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 *Бабича Максима Павловича*

академічної групи *125-18ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс»*

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

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Бабичу Максиму Павловичу*** **академічної групи** ***125-18ск-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс»***

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

Розділ	Зміст	Термін виконання
Розділ 1	Розглянути підходи створення підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс»	29.03.2021
Розділ 2	Виконати обстеження на об'єкті інформаційної діяльності, та обрати метод розробки підсистеми захисту віддаленого доступу	24.05.2021
Розділ 3	Виконати розрахунки кінцевої вартості проекту, та розрахувати період окупності даного проекту після його реалізації	14.06.2021

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

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

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

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатка, __ джерел.

Об’єкт розробки: інформаційно-телекомунікаційна системи Товариство з обмеженою відповідальністю «Продуктсервіс».

Мета роботи: розробка підсистеми захисту віддаленого доступу на базі інформаційної системи ТОВ «Продуктсервіс».

У першому роділлі розглянуто підходи створення підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс».

У спеціальній частині виконано: обстеження на об’єкті інформаційної діяльності, та вибрано метод розробки підсистеми захисту віддаленого доступу.

В економічному розділі було виконано розрахунки кінцевої вартості проекту, та розраховано період окупності даного проекту після його реалізації.

Практична значення проекту полягає в об’єднанні територіально віддалених філій в один мережевий сегмент з центральним офісом, створення захищених каналів передачі даних, та можливість захисту інформації яка в них оброблюється.

АВТОМАТИЗОВАНА СИСТЕМА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, КОМПЛЕКСНА СИСТЕМА ЗАСОБІВ ЗАХИСТУ, ПРИВАТНА ВІРТУАЛЬНА МЕРЕЖА, МАТРИЦЯ ДОСТУПУ.

РЕФЕРАТ

Пояснительная записка: ___ стр., __ рис., __ табл., __ приложения, __ источников.

Объект разработки: информационно-телекоммуникационная системы Общество с ограниченной ответственностью «Продуктсервис».

Цель работы: разработка подсистемы защиты удаленного доступа на базе информационной системы ООО «Продуктсервис».

В первом роженицы рассмотрены подходы создания подсистемы защиты удаленного доступа в комплексной системе защиты информационно-телекоммуникационной системы ООО «Продуктсервис».

В специальной части выполнены: обследование на объекте информационной деятельности, и выбран метод разработки подсистемы защиты удаленного доступа.

В экономическом разделе было выполнено расчеты конечной стоимости проекта, и рассчитан период окупаемости данного проекта после его реализации.

Практическая значение проекта заключается в объединении территориально удаленных филиалов в один сетевой сегмент с центральным офисом, создание защищенных каналов передачи данных и возможность защиты информации, которая в них обрабатывается.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА, МОДЕЛИ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, КОМПЛЕКСНАЯ СИСТЕМА СРЕДСТВ ЗАЩИТЫ, ЧАСТНАЯ ВИРТУАЛЬНОЙ СЕТИ, МАТРИЦА ДОСТУПА.

ABSTRACT

Explanatory note: __ p., __ pic., __ tabl., __ application, __ sources.

Object of development: information and telecommunication systems of Limited Liability Company "ProductService".

Purpose: development of a subsystem for remote access protection on the basis of the information system of ProductService LLC.

In the first maternity hospital approaches of creation of a subsystem of protection of remote access in complex system of protection of information and telecommunication system of ProductService LLC are considered.

In the special part the following is performed: inspection at the object of information activity, and the method of development of the subsystem of protection of remote access is chosen.

In the economic section, the calculations of the final cost of the project were performed, and the payback period of this project after its implementation was calculated.

The practical significance of the project is to unite geographically remote branches into one network segment with the central office, to create secure data transmission channels, and the ability to protect the information processed in them.

AUTOMATED SYSTEM, THREAT MODEL, VIOLATION MODEL, COMPREHENSIVE PROTECTION SYSTEM, PRIVATE VIRTUAL NETWORK, ACCESS MATRIX.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

АРМ – автономне робоче місце;

АТС – автономна телефонна станція;

ЕЦП – електронно-цифровий підпис;

ІТС – інформаційна телекомунікаційна система;

ІС – інформаційна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КМ – комп'ютерна мережа;

КСЗІ – комплексні системи захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

РС – робоча станція;

ТЗ – технічні засоби;

ТЗІ – технічний захист інформації;

ТОВ – товариство з обмеженою відповідальністю.

ЗМІСТ

ВСТУП

На даний момент часу існує істотна проблема передачі інформації з обмеженим доступом по відкритим каналам зв’язку. Ця проблема існує в організація у яких інформаційна система побудована на базі територіально віддалених філій та центрального офісу де між ними здійснюється інформаційний обмін.

Метою роботи є розробка підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс».

Галузь застосування даного проекту є товариство з обмеженою відповідальністю «Продуктсервіс», та аналогічні йому за інформаційною системою підприємства, організації та установи.

При міжмережевій взаємодії між територіально віддаленими об'єктами компанії постає завдання забезпечення безпеки інформаційного обміну між клієнтами і серверами різних мережевих служб. Подібні проблеми мають місце і в бездротових локальних мережах (Wireless Local Area Network, WLAN), а також при доступі віддалених абонентів до ресурсів корпоративної інформаційної системи. В якості основної загрози тут розглядається несанкціоноване підключення до каналів зв'язку та здійснення перехоплення (прослуховування) інформації і модифікація (підміна) передаються по каналам даних (поштові повідомлення, файли, тощо).

Для захисту даних, переданих по зазначеним каналам зв'язку, необхідно використовувати відповідні засоби криптографічного захисту. Криптоперетворення можуть здійснюватися як на прикладному рівні (або на рівнях між протоколами додатків і протоколом TCP/IP), так і на мережевому (перетворення IP-пакетів).

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Комплексна система захисту інформації

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Основні елементи КСЗІ наведені в таблиці 1.1.

Таблиця 1.1 – Основні елементи КСЗІ

Комплексна система захисту інформації	
Організаційні заходи	Складання посадових інструкцій
	Створення правил адміністрування компонент інформаційної системи
	Розробка планів дій у разі виявлення спроб несанкціонованого доступу
	Навчання правилам інформаційної безпеки користувачів
Інженерно-технічні заходи	Система контролю і управління доступом
	Розмежування потоків інформації
	Засоби шифрування
	Систем охоронно-пожежної сигналізації

Організаційні заходи є обов'язковою складовою побудови будь КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності.

Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів;

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, проведена реорганізація системи діловодства та зберігання документів.

Інженерно - технічні заходи - сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно – технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити. Інженерно-технічні заходи, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу.

У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.

Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

Суб'єкти КСЗІ. У процес створення КСЗІ залучаються наступні сторони:

- організація, для якої здійснюється побудова КСЗІ (Замовник);
- організація, що здійснює заходи з побудови КСЗІ (Виконавець);
- державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) (Контролюючий орган);
- організація, в разі необхідності залучена замовником або виконавцем для виконання деяких робіт по створенню КСЗІ (Підрядник).

Об'єктами захисту КСЗІ є інформація, в будь-якому її вигляді і формі подання.

Матеріальними носіями інформації є сигнали. По своїй фізичній природі інформаційні сигнали можна розділити на такі види: електричні, електромагнітні, акустичні, а також їх комбінації.

Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видах коливань, причому інформація, яка підлягає захисту, міститься в їх змінюються параметрах.

Етапи побудови КСЗІ. У побудові КСЗІ можна виділити наступні етапи:

1 Підготовка організаційно-розпорядчої документації.

2 Обстеження інформаційної інфраструктури Замовника.

3 Розробка "Плану захисту інформації.

4 Розробка «Технічного завдання на створення КСЗІ».

5 Розробка «Технічного проекту на створення КСЗІ».

6 Приведення інформаційної інфраструктури Замовника у відповідність з «Технічним проектом на створення КСЗІ».

7 Розробка «Експлуатаційної документації на КСЗІ».

8 Впровадження КСЗІ.

9 Випробування КСЗІ.

10 Проведення державної експертизи КСЗІ і отримання «Атестата відповідності».

11 Підтримка і обслуговування КСЗІ.

1.2 Автоматизована система

Автоматизована система (АС) – це організаційно-технічна система, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювальну інформацію.

Згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу», автоматизовані системи поділяються на наступні класи (залежно від технології обробки і передачі інформації):

АС класу «1» - одномашинний однокористувацький комплекс, який оброблює інформацію однієї або декількох ступенів обмеження доступу.

АС класу «2» - локалізований багатомашинний багатокористу- вацький комплекс, який обробляє інформацію різних ступенів обмеження доступу.

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

1.3 Віддалений доступ до інформаційних ресурсів

При міжмережевій взаємодії між територіально віддаленими об'єктами компанії постає завдання забезпечення безпеки інформаційного обміну між клієнтами і серверами різних мережевих служб. Подібні проблеми мають місце і в бездротових локальних мережах (Wireless Local Area Network, WLAN), а також при доступі віддалених абонентів до ресурсів корпоративної інформаційної системи. В якості основної загрози тут розглядається несанкціоноване підключення до каналів зв'язку та здійснення перехоплення (прослуховування) інформації і модифікація (підміна) передаються по каналам даних (поштові повідомлення, файли, тощо).

Для захисту даних, переданих по зазначеним каналам зв'язку, необхідно використовувати відповідні засоби криптографічного захисту. Криптоперетворення можуть здійснюватися як на прикладному рівні (або на рівнях між протоколами додатків і протоколом TCP / IP), так і на мережевому (перетворення IP-пакетів).

У першому варіанті шифрування інформації, призначеної для транспортування по каналу зв'язку через неконтрольовану територію, повинно здійснюватися на вузлі-відправнику (робочої станції - клієнті або сервері), а дешифровка – на вузлі-одержувачі. Цей варіант передбачає внесення істотних змін в конфігурацію кожної взаємодіючої сторони

(підключення засобів криптографічного захисту до прикладних програм або комунікаційної частини операційної системи), що, як правило, вимагає великих витрат і установки відповідних засобів захисту на кожен вузол локальної мережі. До рішень даного варіанту відносяться протоколи SSL, S-HTTP, S/MIME, PGP/MIME, які забезпечують шифрування і цифровий підпис листів і повідомлень, переданих з використанням протоколу HTTP.

Другий варіант передбачає установку спеціальних засобів, що здійснюють криптоперетворення в точках підключення локальних мереж та віддалених абонентів до каналів зв'язку (мереж загального користування), що проходить по неконтрольованої території. При вирішенні цього завдання необхідно забезпечити необхідний рівень криптографічного захисту даних і мінімально можливі додаткові затримки при їх передачі, так як ці засоби тунелюють передаваємий трафік (додають новий IP-заголовок до тунелюємого пакету) і використовують різні за стійкістю алгоритми шифрування.

У зв'язку з тим, що засоби, які забезпечують криптоперетворення на мережевому рівні повністю сумісні з будь-якими прикладними підсистемами, що працюють в корпоративній інформаційній системі (є «прозорими» для додатків), то вони найбільш часто і застосовуються.

1.4 Технологія Virtual Private Network

VPN (Virtual Private Network - віртуальна приватна мережа) – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

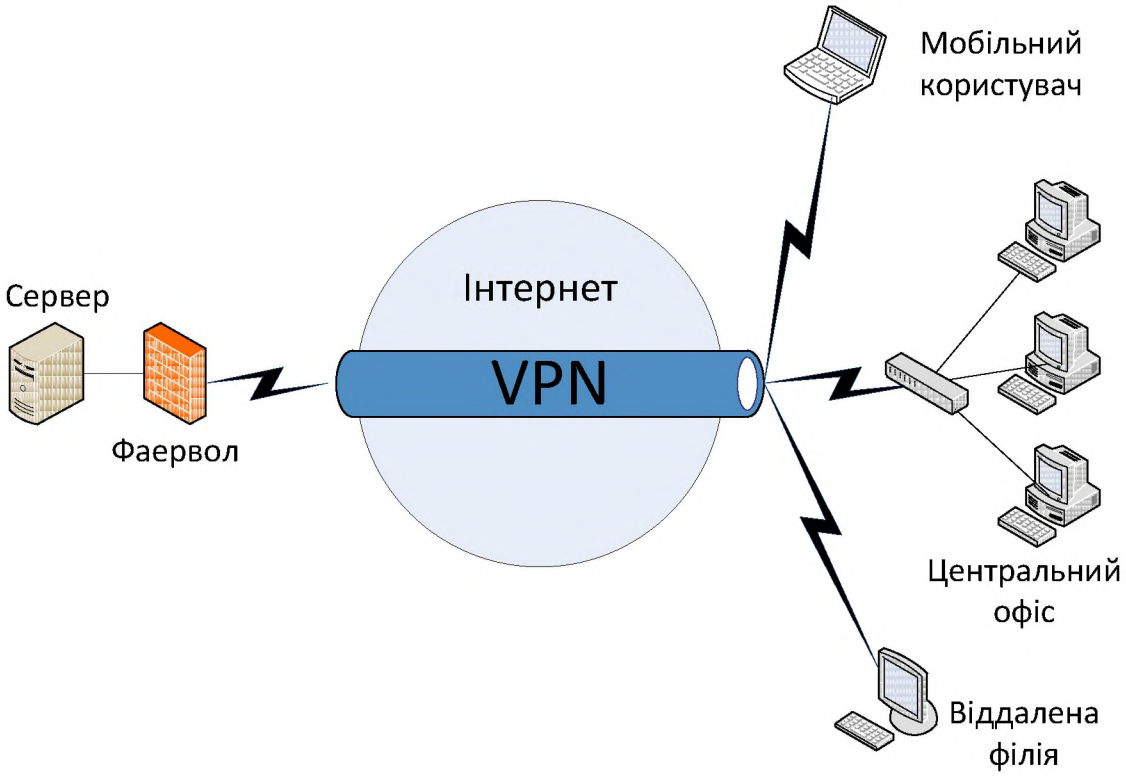


Рисунок 1.1 – Схема VPN

Суть VPN полягає в наступному:

- На всі комп'ютери, що мають вихід в Інтернет, встановлюється засіб, що реалізовує VPN (VPN-агент). Не повинно залишитися жодного незахищеного.

- VPN-агенти автоматично шифрують всю вихідну інформацію (і відповідно розшифровують всю вхідну). Вони також стежать за її цілісністю за допомогою ЕЦП або імітоприставок (криптографічна контрольна сума, розрахована з використанням ключа шифрування). Оскільки інформація, що циркулює в Інтернеті, являє собою безліч пакетів протоколу IP, VPN-агенти працюють саме з ними.

Перед відправкою IP-пакету VPN-агент діє таким чином:

- З декількох підтримуваних їм алгоритмів шифрування і ЕЦП по IP-адресі одержувача вибирає потрібний для захисту даного пакету, а також ключі. Якщо ж в його настройках такого одержувача немає, то інформація не відправляється.

- Визначає і додає в пакет ЕЦП відправника або імітоприставку.

- Шифрує пакет (цілком, включаючи заголовок).

- Проводить інкапсуляцію, тобто формує новий заголовок, де вказується адреса зовсім не одержувача, а його VPN-агента. Ця корисна додаткова функція дозволяє представити обмін між двома мережами як обмін всього лише між двома комп'ютерами, на яких встановлені VPN-агенти. Будь-яка корисна для темних цілей зловмисника інформація, наприклад внутрішні IP-адреси, йому вже недоступна.

При отриманні IP-пакету виконуються зворотні дії:

- Заголовок містить відомості про VPN-агента відправника. Якщо такий не входить в список дозволених в настройках, то інформація просто відкидається. Те ж саме відбувається при прийомі пакету з навмисно або випадково пошкодженим заголовком.

- Згідно налаштувань вибираються алгоритми шифрування і ЕЦП, а також необхідні криптографічні ключі.

- Пакет розшифровується, потім перевіряється його цілісність. Якщо ЕЦП невірна, то він викидається.

- І, нарешті, пакет в його початковому вигляді відправляється справжньому адресату по внутрішній мережі.

Всі операції виконуються автоматично. Складною в технології VPN є тільки настройка VPN-агентів, яка, цілком під силу досвідченому користувачеві. VPN-агент може знаходитися безпосередньо на захищаємому ПК, що корисно для мобільних користувачів, що підключаються до Інтернет. У цьому випадку він забезпечить обмін даними тільки того комп'ютера, на якому він встановлений.

Можливе поєднання VPN-агента з маршрутизатором (в цьому випадку його називають криптографічним) IP-пакетів. До речі, провідні світові виробники останнім часом випускають маршрутизатори з вбудованою підтримкою VPN, наприклад Express VPN від Intel, який шифрує всі що проходять пакети по алгоритму Triple DES.

Як видно з опису, VPN-агенти створюють канали між захищеними мережами, які зазвичай називають «тунелями». І дійсно, вони «прориті» через

Інтернет від однієї мережі до іншої, в яких циркулює інформація захована від чужих очей.

Крім того, всі пакети "фільтруються" відповідно до настройок. Таким чином, всі дії VPN-агентів можна звести до двох механізмів: створення тунелів і фільтрації пакетів які передаються.

Сукупність правил створення тунелів, яка називається "політикою безпеки", записується в настройках VPN-агентів. IP-пакети прямують в той або інший тунель або відкидаються після того, як будуть перевірені:

- IP-адреса джерела (для вихідного пакету - адреса конкретного комп'ютера мережі, що захищається);
- IP-адреса призначення;
- протокол більш високого рівня, якому належить даний пакет (наприклад, TCP або UDP);
- номер порту, з якого або на який відправлена інформація (наприклад, 1080);

1.5 Обстеження на об’єкті інформаційної діяльності

1. Обстеження на ОІД проведено комісією, призначеною розпорядженням по установі, згідно із затвердженою програмою обстеження.
2. Відомості про ОІД:

1.5.1 Загальна характеристика ОІД

Об’єктом інформаційної діяльності являється товариство з обмеженою відповідальністю «Продуктсервіс».

Вид діяльності: роздрібна торгівля харчовими продуктами, побутовою хімією, малими побутовими приладами, елементами одягу. Діяльність підприємства представлена у вигляді мережі супермаркетів, має єдиний центральний офіс.

Фізична адреса центрального офісу: 49000, Україна, Дніпропетровська обл.. м. Дніпро, пров. Аеропортний, буд. 21.

Юридична адреса центрального офісу: 49000, Україна, Дніпропетровська обл.. м. Дніпро, пров. Аеропортний, буд. 21.

1. Характеристика складових ОІД

Контрольована зона обмежена стінами будівлі центрального офісу, та стінами серверних приміщень віддалених відділень підприємства. Забезпечується приватним охоронним агентством на підставі укладеного договору.

Характеристики будівлі центрального офісу:

- центральний офіс ТОВ «Продуктсервіс» розташований в трьох поверховій будівлі, в будівлі мається підвальне приміщення, загальна площа офісного приміщення – приблизно 2025 м^2.
- стіни, та несучі конструкція – монолітна залізобетонна конструкція, товщина 350 мм.
- перекриття між поверхами виконане з пустотних залізобетонних плит
- внутрішні перестінки виконані з гіпсокартону на металевому каркасі, товщиною 150 мм.
- стеля – підвісна, загальна висота від підлоги 300 см., висота міжстелевого проміжку 20 см. (на першому поверсі), 50 см. (на другому та третьому поверхах).
- підлога в приміщеннях офісу покрита кахельною плиткою.
- вікна – металопластикові пакети з двійним склом.
- фасадні двері виконані з металопластику з подвійним склом, тильні виконані з металу та дерева.
- встановлена автономна система опалювання.
- системи електропостачання, водопостачання та каналізації – централізовані. Входять до будівлі через підвальне приміщення, виходять за межі КЗ.

Таблиця 1.2 – Специфікація приміщень будівлі ТОВ «Продуктсервіс»

Номер приміщення	Назва відділу, який займає кабінет
1	Хол. На 1-му поверсі. Рецепція
2	Коридорне приміщення
3	Гардеробна
4	Зал для проведення конференцій
5	Столове приміщення
6	Тамбур, тильний вихід
7	Міжповерховий перехід
8	Кабінет завідуючого складом
9	Санітарний вузол
10	Кімната охорони
11	Технічне приміщення
12	Відділ кадрів
13	Серверна кімната
14	Велика зала(2-й поверх)
15	Кабінет служби безпеки
16	Кабінет системного адміністратора
17	Договірний відділ
18	Фінансовий відділ
19	Відділ торгівлі
20	Кабінет директора
21	Секретар
22	Замісник директора
23	Економісти
24	Відділ маркетингу
25	Бухгалтерія

Режими роботи підприємства:

На підприємстві п’яти денний робочий тиждень. Два вихідних (субота, неділя). Понеділок – п’ятниця: 8:00 – 17:00, Обідня перерва: 12:00 – 13:00

Фізичне середовище

ТОВ «Продуктсервіс» має підключення до телефонної лінії компанії «Укртелеком», має три номери. Для організації телефонної мережі

використовується офісна АТС на 16 номерів. Телефонна лінія має вихід за межі КЗ.

Система електропостачання підключена до централізованої мережі, до підстанції котра знаходиться в 200 м. від будівлі. Має трьох фазний ввід, в підвальному приміщенні встановлено лічильник, шафу автоматики, та шафу запобіжників. Електропроводка розведена по всій будівлі кабелем типа «ШВВП 3х1.5». Лінія електропостачання має вихід за межі КЗ.

Система заземлення виконана згідно норм, має вихід за межі КЗ.

Водопостачання до будівлі підводиться з центральної лінії через підвал будівлі, в підвалі на вводі розташований кран поменшання тиску. Лінія системи водопостачання виходить за межі КЗ.

Газопостачання здійснюється до будівлі через металеву трубу, яка виходить з центральної лінії і входить до будинку через перший поверх і опускається до підвального приміщення котельної. Має вихід за межі КЗ.

Система стічної каналізації підключена до централізованої мережі, система виконана з пластикових труб, та переходів діаметром 100 мм. Має вихід за межі КЗ.

Підприємство має автономну систему опалення, з власною котельною в підвальному приміщенні.

В приміщеннях будівлі існує система вентиляції та кондиціонування повітря. В приміщеннях встановлено вентиляційні канали, які підключено до витяжок, також в кожному приміщенні в якому працюють люди встановлено кондиціонери.

В будівлі встановлено пожежну сигналізацію, у відповідності з проектної документації. Систему пожежної сигналізації виведено на моніторинг до приватного централізованого пульту пожежної охорони «Захист». Підприємства співпрацюють на базі укладеного договору.

В будівлі встановлено охоронну сигналізацію. Систему виведено на централізований пульт охорони.

Інформаційне середовище

Всі робочі станції об'єднані в комп'ютерну мережу з сервером. Вся інформація яка оброблюється на робочих станціях зберігається на сервері. Робочі станції підключені до мережі через мережеві комутатори. До серверу підключено модем, за допомогою якого мається можливість виходу до глобальної мережі Internet. Комп'ютерна мережа построєна на базі технології Fast Ethernet, має топологію «зірка.

Таблиця 1.3 – Характеристики апаратного забезпечення

Параметр	Значення (не нижче)
АРМ	
Процесор	Intel Core i3 3.10 GHz
ОЗУ	8 Гб
Об'єм жорсткого диску	500Gb
Материнська плата	Gigabyte H-61
Блок живлення	400Wt FSP
Привід	Відсутній
Відео	Intel HD Graphics
Порти	4xUSB 2.0, PS/2, Card reader
Мережа	1000 mbps
Додатково	Клавіатура + мишка в комплекті.
Монітор	23" Samsung
Сервер	
Процесор	Intel Xeon 3420
ОЗУ	32Gb пам'яті
Об'єм жорсткого диску	Два SATA диска
Порти	Два порти Gigabit Ethernet
Привід	DVD
Блок живлення	1 блок живлення 800Wt FSP
Комутаційне обладнання	
Комутатор	D-Link DGS-1100-24, D-Link DGS-1210-16, TP-LINK TL-SG2109WEB
Маршрутизатор	TP-LINK TD-8817

Кожна РС має свою унікальну IP адресу, своє мережеве ім'я, інвентарний номер, відповідального за РС. Перелік РС станцій наведено в таблиці 2.4.

Таблиця 1.4 – Перелік РС

№ п\п	IP адреса	Мережеве ім'я	Відповідальна особа
1	192.168.5.101	Director	Відповідальна особа 1
2	192.168.5.102	ZamDir	Відповідальна особа 2
3	192.168.5.103	Secretar	Відповідальна особа 3
4	192.168.5.104	Kadry	Відповідальна особа 4
5	192.168.5.105	SB	Відповідальна особа 5
6	192.168.5.106	Admin	Відповідальна особа 6
7	192.168.5.107-192.168.5.108	Fin1-Fin2	Відповідальна особа 7
8	192.168.5.109-192.168.5.110	Ekonom1-Ekonom2	Відповідальна особа 8
9	192.168.5.111-192.168.5.112	Dogovor1-Dogovor2	Відповідальна особа 9
10	192.168.5.113-192.168.5.114	Sklad1-Sklad2	Відповідальна особа 10
11	192.168.5.115-192.168.5.117	Byhgalt1-Byhgalt3	Відповідальна особа 11
12	192.168.5.118-192.168.5.120	Torg1-Torg3	Відповідальна особа 12
13	192.168.5.121-192.168.5.124	Market1-Market4	Відповідальна особа 13
14	192.168.5.125-192.168.5.130	Konferenc1-Konferenc6	Відповідальна особа 14

В інформаційній системі ТОВ «Продуктсервіс» використовується програмне забезпечення декількох типів (загальносистемне ПЗ, прикладне ПЗ, спеціалізоване ПЗ). Програмне забезпечення також можна розподілити на те яке встановлене на АРМ та сервері. Характеристики ПЗ представлені в таблиці 2.5.

Таблиця 1.5 – Характеристики програмного забезпечення

Тип ПЗ	Найменування	Значення	Ліцензія
АРМ			
Загально системне та прикладне ПЗ	Операційна система (ОС)	MS Windows 7 Ultimate	З № 11AC-JF12-448D-2LG9-0B43-8912 –по № 11AC-JF12-448D-2LG9-0B43-8962

Продовження таблиці 1.5

Тип ПЗ	Найменування	Значення	Ліцензія
	Офісний пакет	MS Office 2010, «1С Бухгалтерия 8», WinRAR	MS Office 2010 (З № 001S-G678-54KL-3514-RTY7-N128 – по № 001S-G678-54KL-3514-RTY7-N168), 1С Бухгалтерия 8 (має ліцензію на 30 користувачів), WinRAR(ліцензія на 50 PC)
Спеціальне ПЗ	Антивірусне, мережеве ПЗ	«AVAST PRO антивірус»	З № 1200EQ6FAA-8215 – по № 1200EQ6FAA-8265
	Клієнтські програми спеціалізованої СКБД	СКДБ розроблена на замовлення(ведення БД товарів на складах)	Без ліцензії
Сервер			
Загально системне та прикладне ПЗ	Операційна система (ОС)	MS Windows Server 2012.	№ 52FF-D8XA-1100-58LX-S741-89F1
	Офісний пакет	MS Office 2010, «1С Бухгалтерия 8»,	MS Office 2010(№ 001S-G678-54KL-3514-RTY7-N126), «1С Бухгалтерия 8»(одна серверна ліцензія)
Спеціальне ПЗ	Антивірусне, мережеве ПЗ	«AVAST PRO антивірус»,	1200EQ6FAA-8214
	Серверні програми спеціалізованої системи управління БД	СКДБ розроблена на замовлення(ведення БД товарів на складах)	Без ліцензії

На підприємстві працюють робітники різних відділів. Список робітників наведено в таблиці 1.6.

Таблиця 1.6 – Список робітників ТОВ «Продуктсервіс»

№ п\п	Відділ	Посада
1	Керівники	Директор
2	Керівники	Замісник директора
3	Бухгалтерія	Головний бухгалтер
4	Бухгалтерія	Бухгалтер
5	Бухгалтерія	Бухгалтер
6	Фінансовий відділ	Головний фінансист
7	Фінансовий відділ	Фінансист
8	Економічний відділ	Головний економіст
9	Економічний відділ	Економіст
10	Відділ торгівлі	Головний менеджер
11	Відділ торгівлі	Менеджер
12	Відділ торгівлі	Менеджер
13	Відділ маркетингу	Головний маркетолог
14	Відділ маркетингу	Маркетолог
15	Відділ маркетингу	Рекламний агент
16	Відділ маркетингу	Рекламний агент
17	Відділ кадрів	Кадровик
18	Договірний відділ	Юрист
19	Договірний відділ	Юрист
20	Склад	Комірник
21	Склад	Комірник
22	Склад	Вантажник
23	Склад	Вантажник
24	Склад	Вантажник
25	Склад	Вантажник
26	Секретар	Секретар
27	Обслуговуючий персонал	Прибиральниця
28	Служба безпеки	Адміністратор безпеки
29	Обслуговуючий персонал	Системний адміністратор

Види інформації яка циркулює в ІС системі підприємства:

- відкрита (загальнодоступна) інформація;
- інформація з обмеженим доступом (персональні данні, комерційна таємниця);

Перелік інформації з обмеженим доступом:

1 Договірна інформація (договори з постачальниками, банками, транспортними компаніями тощо);

2 Бухгалтерські документи (документи бухгалтерської звітності);

3 Фінансова інформація (плани фінансових затрат та інше);

4 Економічна інформація (економічні показники, розрахунки, стратегічні ходи тощо);

5 Банківські реквізити;

6 Касова документація (накладні, касові ордери);

7 Прайсова інформація (прайс листи від постачальників та інщі);

8 Проектні документи (розроблювані проекти тощо);

9 Рекламна інформація (рекламні проекти та інше);

10 Індивідуальні данні робітників;

11 Податкові документи (звіти);

12 Бізнес плани, ідеї;

13 Складська інформація(залишки на складах тощо).

Класифікація інформації з обмеженим доступом.

Інформацію з обмеженим доступом класифікували за трьома критеріями:

- конфіденційність (К0-К4);
- цілісність (Ц0-Ц4);
- доступність (Д0-Д4);

Пояснення критеріїв:

- К0 - розголошення інформації призводить до припинення роботи підприємства, або дуже великих збитків.
- К1- розголошення призводить до значних збитків, якщо не буде вжито заходів.

- К2 - розголошення призведуть до деяких збитків, що може призвести до перебоїв в роботі.
- К3 - підприємство зазнає незначних збитків.
- К4 - може принести малозначний збиток в рідкісних випадках.
- Ц0 - призводить до неправильної роботи підприємства в цілому, або значної її частини і наслідки зміни незворотні.
- Ц1 - несанкціоновані зміни, призводять до неправильної роботи підприємства через деякий час, якщо не буде вжито заходів. Наслідки незворотні.
- Ц2 - несанкціоновані зміни призводять до збоїв в роботі підприємства, можуть призвести до не стабільної роботи.
- Ц3 - несанкціоновані зміни призводять до зміни показників на негативні, незначна нестабільність підприємства.
- Ц4 - несанкціоноване зміни не нанесуть збитків підприємству.
- Д0 - в разі порушення доступності підприємство зазнає сильних збитків. Має можливість припинити свою діяльність.
- Д1 - в разі порушення підприємство зазнає значної нестабільності в роботі.
- Д2 - в разі порушення підприємство зазнає незначних перебоїв в роботі, які не призведуть до значних змін.
- Д3 - в разі порушення робочий процес підприємства не зазнає великого збитку, можливі незначні перебої в роботі.
- Д4 - в разі порушення підприємство не зазнає перебоїв в роботі та збитків, але втрачену інформацію потрібно буде поновити.

Таблиця 1.7 – Класифікація інформації з обмеженим доступом1

Тип інформації з обмеженим доступом	Рівень конфіденційності інформації	Рівень цілісності інформації	Рівень доступності інформації
Договірна інформація	К3	Ц0	Д3
Бухгалтерські документи	К3	Ц2	Д4

Фінансова інформація	К3	Ц0	Д3
Економічна інформація	К2	Ц1	Д2

Продовження таблиці 1.7

Тип інформації з обмеженим доступом	Рівень конфіденційності інформації	Рівень цілісності інформації	Рівень доступності інформації
Банківські реквізити	К4	Ц0	Д3
Касова документація	К3	Ц1	Д3
Прайсова інформація	К3	Ц2	Д3
Проектні документи	К3	Ц1	Д3
Рекламна інформація	К4	Ц2	Д3
Індивідуальні данні робітників	К3	Ц2	Д3
Податкові документи	К4	Ц0	Д1
Бізнес плани, ідеї	К2	Ц1	Д2
Складська інформація	К3	Ц2	Д2

Інформаційні потоки на ОІД ТОВ «Продуктсервіс».

Інформаційний обмін в ІС реалізується по каналам зв'язку, розташованих в рамках КЗ, та каналами зв'язку, котрі виходять за рамки КЗ. Канали зв'язку котрі виходять за межі КЗ можуть представляти собою як виділені, так і загально доступні канали зв'язку.

Канали зв'язку, розташовані в рамках КЗ, представляють собою:

- Канали зв'язку між АРМ користувачів построєні з використанням комутаційного обладнання.

- Канал зв'язку, організований на використанні зйомник носіїв інформації для передачі даних між АРМ користувачів, та передачі друкованої інформації.

Опис інформаційних потоків підприємства: вся інформація оброблюється робочими станціями які входять до складу ІС ТОВ «Продуктсервіс», передається по каналам зв'язку на сервер де зберігається. На віддалених філіях

на початку робочого періоду інформація завантажується з серверу, а в кінці робочого періоду поновлюється, вносяться зміни, зберігається на сервері.

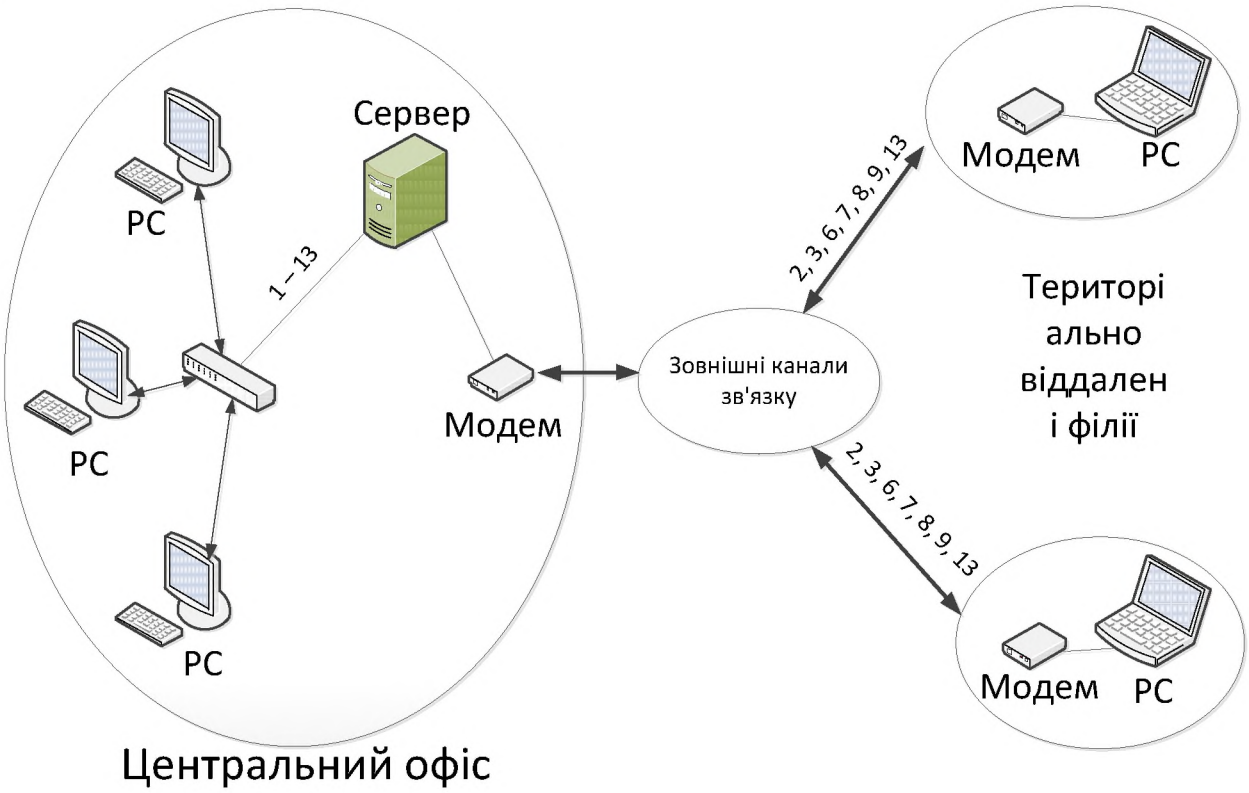


Рисунок 1.2 – Схема інформаційних потоків

1.5.2 Схеми розміщення комунікацій

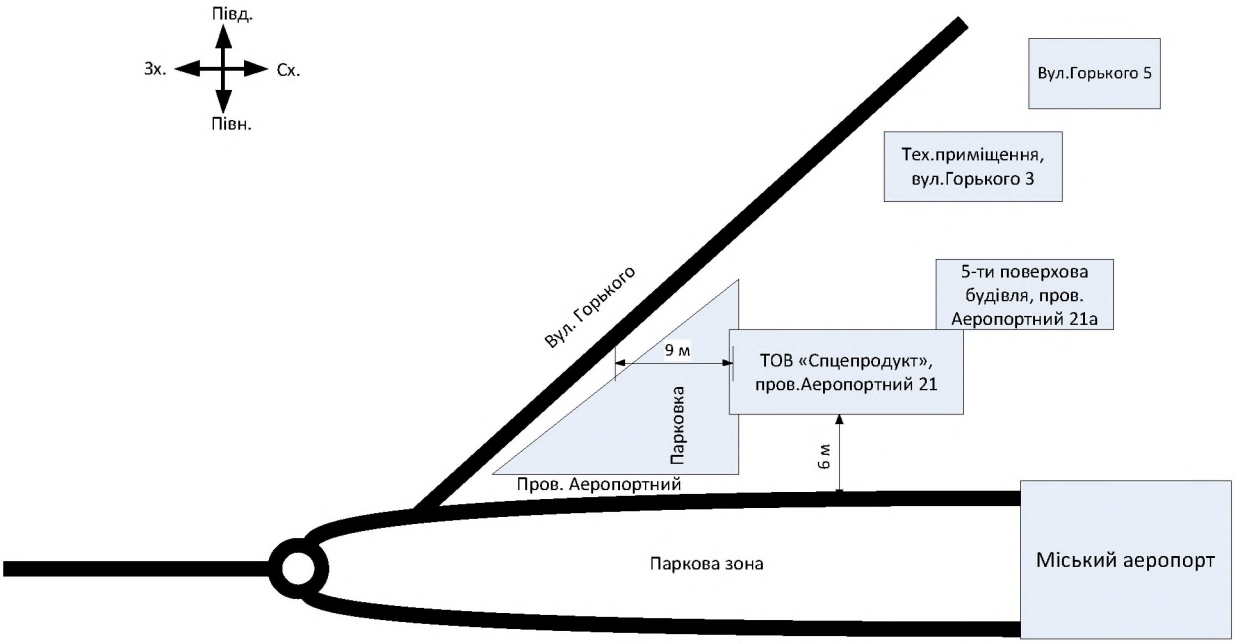


Рисунок 1.3 – Ситуаційний план

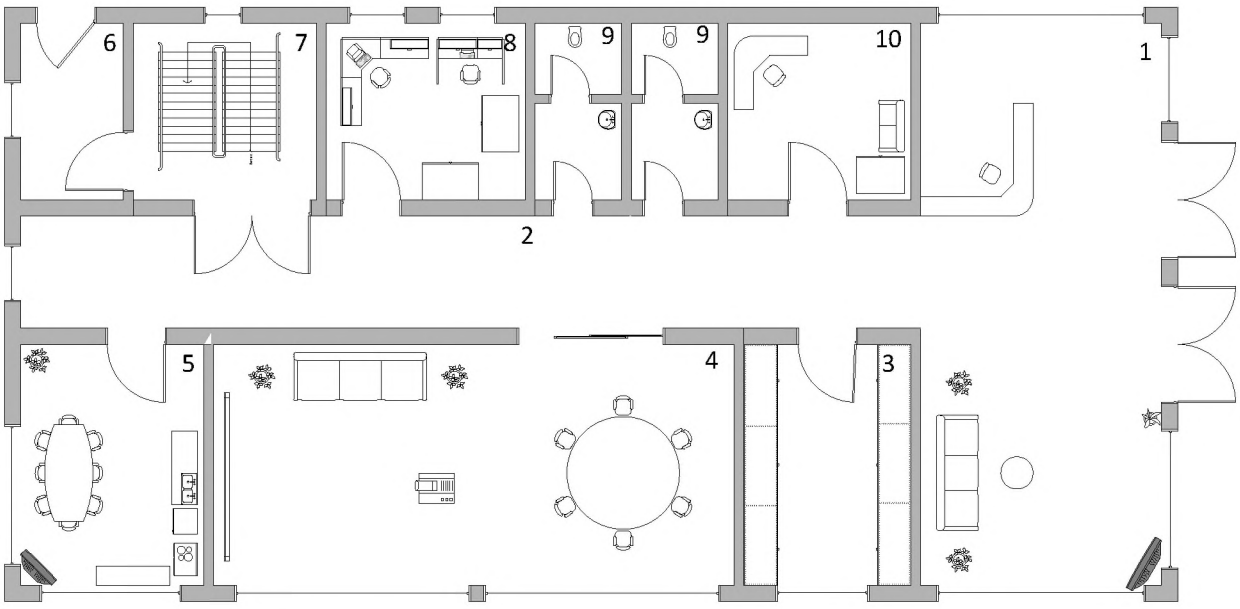


Рисунок 1.4 – Генеральний план 1-го поверху

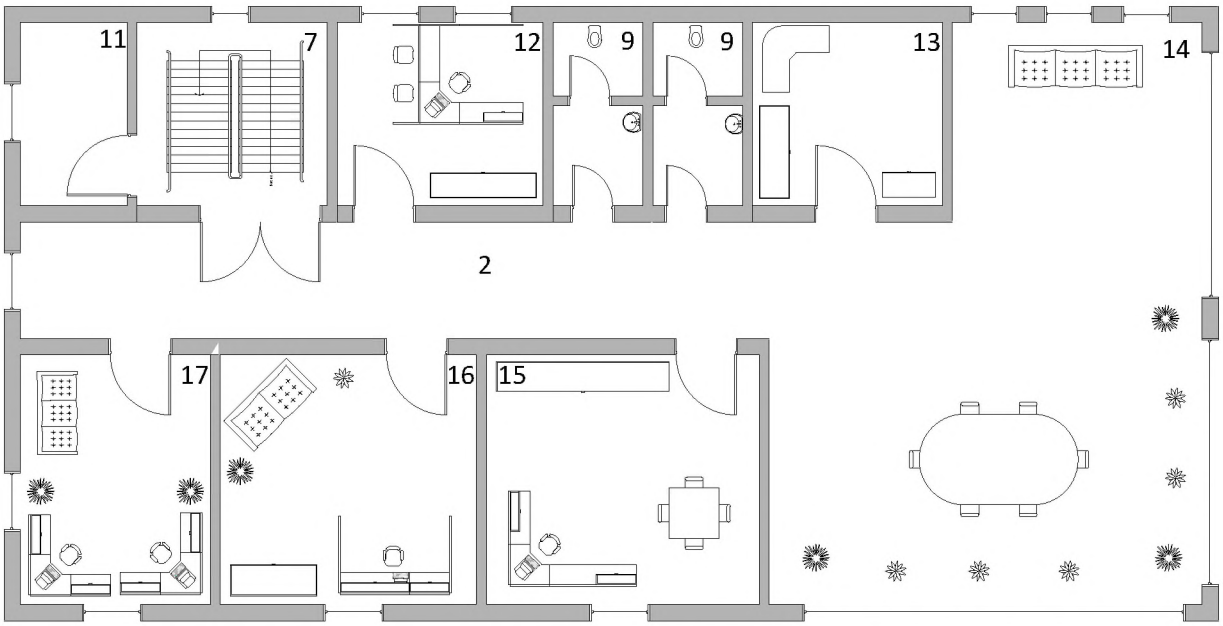


Рисунок 1.5 – Генеральний план 2-го поверху

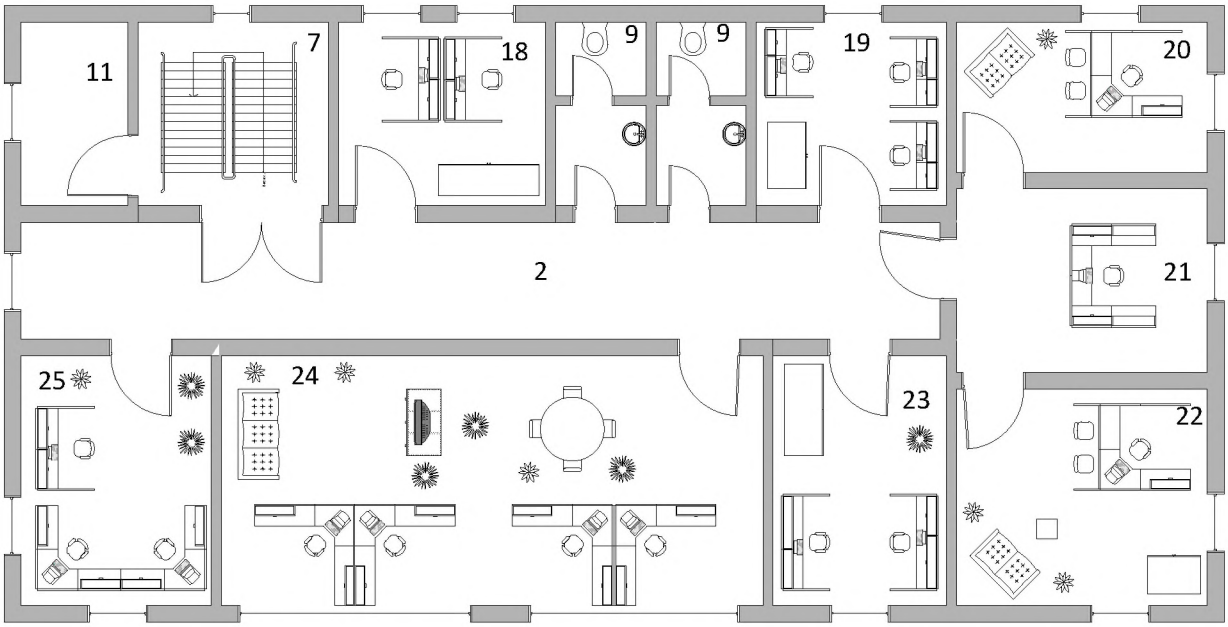


Рисунок 1.6 – Генеральний план 3-го поверху

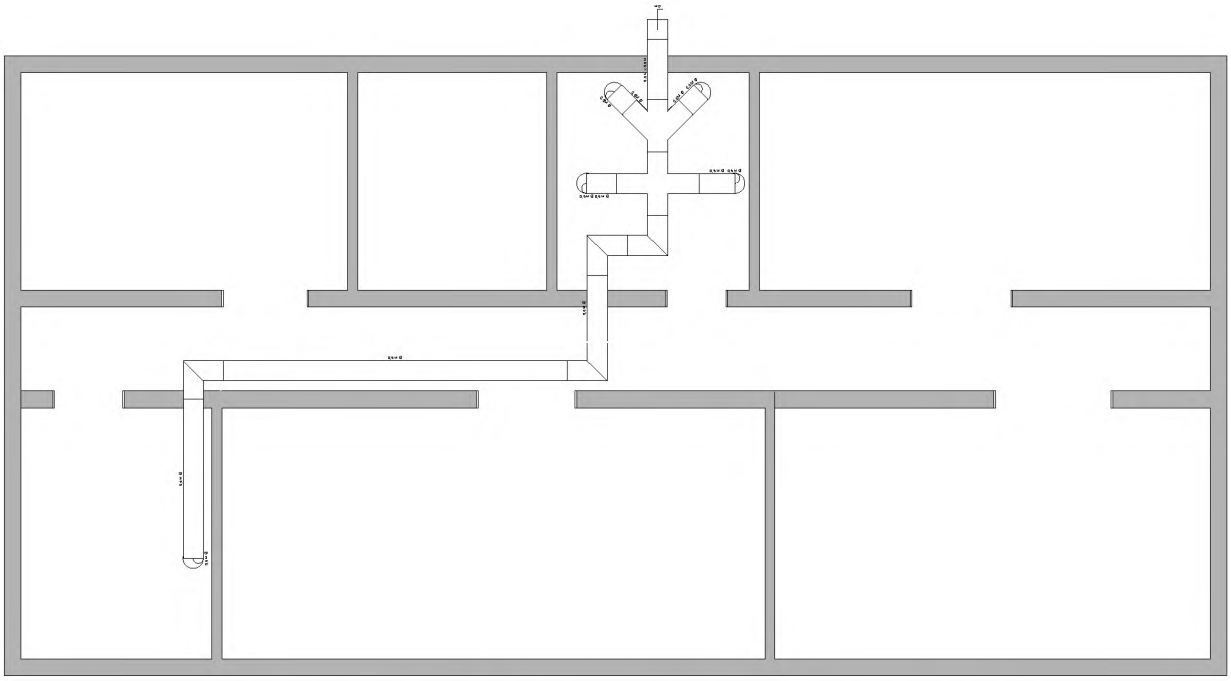


Рисунок 1.7 – Схема каналізаційних комунікацій

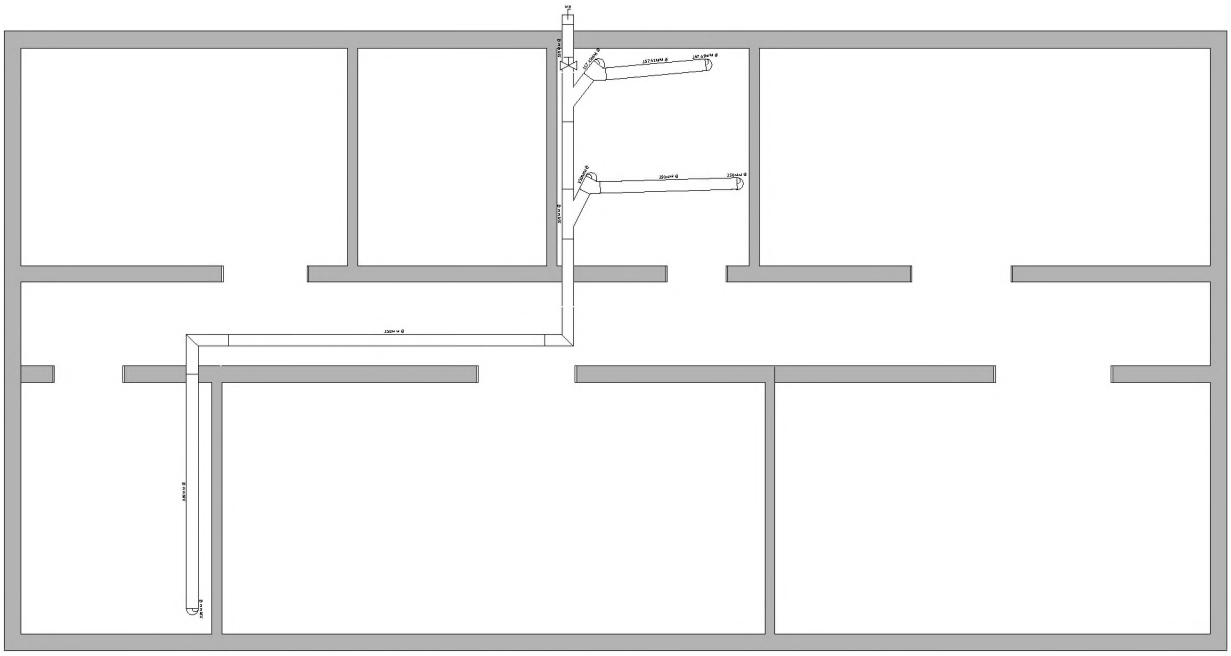


Рисунок 1.8 – Схема комунікацій водопостачання

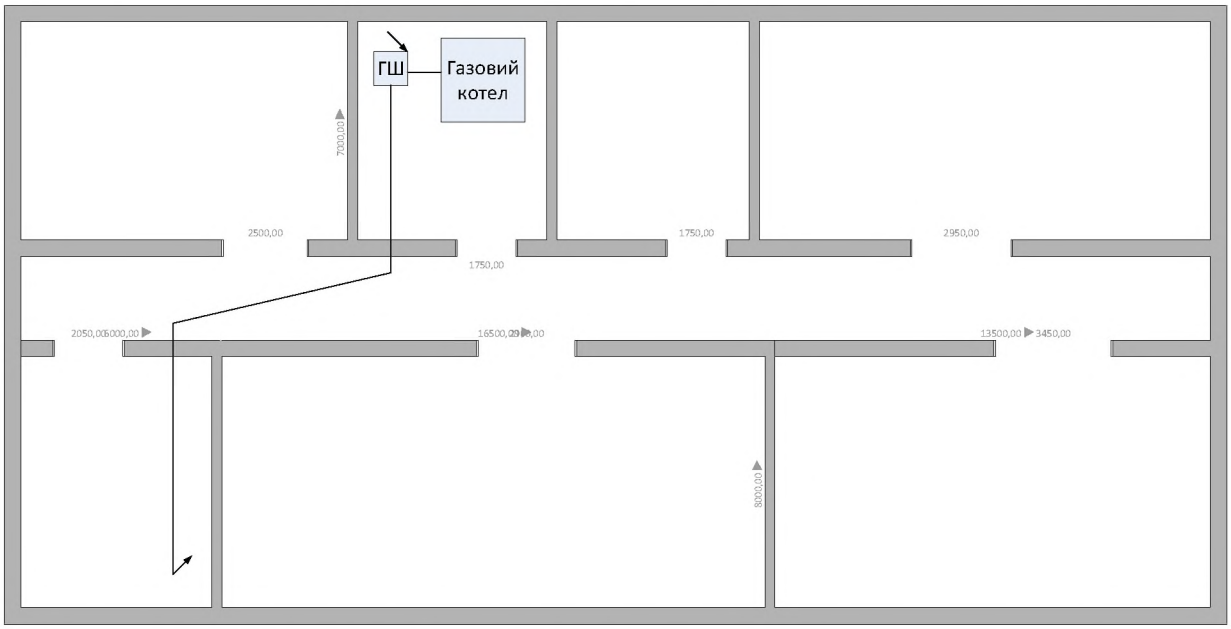
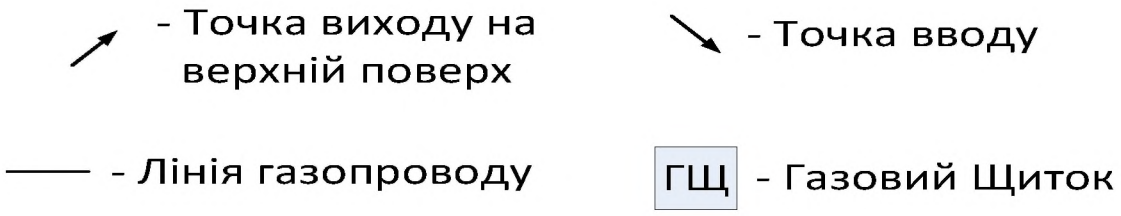


Рисунок 1.9 – Схема комунікацій системи газопостачання



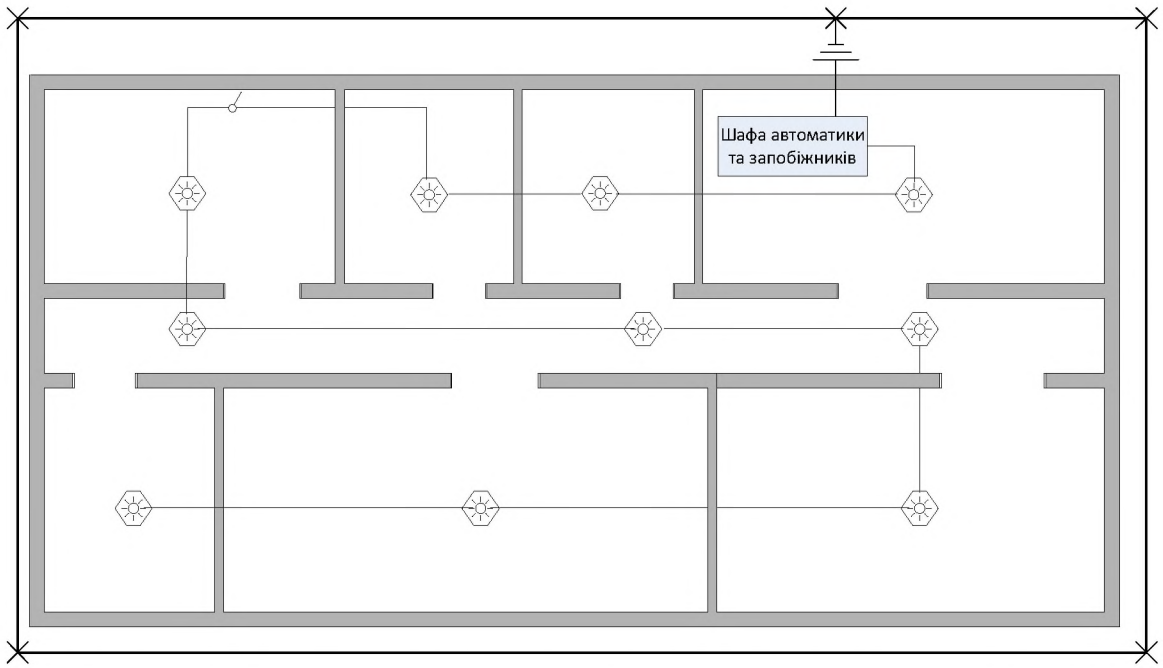


Рисунок 1.10 – Схема заземлення та електроживлення в підвалі

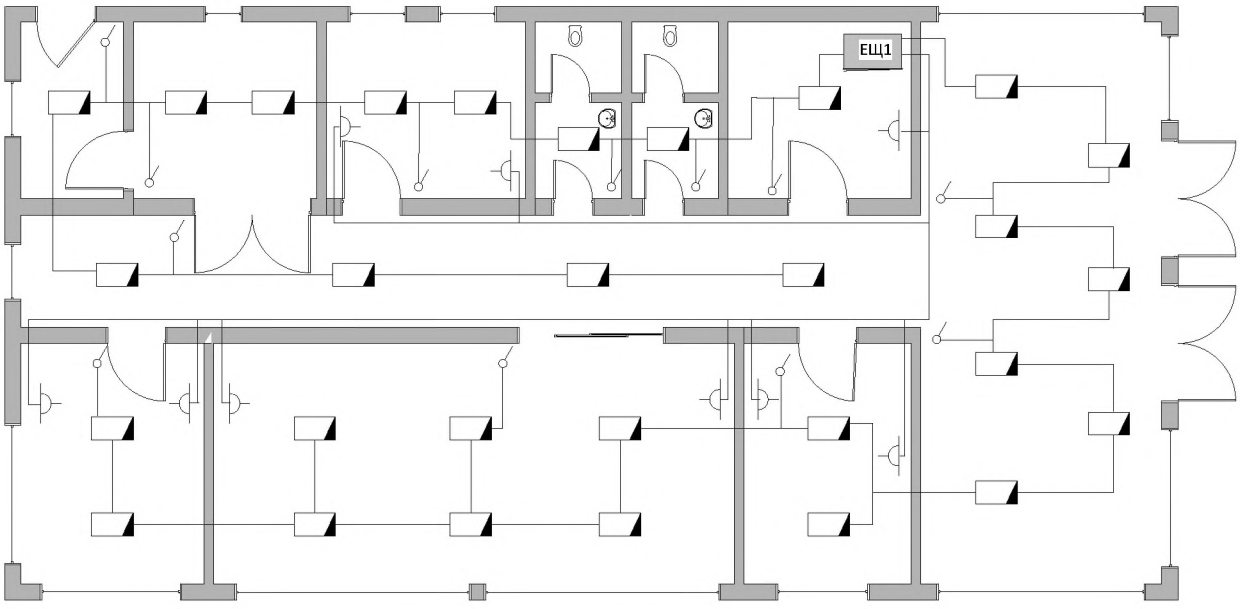
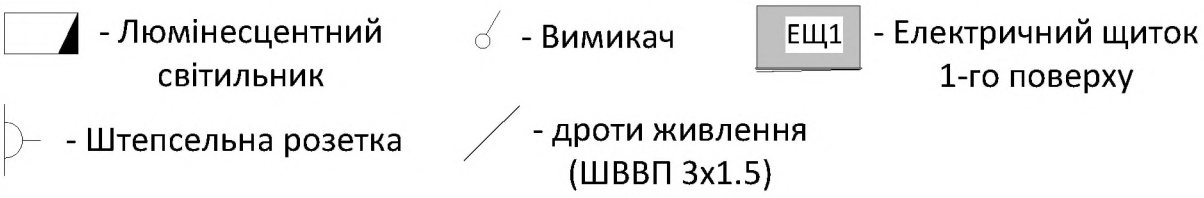


Рисунок 1.11 – Схема електричних комунікацій першого поверху



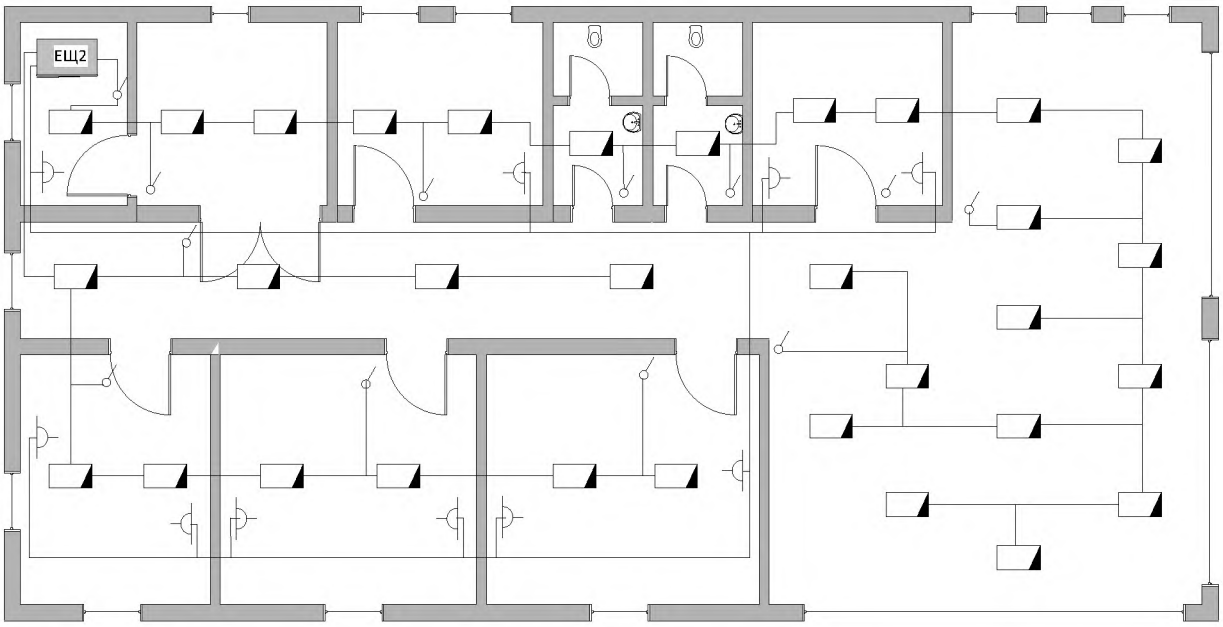


Рисунок 1.12 – Схема електричних комунікацій другого поверху

- Люмінесцентний світильник
- Вимикач
ЕЩ2 - Електричний щиток 2-го поверху
- Штепсельна розетка
- дроти живлення (ШВВП 3х1.5)

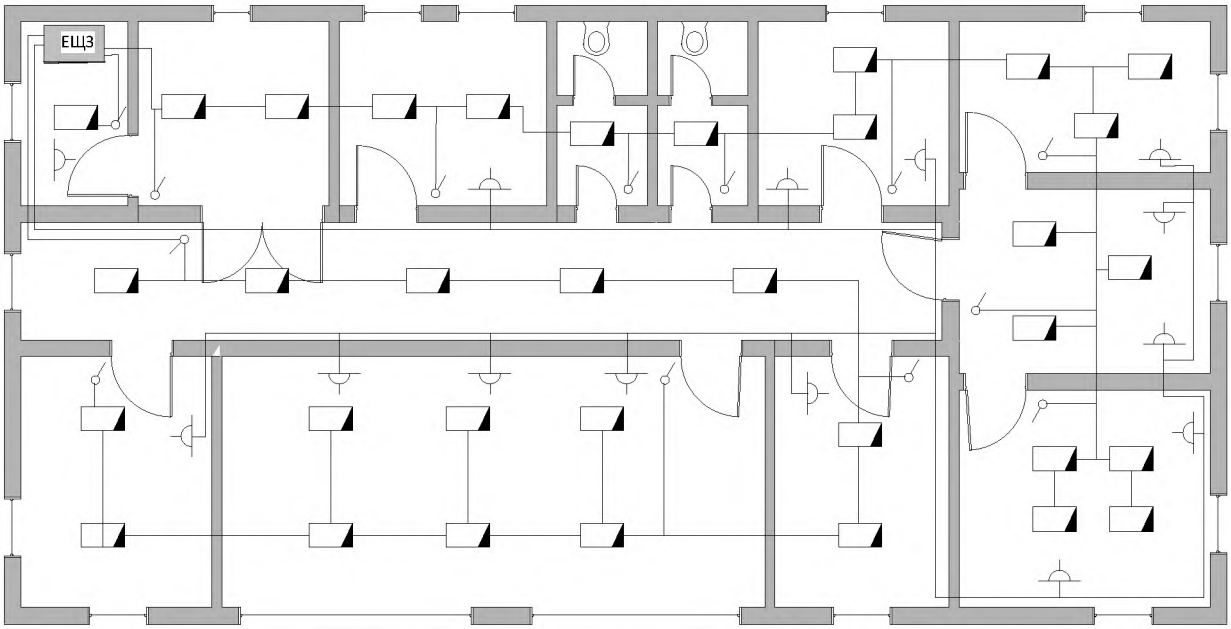


Рисунок 1.13 – Схема електричних комунікацій третього поверху

- Люмінесцентний світильник
- Вимикач
ЕЩ3 - Електричний щиток 3-го поверху
- Штепсельна розетка
- дроти живлення (ШВВП 3х1.5)

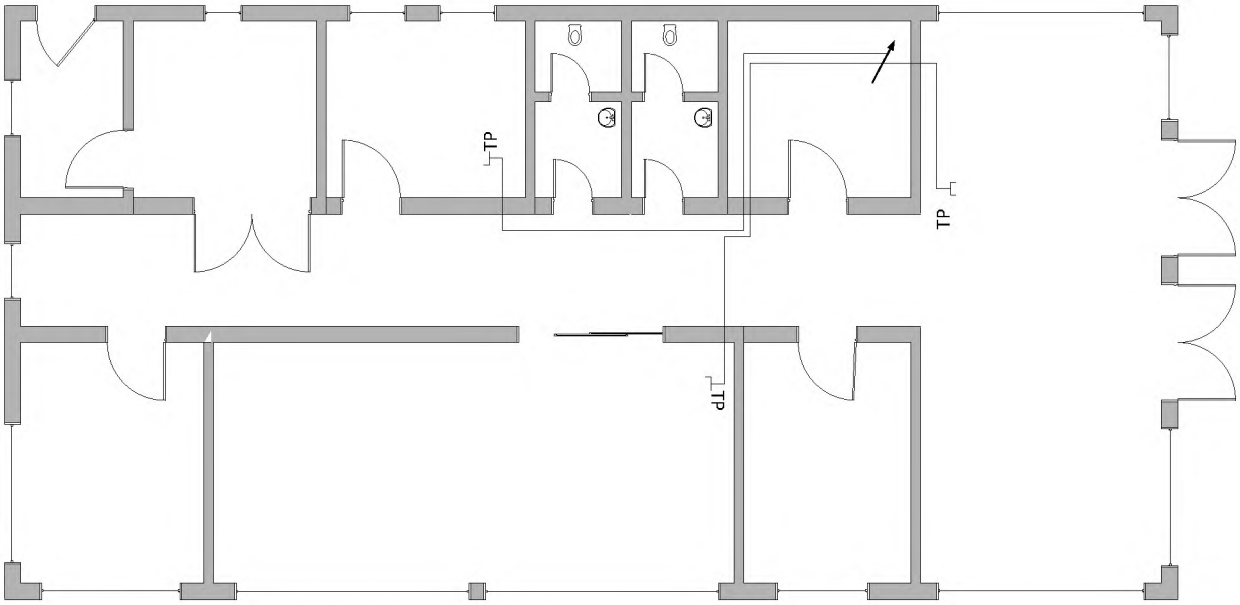


Рисунок 1.14 – Схема ліній телефонного зв’язку першого поверху

TP - Телефонна розетка

- з'єднувальні дроти

- Місце виходу з верхнього поверху

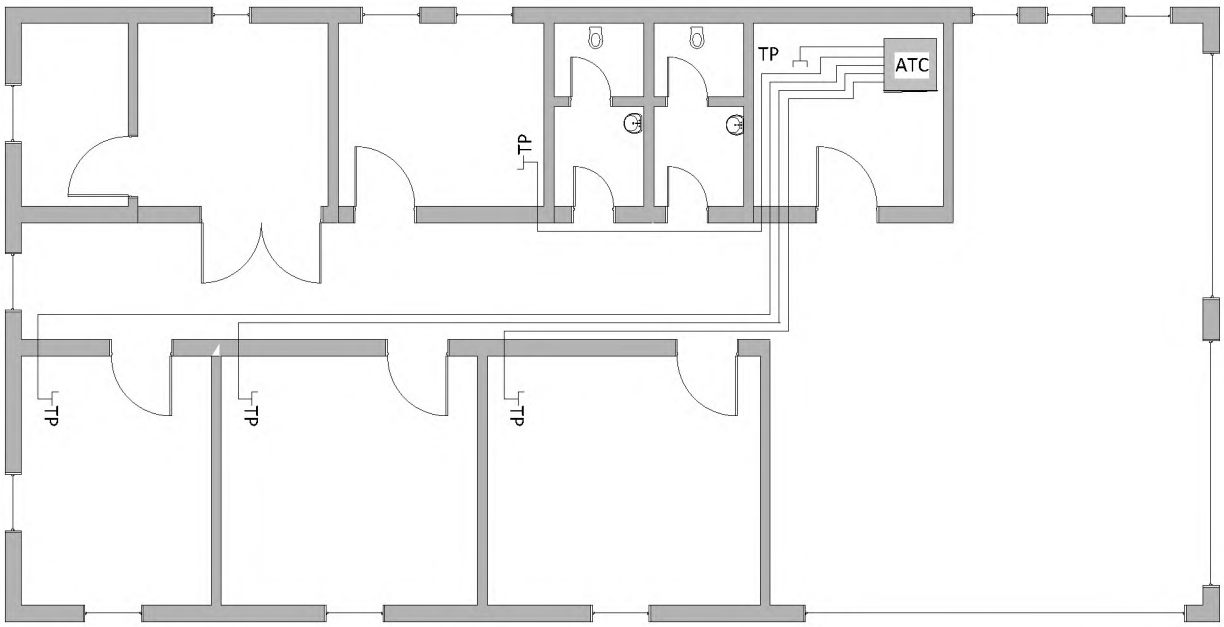


Рисунок 1.15 – Схема ліній телефонного зв’язку другого поверху

TP - Телефонна розетка

- з'єднувальні дроти

АТС - АТС (4х16)

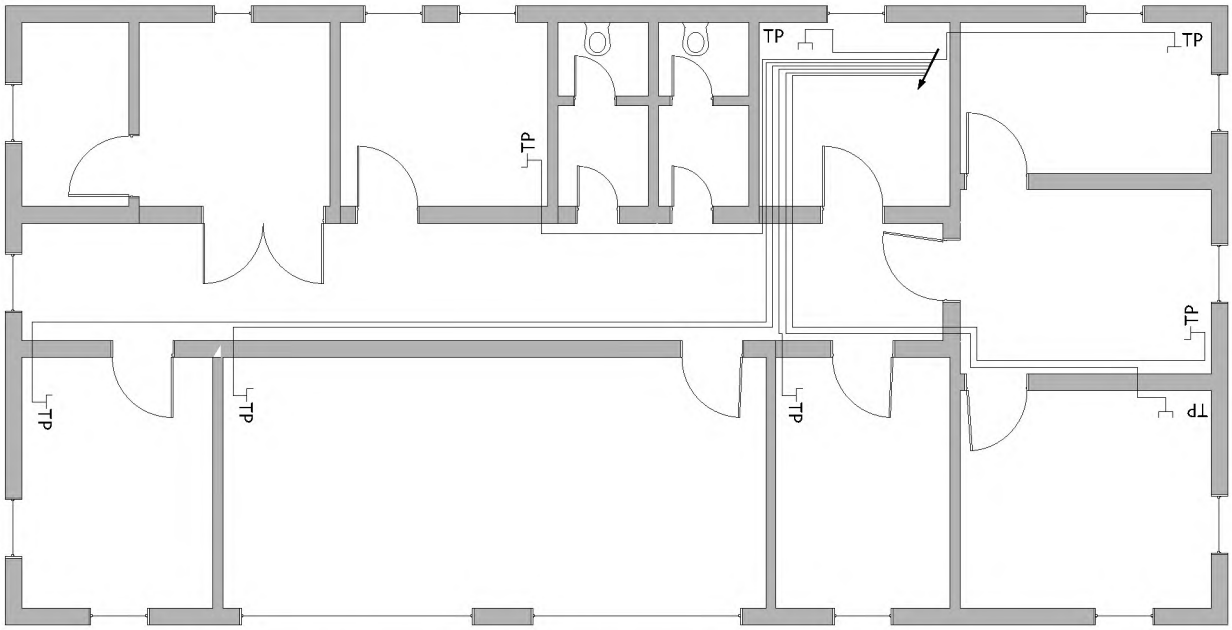


Рисунок 1.16 – Схема ліній телефонного зв’язку третього поверху

ТР - Телефонна розетка

- з'єднувальні дроти

- Місце виходу з нижнього поверху

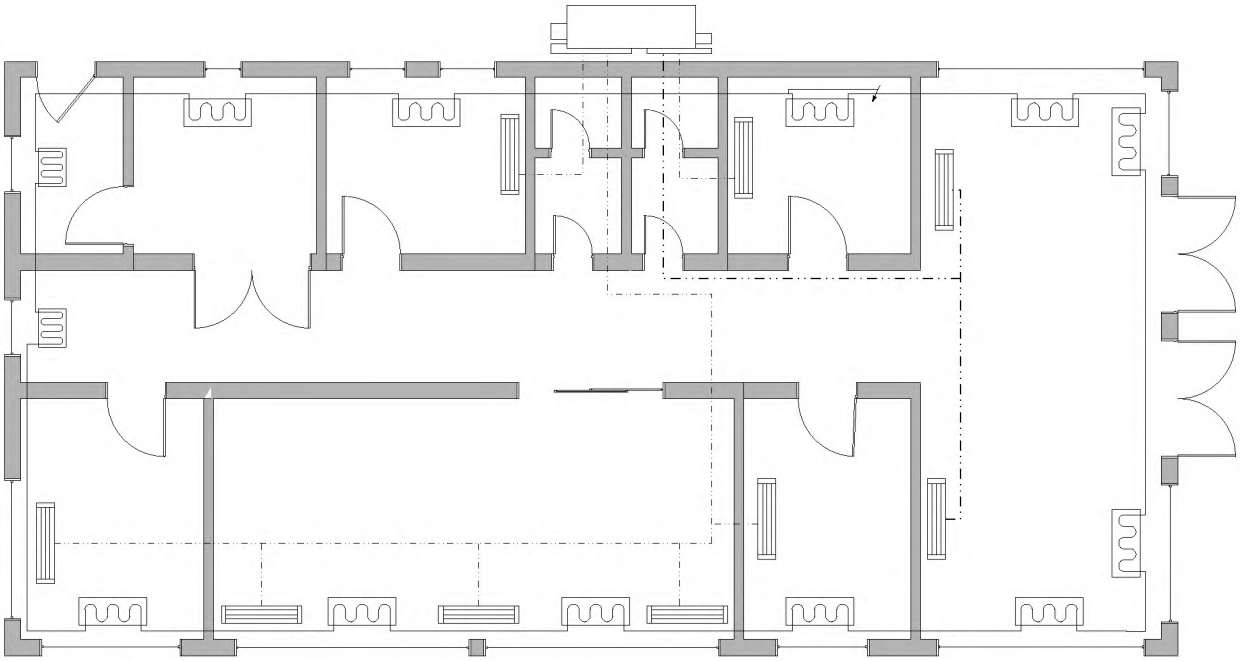


Рисунок 1.17 – Схема систем опалення та кондиціонування 1-го поверху

- Труби системи кондиціонерів

- Батарея

- Кондиціонер

- компресорна установка системи кондиціонерів

- Місце виходу з нижнього поверху

- Труби системи опалення

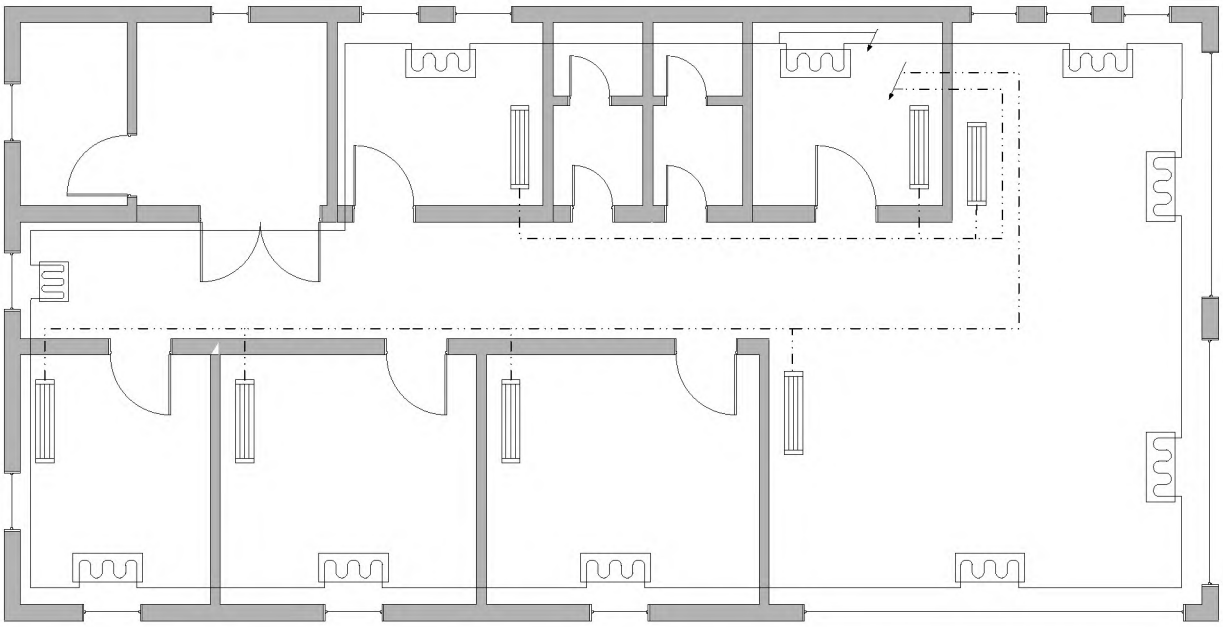


Рисунок 1.18 – Схема систем опалення та кондиціонування 2-го поверху

- Труби системи кондиціонерів

- Батарея

- Кондиціонер

- Місце виходу з нижнього поверху

- Труби системи опалення

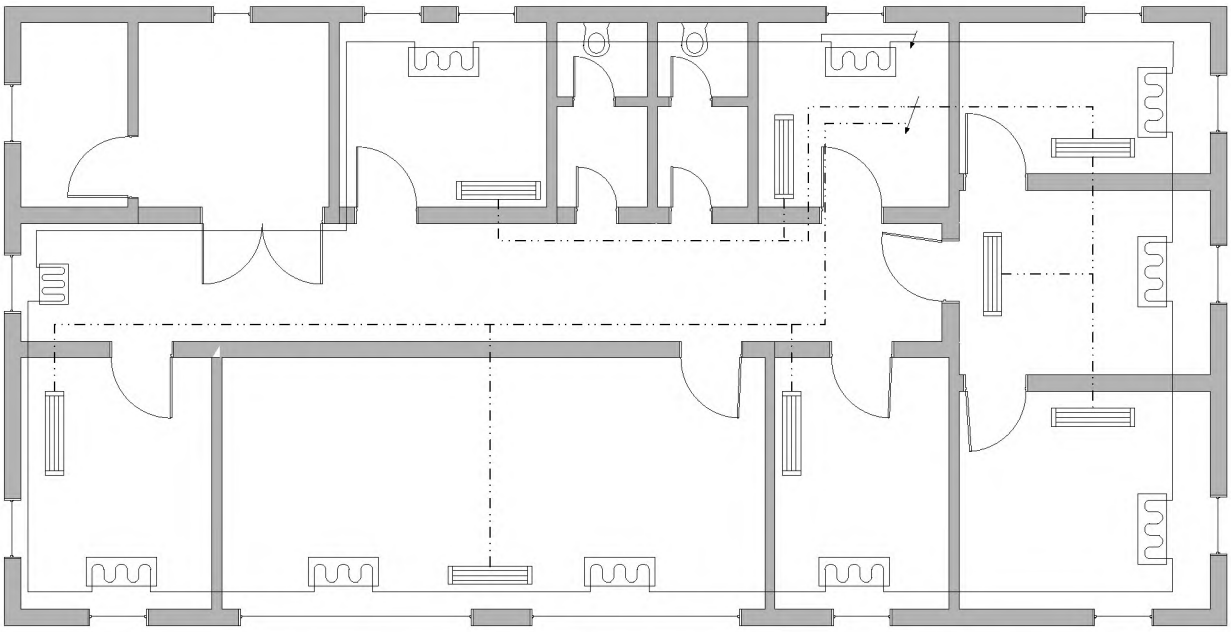


Рисунок 1.19 – Схема систем опалення та кондиціонування 3-го поверху

- Труби системи кондиціонерів

- Батарея

- Кондиціонер

- Місце виходу з нижнього поверху

- Труби системи опалення

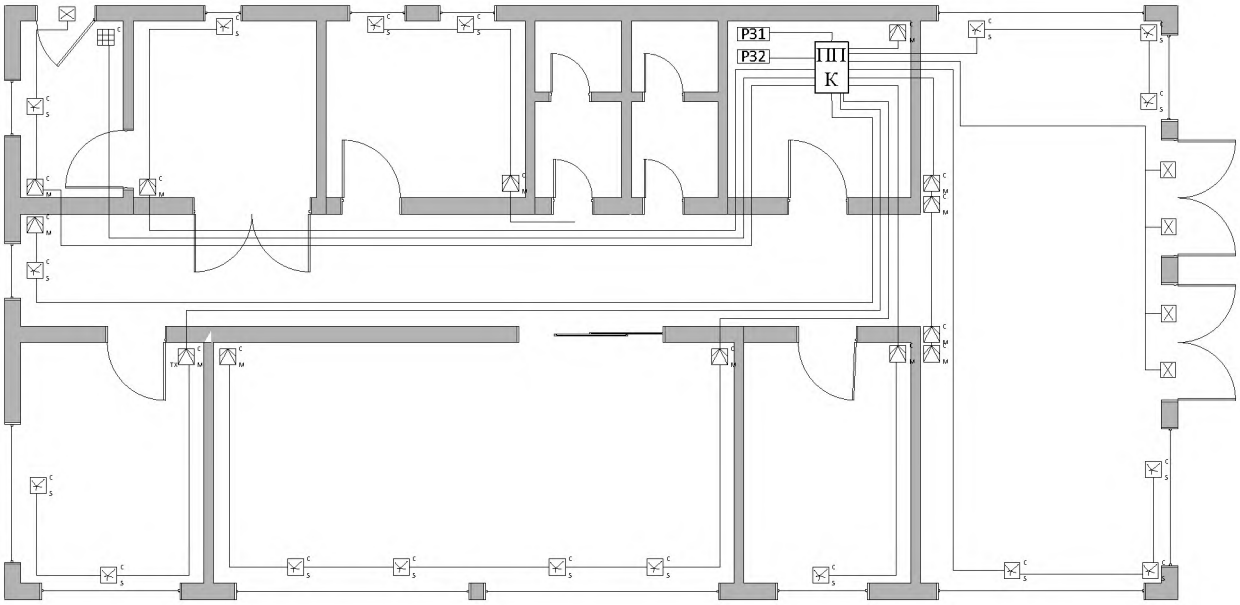


Рисунок 1.20 – Схема охоронної сигналізації 1-го поверху

- Сповіщювач магніто-контактний
- Сповіщювач пасивний інфрачервоний
- Сповіщювач пошкодження скла
- Центральний прибор «Texecom 832»
- Розширювач входів
- Клавіатура

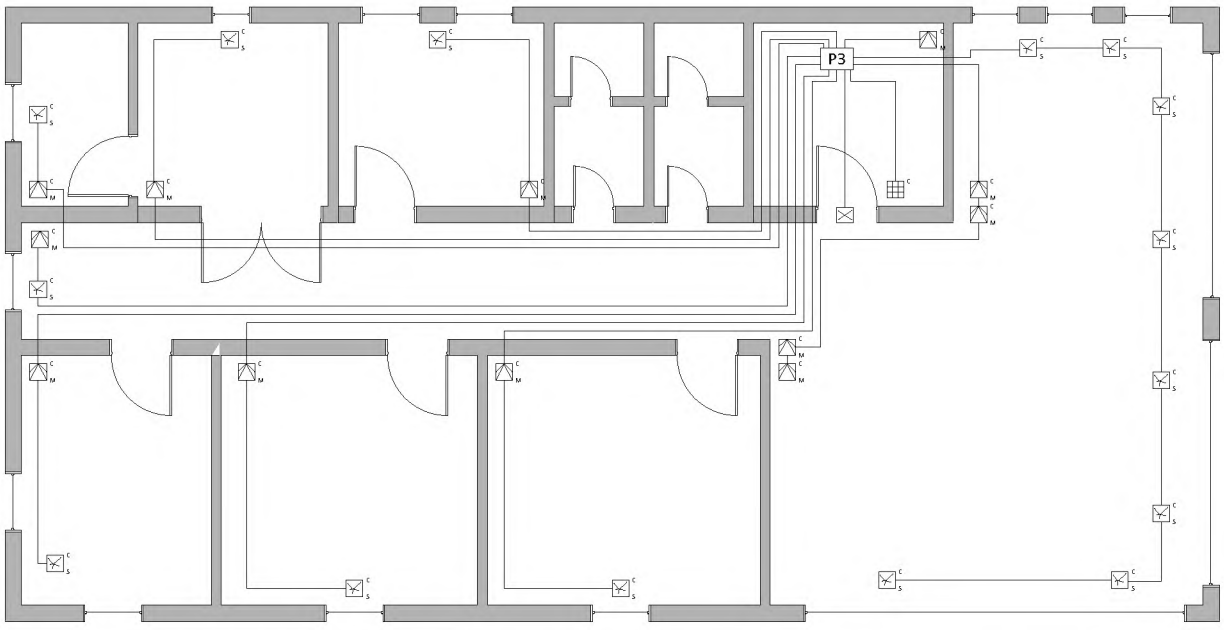


Рисунок 1.21 – Схема охоронної сигналізації 2-го поверху

- Сповіщювач магніто-контактний
- Сповіщювач пасивний інфрачервоний
- Сповіщювач пошкодження скла
- Розширювач входів
- Клавіатура

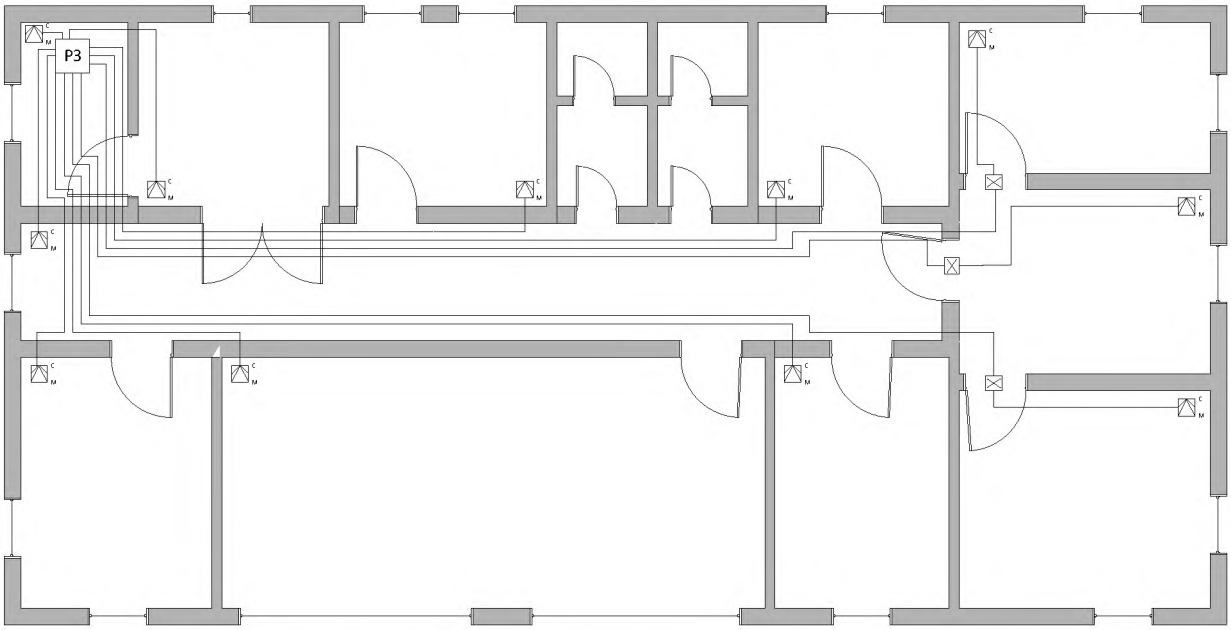


Рисунок 1.22 – Схема охоронної сигналізації 3-го поверху

- Сповіщювач магніто-контактний

РЗ - Розширювач входів

- Сповіщювач пасивний інфрачервоний

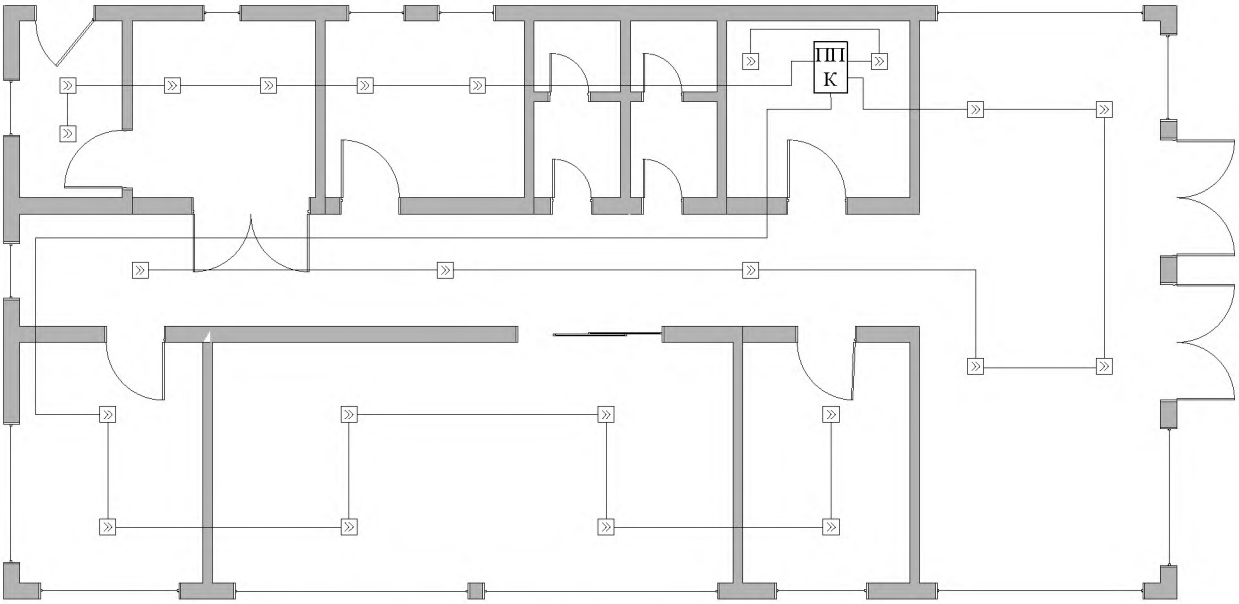


Рисунок 1.23 – Схема пожежної сигналізації 1-го поверху

- Сповіщювач магніто-контактний

ПП
К
- Центральний прибор «Тирас 16П»

РЗ - Розширювач входів

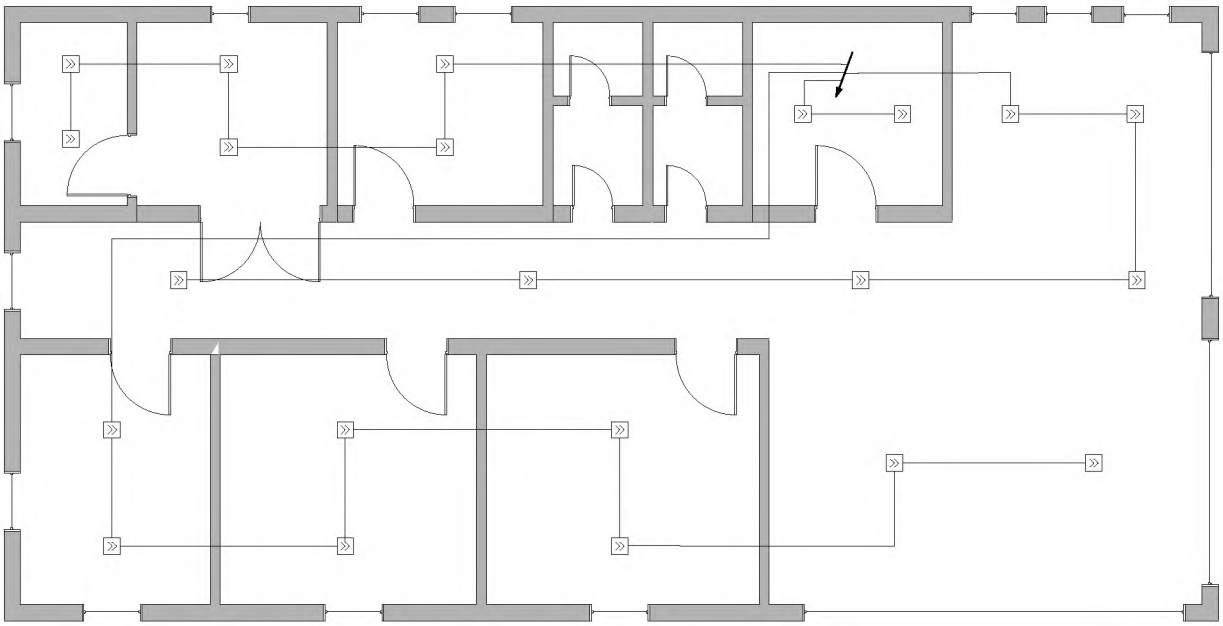


Рисунок 1.24 – Схема пожежної сигналізації 2-го поверху

- Сповіщювач магніто-контактний

- місце переходу між поверхами

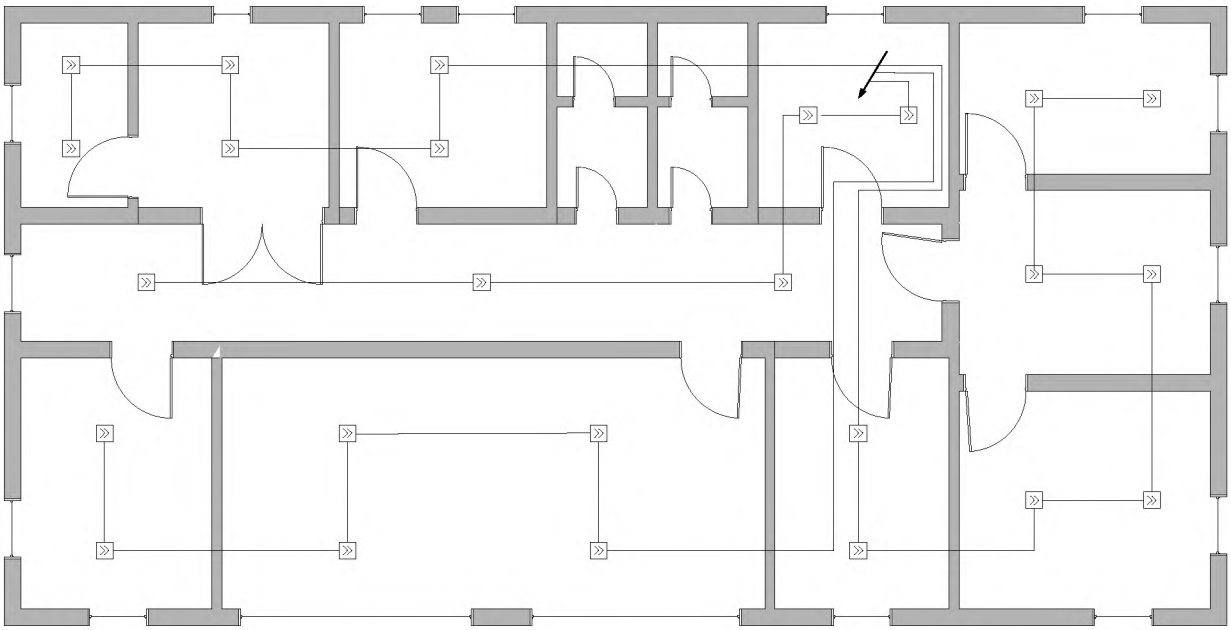


Рисунок 1.25 – Схема пожежної сигналізації 3-го поверху

- Сповіщювач магніто-контактний

- місце переходу між поверхами

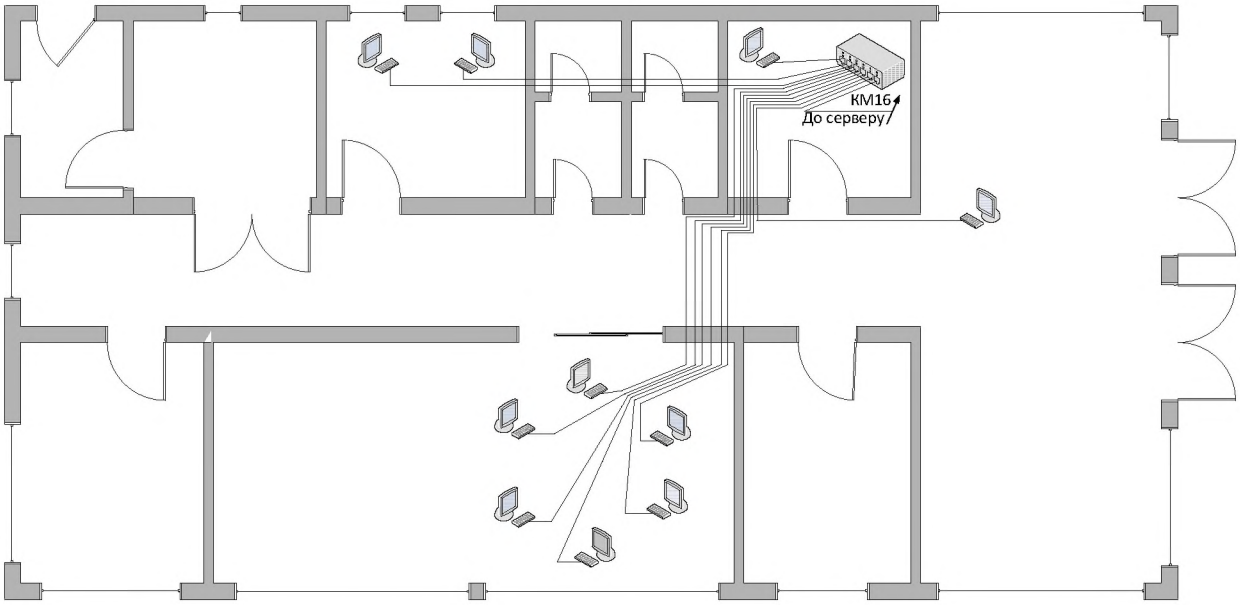
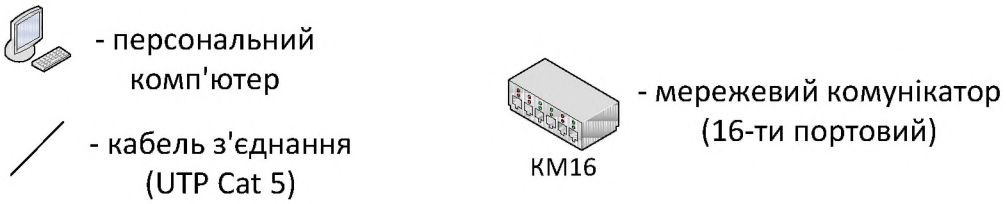


Рисунок 1.26 – Схема комп’ютерної мережі 1-го поверху



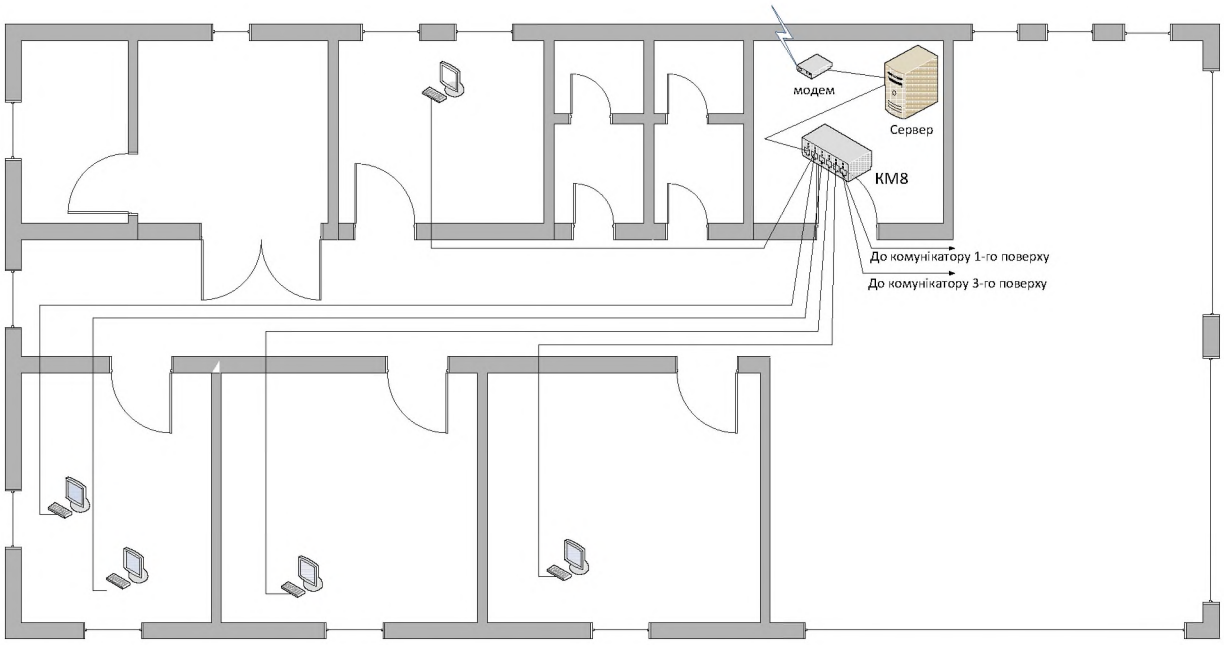
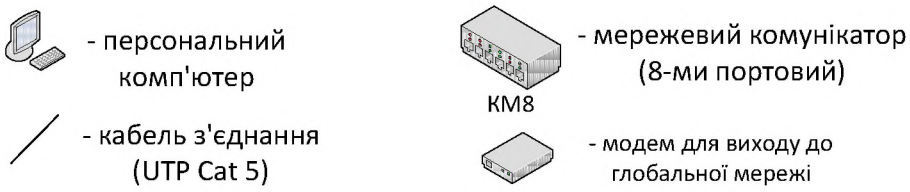


Рисунок 1.27 – Схема комп’ютерної мережі 2-го поверху



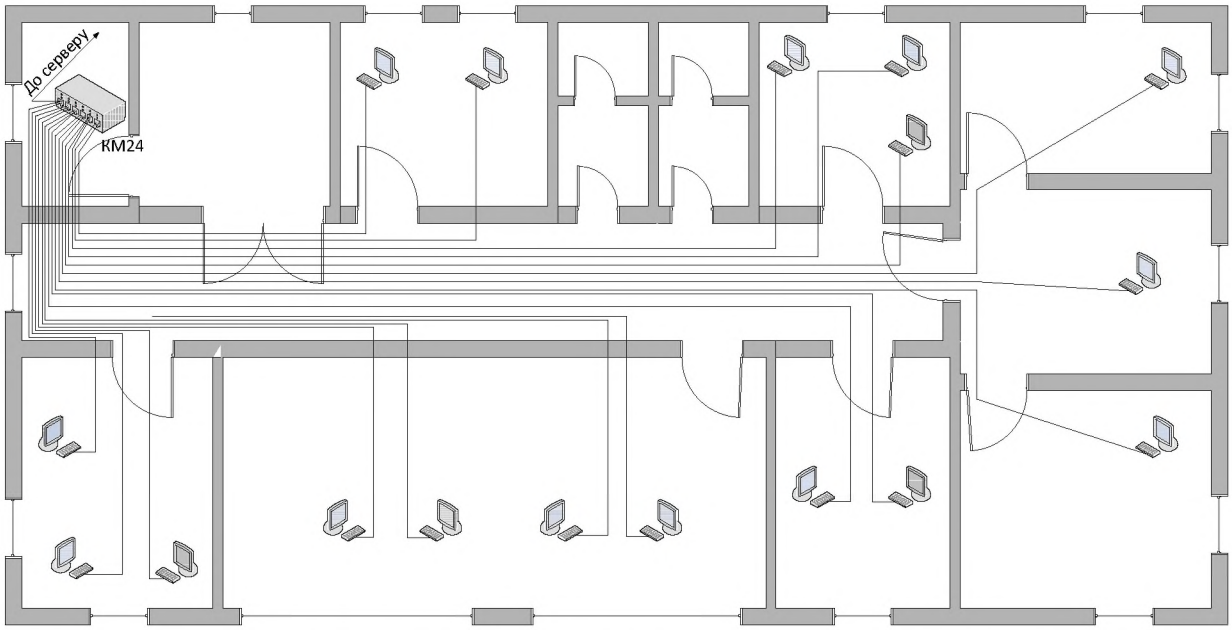
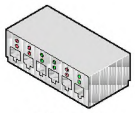


Рисунок 1.28 – Схема комп’ютерної мережі 3-го поверху


- персональний комп'ютер


КМ24

- мережевий комунікатор (24-х портовий)


- кабель з'єднання (UTP Cat 5)

1.6 Висновок

Розглянувши схему побудови КСЗІ, одним із найважливіших етапів є створення захищених каналів зв’язку, безпечна передача даних та об’єднання всіх територіально віддалених мереж в одну мережу. Дані вимоги можна реалізувати за допомогою технології VPN. Ця технологія має широкі можливості при реалізації, має велику сукупність налаштувань та принципів реалізації. Дозволяє об’єднати робочі станції на віддалених філіях в одну мережу, тобто віддалено використовувати мережеві та інформаційні ресурси, та безпечно обмінюватися інформацією.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Модель загроз

Модель загроз призначена для виявлення актуальних загроз інформаційної безпеки ІС з метою подальшої розробки вимог, виявляючі організаційно-режимні та технічні заходи по захисту інформації обмеженого доступу, оброблюємої в ІС та котра передається технічними засобами ІС по незахищених каналах передачі даних.

Джерела загроз

Джерело загрози безпеки ІС - це суб'єкт, матеріальний об'єкт або фізичне явище, що створює загрозу безпеці інформації, що захищається.

Джерела діляться на суб'єктивні (залежать від дій персоналу і, в основному, усуваються організаційними заходами і програмно-апаратними засобами) і об'єктивні (залежать від особливостей побудови та технічних характеристик обладнання, що застосовується в ІС).

До суб'єктивних джерел загроз належать:

- зовнішні суб'єктивні джерела загроз - діяльність зовнішніх порушників, спрямована на вчинення НСД до інформації, що захищається ІС;
- внутрішні суб'єктивні джерела загроз безпеці інформації - дії осіб, які мають доступ до роботи зі штатними засобами ІС та допуск в межі контрольованої зони;

До об'єктивних джерел відносяться:

- стихійні джерела потенційних загроз інформаційної безпеки, які є зовнішніми по відношенню до ІС і під якими розуміються насамперед природні явища (пожежі, землетруси, повені тощо);
- джерела, пов'язані з технічними засобами ІС, які є внутрішніми по відношенню до ІС;

При виявленні моделі загроз користуються критеріями:

- Можливість виникнення джерела ($К_1$) і – визначає ступінь доступності до захищається (для антропогенних джерел), віддаленість від об'єкта, що захищається (для техногенних джерел) або особливості обстановки (для випадкових джерел);

- Готовність джерела ($К_2$) і – визначає ступінь кваліфікації і привабливість вчинення діянь з боку джерела загрози (для антропогенних джерел), або наявність необхідних умов (для техногенних та стихійних джерел);

- Фатальність ($К_3$) і – визначає ступінь непереборності наслідків реалізації загрози;

- (Коп) і для окремого джерела можна визначити як ставлення трьох вище наведених показників до максимального значення (125);

$$К_{ов} = \frac{(К_1 * К_2 * К_3)}{125}$$

Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає самій мінімальному ступені впливу оцінюваного показника на небезпеку використання джерела, а 5 – максимальної.

Таблиця 2.1 – Модель загроз

Загроза	К1	К2	К3	$К_{оп}$
Антропогенні				
Модифікація цінної інформації на паперових носіях	3	3	4	0,288
Знищення або псування носія з цінною інформацією	5	4	4	0,64
Крадіжка носіїв інформації	3	3	4	0,288
Втрата даних в результаті відмови носіїв інформації	4	3	3	0,288
Видалення порушником цінної інформації, що зберігається в базі даних	4	5	4	0,64
Модифікація (підміна) компонентів ОС	3	3	3	0,216

Запуск файлів містять віруси	3	4	3	0,288

Продовження таблиці 2.1

Типові помилки конфігурування інтерпретаторів	3	3	2	0,144
Розголошення конфіденційної інформації в результаті психологічного впливу	2	3	2	0,096
Збір інформації про ОС	2	2	2	0,064
Запуск шкідливого програмного забезпечення, що використовує віддалені уразливості ОС	3	4	3	0,288
Порушення безперервності ведення бізнесу в результаті фізичного впливу	2	2	2	0,064
Порушення конфіденційності інформації в результаті ненавмисних дій	3	3	2	0,144
Техногенні				
Відмова зовнішніх джерел енергозбереження	4	3	5	0,48
Дефекти носіїв даних	2	2	2	0,064
Відмова в обслуговуванні мережевої служби	3	4	4	0,384
Віддалений збір інформації про мережеві служби	3	4	3	0,288
Відмова в обслуговуванні на програмному рівні	3	4	3	0,288
Стихійні джерела				
Стихійне лихо	2	2	2	0,064
Технічна катастрофа	2	2	2	0,064
Пожежа	2	2	2	0,064

При виборі допустимого рівня джерела загроз, передбачається, що джерела загроз, які мають коефіцієнт ($К_{оп}$) менше (0,1 ... 0,2) можуть надалі не враховуватися, як малоймовірні.

2.2 Модель порушника

Модель порушника – це абстрактний формалізований або неформалізований опис порушника, рівня його повноважень, ресурсних можливостей, використовуваних ним програмних і (або) технічних засобів з метою реалізації загроз для інформації.

Під порушником розуміється фізична особа, випадково або навмисно вчиняє дії, наслідком яких є порушення безпеки захищається інформації при її обробці в ІС.

Цілями несанкціонованих дій порушника, здатних привести до здійснення НСД до ресурсів, що захищаються ІС та порушення прийнятих для ІС характеристик інформаційної безпеки, є:

- порушення цілісності захищаються ресурсів;
- порушення конфіденційності захищаються ресурсів;
- порушення доступності захищаються ресурсів;
- створення умов для подальшого проведення атак.

Можливими напрямами несанкціонованих дій порушника в тому числі є:

- доступ до інформації, що захищається з метою порушення її конфіденційності (розкрадання, ознайомлення, перехоплення);
- доступ до інформації, що захищається з метою порушення її цілісності (модифікація даних);
- доступ до технічних і програмних засобів ІС з метою постійного або тимчасового порушення доступності інформації, що захищається для легального користувача;
- доступ до технічних і програмних засобів ІС з метою внесення до них несанкціонованих змін, що створюють умови для проведення атак;
- доступ до засобів захисту інформації з метою зміни їх конфігурації.

Порушники інформаційної безпеки ІС можуть бути наступних типів:

- зовнішні порушники, які здійснюють атаки з-за меж контрольованої зони ІС;
- внутрішні порушники, які здійснюють атаки, перебуваючи в межах контрольованої зони.

В залежності від категорії оброблюваних даних змінюються категорії осіб, зацікавлених у несанкціонованому отриманні інформації обмеженого доступу, тобто змінюються можливості потенційного порушника інформаційної безпеки.

Зовнішній порушник

До зовнішніх порушників ІС відносяться наступні групи осіб:

- представники кримінальних структур;
- інші фізичні особи, що намагаються отримати доступ до інформації в ініціативному порядку, в тому числі «хакери» і т.п. Зовнішній порушник може здійснювати спроби несанкціонованого доступу до інформації через кордони КЗ, в тому числі з використанням каналів передачі даних.

Внутрішній порушник

Можливості внутрішнього порушника ІС істотним чином залежать від діючих в межах КЗ обмежувальних факторів, основними з яких є організаційні, режимні, інженерно-технічні та інші заходи, спрямовані на:

- запобігання і припинення несанкціонованих дій осіб, що мають доступ в КЗ ІС;
- підбір і розстановку кадрів для роботи з ІС;
- організацію контролю та розмежування доступу фізичних осіб в КЗ, а також до штатних засобів ІС і в приміщення, в яких вони розташовані;
- контроль над порядком проведення робіт;
- контроль над дотриманням вимог документації, яка визначає політику безпеки ІС (в тому числі, контроль над виконанням режимних заходів, що регламентують порядок поводження з інформацією, що обробляється в ІС).

Виходячи з прав доступу осіб до ресурсів ІС, потенційних внутрішніх порушників можна розділити на такі категорії:

- Категорія І: зареєстрований користувач з правами адміністратора ІС (системного адміністратора, адміністратора безпеки). Особи даної категорії є довіреними (в силу реалізованих організаційних, режимних та кадрових заходів), і як порушники інформаційної безпеки не розглядаються. Адміністратори ІС проходять інструктаж з питань обробки інформації в ІС, допускаються до роботи з ресурсами ІС після перевірки знань ними положень відповідних посадових інструкцій.

- Категорія II: зареєстрований користувач ресурсів АС. Порушник категорії II може володіти наступною інформацією та даними:

- атрибутами, що забезпечують доступ до деякого підмножини ресурсів (наприклад, паролем, легальним ім'ям доступу);

- відомостями про структуру, функції, принципи, механізми дії і правила роботи технічних засобів і засобів захисту інформації в обсязі експлуатаційної документації;

- знаннями функціональних особливостей ІС;

- відомостями про ресурси ІС: порядок і правила створення, зберігання та передачі інформації, формати повідомлень, структура та властивості інформаційних потоків;

- даними про уразливість ІС, включаючи дані про не документованих можливості технічних засобів ІС;

- даними про реалізовані в системі та засобах захисту інформації принципах і алгоритмах;

- відомостями про можливі для ІС каналах атак;

- інформацією про способи атак.

Порушник категорії II володіє наступними засобами доступу до ресурсів ІС:

- штатними засобами ІС (комп'ютером, підключається безпосередньо до КМ ІС);

- наявними у вільному продажу програмними засобами прослуховування каналів передачі даних;

- наявними у вільному продажу програмними засобами модифікації даних при їх передачі по каналах зв'язку;

- загальнодоступними комп'ютерними вірусами;

- загальнодоступним програмним забезпеченням, призначеним для підготовки та здійснення застосування програмних засобів прихованого інформаційного впливу.

- Категорія III: особи, які мають санкціонований доступ в приміщення з розміщеними ТЗ зі складу ІС, але не мають санкціонованого доступу до ресурсів ІС.

Порушник категорії III може володіти такою інформацією і даними:

- знаннями про «іменах» (логіни) зареєстрованих користувачів;
- знаннями функціональних особливостей ІС;
- фрагментами інформації про топологію мережі (комунікаційної частини підмережі) і про використовувані в ІС комунікаційних протоколах та їх сервісах;
- даними про уразливість ІС, включаючи дані про не документованих можливості технічних і програмних засобів ІС;
- даними про реалізовані в системі та засобах захисту інформації ІС принципах і алгоритмах;
- відомостями про можливі для ІС каналах атак;
- інформацією про способи атак.

2.3 Проектне рішення

2.3.1 Профіль захищеності

Вибраний профіль захищеності комп'ютерної системи, що входить до складу АС класу 3, з вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної 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 }

Критерії конфіденційності:

КД-2 – базова довірча конфіденційність;

КА-2 – базова адміністративна конфіденційність;

КО-1 – повторне використання об'єктів;

КВ-2 – базова конфіденційність при обміні.

Критерії цілісності:

ЦД-1 – мінімальна довірча цілісність;

ЦА-2 – базова адміністративна цілісність;

ЦО-1 – обмежений відкат;

ЦВ-2 – базова цілісність при обміні.

Критерії доступності:

ДР -1– використання ресурсів;

ДВ-1 – ручне відновлення після збоїв.

Критерії спостереженості:

НР-2 – реєстрація;

НИ-2 – одиночна ідентифікація и автентифікація;

НК-1 – однонаправлений достовірний канал;

НО-2 – розподіл обов’язків;

НЦ-2 – цілісність КЗЗ;

НТ-2 – самотестування;

НВ-1 – автентифікація при обміні.

Таблиця 2.2 – Профіль захищеності

Критерій	Вимоги	Реалізація
КД-2	Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, та процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.	В системі мається виділений адміністратор КС, та адміністратор безпеки, маються користувачі, котрим при створенні їх адміністратором, були надані відповідні права доступу. Кожний користувач при створенні нового об’єкту може надати йому необхідні права доступу, та назначити виділених користувачів, або групу користувачів котрим буде надано повний, або не

Критерій	Вимоги	Реалізація
		повний доступ до об’єкту створення (обробки).
КА-2	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта, та процесу шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту. НЕОБХІДНІ УМОВИ: НО-1, НИ-1	Реалізовується за допомогою ОС, та комплексною прикладною програмою «AVAST PRO антивірус», маючу в своєму комплексі фаєрвол.
КО-1	Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або	Реалізовується прикладними програмними продуктами разом з взаємодією ОС.

Критерій	Вимоги	Реалізація
	процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.	
КВ-2	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається. Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. НЕОБХІДНІ УМОВИ: НО-1	При створенні нового об’єкту користувач може вибрати різні атрибути для об’єкту (тільки читання, прихований, архівний), також може визначити користувачів, та групи користувачів, яким буде надано відповідні права доступу (Повний доступ, Зміна, Читання й виконання, Запис даних, Читання атрибутів, Видалення, Зміна прав доступу, Зміна власника). Реалізовується за допомогою ОС.
ЦД-1	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.	Реалізовується за допомогою засобів ОС, при створенні, або модифікації об’єкту користувачем-власником.
ЦА-2	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів,	Адміністратором створені групи користувачів, з однаковими характеристиками, яким

Критерій	Вимоги	Реалізація
	яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. НЕОБХІДНІ УМОВИ: НО-1, НИ-1	надані деякі права доступу ПЗ замовчуванню.
ЦО-1	Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу. НЕОБХІДНІ УМОВИ: НИ-1	Реалізовується засобами ОС. Користувач за допомогою утиліти «Востановление системы» має можливість відмінити певний набір операцій.
ЦВ-2	КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання. Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.	Реалізується на базі технології віддаленого доступу до мережі (VPN).

Критерій	Вимоги	Реалізація
	НЕОБХІДНІ УМОВИ: НО-1	
ДР-1	Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. НЕОБХІДНІ УМОВИ: НО-1	При створенні або зміненні, авторизованими користувачами, на ресурси можна накладати певні обмеження (Повний доступ, Зміна, Читання й виконання, Запис даних, Читання атрибутів, Видалення, Зміна прав доступу, Зміна власника). Реалізується засобами ОС.
ДВ-1	Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування. НЕОБХІДНІ УМОВИ: НО-1	Реалізується засобами ОС, також допоміжними спеціальними програмними продуктами. Являється обов’язком системного адміністратора та адміністратора безпеки.
НР-2	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу	В системі ведеться запис реєстрового журналу. Реалізується засобами ОС, та прикладним програмним забезпеченням орієнтованим на обслуговування системи.

Критерій	Вимоги	Реалізація
	і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації. НЕОБХІДНІ УМОВИ: НИ-1, НО-1	
НИ-2	Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування. НЕОБХІДНІ УМОВИ: НК-1	Кожний користувач має свій персональний логін та пароль. Вони використовуються для авторизованого входу в систему. Логін використовується як ідентифікатор імені для об’єктів які створюються або змінюються. Реалізується засобами ОС.
НК-1	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.	При вході в ОС, використовується електронний ключ «eToken SecurLogon», для аутентифікації.
НО-2	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок	Електронні ключі «eToken SecurLogon» мають різні права доступу до системи.

Критерій	Вимоги	Реалізація
	з використанням даного каналу повинен ініціюватися виключно користувачем. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі. НЕОБХІДНІ УМОВИ: НИ-1	Реалізується за допомогою ПЗ «eToken Windows Logon».
НЦ-2	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.	
НТ-2	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з	При вході користувача в систему, проходить самотестування системи. Реалізовується засобами ОС, та спеціального ПО.

Критерій	Вимоги	Реалізація
	метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ. НЕОБХІДНІ УМОВИ: НО-1.	
НВ-1	Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.	Реалізується засобами «eToken Windows Logon».

2.3.2 Реалізація підсистеми захисту віддаленого доступу

З метою скорочення бюджетів підприємств на обслуговування мережі виробники розробляють нові більш досконалі рішення в області створення мультисервісних мереж передачі даних.

Сьогодні найбільш економічно вигідним рішенням для організації захищеного обміну конфіденційною інформацією є побудова так званої віртуальної захищеної приватної мережі (Virtual Private Network - VPN). У першу чергу захищений обмін конфіденційною інформацією потрібно компаніям, що здійснюють обробку та передачу інформації різної категорії і ступеня конфіденційності всередині розподіленої корпоративної мережі або постійні зв'язки з віддаленими бізнес-партнерами та замовниками; мають територіально рознесені філії, штат мобільних або віддалених співробітників.

Віртуальна приватна мережа формується на основі відкритих каналів зв'язку, наприклад Internet. Термін "віртуальна" підкреслює, що інфраструктура

мережі моделюється на основі реальних каналів зв'язку (виділені лінії, комутовані канали і т. д.). При цьому реальна відкрита мережа може служити основою для цілої безлічі VPN, кінцеве число яких визначається тільки пропускною здатністю відкритих каналів зв'язку.

При виборі засобів побудови корпоративних VPN необхідно враховувати наступні фактори:

- технічні характеристики відкритої зовнішнього середовища передачі інформації;
- переваги та недоліки використовуваних для побудови VPN протоколів;
- варіанти побудови VPN;
- регулювання використання VPN-технологій з боку законодавства;
- специфіка (форма власності, категорювання інформації і т.д.) і фінансові можливості підприємства.

Об'єднання офісів можна здійснювати як на програмному, так і на апаратному рівні.

1. Використовуючи продукт Microsoft Windows Server 2012, можемо запропонувати вам 2 рішення використання VPN мереж:

- VPN з'єднання клієнта віддаленого доступу. Клієнт віддаленого доступу робить VPN з'єднання віддаленого доступу, який підключається до приватної мережі. Microsoft Windows Server 2008 забезпечує доступ до цілої мережі, до якої підключений VPN сервер. Це дозволить також і мобільним клієнтам підключатися з будинку або інших місць через Інтернет до корпоративної мережі і обмінюватися службовою інформацією.
- Site-to-site VPN з'єднання. Маршрутизатор робить site-to-site VPN з'єднання, яке з'єднує дві частини приватної мережі. Microsoft Windows Server 2008 забезпечує підключення до мережі. Таким чином ви отримуєте захищену об'єднану мережу двох офісів.

2. Використовуючи продукти Cisco System для побудови VPN мереж, об'єднання віддалених офісів.

Переваги VPN:

При створенні єдиної мережі компанія отримує ряд переваг:

- оптимізація витрат на міжміський і міжнародний зв'язок за рахунок комунікацій співробітників ПЗ внутрішній мережі.
- підвищення мережевої безпеки до того рівня, який не можуть забезпечити системи безпеки, пропоновані провайдерами телефонного зв'язку.
- надання корпоративним, зовнішнім і віддаленим користувачам мережі безпечного доступу до мережевих ресурсів.

Віртуальні приватні мережі дозволяють зовнішньому користувачу, в тому числі отримав доступ через публічну мережу і пройшов аутентифікацію, скористатися корпоративною мережею нарівні з клієнтами центральної корпоративної мережі.

- скоротити час передачі інформації.
- оптимізувати робочі процеси.
- спростити топологію мережі і скоротити парк мережевого обладнання.
- збільшити мобільність користувачів.
- надати більш гнучкий графік роботи.

Розрізняють декілька видів Virtual Private Network:

- Intranet - мережі для об'єднання в єдину мережу розрізнених філій компанії, що використовують відкриті канали для передачі інформації.
- Remote Access - мережі віддаленого доступу для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і віддаленим користувачем.
- Extranet-мережі для надання зовнішнім користувачам захищеного доступу до корпоративних мережевих ресурсів.

Розрізняють статичні і динамічні VPN. У динамічних Virtual Private Network використовується мережевий протокол, що дозволяє віддаленим вузлам мережі присвоювати динамічні IP-адреси. Такий підхід дозволяє значно

посилити рівень захисту мережі на рівні доступу та убезпечити корпоративні дані.

Крім того, це дозволить підприємству уникнути додаткових витрат на оплату кожного статичного IP-адреси провайдера послуг.

Програмні засоби які допоможуть реалізувати дане проектне рішення:

«GFI EventsManager» - програма реєстрації подій.

Файли реєстрації подій - цінний інструмент для моніторингу мережі та продуктивності, які часто використовуються в недостатній мірі через їх складності та обсягу. У міру зростання організації їй потрібно більш структурований підходу до управління файлами реєстрації подій і їх зберігання.

Належне управління файлами реєстрації подій допоможе досягти кількох цілей:

- Інформаційна система і мережева безпека;
- Моніторинг справності системи;
- Розслідування.

Переваги програмного продукту «GFI EventsManager»:

- централізація подій Syslog, W3C і Windows, створених брандмауерами, серверами, маршрутизаторами, комутаторами, телефонами, ПК та іншим.
- налаштування за допомогою майстра спрощує управління та обслуговування.
- неперевершена система виявлення подій, розширювана до більш 6000000 подій на годину.
- попередньо налаштовані правила обробки для ефективної класифікації подій і управління.
- автоматизований моніторинг подій в режимі 24/7 і сигналізація.
- потужний засіб створення звітів для ефективного моніторингу мережевої активності та швидке повернення капіталовкладень.

GFI EventsManager збирає дані від всіх пристроїв, що використовують файли реєстрації подій Windows, W3C і Syslog і застосовує найкращі в галузі

правила і фільтрацію для виявлення ключових даних. Це дозволяє простежувати, коли співробітники використовують переносні пристрої, піднімають трубку, щоб подзвонити додому, включають ПК, що вони роблять на ПК і до яких файлів вони звертаються протягом робочого дня.

Системні вимоги:

- .NET framework 3.0
- Microsoft Data Access Components (MDAC) 2.6
- Access to MSDE / SQL Server 2012

Комплексний програмний засіб «WinRoute Pro». В WinRoute Pro дуже просто організована настройка підключення локальної мережі до зовнішнього світу. Крім мережевих карт можна підключатися через модем. В модемному з'єднанні можна встановити автоматичне відновлення з'єднання при обриві зв'язку і розрив зв'язку при відсутності активності з'єднання.

WinRoute Pro працює під Windows 2000/XP/7/8/10.

До складу«WinRoute Pro» входить: Firewall; NAT Router; Port mapping; Proxy server і URL-фільтрацію; DHCP server; DNS server; Mail server;

- можливість організації VPN через інтернет з використанням Microsoft's PPTP і IPSec.

Програмно-апаратний засіб аутентифікації користувачів в системі за допомогою електронних ключів «eToken Windows Logon».

«eToken SecurLogon» поєднує ефективний захист мережі з зручністю і мобільністю. При аутентифікації в Windows використовуються ім'я користувача та пароль, що зберігаються в пам'яті eToken. Це дає можливість застосовувати строгу аутентифікацію на основі ключів. При використанні eToken SecurLogon можуть застосовуватися нікому не відомі випадкові складні паролі. Крім того, передбачена можливість використання сертифікатів, що зберігаються в пам'яті eToken, для реєстрації на основі смарт-карт, що підвищує безпеку входу в Windows. Це можливо завдяки тому, що система Windows 2000/XP/7/8/10 дозволяє використовувати різні механізми доступу, що замінюють метод аутентифікації за умовчанням. Механізми ідентифікації і аутентифікації служби

входу в Windows (winlogon), що забезпечує інтерактивну реєстрацію в системі, вбудовані в змінну, динамічно під'єднану бібліотеку (DLL), що іменується GINA (Graphical Identification and Authentication, робочий стіл аутентифікації). Коли система потребує іншого методі аутентифікації, який би замінив механізм "ім'я користувача / пароль" (використовується за замовчуванням) стандартну msgina.dll замінюють новою бібліотекою. При установці eToken SecurLogon замінюється бібліотека робочого столу аутентифікації і створюються нові параметри реєстру. GINA відповідає за політику інтерактивного підключення і здійснює ідентифікацію і діалог з користувачем. Заміна бібліотеки робочого столу аутентифікації робить eToken основним механізмом перевірки справжності, розширюють можливості стандартної аутентифікації Windows 2000/XP, заснованої на застосуванні імені користувача і пароля. Профілі можна створювати за допомогою майстра створення профілів eToken Windows Logon.

Системні вимоги:

- на всіх робочих станціях повинен бути встановлений eToken Runtime Environment;
- eToken SecurLogon встановлюється на комп'ютер з Windows 2000 (SP4), Windows XP (SP2) / 7 / 8 / 10 або Windows 2012. eToken SecurLogon підтримує класичний діалог вітання Windows і не підтримує режим швидкої зміни користувача в Windows.

«eToken SecurLogon» підтримує такі пристрої eToken:

- eToken PRO - USB-ключ, що дозволяє виробляти двохфакторну аутентифікацію. Доступний у версіях 32К і 64К;
- eToken NG-OTP - гібрид USB-ключа та пристрій, що генерує одноразові паролі. Доступний у версіях 32К і 64К;
- смарт-карта eToken PRO - пристрій, що виконує ті ж функції, що і USB-ключ, але має форму звичайної кредитної карти. Доступна у версіях 32К і 64К.

Принцип роботи:

Коли комп'ютер заблокований, з'являється вікно «Блокування комп'ютера Computer Locked». Підключіть eToken до порту USB або кабелю. У вікні введіть PIN-код в поле "eToken Password" і натисніть кнопку "OK" - комп'ютер розблоковано. У разі натискання "CTRL + ALT + DEL" і введення пароля комп'ютер буде розблоковано без використання eToken.

2.3.3 Матриця доступу

При реалізації проекту отримаємо наступну матрицю доступу суб'єктів до інформації з обмеженим доступом, і їх можливості виконання певних дій відносно інформації.

Таблиця 2.3 – Матриця доступу

Посада	Створення	Змінення	Видалення	Читання
Директор	+	+	+	+
Замісник директора	+	+	-	+
Головний бухгалтер	+	+	-	+
Бухгалтер	+	-	-	+
Головний фінансист	+	+	-	+
Фінансист	+	-	-	+
Головний економіст	+	+	-	+
Економіст	-	-	-	+
Головний менеджер	-	-	-	+
Менеджер	-	-	-	-
Головний маркетолог	+	-	-	+
Маркетолог	-	-	-	-
Рекламний агент	-	-	-	-
Кадровик	-	+	-	+
Юрист	+	-	-	+
Комірник	-	+	-	+
Системний адміністратор	+	-	-	+

Адміністратор безпеки	+	+	+	+

2.3.4 Обґрунтування вибору

Переваги VPN

Переваги технології VPN настільки переконливі, що багато підприємств починають будувати свою стратегію з урахуванням використання Інтернету як головного засобу передачі інформації, навіть тієї, яка є вразливою. Переваги VPN вже гідно оцінені багатьма підприємствами.

При правильному виборі VPN:

- отримуємо захищені канали зв'язку за ціною доступу в Інтернет, що в кілька разів дешевше виділених ліній;
- при установці VPN не потрібно змінювати топологію мереж, переписувати програми, навчати користувачів - все це значна економія;
- забезпечується масштабування, оскільки VPN не створює проблем зростання і зберігає зроблені інвестиції;
- незалежні від криптографії і можете використовувати модулі криптографії будь-яких виробників у відповідності з національними стандартами тієї чи іншої країни;
- відкриті інтерфейси дозволяють інтегрувати вашу мережу з іншими програмними продуктами та бізнес-додатками.

Недоліки VPN

До них можна віднести порівняно низьку надійність. У порівнянні з виділеними лініями та мережами на основі Frame relay віртуальні приватні мережі менш надійні, проте в 5-10, а іноді й у 20 разів дешевше. На думку західних аналітиків, це не зупинить продаж VPN, оскільки лише п'ять відсотків користувачів, що торгують, наприклад, на ринку цінних паперів, потрібні такі високі стандарти. Решта 95% не настільки серйозно ставляться до проблем зі зв'язком, а витрати більшої кількості часу на отримання інформації не призводять до колосальних збитків.

У силу того, що послуга VPN надається та підтримується зовнішнім оператором, можуть виникати проблеми зі швидкістю внесення змін до бази доступу, в налаштування firewall, а також з відновленням обладнання, що вийшло з ладу. В даний час проблема вирішується вказівкою в договорах максимального часу на усунення неполадок і внесення змін. Зазвичай цей час становить кілька годин, але зустрічаються провайдери, що гарантують усунення несправностей протягом доби.

Ще один істотний недолік - у споживачів немає зручних засобів управління VPN. Хоча останнім часом розробляється обладнання, що дозволяє автоматизувати управління VPN. Серед лідерів цього процесу – компанія Indus River Networks Inc., дочірня компанія MCI WorldCom і Novell.

2.4 Висновок

Зробивши обстеження на об’єкті інформаційної діяльності. Були зроблені висновки, виявленні загрози, описані можливі порушники стосовно інформаційної безпеки підприємства. На базі цих висновків та спостережень розроблено та запропоновано проектне рішення існуючих проблем. Проектне рішення вбачає в собі реалізацію VPN мережі на підприємстві, з використання додаткових програмних та апаратних засобів. При виконанні всіх вимог даного проектного рішення підприємство зазнає збільшення в прибутку, зменшення витрат на захист інформації, зменшення витрат спричинених розголошенням інформації з обмеженим доступом.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є обґрунтування економічної доцільності розробки підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс». Досягнення цієї мети потребує виконання таких розрахунків, як:

– капітальні витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

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

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи підприємства

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи підприємства, $t_{тз}$=10;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в$=*24*;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=*32*;

$t_р$ – тривалість розробки засобів захисту інформації в інформаційно-комунікаційній системі підприємства, $t_м$=*28*;

$t_д$ – тривалість підготовки технічної документації, $t_д$=*10*.

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 10+24+32+28+10 = 104 \text{ години.}$$

Розрахунок витрат на розробку підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи підприємства

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = З_{зп} + З_{мч} = 13624+2223,52 = 15847,52 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 104*131 = 13624 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

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

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$З_{мч}$= t*$С_{мч}$=104*21,38=2223,52 грн.

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 0,7 \cdot 14 \cdot 1,55 + \frac{4680 \cdot 0,5}{1920} + \frac{6020 \cdot 0,2}{1920} = 21,38 \text{ грн.}$$

В інформаційній системі ТОВ «Продуктсервіс» використовується апаратне та програмне забезпечення, яке можливо використовувати для реалізації розробки підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи. Запропоновваний підхід передбачається реалізовувати за допомогою технології VPN, що не потребує додаткових витрат.

Але проектне рішення вбачає в собі реалізацію VPN мережі на підприємстві з використання додаткових програмних та апаратних засобів, а саме: програма реєстрації подій «GFI EventsManager» (вартість – 80370 грн.); комплексний програмний засіб «WinRoute Pro» (вартість – 5600 грн.); програмно-апаратний засіб аутентифікації користувачів в системі за допомогою електронних ключів «eToken Windows Logon» (вартість – 3112 грн.).

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 7000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$$=15847,52 + 80370 +5600+3112+7000=111929,5 \text{ грн.}$$

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

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

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

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

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

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.}$$

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

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

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

Вартість відновлення й модернізації системи на підприємстві ТОВ «Продуктсервіс» складатиме 6220 грн. щорічно.

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Чинне законодавство України передбачає поступове перенесення вартості матеріальних активів на витрати підприємства. Нарахування амортизації на підприємстві ТОВ «Продуктсервіс» здійснюється прямолінійним методом. Для програмного забезпечення строк корисного використання встановлений 3 роки. Отже, сукупні річні амортизаційні відрахування складуть:

$$С_а = 80370/3+5600/3+3112/3 = 29694 \text{ грн}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 16200 грн. Додаткова заробітна плата – 9% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,15 ставки. Отже,

$$С_з = (16200*12 + 16200*12*0,09)*0,15= 31784,4 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 31784,4*0,22 = 6992,7 \text{ грн.}$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,7 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,7*14*1920*1,55 = 29164,8 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 111929,5*0,01=1119,3 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 29694+31784,4+6992,7+29164,8+1119,3= 98755,2 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 6220+98755,2=104975,2 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

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

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 16200 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15100 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 13 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 240 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 2000 грн.;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 25.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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

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

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

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

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{15100 \cdot 13}{176} \cdot 4 = 4461{,}36 \text{ грн},$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

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

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{15100 \cdot 13}{176} \cdot 6 = 6692{,}05 \text{ грн}.$$

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

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{16200 \cdot 1}{176} \cdot 2 = 184{,}09 \text{ грн.}$$

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

$$П_в = 6692{,}05+184{,}09+2000 = 8876{,}14 \text{ грн.}$$

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

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{240000}{2080} \cdot (4+2+6) = 1384{,}62 \text{ грн.}$$

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

$$U = 4461{,}36+8876{,}14+1384{,}62 = 14722{,}12 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{25} 14722{,}12 = 368053 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (74%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 368053*0,74 - 104975,2 = 167384,02 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{167384,02}{111929,5} = 1,5, \quad \text{частки одиниці,}$$

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

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,5 > (6 - 5)/100 = 1,5 > 0,01.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1,5} = 0,69 \text{ років (біля 8 місяців).}$$

3.4 Висновок

На підставі здійснених розрахунків можна дійти висновку, що розробка підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс» є економічно доцільною, оскільки дозволяє отримати економічний ефект у розмірі 167384,02 грн.

При капітальних витратах у 111929,5 грн., ТОВ «Продуктсервіс» отримуватиме 1,5 грн. економічного ефекту на кожну гривню капітальних витрат (ROSI=1,5).

Експлуатаційні витрати складають 104975,2 грн.

Термін окупності – біля 8 місяців.

ВИСНОВКИ

Під час виконання роботи було виконано: обстеження на об’єкті інформаційної діяльності, виконано аналіз існуючих загроз, запропоновано та розроблено метод вирішення існуючих загроз відносно до захисту інформації, яка циркулює по відкритим каналам зв’язку, представлено обґрунтування вибору методу відносно до даного підприємства.

У економічному розділі було виконано розрахунок кінцевої вартості проекту, розробка підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс» є економічно доцільною, оскільки дозволяє отримати економічний ефект у розмірі 167384,02 грн. При капітальних витратах у 111929,5 грн., ТОВ «Продуктсервіс» отримуватиме 1,5 грн. економічного ефекту на кожну гривню капітальних витрат (ROSI=1,5). Експлуатаційні витрати складають 104975,2 грн. Термін окупності – біля 8 місяців.

ПЕРЕЛІК ПОСИЛАНЬ

1. С.В. Запечников, Н.Г. Милославская, А.И. Толстой. «Основы построения виртуальных частных сетей». Для высших учебных заведений. Горячая Линия – Телеком, 2003. – 248 с.

2. Стивен Браун. «Виртуальные частные сети». Лори, 2001. – 503 с.

3. Ричард Тиббс, Эдвард Оукс. «Межсетевые экраны и виртуальные частные сети: Принципы и практика (Безопасность)». – 658 с.

4. Защита информации, передаваемой по каналам святи (Електрон. ресурс) / Спосіб доступу: URL: http://www.i-teco.ru/article37.html

5. Введение в Виртуальные Частные Сети (VPN) (Електрон. ресурс) / Спосіб доступу: URL: http://www.hub.ru/archives/2269

6. ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення».

7. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»

8. НД ТЗІ 1.4-001-2000 «Типове положення про службу Захисту інформації в автоматизованій системі».

9. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

10. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення».

11. НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категорювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».

12. НД ТЗІ 1.1-002-99 «Загальні положення про захист інформації в комп'ютерних системах від несанкціонованого доступу».

13. НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи».

14. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

15. НД ТЗІ 2.5-005-99. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

16. НД ТЗІ 3.7-001-99. «Методичні вказівки для розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованих системах».

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	32	
6	А4	2 Розділ	23	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Розробка підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс»
Бабича Максима Павловича

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

Об'єкт розробки: інформаційно-телекомунікаційна системи Товариство з обмеженою відповідальністю «Продуктсервіс».

Мета роботи: розробка підсистеми захисту віддаленого доступу на базі інформаційної системи ТОВ «Продуктсервіс».

У першому роділлі розглянуто підходи створення підсистеми захисту віддаленого доступу в комплексній системі захисту інформаційно-телекомунікаційної системи ТОВ «Продуктсервіс».

У спеціальній частині виконано: обстеження на об'єкті інформаційної діяльності, та вибрано метод розробки підсистеми захисту віддаленого доступу.

В економічному розділі було виконано розрахунки кінцевої вартості проекту, та розраховано період окупності даного проекту після його реалізації.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник