ в ІКС підприємства «Мередіан».

Виконання техніко-економічного обґрунтування доцільності проектування складається з:

1. Розрахунку капітальних витрат на впровадження КСЗІ;
2. Розрахунку річних експлуатаційних витрат утримання та обслуговування КСЗІ;
3. Визначення річного економічного ефекту від впровадження КСЗІ;
4. Визначення та аналіз показників економічної ефективності запропонованих проектних рішень;
5. Висновку про економічну доцільність проектного рішення.

## 3.1 Розрахунок (фіксованих) капітальних витрат

Фіксовані (капітальні) витрати здійснюються на етапі створення КСЗІ. Перелік впроваджених проектних рішень наведено в таблиці 3.1

Таблиця 3.1 – Проектні рішення щодо впровадження КСЗІ на підприємстві

| Найменування | Опис рішення | Витрати, грн |
|---|---|---|
| Елементи політики безпеки | Впровадження положень на підприємстві, оновлення матриці розмежування доступу | Безкоштовно |
| | Розподіл обов'язків адміністратора системи та виділення адміністратора безпеки | Заробітна плата |
| Групова політика контролеру домену Active Directory | Застосування групової політики для керування доступу користувачів до об'єктів системи та ведення аудиту подій | Безкоштовно |

Продовження таблиці 3.1

| | | |
|---|---|---|
| Залучення RAID-масивів жорстких дисків | Закупівля RAID-контролерів та додаткових жорстких дисків на серверах | 72 903 |
| Заходи із реалізації послуг безпеки | Впровадження використання сторонніх програмних застосунків | Безкоштовно |
| | Налаштування локальної мережі | Безкоштовно |

3.1.1 Визначення трудомісткості розробки КСЗІ

Трудомісткість розробки КСЗІ визначається тривалістю кожної робочої операції:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин}, \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку КСЗІ;

$t_{тз}$ = 17 годин;

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

$t_{в}$ = 14 годин;

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

$t_{а}$ = 19 годин;

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

$t_{вз}$ = 10 годин;

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

$t_{озб}$= 17 годин;

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

$t_{овр}$= 15 годин;

$t_{д}$ – тривалість документального оформлення КСЗІ;

$t_{д}$= 11 годин.

$$t = 17 + 14 + 19 + 10 + 17 + 15 + 11 = 103 \text{ години}.$$

3.1.2 Розрахунок витрат на створення КСЗІ

Витрати на розробку КСЗІ $К_{рп}$ складають з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки КСЗІ $З_{мч}$:

$$К_{рп} = З_{зп}+З_{мч}, \text{ грн.} \quad (3.2)$$

Заробітна плата виконавця розробки розраховується за формулою:

$$З_{зп}= t \cdot З_{іб}, \text{ грн,} \quad (3.3)$$

де $t$ – загальна тривалість розробки КСЗІ, годин;

$t$ = 102 години;

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

Середньомісячна заробітна плата спеціаліста з інформаційної безпеки становить 25000 грн [11], всього в місяця 21 робочих днів по 8 годин, тому середньогодинна заробітна плата дорівнює:

$$З_{іб} = 25000/(21 \cdot 8) = 149 \text{ грн/годину.}$$

$$З_{зп} = 102 \cdot 149 = 15198 \text{ грн.}$$

Вартість машинного часу для розробки КСЗІ визначається за формулою:

$$З_{мч} = t \cdot С_{мч}, \text{ грн} \quad (3.4)$$

де $t$ – трудомісткість розробки КСЗІ на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн,} \quad (3.5)$$

де $P$ – встановлена потужність ПК, кВт;

$P$ = 0,5 кВт;

$t_{нал}$ - кількість задіяних робочих станцій;

$t_{нал}$ = 1;

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

$C_e$ = 4,32 грн/кВт · година;

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

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

$H_a$ = 1/5 = 0,2;

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

$H_{апз}$ = 1/2 = 0,5;

$К_{лпз}$ - вартість ліцензійного програмного забезпечення;

$F_p$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_p$ = 1920);

$F_p$ = 1920 годин;

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання. Первісна вартість ПК = 14366, мінімальний термін корисного використання – 5 років, термін використання ПК – 2,5 роки.

$$Ф_{зал} = 14366 – (14366 \cdot 2,5)/5 = 7183 \text{ грн.}$$

Вартість програмного забезпечення, залученого на етапі проектування, відображено в таблиці 3.2.

Таблиця 3.2 – Вартість ліцензійного програмного забезпечення

| Назва програмного забезпечення | Вартість, грн |
|---|---|
| Mem Reduct | Безкоштовно |
| VeraCrypt | Безкоштовно |

$К_{лпз}$ = 0 грн;

$$C_{мч} = 0{,}5 \cdot 1 \cdot 4{,}32 + \frac{7183 \cdot 0{,}2}{1920} + \frac{0 \cdot 0{,}2}{1920} = 2{,}91 \text{ грн.}$$

$$З_{мч} = 102 \cdot 2{,}91 = 296{,}8 \text{ грн.}$$

$$К_{рп} = 15198 + 296{,}8 = 15494{,}8 \text{ грн.}$$

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта КСЗІ складають:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}, \quad (3.6)$$

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

Для розробки проекту інформаційної безпеки підприємства був залучений зовнішній консультант з питань аудиту безпеки. Вартість однієї години консультації – 1,2 тис. грн. Загальний час, який було відведено на консультації – 11 годин.

$К_{пр} = 1200 \cdot 11 = 13{,}2$ тис. грн;

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

$К_{зпз} = 0$ тис. грн;

$К_{рп}$ – вартість розробки КСЗІ;

$К_{рп} = 15{,}549$ тис. грн;

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

$К_{аз} = 72{,}903$ тис. грн;

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

Для навчання адміністратора системи придбали курс на платформі Udemy під назвою «Адміністрування Windows Server та Active Directory», ціна курсу – 2 тис. грн. Весь персонал підприємства повинен пройти безкоштовний курс на платформі Coursera з питань безпеки в ІТ.

$К_{навч} = 2$ тис. грн;

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

Для встановлення системи RAID-масивів жорстких дисків на підприємстві був залучений технічний спеціаліст з відповідним рівнем кваліфікації. Вартість однієї години роботи спеціаліста – 2,5 тис. грн. Загальний час, який було відведено на технічні роботи – 6 годин. Налагодженням системи інформаційної безпеки, а саме розмежуванням доступу в домені Active Directory, займався адміністратор безпеки. Середньомісячна заробітна плата адміністратора безпеки на підприємстві становить 28 тис. грн. Відповідно середньогодинна заробітна плата буде дорівнювати 28000/(21 · 8) = 167 грн/година. Загальний час, витрачений на налагодженням системи інформаційної безпеки – 5 годин.

$$К_н = 2500 \cdot 6 + 167 \cdot 5 = 15{,}835 \text{ тис. грн.}$$

Згідно з формулою (3.6) капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта КСЗІ складають:

$$К = 13{,}2 + 0 + 15{,}549 + 72{,}903 + 2 + 15{,}835 = 119{,}487 \text{ тис. грн.}$$

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційними втратами є поточні витрати на експлуатацію та обслуговування об’єкта проектування за визначений період (рік), що виражені у грошовій формі. До поточних (експлуатаційних) витрат відносяться:

– вартість відновлення і модернізації системи ($С_в$);

– витрати на керування системою в цілому ($С_к$);

– витрати, викликані активністю користувачів системи ($С_{ак}$ – “активність користувача”);

Річні поточні (експлуатаційні) витрати на обслуговування КСЗІ визначимо за формулою:

$$С = С_в + С_к + С_{ак}, \text{ тис. грн.} \qquad (3.7)$$

3.2.1 Розрахунок вартості відновлення і модернізації системи

В період експлуатації виконується підтримка всієї системи шляхом регулярного оновлення ліцензійного програмного забезпечення. У вартість ліцензійного ПЗ входить підтримка модернізації продукту до нових версій.

$C_в$ = 0 тис. грн.

3.2.2 Розрахунок витрат на керування системи

Витрати на керування КСЗІ розраховуються за формулою:

$$C_к = C_н + C_а + C_з + C_{єв} + C_{ел} + C_о + C_{тос}, \text{ грн.} \quad (3.8)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів ($C_н$) включають в себе проведення одноденних тренінгів персоналу 2 рази на рік, вартість одного становить 12000 грн.

$C_н$ = 24000 грн.

Річний фонд амортизації відрахувань ($C_а$) визначається від суми капітальних інвестицій за видами основних фондів і нематеріальних активів. При залученні RAID-масиву жорстких дисків в систему річний фонд амортизації відрахувань складає:

$C_а$ = 72903/5 = 14580,6 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує КСЗІ ($C_з$), розраховується за формулою:

$$C_з = З_{осн} + З_{дод}, \text{ грн,} \quad (3.9)$$

де $З_{осн}$, $З_{дод}$ – основна та додаткова заробітна плата відповідно, грн на рік.

Виконання робіт з обслуговування КСЗІ вимагає залучення спеціаліста з інформаційної безпеки. Директор підприємства прийняв рішення найняти спеціаліста на 0,25 ставки. Місячний посадовий оклад – 20000 грн, додатковий оклад становить 10 % основної заробітної плати.

$$З_{осн} = 20000 \cdot 0{,}25 \cdot 12 = 60000 \text{ грн.}$$

$$З_{дод} = 60000 \cdot 0,1 = 6000 \text{ грн.}$$

$$С_з = 60000 + 6000 = 66000 \text{ грн.}$$

На 2024 рік єдиний соціальний внесок (ЄСВ) становить 22% [12].

$$С_{єв} = 66000 \cdot 0,22 = 14\ 520 \text{ грн.}$$

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

$$С_{ел} = P \cdot F_р \cdot Ц_е, \text{ грн,} \qquad (3.10)$$

де $P$ – встановлена потужність апаратури КСЗІ, кВт;

$P = 0,5$ кВт;

$F_р$ – річний фонд робочого часу КСЗІ, годин;

$F_р = 1920$ годин;

$Ц_е$ – тариф на електроенергію, грн/кВт · годин;

$Ц_е = 4,32$ грн/кВт · годин.

$С_{ел} = 0,5 \cdot 1920 \cdot 4,32 = 4147,2$ грн.

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) відсутні.

$С_о = 0$.

Витрати на технічне й організаційне адміністрування та сервіс КСЗІ ($С_{тос}$) складають 2% від вартості капітальних витрат.

$$С_{тос} = К \cdot 0,02 = 119487 \cdot 0,02 = 2389,7 \text{ грн.}$$

Відповідно до формули (3.8), витрати на керування КСЗІ становлять:

$$С_к = 24000 + 14580,6 + 59400 + 14520 + 4147,2 + 2389,7 = 119037,5 \text{ грн.}$$

### 3.2.3 Розрахунок вартості витрат, викликаних активністю користувача КСЗІ

Витрати, викликані активністю користувача КСЗІ ($С_{ак}$) визначаємо з відповідністю до вагових часток статей витрат у сукупній вартості КСЗІ. Підстаття, що буде використовуватися в розрахунках, називається futz-фактор.

Цей параметр визначає обсяг витрат, пов'язаних з наслідками некомпетентних дій користувачів. Вагова частка становить 30% від сукупній вартості КСЗІ.

$$C_{ак} = 119487 \cdot 0,3 = 35846,1 \text{ грн.}$$

Відповідно до формули (3.7), річні поточні (експлуатаційні) витрати на обслуговування КСЗІ становлять:

$$C = 119,037 + 35,846 = 154,883 \text{ тис. грн.}$$

3.3 Оцінки можливого збитку у разі реалізації загрози

Метою даної оцінки є визначення обсягу матеріальних витрат виходячи з імовірності виникнення загрози й можливих економічних витрат від її реалізації.

3.3.1 Оцінка величини збитку

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі визначається за формулою:

$$U = П_п + П_в + V, \tag{3.11}$$

де $П_П$ – оплачувані втрати робочого часу та простою співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_В$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурацій та ін.), грн;

$V$ – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі;

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

$$П_п = \frac{\sum З_с}{F} \cdot t_п, \tag{3.12}$$

де $З_с$ – заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі;

$F$ – місячний фонд робочого часу (при 40-а годинному робочому тижні $F$ = 176 годин);

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

$t_п$ = 4 години;

Заробітна плата всіх співробітників підприємства наведена в таблиці 3.4.

Таблиця 3.4 – Заробітна плата співробітників підприємства

| Посада | Кількість працівників | Місячна заробітна плата, грн | Єдиний соціальний внесок, грн | Місячна заробітна плата з урахуванням ЄСВ, грн |
|---|---|---|---|---|
| Адміністратор системи | 1 | 28000 | 6160 | 34160 |
| Адміністратор безпеки | 1 | 28000 | 6160 | 34160 |
| Директор | 1 | 30000 | 6600 | 36600 |
| Секретар | 1 | 17000 | 3740 | 20740 |
| Конструктор | 4 | 24000 | 5280 | 29280 |
| Менеджер | 3 | 23000 | 5060 | 28060 |
| Бухгалтер | 3 | 20000 | 4400 | 24400 |

$$\sum З_с = 34160 + 34160 + 36600 + 20740 + 29280 \cdot 4 + 28060 \cdot 3 + 24400 \cdot 3 =$$

$$= 400160 \text{ грн на місяць.}$$

Згідно формули (3.12) оплачувані втрати робочого часу та простою співробітників атакованого вузла або сегмента корпоративної мережі становлять:

$$П_п = \frac{400160}{176} \cdot 4 = 9094{,}5 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі визначаються за формулою:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.13),$$

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

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

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

$П_{зч}$ = 5000 грн.

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

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви}. \quad (3.14)$$

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

$t_{ви}$ = 3 години;

$$П_{ви} = \frac{400160}{176} \cdot 3 = 6820{,}9 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ розраховуються за наступною формулою:

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в, \quad (3.15)$$

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

$t_в$ = 3 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів).

Заробітна плата обслуговуючого персоналу системи складається з заробітної плати адміністратора системи (28000 грн на місяць, 34160 грн на місяць з урахуванням ЄСВ) та заробітної плати спеціаліста (20000 грн на ставці 0,25, що дорівнює 5000 грн, 6100 грн з урахуванням ЄСВ).

Згідно формули (3.15) витрати на відновлення вузла або сегмента корпоративної мережі становлять:

$$П_{пв} = \frac{34160 + 6100}{176} \cdot 3 = 686{,}3 \text{ грн.}$$

Відповідно до формули (3.13), витрати на відновлення працездатності вузла або сегмента корпоративної мережі становлять:

$$П_в = 6820{,}9 + 686{,}3 + 5000 = 12507{,}2 \text{ грн.}$$

Втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі ($V$) визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_r} \cdot (t_n \cdot t_в \cdot t_{ви}), \tag{3.16}$$

де $F_r$ – річний фонд часу роботи організації (52 робочих тижнів, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 годин.

$O$ – обсяг продажів атакованого вузла або сегмента корпоративної, грн у рік;

$O$ = 1100000 грн у рік.

$$\text{V} = \frac{1100000}{2080} \cdot (4 \cdot 3 \cdot 3) = 19038{,}5 \text{ грн.}$$

Відповідно до формули (3.11), упущена вигода від простою атакованого вузла або сегмента корпоративної мережі складає:

$$U = 9094{,}5 + 12507{,}2 + 19038{,}5 = 40640{,}2 \text{ грн.}$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі розраховуємо за формулою:

$$B = \sum_I \sum_N U, \tag{3.17}$$

де $I$ - число атакованих вузлів або сегментів корпоративної мережі;

$I$ = 4;

$N$ – середнє число атак на рік;

$N = 7$;

$$B = \sum_4 \sum_7 40640{,}2 = 1137{,}925 \text{ тис. грн.}$$

3.3.2 Загальний ефект від впровадження КСЗІ

Загальний ефект від впровадження КСЗІ ($E$) визначається з урахуванням ризиків порушення інформаційної безпеки і розраховується за формулою:

$$E = B \cdot R - C, \tag{3.18}$$

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

$R$ – очікувана ймовірність атаки на вузол або сегмент корпоративної мереж, частки одиниці;

$R = 0{,}4$;

$C$ – щорічні витрати на експлуатацію КСЗІ, тис. грн.

$E = 1137{,}925 \cdot 0{,}4 - 154{,}883 = 300{,}287$ тис. грн.

3.4 Визначення показників економічної ефективності КСЗІ

Для оцінки економічної ефективності необхідно визначити наступні показники:

– коефіцієнт повернення інвестицій *ROSI*;

– термін окупності капітальних інвестицій $T_o$.

Коефіцієнт повернення інвестицій *ROSI* показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження КСЗІ. Визначається за формулою:

$$ROSI = \frac{E}{K}, \text{ частки одиниці} \tag{3.19}$$

де $E$ – загальний ефект від впровадження КСЗІ, тис. грн;

$K$ – капітальні інвестиції на впровадження КСЗІ, тис. грн.

$$ROSI = \frac{300,287}{119,487} = 2,51 \text{ частки одиниці.}$$

Підприємство «Мередіан» здійснює фінансування капітальних інвестицій у КСЗІ за рахунок позикових коштів, тобто за рахунок банківського кредиту. Підприємство уклало угоду з Приват банком на отримання позикових коштів з процентною ставкою в 9% [13].

Проект вважається економічно доцільним, якщо розрахункове значення коефіцієнту повернення інвестицій *ROSI* перевищує величину банківської кредитної ставки з урахуванням інфляції:

$$ROSI > (N_{кр} - N_{інф})/100, \quad (3.20)$$

де $N_{кр}$ – банківська кредитна ставка, %;

$N_{кр} = 9\%$;

$N_{інф}$ – річний рівень інфляції, %;

$N_{інф} = 102\%$ [14].

Розрахункове значення коефіцієнту повернення інвестиції становить:

$$ROSI > (9-0,02)/100;$$

$$2,51 > 0,0898.$$

Проект є економічно доцільним.

Термін окупності капітальних інвестицій $T_o$ показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження КСЗІ, розраховується за формулою:

$$T_o = \frac{K}{E} = \frac{1}{ROSI}, \text{ років} \quad (3.21)$$

$T_o = 0,4$ роки.

3.5 Висновок до економічного розділу

В цьому розділі було виконано розрахунки наступні величин:

– капітальні витрати на впровадження КСЗІ ($K$ = 119,487 тис. грн.);

– річні експлуатаційні витрати на утримання та обслуговування КСЗІ ($C$ = 154,883 тис. грн);

– загальний збиток від атаки на вузол або сегмент корпоративної мережі ($B$ = 1137,925 тис. грн);

– загальний ефект від впровадження КСЗІ ($E$ = 300,287 тис. грн);

– термін окупності капітальний інвестицій ($T_o$ = 0,4 роки, приблизно 5 місяців).

# ВИСНОВКИ

У першому розділі кваліфікаційної роботи було проаналізовано необхідність створення комплексної системи захисту інформації в товаристві з обмеженою відповідальністю «Мередіан» та виконано обстеження середовищ функціонування підприємства. Проаналізовано модель загроз та модель порушника, на основі чого були визначені вимоги до функцій захисту інформації в інформаційно-комунікаційній системі підприємства.

У другому розділі кваліфікаційної роботи було проведено аналіз стану послуг безпеки інформації, згідно яких було запропоновано наступні проектні рішень щодо реалізації визначеного рівня захисту інформації: розроблено положення політики безпеки, змінено матрицю розмежування доступу до інформації в ІКС з впровадженням нових ролей, впроваджено залучення RAID-масивів жорстких дисків, запропоновані заходи з реалізації послуг безпеки.

У третьому розділі виконано обґрунтування економічної доцільності розробки, в результаті чого було розраховано: капітальні витрати на впровадження та обслуговування КСЗІ – 119,487 тис. грн, експлуатаційні витрати на впровадження та обслуговування КСЗІ – 154,883 тис. грн. В результаті оцінки можливого збитку у разі реалізації загрози визначено загальний збиток від атаки на вузол або сегмент корпоративної мережі – 1137,925 тис. грн. Загальний ефект від впровадження КСЗІ становить 300,287 тис. грн з терміном окупності капітальних інвестицій 4,8 місяців.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Про захисті інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 81/94-ВР, поточна редакція – від 28.06.2024 № 3783-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

2. Про інформацію: Закон України від 02.10.1992 №2658-XII, поточна редакція – від 27.07.2023 №3005-XI. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

3. Про захист персональних даних: Закон України від 01.06.2012 № 2297-VI, поточна редакція – від 27.04.2024 №3585-IX. URL: https://zakon.rada.gov.ua/laws/show/2297-17/ed20240427#Text.

4. Цивільний кодекс України від 16.01.2003 № 435-IV, поточна редакція – від 28.06.2024 № 3778-IX;

5. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» від 08.11.2005 №125 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

6. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» від 28.04.1999 №22. URL: https://tzi.ua/assets/files/1.1_003_99.pdf.

7. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» від 04.12.2000 №53 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf.

8. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» від 28.04.1999 №22. URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf.

9. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в

комп'ютерних системах від несанкціонованого доступу» від 28.04.1999 №22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf.

10. East Imperial Soft: стаття «Типи RAID-масивів: просте пояснення особливостей, переваг та недоліків» від 02.08.2022, останнє оновлення – 03.08.2022.URL: https://www.magicuneraser.com/ua/press/types_of_raid_arrays.php

11. Work.ua: статистика зарплат в Україні. URL: https://www.work.ua/salary-%D1%81%D0%BF%D0%B5%D1%86%D1%96%D0%B0%D0%BB%D1%96%D1%81%D1%82+%D0%B7+%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8/?count=by-resumes.

12. Мінфін: Єдиний соціальний внесок. URL: https://index.minfin.com.ua/ua/labour/social/.

13. Приват Банк: Фінансування та кредити для корпоративних клієнтів. URL: https://privatbank.ua/business/corporate/financing.

14. Мінфін: Індекс інфляції в Україні 2024. URL: https://index.minfin.com.ua/ua/economy/index/inflation/.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

| № | Формат | Найменування | Кількість листів | Примітка |
|---|---|---|---|---|
| 1 | А4 | Реферат | 2 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 2 | |
| 4 | А4 | Вступ | 1 | |
| 5 | А4 | 1 Розділ | 38 | |
| 6 | А4 | 2 Розділ | 27 | |
| 7 | А4 | 3 Розділ | 14 | |
| 8 | А4 | Висновки | 1 | |
| 9 | А4 | Перелік посилань | 2 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 2 | |
| 12 | А4 | Додаток В | 7 | |
| 13 | А4 | Додаток Г | 8 | |
| 14 | А4 | Додаток Д | 4 | |
| 15 | А4 | Додаток Е | 5 | |
| 16 | А4 | Додаток Є | 1 | |
| 17 | А4 | Додаток Ж | | |
| 18 | А4 | Додаток З | | |

# ДОДАТОК Б. Ситуаційний план ОІД

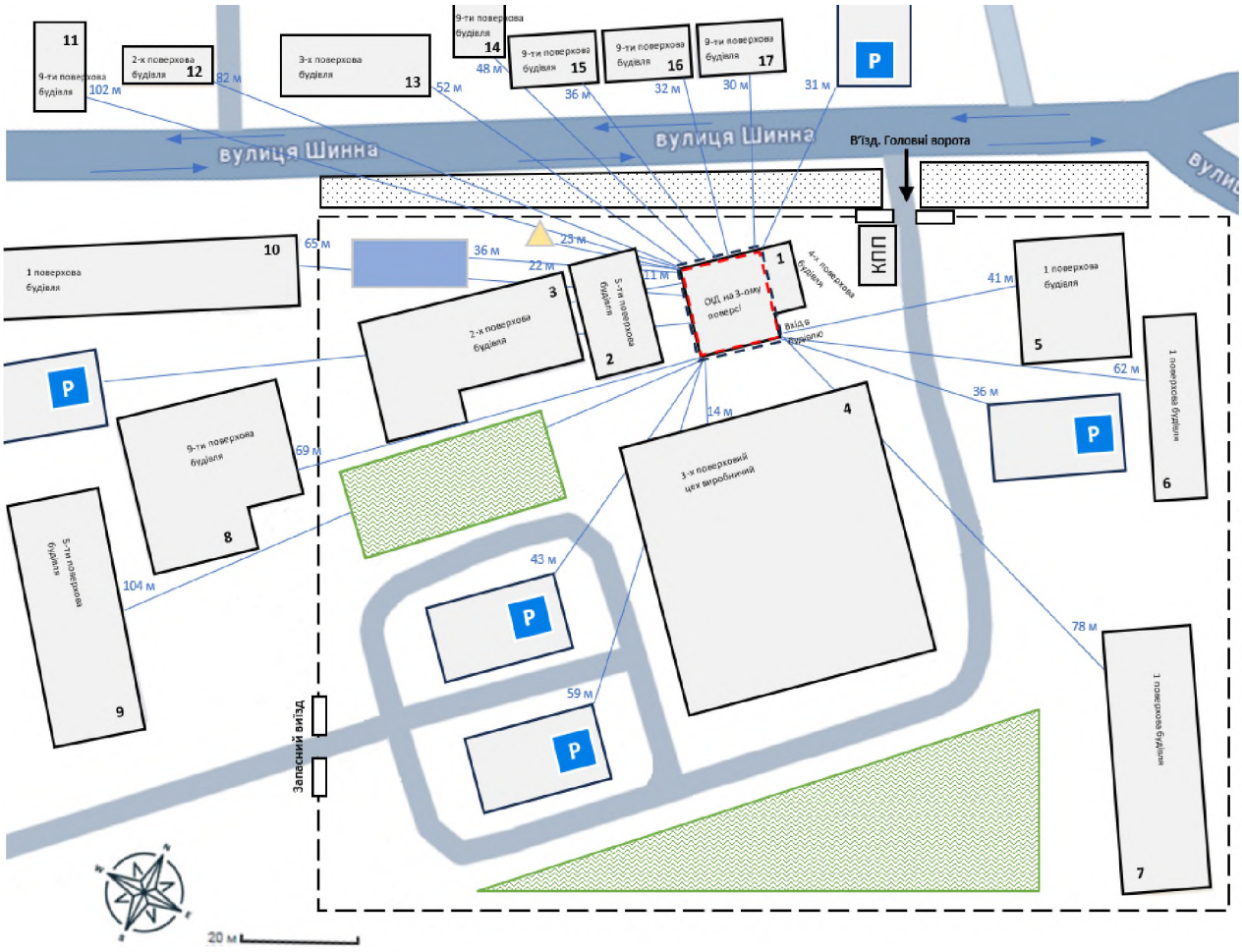


Рисунок Б.1 – Ситуаційний план ОІД

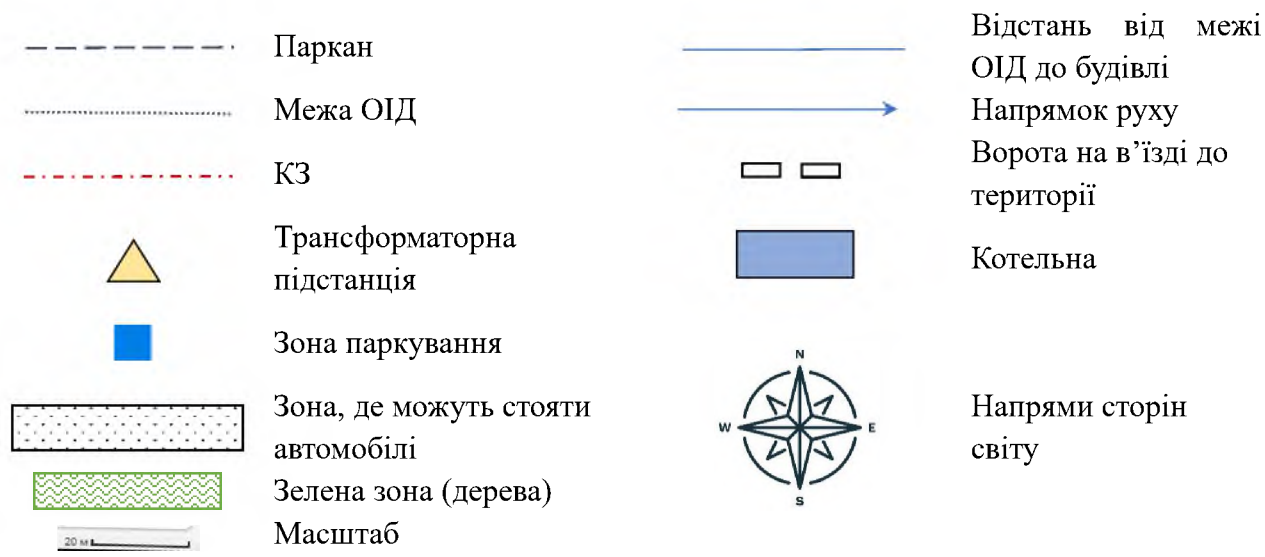


Рисунок Б.2 – Умовні позначення до ситуаційного плану ОІД

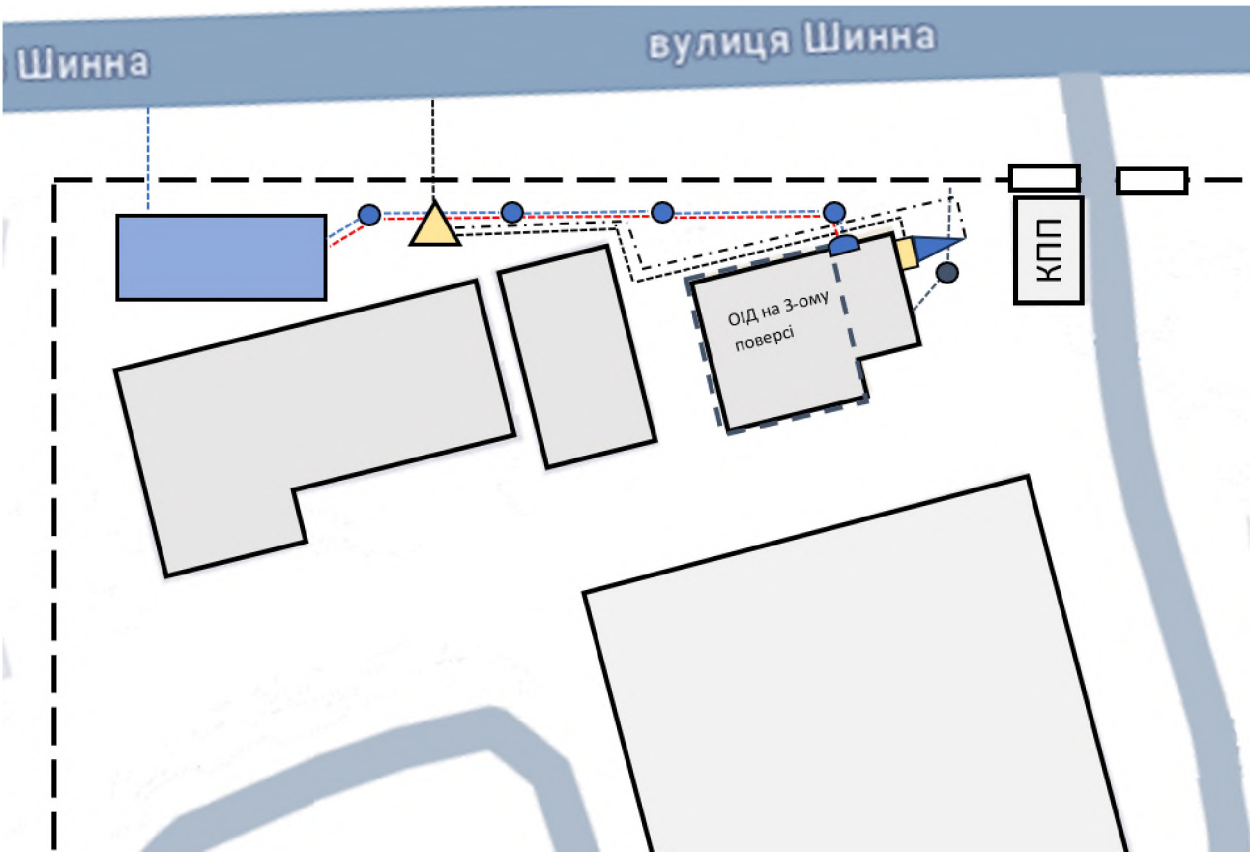


Рисунок Б.3 – Схема комунікацій на ситуаційному плані ОІД

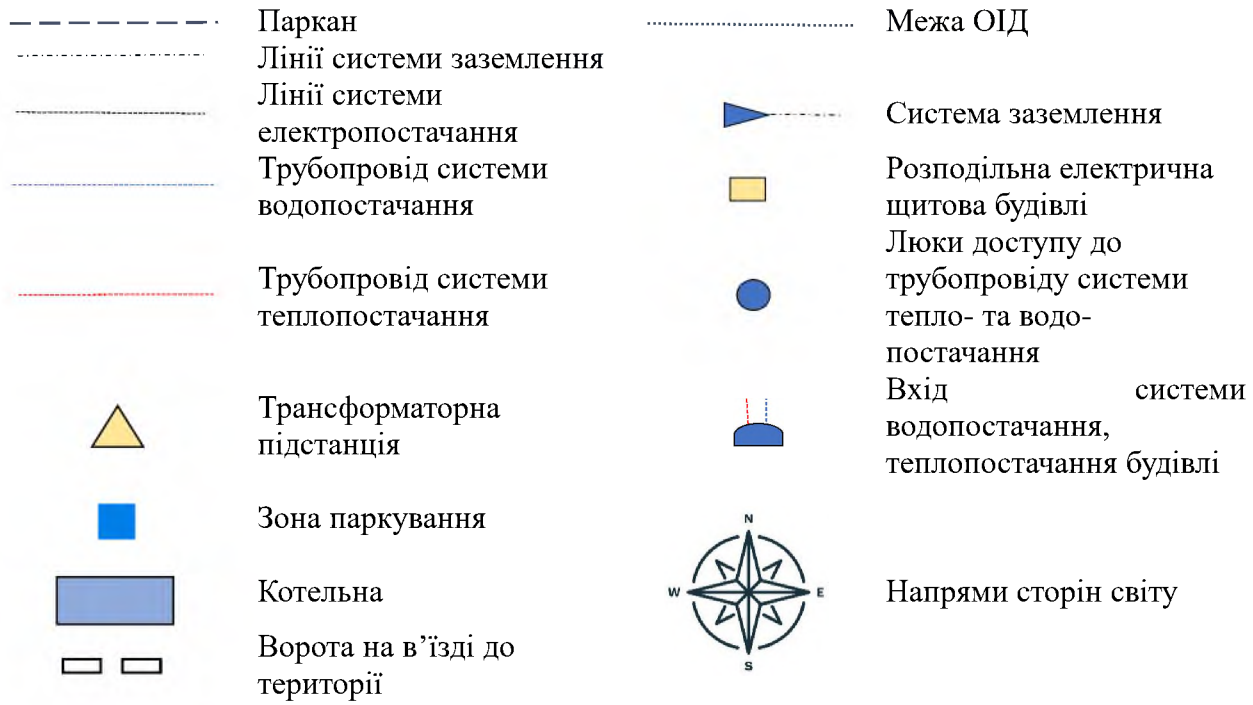


Рисунок Б.4 – Умовні позначення до схеми комунікацій на ситуаційному плані ОІД

# ДОДАТОК В. Генеральний план ОІД

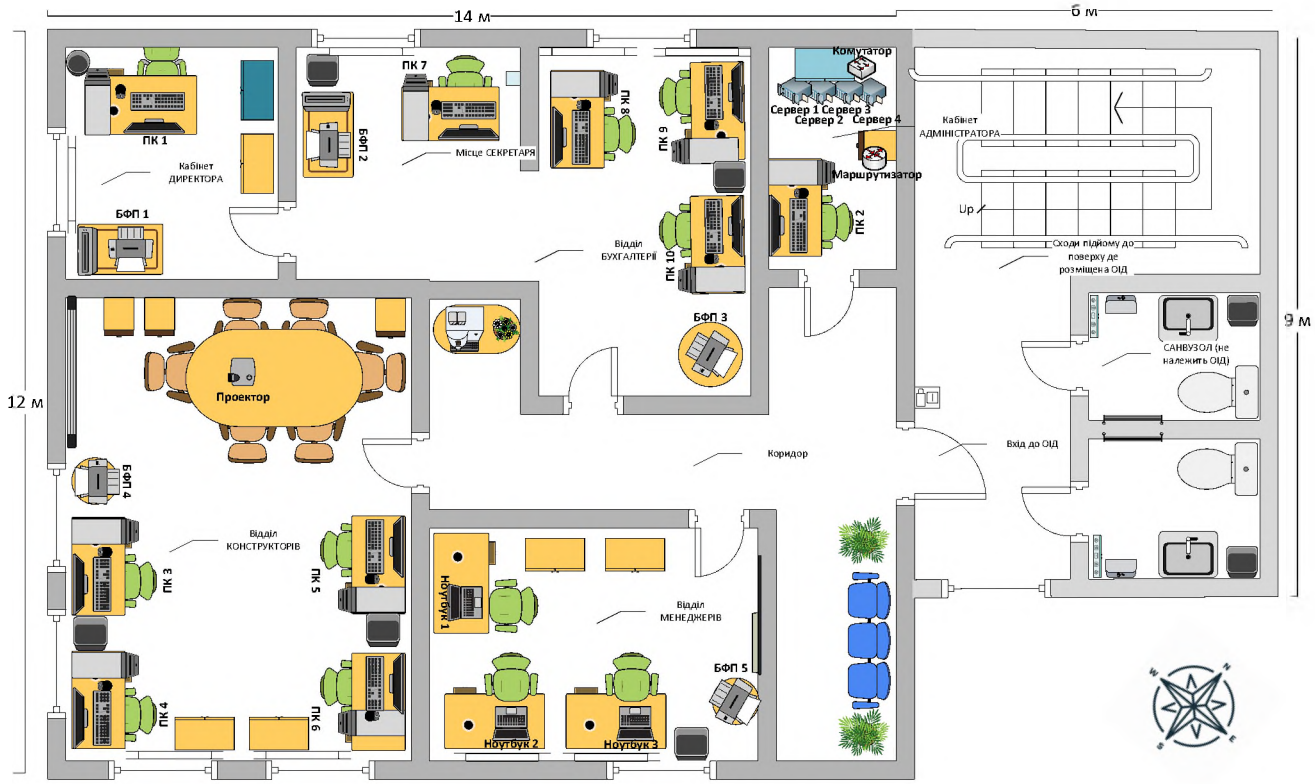


Рисунок В.1 – Генеральний план ОІД

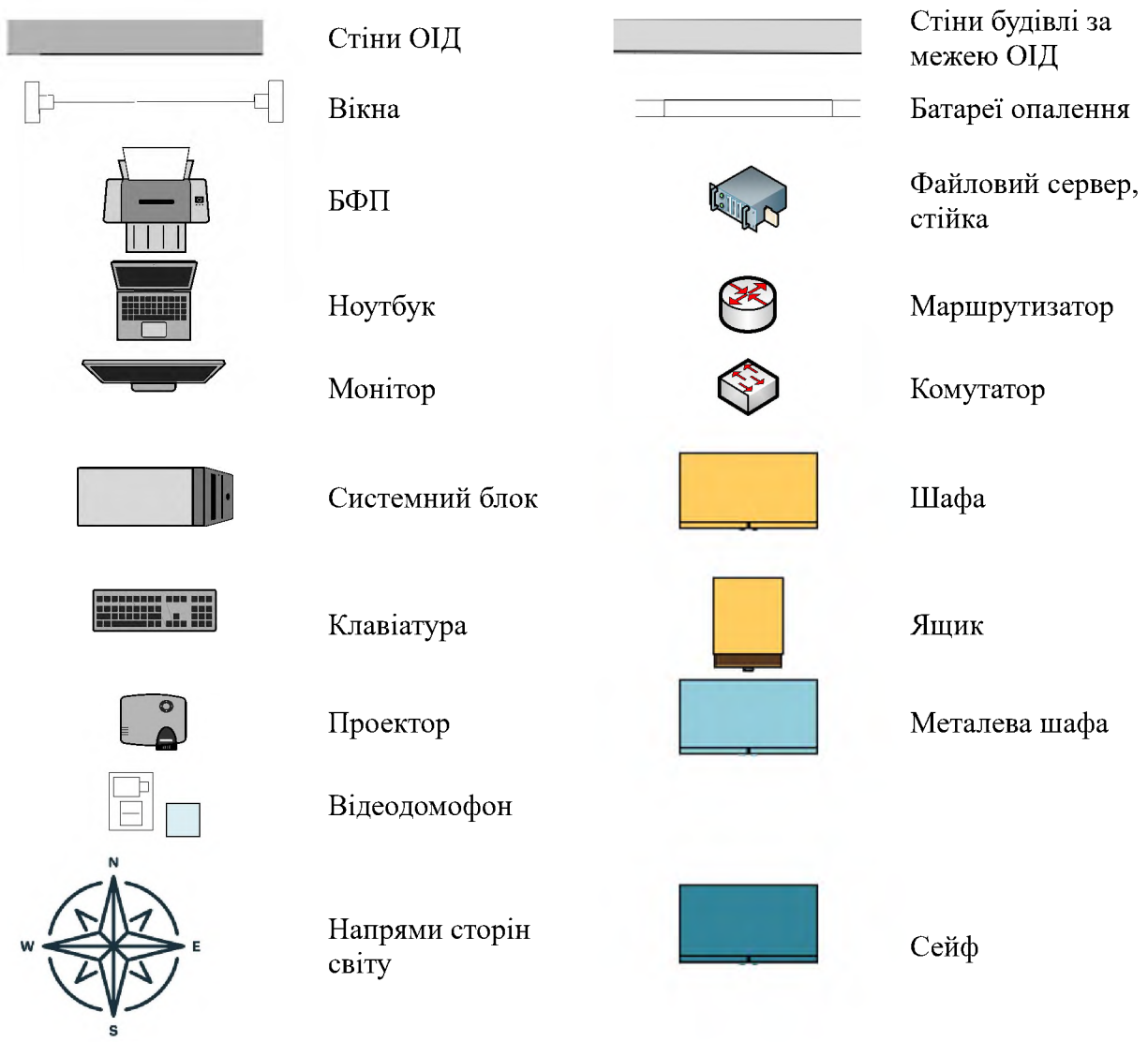


Рисунок В.2 – Умовні позначення до генерального плану

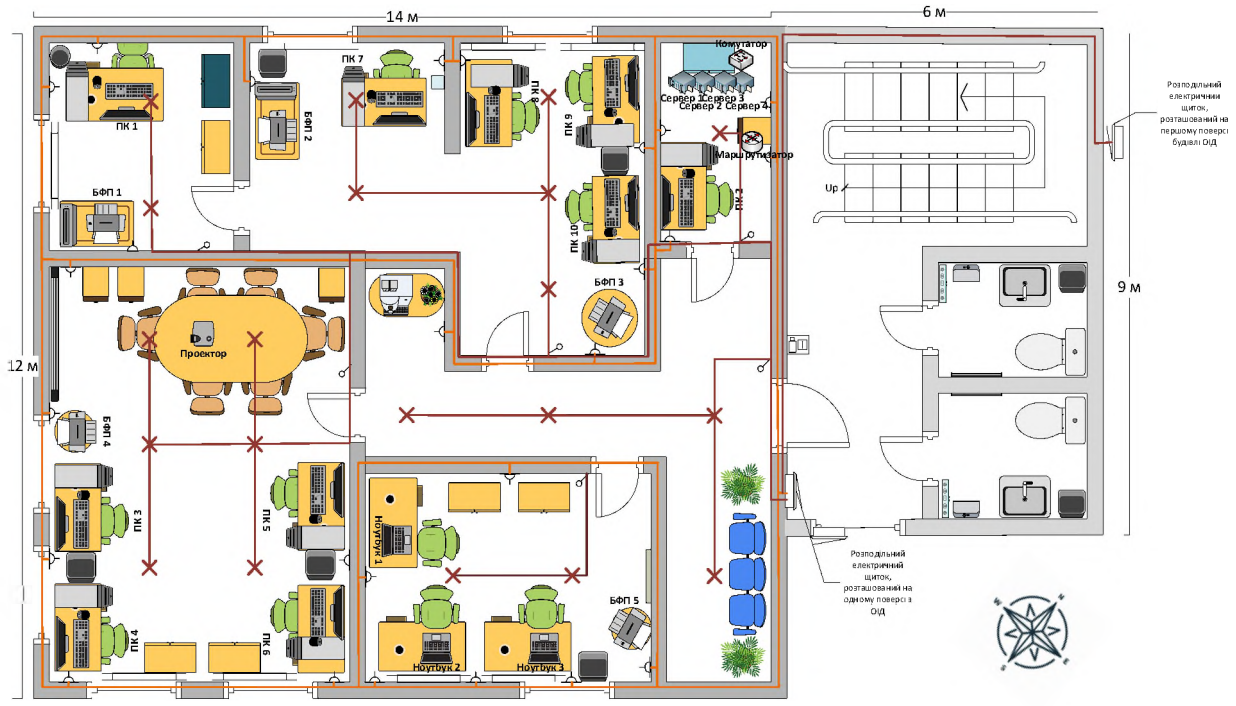


Рисунок В.3 – Лінії системи електропостачання та освітлення на генеральному плані ОІД

Лінії системи електропостачання

Лінії системи освітлення

Розподільний електричний щиток

Штепсельна розетка


Напрями сторін світу

Вимикач

Рисунок В.4 – Умовні позначення до ліній системи електропостачання та освітлення на генеральному плані ОІД

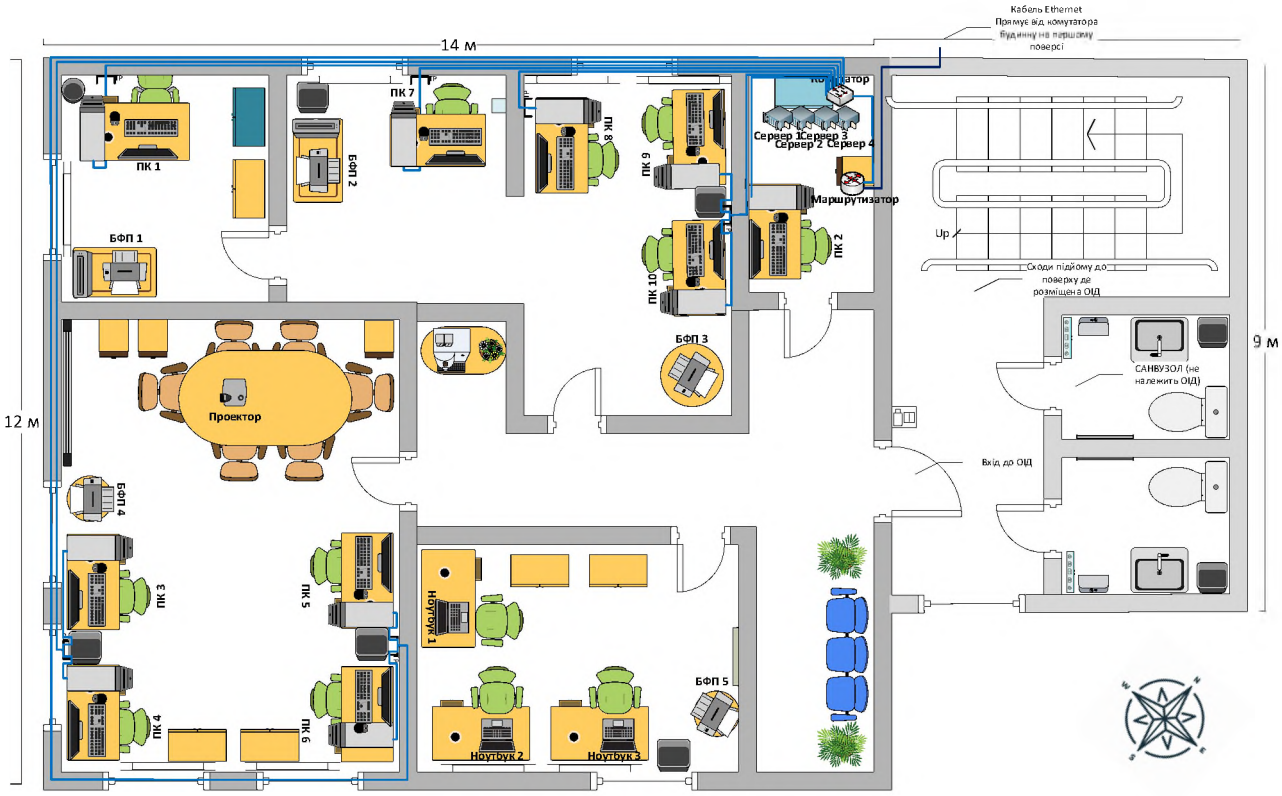


Рисунок В.5 – Комп’ютерна мережа на генеральному плані ОІД

Кабель Ethernet від комутатора в ОІД

Кабель Ethernet від комутатора будинку

Коммутатор

Маршрутизатор


Розетка RJ45


Напрями сторін світу

Рисунок В.6 – Умовні позначення до комп’ютерної мережі на генеральному плані ОІД

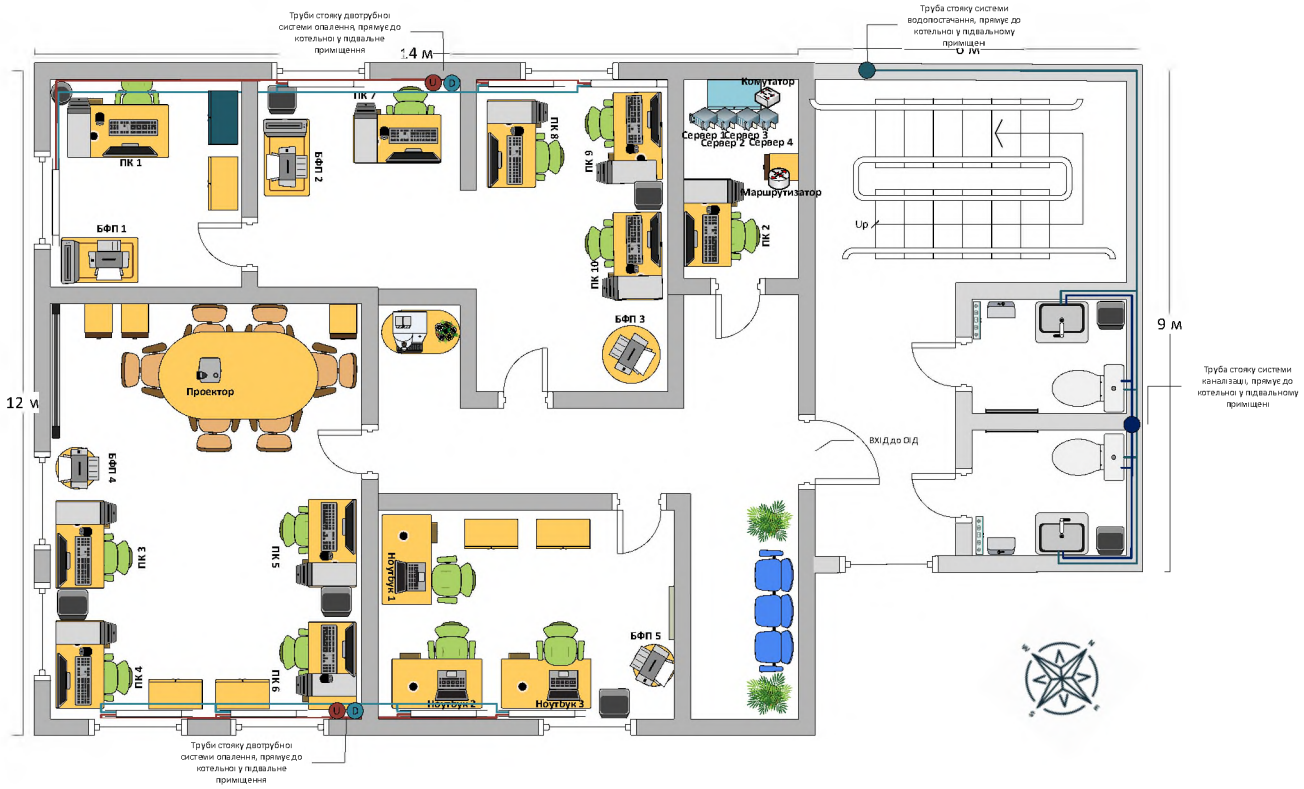


Рисунок В.7 – Лінії системи опалення та водопостачання на генеральному плані ОІД


Рисунок В.8 – Умовні позначення до ліній системи опалення та водопостачання на генеральному плані ОІД

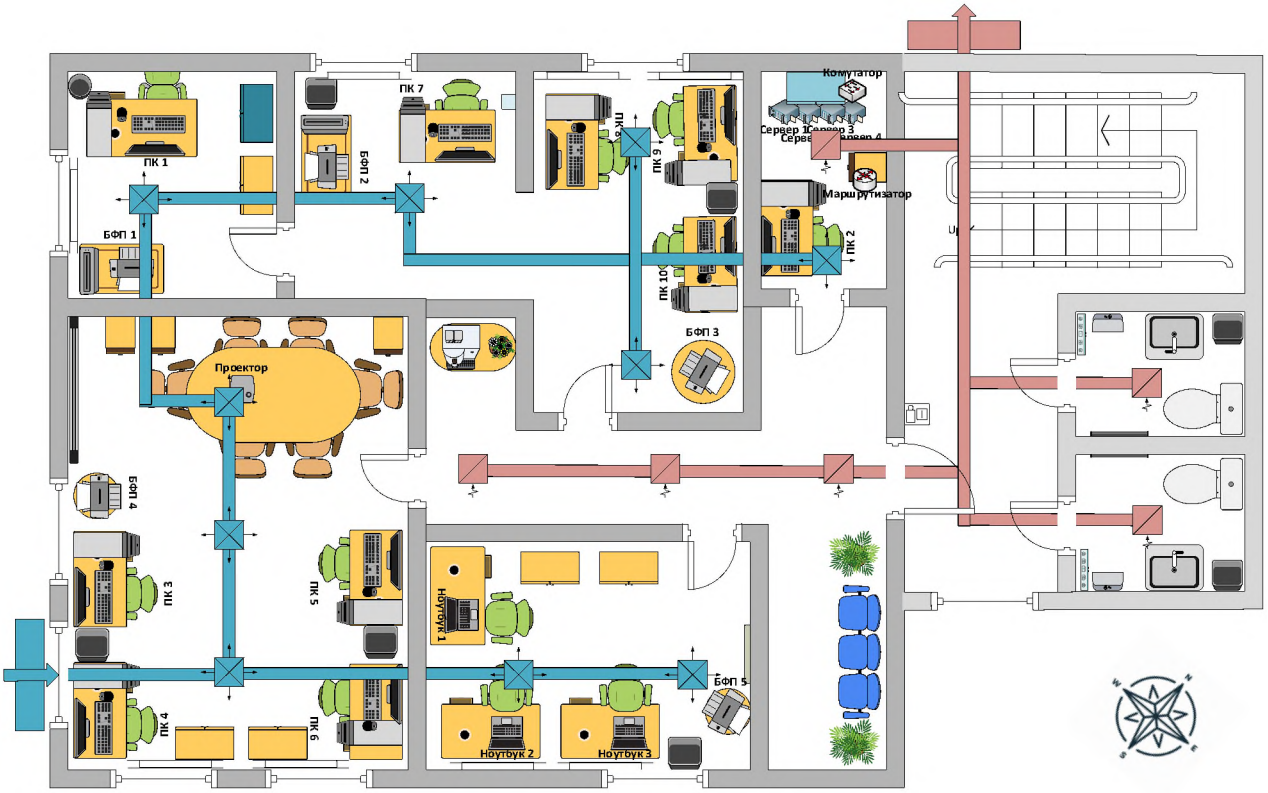


Рисунок В.9 – Система вентиляції на генеральному плані ОІД

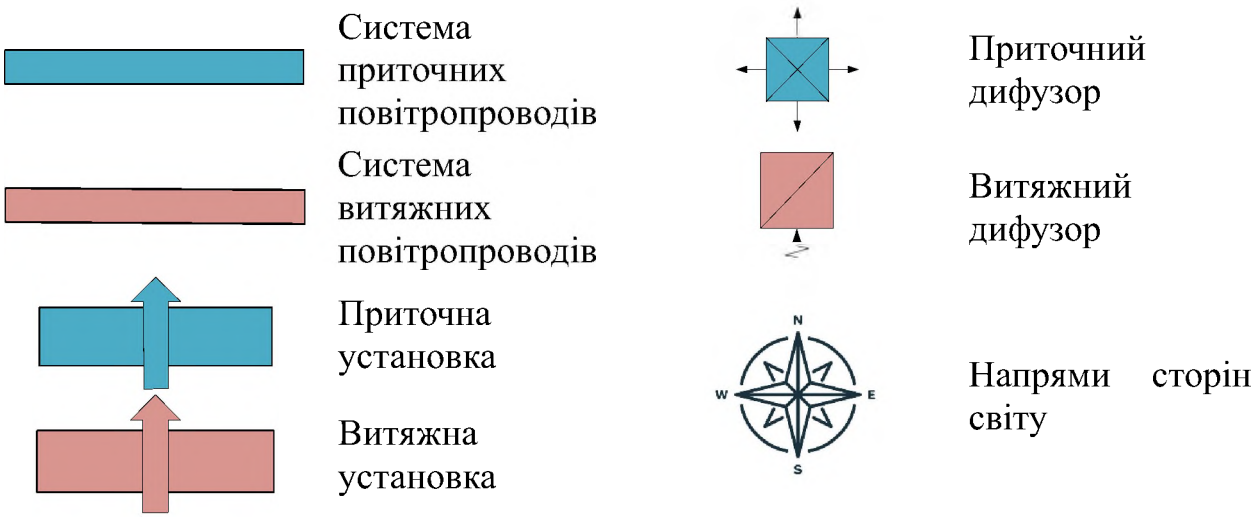


Рисунок В.10 – Умовні позначення до система вентиляції на генеральному плані ОІД

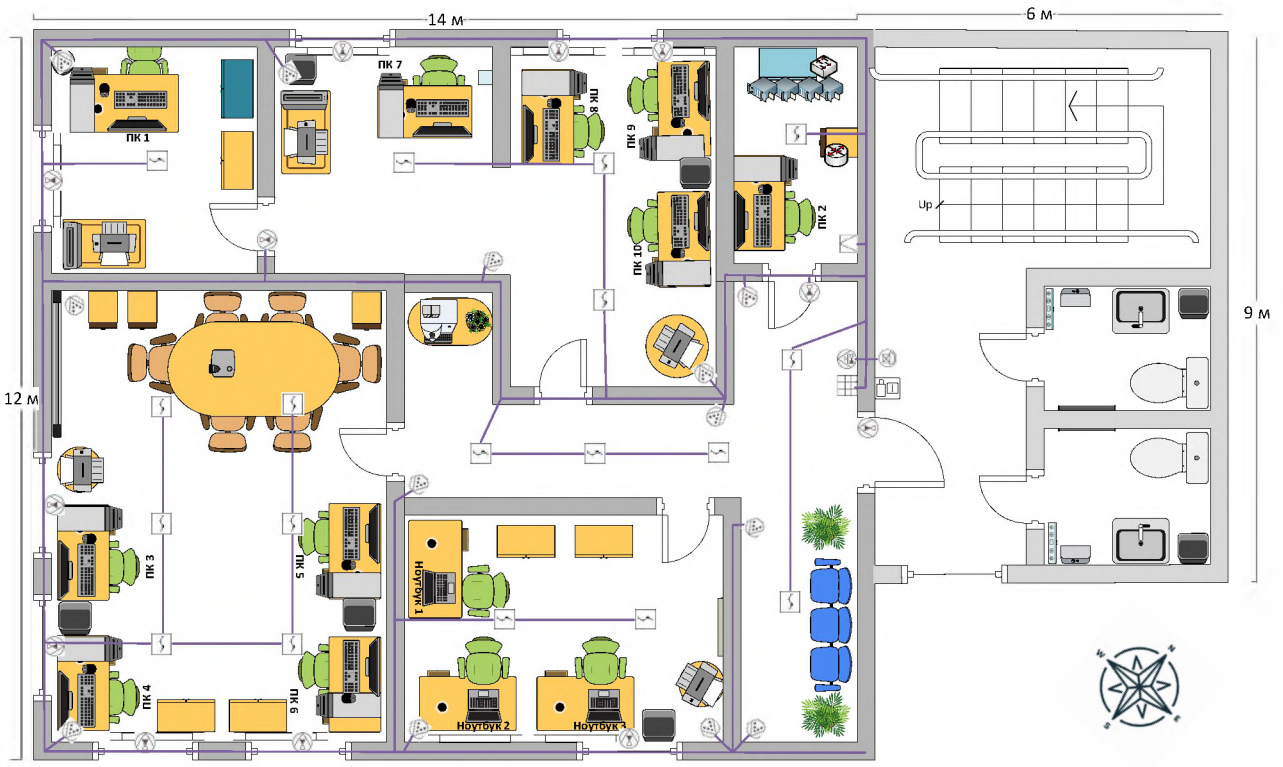


Рисунок В.11 – Лінії системи охоронно-пожежної сигналізації на генеральному плані ОІД

| | | | |
|---|---|---|---|
| | ПКП | | Датчик диму |
| | Клавіатура ПКП | | Сповіщувач точковий магнітоконтактний |
| | Сповіщувач точковий ручний магнітоконтактний | | Сповіщувач об'ємний інфрачервоний |
| | Комбінований світло-звуковий сповіщувач | | |
| N W E S | Напрями сторін світу | | Лінії системи охоронно-пожежної сигналізації |

Рисунок В.12 – Умовні позначення до ліній системи охоронно-пожежної сигналізації на генеральному плані ОІД

# ДОДАТОК Г. Перелік і склад ОТЗ та ДТЗС в ІКС

Таблиця Г.1 – Перелік ОТЗ в ІКС

| Назва | Модель | Серійний номер | Розміщення | Відстань до межі ОІД, м |
|---|---|---|---|---|
| ПК 1 (Монітор) | SAMSUNG LS22C310EAIXCI | 245011 | Кабінет директора, на столі | 1,7 |
| ПК 2 (Монітор) | SAMSUNG LS22C310EAIXCI | 245012 | Кабінет адміністратора, на столі | 2,3 |
| ПК 3 (Монітор) | SAMSUNG LS22C310EAIXCI | 245013 | Відділ конструкторів, на столі | 0,42 |
| ПК 4 (Монітор) | SAMSUNG LS22C310EAIXCI | 245014 | Відділ конструкторів, на столі | 0,42 |
| ПК 5 (Монітор) | SAMSUNG LS22C310EAIXCI | 245015 | Відділ конструкторів, на столі | 5,65 |
| ПК 6 (Монітор) | SAMSUNG LS22C310EAIXCI | 245016 | Відділ конструкторів, на столі | 5,65 |
| ПК 7 (Монітор) | SAMSUNG LS22C310EAIXCI | 245017 | Відділ бухгалтерії, на столі | 1,71 |
| ПК 8 (Монітор) | SAMSUNG LS22C310EAIXCI | 245018 | Відділ бухгалтерії, на столі | 1,28 |
| ПК 9 (Монітор) | SAMSUNG LS22C310EAIXCI | 245019 | Відділ бухгалтерії, на столі | 0,6 |
| ПК 10 (Монітор) | SAMSUNG LS22C310EAIXCI | 245020 | Відділ бухгалтерії, на столі | 2,57 |
| ПК 1 (Клавіатура) | LOGITECH K120 | 75231 | Кабінет директора, на столі | 0,77 |
| ПК 2 (Клавіатура) | LOGITECH K120 | 75232 | Кабінет адміністратора, на столі | 1,7 |
| ПК 3 (Клавіатура) | LOGITECH K120 | 75233 | Відділ конструкторів | 0,68 |
| ПК 4 (Клавіатура) | LOGITECH K120 | 75234 | Відділ конструкторів, на столі | 0,68 |
| ПК 5 (Клавіатура) | LOGITECH K120 | 75235 | Відділ конструкторів, на столі | 5 |

Продовження таблиці Г.1

| Назва | Модель | Серійний номер | Розміщення | Відстань до межі ОІД, м |
|---|---|---|---|---|
| ПК 6 (Клавіатура) | LOGITECH K120 | 75236 | Відділ конструкторів, на столі | 5 |
| ПК 7 (Клавіатура) | LOGITECH K120 | 75237 | Відділ бухгалтерії, на столі | 0,77 |
| ПК 8 (Клавіатура) | LOGITECH K120 | 75238 | Відділ бухгалтерії, на столі | 1,37 |
| ПК 9 (Клавіатура) | LOGITECH K120 | 75239 | Відділ бухгалтерії, на столі | 0,6 |
| ПК 10 (Клавіатура) | LOGITECH K120 | 75240 | Відділ бухгалтерії, на столі | 2,65 |
| ПК 1 (Системний блок) | VINGA CS112B | 13541 | Кабінет директора, на столі | 0,85 |
| ПК 2 (Системний блок) | VINGA CS112B | 13542 | Кабінет адміністратора, на столі | 1,28 |
| ПК 3 (Системний блок) | VINGA CS112B | 13543 | Відділ конструкторів, на столі | 0,42 |
| ПК 4 (Системний блок) | VINGA CS112B | 13544 | Відділ конструкторів, на столі | 0,42 |
| ПК 5 (Системний блок) | VINGA CS112B | 13545 | Відділ конструкторів, на столі | 4,71 |
| ПК 6 (Системний блок) | VINGA CS112B | 13546 | Відділ конструкторів, на столі | 4,71 |
| ПК 7 (Системний блок) | VINGA CS112B | 13547 | Відділ бухгалтерії, на столі | 0,85 |
| ПК 8 (Системний блок) | VINGA CS112B | 13548 | Відділ бухгалтерії, на столі | 0,6 |
| ПК 9 (Системний блок) | VINGA CS112B | 13549 | Відділ бухгалтерії, на столі | 1,71 |
| ПК 10 (Системний блок) | VINGA CS112B | 13550 | Відділ бухгалтерії, на столі | 3,68 |

Продовження таблиці Г.1

| Назва | Модель | Серійний номер | Розміщення | Відстань до межі ОІД, м |
|---|---|---|---|---|
| Ноутбук 1 | Asus ExpertBook B1 B1502CBA-BQ0499 | 73531 | Відділ менеджерів, на столі | 2,65 |
| Ноутбук 2 | Asus ExpertBook B1 B1502CBA-BQ0499 | 73532 | Відділ менеджерів, на столі | 0,6 |
| Ноутбук 3 | Asus ExpertBook B1 B1502CBA-BQ0499 | 73533 | Відділ менеджерів, на столі | 0,6 |
| БФП 1 | CANON I-SENSYS MF264DW C WI-FI | 11351 | Кабінет директора, на столі | 1,02 |
| БФП 2 | CANON I-SENSYS MF264DW C WI-FI | 11352 | Відділ бухгалтерії, на столі | 1,45 |
| БФП 3 | CANON I-SENSYS MF264DW C WI-FI | 11353 | Відділ бухгалтерії, на столі | 2,91 |
| БФП 4 | CANON I-SENSYS MF264DW C WI-FI | 11354 | Відділ конструкторів, на столі | 0,43 |
| БФП 5 | CANON I-SENSYS MF264DW C WI-FI | 11355 | Відділ менеджерів, на столі | 1,03 |
| Проектор | BENQ MS550 | 54635 | Відділ конструкторів, на столі | 3 |
| Маршрутизатор | MIKROTIK RB4011IGS+5HACQ2HND-IN | 16547 | Кабінет адміністратора, на столі | 0,51 |
| Комутатор (Switch) | MIKROTIK CRS328-24P-4S+RM | 36512 | Кабінет адміністратора, у шафі | 0,43 |
| Сервер 1 | HP Proliant DL 380 Gen10 (8x2.5) SFF | 56481 | Кабінет адміністратора, у шафі | 0,2 |
| Сервер 2 | HP Proliant DL 380 Gen10 (8x2.5) SFF | 56482 | Кабінет адміністратора, у шафі | 0,2 |
| Сервер 3 | HP Proliant DL 380 Gen10 (8x2.5) SFF | 56483 | Кабінет адміністратора, у шафі | 0,2 |
| Сервер 4 | HP Proliant DL 380 Gen10 (8x2.5) SFF | 56484 | Кабінет адміністратора, у шафі | 0,2 |

Таблиця Г.2 – Перелік ДТЗС в ІКС

| Назва | Модель | Серійний номер | Розміщення | Відстань до ОТЗ, м |
|---|---|---|---|---|
| Шафа підлогова | MIRSAN GTN 19" 12U 600X600 | 56431 | Кабінет адміністратора, на стіні | 0,01 |
| Сейф офісний | Griffon R.48.E (ВхШхГ:480x380x370) | 1543 | Кабінет директора, у шафі | 0,95 |
| ПКП | Satel INTEGRA 64 Plus | 63290 | Кабінет адміністратора, на стіні | 1,16 |
| Клавіатура до ПКП | SATEL INT-SK-GR | 12873 | Коридор, на стіні біля вхідних дверей до ОІД | 2,55 |
| Комбінований світло-звуковий сповіщувач | Atis LD-95 (red) | 98313 | За межами ОІД, на стіні біля вхідних дверей до ОІД | 2,7 |
| Сповіщувач точковий ручний | TIRAS СПР-"Тирас" | 11352 | Коридор, на стіні біля вхідних дверей до ОІД | 2,18 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36501 | Коридор, в куті, направлений на стільці | 2,12 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36502 | Коридор, направлений на вхідні двері до ОІД | 2,95 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36503 | Коридор, в куті, біля вхідних дверей до кабінету адміністратора, направлений на вхідні двері до ОІД | 2,12 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36504 | Коридор, направлений на вхідні двері до відділу менеджерів | 2,12 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36505 | Коридор, в куті, біля вхідних дверей до відділу конструкторів | 2,19 |

Продовження таблиці Г.2

| Назва | Модель | Серійний номер | Розміщення | Відстань до ОТЗ, м |
|---|---|---|---|---|
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36506 | Відділ бухгалтерії, в правому нижньому куті кімнати | 2,01 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36507 | Відділ бухгалтерії, в лівому верхньому куті кімнати | 2,12 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36508 | Відділ бухгалтерії, направлений на ПК 8 та ПК 9 | 3,53 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36509 | Кабінет директора | 2 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36510 | Відділ конструкторів, в лівому верхньому куті кімнати | 2,12 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36511 | Відділ конструкторів, в лівому нижньому куті кімнати | 2 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36512 | Відділ менеджерів, в лівому нижньому куті кімнати | 2,12 |
| Сповіщувач об'ємний інфрачервоний | Crow Swan Quad | 36513 | Відділ менеджерів, в правому нижньому куті кімнати | 2,01 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14531 | Вхідні двері до ОІД | 3,83 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14532 | Вхідні двері до кабінету адміністратора | 2,24 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14533 | Вікно, відділ бухгалтерії, біля ПК 9 | 2 |

Продовження таблиці Г.2

| Назва | Модель | Серійний номер | Розміщення | Відстань до ОТЗ, м |
|---|---|---|---|---|
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14534 | Вікно, відділ бухгалтерії, біля ПК 8 | 2 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14535 | Вікно, відділ бухгалтерії, біля ПК 7 | 2,12 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14536 | Вікно, кабінет директора | 2,28 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14537 | Вікно, відділ конструкторів, біля ПК 3 | 2 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14538 | Вікно, відділ конструкторів, біля ПК 4 (ліва стіна) | 2 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14539 | Вікно, відділ конструкторів, біля ПК 4 (нижня стіна) | 2,12 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14540 | Вікно, відділ конструкторів, біля ПК 6 | 2,03 |
| Сповіщувач точковий магнітоконтактний | ЭСМК-7ЭП | 14541 | Вікно, відділ менеджерів | 2 |
| Датчик диму | Артон СПД-3.2 | 55871 | Коридор, на стелі, зона біля дверей до кабінету адміністратора | 2,7 |
| Датчик диму | Артон СПД-3.2 | 55872 | Коридор, на стелі, зона біля стільців | 2,47 |
| Датчик диму | Артон СПД-3.2 | 55873 | Коридор, на стелі, зона біля вхідних дверей до відділу менеджерів | 2,47 |
| Датчик диму | Артон СПД-3.2 | 55874 | Коридор, на стелі, зона біля вхідних дверей до відділу бухгалтерії | 2,8 |

Продовження таблиці Г.2

| Назва | Модель | Серійний номер | Розміщення | Відстань до ОТЗ, м |
|---|---|---|---|---|
| Датчик диму | Артон СПД-3.2 | 55875 | Коридор, на стелі, зона біля вхідних дверей до відділу конструкторів | 2,7 |
| Датчик диму | Артон СПД-3.2 | 55876 | Відділ менеджерів, на стелі, зона біля Ноутбука 2 | 2,27 |
| Датчик диму | Артон СПД-3.2 | 55877 | Відділ менеджерів, на стелі, зона біля вхідних дверей | 2,21 |
| Датчик диму | Артон СПД-3.2 | 55878 | Відділ конструкторів, на стелі, зона біля ПК 6 | 2,12 |
| Датчик диму | Артон СПД-3.2 | 55879 | Відділ конструкторів, на стелі, зона біля ПК 5 | 2,15 |
| Датчик диму | Артон СПД-3.2 | 55880 | Відділ конструкторів, на стелі, зона біля ПК 4 | 2,08 |
| Датчик диму | Артон СПД-3.2 | 55881 | Відділ конструкторів, на стелі, зона біля ПК 3 | 2,08 |
| Датчик диму | Артон СПД-3.2 | 55882 | Відділ конструкторів, на стелі, зона біля вхідних дверей | 2,7 |
| Датчик диму | Артон СПД-3.2 | 55883 | Відділ конструкторів, на стелі, зона біля БФП 4 | 2,35 |
| Датчик диму | Артон СПД-3.2 | 55884 | Кабінет директора | 2,02 |
| Датчик диму | Артон СПД-3.2 | 55885 | Відділ бухгалтерії, на стелі, зона біля ПК 7 | 2,01 |

Продовження таблиці Г.2

| Назва | Модель | Серійний номер | Розміщення | Відстань до ОТЗ, м |
|---|---|---|---|---|
| Датчик диму | Артон СПД-3.2 | 55886 | Відділ бухгалтерії, на стелі, зона біля ПК 8 та ПК 9 | 2,1 |
| Датчик диму | Артон СПД-3.2 | 55887 | Відділ бухгалтерії, на стелі, зона біля ПК 10 | 2,1 |
| Датчик диму | Артон СПД-3.2 | 55888 | Кабінет адміністратора | 2,03 |

# ДОДАТОК Д. Характеристика складу ІКС підприємства

Таблиця Д.1 – Характеристика складу ІКС

| Назва | Назва в ІКС | Характеристика | Серійний номер |
|---|---|---|---|
| Персональний комп'ютер | ПК 1 | Процесор: AMD RYZEN 5 5500GT;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>SSD: SAMSUNG M.2 2280 512GB PM9A1;<br>Материнська плата: GIGABYTE B450M DS3H; | 46811<br>77563<br>57091<br>31390 |
| Персональний комп'ютер | ПК 2 | Процесор: AMD RYZEN 5 5500GT;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>SSD: SAMSUNG M.2 2280 512GB PM9A1;<br>Материнська плата: GIGABYTE B450M DS3H; | 46812<br>77564<br>57092<br>31391 |
| Персональний комп'ютер | ПК 3 | Процесор: AMD Ryzen 5500;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>Жорсткий диск: WD 1 TB 3.5";<br>Материнська плата: GIGABYTE B450M DS3H;<br>Відеокарта: ASUS RADEON RX 6600 8GB DUAL. | 146913<br>77565<br>547993<br>31392<br>98635 |
| Персональний комп'ютер | ПК 4 | Процесор: AMD Ryzen 5500;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>Жорсткий диск: WD 1 TB 3.5";<br>Материнська плата: GIGABYTE B450M DS3H;<br>Відеокарта: ASUS RADEON RX 6600 8GB DUAL. | 146914<br>77566<br>547994<br>31393<br>98636 |
| Персональний комп'ютер | ПК 5 | Процесор: AMD Ryzen 5500;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>Жорсткий диск: WD 1 TB 3.5";<br>Материнська плата: GIGABYTE B450M DS3H;<br>Відеокарта: ASUS RADEON RX 6600 8GB DUAL. | 146915<br>77567<br>547995<br>31394<br>98637 |
| Персональний комп'ютер | ПК 6 | Процесор: AMD Ryzen 5500;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>Жорсткий диск: WD 1 TB 3.5";<br>Материнська плата: GIGABYTE B450M DS3H;<br>Відеокарта: ASUS RADEON RX 6600 8GB DUAL. | 146916<br>77568<br>57093<br>31395 |

Продовження таблиці Д.1

| Назва | Назва в ІКС | Характеристика | Серійний номер |
|---|---|---|---|
| Персональний комп'ютер | ПК 7 | Процесор: AMD RYZEN 5 5500GT;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>SSD: SAMSUNG M.2 2280 512GB PM9A1;<br>Материнська плата: GIGABYTE B450M DS3H; | 46813<br>77569<br>57094<br>31396 |
| Персональний комп'ютер | ПК 8 | Процесор: AMD RYZEN 5 5500GT;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>SSD: SAMSUNG M.2 2280 512GB PM9A1;<br>Материнська плата: GIGABYTE B450M DS3H; | 46814<br>77570<br>57095<br>31397 |
| Персональний комп'ютер | ПК 9 | Процесор: AMD RYZEN 5 5500GT;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>SSD: SAMSUNG M.2 2280 512GB PM9A1;<br>Материнська плата: GIGABYTE B450M DS3H; | 46815<br>77571<br>57096<br>31398 |
| Персональний комп'ютер | ПК 10 | Процесор: AMD RYZEN 5 5500GT;<br>ОЗП: Kingston FURY Beast DDR4 16GB 3200 MHz (2×8 GB);<br>SSD: SAMSUNG M.2 2280 512GB PM9A1;<br>Материнська плата: GIGABYTE B450M DS3H; | 46816<br>77572<br>57097<br>31399 |
| Ноутбук | Ноутбук 1 | Процесор: Intel Core i3 1215U (3.3-4.4 ГГц);<br>ОЗП: DDR4 8 GB;<br>SSD: 256 GB;<br>Відеокарта: Intel UHD Graphics; | 44589<br>21337<br>11392<br>85210 |
| Ноутбук | Ноутбук 2 | Процесор: Intel Core i3 1215U (3.3-4.4 ГГц);<br>ОЗП: DDR4 8 GB;<br>SSD: 256 GB;<br>Відеокарта: Intel UHD Graphics; | 44590<br>21338<br>11393<br>85211 |
| Ноутбук | Ноутбук 3 | Процесор: Intel Core i3 1215U (3.3-4.4 ГГц);<br>ОЗП: DDR4 8 GB;<br>SSD: 256 GB;<br>Відеокарта: Intel UHD Graphics; | 44591<br>21339<br>11394<br>85212 |
| Багато-функціональний пристрій | БФП 1 | Технологія друку: Лазерна;<br>Тип друку: Монохромний;<br>Максимальний формат друку: A4;<br>Частота процесору: 400 MHz;<br>Рівень шуму: 51 дБ; | 69861 |

Продовження таблиці Д.1

| Назва | Назва в ІКС | Характеристика | Серійний номер |
|---|---|---|---|
| Багато-функціональний пристрій | БФП 2 | Технологія друку: Лазерна;<br>Тип друку: Монохромний;<br>Максимальний формат друку: А4;<br>Частота процесору: 400 MHz;<br>Рівень шуму: 51 дБ; | 69862 |
| Багато-функціональний пристрій | БФП 3 | Технологія друку: Лазерна;<br>Тип друку: Монохромний;<br>Максимальний формат друку: А4;<br>Частота процесору: 400 MHz;<br>Рівень шуму: 51 дБ; | 69863 |
| Багато-функціональний пристрій | БФП 4 | Технологія друку: Лазерна;<br>Тип друку: Монохромний;<br>Максимальний формат друку: А4;<br>Частота процесору: 400 MHz;<br>Рівень шуму: 51 дБ; | 69864 |
| Багато-функціональний пристрій | БФП 5 | Технологія друку: Лазерна;<br>Тип друку: Монохромний;<br>Максимальний формат друку: А4;<br>Частота процесору: 400 MHz;<br>Рівень шуму: 51 дБ; | 69865 |
| Сервер | Сервер 1 | Форм-фактор: 1U;<br>Процесор: Intel XEON Silver 8 Core 4110 [2.10GHz - 3.00GHz]<br>ОЗП: 16 GB;<br>Мережевий адаптер: HP ×4;<br>Жорсткий диск: DELL 2TB 7.2K RPM SATA 6GBPS ×2; | 55235 |
| Сервер | Сервер 2 | Форм-фактор: 1U;<br>Процесор: Intel XEON Silver 8 Core 4110 [2.10GHz - 3.00GHz]<br>ОЗП: 16 GB;<br>Мережевий адаптер: HP ×4;<br>Жорсткий диск: DELL 2TB 7.2K RPM SATA 6GBPS ×2; | 55236 |
| Сервер | Сервер 3 | Форм-фактор: 1U;<br>Процесор: Intel XEON Silver 8 Core 4110 [2.10GHz - 3.00GHz]<br>ОЗП: 16 GB;<br>Мережевий адаптер: HP ×4;<br>Жорсткий диск: DELL 2TB 7.2K RPM SATA 6GBPS ×2; | 55237 |
| Сервер | Сервер 4 | Форм-фактор: 1U;<br>Процесор: Intel XEON Silver 8 Core 4110 [2.10GHz - 3.00GHz]<br>ОЗП: 16 GB;<br>Мережевий адаптер: HP ×4;<br>Жорсткий диск: DELL 2TB 7.2K RPM SATA 6GBPS ×2; | 55238 |

Продовження таблиці Д.1

| Назва | Назва в ІКС | Характеристика | Серійний номер |
|---|---|---|---|
| Комутатор | Комутатор | Тип: керований 2-ого типу;<br>Форм-фактор: в стійку;<br>Типи портів: 4×SFP+, 24× Gigabit Ethernet; | 669512 |
| Маршрутизатор | Маршрути-затор | Режим роботи: провідний маршрутизатор, Wi-Fi маршрутизатор;<br>Стандарт Wi-Fi 802.11: n , ac , g , b;<br>Робоча частота:<br>2.4 / 5 ГГц;<br>Кількість антен: 4;<br>Вхідний інтерфейс:<br>SFP+;<br>Кількість LAN-портів: 10.<br>Підтримка VPN: є. | 139560 |

# ДОДАТОК Е. Модель загроз ІКС підприємства

Таблиця Е.1 – Модель загроз

| Вид загрози | Джерело загрози | Вразливість | Коп_д | Коп_в | Коефіцієнт небезпеки |
|---|---|---|---|---|---|
| Витік інформації через апаратні закладки, що встановлюються у мережі електроживлення | Представники організацій, що взаємодіють з питань технічного забезпечення систем життєдіяльності організації | Апаратні закладки, що встановлюються у мережі електроживлення | 0,01 | 0,13 | 0,01 |
| | Хакери | | 0,26 | 0,13 | 0,03 |
| Витік інформації через апаратні закладки, що встановлюються у приміщенні | Технічний персонал, який обслуговує будови та приміщення, в яких розташовані компоненти ІКС | Апаратні закладки, що встановлюються у приміщенні | 0,01 | 0,21 | 0,01 |
| | Хакери | | 0,26 | 0,21 | 0,05 |
| | Агенти конкурентів | | 0,32 | 0,21 | 0,07 |
| | Колишні працівники | | 0,06 | 0,21 | 0,01 |
| | Користувачі ІКС | | 0,14 | 0,21 | 0,03 |
| Витік інформації через апаратні закладки, що встановлюються у технічних засобах | Технічний персонал, який обслуговує будови та приміщення, в яких розташовані компоненти ІКС | Апаратні закладки, що встановлюються у технічних засобах | 0,01 | 0,26 | 0,01 |
| | Хакери | | 0,26 | 0,26 | 0,07 |

Продовження таблиці Е.1

| | | | | | |
|---|---|---|---|---|---|
| Витік інформації через програмні закладки, а саме нелегальні копії ПЗ | Хакери | Програмні закладки: нелегальні копії ПЗ | 0,26 | 0,19 | 0,05 |
| Витік інформації через програмні закладки, а саме шкідливі програми | Хакери | Програмні закладки: шкідливі програми | 0,26 | 0,21 | 0,05 |
| Витік інформації через елементи, що піддаються впливу електромагнітного поля, а саме магнітні носії | Хакери | Елементи, що піддаються впливу електромагнітного поля: магнітні носії | 0,26 | 0,14 | 0,04 |
| | Агенти конкурентів | | 0,32 | 0,14 | 0,04 |
| | Колишні працівники | | 0,06 | 0,14 | 0,01 |
| Витік інформації через елементи, що піддаються впливу електромагнітного поля, а саме мікросхеми | Хакери | Елементи, що піддаються впливу електромагнітного поля: мікросхеми | 0,26 | 0,1 | 0,03 |
| | Агенти конкурентів | | 0,32 | 0,1 | 0,03 |
| Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу | Агенти конкурентів | Місце розташування об’єкта: наявність прямої видимості об’єктів | 0,32 | 0,1 | 0,03 |
| Перегляд ІзОД на екранах моніторів з робочих місць користувачів ІКС сторонніми особами | Колишні працівники | Місце розташування об’єкта: наявність прямої видимості об’єктів | 0,06 | 0,29 | 0,02 |
| | Користувачі ІКС | | 0,14 | 0,29 | 0,04 |
| Доступ до ІзОД сторонніми особами | Користувачі ІКС | Порушення режиму охорони та захисту: доступу до технічних засобів | 0,14 | 0,19 | 0,03 |
| | Агенти конкурентів | | 0,32 | 0,19 | 0,06 |
| | Колишні працівники | | 0,29 | 0,19 | 0,05 |
| Втрата носіїв інформації, що містять ІзОД | Користувачі ІКС | Порушення режиму використання інформації: зберігання та знищення носіїв інформації | 0,14 | 0,64 | 0,09 |

| | | | | | |
|---|---|---|---|---|---|
| Несанкціоноване призначення атрибутів доступу користувачам | Обслуговуючий персонал ІКС (Адміністратор) | Порушення режиму безпеки системи: підвищені привілеї | 0,64 | 0,8 | 0,51 |
| Порушення доступності інформації під час відмови та несправності технічних засобів, що обробляють інформацію | Мережеве обладнання | Відмови та несправності технічних засобів, що обробляють інформацію | 0,38 | 0,24 | 0,09 |
| | Технічне обладнання | | 0,15 | 0,24 | 0,04 |
| Порушення цілісності і доступності інформації через відмову або несправність технічних засобів, що зберігають інформацію (внутрішні) | Технічне обладнання | Відмови та несправності технічних засобів, що зберігають інформацію (внутрішні) | 0,15 | 0,32 | 0,05 |
| | Сервери | | 0,26 | 0,32 | 0,08 |
| Порушення доступності інформації під час відмови та несправності технічних засобів, що забезпечують працездатність засобів обробки інформації | Технічне обладнання | Відмови та несправності технічних засобів, що забезпечують працездатність засобів обробки інформації | 0,15 | 0,16 | 0,02 |
| Порушення доступності інформації через старіння і розмагнічування жорстких дисків | Технічне обладнання | Старіння і розмагнічування носіїв інформації: жорстких дисків | 0,15 | 0,14 | 0,02 |
| | Сервери | | 0,26 | 0,14 | 0,04 |
| Порушення доступності інформації та системи через старіння і | Мережеве обладнання | Старіння і розмагнічування носіїв інформації: елементів мікросхем | 0,38 | 0,14 | 0,05 |
| | Технічне обладнання | | 0,15 | 0,14 | 0,02 |
| | Сервери | | 0,26 | 0,14 | 0,04 |

| | | | | | |
|---|---|---|---|---|---|
| розмагнічування елементів мікросхем | | | | | |
| Порушення доступності, цілісності інформації та доступності системи через старіння кабелів і з'єднувальних ліній | Мережеве обладнання | Старіння і розмагнічування носіїв інформації: кабелів і з'єднувальних ліній | 0,38 | 0,13 | 0,05 |
| | Технічне обладнання | | 0,15 | 0,13 | 0,02 |
| | Сервери | | 0,26 | 0,13 | 0,03 |
| Порушення цілісності та доступності системи/інформації через збої операційних систем і СУБД | Користувачі ІКС | Збої програмного забезпечення: операційних систем і СУБД | 0,14 | 0,10 | 0,01 |
| | Прикладне забезпечення | | 0,21 | 0,10 | 0,02 |
| | Системне забезпечення | | 0,29 | 0,10 | 0,03 |
| Порушення цілісності та доступності інформації через збої прикладних програм | Користувачі ІКС | Збої програмного забезпечення: прикладних програм | 0,14 | 0,14 | 0,02 |
| | Прикладне забезпечення | | 0,21 | 0,14 | 0,03 |
| | Системне забезпечення | | 0,29 | 0,14 | 0,04 |
| Порушення цілісності та доступності системи/конфіденційності, цілісності та доступності інформації через збої антивірусних програм | Хакери | Збої програмного забезпечення: антивірусних програм | 0,26 | 0,14 | 0,04 |
| | Прикладне забезпечення | | 0,21 | 0,14 | 0,03 |
| | Системне забезпечення | | 0,29 | 0,14 | 0,04 |
| Порушення цілісності та доступності інформації на обладнані, що обробляє інформацію через збої електропостачання | Система електропостачання | Збої електропостачання: обладнання, що обробляє інформацію | 0,19 | 0,24 | 0,05 |
| | Представники організацій, що взаємодіють з питань технічного забезпечення систем життєдіяльності організації | | 0,01 | 0,24 | 0,02 |
| Порушення цілісності та | Хакери | Збої локальної мережі | 0,26 | 0,16 | 0,04 |

| | | | | | |
|---|---|---|---|---|---|
| доступності інформації, що міститься на серверах, через збої локальної мережі | Мережеве обладнання | | 0,38 | 0,16 | 0,06 |
| Порушення цілісності та доступності системи/інформації через пошкодження життє-забезпечувальних комунікацій | Пожежа | Пошкодження життє-забезпечувальних комунікацій: електро-, водо-, теплопостачання | 0,19 | 0,24 | 0,05 |
| | Представники організацій, що взаємодіють з питань технічного забезпечення систем життєдіяльності організації | | 0,01 | 0,24 | 0,02 |
| Порушення конфіденційності, цілісності та доступності інформації, що міститься на серверах через пошкодження корпусів технологічного обладнання | Пожежа | Пошкодження огороджувальних конструкцій: корпусів технологічного обладнання (серверна шафа) | 0,19 | 0,10 | 0,02 |
| | Користувачі ІКС | | 0,14 | 0,10 | 0,01 |

ДОДАТОК Є. Перелік документів на оптичному носії

Чурсина_ 125-20-1_Пояснювальна_записка.docx

Чурсина_ 125-20-1_Пояснювальна_записка.pdf

Чурсина_ 125-20-1_Презентація.pptx

Чурсина_ 125-20-1_Пояснювальна_записка.pdf.p7s

# ДОДАТОК Ж. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 94б («відмінно»).

Керівник розділу _____ Дар'я ПІЛОВА

(підпис) (ім'я, прізвище)

ДОДАТОК З. Відгук

на кваліфікаційну роботу бакалавра на тему:

«Комплексна система захисту інформації інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Мередіан»

студентки групи 125-20-1

Чурсиної Марії Кирилівни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 124 сторінках та містить 15 рисунків, 31 таблиця, 14 джерел та 9 додатків.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІКС товариства з обмеженою відповідальністю «Мередіан».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІКС, розробка моделі порушника, аналіз джерел загроз та вразливостей, визначення актуальних загроз, формування вимог до захисту інформації та розробка проектних рішень їх реалізації.

Запропоновано матрицю розмежування доступу, розроблені положення групової політики контролеру домену Active Directory. Розроблені проектні рішення впровадження резервного копіювання та криптографічного захисту інформації при використанні зовнішніх носіїв.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей товариства з обмеженою відповідальністю «Мередіан»..

До недоліків відноситься недостатньо обґрунтована модель загроз та профіль захищеності.

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

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

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

Кваліфікаційна робота заслуговує оцінки «_____».

**Керівник кваліфікаційної роботи, професор** **Котух Є.В.**

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