Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)
факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеню бакалавра

**студента** Цапенко Олександр Володимирович
(П.І.Б.)
**академічної групи** 123-17ск-1
(шифр)
**Спеціальності** 123 Комп'ютерна інженерія
(код і назва спеціальності)
**за освітньо-професійною програмою** 123 Комп'ютерна інженерія
(офіційна назва)
**на тему** Комп'ютерна система філії АТ «Дніпропетровськгаз» з опрацюванням побудови та налаштувань комп'ютерної мережі
(назва за наказом ректора)

| **Керівник** | **Прізвище, ініціали** | **Оцінка за шкалою** | | **Підпис** |
|---|---|---|---|---|
| | | **рейтинг.** | **інституційною** | |
| кваліфікаційної роботи | проф. Цвіркун Л.І., | | | |
| розділів: | | | | |
| апаратний розділ | доц. Ткаченко С.М. | | | |
| розрахунок мережі | ас. Панферова Я.В. | | | |
| економічний розділ | ст. викл. Яремчук І.О. | | | |
| охорона праці | доц. Яворська О.О. | | | |
| Рецензент | | | | |
| Нормоконтролер | проф. Цвіркун Л.І. | | | |

**Дніпро**
**2020**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
інформаційних систем
та технологій
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

«_____»_____2020 року

# ЗАВДАННЯ
## на кваліфікаційну роботу
## ступеня бакалавр

**студенту** Цапенко О.В. **академічної групи** 123-17ск-1
(прізвище та ініціали) (шифр)

**спеціальності** 123 Комп'ютерна інженерія

**за освітньо-професійною програмою** 123 Комп'ютерна інженерія
(офіційна назва)

**на тему** Комп'ютерна система філії АТ «Дніпропетровськгаз» з опрацюванням побудови та налаштувань комп'ютерної мережі

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

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Стан питання та постановка завдання | На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи. | 18.05.2020 |
| Технічні вимоги до комп'ютерної системи | На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи. | 25.05.2020 |
| Спеціальна частина | Розв'язати завдання з розробки комп'ютерної системи з опрацюванням побудови і захисту інформації та налаштуванням корпоративної мережі | 01.06.2020 |
| Економічна частина | Економічно обґрунтувати доцільність витрат на створення та дослідження системи | 08.06.2020 |
| Охорона праці | Розробити організаційно-технічні заходи, щодо реалізації правил безпеки при експлуатації системи | 15.06.2020 |

**Завдання видано** _____ проф. Цвіркун Л.І.
(підпис п. керівника) (прізвище, ініціали)

**Дата видачі** 27.01.2020

**Дата подання до екзаменаційної комісії** 18.05.2020

**Прийнято до виконання** _____ Цапенко О.В.
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: _____ с., _____ рис., _____ табл., _____ додатки, _____ джерел.

Об’єкт розробки: комп’ютерна система філії АТ «Дніпропетровськгаз» з опрацюванням побудови та налаштувань комп’ютерної мережі.

Мета: створення Комп’ютерної системи філії АТ «Дніпропетровськгаз» з опрацюванням побудови та налаштувань комп’ютерної мережі.

У роботі викладені результати обстеження об’єкту інформаційної діяльності філії публічного акціонерного товариства «Дніпропетровськгаз», розроблена модель загроз витоку конфіденційної інформації.

Розроблена комп’ютерної системи з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову системи контролю філії АТ «Дніпропетровськгаз», а також для збору і підготовки статистичної інформації.

В спеціальній частині розроблені вимоги до кожної складової комплексу технічного захисту інформації, обґрунтований вибір технічних засобів та інженерних заходів.Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках.

Практична значимість полягає в тому, що впровадження комплексу технічного захисту інформації підвищить рівень захисту конфіденційної інформації, що циркулює на об’єкті інформаційної діяльності філії «Дніпропетровськгаз», від витоку технічними каналами.

СИСТЕМА, КОМП’ЮТЕР, КОНТРОЛЬ, МЕРЕЖА, НАЛАШТУВАННЯ

# ЗМІСТ

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

КТЗІ – комплекс технічного захисту інформації;

КЗ – контрольована зона;

ПАТ – публічне акціонерне товариство;

ТЗПІ – технічні засоби прийому, передачі і обробки інформації;

ТЗР – технічний засіб розвідки;

НАК – національна акціонерна компанія;

ЛОМ – локальна обчислювальна мережа;

НД ТЗІ – нормативний документ технічного захисту інформації;

ПК – персональний комп’ютер;

КПП – контрольно-пропускний пункт;

ОІД – об’єкт інформаційної діяльності.

# ВСТУП

Будь-яка компанія, що розвивається стикається з проблемою систематизації інформації та автоматизації процесів, що беруть участь в обробці цієї інформації.

Корпоративні інформаційні системи орієнтовані на вирішення корпоративних завдань і призначені для комплексної автоматизації всіх видів господарської діяльності компанії, які потребують єдиного управління.

Підприємства нафтогазової промисловості України мають великий грошовий обіг, який нараховує мільйони гривень. Тому необхідність захисту інформації у мережі з обмеженим доступом, яка циркулює на таких об’єктах, не визиває сумніву. Тим паче інформація, що знаходиться у володінні нафтогазових підприємств, може належати державі.

Для таких підприємств необхідно створювати комплексну систему захисту інформації, обов’язковою складовою якої є комплекс технічного захисту інформації, спрямований на захист інформації з обмеженим доступом від витоку технічними каналами.

При проектуванні комплексу технічного захисту інформації важливо враховувати такі фактори, як сучасний стан розвитку технічних засобів розвідки і спеціального впливу, які з кожним роком стають все більш досконалими, а також методики соціальної інженерії. Тому комплекс технічного захисту інформації повинен відповідати сучасним реаліям розвитку інформаційної боротьби.

# 1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

## 1.1 Характеристика підприємства та умов застосування КС

### 1.1.1 Характеристика філії

Синельниківське управління по експлуатації газового господарства є структурним підрозділом публічного акціонерного товариства по газопостачанню та газифікації «Дніпропетровськгаз» (без права юридичної особи). Розташоване за адресом: м. Синельникове, вул. Миру, 64.

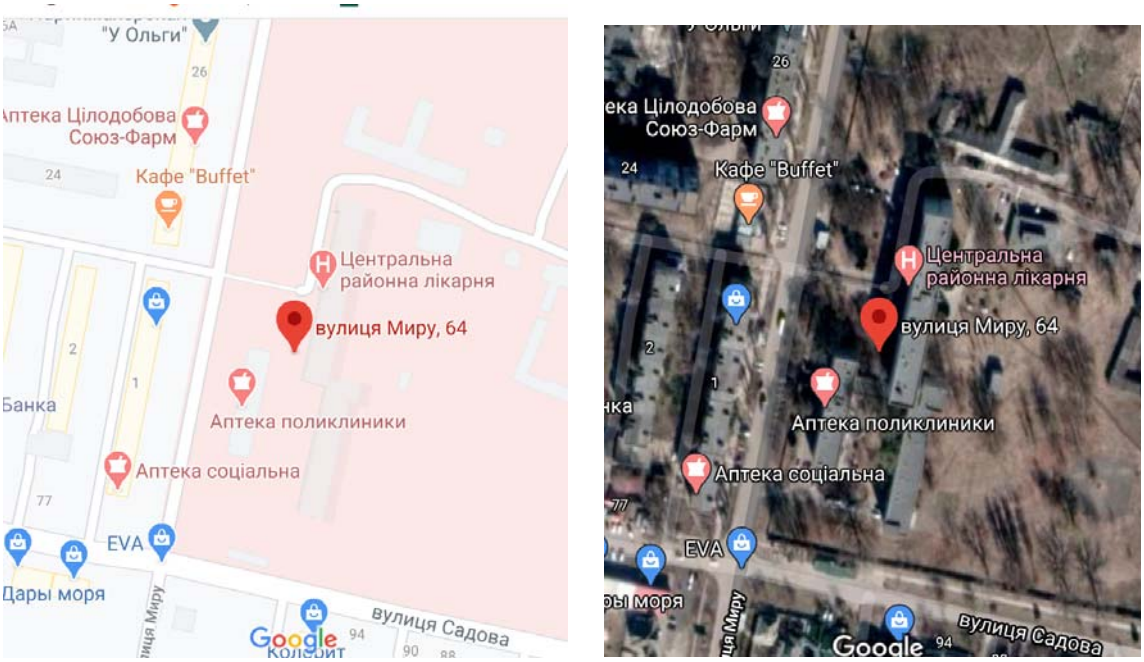



Рисунок 1.1 – Топологія розташування філії

Основними напрямами діяльності є :

– експлуатація державних, комунальних та приватних газопроводів та споруд на них (незалежно від форм власності);
– обслуговування внутрішніх систем газопостачання та газових приладів;
– локалізація та ліквідація аварійних ситуацій службами АДС на газопроводах, що експлуатуються;
– постачання природного і скрапленого газу.

Сфера діяльності підприємства охоплює 78 населених пунктів, 19 промислових підприємств і 512 об’єктів комунального та побутового призначення. Штат співробітників налічує 296 осіб. Схема підпорядкування філії та її структура зображені на рис. 1.2 та рис. 1.3 відповідно.

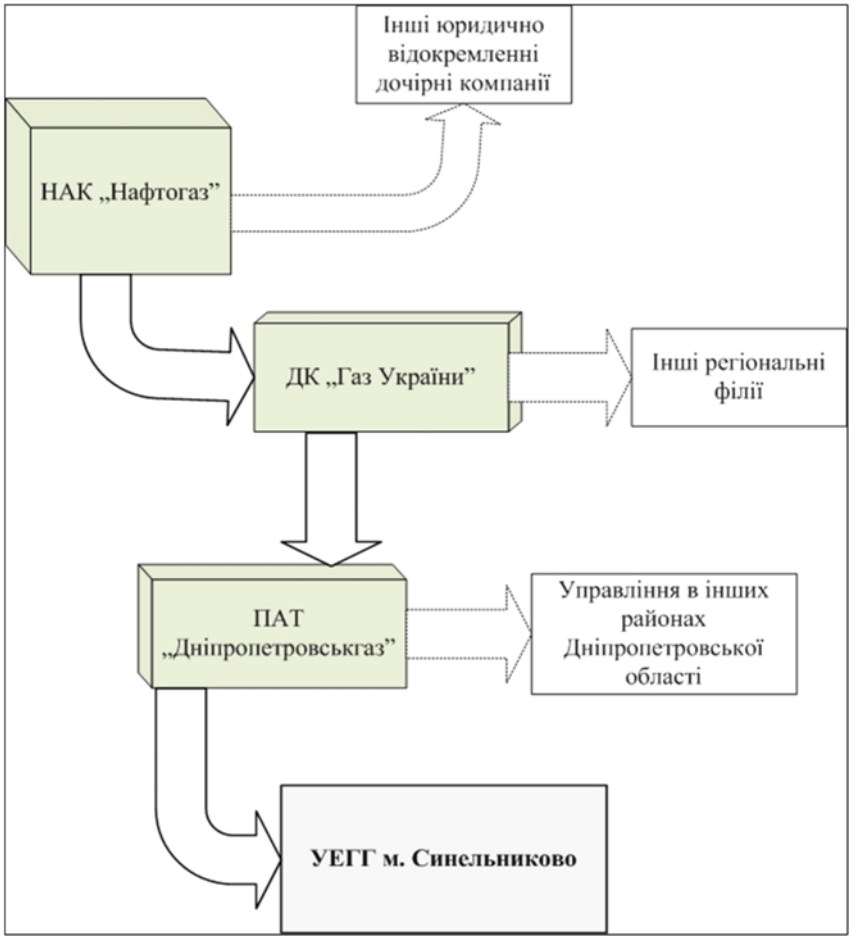



Рисунок 1.2 – Структурна схема підприємства

Адміністративний корпус являє собою триповерхову будівлю. Фундамент залізобетонний. Несучі стіни викладені з цегли товщиною 50 см і обкладені декоративною плиткою. Перекриття - залізобетонні плити. Дах чотирискатний, покриття шиферне, ферма даху трикутна, дерев’яна. Вікна металопластикові, однокамерні, металеві решітки відсутні. Всередині будівлі стіни покриті штукатуркою, пофарбовані. Підлога бетонна, покрита лінолеумом. Вхідні двері металеві з навісним замком. Всередині всі двері дерев’яні з врізаними замками (окрім

спеціальних службових приміщень, входи до яких, обладнані металевими дверми з навісними замками).

Абонентський відділ – нова одноповерхова цегляна будівля, яка прилягає до гаражів. Зовні стіни оброблені декоративною штукатуркою і пофарбовані. Дах двоскатний з дерев'яною фермою, покриту шифером. Вхід має скляний тамбур з метало-пластиковими дверми. Вхідні двері – металеві з навісним замком.

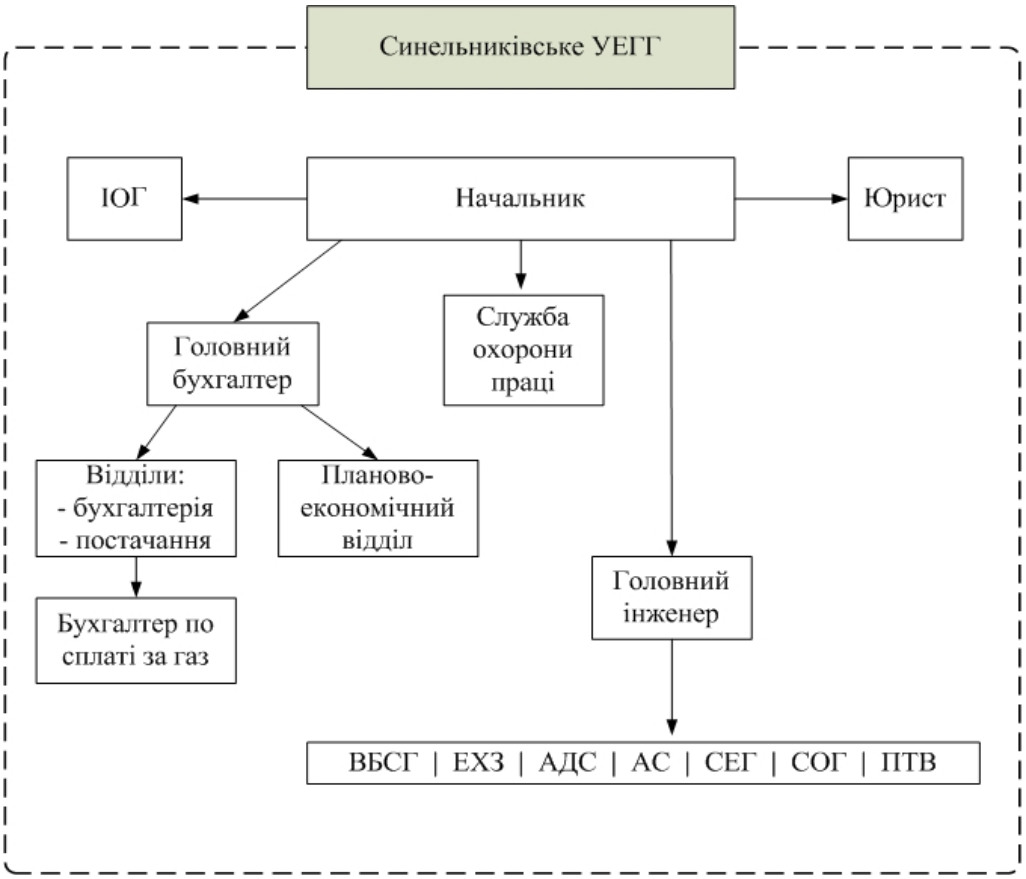



Рисунок 1.3 – Схема підрозділів

ВБСГ – внутрішньо-будинкова служба газопостачання
ЕХЗ – служба електрохімічного захисту
АДС – аварійно-диспетчерська служба
АС – аварійна служба
СЕГ – служба експлуатації газопроводів
ПТВ – планово-технічний відділ
СОГ – служба обліку газу
ІОГ – інформаційно-обчислювальна група

Гаражі і ремонтні цехи являють собою одноповерхові цегляні будівлі з односкатним дахом покритим смолою. Обладнані металевими вхідними дверми з навісним замком, а також металевими воротами.

Електроживлення ведеться від міської мережі через трансформаторну підстанцію, яка розташована на території підприємства. Від підстанції живлення подається на електрощитові у адміністративному корпусі, абонентському відділі та гаражах.

Водопостачання ведеться від міського водопроводу. Водопровід мається у адміністративному корпусі, абонентському відділі та гаражах. Каналізація централізована, під'єднана до міської мережі і використовується як для потреб співробітників, так і в рамках технологічного процесу.

Система опалення незалежне, централізоване. Газопостачання до котельної ведеться від службового газопроводу.

Від котельної ведеться система металевих труб і радіаторів у адміністративному корпусі і абонентському відділі.

### 1.1.2 Аналіз структури і призначення інформаційних служб

Інформаційно-обчислювальна група (далі – ІОГ) є структурним підрозділом Синельниківського УЕГГ ПАТ "Дніпропетровськгаз" (далі – ПАТ) і знаходиться в безпосередньому підпорядкуванні головного інженера УЕГГ та начальника інформаційно-обчислювального відділу ПАТ.

Завдання ІОГ:

- впровадження обчислювальної техніки та нових програмних засобів та програм в УЕГГ;
- аналіз причини збоїв та помилок у роботі обчислювальної техніки та програмних засобів і вжиття заходів з їх усунення;
- вивчення заявки підрозділів УЕГГ на придбання обчислювальної техніки, комплектуючих деталей та периферійних пристроїв, розробку програм та

програмних засобів і вжиття заходів з їх задоволення;

- вибір типу, конфігурації та склад устаткування для вирішення інженерно-технічних та економічних завдань, пов'язаних з діяльністю УЕГГ;
- контроль своєчасного заповнення баз даних по програмах, що впроваджуються;
- контроль за роботою користувачів, завантаження та ефективність використання обчислювальної техніки.

Функції ІОГ:

- проведення в усіх підрозділах УЕГГ робіт із впровадження автоматизованої обробки інформації та вирішення інженерних, економічних та інших завдань на основі використання засобів обчислювальної техніки;
- організація раціонального завантаження обчислювальної техніки, операторів і виконавців, забезпечення контролю за ходом вступу інформації по комп'ютерній мережі та виконанням робіт у встановлені терміни;
- створення умов для зберігання нормативної, довідкової та архівної інформації, яка неодноразово використовується в обчислювальних процесах;
- забезпечення ефективності та високої якості робіт, що виконуються, розробка і впровадження заходів щодо вдосконалення використання наявних засобів і технології механізованої та автоматизованої обробки інформації;
- участь в укладенні договорів на виконання робіт зі сторонніми установами (організаціями);
- супровід прикладних програм і програмного забезпечення для виробничих потреб УЕГГ;
- організація планового технічного обслуговування обчислювальної техніки в УЕГГ;
- організація навчання користувачів обчислювальної техніки роботі з новими програмними продуктами;
- створення та розвиток корпоративного мережевого зв’язку та локальних комп'ютерних мереж.

Таблиця 1.1 – Взаємодія ІОГ

| **ІОГ отримує** | **ІОГ представляє** |
|---|---|
| Від усіх підрозділів УЕГГ<br><br>Пропозиції для включення в річний і перспективний план комп'ютеризації, пропозиції та технічні завдання на розробку програмного забезпечення.<br>Склад інформації для збору і передачі по корпоративним каналам зв'язку. | Усім підрозділам УЕГГ<br><br>Пропозиції із автоматизації обчислювальних процесів, можливості комп'ютеризації, інформація про нові розробки, пропозиції із автоматизації передачі та обробки ділової інформації |
| Від бухгалтерії<br>фінансової та планово-економічної групи<br><br>Інформацію про оплату робіт із технічного обслуговування обчислювальної техніки, договірних робіт, рахунків на придбання устаткування і комплектуючих, про виділення засобів на придбання нової обчислювальної техніки, програмного забезпечення і комплектуючих. | Бухгалтерії,<br>фінансовій та планово-економічній групі<br><br>Плани комп'ютеризації, договори на постачання і обслуговування засобів обчислювальної техніки, розподіл придбаного устаткування, заявки на виділення засобів для придбання обчислювальної техніки, програмного забезпечення та літератури. |
| Від виробничо-технічного відділу<br>Технічну інформацію про особливості експлуатації і технічного обслуговування газового господарства, кількість абонентів та газових приладів для визначення об'ємів масового обслуговування населення. | Виробничо-технічному відділу<br>Пропозиції із автоматизації ведення архівів та баз даних. |

З метою забезпечення безпеки на підприємстві працює служба економічної безпеки (далі СЕБ), на яку покладається реалізація наступних основних завдань:

- вивчення, аналіз і оцінка стану організації безпеки підприємства, розробка пропозицій і рекомендацій для її удосконалення;
- попередження та локалізація реальних і потенційних погроз з боку потенційних споживачів, недобросовісних конкурентів та кримінальних структур
- життєве важливим інтересам підприємства, його співробітникам;
- взаємодія з територіальними структурами виконавчої служби Міністерства юстиції, МВС України та інших правоохоронних органів у частині повернення дебіторської заборгованості;
- захист таємниці та конфіденційної інформації;
- моніторинг відомостей про установи, організації та фірми, що

зацікавлені в отриманні інформації, яка становить комерційну таємницю або інші конфіденційні дані, з метою недопущення нанесення шкоди інтересам підприємства;

- перевірка надійності підприємств, установ та організацій, які виступають в якості контрагентів при укладанні договорів підприємства;
- контроль і аналіз обстановки, що складається в структурних підрозділах ПАТ;
- охорона приміщень і матеріальних цінностей підприємства, його співробітників;
- створення сприятливих умов для здійснення підприємства своєї діяльності.

З метою реалізації завдань виконує наступні функції за такими напрямками:

Внутрішня економічна безпека:

- контроль за дотриманням співробітниками діючих у підприємства та його структурних підрозділах режимів, встановлених згідно з вимогами відповідних положень та інструкцій Міністерства палива та енергетики України, НКРЕ України, внутрішніх нормативних документів НАК «Нафтогаз України», ПАТ «Дніпропетровськгаз», за необхідності, перевіряє дотримання працівниками підприємства їх функціональних обов'язків, забезпечення захисту комерційної таємниці та конфіденційної інформації;
- сприяння в організації якісного підбору кадрів на роботу у підприємства, відстеження наявності небезпечних для підприємства тенденцій у поведінці співробітників, що звільняються;
- вивчення інформації про ділові та особисті якості співробітників ПАТ, підготовка відповідних відомостей з цих питань Голові правління підприємства, Заступнику Голови правління ПАТ з економічної безпеки;
- проведення за дорученням Заступника Голови правління ПАТ з

економічної безпеки службових перевірок та розслідувань за фактами виявлених порушень з боку співробітників;

- у межах своєї компетенції бере участь у проведенні планових та позапланових перевірок структурних підрозділів ПАТ;
- взаємодія з правоохоронними органами в частині сприяння та надання практичної допомоги по кримінальних справах, порушених за ініціативою ПАТ;
- збір, накопичення, узагальнення та аналіз відомостей, що мають практичне значення для забезпечення економічної та інформаційної безпеки ПАТ, розробка необхідних управлінських рішень та нормативних документів з питань безпеки з метою удосконалення діяльності ПАТ;
- реалізація заходів, спрямованих на встановлення осіб з числа співробітників ПАТ, які виявляють зацікавленість до конфіденційної інформації, не маючи на це належних повноважень або необхідного доступу;
- забезпечення надійного захисту документів, що містять відомості про комерційну та службову таємницю, іншу конфіденційну інформацію;
- захист електронної інформації під час технологічного процесу її оброблення, транспортування чи зберігання в автоматизованих системах різного рівня й призначення, а також контроль за станом технічного захисту комп'ютерних мереж, телефонного та факсового зв'язку від несанкціонованого доступу.

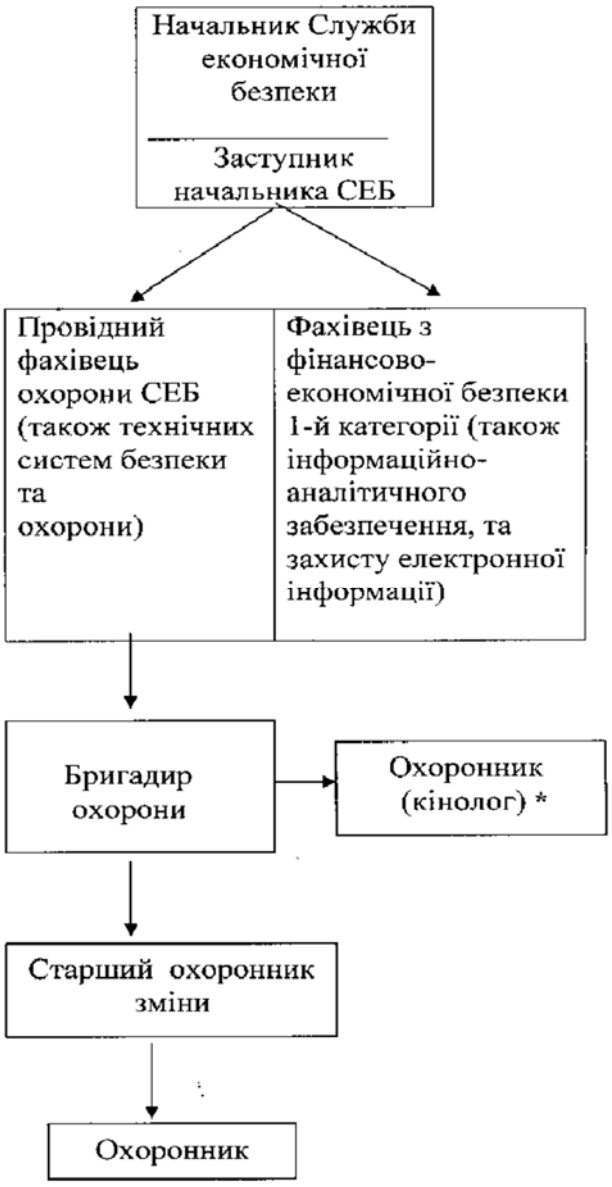



Рисунок 1.3 – Схема служби економічної безпеки

Зовнішня економічна безпека:

– перевірка, накопичення та аналітична обробка відомостей про фінансово- економічну діяльність суб'єктів: потенційних споживачів та контрагентів ПАТ (фінансовий стан, ділова репутація, засновники, партнери тощо); участь у підготовці та проведенні тендерів;
– підготовка та реалізація заходів щодо припинення протиправних зазіхань на економічні інтереси ПАТ, збір необхідної інформації з метою попередження та відшкодування заподіяного матеріального збитку;

- супроводження та забезпечення економічних інтересів ПАТ при здійсненні господарських операцій;
- взаємодія з правоохоронними органами в частині сприяння та надання практичної допомоги у кримінальних справах, порушених за ініціативою ПАТ;
- забезпечення взаємодії з місцевими органами влади, структурами МВС, службою безпеки України, прокуратури, судами, підрозділами ДПА, службою безпеки інших установ з метою захисту інтересів ПАТ;
- за необхідності, разом з іншими структурними підрозділами ПАТ, у межах своєї компетенції, брати участь у підготовці відповідей (інформації) на письмові запити правоохоронних, податкових, судових та інших державних контролюючих органів.
- Охоронна діяльність (структура підрозділу зображена рис. 1.3):
- виявляє та блокує канали й способи розкрадання майна, матеріальних цінностей (обладнання, транспорту тощо), розташованих на підпорядкованій території, в складських та інших господарських, виробничих та службових приміщеннях, які належать ПАТ (далі - приміщень);
- вивчає і впроваджує сучасні форми і методи охорони, аналізує стан охорони приміщень, у тому числі витрати на охорону, надає пропозиції керівництву щодо її покращення;
- забезпечення пропускного та внутрішнього режиму;
- охорона установ, приміщень ПАТ за допомогою технічних засобів;
- фізична охорона установ, приміщень ПАТ, його співробітників ;
- постійний контроль за несенням служби охоронцями;
- участь у підготовці завдань на проектування, забезпечення контролю за якісним і своєчасним виконанням робіт та прийняттям технічних засобів, відеоспостереження та охорони в експлуатацію;
- контроль за працездатністю та належною експлуатацією систем ОПС, відеоспостереження, системи контролю доступу та засобів зв'язку;

- проведення інструктажів з посадовими особами ПАТ, відповідальними за зберігання цінностей, та охоронцями щодо порядку здачі під охорону (зняття з охорони) приміщень ПАТ, правил користування засобами сигналізації;
- контроль за своєчасним проведенням регламентних робіт та обслуговуванням технічних засобів охорони;
- збір інформації щодо забезпечення належного контролю за дотриманням встановленого режиму доступу до приміщень філії ПАТ.

### 1.1.3 Аналіз структури локальної обчислювальної мережі

Локальна мережа управління побудована з використанням топології – «зірка». Функціональні вузли мережі являють собою центральний комутатор до якого під'єднанні шість допоміжних комутаторів, що поєднують персональні комп'ютери користувачів та оргтехніку (МФУ). На підприємстві розташовані шість серверів, які знаходиться в окремому приміщенні на другому поверсі. Сервера використовуються як сервера баз даних, файл-сервер, сервер програм. Локальна мережа налічує 52 персональних комп'ютера. ЛОМ підприємства поєднана із центральним офісом у м. Дніпропетровськ через налаштоване VPN з'єднання поверх мережі Інтернет. VPN з'єднання використовує технологію MPLS (multiprotocol label switching). Доступ до мережі Інтернет надається ВАТ «Укртелеком». Послуга являє собою виділений ADSL канал з пропускною спроможністю 20 МБіт. Кожну ніч проводиться синхронізація баз даних управління з базами даних центрального офісу «Дніпропетровськгаз».

Також на даний час розробляється проект резервного каналу зв'язку з центральним офісом. Він являє собою радіоканал передачі інформації на базі мобільної мережі «Київстар». Антена буде встановлена на вже існуючій металевій вишці, яка використовується для радіозв'язку з аварійно-ремонтними бригадами.

Операційна система, яка використовується на ПК – Windows 7 Professional, на серверах – CentOS. На сервері використовується мережевий екран Netfilter .

Програмне оснащення налічує ряд вузькоспеціалізованих продуктів, таких як: 1С ЗиК, 1С-Бухгалтерія, Сибил, Gasoline, Lotus Notes. Використання цих продуктів зумовлено діяльністю підприємства і особливістю технологічного процесу.

Для забезпечення функціонування локальної мережі на підприємстві працює системний адміністратор.

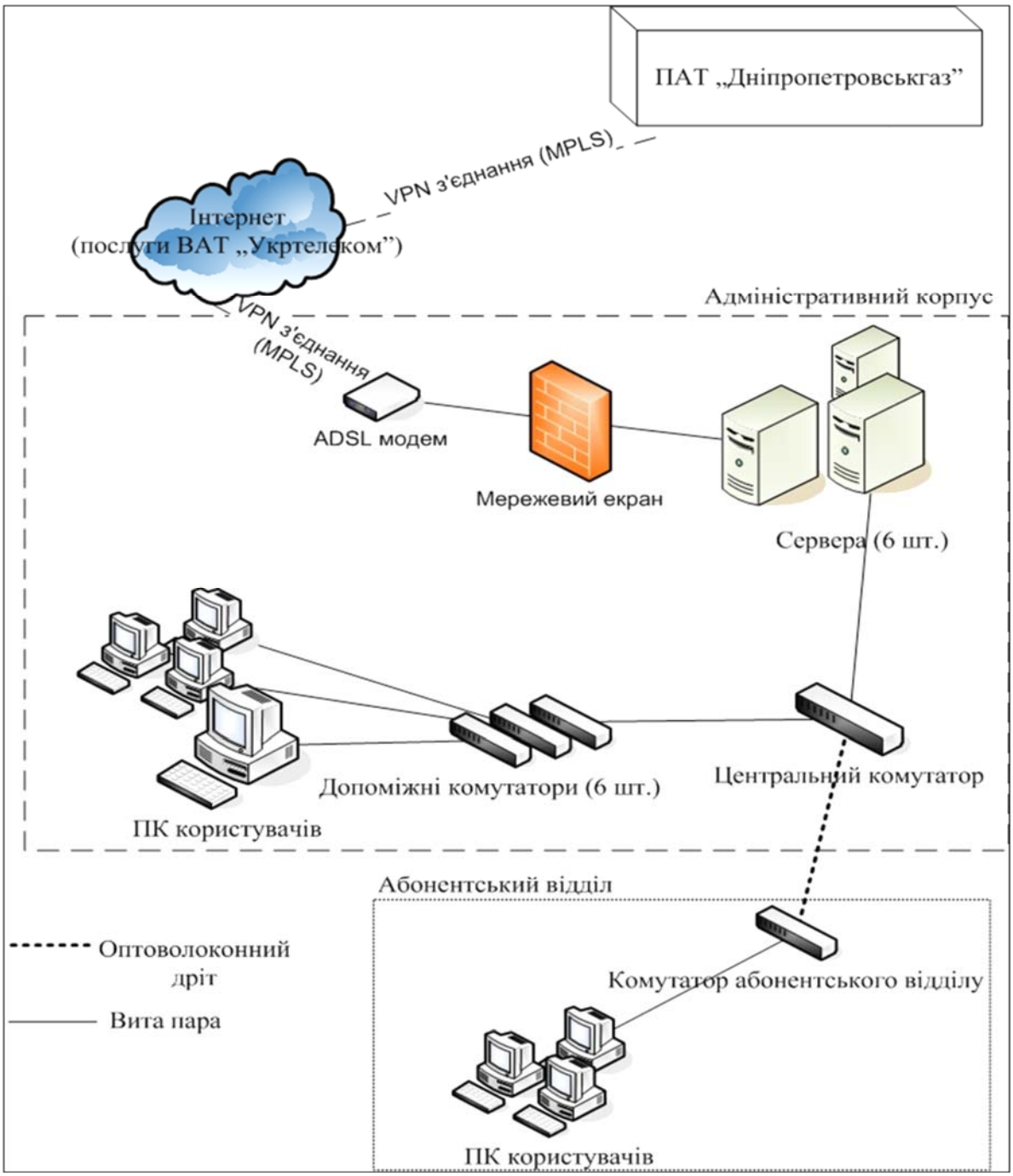



Рисунок 1.4 – Схема локальної мережі

Таблиця 1.2 - Інвентаризація апаратного забезпечення

| **Ім'я в мережі** | **Виробник** | **Модель материнської плати** | **Модель процесору** | **Об'єм жорсткого диску** | **Операційна система** |
|---|---|---|---|---|---|
| sn-ads-01 | ASUSTeK Computer INC. | P5KPL-AM IN/ROEM/SI | Intel(R) Core(TM) i5-2300 CPU @ 2.80GHz | 320 072 | Microsoft Windows XP Professional |
| sn-ads-02 | Phoenix Technologies, LTD | i845-PC87366 | Intel(R) Core(TM) i5-2300 CPU @ 2.80GHz | 40 020 | Microsoft Windows XP Professional |
| sn-ats-01 | ASUSTeK Computer INC. | P5KPL-VM | Intel(R) Celeron(R) CPU 2.80GHz | 320 072 | Microsoft Windows XP Professional |
| sn-ats-02 | GigaByte Technology Co., Ltd. | VT8601 | Intel(R) Celeron(R) CPU 2.80GHz | 40 020 | Microsoft Windows XP Professional |
| sn-buh-01 | ASUSTeK Computer INC. | P5KPL-AM IN/ROEM/SI | Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz | 327 704 | Microsoft Windows XP Professional |
| sn-buh-02 | ASUSTeK Computer INC. | P5KPL-AM IN/ROEM/SI | Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz | 327 704 | Microsoft Windows XP Professional |
| sn-buh-03 | ASUSTeK Computer INC. | P5PE-VM | Intel(R) Celeron(R) CPU 2.80GHz | 80 026 | Microsoft Windows XP Professional |
| sn-buh-04 | ASUSTeK Computer INC. | P5PE-VM | Intel(R) Celeron(R) CPU 2.80GHz | 80 026 | Microsoft Windows XP Professional |
| sn-buh-05 | ASUSTeK Computer INC. | P5LD2-VM SE | Intel(R) Celeron(R) CPU 3.06GHz | 160 041 | Microsoft Windows XP Professional |
| sn-buh-06 | ASUSTeK Computer INC. | P5RD2-VM | Intel(R) Celeron(R) CPU 2.80GHz | 40 020 | Microsoft Windows XP Professional |
| sn-buh-07 | ASUSTeK Computer INC. | P5KPL-VM | Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz | 250 059 | Microsoft Windows XP Professional |
| sn-buh-08 | ASUSTeK Computer INC. | P5LD2-VM | Intel(R) Celeron(R) CPU 2.66GHz | 80 026 | Microsoft Windows XP Professional |

Продовження таблиці1.2

| **Ім'я в мережі** | **Виробник** | **Модель материнської плати** | **Модель процесору** | **Об'єм жорсткого диску** | **Операційна система** |
|---|---|---|---|---|---|
| sn-buh-09 | Phoenix Technologies, LTD | P5LD2-VM | AMD Sempron(tm) 2200+ | 40 060 | Microsoft Windows XP Professional |
| sn-dir-02 | ASUSTeK Computer INC. | P5E-VM DO | AMD Sempron(tm) 2200+ | 250 059 | Microsoft Windows XP Professional |
| sn-fin-01 | MSI | MS-7592 | AMD Sempron(tm) 2200+ | 80 026 | Microsoft Windows XP Professional |
| sn-ivo-01 | ASUSTeK Computer INC. | P8H67-M | Intel(R) Core(TM) i5-2300 CPU @ 2.80GHz | 500 107 | Microsoft Windows 7 Professional |
| sn-ivo-02 | ASUSTeK Computer INC. | P8H67-M | Intel(R) Core(TM) i5-2300 CPU @ 2.80GHz | 500 107 | Microsoft Windows 7 Professional |
| sn-lab-01 | Phoenix Technologies, LTD | P8H67-M | Intel(R) Core(TM) i5-2300 CPU @ 2.80GHz | 10 248 | Microsoft Windows XP Professional |
| sn-lab-02 | Intel Corporation | D865GVHZ | Intel(R) Celeron(R) CPU 2.40GHz | 43 879 | Microsoft Windows XP Professional |
| sn-ok-01 | ASUSTeK Computer INC. | P5GC-MX/1333 | Intel(R) Celeron(R) CPU 2.40GHz | 160 041 | Microsoft Windows XP Professional |
| sn-ot-01 | ASUSTeK Computer INC. | P5KPL-AM IN/ROEM/SI | Intel(R) Celeron(R) CPU 3.06GHz | 120 034 | Microsoft Windows XP Professional |
| sn-peo-01 | ASUSTeK Computer INC. | P5KPL-AM IN/ROEM/SI | Intel(R) Celeron(R) CPU 3.06GHz | 320 072 | Microsoft Windows XP Professional |
| sn-peo-02 | ASUSTeK Computer INC. | P5KPL-VM | Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz | 250 059 | Microsoft Windows XP Professional |
| sn-pto-01 | ASUSTeK Computer INC. | P5KPL-VM | Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz | 250 059 | Microsoft Windows XP Professional |

Продовження таблиці1.2

| Ім’я в мережі | Виробник | Модель материнської плати | Модель процесору | Об’єм жорсткого диску | Операційна система |
|---|---|---|---|---|---|
| sn-pto-02 | ASUSTeK Computer INC. | P5KPL-VM | Core(TM)2 Duo CPU E4600 @ 2.40GHz | 250 059 | Microsoft Windows XP Professional |
| sn-pto-03 | ASUSTeK Computer INC. | P8H67-M | Core(TM)2 Duo CPU E4600 @ 2.40GHz | 500 107 | Microsoft Windows 7 Professional |
| sn-pto-04 | ASUSTeK Computer INC. | P5GC-MX/1333 | Intel(R) Celeron(R) CPU 2.40GHz | 80 026 | Microsoft Windows XP Professional |
| sn-rmu-01 | ASUSTeK Computer INC. | P8H67-M | Intel(R) Celeron(R) CPU 2.40GHz | 500 107 | Microsoft Windows 7 Professional |
| sn-sls-01 | ASUSTeK Computer INC. | P5PE-VM | AMD Sempron(tm) 2200+ | 40 060 | Microsoft Windows XP Professional |
| sn-sls-02 | Phoenix Technologies, LTD | | AMD Sempron(tm) 2200+ | 40 060 | Microsoft Windows XP Professional |
| sn-slu-01 | ASUSTeK Computer INC. | P5GC-MX/1333 | Core(TM)2 Duo CPU E4600 @ 2.40GHz | 160 041 | Microsoft Windows XP Professional |
| sn-slu-02 | ASUSTeK Computer INC. | P7P55 LX | Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz | 500 107 | Microsoft Windows 7 Professional |
| sn-slu-03 | ASUSTeK Computer INC. | P7P55 LX | Intel(R) Core(TM) i3 CPU 540 @ 3.07GHz | 503 927 | Microsoft Windows 7 Professional |
| sn-slu-04 | ASUSTeK Computer INC. | P5KPL-AM IN/ROEM/SI | Intel(R) Core(TM) i3 CPU 540 @ 3.07GHz | 320 072 | Microsoft Windows 7 Professional |
| sn-slu-05 | Intel Corporation | D865GBF | Intel(R) Core(TM) i3 CPU 540 @ 3.07GHz | 40 020 | Microsoft Windows XP Professional |
| sn-slu-06 | Intel Corporation | D865GLC | Core(TM) i3 CPU 540 @ 3.07GHz | 20 020 | Microsoft Windows XP Professional |

Продовження таблиці1.2

| Ім’я в мережі | Виробник | Модель материнської плати | Модель процесору | Об’єм жорсткого диску | Операційна система |
|---|---|---|---|---|---|
| sn-slu-07 | Intel Corporation | D865GVHZ | Intel(R) Celeron(R) CPU 2.40GHz | 40 020 | Microsoft Windows XP Professional |
| sn-slu-08 | Intel Corporation | D845GRG | Intel(R) Celeron(R) CPU 2.40GHz | 19 092 | Microsoft Windows XP Professional |
| sn-slu-09 | Intel Corporation | D865GVHZ | Intel(R) Celeron(R) CPU 2.40GHz | 40 020 | Microsoft Windows XP Professional |
| sn-slu-10 | Intel Corporation | D865GLC | Intel(R) Xeon(R) CPU E5335 @ 2.00GHz | 40 020 | Microsoft Windows XP Professional |
| sn-slu-11 | ASUSTeK Computer INC. | P5KPL-CM | Intel(R) Celeron(R) 2.00GHz | 83 880 | Microsoft Windows XP Professional |
| sn-slu-12 | Shuttle Inc | MK35 | Intel(R) Celeron(R) CPU 440 @ 2.00GHz | 40 060 | Microsoft Windows XP Professional |
| sn-slz-01 | ASUS | P4BP-MX | Intel(R) Celeron(R) CPU 440 @ 2.00GHz | 41 110 | Microsoft Windows XP Professional |
| sn-srv-01 | Supermicro | X7DVL | Intel(R) Xeon(R) CPU E5335 @ 2.00GHz | 390 061 | Microsoft(R) Windows(R) Server 2003, Standard Edition |
| sn-srv-02 | INTEL_ | D865GLC_ | Intel(R) Celeron(R) CPU 2.40GHz | 160 052 | Microsoft(R) Windows(R) Server 2003, Standard Edition |
| sn-srv-03 | Supermicro | P4DE6 | Intel(R) XEON(TM) CPU 2.00GHz | 220 028 | Microsoft(R) Windows(R) Server 2003, Standard Edition |
| sn-srv-04 | HP | ProLiant ML350 G6 | Intel(R) Xeon(R) CPU X5650 @ 2.67GHz | 2 479 810 | Microsoft(R) Windows(R) Server 2003 Standard x64 Edition |
| sn-srv-06 | ASUSTeK Computer INC. | P5KPL-VM | Core(TM)2 Duo CPU E4500 @ 2.20GHz | 390 061 | Ubuntu 11.10 |

Продовження таблиці1.2

| Ім’я в мережі | Виробник | Модель материнської плати | Модель процесору | Об’єм жорсткого диску | Операційна система |
|---|---|---|---|---|---|
| sn-srv-07 | Intel Corporation | D865GLC | Intel(R) Celeron(R) CPU 2.40GHz | 38 167 | CentOS release 5.2 (Final) |
| sn-ur-01 | ASUSTeK Computer INC. | P8H67-M | Intel(R) Celeron(R) CPU 2.40GHz | 500 107 | Microsoft Windows 7 Professional |
| sn-vdgo-03 | Award Software International, Inc. | i815EP-W83627 | Intel(R) Celeron(R) CPU 2.40GHz | 20 547 | Microsoft Windows XP Professional |

### 1.1.4 Аналіз переліку інформації з обмеженим доступом

На об’єкті інформаційної діяльності філії ПАТ «Дніпропетровськгаз» циркулює інформація, що належить державі і перебуває у володінні та розпорядженні філії ПАТ «Дніпропетровськгаз».

Перелік інформації з обмеженим доступом являє собою задокументований перелік відомостей, що становлять конфіденційну інформацію і має наступний вигляд:

1) плани, аналітичні довідки, довгострокові перспективи ПАТ;
2) штатні розклади філії ПАТ;
3) особисті справи співробітників філії ПАТ;
4) зведені дані, інформація про вартість природного й зрідженого газу;
5) інформація про стан банківських рахунків. Виписки банку;
6) інформація про джерела кредитів і умовах їхнього одержання. Договори, контракти;
7) інформація про стан кредитів і боргових зобов'язань. Узагальнений бухгалтерський облік;
8) інвестиційна діяльність. Плани, письма;
9) акти комплексних і документальних ревізій фінансово-господарської діяльності. Акти, довідки;

10) аналітичні документи по бухгалтерському обліку і дані про зарплату. Рахунки, накладні, розрахункові відомості;
11) інформація про дебіторську і кредиторську заборгованість. Аналітичні звіти й довідки;
12) зведений баланс природного й зрідженого газу;
13) плановий розподіл ресурсів природного й зрідженого газу. Аналітичні довідки, розрахунки, листи;
14) обсяги реалізації природного газу споживачам і дилерам. Добові дані про використання природного газу підприємствами й містами;
15) зведені дані про комерційні зв'язки з партнерами. Аналітичні довідки, звіти, листи;
16) дані про підготовку, проведення й результати переговорів з діловими партнерами. Накази, розпорядження, протоколи нарад, засідань, переговорів, проекти договорів, договору;
17) узагальнена інформація про виконання контрактів;
18) інформація про методику розрахунку вартості робіт і послуг. Розрахунки, договори, контракти;
19) інформація про структуру, елементи й розрахунок цін на природний газ (крім населення). Розрахунки, аналітичні довідки;
20) діюча структура калькуляції продукції власного виробництва, калькуляція витрат виробництва. Розрахунки, аналітичні довідки;
21) інформація про витрати підприємства. Розрахунки, аналітичні довідки, договори, листи;
22) інформація про розміри зниження ціни на продукцію й послуги після підписання контрактів з діловими партнерами;
23) протоколи засідання наглядацьких ряд, ревізійних комісій і загальних зборів акціонерів. Устав, зміни й доповнення до нього: установчі договори, внутрішні становища;

24) дані про технічний стан раціоналізаторських пропозицій, які можуть мати комерційну цінність. Технічна документація, листи, протоколи, рішення;
25) плани трас кабельних ліній зв'язку, Технічна документація, аналітичні довідки, перспективні плани, накази, протоколи технічних рад;
26) схеми організації ліній зв'язку, технологічного зв'язку, телемеханіки й комп'ютерних мереж. Перспективи їхнього розвитку. Паролі електронної пошти, паролі;
27) загальна інформація відносно власних записів користувачів комп'ютерної мережі;
28) перелік програмного забезпечення;
29) інформація про порядок і стан організації захисту комерційної таємниці;
30) інформація про стан організаційно-технічних мір комплексного захисту інформації. Схеми;
31) схеми розташування технічної, охоронної й протипожежної сигналізації;
32) інформація про порядок охорони стаціонарних об'єктів;
33) організація профілактичних заходів для питань безпеки;
34) матеріали перевірок, ревізій, службових розслідувань;
35) інформація відносно претензійно - позовної роботи;
36) інформація відносно дозволу судових справ;
37) опис системи реалізації обмежень доступу та регулювання проходу і проїзду, зберігання бланків перепусток;
38) відомості про питому міцність фізичних бар'єрів на шляхах проникнення до життєве важливих місць, уразливих у терористичному відношенні;
39) відомості про місця установлення та принцип дії приладів і пристроїв, що використовуються у системах фізичного захисту, або охорони на підприємствах філії ПАТ «Дніпропетровськгаз»;

40) порядок взаємодії персоналу об'єкта та караулу охорони під час здійснення доступу персоналу до виконання робіт у місцях, що охороняються.
41) облікові картки про надання допуску до державної таємниці;
42) номенклатура посад працівників, робота яких передбачає оформлення допуску до державної таємниці;
43) накази та розпорядження про надання (скасування) допуску до державної таємниці.

Для обробки інформації використовується такі програмні продукти:

- 1С Зарплата и Кадри;
- 1С-Бухгалтерія;
- Сибил;
- Gasoline;
- Microsoft Office.

Для розсилки документів використовується Lotus Notes.

Інформація зазначена у пунктах 1-4 зберігається на паперових носіях у відповідних відділах. Зокрема плани, аналітичні довідки, довгострокові перспективи

ПАТ надаються на паперових носіях у центральному офісі «Дніпропетроськгаз» чи безпосередньо від НАК «Нафтогаз». Інформація зазначена у пунктах 5-7 зберігається у відповідних банківських установах. Доступ до цієї інформації (з подальшою передачею і обробкою) здійснюється за допомогою клієнт-банківської системи через мережу Інтернет. Доступ надається бухгалтерам з відповідними правами. Інформація пунктів 8, 9 передається у програмній середі Lotus Notes з подальшою обробкою і зберіганням на ПК чи паперових носіях. Аналітичні документи по бухгалтерському обліку і дані про зарплату, рахунки, накладні, розрахункові відомості обробляється у програмній середі 1С Зарплата и Кадри і в подальшому зберігається на ПК чи паперових носіях. Інформація зазначена у пунктах 15-20 надається безпосередньо з НАК «Нафтогаз» через відповідні відомства по каналу зв’язку. Інформація зазначена у пунктах 25-33 та 37-43

обробляється СЕБ. Інформація зазначена у пунктах 34-36 обробляється відповідними службами до яких вона поступила у електронному вигляді чи на паперових носіях. Приклади інформаційних потоків схематично зображені на рис. 1.5 та рис.1.6.

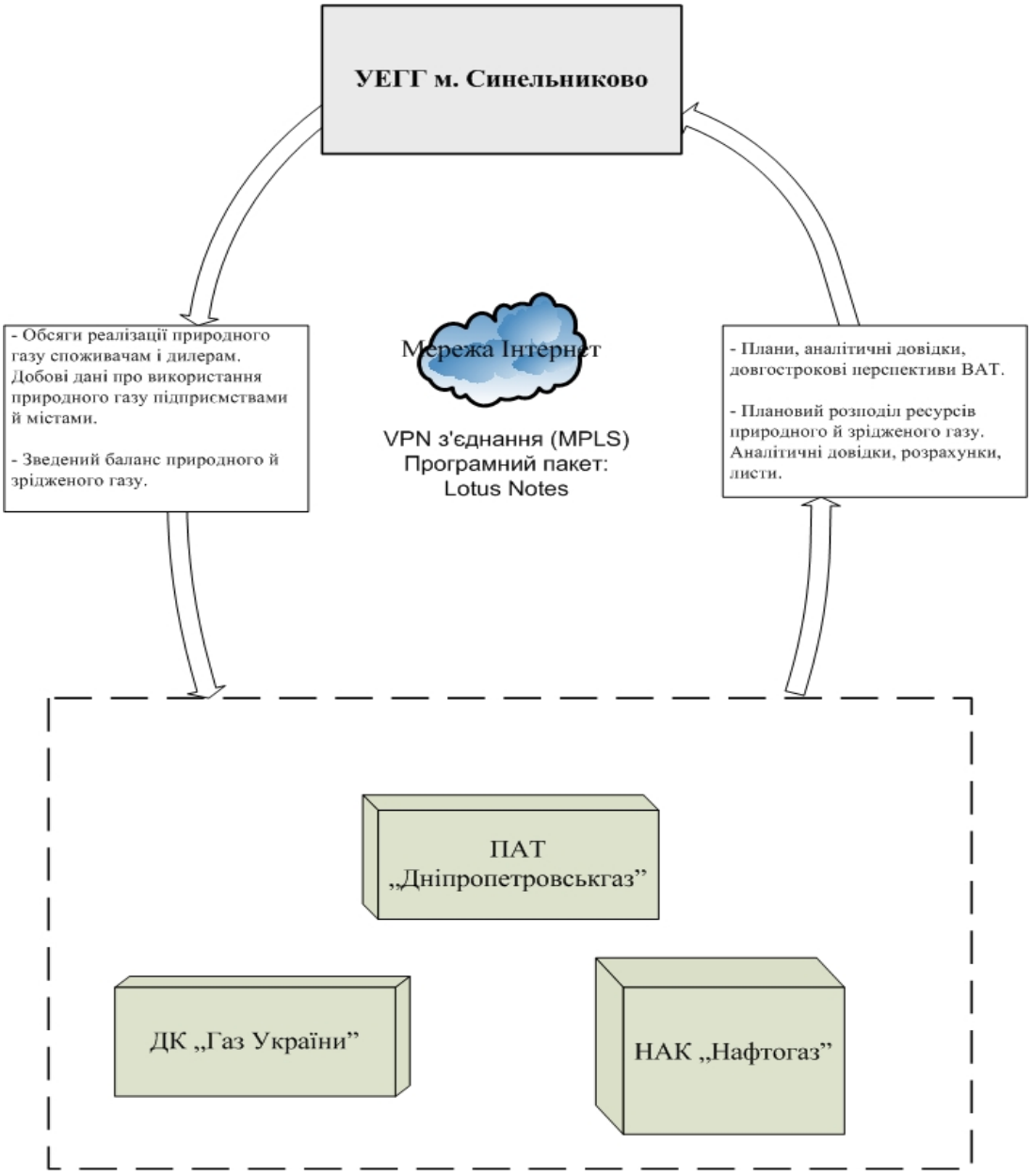



Рисунок 1.5 – Схема циркуляції інформації з керуючими компаніями

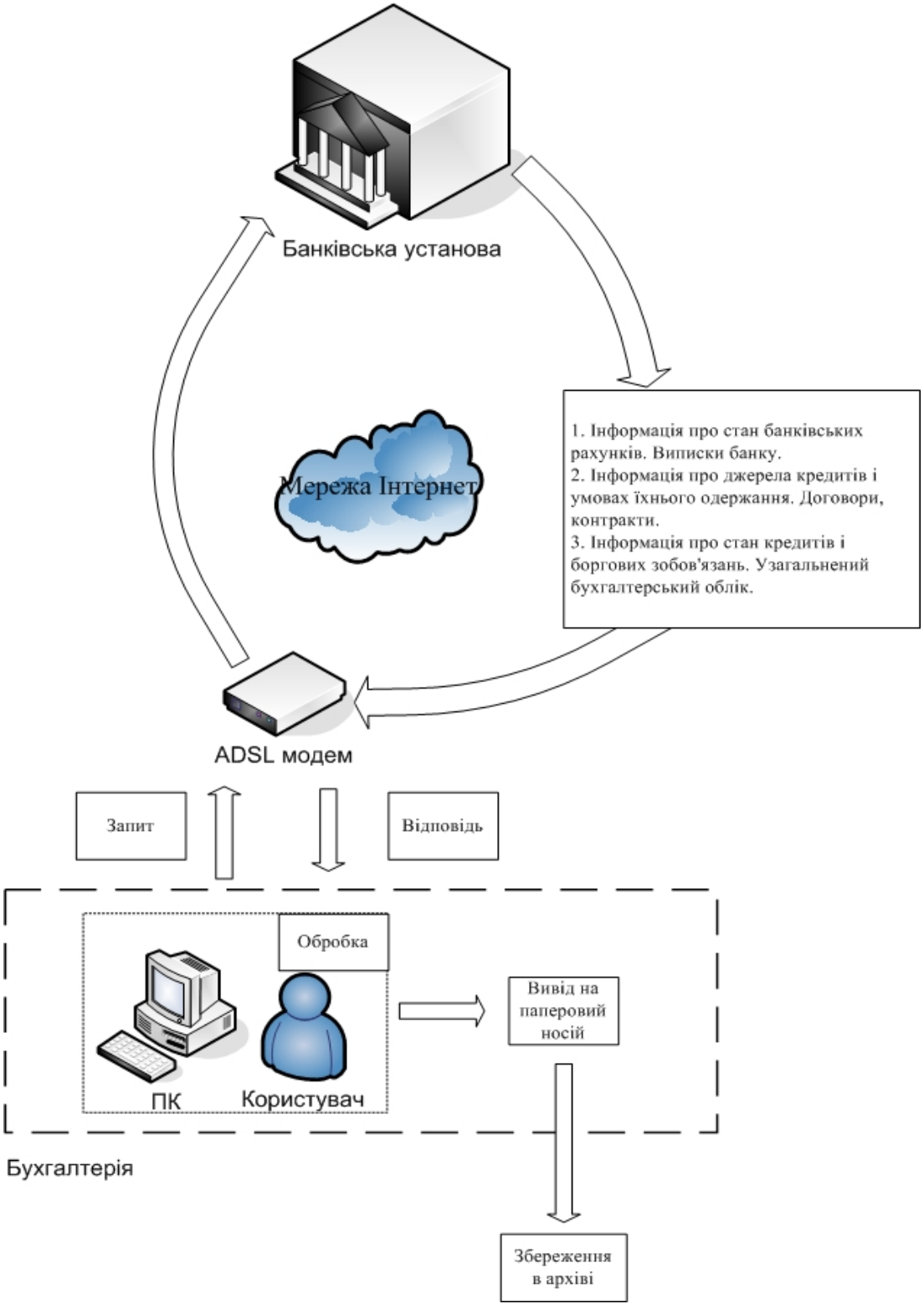



Рисунок 1.6 – Схема запиту до банківської інформації

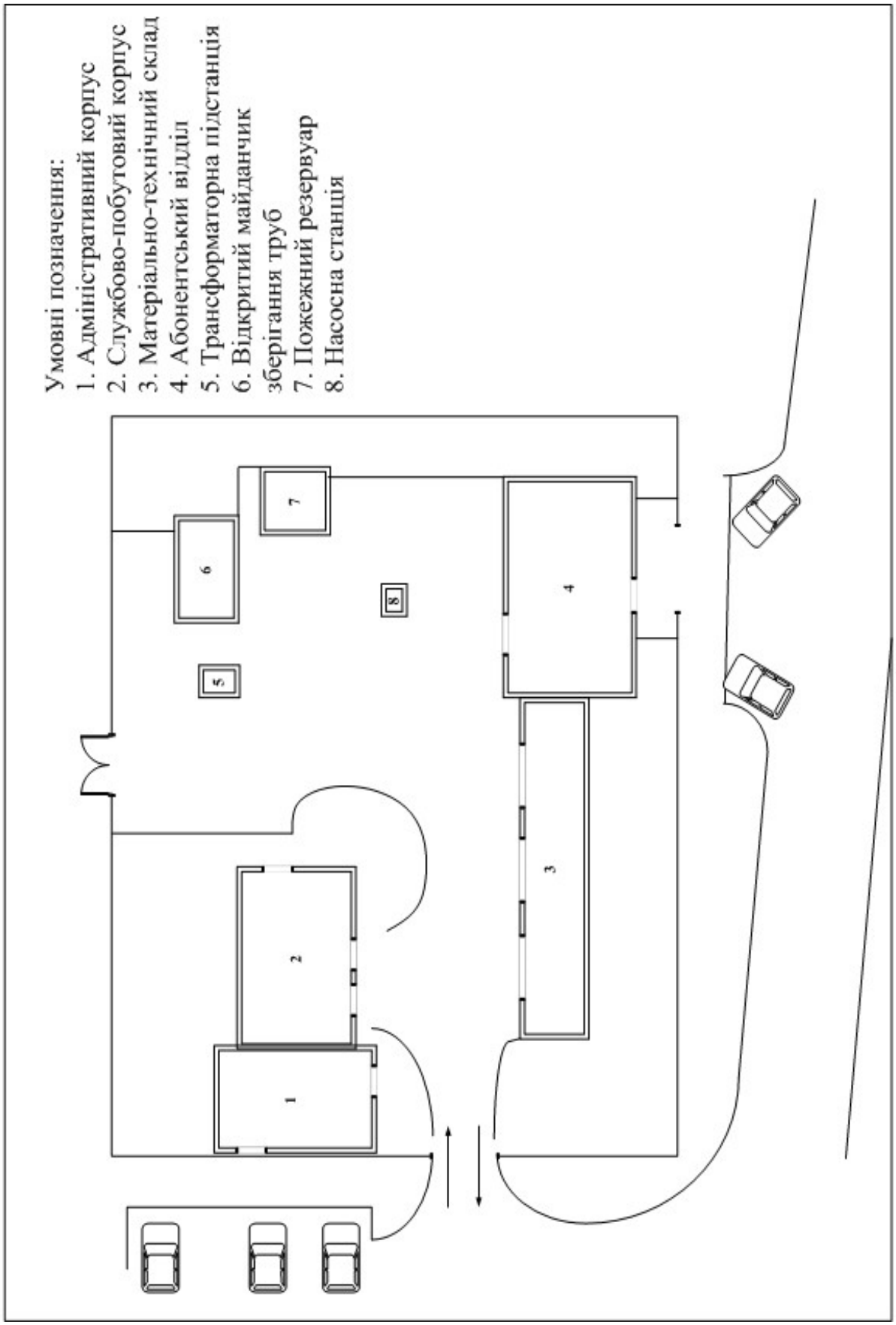
## 1.2 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

### 1.2.1 Модель загроз витоку інформації з обмеженим доступом

На території філії ПАТ «Дніпропетровськгаз» в м. Синельниково знаходяться:

- адміністративний корпус;
- службово-побутовий корпус;
- матеріально-технічний склад;
- абонентський відділ;
- трансформаторна підстанція;
- відкритий майданчик зберігання труб;
- пожежний резервуар;
- насосна станція.

Підприємство знаходиться на перехресті вул. Миру і 8 Березня. Зі сходу до паркану прилягає парк (переважно акація, клен та бук), який простягається від вул. 8 Березня вздовж паркану до кінця старої території управління. На півночі знаходиться підстанція і територія старого управління з будівлями, які нині не використовуються, далі – двоповерхові жилі будинки. На заході через дорогу розташовується пустир, який простягаються приблизно на 150 м до полоси дерев, за якими починається поле, навпроти корпусу є відкрита стоянка, також автомобілі зупиняються вздовж дороги біля пустиря. В південній стороні через дорогу знаходиться жилий сектор, з приватними одноповерховими будинками. В південно-західному напрямку на відстані 40 м від паркану знаходиться крамниця будівельних матеріалів, автомийка та пункт прийому металобрухту (всі споруди прилягають один до одного і знаходяться на території одного власника). Схема розташування структур зображена на рис. 1.7, ситуаційний план зображений на рис. 1.8.




с

Рисунок 1.7 – Схема розташування об’єктів

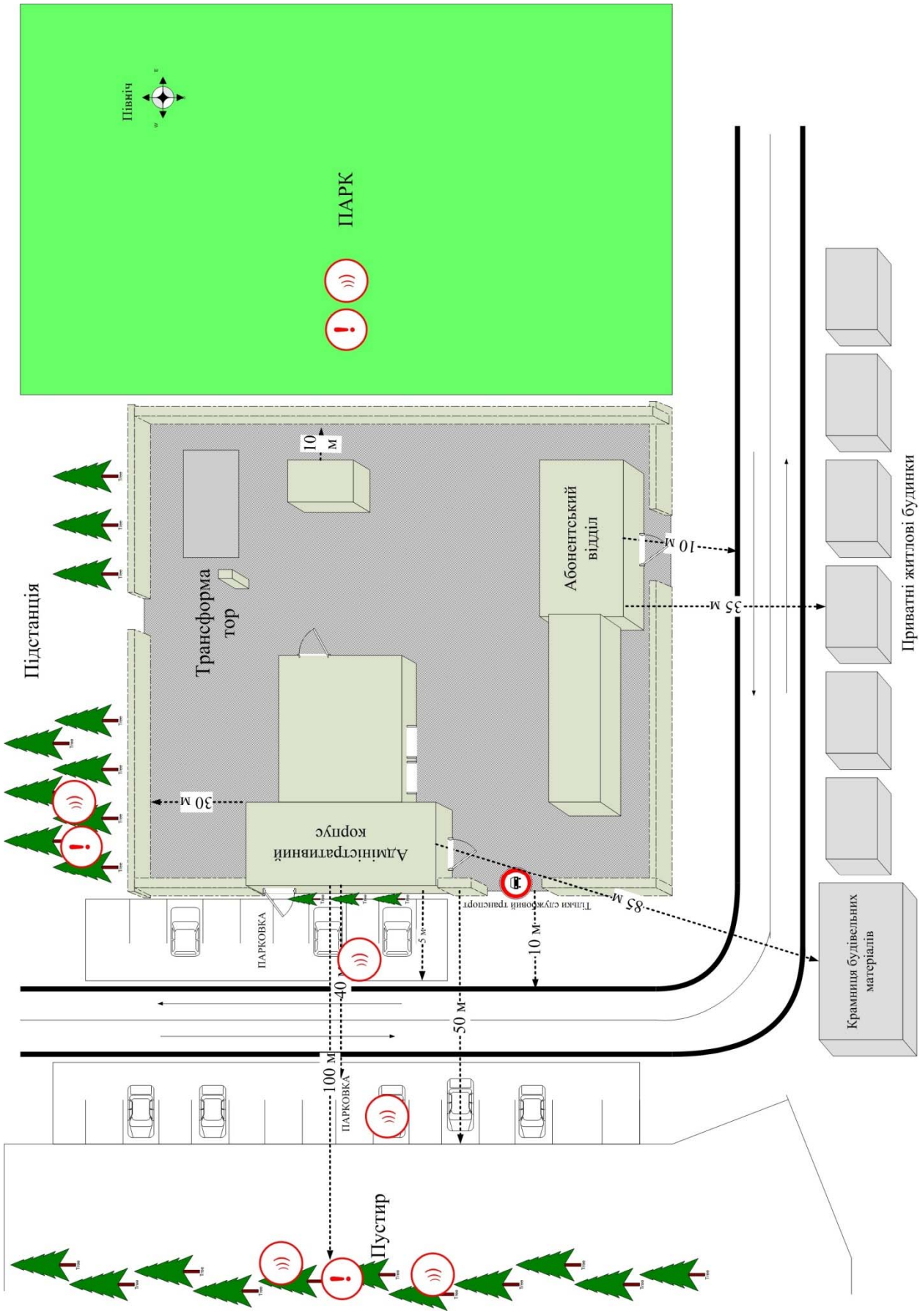



Рисунок 1.8 – Ситуаційний план

### 1.2.2 Визначення меж контрольованої зони

Згідно із визначенням контрольована зона – це територія на якій неможливе перебування осіб, чи транспортних засобів, які не мають перепустки. Опираючись на це визначення, а також на результати проведеного обстеження та враховуючи особливості технологічного процесу на підприємстві можна зробити висновок, що встановлення меж контрольованої зони в межах огородженої території при діючому режиму доступу не являється можливим. Також не вдається обмежити контрольовану зону адміністративним корпусом. Це обумовлене наступними причинами:

- доступ на територію підприємства в робочий час (з 8 до 17г) можливий для будь-яких осіб;
- перебування осіб на огородженій території і в будівлях не контролюється.

Контрольоване перебування відвідувачів можливе лише на робочих місцях у кабінетах співробітників підприємства. Проїзд контролюється охороною, тому проїзд транспорту, що не належить підприємству не можливий. Транспортні засоби співробітників розміщуються за межами огородженої території на відкритій стоянці.

## 1.3 Огляд існуючих інженерних рішень КС в галузі

### 1.3.1 Аналіз технічних каналів витоку інформації

Озвучення мовної інформації з обмеженим доступом можливе у наступних випадках:

- при проведенні переговорів і нарад у залі засідань;
- при ділових зустрічах у кабінетах начальника, головного бухгалтера, юриста, головного інженера;
- в рамках технологічного процесу у приміщеннях служб ІОГ, АДС, ПЕВ.

Опираючись на результати обстеження можна виділити наступні канали витоку акустичної інформації:

Таблиця 1.3 – Характеристика каналів витоку акустичної інформації

| Назва каналу | Тип ТЗР і місце встановлення | За рахунок чого реалізується |
|---|---|---|
| Повітряний | Направлений мікрофон<br><br>Встановлення можливе на деревах, що розташовані з півночі та заходу. | Перехват конфіденційної інформації при її озвученні у приміщеннях, що мають вікна з північної та західної сторін. Перехват може реалізовуватись з використанням направленого мікрофона, в той час, коли у приміщеннях відчинені вікна. |
| Оптико-електронний | Лазерний мікрофон<br><br>Встановлення можливе на деревах, що розташовані з півночі та заходу. | Перехват конфіденційної інформації при її озвученні у приміщеннях, що мають вікна з північної та західної сторін. |
| Вібраційний | Електронний стетоскоп<br><br>Вікна і віконні рами західної сторони адміністративного корпусу, стіни і труби системи опалення на сходах та коридорі. | Вздовж західної стіни адміністративного корпусу ростуть дерева (по висоті будівлі), що надає доступ до вікон на другому і третьому поверсі. Також через неконтрольоване перебування осіб на території, дозволяє зловмиснику без перешкод встановити датчики на труби системи опалення чи стіни на сходах. |

### 1.3.2 Канали витоку інформації, що обробляється ТЗПІ

Серед технічних каналів витоку інформації, що оброблюється технічними засобами прийому, обробки і передачі інформації можна виділити електричний, за рахунок просочування інформативного сигналу в кола електроживлення та заземлення. У зв’язку з тим, що не встановлена контрольована зона, зловмисник має доступ до лінії електроживлення на ділянці від трансформатору, а також до виводу заземлення.

Канал ПЕМВН існує за рахунок розповсюдження електромагнітного поля, який може бути модульоване інформативним сигналом. Джерелами цього випромінювання є ОТЗС розташовані у приміщенні серверної на другому поверсі адміністративного корпусу, а також приміщеннях служб де оброблюється інформація з обмеженим доступом. Також ці випромінювання можуть наводитись на лінії інженерних комунікацій, таких як електрична мережа.

Тому досить вірогідне:

– застосування ТЗР для перехоплення інформативних сигналів з кола електроживлення;
– розміщення ТЗР у автомобілях, які можуть бути розташовані на відстані 10 м від адміністративного корпусу із заходу.

### 1.4 Визначення можливих напрямків рішення поставлених завдань

Проаналізувавши результати проведеного обстеження та моделі загроз можна зробити висновок, що канали витоку інформації існують за рахунок наступних причин:

– недостатня інформованість співробітників філії про важливість забезпечення безпеки інформації з обмеженим доступом;
– відсутність системи контролю і управління доступом;
– архітектурні особливості споруд, їх розташування на місцевості, особливості оточуючого середовища.

Тому для захисту інформації від витоку технічними каналами необхідно створити комплекс технічного захисту інформації. До етапів проектування комплексу ТЗІ пропонується включити:

- проектування виділеного приміщення в кімнаті для ведення переговорів і нарад;
– розробку системи відеонагляду;
– проектування захищеного приміщення серверної;
– розробку організаційних заходів захисту інформації.

### 1.5 Висновок

В розділі стан питання і постановка задачі було проведене обстеження інформаційної діяльності філії «Дніпропетровськгаз», за результатами обстеження була розроблена модель загроз інформації, в якій було розроблено ситуаційний план і проаналізовані технічні канали витоку інформації. Опираючись на отримані результати була поставлена задача на проектування комплексу технічного захисту інформації.

# 2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ КОМП'ЮТЕРНА СИСТЕМА ФІЛІЇ АТ «ДНІПРОПЕТРОВСЬКГАЗ»

## 2.1 Вимоги до системи в цілому

Об'єктом розробки є комплекс технічного захисту інформації філії Публічного акціонерного товариства «Дніпропетровськгаз» в місті Синельниково.

Область застосування – об'єкт інформаційної діяльності філії Публічного акціонерного товариства «Дніпропетровськгаз» в місті Синельниково.

Вихідними даними для розробки комплексу ТЗІ є результати обстеження об'єкту інформаційної діяльності філії ПАТ «Дніпропетровськгаз» в місті Синельниково та Модель загроз.

Комплекс ТЗІ призначений для захисту інформації з обмеженим доступом від витоку технічними каналами на ОІД філії ПАТ «Дніпропетровськгаз».

Комп'ютерна система повинна виконувати наступні функції:

Збір інформації.  Повинен забезпечуватися прийом відео потоку від IP – камер що встановлені в приміщеннях підприємства та передача цих даних для подальшого аналізу та обробки та зберігання.

Аналіз та обробка інформації. Комп'ютерна система повинна на підставі отриманих даних проводити їх попередню обробку і проводити аналіз з видачею результатів відповідно до закладених алгоритмів роботи.

Зберігання оперативних даних системи, даних для формування аналітичних звітів, документів системи, сформованих у процесі роботи. Ця функція повинна забезпечити періодичне резервне копіювання і збереження даних на додаткових носіях інформації.

Запис відео потоків камер проводиться на носії, що встановлені на відео сервері. Вся відеоінформація, що зберігатиметься на сервері підприємства належить до інформації з обмеженим доступом, та захищається на основі технології DRM, що позбавляє користувача прямого доступу комп'ютера.

Комплекс ТЗІ створюється з метою підвищення рівня інформаційної безпеки філії шляхом запобігання неконтрольованого розповсюдження конфіденційної інформації під час її обробки технічними засобами, а також при її озвученні під час проведення нарад, переговорів тощо.

Впровадження комплексу ТЗІ сприяє захисту інтересів ПАТ «Дніпропетровськгаз», а також держави і дозволить мінімізувати збитки, що може спричинити витік інформації з обмеженим доступом.

Впровадження комплексу ТЗІ сприяє захисту інтересів ПАТ «Дніпропетровськгаз», а також держави і дозволить мінімізувати збитки, що може спричинити витік інформації з обмеженим доступом.

Комп’ютерна система повинна включати обладнання необхідне для підключення до загальнопромислової мережі, програмне забезпечення яке реалізує алгоритм управління, сервер баз даних. Система повинна включати наступні підсистеми: передачі інформації, відображення, вводу та доступу до інформації, аналізу інформації, управління, збору інформації, аварійного захисту та інтеграції з ыншими системами.

Функціонування системи має відповідати наступним критеріям: забезпечувати безперебійне функціонування системи; забезпечення мінімального часу на обслуговування; забезпечувати можливість роботи в різних режимах.

### 2.1.1 Вимоги до структури і функціонуванню системи

До складу комплексу ТЗІ повинні входити наступні інженерно-технічні засоби і заходи:

- організація виділеного приміщення для ведення переговорів і нарад, на яких озвучується інформація з обмеженим доступом;
- розробка системи відеонагляду;
- розробка інженерно-технічних заходів для захисту інформації від витоку технічними каналами зазначених у моделі загроз;
- розробка захищеного приміщення серверної.

Комп’ютерна система повинна забезпечувати наступні показники призначення:

- обмеження доступу співробітників і відвідувачів об'єкта в приміщення, що охороняються;
- часовий контроль переміщень співробітників і відвідувачів по об'єкту;
- контроль над діями охорони під час чергування;
- табельний облік робочого часу кожного співробітника;
- фіксацію часу приходу і відходу відвідувачів;
- часовий і персональний контроль відкриття внутрішніх приміщень;
- реєстрацію та видачу інформації про спроби несанкціонованого проникнення в приміщення.
- аналіз відеоданих відповідно до закладеного алгоритму.

Структура мережі повинна складатися з пяти під мереж LAN1 – LAN5.

Інтенсивність трафіку $\mu = 110$ (кадрів/с).

Блок адрес - 192.168.IPn.0/21; для виділення підмереж IPn = 8.

Зовнішня адреса HTTP-сервера: 209.165.200.4;

3) середня довжина вихідного повідомлення в найбільшій мережі – 600 байт;

4) затримка передачі пакету в найбільшій мережі $– \leq 5$ мс

### 2.1.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему і режиму його роботи

Підготовка операторів, інженерів та фахівців з програмного забезпечення для систем контролю здійснюється на спеціалізованих курсах відповідних фірм виробників продукції яке використовується при створенні системи, а також в політехнічних університетах.

До самостійної роботи допускаються тільки оператори, попередньо навчені, пройшли інструктаж і які засвоїли безпечні прийоми роботи.

Для забезпечення роботи системи потрібно 4 оператора, 2 інженера-системотехніка з налагодження та обслуговування обладнання.

Режим роботи персоналу – змінний.

### 2.1.3 Показники призначення

Створюваний комплекс ТЗІ має відповідати вимогам чинного законодавства України і діючим нормативно-правовим актам, тому при створенні комплексу ТЗІ слід використовувати наступні документи:

- Закон України «Про інформацію»;
- Указ про положення про технічний захист інформації в Україні;
- ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення»;
- НД ТЗІ 1.1-005-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»;
- ТР ЕОТ - 95 «Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок»;
- НД ТЗІ 3.1-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи».

Витрати на створюваний комплекс ТЗІ не повинні перевищувати можливих збитків зазнаних від витоку інформації з обмеженим доступом.

Створюваний комплекс ТЗІ має відповідати наступним умовам:

- встановлення інженерних конструкцій і технічних засобів не повинно потребувати значних змін в конструкції будівлі;
- комплекс ТЗІ не повинен заважати технологічному процесу і ведення господарства філії ПАТ «Дніпропетровськгаз», а також створювати

- незручності під час роботи працівників;
- монтаж конструкції має бути розрахований на можливе подальше удосконалення і модернізації, а також враховувати легкий демонтаж конструкцій і технічних засобів під час ремонту.

Основними критеріями при проектуванні комп'ютерної системи виробництва є критерії якості доступу до продуктивність, надійність, розширюваності та дотримання технологічних параметрів із заданою точністю.

Система повинна повністю забезпечувати режими роботи ручний та автоматичний. У разі зміни конфігурації обладнання система повинна мати можливість простого налаштування на нові умови роботи.

Під час першого налаштування обладнання повинна бути забезпечена можливість ручного режиму роботи. У тому випадку, якщо система починає працювати в штатному режим повинна бути реалізована можливість перемикання на автоматичний режим.

### 2.1.4 Вимоги до надійності

При аварійних ситуаціях - вихід з ладу окремого робочого місця не повинно приводити до втрати інформації. Перебої з електропостачанням на повинні впливати на працездатність обладнання. Необхідні резервні джерела енергії такої потужності, щоб забезпечити можливість впродовж 10 хвилин завершити роботу і зберегти дані.

Для технічних пристроїв використовуються такі показники надійності, як середній час наработки на відмову, імовірність відмови, інтенсивність відмов.

Необхідно забезпечити збереження даних і захист їх від спотворень. Крім цього, повинна підтримуватися узгодженість (несуперечність) даних, наприклад, якщо для підвищення надійності на декількох файлових серверах зберігається декілька списків даних, то треба постійно забезпечувати їх ідентичність.

Надійність програмного забезпечення повинна забезпечуватися за рахунок використання ліцензійних програмних продуктів.

На етапі повного функціонування комп’ютерної системи підприємства, її обслуговування повинно забезпечуватися системним адміністратором. Ремонт системи має виконуватися спеціалістами підрядниками. Елементи системи, що вийшли з ладу повинні замінюватися новими.

### 2.1.5 Вимоги до захисту інформації від несанкціонованого доступу

Для захисту програмного забезпечення системи від несанкціонованого доступу забороняється допуск до налаштувань та обслуговування людей, які не мають на те відповідного дозволу керівництва.

Повинна бути забезпечена програмний та апаратний захист від некваліфікованих дій користувача та від спроб несанкціонованого доступу користувачів до внутрішньо системної інформації. Залежно від статусу користувача повинні бути передбачені різні рівні доступу до внутрішньо системної інформації.

Захисту підлягає інформація з обмеженим доступом. Вибір запропонованих приладів повинен бути доцільним та відповідати вимогам до захисту інформації з обмеженим доступом.

До відкритої інформації, що циркулює, належить:

- статутні документи підприємства;
- інформація про замовлення;
- прайси на продукцію підприємства;
- договори про надання клієнтам послуг;
- інформація про штат співробітників підприємства, наявність вільних місць;
- інформація про місце розташування офісу.

До конфіденційної інформації, що циркулює в ТОВ «Еванс», належить:

- організаційно-розпорядча інформація;
- внутрішні документи (накази, службові записки і т. д.);
- персональні дані про співробітників;
- інформація про паролі системи;

- трудові договори співробітників;
- інформація з сервера БД;
- база даних клієнтів підприємства;
- дані про особисті рахунки замовників;
- інформація служби охорони.

У тому числі до інформації, що становить комерційну таємницю підприємства, належить:

- відомості про фінанси підприємства;
- відомості про плани підприємства (плани закупівель, продажу тощо);
- відомості про постачальників;
- відомості про способи придбання і реалізації продукції підприємства;
- зміст договорів і контрактів, однією зі сторін яких виступає підприємство.

### 2.2 Вимоги до функцій, які виконує КС

Система повинна забезпечувати виконання таких функцій:

- автоматизований збір і первинну обробку технологічної інформації;
- автоматичний контроль стану технологічного процесу, попереджувальну сигналізацію при виході технологічних показників за встановлені межі;
- керування технологічним процесом в реальному масштабі часу;
- подання інформації в зручному для сприйняття та аналізу вигляді на кольорових графічних операторських станціях у вигляді графіків, мнемосхем, гістограм, таблиць.
- автоматичну обробку, реєстрацію та зберігання виробничої інформації, обчислення усереднених, інтегральних та питомих показників;
- автоматичне формування звітів та робочих листів за затвердженою формою за певний період часу, і вивід їх на друк за розкладом та на вимогу;

- отримання інформації від системи протиаварійного захисту, сигналізацію та спрацювання системи;
- контроль над працездатним станом засобів мережі, включаючи вхідні та вихідні ланцюги польового обладнання;
- підготовку вихідних даних для розрахунку матеріальних та енергетичних балансів по виробництву, розрахунків витратних норм по сировині, енергетиці;
- автоматизовану передачу даних в єдину мережу підприємства;
- захист баз даних та програмного забезпечення від несанкціонованого доступу;
- діагностику та видачу повідомлень по відмовах всіх елементів комплексу технічних засобів з точністю до модуля.

### 2.3 Вимоги до видів забезпечення КС

#### 2.3.1 Вимоги до інформаційного забезпечення

Математичні методи та алгоритми, які використовуються для шифрування та дешифрування даних, а також програмне забезпечення, що реалізує їх, повинні бути сертифіковані уповноваженими організаціями для використання в державних органах.

Структура та способи організації даних в системі повинні бути обґрунтовані на етапі технічного проектування.

Технічні засоби, що забезпечують зберігання інформації, повинні використовувати сучасні технології, що дозволяють забезпечити підвищену надійність зберігання даних та оперативну заміну обладнання.

Робота системи повинна відповідати стандартам провідних компаній розробників Cognimatics (Швеція), Flonomics (США), Aimetis (Канада) потік з одної IP-камери по протоколам ONVIF  с роздільною здатністю Full-HD (1920×1080), базовим кодеком H.264 и частотою 25 кадрів в секунду, при умові високої активності в кадрі не повинен генерувати трафік більший ніж 7 Мбіт/с.

Організація сховища потрібного обєму при умові використання RAID-7.3 або RAID N+M.

При проектуванні та розгортанні системи необхідно розглянути можливість використання накопиченої інформації з уже функціонуючих інформаційних систем.

Прикладне програмне забезпечення системи для організації взаємодії з користувачем повинно використовувати українську мову.

Для реалізації функцій АСУТП повинні використовуватися сучасні засоби конфігурації та візуального програмування, орієнтовані на фахівців-розробників. Такі рішення дозволяють істотно мінімізувати час розробки, та надають винятково наочність алгоритмам керування та обробки інформації.

Зважаючи на відсутність вітчизняних нормативних документів, як їх прототип необхідно використовувати МЕК 61131-3, який регламентує мови програмування які можуть використовуватися для розробки прикладного програмного забезпечення систем.

### 2.3.2 Вимоги до програмного забезпечення

Для реалізації завдань комп'ютерної системи повинно використовуватися спеціалізоване програмне забезпечення, яке повинно функціонувати на програмованому логічному контролері.

Характеристики програмного забезпечення повинні задовольняти вимогам щодо виконання функцій, зазначених у попередніх розділах.

Мережеві програмні засоби, що забезпечують об'єднання підсистем, операторських станцій та засобів архівування даних в єдину систему, повинні реалізовувати завантаження та керування запуском завдань, забезпечувати обмін між завданнями та базами даних, і надавати доступ до периферійних пристроїв.

Комп'ютерна система повинна мати можливість оперативного конфігурування прикладного програмного забезпечення в процесі функціонування системи.

Всі помилкові ситуації, що виникають при роботі програм, повинні діагностуватися, супроводжуватися повідомленнями, та не повинні викликати порушень в роботі системи.

Технічне забезпечення системи повинно максимально та найбільш ефективним чином використовувати існуючі технічні засоби.

Комплекс технічних засобів комп'ютерної системи повинен бути достатній для реалізації визначених функцій, та будуватися на базі наступних спеціалізованих програмно-технічних комплексів:

Засоби вимірювання, що входять в систему контролю, керування повинні мати сертифікат про затвердження типу, опис типу, методику повірки. У специфікацію обладнання системи повинні бути включені спеціальні технічні та програмні засоби для калібрування вимірювальних каналів.

Метрологічне обслуговування комп'ютерної системи має забезпечувати можливість як поелементної, так і комплексної повірки або калібрування вимірювальних каналів.

Для технічних засобів, що беруть участь в процесі вимірювання контрольованих параметрів повинні бути забезпечені відповідні умови експлуатації та їх контроль.

Організаційне забезпечення системи повинно бути достатнім для ефективного виконання персоналом покладених на нього обов'язків при здійсненні автоматизованих та пов'язаних з ними неавтоматизованих функцій системи.

# 3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

## 3.1 Розробка схеми організаційної структури підприємства

Організаційна структура підприємства визначається функціональними підрозділами які є на підприємстві і зв'язками між ними.

Тому для підвищення рівня інформаційної безпеки на доцільно розробити систему відоспостереження . Для розробки системи відоспостереження обрано дротові камери IP-відеоспостереження, оскільки можлива прокладка кабелю на всій території підприємства.

Доступ до інформаційних ресурсів підприємства розмежований. Відповідно до класу інформаційних ресурсів повнота доступу забезпечується системою паролів.

Враховуючи, що комп'ютерна мережа є розподіленою. До комп'ютерної системи входить мережа відео нагляду [1].

## 3.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

### 3.2.1 Розробка архітектури комп'ютерної мережі та вибір обладнання

У моделі загроз були зазначено, що на території філії немає чітко встановленої контрольованої зони, в межах якої здійснювався би контроль за перебуванням відвідувачів. Тому необхідно розробити таку систему контролю і управління доступом, яка б дозволила вирішити наступні задачі:

– контроль за пересуванням відвідувачів;

– контроль за діями відвідувачів;

– фіксацію відвідувачів і їх цілей;

– неможливість проникнення сторонніх осіб до особливо важливих об'єктів.

Для реалізації цих задач пропонується наступні рішення:

– встановлення системи відеоспостереження;

– вести прийом відвідувачів за попереднім записом;

– для співробітників ввести доступ по карткам;

– встановити контрольно-пропускний пункт.

Відповідно до поставлених технічних вимог було розроблено структурну схему, яка наведена на рис. 3.1.

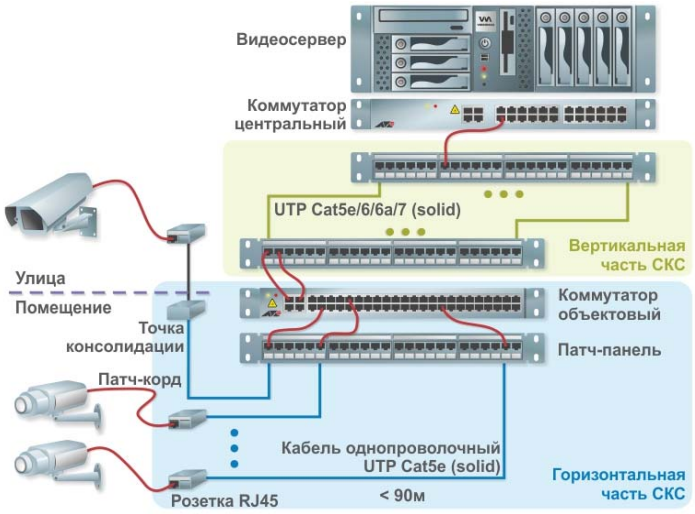



Рисунок 3.1 – Структурна схема

Тут можна помітити, що правильне з'єднання камери з комутатором здійснюється через фіксований сегмент мережі між розеткою і патч-панеллю, виконаний сплетений кабелем (solid). Камера від'єднується з розеткою і комутатора з відповідним портом патч-панелі здійснюється патч-кордом у вигляді гнучкого багатодротяна (patch) кабелю з роз'ємами RJ45, виготовленим і протестованим в заводських умовах. Це єдиний варіант з'єднання, передбачений стандартом.

Мною було запропоновано посилити захист IP-відеокамер за допомогою використання додаткових водонепроникних металевих корпусів.

У зв'язку з необхідністю забезпечити високу надійність інформації та захист її від перешкод, був використаний кабель (вита пара) з додатковою екранізацією.

Роз'єми і з'єднання кабелів так само виконані з додатковою екранізацією і пропайкою і захистом з допомогою силіконового герметика, що в цілому дуже позитивно впливає на збільшення напрацювання на відказ і зводить перешкоди в системі відеоспостереження до нуля.

Таким чином, відповідно до характеристик та відстані між об’єктами підприємства розроблено структурну схему комп’ютерної мережі підприємства, яка складається з пяти локальних мереж.

LAN1 – локальна мережа, яка об’єднує камери відео спостереження в адміністративному корпусі у кількості 16 шт. Усі камери отримують живлення від комутатора, комутатор обладнаний відповідним інтерфейсом. Перша локальна мережа включає також камери що розташовані з першого по третій поверхи спостереження в адміністративному корпусі (Рис. 3.5 – 3.7).

LAN2 – локальна мережа, яка об’єднує камери відео спостереження, що розташовані по території та в службово-побутовому корпусі. Ці камери означені зеленим кольором (Рис. 3.2). Дані камери підключені до комутатора, який розташований у спеціальному приміщенні в адміністративному корпусі. Загальна кількість камер - 16. Зв'язок з комутатором центрального офісу проходить по оптичній лінії зв’язку.

LAN3 – локальна мережа, яка об’єднує комп’ютери, що встановлені в матеріально-технічному складі. Всього передбачено 8 робочих місць. Мережа №3 через комутатор зв’язана з роутером, який встановлений в шафі адміністративного корпусу. Зв'язок з сервером забезпечує та ж оптична лінія зв’язку що і мережу №2.

LAN4 – локальна мережа що забезпечує функціонування абонентського відділу (17 комп’ютерів).

LAN5 – об’єднує всього 6 терміналів. До комутатора підключені термінали трансформаторної станції, насосної станції. Далі через маршрутизатор забезпечується звязок з усією мережею.

Усі локальні мережі підключені до центрального маршрутизатора, до якого також підключений комутатор термінала системного адміністратора і центрального сервера.

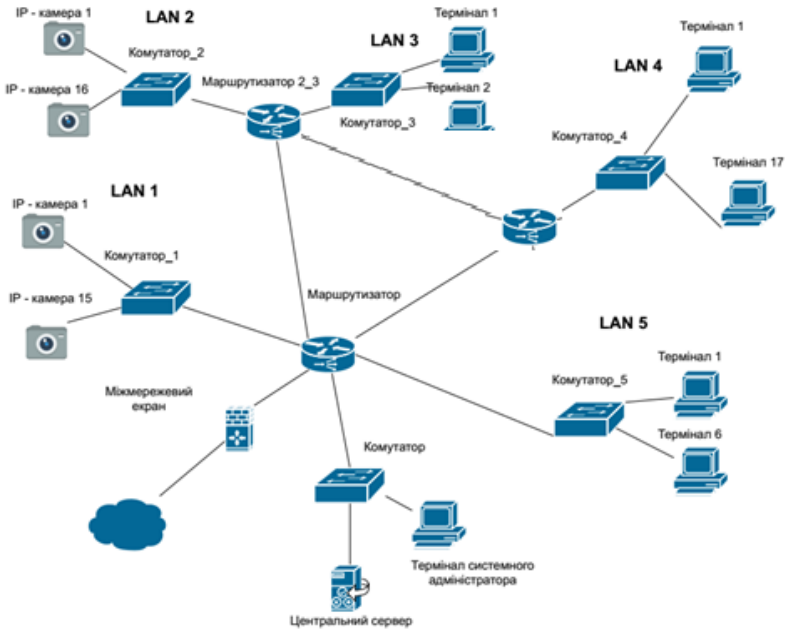



Рисунок 3.3 – Структура комп’ютерної мережі підприємства

Таблиця 3.3 – Перелік технічних засобів відеоспостереження

| Тип приладу | Зовнішній вигляд | Призначення | Характеристики | Кількість |
|---|---|---|---|---|
| Ч/б камера спостереження |  | Відеоспостереження в середині будівлі | Матриця - 1/3" SONY CCD<br>F – 3.6 мм | 7 шт. |
| Камера спостереження |  | Вуличне відеоспостереження | Матриця - 1/3" SONY HD CCD<br>F – 6 мм | 4 шт. |
| Плата відеозахвату |  | Організація відеоспостереження на ПК | 4 канали<br>Роздільна здатність 768x576 | 1 шт. |
| Персональний комп’ютер | - | Організація відеоспостереження | - | 1 шт. |

Розміщення камер спостереження, а також розташування пункту спостереження зображено на рис. 3.5…рис. 3.7.

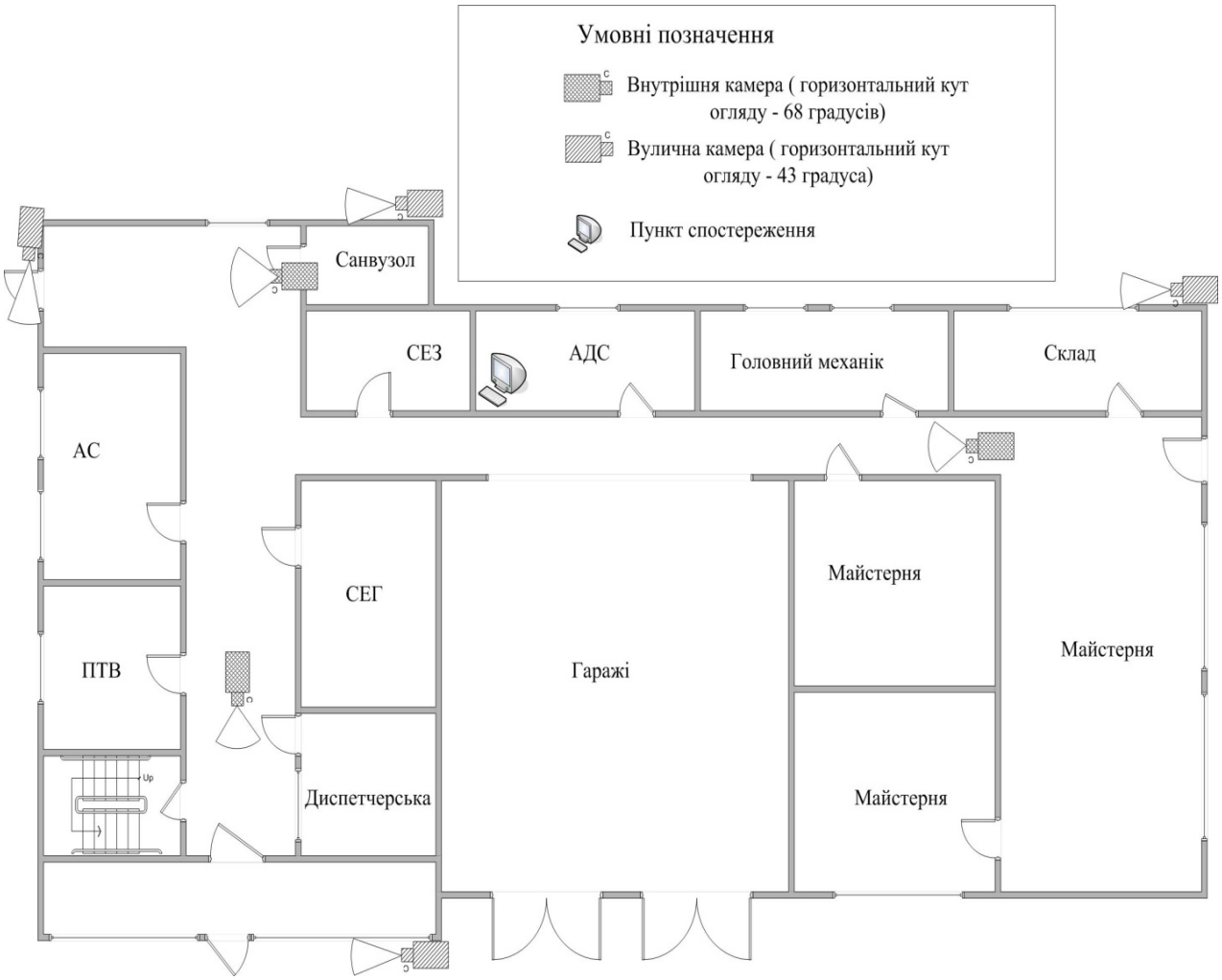



Рисунок 3.5 – Схема розташування камер спостереження на першому поверсі

Підключення камер спостереження до плати на ПК за допомогою коаксіального дроту. Живлення камер від єдиного блоку живлення на 12 В у приміщені АДС де розташований пункт спостереження.

Контрольно-пропускний пункт встановити на першому поверсі в приміщенні диспетчерської. В задачі КПП слід включити:

– охорону адміністративного корпусу;

– організацію черги на прийом відвідувачів і сповіщення про це відповідних служб;

– контроль за правом доступу співробітників і відвідувачів;

– ведення журналу доступу.

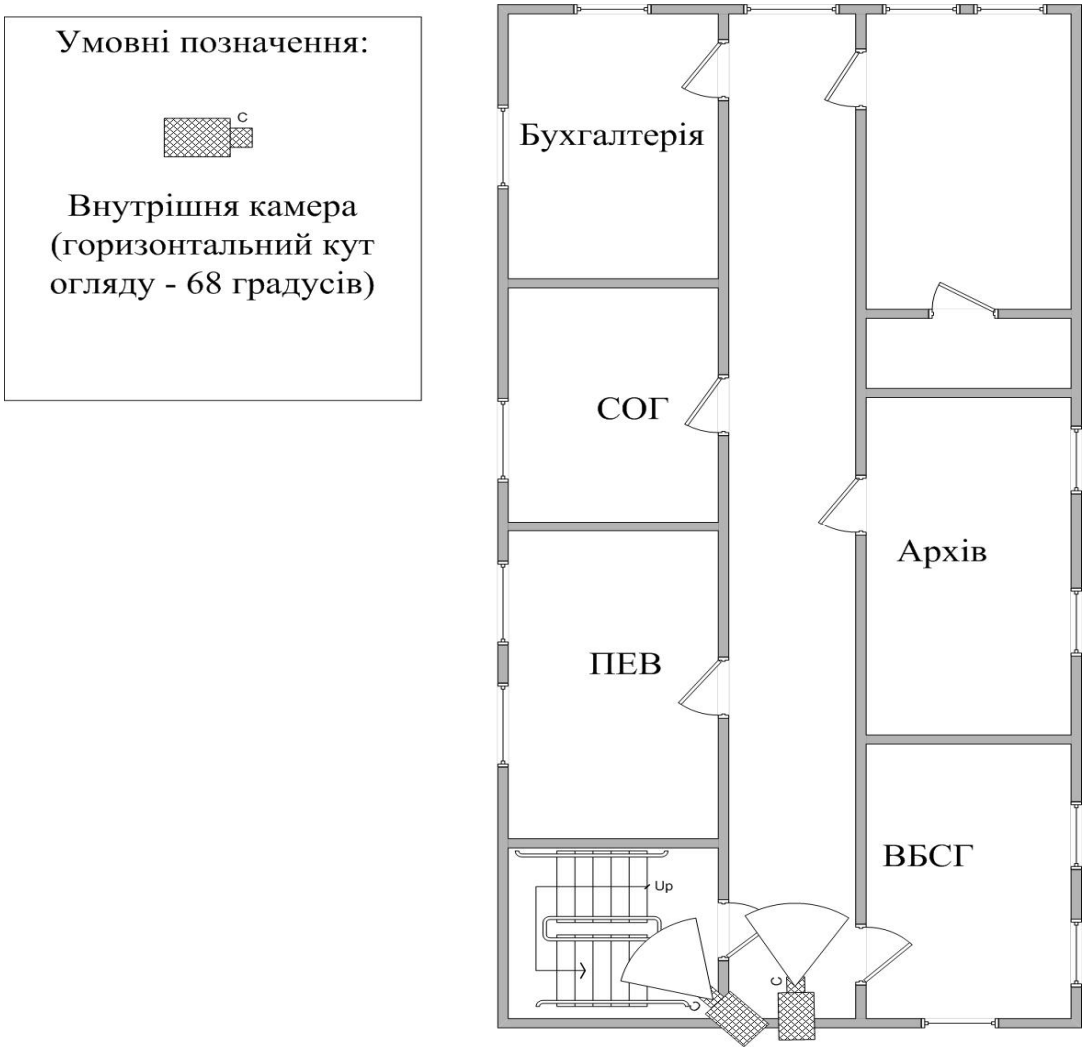



Рисунок 3.6 – Схема розташування камер спостереження на другому поверсі

Пересування осіб по території слід обмежити. Обмежити доступ до майстерень та складу, встановити на дверях доводчик та табличку з написом «Стороннім вхід заборонено». Обмежити пересування по території далі від входу.

Забезпечити співробітників філії пластиковими картками із зображеними на них фотографією власника, прізвищем, ім’ям, по батькові та назву служби де він працює.


Рисунок 3.7 – Схема розташування камер спостереження на третьому поверсі

Отриману відеоінформацію зовнішня точка доступу, що розташована на головному офісі, передає інформацію на сервер де і зберігається протягом тижня на жорсткому диску.

За системою відеоспостереження слідкують охоронці, які знаходяться в кабінеті охорони. В їх обов'язки входить забезпечення безперебійної роботи системи відеоспостереження, контроль за дотриманням правил доступу до відеоданих та робота з відеоінформацією.

Таким чином, доступ до відеоінформації відкрито таким співробітникам:

– директор;
– заступник директора ;
– охоронники;
– системний адміністратор.

При цьому перелічені співробітники матимуть наступні права доступу до відеоінформації:

Таблиця 3.1 - Права доступу

| Співробітники | Перегляд | Зберігання | Знищення | Копіювання | Модифікація |
|---|---|---|---|---|---|
| Директор | + | + | + | + | + |
| Заступник директора | + | - | - | - | - |
| Охоронники | + | - | - | - | - |
| Системний адміністратор | + | - | - | - | - |

Усі інші співробітники доступу до відеоінформації не мають.

Вся відеоінформація, що зберігатиметься на сервері підприємства належить до інформації з обмеженим доступом, та захищається на основі технології DRM, що позбавляє користувача прямого доступу комп'ютера.

### 3.2.2 Проектування виділеного приміщення серверної

Приміщення серверної розташоване на другому поверсі адміністративного корпусу у кімнаті інформаційно-обчислювальної групи (зображено на рис. 3.8). Для захисту інформації від витоку побічними електромагнітними випромінюваннями та наводками, колами електроживлення, а також для зменшення впливу поля, що утворюється підстанцією, у приміщенні серверної рекомендуються наступні інженерно-технічні заходи:

– електромагнітне екранування приміщення серверної кімнати;

– включення в лінію електроживлення протизавадного фільтра;


Рисунок 3.8 – Схема серверного приміщення

До електромагнітного екрану висуваються наступні вимоги:

- забезпечення ефективності екранування в діапазоні частот від 150 МГц до 1 ГГц не менше 20 дБ.
- з’єднання листів екрану виконати суцільним швом з напуском;
- протизавадний фільтр встановити із зовнішньої сторони екрану, для цього передбачити у конструкції екрану короб для монтажу фільтрів і виводу кабелів живлення;
- передбачити в конструкції екрану виводи системи кондиціонування;
- кабелі розмістити в пластикових коробах;
- не допускати гальванічного контакту екрану з металевими конструкціями будівлі;
- електричний контакт дверної лутки з екраном виконати із застосуванням спеціальної гребінки;

– забезпечити електричний контакт дверей і дверної лутки.

### 3.3 Розрахунок протизавадного фільтра

Для вибору протизавадного фільтра необхідно визначити номінальний струм в мережі. Для цього необхідно розрахувати споживну потужність пристроїв задіяних в приміщеннях. Загальна потужність дорівнює сумі всіх споживачів і визначається за формулою:

$$P_{\text{з}} = \sum P_{\text{сп}}, \quad (3.1)$$

де $P_{\text{з}}$ – загальна потужність;

$P_{\text{сп}}$ – потужність споживачів.

Для визначення номінального струму використаємо формулу:

$$I_{\text{н}} = \frac{P_{\text{з}}}{U_{\text{п}}}, \quad (3.2)$$

де $I_{\text{н}}$ – номінальний струм;

$U_{\text{п}}$ – напруга мережі.

Визначення споживної потужності для приміщення серверної:

Таблиця 3.4 – Перелік споживачів і їх потужність у приміщені серверної

| **Пристрій** | **Споживна потужність, Вт** | **Кількість** |
|---|---|---|
| Сервер | 530 | 6 |
| Кондиціонер | 2050 | 1 |

Загальна потужність споживачів за формулою (3.1) буде дорівнювати:

$P_{\text{з}}=\sum P_{\text{сп}}=530\cdot 6+2050=5230$ (Вт)

а номінальний струм за формулою (2.2):

$$I_{\text{н}} = \frac{5230}{220} = 23{,}7 \text{ (А)}$$

В лінію електроживлення цього приміщення слід встановити протизавадний фільтр – ФП-14.

Таблиця 3.5 – Технічні характеристики протизавадного фільтра ФП-14

| | |
|---|---|
| Кількість дротів | 2 |

| | |
|---|---|
| Номінальний струм, не більше | 40 А |
| Номінальна напруга: | |
| - при постійному струмі | 1000 В |
| - при змінному струмі частотою 50 Гц | 500 В |
| - при змінному струмі частотою 400 Гц | 220 В |
| Згасання в діапазоні, дБ | |
| 20-150 КГц | 30 |
| 0,15 МГц - 1 ГГц | 100 |
| 1,0-1,8 ГГц | - |
| 1,8 -10,0 ГГц | - |
| Маса фільтра | 10,0 кг |

В якості екрану можуть виступати наступні матеріали:

– цільний сталевий лист;

– металева сітка;

– металеві двері і лутка дверей.

Характеристики матеріалів для побудови електромагнітного екрану представлені у табл. 3.6.

Таблиця 3.6 – Порівняльна характеристика матеріалів екранування

| **Тип екрану** | **Матеріал** | **Частота, КГц** | | | | |
|---|---|---|---|---|---|---|
| | | **10** | **100** | 1000 | 10000 | 100000 |
| | | **Затухання, дБ** | | | | |
| Металевий лист товщиною 0,5 мм | Сталь | 64 | 87 | 120 | 120 | 120 |
| | Мідь | 67 | 70 | 88 | 120 | 120 |
| | Алюміній | 65 | 66 | 80 | 120 | 120 |
| Металева сітка | Мідь, розмір комірки 1х1 мм | 65 | 55 | 50 | 42 | 32 |
| | Сталь, розмір комірки 1х1 мм | 48 | 47 | 42 | 36 | 29,5 |

З табл. 3.6 видно, що найкращими характеристиками екранування володіє листова мідь, але цей матеріал значно дорожчий за сталь чи алюміній. Однак враховуючи встановлені вимоги, можна зробити висновок, що всі метали забезпечують рівень затухання в заданому діапазоні частот більше 20 дБ. Тому листова сталь, товщиною 0,5 мм цілком задовольняє поставлені вимоги.

Пропонується встановити екрановані двері виробництва фірми «Практика». Електричний контакт цих дверей забезпечується луженим оплітком,

вставленої в екрановану смугу. По всьому контуру прилягання дверей на полотні дверей прокладається контактна планка, з нержавіючої сталі, яка кріпиться до зачищеній поверхні полотна дверей заклепками з кроком 50 мм. Несучим елементом двері є рама. Вона являє собою зварену конструкцію з гнутого профілю. Рама двері приварюється безпосередньо до металевих панелей екранованого приміщення безперервним швом. Для зручності експлуатації з зовнішнього боку полотна є ручка-штурвал. Дверне полотно забарвлене порошковою фарбою.

У випадку, якщо не буде встановлений режим запропонованої системи контролю і управління доступом, то необхідно забезпечити екран серверної окремим захисним заземленням.

У моделі загроз було зазначено, що однією з причин витоку інформації технічними каналами є недостатня інформованість співробітників філії про необхідність забезпечення безпеки конфіденційної інформації, що циркулює на підприємстві. Тому пропонується ряд рекомендаційних заходів, виконання яких допоможе підвищити рівень захисту інформації з обмеженим доступом від витоку технічними каналами:

1) створити службу захисту інформації на базі штату філії, або залучити фахівців з інформаційної безпеки;
2) внести до обов’язків співробітників філії пункт про необхідність забезпечення безпеки інформації з обмеженим доступом, визначити відповідальність у разі невиконання цих обов’язків;
3) проводити тренінги і семінари з інформаційної безпеки для співробітників, діяльність яких пов’язана з обробкою конфіденційної інформації;
4) проводити тренінги і семінари з інформаційної безпеки для співробітників в задачі яких не входить робота з конфіденційною інформацією, але діяльність котрих може впливати на режим роботи ТЗПІ на яких оброблюється інформація з обмеженим доступом;

5) якщо діяльність співробітників філії потребує озвучення конфіденційної інформації, то в такому разі необхідно використовувати виділене приміщення для переговорів і нарад;
6) проводити бесіди зі співробітниками філії про знання їх обов'язків про забезпечення захисту інформації;
7) заборонити вести переговори про відомості, що становлять конфіденційну інформацію, із членами родини, друзями, сторонніми особами, а також співробітниками філії, діяльність котрих не передбачає доступ до інформації з обмеженим доступом;
8) не залишати відвідувачів одних у приміщеннях де циркулює конфіденційна інформація;
9) не зберігати будь-які речі залишені чи подаровані відвідувачами у приміщеннях де циркулює конфіденційна інформація, донести до відома співробітників, що такі речі можуть містити закамуфльовані технічні засоби розвідки.

### 3.4 Висновок

В спеціальній частині були розглянуті інженерно-технічні заходи і засоби захисту від витоку конфіденційної інформації технічними каналами та виконаний їх порівняльний аналіз. На основі отриманих результатів був запропонований проект комплексу технічного захисту інформації філії Публічного акціонерного товариства «Дніпропетровськгаз».

# 4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

## 4.1 Розробка моделі комп'ютерної системи в Packet Tracer

Відповідно до організаційної структури клубу та вимогам розташування пристроїв за допомогою програмного забезпечення Cisco Packet Tracer модель була розроблена мережі організації, яка зображена на рис. 4.1.

Топологія мережі була виконана в середовищі програмного забезпечення Cisco Packet Tracer.

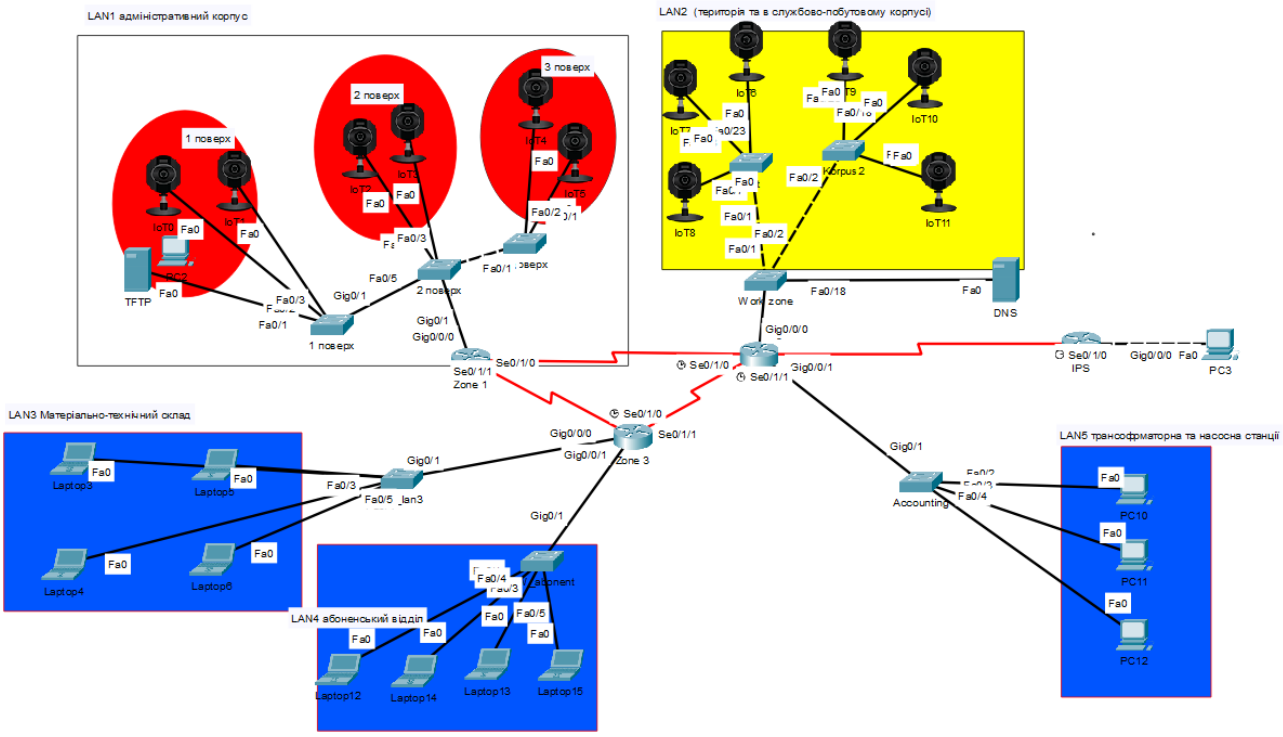



Рисунок 4.1 – Побудована модель комп'ютерної мережі

## 4.2 Розрахунок схеми адресації корпоративної мережі

Для проектованої комп'ютерної мережі необхідно розробити адресацію з врахуванням наступних вимог до мережі: використовувати блок приватних IP-адрес 192.168.0.0/17 (255.255.252.0), та врахувати кількість вузлів у різних сегментах мереж. Мережу, в якій містяться VLAN-мережі, розрахувати порівну.

Також необхідно провести розрахунок схеми IP-адресації послідовних каналів між маршрутизаторами з діапазону 10.0.11.0/24.

Розробка схеми адресації здійснюється за допомогою методу VLSM. VLSM (variable length subnet masks) – мережеві маски змінної довжини, що використовуються у безкласовій маршрутизації. VLSM дозволяє використання більш ніж однієї мережевої маски в межах одного адресного простору. VLSM максимізує використання адресного простору і його використовують для сегментування сегментованих локальних мереж.

Для розрахунку IP адресації спочатку визначається кількість мереж. Для того, щоб розбити вихідну мережу, необхідно визначити кількість біт, необхідних для визначення п’яти мереж (для визначення п’яти мереж необхідно 3 біти ($2^3$=8), оскільки при використанні 2 біт вихідну мережу можна розділити лише на 4 підмережі ($2^2$=4). Мережі повинні бути розраховані на 30 адрес. Відповідно, необхідна кількість біт для отримання необхідної кількості IP-адрес - 6 ($2^6$=64).

Важливо зазначити, що з загальної кількості IP-адрес на визначення вузлів відводиться на 2 менше, оскільки перша адреса визначає мережу, а остання визначає адресу широкомовної россилки.

*Таким чином розрахунок IP-адреси методом VLSM для мережі LAN1 має вигляд:* 192.168.0.|000|0 0000

Символами “| |” виділена частина IP-адреси, що визначає підмережу вихідної мережі. Маска підмережі - 17 одиниць (255.255.128.0). Адреса підмережі - 192.168.0.0. Перша допустима адреса підмережі визначається як значення I в наймолодшому біті IP-адреси у хостовій частині. Остання допустима адреса визначається як значення одиниць в усіх розрядах хостової частини, крім наймолодшого - 192.168.0.000|1 1110| (192.168.0.30). Широкомовна адреса визначається як усі одиниці в усіх розрядах хостової частини IP-адреси -192.168.0.000|1 1111| (192.168.0.31).

*Розрахунок IP-адрес методом VLSM для підмережі IAM2:*

Необхідна кількість IP-адрес - 30, відповідно, для виділення необхідна та ж кількість біт - 5.

Частину адреси, що визначає підмережу, необхідно збільшити на 1, додавши 1 до молодшого біта:

192.168.0.|001|0 0000

Таким чином, адреса підмережі: 192.168.6.|001|0 0000 (192.168.0.32/17)

Перша допустима адреса 192.168.6.|00110 0001 (192.168.0.33/17)

Остання допустима адреса: 192.168.6.|00111 1110 (192.168.0.61/17)

Адреса широкомовної розсилки: 192.168.0. |00111 1111 (192.168.0.62/17)

*Розрахунок IP-адрес методом VLSM для підмережі LAN3:*

Необхідна кількість IP-адрес - 25, відповідно, для виділення необхідна та ж кількість біт - 5.

Частину адреси, що визначає підмережу, необхідно збільшити на 1, додавши I до молодшого біта:

|010|0 0000

Таким чином, адреса підмережі: 192.168.6.|010|0 0000 (192.168.0.64/17)

Перша допустима адреса: 192.168.6.|010|0 000 1 (192.168.0.65/17)

Остання допустима адреса: 192.168.0. |010|1 1110 (192.168.0.93/17)

Адреса широкомовної розсилки: 192.168.0. |010|1 1111 (192.168.0.94/17)

В таблиці 1 представлена розрахована схема 1P-адресації мережі за методом VLSM.

*Розрахунок IP-адрес методом VLSM для підмережі LAN4:*

Необхідна кількість IP-адрес - 30, відповідно, для виділення необхідна та ж кількість біт - 5.

Частину адреси, що визначає підмережу, необхідно збільшити на 1, додавши 1 до молодшого біта:192.168.0.|011|0 0000

Таким чином, адреса підмережі: 192.168.0. |011|0 0000 (192.168.6./17)

Перша допустима адреса: 192.168.0. |011|0 0001 (192.168.6./17)

Остання допустима адреса: 192.168.0. |011[1 1110(192.1686./17)

Адреса широкомовної розсилки: 192.168.0. |011|1 1111 (192.168.6.17) *Розрахунок IP-адрес методом VLSM для підмережі LAN5:*

Необхідна кількість IP-адрес - 30, відповідно, для виділення необхідна та ж кількість біт - 5.

Частину адреси, що визначає підмережу, необхідно збільшити на 1, додавши 1 до молодшого біта:192.168.0 |100|0 0000

*Розрахунок IP-адрес методом VLSM для підмережі VLAN28:*

Адреса підмережі: 192.168.6. 1100|0 0000 (192.168.136.0/24)

Перша допустима адреса: 192.168.6. 1100|0 ООО 1 (192.168.136. 1/24)

Остання допустима адреса: 192.168.6. 1100| 1 1110(192.168.139. 254/24)

Адреса широкомовної розсилки: 192.168.6. 1|00|1 1111 (192.168.136. 254/24) *Розрахунок IP-адрес методом VLSM для підмережі VLAN38:*

Адреса підмережі: 192.168.6.1|01|0 0000(192.168.137.0/24)

Перша допустима адреса 192.168.6.110110 0001 (192.168.137. 1/24)

Остання допустима адреса: 192.168.6.110111 1110(192.168.141. 254/24)

Адреса широкомовної розсилки: 192.168.6.110111 1111 (192.168.6.224/24)

*Розрахунок IP-адрес методом VLSM для підмережі VLAN99:*

Адреса підмережі: 192.168.6.1|10|0 0000 (192.168.139.0/24)

Перша допустима адреса: 192.168.6.1110|0 0001 (192.168.139.1/24)

Остання допустима адреса: 192.168.6.1110| 1 1110(192.168.145.254/24)

Адреса широкомовної розсилки: 192.168.6.1110| 1 1111 (192.168.139.1/24)

*Розрахунок IP-адрес методом VLSM для підмережі VLAN 48:*

Адреса підмережі: 192.168.0. 111110 0000 (192.168.138.0/24)

Перша допустима адреса: 192.168.0. 111110 0001 (192.168.138.1/24)

Остання допустима адреса: 192.168.0. 1|11|1 1110(192.168.140.254/24)

Адреса широкомовної розсилки: 192.168.0. 1|11|1 1111 (192.168.140.254/24) Розрахунок схеми IP-адресації послідовних каналів між маршрутизаторами з діапазону 192.168.2.0/24 виконується аналогічно.

В таблиці 4.1 представлена розрахована схема 1P-адресації мережі за методом VLSM.

Таблиця 4.1 – Схема адресації мережі

| Назва підмережі | Необхідна кількість вузлів | Адреса підмережі | Маска підмережі у десятковому форматі | Діапазон допустимих IP-адресів вузлів | |
|---|---|---|---|---|---|
| LAN1 | 90 | 192.168.0.0 | 255.255.252.0 | 192.168.0.1 | 192.168.131.254 |
| LAN2 | 52 | 192.168.136.0 | 255.255.252.0 | 192.168.136.1 | 192.168.139.254 |
| LAN3 | 74 | 192.168.132.0 | 255.255.252.0 | 192.168.132.1 | 192.168.135.254 |
| LAN4 | 60 | 192.168.141.128 | 255.255.255.192 | 192.168.141.129 | 192.168.141.190 |
| | | | | | |
| VLAN28 | 28 | 192.168.136.0 | 255.255.255.0 | 192.168.136.1 | 192.168.139.254 |
| VLAN38 | 38 | 192.168.137.0 | 255.255.255.0 | 192.168.137.1 | 192.168.141.254 |
| VLAN48 | 48 | 192.168.138.0 | 255.255.255.0 | 192.168.138.1 | 192.168.140.254 |
| VLAN99 | 99 | 192.168.139.0 | 255.255.255.0 | 192.168.139.1 | 192.168.145.254 |
| | | | | | |
| WAN1 | 2 | 192.168.141.192 | 255.255.255.252 | 192.168.141.193 | 192.168.141.194 |
| WAN2 | 2 | 192.168.141.196 | 255.255.255.252 | 192.168.141.197 | 192.168.141.198 |
| WAN3 | 2 | 192.168.141.200 | 255.255.255.252 | 192.168.141.201 | 192.168.141.202 |
| WAN4 | 2 | 192.168.141.204 | 255.255.255.252 | 192.168.141.205 | 192.168.141.206 |
| WAN5 | 2 | 209.165.202.0 | 255.255.255.248 | 209.165.202.3 | 209.165.202.4 |

В таблиці 4.2 перелічені адреси всіх пристроїв у мережі.

Таблиця 4.2 – Схема адресації пристроїв

| Пристрій | Інтерфейс | IP-адреса | Ма-ска | Шлюз | VLAN | Для ПК інтер-фейс підк-люче-ного при-строю |
|---|---|---|---|---|---|---|
| **Zone 1** | S 0/1/1 | 192.168.141.194 | /30 | - | 192.168.141.192 | - |
| | S 0/1/0 | 192.168.141.197 | /30 | - | 192.168.141.195 | - |
| | G 0/0/0 | 192.168.0.1 | /22 | - | 192.168.0.0 | - |
| | G 0/0/1 | 192.168.135.254 | /22 | - | 192.168.135.252 | - |
| Laptop0 | - | 192.168.135.253 | /22 | 192.168.135.1 | 192.168.135.0 | Fa 0 |
| Laptop7 | - | 192.168.135.252 | /22 | 192.168.135.1 | 192.168.135.0 | Fa 0 |
| TFTP | - | 192.168.135.251 | /22 | 192.168.135.1 | 192.168.135.0 | Fa 0 |
| Laptop9 | - | 192.168.0.3 | /22 | 192.168.0.1 | 192.168.0.0 | Fa 0 |
| Laptop8 | - | 192.168.0.2 | /22 | 192.168.0.1 | 192.168.0.0 | Fa 0 |
| PC0 | - | 192.168.0.4 | /22 | 192.168.0.1 | 192.168.0.0 | Fa 0 |
| PC1 | - | 192.168.0.5 | /22 | 192.168.0.1 | 192.168.0.0 | Fa 0 |
| **Floor 3** | S 0/1/1 | 192.168.141.202 | /30 | - | 192.168.141.200 | - |
| | S 0/1/0 | 192.168.141.198 | /30 | - | 192.168.141.196 | - |
| | G 0/0/0 | 192.168.141.1 | /25 | - | 192.168.141.0 | - |
| **LAN3** | | | | | | |
| Laptop3 | - | 192.168.141.2 | /25 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| Laptop4 | - | 192.168.141.3 | /25 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| Laptop5 | - | 192.168.141.4 | /25 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| Laptop6 | - | 192.168.141.5 | /25 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| **LAN4** | | | | | | |
| Laptop12 | - | 192.168.141.189 | /26 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| Laptop13 | - | 192.168.141.187 | /26 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| Laptop14 | - | 192.168.141.188 | /26 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| Laptop15 | - | 192.168.141.186 | /26 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| HTTP | - | 192.168.141.185 | /26 | 192.168.141.1 | 192.168.141.0 | Fa 0 |
| **Floor 2** | S 0/1/1 | 192.168.141.201 | /30 | - | 192.168.141.199 | - |
| | S 0/1/0 | 192.168.141.193 | /30 | - | 192.168.141.191 | - |
| | S 0/2/0 | 209.165.201.226 | /28 | - | 209.165.201.224 | - |
| | G 0/0/0.28 | 192.168.136.1 | /24 | - | 192.168.136.0 | - |
| | G 0/0/0.38 | 192.168.137.1 | /24 | - | 192.168.137.0 | - |
| | G 0/0/0.48 | 192.168.138.1 | /24 | - | 192.168.138.0 | - |
| | G 0/0/0.99 | 192.168.139.1 | /24 | - | 192.168.139.0 | |
| | G 0/0/1 | 192.168.140.1 | /24 | - | 192.168.140.0 | - |
| **LAN5** | | | | | | |
| PC10 | - | 192.168.140.253 | /24 | 192.168.140.1 | 192.168.140.0 | Fa 0 |
| PC11 | - | 192.168.140.252 | /24 | 192.168.140.1 | 192.168.140.0 | Fa 0 |
| PC12 | - | 192.168.140.251 | /24 | 192.168.140.1 | 192.168.140.0 | Fa 0 |
| Laptop1 | - | 192.168.137.11 | /24 | 192.168.137.1 | 192.168.137.0 | Fa 0 |
| Laptop2 | - | 192.168.136.11 | /24 | 192.168.136.1 | 192.168.137.0 | Fa 0 |
| Laptop10 | - | 192.168.137.12 | /24 | 192.168.137.1 | 192.168.137.0 | Fa 0 |
| Laptop11 | - | 192.168.136.12 | /24 | 192.168.136.1 | 192.168.137.0 | Fa 0 |
| Laptop16 | - | 192.168.138.11 | /24 | 192.168.138.1 | 192.168.137.0 | Fa 0 |
| Laptop17 | - | 192.168.138.12 | /24 | 192.168.138.1 | 192.168.137.0 | Fa 0 |
| DNS | - | 192.168.137.9 | /22 | 192.168.137.1 | 192.168.137.0 | Fa 0 |

### 4.3 Розрахунок налаштувань маршрутизації корпоративної мережі

Маршрутизація – процес визначення маршруту прямування інформації між мережами. Маршрутизатор приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж.

Існує два типи маршрутизації:

- статична маршрутизація – маршрути задаються вручну адміністратором;
- динамічна маршрутизація – маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації – RIP, OSPF , EIGRP, IS-IS, BGP, HSRP, які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора. Технологія віртуальних мереж створює гнучку основу для побудови великої мережі, з'єднаної маршрутизаторами, тому що комутатори дозволяють створювати повністю ізольовані сегменти програмним шляхом, не прибігаючи до фізичної комутації.

Маршрутизація були налаштовані протоколом EIGRP, з відключенням інтерфейсів, які ведуть до локальних мереж. Програма з налалштувань представлені в Додатку А.

### 4.4 Налаштування роботи Інтернет

Для того щоб надати робочим станціям мережі організації доступ до мережі Інтернет на прикордонному маршрутизаторі було налаштовано протокол NAT та маршрут за замовчуванням до провайдера.

NAT (Network Address Translation) – трансляція мережевих адрес. Процедура зі зміни адрес в заголовках IP-пакетів при їх проходженні через маршрутизатор або інший пристрій. Основною метою використання NAT є економія кількості публічних IPv4-адрес. Використання NAT дозволяє застосовувати приватні адреси всередині мережі, перетворюючи їх в публічні тільки в разі потреби.

Пристроям всередині підприємства можуть присвоюватися приватні адреси, а самі пристрої можуть функціонувати з унікальними локальними адресами.

При необхідності відправки трафіку в іншу організацію або Інтернет (або отримання трафіку з іншої організації або Інтернету) прикордонний маршрутизатор перетворює адреси в унікальні публічні глобальні адреси.

Динамічний NAT. Метод динамічного перетворення мережевих адрес (динамічний NAT) використовує пул публічних адрес, які присвоюються в порядку живої черги.

Коли внутрішній пристрій запитує доступ до зовнішньої мережі, динамічний NAT привласнює доступний публічний IPv4-адрес з пулу.

Для динамічного NAT потрібна достатня кількість публічних адрес, доступних для загальної кількості одночасних сеансів користувачів.

Налаштування NAT на Zona2:

Floor2 (config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224

Floor2 (config)#ip nat inside source list 10 pool Internet

Floor2 (config)#ip nat inside source static 192.168.141.185 209.165.202.2

Floor2 (config)#ip route 0.0.0.0 0.0.0.0 209.165.202.3

Floor2 (config)#access-list 10 permit 192.168.0.0 0.0.255.255

### 4.5 Перевірка роботи комп'ютерної системи

Для перевірки налаштувань маршрутизації із мережі LAN 1 до мережі LAN 3 за допомогою команди tracert було отримано маршрут слідування. Результати виконання команди наведені на рис. 4.2.

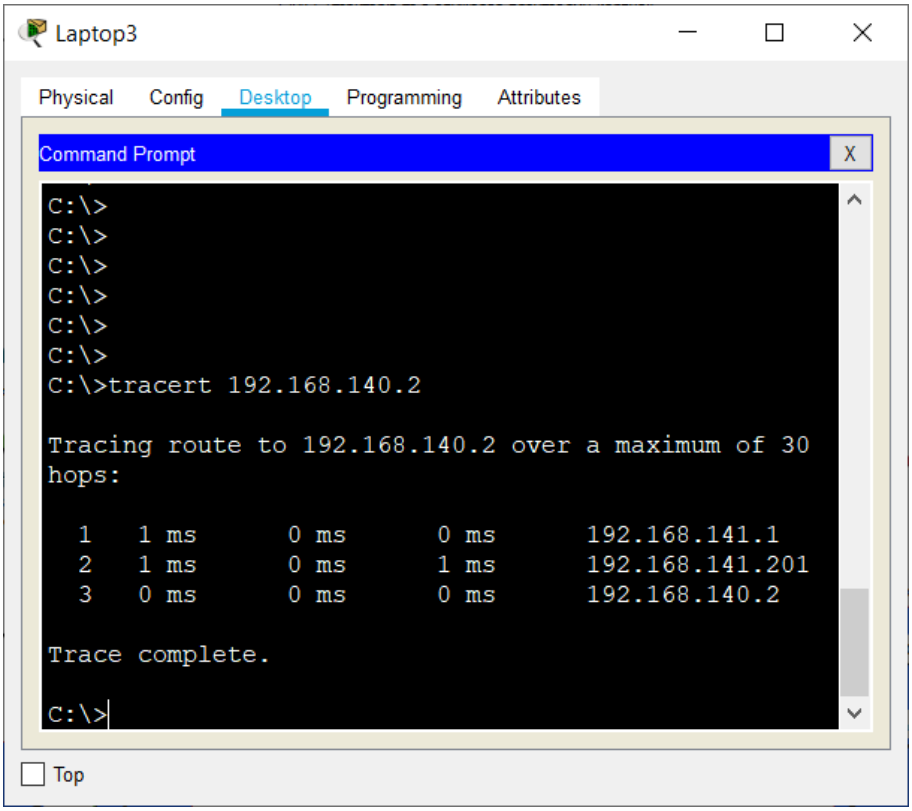



Рисунок 4.2 – Команда tracert між вузлами мережі LAN 1 і LAN 3

Про правильні налаштування маршрутизації свідчить наявність у таблиці маршрутизації маршрутизаторів, записів усіх мереж організації, отриманих за протоколом EIGRP. Таблиця маршрутизації центрального маршрутизатора Router наведена на рисунку 4.3.

Routing Table for Zone 2

| Type | Network | Port | Next Hop IP | Metric |
|---|---|---|---|---|
| S | 0.0.0.0/0 | --- | 209.165.202.4 | 1/0 |
| D | 192.168.128.0/22 | Serial0/1/0 | 192.168.141.194 | 90/2170112 |
| C | 192.168.136.0/24 | GigabitEthernet0/0/0.28 | --- | 0/0 |
| L | 192.168.136.1/32 | GigabitEthernet0/0/0.28 | --- | 0/0 |
| C | 192.168.137.0/24 | GigabitEthernet0/0/0.38 | --- | 0/0 |
| L | 192.168.137.1/32 | GigabitEthernet0/0/0.38 | --- | 0/0 |
| C | 192.168.138.0/24 | GigabitEthernet0/0/0.48 | --- | 0/0 |
| L | 192.168.138.1/32 | GigabitEthernet0/0/0.48 | --- | 0/0 |
| C | 192.168.140.0/24 | GigabitEthernet0/0/1 | --- | 0/0 |
| L | 192.168.140.1/32 | GigabitEthernet0/0/1 | --- | 0/0 |
| D | 192.168.141.0/25 | Serial0/1/1 | 192.168.141.202 | 90/2170112 |
| C | 192.168.141.192/30 | Serial0/1/0 | --- | 0/0 |
| L | 192.168.141.193/32 | Serial0/1/0 | --- | 0/0 |
| D | 192.168.141.196/30 | Serial0/1/1 | 192.168.141.202 | 90/2681856 |
| D | 192.168.141.196/30 | Serial0/1/0 | 192.168.141.194 | 90/2681856 |
| C | 192.168.141.200/30 | Serial0/1/1 | --- | 0/0 |
| L | 192.168.141.201/32 | Serial0/1/1 | --- | 0/0 |
| C | 209.165.202.0/27 | Serial0/2/0 | --- | 0/0 |
| L | 209.165.202.3/32 | Serial0/2/0 | --- | 0/0 |

Рисунок 4.3 – Таблиця маршрутизації

### 4.5.1 Перевірка налаштувань VLAN

Правильність налаштування VLAN також перевірено командою show vlan brief (рис. 4.4), де вказуються активні мережі VLAN, їх номера та імена, а також порти до яких вони відносяться.

```
Clients#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4,
Fa0/5, Fa0/6
                                                 Gig0/2
28   VLAN0028                          active    Fa0/7, Fa0/8,
Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12,
Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16,
Fa0/17
38   VLAN0038                          active    Fa0/18, Fa0/19,
Fa0/20, Fa0/21
                                                 Fa0/22
48   VLAN0048                          active    Fa0/23, Fa0/24
99   VLAN0099                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 4.4 – Перевірка налаштування VLAN

### 4.5.2 Перевірка налаштувань NAT

Для перевірки правильності роботи NAT було згенеровано ICMP-пакет із мережі LAN 1 до мережі провайдера. Про правильність налаштувань та роботи NAT свідчить таблиця NAT-перетворень маршрутизатора Router_3, яка наведена на рис. 4.5.

NAT Table for Zone 2

| Protocol | Inside Global | Inside Local | Outside Local | Outside Global |
|---|---|---|---|---|
| icmp | 209.165.202.5:22 | 192.168.141.2:22 | 209.165.201.225:22 | 209.165.201.225:22 |
| --- | 209.165.202.2 | 192.168.141.185 | --- | --- |

Рисунок 4.5 – Про правильність налаштувань та роботи NAT свідчить таблиця NAT-перетворень

.

# 5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

## 5.1 Організація виділеного приміщення

Кімната для проведення переговорів, засідань і нарад знаходиться на третьому поверсі адміністративного корпусу. Займає одну кімнату розміром 4х6 м. Має два вікна у західній стіні. Освітлюється за допомогою чотирьох люмінесцентних ламп. Технічні засоби обробки інформації відсутні. Також в кімнаті є два радіатори системи опалення.

Товщина стін – 28 см. Значення рівня звукоізоляції для стін товщиною в одну цеглину (з урахуванням оздоблення штукатуркою) на частоті акустичного сигналу 250 Гц - не менше 44 дБ.

Перекриття мають значення рівня звукоізоляції на рівні не менше 47 дБ на частоті акустичного сигналу 250 Гц.

Вікна мають однокамерний склопакет з товщиною скла 3 мм і повітряним прошарком 10 мм. Значення рівня звукоізоляції для вікон з товщиною 3/10/3 мм – не менше 24 дБ. Каркас вікна закріплений без використання віброізолюючих матеріалів і вставок.

Розміщення виділеного приміщення схематично зображено на рис. 5.1.

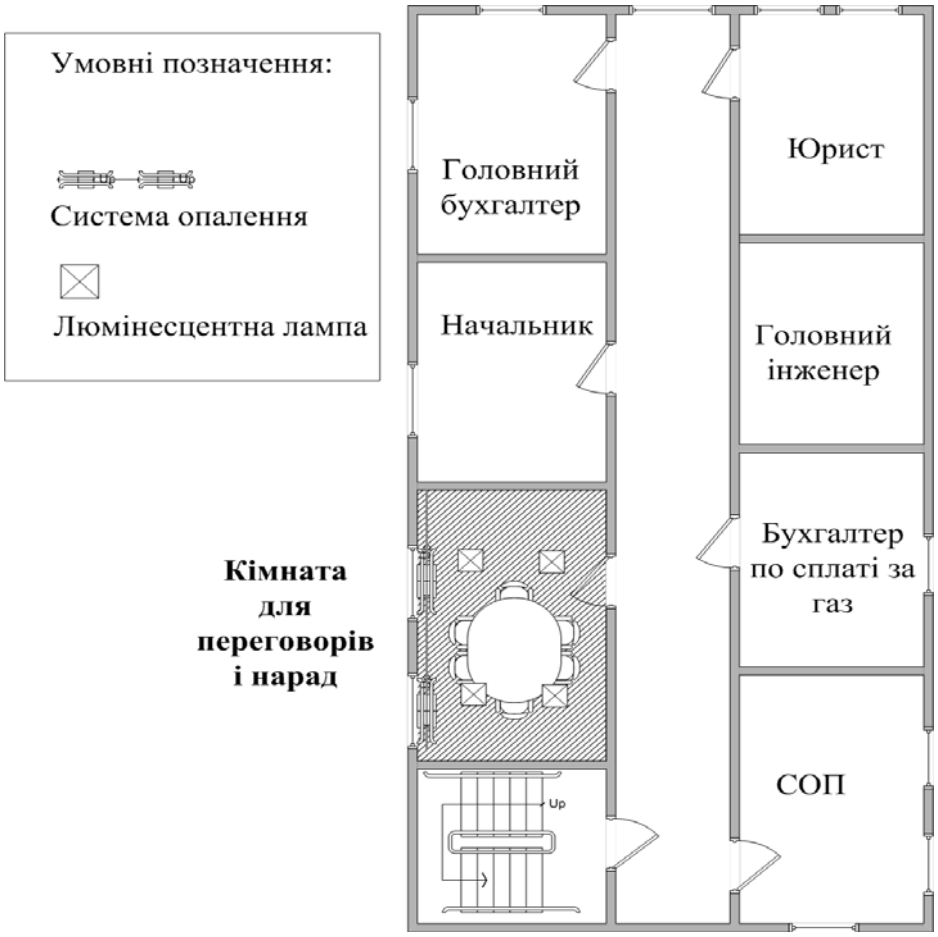



Рисунок 5.1 - Схема розміщення виділеного приміщення

Одинарні дерев’яні двері товщиною 4 см забезпечують рівень звукоізоляції в 24 дБ. Лутка дверей встановлена без використання віброізолюючих матеріалів і вставок. Двері прилягають до лутки з зазором в 0.5 – 1 мм.

Для забезпечення захисту від витоку технічними каналами акустичної інформації з обмеженим доступом під час її озвучення рекомендується провести інженерні заходи з підвищення рівня звукоізоляції і віброізоляції приміщення для переговорів і нарад шляхом переобладнання кімнати з використанням звукоізоляційних матеріалів і конструкцій. Також рекомендується використати генератори коливань із встановленням випромінювачів на таких елементах як скло вікна, рами вікна, дверях, трубах системи опалення.

Слід брати до уваги, що рівень шуму при проведенні нарад і переговорів може дорівнювати 65 дБ. Враховуючи, що діапазон частот людської мови від

300 Гц до 3,4 кГц, необхідно забезпечити рівень звукоізоляції на частоті 300 Гц не менше 65 дБ.

Необхідно буде забезпечити звукоізоляцію стін, підлоги, стелі, дверей і вікна, а також віброізоляцію системи опалення, дверної лутки, дверей і каркасу вікна. Для цього доцільно буде використати багатошарові панелі звукоізоляції, закріплені на відстані 5 см від стіни. Для віброізоляції слід використати спеціальні прокладки, які будуть розв'язувати стики огороджувальних конструкцій, труби системи опалення, площу прилягання дверей до лутки, а також рами вікна. Простір між стіною і панелями необхідно буде заповнити волокнистим матеріалом для підвищення рівня звукоізоляції.

Стандартні одинарні двері, які встановлені на вході в приміщення, не можуть забезпечити необхідний звукоізоляції, навіть якщо виконано вимоги на щільність і ретельність виконання і підгонки дверного полотна до дверної коробки і усунені щілини між дверима та підлогою. Тому дверну лутку слід замінити спеціалізовану із тамбуром. Дверну лутка ущільнити на стиках прокладками з пористої гуми. Всередині тамбуру двері оббити спеціальною звуко-поглинаючою тканиною. Стики слід ущільнити вставками з пористої гуми.

Істотне підвищення звукоізоляції в порівнянні, зі звичайним вікном дають віконні рами спеціальної конструкції. Тому слід використати рами з комбінацією скла з різною товщиною (4-7 мм), встановлених на відстані не менше 20 мм і які мають високоякісний притвор з ущільнюючої гуми. Необхідно забезпечити ущільнення прилягаючих елементів конструкції гумовими вставками. Раму вікна закріпити на герметику. Також слід використати штори із звуко-поглинаючої тканини.

На сьогоднішній день ринок звукоізоляційних матеріалів надає широкий вибір споживачу, серед яких найбільшу ефективність мають багатошарові панелі.

З табл. 5.1 можна зробити висновок панелі ЗИПС-СИНЕМА мають найбільш прийнятні характеристики.

Таблиця 5.1 – Порівняльна характеристика багатошарових звукоізоляційних панелей за індексом додаткової звукоізоляції

| Частота акустичного сигналу, Гц | Тип багатошарової звукоізоляційної панелі | | |
|---|---|---|---|
| | ЗИПС-ВЕКТОР | ЗИПС-МОДУЛЬ | ЗИПС-СИНЕМА |
| | Значення індексу додаткової звукоізоляції, дБ | | |
| 250 | 13 | 16 | 18 |
| 315 | 13 | 16 | 18 |
| 500 | 18 | 20 | 24 |
| 630 | 18 | 20 | 25 |
| 1250 | 14 | 19 | 24 |
| 2500 | 19 | 21 | 24 |

Таблиця 5.2 – Перелік звукоізоляційних матеріалів і їх властивості

| Вид матеріалу | Назва Зовнішній вигляд | Характеристики |
|---|---|---|
| Мінеральна вата | «AcousticWool»  | Об’ємна щільність, р, кг/м$^3$ - 54; |
| Звукоізолююча багатошарова панель | «ЗИПС-СИНЕМА» | Поверхнева щільність системи – 39 кг/м$^2$ |
| Звукоізолюючі штори | «Саундтекс» - | Рівень звукоізоляції – 12 Дб |
| Звукоізоляційна стрічка | «Vibrosil»  | Об’ємна щільність, р, кг/м$^3$ - 32; |

Продовження таблиці 5.2

| **Вид матеріалу** | **Назва**<br>**Зовнішній вигляд** | **Характеристики** |
|---|---|---|
| Спеціалізовані кріплення для звукоізоляції | «Vibrofix»<br>  | Значення резонансної частоти – 6-10 Гц; |
| Звукоізолююча мембрана для підлоги | «Vibrostop»<br>  | Об’ємна щільність, р, кг/м$^3$ - 32; |

Дана панель дозволить забезпечити необхідний рівень звукоізоляції майже на всьому діапазоні частот. Для більшої ефективності простір між стіною і панелями слід заповнити мінеральною ватою «AcousticWool».

Встановлення подвійних дверей з тамбуром та подальшим внутрішнім оздобленням забезпечить рівень звукоізоляції в 65 дБ на частоті 500 Гц.

Встановлення рекомендованого склопакету забезпечить рівень звукоізоляції в 44 дБ на частоті 250 Гц.

Використання звукоізолюючої мембрани не дасть необхідний рівень звукоізоляції. Тому рекомендується реконструкція підлоги. Схема звукоізоляції підлоги наведена на рис. 5.2. Перелік рекомендованих звукоізоляційних матеріалів наведено у табл. 5.2.

Вікна і двері не можуть забезпечити необхідній рівень звукоізоляції на низьких частотах, тому ці елементи являються найбільш вразливими. В такому випадку для захисту від витоку віброакустичним і оптико-електронним каналами акустичної інформації пропонується використання генератора акустичних

коливань із встановленням випромінювачів на склі вікна, рамі вікна, дверях та на трубах системи опалення в місцях виводу з кімнати. Серед генераторів акустичних коливань зазначених у Переліку можливе використання наступних приладів.

Таблиця 5.3 – Перелік генераторів акустичних коливань

| **Тип приладу** | **Назва**<br>**Зовнішній вигляд** | **Характеристики** |
|---|---|---|
| Генератор акустичного шуму | МАРС-ТЗО-4-2<br>  | - діапазон частот шумового сигналу – від 180 до 5600 Гц;<br>- діапазон рівнів шумових сигналів на виходах – не менше 20 дБ; |
| Генератор акустичного шуму | Базальт-4ГА<br>  | - діапазон частот шумового сигналу – від 170 до 5700 Гц;<br>- діапазон рівнів шумових сигналів на обох виходах – не менше 20 дБ; |
| Генератор акустичного шуму | DNG-2300<br>  | - Діапазон частот шумового сигналу акустичних коливань – від 250 до 6500 Гц;<br>- Діапазон частот шумового сигналу вібраційних коливань – від 250 до 5000 Гц; |

За технічними характеристиками ці пристрої практично однакові, тому вибір основується ціні приладу. Тому пропонується застосування DNG-2300.

В якості випромінювачів рекомендується TRN-2000.

Монтаж конструкцій і розміщення обраних засобів захисту

Багатошарові панелі кріпляться за допомогою спеціалізованого віброізолюючого алюмінієвого профілю «Vibrofix» на відстані 5 см від стіни та стелі. Стики розв’язуються за допомогою звукоізоляційної стрічки «Vibrosil», для зменшення рівня вібрацій жорстких конструкцій.

Монтаж панелей звукоізоляції буде проводитись за схемою, що зображена на рис. 5.2.

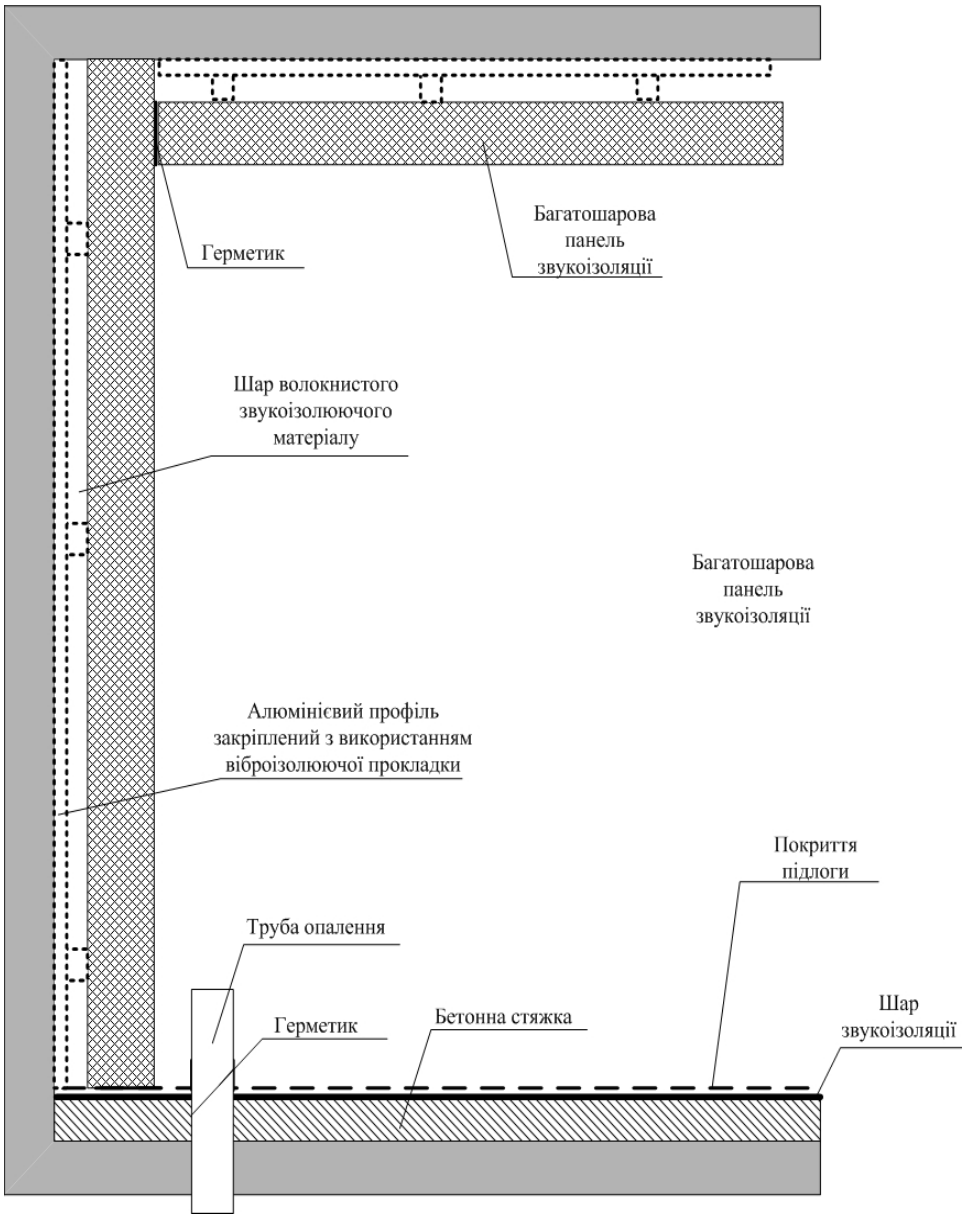



Рисунок 5.2 - Схема монтажу панелей звукоізоляції

Розміщення випромінювачів акустичних коливань схематично зображено на рис. 5.3.

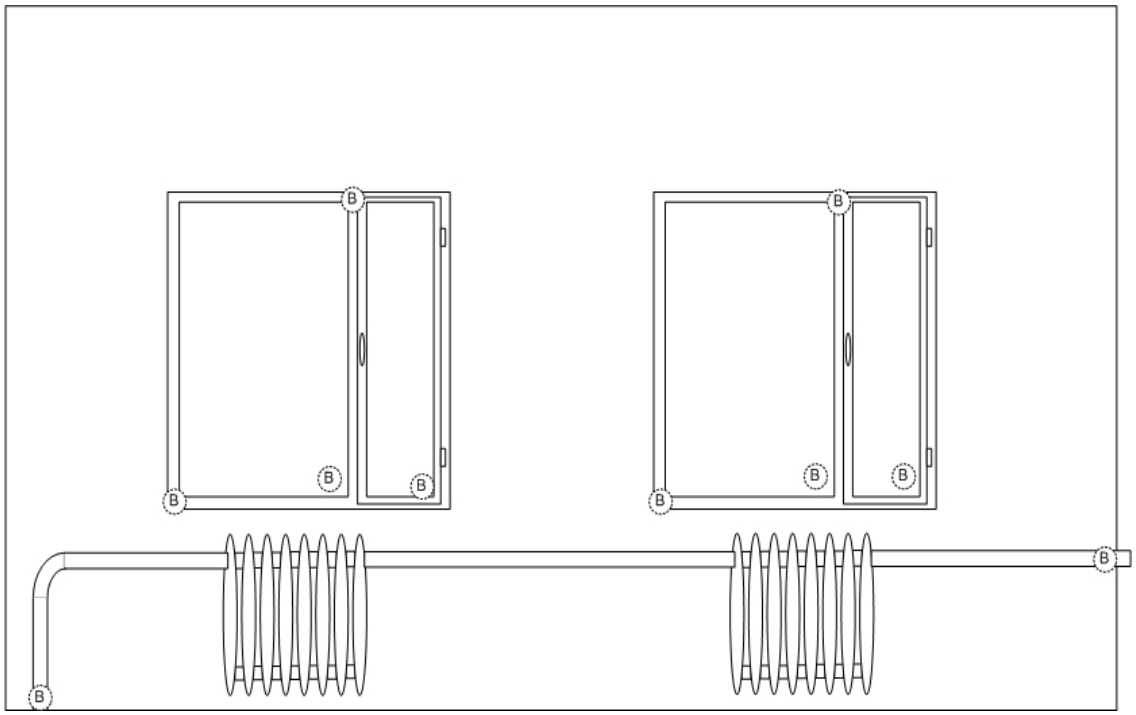



Рисунок 5.3 – Розміщення випромінювачів акустичних коливань

Позначка В – випромінювач

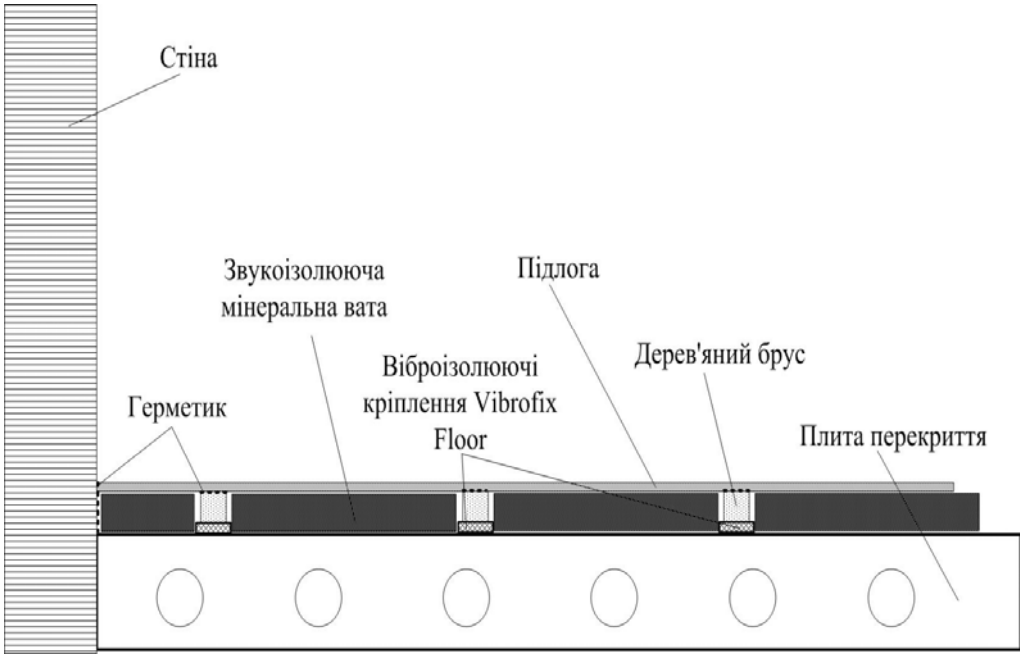



Рисунок 5.4 - Схема монтажу звукоізоляції підлоги

### 5.1.1 Організаційні заходи

Для забезпечення захисту інформації з обмеженим доступом під час проведення переговорів і нарад пропонуються рекомендації з організації таких

заходів. Переговори з участю представників сторонніх організації і підприємств повинні проводитись з дозволу начальника філії, який має назначити відповідальну за організацію переговорів особу. Для відповідального за організацію переговорів і нарад пропонуються наступні рекомендації:

- перед проведенням переговорів чи нарад приміщення необхідно обстежити на наявність сторонніх предметів, що можуть являти собою закамуфльовані технічні засоби розвідки, або зміні обстановки чи оздобленні кімнати, в яких ці засоби можуть розміщуватись;
- також рекомендується перевіряти на наявність технічних засобів розвідки прилягаючі приміщення начальника і стіни сходів, а також вікон і дверей;
- не допускати у приміщення сторонніх осіб без супроводу;
- не рекомендується використання і розташування у виділеному приміщенні засобів стільникового зв’язку, побутової техніки;
- переговори проводити при закритих вікнах і дверях;
- після проведення переговорів слід провести повторне обстеження, після чого необхідно замкнути і опечатати приміщення. Ключ передати на зберігання службі охорони.

# 6 ЕКОНОМІЧНА ЧАСТИНА

Метою економічного розділу є визначення витрат на розробку і впровадження комплексу технічного захисту інформації філії ПАТ «Дніпропетровськгаз». Актуальність даного питання полягає в тому, що впровадження КТЗІ у філії ПАТ «Дніпропетровськгаз» є економічно вигідним рішенням із захисту конфіденційної інформації від витоку технічними каналами.

Для визначення економічного ефекту потрібно:

- розрахувати капітальні витрати на проектування та впровадження комплексу технічного захисту інформації;
- розрахувати річні експлуатаційні витрати на функціонування комплексу технічного захисту інформації;
- оцінити можливий збиток від витоку конфіденційної інформації та загальний ефект від розробки комплексу технічного захисту інформації;
- розрахувати термін окупності капітальних витрат.

## 6.1 Розрахунок капітальних витрат для впровадження проекту

Капітальні витрати – це грошові кошти, призначені для створення та придбання основних фондів і нематеріальних активів, які підлягають амортизації. Для розрахунку капітальних витрат на проектування та впровадження комплексу технічного захисту інформації використаємо формулу (6.1):

$$К = К_{пр} + К_{об} + К_{вс}, \quad (6.1)$$

де К – капітальні витрати, грн;

$К_{пр}$ – вартість розробки комплексу технічного захисту інформації, грн;

$К_{об}$ – вартість обладнання комплексу технічного захисту інформації, грн;

$К_{вс}$ – витрати на впровадження комплексу технічного захисту інформації, грн.

Витрати на розробку комплексу технічного захисту інформації визначається за формулою (6.2):

$$К_{пр} = З_в \cdot t, \quad (6.2)$$

де $З_в$ – середньо-годинна заробітна плата спеціаліста з розробки, грн/год;

t – загальна тривалість розробки та впровадження комплексу технічного захисту інформації, год.

Середньо-годинна заробітна плата спеціаліста з розробки складає 60 грн/год.

Загальна тривалість розробки та впровадження комплексу технічного захисту інформації визначається за формулою (6.3):

$$t = t_{обс} + t_{мз} + t_{тз} + t_{пз} \text{ ,год}, \quad (6.3)$$

де $t_{обс}$ – тривалість проведення обстеження ОІД, год;

$t_{мз}$ – тривалість розроблення моделі загроз для ІзОД, год;

$t_{тз}$ – тривалість розроблення технічного завдання на комплекс технічного захисту інформації, год;

$t_{пз}$ – тривалість розроблення пояснювальної записки з проектування комплексу технічного захисту інформації, год.

$t = t_{обс} + t_{мз} + t_{тз} + t_{пз} = 16 + 12 + 5 + 12 = 45$ год.

Витрати на розробку комплексу технічного захисту інформації визначається за формулою (6.4):

$К_{пр} = З_в \cdot t = 60 \cdot 45 = 2700$ (грн.)

Витрати на будівельні матеріали, пасивні і активні засоби захисту, призначеного для розробки комплексу технічного захисту інформації філії ПАТ «Дніпропетровськгаз», представлені в табл. 6.1.

Таблиця 6.1 – Вартість матеріалів та обладнання

| **Назва** | **Ціна за одиницю, грн** | **Кількість** | **Загальна ціна, грн** |
|---|---|---|---|
| Багатошарова панель звукоізоляції «ЗИПС СИНЕМА» | 332 | 35 | 11620 |
| Подвійні двері | 7445 | 1 | 7445 |
| Металопластикове вікно | 2540 | 2 | 5080 |
| Генератор акустичного шуму DNG-2300 | 6360 | 1 | 6360 |
| Випромінювач TRN-2000 | 600 | 10 | 6000 |
| Засоби кріплення звукоізоляції«Vibrofix» | 1272 | - | 1272 |
| Звукоізоляційна мінеральна вата «AcousticWool» | 120 | 3 | 360 |
| Розхідні матеріали звукоізоляції (герметик, ущільнювачі) | 800 | - | 800 |
| Камери спостереження | 2400 | - | 2400 |
| Персональний комп’ютер | 2500 | 1 | 2500 |
| Плата відеозахвату | 800 | 1 | 800 |
| Коаксіальний кабель (150 м) | 1500 | - | 1500 |
| Розхідні матеріали для організації відеоспостереження | 150 | - | 150 |
| Протизавадний фільтр ФП-14 | 9500 | 1 | 9500 |
| Матеріали екрану виділеного приміщення серверної | 35000 | - | 35000 |
| Загальна сума | – | – | 90787 |

Отже витрати на обладнання, призначеного для розробки комплексу технічного захисту інформації становлять 90787 грн.

Витрати на впровадження комплексу ТЗІ розраховується із формули (6.5):

$$К_{вс} = К_{зв} + К_{серв} + К_{скуд}, \quad (6.5)$$

де $К_{зв}$ – витрати на монтаж звукоізоляції;

$К_{серв}$ – витрати на екранування серверної;

$К_{скуд}$ – витрати на встановлення відеоспостереження;

Монтаж звукоізоляції вираховується із вартості 80 гривень за квадратний метр, тоді:

$К_{зв}=80 \cdot 52,5=4200$ (грн.)

Монтаж екранованого приміщення вираховується із вартості заявленої компанією виконавцем:

$К_{серв}$=12000 (грн.)

Вартість встановлення відеоспостереження вираховується із вартості заявленої компанією виконавцем:

$К_{скуд}$=5900 (грн.)

Тоді за формулою (6.5) витрати на встановлення КТЗІ становлять:

$К_{вс} = К_{зв} + К_{серв} + К_{скуд}$ =4200 + 12000 + 5900 = 18100 (грн.)

Капітальні витрати на проектування та впровадження системи активної протидії знайдемо за формулою (3.1):

$К = К_{пр} + К_{об} + К_{вс}$ = 900 + 90787 + 18100 = 109787 (грн.)

### 6.2 Розрахунок експлуатаційних витрат

Експлуатаційні витрати на комплекс технічного захисту інформації складаються з витрат на Upgrade-відновлення й модернізацію системи інформаційної безпеки ($С_в$), що за моделлю Gartner Group складають 21% від вартості комплексу в цілому і вартості електроенергії, що споживається апаратурою КТЗІ протягом року ($С_е$), яка визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 1{,}06 \cdot 1991 \cdot 0{,}7 = 1477 \text{ (грн.)}, \quad (6.6)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

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

Тоді експлуатаційні витрати (С) за формулою (6.7):

$$С = К \cdot 0{,}21 + С_{ел}, \text{грн.} \quad (6.7)$$

С =109787 · 0,21 + 1477=24532 (грн.)

Отже експлуатаційні витрати становлять 24532 гривні на рік.

### 6.3 Оцінка можливого збитку від витоку інформації

#### 6.3.1 Оцінка величини збитку

Для оцінки величини збитку від витоку інформації технічними каналами необхідно проаналізувати цінність інформації з обмеженим доступом, що циркулює на об'єкті інформаційної діяльності філії ПАТ «Дніпропетровськгаз». Величина збитків (В) буде складатись з величини збитків зазнаних від компрометації інформації з обмеженим доступом ($В_к$) та витрат на відшкодування збитків ($П_в$). Компрометація інформації про стан системи захисту інформації, порядок охорони стаціонарних об'єктів може бути використана для атаки на локальну мережу філії, з ціллю несанкціонованого доступу до конфіденційної інформації, що циркулює в мережі, такої як інформація про реалізацію природного і скрапленого газу. Збитки можна оцінити від обсягу реалізації скрапленого газу за 2019 рік, що становить приблизно 1 млн. 135 тис. грн. Для розрахунку витрат на відшкодування збитків необхідні визначити витрати на повторне введення інформації $П_в$ за формулою (6.7):

$$П_в = \frac{\sum Зс}{F} \cdot t_в, \tag{6.8}$$

де $З_с$ – місячна зарплатня працівника задіяного в повторному введенні;

F – місячний фонд робочого часу, що становить 176 год.;

$t_в$ – витрачений на повторне введення час, що становлять 2 неділі.

Тоді за формулою (6.7) витрати на відшкодування збитків становлять:

Пв=5*7500*80/175=5681 (грн.)

Тоді величина збитку буде становити за формулою (6.8):

$$В = В_к + П_в = 1135000+5681=1140681 \text{ (грн)} \tag{6.9}$$

#### 6.3.2 Загальний ефект від впровадження КТЗІ

Загальний ефект від впровадження комплексу ТЗІ визначається за формулою (6.9):

$$Е = В – С, \text{ грн.} \tag{6.10}$$

де Е – загальний ефект від впровадження комплексу технічного захисту інформації, грн;

С – щорічні витрати на експлуатацію комплексу технічного захисту інформації, грн.

Е = 1140681 – 24532 = 1116149 грн.

### 6.4 Визначення та аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій визначається за формулою (6.8):

$$ROSI = \frac{E}{K} = \frac{1116149}{109787} \approx 10,1 \qquad (6.11)$$

де ROSI – коефіцієнт повернення інвестицій;

Е – загальний ефект від впровадження комплексу технічного захисту інформації, грн;

К – капітальні витрати на проектування та впровадження комплексу технічного захисту інформації, грн.

Термін окупності капітальних інвестицій показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження комплексу технічного захисту інформації, термін окупності визначається за формулою (6.9):

$$T_O = \frac{1}{ROSI} = \frac{1}{10,1} = 0,09\,років \approx 1 місяць, \qquad (6.12)$$

де $T_0$ – термін окупності капітальних інвестицій, рік .

То=1/10,1=0,09 років.

### 6.5 Висновок

В економічному розділі був зроблений розрахунок капітальних витрат на впровадження КТЗІ та річних експлуатаційних витрат на функціонування цього комплексу, які склали 109787 і 24532 грн. відповідно, термін окупності капітальних інвестицій становить 1 місяць, при коефіцієнті повернення інвестицій ROSI

– 10,1.

Ці показники доказують, що впровадження комплексу технічного захисту інформації на філії ПАТ «Дніпропетровськгаз» є ефективною і економічно доцільною мірою захисту інформації з обмеженим доступом від витоку технічними каналами.

# 7 ОХОРОНА ПРАЦІ

## 7.1 Аналіз небезпечних та шкідливих факторів

Філія Публічного акціонерного товариства «Дніпропетровськгаз» є об’єктом газової промисловості і тому відноситься до пожежонебезпечних об’єктів. До території філії прилягає відкрита трансформаторна підстанція та лінія електропередачі 110 кВ. На підприємстві існує служба охорони праці.

На співробітників філії рід шкідливих виробничих факторів, таких як:

– фізичні фактори – дія електричних і магнітних полів промислової частоти, мерехтіння екранів моніторів, випромінювання моніторів з електронно-променевими трубками, акустичний і вібраційний шум від роботи вентиляторів корпусів персональних комп’ютерів, акустичний і вібраційний шум утворюваний у майстернях;
– хімічні і біологічні шкідливі фактори не виявлені;
– напруженість праці – технологічний процес філії передбачає використання вузькоспеціалізованих програмних продуктів, використання яких вимагає інтенсивної розумової праці і створює нервово-емоційне напруження.

Робота багатьох працівників відділів пов’язана з використанням електричного устаткування (ПК, друкуючих пристроїв), тому існує небезпека ураження електричним струмом. Відділи філії за ступенем електробезпеки відносяться до приміщень без підвищеної небезпеки ураження електричним струмом. Ці приміщення сухі, з нормальною температурою, ізольованими полами, незначною запиленістю. Робота пристроїв задіяних у комплексі технічного за-хисту інформації не створює шкідливих умов праці співробітникам філії

**7.2 Інженерно-технічні заходи з охорони праці на філії «Дніпропетровськгаз»**

Рівні звуку на робочих місцях відповідають нормам, визначеним ДержСанПін 3.3.2-007-98.

Для запобігання впливу шуму необхідно вживати наступні заходи:

- застосовувати більш сучасне обладнання, зі здійсненням своєчасної профілактики та модернізації;
- використовувати шумопоглинаючі матеріали при обшивці стін та стелі.

Для того, щоб уникнути несприятливих факторів сенсорної напруги необхідно:

- періодично робити короткі перерви для відпочинку (15 хвилин через кожен час роботи) та виконувати фізичні вправи;
- розміщення технічних засобів і крісла в робочій зоні повинне забезпечувати зручний доступ до основних функціональних вузлів і блоків апаратури.

Згідно з ДНАОТ 0.00-1.31-99 освітлення в приміщенні може бути комбінованим, при якому недостатнє природне освітлення має бути доповнене штучним.

Для зменшення впливу навантаження на зорову систему, треба провести наступні заходи:

- у якості джерел штучного освітлення використовувати люмінесцентні лампи, які краще поєднуються з природним освітленням;
- розташовувати робочі місця таким чином, щоб у поле зору користувача не потрапляли вікна чи поверхні світильників. Крім того, джерела світла не повинні розташовуватися за спиною;
- світильники місцевого освітлення повинні мати захищений кут не менше $40^{O}$;
- в мережі штучного освітлення потрібно передбачити регулювання інтенсивності штучного освітлення;

– забезпечити періодичне виконання комплексу фізичних вправ для очей, передбачених ДержСанПін 3.3.2-007-98.

У відповідності до ГОСТ 12.1.005-88 ССБТ "Повітря робочої зони, загальні санітарно-гігієнічні вимоги", робота працівника лабораторії може бути віднесена до легкої фізичної роботи категорії 1Б з енерговитратами організму 138-172 Дж/с або 120-150 ккал/год.

Для усунення існуючих шкідливих факторів створених в приміщенні, яке було наповнене димом, у відповідності до СНіП 2.04.0591 "Опалення, вентиляція і кондиціонування», необхідно забезпечити оптимальну вентиляцію приміщення, оптимальні параметри мікроклімату, а також необхідні умови для подальшої безпечної і комфортної роботи у відділах ТОВ «АрхівКом», де встановлені технічні засоби задимлення.

Оптимальні норми параметрів мікроклімату з урахуванням категорії роботи працівників відповідно до ГОСТ 12.1.005-88 ССБТ "Повітря робочої зони, загальні санітарно-гігієнічні вимоги" наступні:

– в холодний період року температура повітря дорівнює 21-23 °С, швидкість руху повітря становить не більше 0,1 м / с, відносна вологість - 60%;
– в теплий період року температура повітря дорівнює 20-23 °С, швидкість руху повітря становить не більше 0,2 м / с, відносна вологість - 75%.

Для забезпечення даних умов мікроклімату в холодну пору року застосовують систему центрального опалення, а в теплу пору року - кондиціонери.

У відповідності з вимогами до електробезпеки комп'ютерних систем, повинні бути передбачені наступні заходи по захисту від ураження електричним струмом:

– лінія електромережі для живлення ПК, периферійних пристроїв та устаткування для обслуговування, ремонту та налагодження ПК виконується як

- окрема групова трьох-провідна мережа, шляхом прокладання фазового, нульового робочого і нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електропристроїв;
- заземлення повинно відповідати вимогам ДНАОП 0.00-1.21-98 "Правила безпечної експлуатації електрообладнання споживачів";
- необхідно забезпечити встановлення на помітному та доступному місці аварійного резервного вимикача, який може повністю вимкнути електричне живлення приміщення, крім освітлення;
- на кожній розетці повинен бути зазначений рівень напруги;
- працівники повинні пройти інструктаж з електробезпеки і дотримуватися його.

Рекомендації по охороні праці на об’єкті інформаційної діяльності:

- поліпшити контроль за виконанням вимог та інструкцій з техніки безпеки;
- усунути в обладнанні конструктивні недоліки, наслідки яких можуть призвести до травм;
- провести вимірювання опору заземлюючих пристроїв обладнання, ізоляції електроустановок, апаратів, електромережі об’єкта інформаційної діяльності з оформленням документів у строки і норми згідно техніки безпеки.

### 7.3 Розрахунок захисного заземлення серверної

Розрахунок захисного заземлення для серверного устаткування полягає у визначенні кількості необхідних вертикальних електродів.

Вихідними даними для розрахунку є:

- підприємство розміщене в другій кліматичній зоні;
- ґрунт – суглинок;
- значення опору заземлюючого пристрою відповідно до ПУЕ – 4 Ом;

– в якості вертикального заземлювача використовуються сталеві стрижні діаметром 15 мм і довжиною 5 м;
– в якості горизонтального заземлювача використовується сталева смуга товщиною 4 мм.

Розрахунковий питомий опір для однорідного ґрунту визначається за формулою (7.1):

$$\rho = \rho_{вим} \cdot \Psi, \text{ Ом·м}, \quad (7.1)$$

де Ψ - коефіцієнт сезонності для вертикального і горизонтального електродів, для другої кліматичної зони він має значення 1,3.

ρ = 100 · 1,3 = 130 Ом·м.

Для розрахунку опору вертикальних і горизонтальних заземлювачів використаємо формули (7.2) і (7.3) відповідно:

$$R = \frac{\rho}{2 \cdot \pi \cdot l} \cdot \left( \ln \frac{2 \cdot l}{d} + 0{,}5 \cdot \ln \frac{4 \cdot t + l}{4 \cdot t - l} \right) \quad (7.2)$$

$$R = \frac{\rho}{2 \cdot \pi \cdot l} \cdot \ln \frac{l^2}{d \cdot t} \quad (7.3)$$

де $l$ – довжина вертикального електроду;

d – діаметр вертикального електроду (для сталевої смуги d=0,5 ширини смуги);

t – відстань від поверхні землі до центру заземлювача;

Тоді за формулою (7.2) опір одного вертикального заземлювача:

$R$ =4,14·(6,5+0,5·0,82)=28,67 (Ом)

Один вертикальний заземлювач не відповідає вимогам, тому рекомендується збільшити їх кількість до 10, тоді за формулою (7.4):

$$R_в = \frac{R}{n \cdot ŋ} = \frac{28{,}67}{10 \cdot 0{,}67} = 4{,}27 \text{ (Ом)} \quad (7.4)$$

де ŋ - коефіцієнт використання вертикальних електродів без урахування впливу смуги зв’язку, n - кількість вертикальних заземлювачів.

$R_в = \frac{28{,}67}{10 \cdot 0{,}67} = 4{,}27$ (Ом)

Для з’єднання десяти вертикальних заземлювачів необхідно 10 м сталевої смуги шириною 4 см. Опір горизонтального заземлювача за формулою (7.3):

$$R_г = \frac{130}{2 \cdot 3,14 \cdot 50} \cdot \ln \frac{10^2}{0,02 \cdot 0,7} = 4,14 \cdot 8,87 = 3,67 \text{ (Ом)}$$

Загальний опір заземлювача визначається за формулою (7.5):

$$R_з = \frac{R_в \cdot R_г}{R_в \cdot \eta_г + R_г \cdot \eta_в \cdot n}, \text{ Ом} \quad (7.5)$$

де $\eta_в$ - коефіцієнт використання вертикальних електродів без урахування впливу смуги зв'язку;

n - кількість вертикальних заземлювачів;

$\eta_г$ - коефіцієнт використання горизонтального електрода, що з'єднує вертикальні заземлювачі.

$$R_з = \frac{28,67 \cdot 3,63}{28,67 \cdot 0,34 + 10 \cdot 0,67 \cdot 3,63} = 3,05 \text{ (Ом)}$$

Для штучного захисного заземлення достатньо 10 сталевих труб діаметром 15 мм і довжиною 5 м, а також 50 метрів сталевої смуги для з'єднання труб. Труби слід заглибити на 0,7 м від землі.

### 7.4 Пожежна профілактика філії «Дніпропетровськгаз»

Управління по експлуатації газового господарства є об'єктом газової промисловості і тому відноситься до пожежонебезпечних об'єктів. В технологічному процесі використовуються легкозаймисті і горючі рідини такі як мазут, бензин, дизельне паливо та ін.. Адміністративний корпус відноситься до категорії В і має другий ступінь вогнестійкості. Виникнення пожежі можливе за рахунок невиконання умов зберігання і експлуатації легкозаймистих і горючих рідин, короткого замикання електропроводки.

Для забезпечення пожежної безпеки необхідно:

- проводити регулярні перевірки працездатності існуючої на об'єкті пожежної сигналізації (датчики диму, комбіновані датчики - температури, диму та відкритого вогню, тривожну кнопку);
- провести інструктаж з пожежної безпеки з працівниками;

- скласти необхідні інструкції, розмістити плакати з правилами пожежної безпеки та правилами поведінки при пожежі;
- забезпечити наявність плану евакуації людей в аварійних ситуаціях.

### 7.5 Безпека в надзвичайних ситуаціях

Філія ПАТ «Дніпропетровськгаз» має розроблений план евакуації у разі виникнення надзвичайних ситуацій. В разі виникнення аварії природного чи техногенного характеру евакуація в адміністративному корпусі здійснюється через два виходи. Рекомендується розблокувати вхідні двері в західній частині адміністративного корпусу, для забезпечення додаткового аварійного виходу.

### 7.6 Висновок

В даному розділі визначенні шкідливі і небезпечні виробничі фактори філії Публічного акціонерного товариства «Дніпропетровськгаз», проаналізований вплив розроблювального комплексу технічного захисту інформації на умови праці співробітників, визначені необхідні інженерно-технічні вимоги з охорони праці, розроблені заходи з безпеки у надзвичайних ситуаціях і рекомендації з пожежної безпеки.

Розрахунок захисного заземлення встановив, що для заземлювача достатньо 10 сталевих труб діаметром 15 мм і довжиною 5 м, а також 50 м сталевої смуги товщиною 4 см для з’єднання вертикальних заземлювачів. Загальний опір заземлювача становить 3,05 Ом.

# ВИСНОВКИ

У кваліфікаційній роботі було проведене обстеження об’єкту інформаційної діяльності філії Публічного акціонерного товариства «Дніпропетровськгаз», розроблено модель загроз витоку інформації, в якій були проаналізовані ситуаційний план філії та основні технічні канали витоку інформації з обмеженим доступом і причини їхнього виникнення. За результатами обстеження і аналізу моделі загроз було створено проект комплексу технічного захисту інформації.

За ступенем захищеності система відповідає стандартам IP-67, а також камери відеоспостереження мають додатковий захист (водонепроникний металевий корпус). Для захисту від перешкод, всі кабелі прокладені з додатковою екранізацією, пропайкой і селеконовым герметиком.

Для живлення відеокамер використовували PoE (Power over Ethernet) - технологія, що дозволяє передавати віддаленому пристрою разом з даними електричну енергію через стандартну виту пару в мережі Ethernet. Технологія PoE істотно полегшує організацію живлення IP-камер, знижує витрати і не впливає на якість переданих даних.

Розроблена комп’ютерна мережа реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота. Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці, або додатках.

В економічному розділі був зроблений розрахунок капітальних витрат на проектування та впровадження комплексу технічного захисту інформації та річних експлуатаційних витрат на функціонування цього комплексу, які склали 109787 і 24532 грн. відповідно, термін окупності капітальних інвестицій становить 1 місяць, при коефіцієнті повернення інвестицій ROSI – 10,1. Ці показники доказують, що впровадження комплексу технічного захисту інформації на філії ПАТ «Дніпропетровськгаз» є ефективною і економічно доцільною мірою захисту інформації з обмеженим доступом від витоку технічними каналами.

У розділі охорони праці виконаний розрахунок захисного заземлення серверного приміщення філії Публічного акціонерного товариства

«Дніпропетровськгаз». Розрахунок захисного заземлення встановив, що для заземлювача достатньо 10 сталевих труб діаметром 15 мм і довжиною 5 м, а також 50 м сталевої смуги товщиною 4 см для з’єднання вертикальних заземлювачів. Загальний опір заземлювача становить 3,05 Ом.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2020. – 69 с.
2. Методичні вказівки з виконання заходів щодо охорони праці та розрахункової частини розділу «Охорона праці та безпека в надзвичайних ситуаціях» в дипломних проектах студентів всіх спеціальностей /Уклад. В.І. Голінько, В. Ю. Фрундін, Ю.І. Чеберячко, М.Ю. Іконніков - Дніпропетровськ: - Дніпропетровськ: Національний гірничий університет, 2013. – 12 с.
3. Методичні вказівки з виконання економічного розділу в дипломних проектах студентів спеціальності "Комп'ютерні системи " / Уклад. О.Г. Вагонова, О.Б. Нікітіна Н.М. Романюк – Дніпропетровськ: Національний гірничий університет. – 2013. – 11 с.
4. https://netacad.com – Комп'ютерна академія Cisco.
5. Э. Таненбаум., Д.Уэзеролл. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил.
6. В.Г. Олифер., Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 с.: ил.
7. Указ про положення про технічний захист інформації в Україні
8. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення
9. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи

10. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегрудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.; Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с.
11. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегрудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.; Арий, 2008. – Том II. Информационная безопасность. – 344 с.
12. Инженерно-техническая защита информации / Торокин А.А. – М.: Гелиос АРВ, 2005. – 960 с.
13. Защита от утечки информации по техническим каналам: учебное пособие / Бузов Г.А., Калинов С.В., Кондратьев А.В. – М.: Горячая линия – Телеком, 2005. – 416 с.
14. Хорев А.А. Способы и средства защиты информации (Електрон. Ресурс) / Спосіб доступу: URL: http://www.analitika.info/zaschita.php - Заголовок з екрану
15. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации (Електрон. ресурс) / Спосіб доступу: URL:http://www.analitika.info/kanalutechki.php - Заголовок з екрану

# ДОДАТОК А

## ТЕКСТ ПРОГРАМИ НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

**Міністерство освіти і науки України**
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**“ДНІПРОВСЬКА ПОЛІТЕХНІКА”**

# ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.20005-01 12 01

Листів 14

2020

# АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи.

Програма призначена для забезпечення налаштування DHCP, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній, домену комп’ютерної системи.

# ЗМІСТ

**1. Програмування Zone 1**

```
interface GigabitEthernet0/0/0
 ip address  192.168.128.1 255.255.252.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 ip address  192.168.132.1 255.255.252.0
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address  192.168.141.197 255.255.255.252
 ip nat inside
!
interface Serial0/1/1
 ip address  192.168.141.194 255.255.255.252
 ip nat inside
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 39
 passive-interface GigabitEthernet0/0/0
 passive-interface GigabitEthernet0/0/1
 network  192.168.128.0 0.0.3.255
 network  192.168.132.0 0.0.3.255
 network  192.168.141.192 0.0.0.3
 network  192.168.141.196 0.0.0.3
 no auto-summary
```

2. **Програмування Zone 2**

```
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password 7 0822455D0A16
!
!
ip dhcp excluded-address  192.168.136.1  192.168.136.10
ip dhcp excluded-address  192.168.137.1  192.168.137.10
ip dhcp excluded-address  192.168.138.1  192.168.138.10
!
ip dhcp pool vlan28
 network  192.168.136.0 255.255.255.0
 default-router  192.168.136.1
 dns-server  192.168.137.9
ip dhcp pool vlan38
 network  192.168.137.0 255.255.255.0
 default-router  192.168.137.1
 dns-server  192.168.137.9
ip dhcp pool vlan48
 network  192.168.138.0 255.255.255.0
```

```
 default-router  192.168.138.1
 dns-server  192.168.137.9
!
!
!
no ip cef
no ipv6 cef
!
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.28
 encapsulation dot1Q 28
 ip address  192.168.136.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0/0.38
 encapsulation dot1Q 38
 ip address  192.168.137.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0/0.48
 encapsulation dot1Q 48
 ip address  192.168.138.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0/1
 ip address  192.168.140.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address  192.168.141.193 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/1/1
 ip address  192.168.141.201 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/2/0
 ip address 209.165.202.3 255.255.255.224
 ip nat outside
!
interface Serial0/2/1
 no ip address
```

```
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 39
 redistribute static
 passive-interface GigabitEthernet0/0/0
 passive-interface GigabitEthernet0/0/1
 passive-interface GigabitEthernet0/0/0.28
 passive-interface GigabitEthernet0/0/0.38
 passive-interface GigabitEthernet0/0/0.48
 network  192.168.136.0 0.0.3.255
 network  192.168.140.0 0.0.0.255
 network  192.168.141.192 0.0.0.3
 network  192.168.141.200 0.0.0.3

!
ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224
ip nat inside source list 10 pool Internet
ip nat inside source static  192.168.141.185 209.165.202.2
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.4
!
ip flow-export version 9
!
!
access-list 10 permit  192.168.0.0 0.0.255.255
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
```

**3. Програування Zone 3**

```
interface GigabitEthernet0/0/0
 ip address  192.168.141.1 255.255.255.128
 duplex auto
```

```
 speed auto
!
interface GigabitEthernet0/0/1
 ip address  192.168.141.129 255.255.255.192
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address  192.168.141.198 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/1/1
 ip address  192.168.141.202 255.255.255.252
 ip nat inside
!
interface Serial0/2/0
 ip address  192.168.141.205 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 39
 passive-interface GigabitEthernet0/0/0
 passive-interface GigabitEthernet0/0/1
 network  192.168.141.0 0.0.0.127
 network  192.168.141.200 0.0.0.3
 network  192.168.141.196 0.0.0.3
 network  192.168.141.204 0.0.0.3

!
ip classless
!
ip flow-export version 9
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
```

```
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
```

# ВІДГУКИ КОНСУЛЬТАНТІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ