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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Лєвіна Єгора Геннадійовича*

академічної групи *125-20-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка комплексу технічного захисту інформації на об'єкті інформаційної діяльності ТОВ «Готік»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Мацюк С.М.			
розділів:				
спеціальний	к.т.н., доц. Мацюк С.М.			
економічний	к. е. н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Лєвіну Є.Г.*** **академічної групи** ***125-20-3***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

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

на тему ***Розробка комплексу технічного захисту інформації на об'єкті інформаційної діяльності ТОВ «Готік»***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № _____

Розділ	Зміст	Термін виконання
1	Обстеження ОІД підприємства, розробка моделі загроз, порушника та аналіз ризиків.	26.05.2024
2	Розробка політики безпеки інформації, вибір профілю захищеності, розробка комплексу технічного захисту інформації для підприємства.	19.06.2024
3	Розрахунок річних витрат на розробку комплексу технічного захисту інформації, оцінка величини збитку. Розрахунок ефективності запропонованого комплексу.	26.06.2024

Завдання видано _____ Мацюк С.М.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.05.2024

Дата подання до екзаменаційної комісії: 01.07.2024

Прийнято до виконання _____ Лєвін Є.Г.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 77 сторінок, 10 рисунки, 18 таблиць, 12 додатків, 11 джерел.

Об'єкт розробки: комплексу технічного захисту інформації на об’єкті інформаційної діяльності ТОВ «Готік».

Мета роботи: підвищення рівня захищеності інформації з обмеженим доступом, що циркулює на ОІД ТОВ «Готік».

У першому розділі кваліфікаційної роботи проведено обстеження ОІД ТОВ «Готік», проаналізовані існуючі канали витоку інформації, створені моделі загроз та порушника, а також сформульовані основні задачі даної кваліфікаційної роботи.

У спеціальній частині проведена оцінка стану захищеності на ОІД, в рамках розробки комплексу технічного захисту інформації (КТЗІ) запропоновані організаційні, інженерні та технічні заходи щодо захисту інформації від витоку акустичними та електричними каналами витоку інформації.

В економічному розділі визначені витрати на розробку і впровадження системи захисту інформації та проведено аналіз її економічної ефективності.

Практичне значення результатів кваліфікаційної роботи полягає у забезпеченні захисту інформації з обмеженим доступом на ОІД ТОВ «Готік» при впровадженні розроблювального КТЗІ на цьому підприємстві.

КАТЕГОРІЮВАННЯ, АНАЛІЗ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АНАЛІЗ РИЗИКІВ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

The explanatory note consists of 77 pages, 10 images, 18 tables, 12 appendices, 11 sources.

Object of development: technical protection complex at the information activities object of "Gotik" LLC.

The purpose of work: increasing the level of security of information with limited access circulating at the information activities object of "Gotik" LLC.

In the first section of the qualification work, an examination of the information activities object (IAO) of "Gotik" LLC was carried out, the existing channels of information leakage were analyzed, models of threats and intruders were created, and the main tasks of this qualification work were formulated.

In the special part, an assessment of the state of security at IAO was carried out, as part of the development of a complex of technical information protection (CTIP), organizational, engineering and technical measures were proposed to protect information from leakage through acoustic and electrical channels of information leakage.

In the economic section, the costs for the development and implementation of the information protection system are determined and an analysis of its economic efficiency is carried out.

The practical significance of the results of the qualification work is to ensure the protection of information with limited access on the IAO of Gotik LLC during the implementation of the development CTIP at this enterprise.

CATEGORIZATION, THREAT ANALYSIS, INTRUDER MODEL, RISK ANALYSIS, UNAUTHORIZED ACCESS, OBJECT OF INFORMATION ACTIVITY, INFORMATION SECURITY POLICY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСП – деревостружкова плита;

ДТЗС – допоміжні технічні засоби та системи;

ІД – інформаційна діяльність;

ІзОД – інформація з обмеженим доступом;

КЗ – контрольована зона;

КТЗІ – комплекс технічного захисту інформації;

ЛАЛС – лазерні акустичні локаційні системи;

ОІД – об’єкт інформаційної діяльності;

ПЕМВН – побічні електромагнітні випромінювання і наводки;

СЗІ – служба захисту інформації;

ТЗІ – технічний захист інформації;

ТЗПІ – технічні засоби зберігання, обробки і передачі інформації;

ТОВ – товариство з обмеженою відповідальністю;

ТР – технічна розвідка.

ЗМІСТ

ВСТУП ... 8
РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ ... 9
1.1 Загальні відомості про ТОВ «Готік» ... 9
1.2 Види інформації, яка циркулює на ОІД та її категоріювання ... 9
1.3 Обґрунтування необхідності створення КТЗІ ... 13
1.4 Категоріювання приміщень, де циркулює інформація з обмеженим доступом ... 14
1.5 Встановлення контрольованої зони ... 14
1.6 Обстеження ОІД ... 14
1.7 Аналіз загроз інформації, що циркулює на ОІД ... 22
1.8 Аналіз найбільш вагомих загроз інформації з обмеженим доступом, яка циркулює на ОІД ... 27
1.9 Постановка задачі ... 27
РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА ... 29
2.1 Оцінка існуючого стану захищеності ОІД ... 29
2.2 Основні організаційні заходи захисту ... 30
2.3 Розробка заходів захисту акустичної (мовної) інформації під час проведення закритих заходів ... 32
2.4 Розробка заходів захисту інформації від витоку колами електроживлення ... 44
2.5 Висновок ... 47
РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА ... 49
3.1 Обґрунтування витрат на реалізацію комплексу технічного захисту інформації ... 49
3.2 Розрахунок капітальних витрат ... 49
3.3 Розрахунок експлуатаційних витрат ... 51
3.4 Оцінка величини збитку ... 52
3.6 Загальний ефект від впровадження комплексу технічного захисту інформації ... 54
3.7 Визначення та аналіз показників економічної ефективності ... 54
3.8 Висновок ... 55
ВИСНОВКИ ... 56
ПЕРЕЛІК ПОСИЛАНЬ ... 57
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи ... 58
ДОДАТОК Б. Перелік документів на оптичному носії. ... 59
ДОДАТОК В. Наказ про створення служби захисту інформації ... 60
ДОДАТОК Г. Наказ про створення комісії по категоріюванню та обстеженню ОІД ... 62

ДОДАТОК Ґ. Наказ про встановлення контрольованої зони 63
ДОДАТОК Д. Акти категоріювання приміщень 64
ДОДАТОК Е. Наказ про встановлення контрольованої зони 68
ДОДАТОК Є. Ситуаційний план ОІД ТОВ «Готік» 69
ДОДАТОК Ж. План розміщення технічних засобів захисту акустичної (мовної) інформації в залі засідань 70
ДОДАТОК З. Плани комунікацій на ОІД 71
ДОДАТОК И. Відгук керівника економічного розділу 75
ДОДАТОК І. Відгук керівника кваліфікаційної роботи 76

ВСТУП

До недавнього часу саме поняття інформаційної безпеки асоціювалося виключно з режимними державними підприємствами, проте інтенсивність розвитку автоматизації приватного бізнесу, введення поняття «комерційна таємниця» і жорстка конкуренція у сфері виробництва примушують керівників підприємств різного масштабу все більше замислюватися над забезпеченням безпечної експлуатації інформаційних ресурсів.

Пріоритетним напрямом у процесі формування та забезпечення інформаційної безпеки будь-якої компанії є збереження в таємниці важливої комерційної інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

Стрімкий темп розвитку техніки в останні десятиліття викликав ще більш бурхливий розвиток технічних пристроїв і систем розвідки. Тому все актуальнішою стає проблема витоку інформації з обмеженим доступом технічними каналами.

Запобігання витоку інформації технічними каналами передбачає створення організаційних і технічних заходів захисту, що являють собою комплекс технічного захисту інформації.

В Україні сьогодні питанням інформаційної безпеки приділяють особливу увагу. На теперішній час сформована належна законодавча база. Усе більшого значення набуває необхідність забезпечення конфіденційності інформації з обмеженим доступом, ознайомлення, використання чи розголошення якої може завдати шкоди суспільству й державі, юридичним та фізичним особам.

Для ТОВ «Готік», на якому циркулює інформація з обмеженим доступом, захист цієї інформації є важливою складовою ведення бізнесу. Тому створення комплексу технічного захисту інформації на даному об’єкті є актуальним.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про ТОВ «Готік»

Підприємством, на якому розташований ОІД, є ТОВ «Готік» - міжнародна аутсорсингова компанія, яка надає послуги у сфері телефонного обслуговування та інформаційної підтримки клієнтів різноманітних компаній. Форма власності – приватна. Співпрацює із компаніями-замовниками, які ведуть свою діяльність в сфері телекомунікацій (інтернет-провайдери, мобільні оператори та ін.). Компанія забезпечує цілодобову інформаційну підтримку в телефонному режимі, також займається телемаркетингом – продажами та оформленням договорів по телефону.

Старші спеціалісти та тренери організовують навчання операторів, розробляють проєкти та методи проведення ефективних телефонних переговорів, що, в свою чергу, забезпечить якісне обслуговування клієнтів.

Організаційна структура компанії:

1 Директор -1чол.;
2 Старші спеціалісти – 7 чол.;
3 Тренери - 5 чол.;
4 Група контролю якості роботи операторів –5 чол.;
5 Оператори – 95 чол.;
6 Бухгалтери – 3 чол.;
7 Системні адміністратори – 2 чол.;
8 Охорона – 5 чол.;
9 Тех. персонал – 5 чол.

1.2 Види інформації, яка циркулює на ОІД та її категоріювання

На ОІД циркулює як відкрита інформація, так і інформація з обмеженим доступом.

Категоріювання інформації передбачає визначення правового режиму, приміщення в якому вона зберігається, осіб, які мають доступ до неї та вид, у якому вона циркулює на ОІД.

Категоріювання інформації, яка циркулює на ОІД, представлено у виді таблиці 1.1

Таблиця 1.1 - Категоріювання інформації, що циркулює на ОІД

№	Інформація	Режим доступу	Правовий режим	Носій, що зберігає інформацію	Приміщення	Особи, що мають доступ
1	2	3	4	5	6	7
1	Організаційно-статутна інформація	Відкрита		Паперовий	Кабінет директора	Всі робітники компанії
2	Умови контрактів, укладених із замовниками	З обмеженим доступом	Комерційна таємниця	Акустичний	Зал засідань	Директор, старші спеціалісти, тренери
				Паперовий	Кабінет директора	
3	Інформація про робітників, трудові договори	З обмеженим доступом	Конфіденційна	Паперовий	Приміщення відділу кадрів	Директор, відділ кадрів, старші спеціалісти

Продовження таблиці 1.1

1	2	3	4	5	6	7
4	Бази даних клієнтів	З обмеженим доступом	Конфіденційна	Електронний	Серверна	Директор, ст. спеціалісти, оператори
5	Інформація бухгалтерської звітності	З обмеженим доступом	Конфіденційна	Електронний	Кабінет бухгалтерів	Директор, бухгалтери
				Паперовий		
6	Проєкти спеціалістів	З обмеженим доступом	Комерційна таємниця	Електронний	Серверна, приміщення ст.спеціалістів і тренерів	Директор, ст.спеціалісти, тренери
				Акустичний	Зал засідань, кімнати операторів	
				Паперовий	Кабінет директора	
7	Інформація, яку повинні надавати оператори клієнтам	Відкрита		Електронний	Сервер у приміщенні системного адміністратора	Директор, ст.спец-ти,тренери, оператори, клієнти
				Акустичний	Кімнати операторів	

Обмін інформацією між відділами та структурними одиницями компанії представлений у вигляді схеми інформаційних потоків на ОІД (Рисунок 1.1).

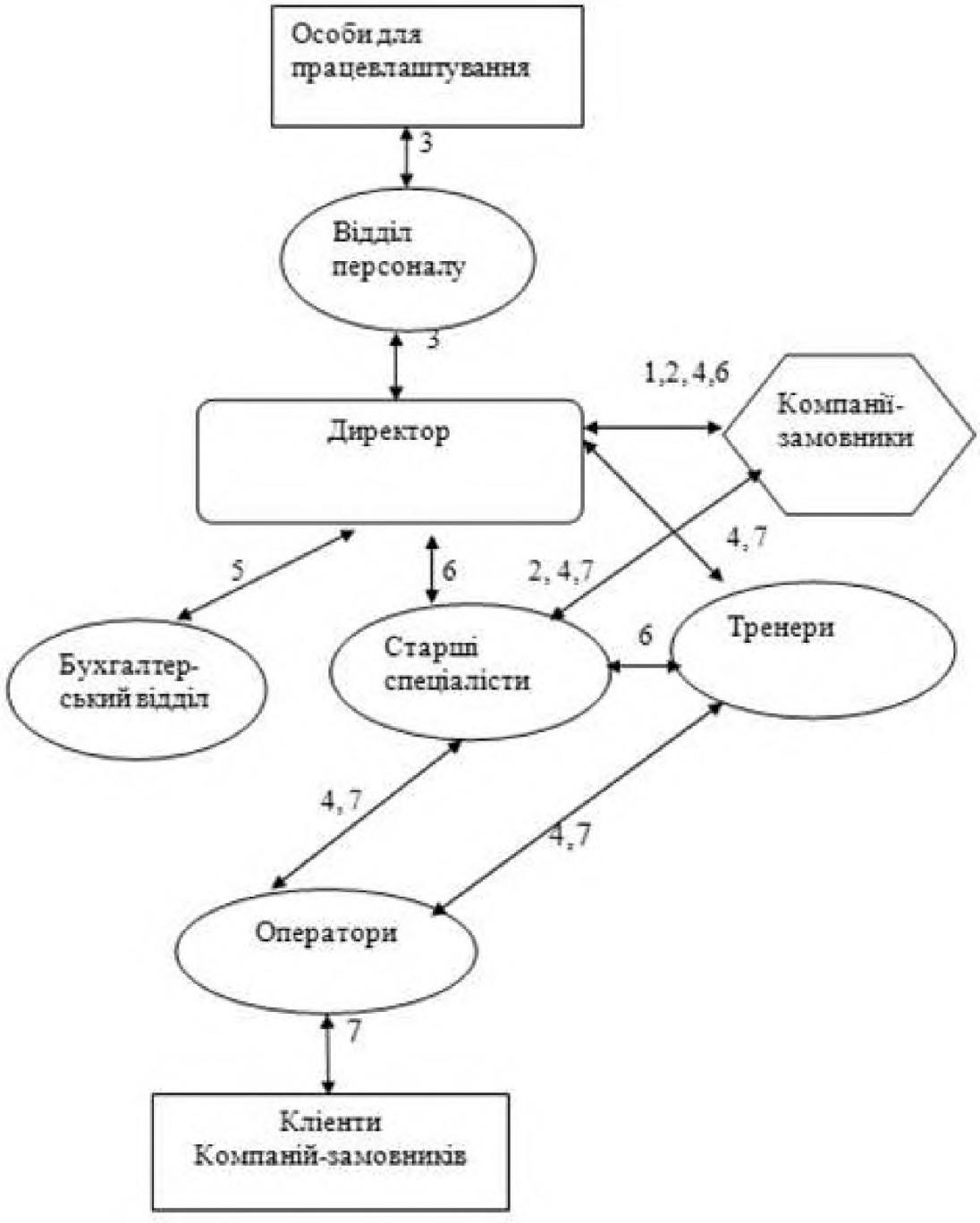


Рисунок 1.1 - Схема інформаційних потоків на ОІД

На рисунку 1.1 вказані основні інформаційні потоки на ОІД. Номером зазначений вид інформації, яка передається між відділами та структурними одиницями компанії. Обмін даною інформацією відбувається у двосторонньому напрямку.

Обмін інформацією, що містить комерційну таємницю проходить між наступними ланками:

- директор – компанії-замовники;
- компанії-замовники – старші спеціалісти;
- директор – старші спеціалісти;
- старші спеціалісти – тренери.

Обмін конфіденційною інформацією відбувається між наступними ланками:

- особи для працевлаштування - відділ персоналу;
- відділ персоналу - директор;
- директор - бухгалтерський відділ;
- директор - компанії-замовники;
- компанії-замовники - старші спеціалісти;
- директор - тренери;
- старші спеціалісти, тренери - оператори;
- тренери - група контролю якості.

1.3 Обґрунтування необхідності створення КТЗІ

На ОІД циркулює інформація з обмеженим доступом, яка являє собою конфіденційну інформацію та інформацію, що становить комерційну таємницю. На ОІД не зберігається та не оброблюється інформація, що становить інші види таємниць.

На підставі наявності ІзОД на ОІД та необхідності збереження конфіденційності даної інформації було прийнято рішення про створення служби захисту інформації на підприємстві, а також розробки комплексу технічного захисту інформації. Наказ про створення СЗІ на підприємстві приведений у Додатку.

Наказ на створення комісії по категоріюванню та обстеженню об’єкта наведений у Додатку.

1.4 Категоріювання приміщень, де циркулює інформація з обмеженим доступом

Відповідно до положення про категоріювання об'єктів, встановлюються чотири категорії об'єктів залежно від правового режиму доступу до інформації, що циркулює в них:

- до першої категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю, для якої встановлено гриф секретності "особливої важливості";
- до другої категорії відносяться об’єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю, для якої встановлено гриф секретності "цілком таємно";
- до третьої категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю, для якої встановлено гриф секретності "таємно", а також інформація, що містить відомості, які становлять іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству й державі;
- до четвертої категорії відносяться об'єкти, в яких циркулює конфіденційна інформація.

Відповідно до акту категоріювання приміщень ОІД, який наведено в Додатку, на ОІД розташовані приміщення четвертої категорії.

1.5 Встановлення контрольованої зони

Контрольована зона – територія, на якій унеможливлюється несанкціоноване перебування сторонніх осіб. Встановлення контрольованої зони на ОІД регламентовано наказом №124, який наведено у Додатку.

1.6 Обстеження ОІД

Згідно із НД ТЗІ 3.1-001-07(п.5,6) [2], першим етапом створення КТЗІ є виконання передпроєктних робіт, в яких, зокрема, передбачається проведення обстеження діючого ОІД. Метою обстеження є підготовка вихідних даних для формування вимог щодо створення КТЗІ.

Результати обстеження ОІД викладено у відповідному акті обстеження.

ЗАТВЕРДЖЕНО

Директор ТОВ «Готік»

Коваленко О.О.

_____(підпис)

03 січня 2024 р.

АКТ

обстеження об'єкту інформаційної діяльності

ТОВ «Готік»

1 Обстеження на ОІД проведено 02 січня 2024р. комісією у складі: голова комісії Прокопенко С.С, члени: Антоненко В.О, Кірлаш О.Д., призначеною наказом № 177 від 02 січня 2024 року. Обстеження проведено згідно із НД ТЗІ 3.1-001-07[2].

2 Загальні відомості:

2.1 Характеристика ОІД

Об'єкт інформаційної діяльності належить ТОВ «Готік» - міжнародній компанії, яка надає послуги у сфері телефонних продажів, реклами, онлайн консультацій в телефонному режимі.

ОІД – комплекс приміщень, розташованих в адміністративній будівлі за адресою: м. Дніпро, вул. Молодогвардійська 7.

ОІД складають приміщення:

- кабінет директора та приймальна директора;
- зал засідань;
- кімната операторів;
- приміщення тренерів і старших спеціалістів;
- серверна.

Межі контрольованої зони об'єкта співпадають із зовнішніми стінами будівлі, у якій розташований ОІД, окрім частини західної сторони будівлі. Із західної сторони контрольована зона обмежена парканом заввишки 2 м, який огороджує внутрішній двір організації.

Північна сторона офісу - зовнішня стіна будівлі (на відстані 26 м – одноповерховий будинок, в якому розміщено кафе; також на відстані 23м- знаходиться 3 поверховий житловий будинок)

Південна сторона офісу – зовнішня стіна будівлі (на відстані 18 м знаходиться 5-поверховий житловий будинок, на відстані 18 м – проїжджа частина вулиці, за якою розташована лісопаркова зона),

Західна сторона – внутрішній двір та зовнішня стіна будівлі (на відстані 6 м від паркану внутрішнього двору знаходиться парковка загального користування).

Східна сторона - зовнішня стіна будівлі (на відстані 20 м знаходиться 2-поверховий житловий будинок).

Охорона периметру КЗ та пропускний режим забезпечується обладнаним контрольно-пропускним пунктом (турнікет із електромагнітними зчитувачами).

Ситуаційний план ОІД ТОВ «Готік» наведений у Додатку.

2.2 Характеристика складових ОІД

Архітектурно-будівельні особливості приміщення:

– стіни – цегляні, товщина - 280 мм;

– перекриття - монолітні ж/б плити;

– стеля - підвісна, виготовлена з гіпсокартону, товщина - 60 мм, відстань між стелею та перекриттям 450мм;

– висота приміщень – 3 м;

– вікна – металопластикові, подвійні, розмір 2х1,5м;

– двері – вхідні-металеві, розмір 2.2х1.5 м, міжкімнатні – ДСП товщиною 40 мм, розмір 2.2х1.1м.

Приміщення, які призначені для обробки або зберігання інформації з обмеженим доступом:

1) кабінет директора;

2) зал засідань;

3) серверна;

4) приміщення тренерів і старших спеціалістів;

5) кабінет бухгалтерів.

В будинку без належного контролю не працюють іноземні громадяни, неконтрольоване перебування сторонніх осіб унеможливлено.

Складові ОІД, що можуть впливати на показники ефективності захищеності ІзОД і які можуть бути середовищем поширення за межі КЗ її носіїв:

- внутрішня телефонна лінія, яка підключається до АТС, має вихід за КЗ. Використовується кабель КСППБ, призначений для ліній міжстанційного та абонентського зв'язку з ущільненням багатоканальними системами передачі з тимчасовим поділом каналів і імпульсно-кодовою модуляцією зі швидкістю передачі до 2048 кБіт/с при напрузі дистанційного живлення до 500 В постійного струму. АТС № 9 знаходиться за адресою вул.Молодогвардійська, 12, на відстані 51 м від ОІД.

План-схема розташування телефонних ліній наведена у Додатку З, рисунок З.1.

- Система електроживлення, від якої живляться ОТЗ та ДТЗС підключається до трансформаторної підстанції, яка має сторонніх споживачів, має вихід за межі КЗ. Трансформаторна підстанція знаходиться на відстані 38 м від ОІД.

План-схема розташування телефонних ліній наведена у Додатку З, рисунок З.2.

- Система заземлення не виходить за межі КЗ;

- Система опалення – газова котельня, яка знаходиться на задньому дворі (не виходить за границі КЗ);

- Система водопостачання – міськводоканал, водонапірна станція № 12 на відстані 53 м.

- Система пожежної сигналізації автономна, включає в себе димові сповіщувачі, сповіщувачі ручний та світлозвуковий, які підключені з'єднувальним дротом до централі, система охоронної сигналізації складається з інфрачервоних сповіщувачів руху, магнітоконтактних датчиків та датчиків розбиття скла, які підключені до централі.

У таблиці 1.2 наведений перелік та характеристика складових системи охоронно-пожежної сигналізації.

План-схема охоронної та пожежної сигналізації наведена Додатку З, рисунок З.4.

Таблиця 1.2 - Перелік та характеристика складових системи охоронно-пожежної сигналізації ТОВ «Готік»

№	Пристрій	К-сть	Виробник	Технічні характеристики
1	2	3	4	5
1	Димовий датчик СПД - 2 Тірас 	27	Україна	Тип датчика: провідний; Тип сенсора: фотоелектричний; Площа покриття: 100 м ²; Робоча напруга: 8 - 28 В; Чутливість: 0,05-0,2 дБ / м Струм в черговому режимі: 0,1 мА; Діапазон робочих температур: -10 ° С ~ +55 ° С; Робоча вологість: 93% при температурі +35 ° С; Розміри: 99 × 46 мм; Маса: 0,15 кг
2	Сповіщувач пожежний ручний Тірас –СПР1 	1	Україна	Робоча напруга - 8-28 В; Електричний опір контактів для послідовного включення – не більше 0,5 Ом; Внутрішній опір контактів для паралельного включення при струмі (20±2) мА – не більше 450 Ом; Діапазон робочих температур – від -10 до +55 °С; Ступінь захисту оболонки – IP 40; Габаритні розміри – 93х90х43мм; Маса – 0,12 кг

Продовження таблиці 1.2

1	2	3	4	5
3	Світло-звуковий оповіщувач «Джміль» 	1	Україна	Напруга живлення- 12±3 В; Струм живлення,не більше: світлового оповіщувача – 0,025 А; звукового оповіщувача – 0,15 А; Акустична потужність - не менше 80 дБ; Діапазон робочих температур - 10 +55 ºС; Резонансна частота - 2,5 +4,5 кГц; Маса - не більше 0,3 кг; Габаритні розміри - не більше 92×47×112 мм.
4	Сповіщувач руху інфрачервоний «Рух» 	14	Україна	Кут огляду в горизонтальній площині - не менше 85 º; Напруга живлення – 10.2 -15 В; Струм живлення не більше 25 мА; Тривалість тривожного сигналу не менше 2 с; Діапазон робочих температур -10 до +55 º С; Час відновлення після режиму тривоги - не більше 10 с; Габаритні розміри - 105х70х46 мм; Маса 120 г.
5	Сповіщувач охоронний магніто-контактний СОМК 1-1 	10	Україна	Діапазон робочих напруг -1-72 В; Діапазон ком. токів 0.1-100 мА; Електричний опір сповіщувача в чергувальному режимі не більше 0.5 Ом; Опір в режимі «Тривога» - не менше 200 кОМ; Метод установки –накладний; Габарити 50х14х10 мм; Маса 15.5.г.

Продовження таблиці 1.2

1 1	2	3	4	5
	Сповіщувач розбиття скла СОЛО 	11	Україна	Кут огляду в горизонтальній площині, не менше 120 °; Напруга живлення –10-15 В; Струм споживання – не більше 24 мА; Тривалість тривожного сповіщення 2-10 с; Дальність дії 3-8 м; Габарити 100х66х35 мм; Маса 100 г.
	Централь Satel VERSA-15 	1	Польща	Максимальна кількість зон в системі – 30; Максимальна емність акумулятора – 17 Ач; Модуль GSM – вбудований; Номінальна напуга живлення головної плати – 18 В; Максимальний струм програмувальних виходів – 50 мА; Діапазон робочих температур від -10 до +55 ° С. Габарити – 260х135 мм.
	Блок безперебійного живлення БЖ-1230 	1	Україна	Діапазон напруг живлення (від мережі) - 187 – 242 В; Потужність, що споживається від мережі, не більше - 70 ВА; Струм, що споживається від мережі, не більше - 0,38 А; Максимальна напруга заряду батареї (при температурі навколишнього середовища +200 ° С) - 13,65В; Акумуляторна батарея - номінальна напруга - 12В; - ємність - 7 – 18 А*год; Напруга відключення батареї від навантажування - 10,5 – 10,9В; Максимальний струм через вихід „ВН” - 200 мА; Габаритні розміри мм 215±5 х 300±5 х 85±5.

- Система контролю і управління доступом: у холі встановлено контрольно-пропускний пункт, реалізований за допомогою турнікету і зчитувача магнітних брелків.

2.4. Результати аналізу наявності в установі:

– на ОІД є затверджена схема КЗ відповідно з наказом № 124 від 03.01.2024, в межах якої розташований ОІД. Схема КЗ позначена на ситуаційному плані;

– дані про можливі місця розміщення ззовні КЗ засобів технічної розвідки тривалого перехоплення зазначені в таблиці 1.3 та позначені на ситуаційному плані (Додаток Ж).

Таблиця 1.3 – Можливі місця розміщення засобів технічної розвідки

№	Приміщення, у якому обробляється ІзОД	Місця, де можуть бути розташовані засоби ТР	Мінімальна відстань до ОІД, м
1	Східна сторона будівлі (кабінет директора)	Житловий 5 поверховий будинок	--
2	Південна сторона будівлі (зал засідань, кабінет директора, кімната операторів)	Житловий 5 поверховий будинок	--
3	Західна сторона будівлі (серверна)	Парковка загального користування	10

Межі контрольованої зони зі східної та південної сторони співпадають із контуром будівлі. Це дає можливість безперешкодного встановлення засобів технічної розвідки на мінімальній відстані до ОІД. Це становить загрозу несанкціонованого зніманню інформації, і, як наслідок, порушення її конфіденційності.

1 Пропозиції щодо необхідності:

- побудувати модель порушника та модель загроз для ОІД;

- створення відомості про вірогідність та опис загроз необхідно викласти в “Окремій Моделі загроз для інформації, яка циркулює на ОІД організації.”

– розроблення технічних вимог та завдань з питань ТЗІ.

Голова комісії _____ С.С.Прокопенко

Члени комісії: _____ В.О.Антоненко, О.Д. Кірлаш.

1.7 Аналіз загроз інформації, що циркулює на ОІД

Виходячи із результатів проведеного обстеження на ОІД була побудована модель порушника та модель загроз для інформації, яка циркулює на ОІД.

1.7.1 Побудова моделі порушника

Класифікація порушників у моделі порушника проводиться за двома основними показниками: рівень можливостей та рівень кваліфікації порушника. Також до уваги прийнято місце здійснення дії порушника та його мотив.

Класифікація порушників здійснюється за наступними категоріями:

Внутрішні порушники:

Пв1 – директор, системний адміністратор, адміністратор безпеки;

Пв2 – тренери, старші спеціалісти;

Пв3 – оператори;

Пв4 – техпрацівники, охорона, інші відділи (відділ кадрів і бухгалтерія);

Пв5 – відвідувачі.

Зовнішні порушники:

Пз1 – конкуренти;

Пз2– кримінальні структури;

Пз3 – випадкові особи.

Можливості порушників можна поділити за наступними рівнями:

М1 - даний рівень визначає найнижчий рівень можливостей порушника, повна відсутність прав доступу до ІзОД на ОІД;

М2 - другий рівень визначається можливістю доступу до ІзОД шляхом використання службових повноважень, примітивних засобів технічної розвідки

М3 - третій рівень визначається можливістю управління функціонуванням доступу до ІзОД на ОІД шляхом використання службових повноважень, можливістю модифікувати інформацію.

М4 - четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проєктування, реалізацію, впровадження та адміністрування на ОІД.

Дана класифікація є ієрархічною, тобто кожний наступний рівень включає в себе

функціональні можливості попереднього.

За рівнем знань про ОІД порушники поділяються на такі категорії:

З1 - володіють незначним рівнем знань та досвідом роботи з технічними засобами, не володіють знаннями по особливостям функціонування ПЗ та СТЗІ на ОІД;

З2 - володіють інформацією про функціональні особливості ОІД, вміють користуватися штатними засобами;

З3 - володіють високим рівнем знань та досвідом роботи з технічними засобами та їхнього обслуговування;

З4 - володіють високим рівнем знань у галузі обчислювальної техніки, проєктування та експлуатації АС на ОІД

Метою порушника можуть бути:

К1 - отримання необхідної інформації у потрібному обсязі та асортименті;

К2 - мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

К3 - нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Мотив, який переслідує порушник:

Ц1 – безвідповідальність;

Ц2 – самоствердження;

Ц3 – вилучення матеріальної вигоди;

Ц4 – помста.

За рівнем доступу до ОІД порушники поділяються за наступними категоріями:

Д1 - з одержанням доступу на контрольовану територію, але без доступу до ТЗПІ;

Д2 - з одержанням доступу до ТЗПІ;

Д3 - з одержанням доступу до місць накопичення і зберігання даних;

Д4 - без одержання доступу на контрольовану територію організації

Рівень загрози, яку несе порушник, наведено з розподілом від 1 до 5. Мінімальне значення - 1, максимальне – 5.

У таблиці 1.4 наведена модель порушника для ОІД ТОВ «Готік»

Таблиця 1.4 - Модель порушника

Порушник	Рівень можливостей порушника	Мотив порушника	Мета порушника	Рівень кваліфікації	Місце здійснення дії порушника	Рівень загрози, що несе порушник
Пв1	М4	Ц1,4	К1-3	З4	Д3	4
Пв2	М3	Ц1,2,4	К1-3	З2,3	Д2	3
Пв3	М2	Ц1,2,4	К-1,3	З2	Д2	3
Пв4	М1	Ц1,2,4	К-1	З1	Д1	2
Пв5	М1	Ц2,3	К-1	З1	Д1	2
Пз1	М1	Ц2,3	К1,3	З3,4	Д1, Д4	5
Пз2	М1	Ц2,3	К1,3	З3,4	Д1, Д4	5

Таким чином, найбільшу загрозу ОІД несуть порушники груп Пз2 (Конкуренти), так як особи цих груп мають мотив та достатній рівень кваліфікації. Вагому загрозу можуть нести порушники групи Пв1 (Директор, системний адміністратор, адміністратор безпеки), так як у осіб даної групи є права доступу до всіх інформаційних ресурсів підприємства, але з огляду на те, що дані особи мають безпосередню зацікавленість у роботі підприємства, їх можна не розглядати як потенційну загрозу.

1.7.2 Побудова моделі загроз

Виходячи із моделі порушника та переліку шляхів реалізації загроз була побудована модель загроз інформації, яка циркулює на ОІД.

Оцінка рівнів загрози для інформації на об’єкті проводиться за двома показниками: рівень збитків та ймовірність реалізації загрози. Рівень небезпеки певної загрози буде являтись добутком цих величин.

Рівень збитків представлений у вигляді показників, які відображають збиток компанії у разі реалізації загрози. Збитком в даній ситуації будуть вважатися затрати часу на відновлення втрачених властивостей інформації.

Рівень збитків ранжується за наступними рівнями:

3-значний (12-24);

2-помірний(2-12год);

1- незначний (до 2 год).

Ймовірність реалізації загрози оцінюється числовим значенням від 0до 1 :

0-відсутність загрози;

0.1-мінімальна ймовірність реалізації загрози;

1-найвища ступінь імовірності реалізації загрози

У таблиці 1.5 показані рівні загроз інформації, сірим кольором виділені критичні показники, тобто ті, які несуть найбільші збитки та які мають найвищий рівень ймовірності реалізації.

Таблиця 1.5 - Залежність рівня небезпеки загрози від ймовірності її реалізації та рівня збитків

Рівень збитків / Ймовірність Реалізації	1-незначний	2-помірний	3-значний
0.1	0.1	0.2	0.3
0.25	0.25	0.5	**0.75**
0.5	0.5	**1**	**1.5**
0.75	**0.75**	**1.5**	**2.25**
1	**1**	**2**	**3**

Побудована модель загроз представлена у таблиці 1.6

Таблиця 1.6 - Модель загроз інформації, що циркулює на ОІД

№	Інформ. ресурс	Джерело загрози	Вразливість	Загроза	Властивості інформації,	Ймовірність реалізації	Рівень	Рівень загрози
1	2	3	4	5	6	7	8	9
1	Проєкти спеціалістів	Інформативний сигнал в колах електроживле-ння	Відсутність захисту лінії електроживлення за межами КЗ	Зйом інформації, шляхом перехвату інформативного сигналу з ліній електроживлення	К	0.25	3	0.75
		ПЕМВН	Відсутність захисту ОТЗ та ДТЗС від електромагнітних випромінювань	Зйом інформації шляхом перехвату ПЕМН	К	0.1	3	0.3
		Акустична інформація	Відсутність звукозахисного обладнання у кімнаті переговорів	Перехоплення акустичної інформації під час проведення переговорів	К	0.75	3	2.25
2	Умови контрактів, укладених із замовни-ками	Акустична інформація	Відсутність звукозахисного обладнання у кімнаті переговорів	Перехоплення акустичної інформації під час проведення переговорів	К	0.75	3	2.25
3	Бази даних клієнтів	ПЕМВН та інформативний сигнал в колах електроживлен ня	Відсутність захисту ОТЗ та ДТЗС від електромагнітних випромінювань	Зйом інформації шляхом перехвату ПЕМВН	К	0.1	3	0.3
		Інформативний сигнал в колах електрожив-лення	Відсутність фільтрації ліній електроживлення	Зйом інформації, шляхом перехвату інформативного сигналу з ліній електроживлення	К	0.25	3	0.75
4	Інформація бухгалтер-ської звітності	ПЕМВН	Відсутність захисту ОТЗ та ДТЗС від електромагнітних випромінювань	Зйом інформації шляхом перехвату ПЕМВН	К	0.1	3	0.3

1.8 Аналіз найбільш вагомих загроз інформації з обмеженим доступом, яка циркулює на ОІД

Після проведення обстеження ОІД та розробки окремої моделі загроз інформації, яка циркулює на ОІД, було виявлено, що існують канали витоку інформації, ймовірність реалізації яких достатньо висока. До таких каналів витоку інформації можна віднести:

- витік акустичної (мовної) інформації під час проведення переговорів у залі засідань;
- канал витоку інформації колами електроживлення;
- канал витоку інформації шляхом перехвату ПЕМВН.

Витік акустичної інформації під час проведення конфіденційних переговорів у залі засідань є одним із найвагоміших каналів витоку інформації. Це пов'язано з тим, що реалізація даного каналу, порівняно з іншими, не потребує значних матеріальних витрат. Крім того, витік інформації, що складає комерційну таємницю може призвести до серйозних збитків підприємства.

Витік інформації колами електроживлення є актуальним, оскільки система електроживлення має вихід за межі контрольованої зони. Це значить, що інформативні сигнали, які просочуються у лінії електроживлення можуть бути перехоплені за межами контрольованої зони.

Витік інформації шляхом перехвату ПЕМВ для даного ОІД є малоймовірним, оскільки реалізація даного каналу витоку інформації потребує значних матеріальних затрат.

1.9 Постановка задачі

Метою кваліфікаційної роботи є розробка комплексу технічного захисту інформації ТОВ «Готік». Комплекс технічного захисту інформації призначається для забезпечення захисту інформації від витоку технічними каналами, актуальність і вагомість яких ґрунтується на основі проведеного обстеження підприємства та побудованої моделі загроз.

Тому у кваліфікаційній роботі необхідно виконати наступні задачі:

1 Розробити організаційні заходи захисту ІзОД від витоку технічними каналами;

2 Розробити організаційні, первинні технічні заходи захисту акустичної (мовної) інформації;

3 Зробити обґрунтування вибору інженерно-технічних рішень та вибору технічних засобів захисту акустичної (мовної) інформації;

4 Розробити організаційні та технічні заходи захисту інформації від витоку колами електроживлення.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка існуючого стану захищеності ОІД

На етапі проведення обстеження ОІД та розробки моделі загроз ІзОД, яка циркулює на ОІД товариства з обмеженою відповідальністю «Готік», було виявлено незахищені канали витоку інформації, ймовірність реалізації яких є суттєвою.

До таких каналів витоку інформації можна віднести:

- витік акустичної (мовної) інформації, що циркулює у залі засідань;
- витік інформації колами електроживлення.

Витік акустичної (мовної) інформації може статися прямим акустичним, віброакустичним, оптикоелектричним та акустоелектричним каналами.

Прямий акустичний канал реалізується за допомогою підслуховуючих пристроїв (направлених мікрофонів, радіо стетоскопів). Зйом інформації даним каналом можливий, оскільки вікна та одна зовнішня стіна залу засідань є межею контрольованої зони, а це значить що зовнішня сторона стіни та вікна є неконтрольованими для встановлення підслуховуючих пристроїв.

Віброакустичний канал витоку інформації виникає за рахунок подовжніх коливань конструкцій обгороджувальних конструкцій і арматури системи центрального опалення. Для перехоплення акустичних коливань у цьому випадку використовуються засоби розвідки з контактними мікрофонами електронні стетоскопи, радіостетоскопи (передача інформації з радіоканалу).

Поширення віброакустичного сигналу в залі засідань можливе на поверхні вікон.

Акустоелектричний канал витоку інформації виникає за рахунок перетворень акустичних сигналів в електричні (електроакустичних перетворень) і включає перехоплення акустичних коливань через ДТЗС, що володіють "мікрофонним ефектом", а також шляхом ВЧ-нав'язування.

У залі засідань до засобів, що володіють мікрофонним ефектом, можна віднести датчики пожежної та охоронної сигналізації, телефонний апарат. Зйом

інформації даним каналом передбачає безпосереднє підключення до з'єднувальних ліній і встановлення високочутливих низькочастотних підсилювачів. Безпосереднє підключення до з'єднувальних ліній системи охоронно-пожежної сигналізації неможливе, оскільки лінії за межі КЗ не виходять. Телефонний апарат підключений до лінії телефонного звязку загального користування.

Оптико-електронний (лазерний) канал витоку акустичної інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких поверхонь, що відбивають. Для перехоплення мовної інформації з даного каналу використовуються складні лазерні акустичні локаційні системи (ЛАЛС). Даний канал витоку може бути реалізований у залі засідань оскільки у приміщенні є відображувальні поверхні (вікно, лампи денного освітлення).

Електричний канал витоку інформації виникає за рахунок наводок електромагнітних випромінювань ТЗПІ на з'єднувальні лінії ДТЗС і сторонні провідники, які виходять за межі КЗ, та просочування інформативних сигналів в кола електроживлення та заземлення.

На ОІД за межі КЗ виходить лише система електроживлення, тому для захисту інформації від витоку електричним каналом необхідно забезпечити захист лінії електроживлення.

Для захисту інформації з обмеженим доступом застосовуються організаційні, інженерні та технічні заходи та засоби захисту.

В першу чергу, необхідно регламентувати порядок та правила роботи з ІзОД. Для цього застосовуються організаційні заходи.

2.2 Основні організаційні заходи захисту

Організаційні заходи захисту інформації - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту інформації шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

Основні задачі, які повинні вирішувати організаційні заходи захисту інформації:

1) визначення відповідальної особи за ТЗІ;

2) забезпечення проведення закритих заходів у залі засідань;

3) забезпечення перевірки справності та працездатності технічних засобів і систем забезпечення ІД;

4) забезпечення перевірки справності та працездатності засобів ТЗІ;

Для вирішення даних задач на об'єкті було розроблено правила, які забезпечують безпеку інформації під час трудової діяльності працівників. Усі працівники повинні бути ознайомлені з переліком інформації, яка складає комерційну таємницю та конфіденційну інформацію, та підписати угоду про нерозголошення ІзОД, з якою вони стикаються у ході виконання службових обов'язків.

Усі працівники, які мають доступ до інформації з обмеженим доступом, повинні бути ознайомлені із правилами роботи з ІзОД та доступу на КЗ. У разі невиконання встановлених правил співробітник несе адміністративне покарання у вигляді догани, штрафу або звільнення.

2.2.1 Правила доступу на контрольовану зону

На території КЗ ТОВ «Готік» виключене перебування сторонніх осіб.

Для забезпечення режиму доступу на КЗ співробітників та відвідувачів необхідне виконання наступних правил:

1 Вхід до контрольованої зони відбувається за допомогою магнітних ключів, які видаються кожному співробітнику особисто.

2 Охоронець повинен перевірити належність ключа особі.

3 У разі відсутності ключа у співробітника, необхідно викликати старшого спеціаліста, який у журналі обліку відвідувань письмово підтверджує необхідність присутності даної особи на ОІД.

4 Після підтвердження необхідності присутності особи та встановлення особи, їй видається тимчасова перепустка.

5 Після завершення робочої зміни тимчасова перепустка здається охоронцеві та робиться відповідний запис у журналі обліку відвідувань про закінчення терміну тимчасової перепустки.

6 Для відвідувачів та осіб для працевлаштування, за умов надання документів, підтверджуючих особу, видається тимчасова перепустка, охоронець робить запис у журнал обліку відвідувань.

7 По території ОІД дані особи пересуваються у супроводі охоронця.

8 У разі надання особою перепустки або використання ключа, який їй не належить, ключ або перепустка конфіскуються.

9 За передачу ключа або перепустки іншій особі та за надання особою перепустки або ключа, що їй не належать, особа несе адміністративну відповідальність (догана, звільнення).

2.2.2 Правила роботи з ІзОД

1 При роботі працівників з ІзОД не допускається присутність у приміщенні сторонніх осіб;

2 Забороняється залишати робоче місце, не заблокувавши робочу станцію;

3 Забороняється застосування зйомних носіїв інформації для копіювання та збереження ІзОД;

4 Забороняється використання ІзОД у власних корисних цілях;

5 Співробітник повинен ставити до відома адміністратора СЗІ про факти чи спроби несанкціонованого доступу до ІзОД;

5 Забороняється підключати до робочої станції сторонні пристрої.

2.3 Розробка заходів захисту акустичної (мовної) інформації під час проведення закритих заходів

Для проведення закритих заходів на ОІД ТОВ «Готік» використовується зал засідань. Тому проводити переговори та навчання операторів із озвученням ІзОД необхідно саме в цьому приміщенні.

У залі засідань можна виділити наступні канали витоку акустичної інформації:

- прямий акустичний канал;
- віброакустичний канал;
- оптикоелектронний канал;
- акустоелектричний канал.

У залі засідань проходять наступні комунікації:

- система охоронно-пожежної сигналізації;
- система електроживлення та освітлення;
- система опалення;
- телефонна лінія.

За межі КЗ виходять системи електроживлення та телефонна лінія.

Для здійснення повної захищеності акустичної інформації при проведенні закритих заходів в залі засідань, необхідне застосування в комплексі ряду запропонованих організаційних, інженерних та технічних рішень.

Для виключення можливості витоку акустичної інформації телефонними лініями зв'язку необхідно демонтувати телефонний апарат, так його наявність у приміщенні не несе істотної службової необхідності. Тому телефонний апарат і прокладену до нього лінію телефонної мережі рекомендовано демонтувати, адже встановлення додаткових технічних засобів захисту спричинить додаткові нецілеспрямовані матеріальні затрати.

2.3.1 Оцінка рівня звукоізоляції огороджувальних конструкцій залу засідань

Огороджувальні конструкції залу засідань складаються із стін в півтори цеглини, однокамерного вікна із металопластикової конструкції розміром 15х2 м, двері із ДСП-профілю, товщиною 45 мм.

Оцінка рівня загасання стін залу засідань

Маса 1 квадратного метра огороджувальної стіни– 556 кг.

Середня гучність звуку людини в службовому приміщенні складає близько 50 ... 60 дБ.

Для розрахунку звукоізоляційних властивостей стін приміщення було використано формулу 2.1 [4]:

$$K_{or} = 20\log(q_{or}f) - 47.5 \text{ дБ}, \quad (2.1)$$

де q_{or} – маса 1 м^2 огородження, кг;

f – частота звуку, Гц.

В таблиці 2.1 наведені звукоізолюючі властивості стін на частотах 100…4000 Гц, розраховані за формулою 2.1 .

Таблиця 2.1 – Рівні звукоізоляції, що забезпечуються стінами залу засідань залі засідань

Частота, Гц	Звукоізоляція, дБ
500	62
1000	68
2000	74
4000	80

Із таблиці 2.1 видно, що витік акустичного сигналу через стіни конструкції є неможливим, оскільки стіна забезпечує необхідне затухання звукового сигналу в частотному діапазоні людської мови.

Затухання звукового сигналу, яке забезпечують вхідні двері хідні наведено у таблиці 2.2 [5].

Таблиця 2.2 – Звукоізолюючі властивості дверей, які знаходяться на вході у зал засідань

Частота, Гц	Звукоізоляція, дБ
500	30
1000	31
2000	28
4000	29

Із таблиці 2.2 видно, що двері, які встановлені на вході в зал засідань не забезпечують відповідного рівня звукоізоляції і їх необхідно замінити.

Вікно у залі засідань є також можливим джерелом загрози витоку акустичної(мовної) інформації під час проведення закритих заходів.

У таблиці 2.3 наведені рівні затухання звукового сигналу, які забезпечує вікно.

Таблиця 2.3 – Звукоізолюючі характеристики вікна

Частота, Гц	Звукоізоляція, дБ
500	37
1000	40
2000	42
4000	44

Як видно із таблиці, вікна також є елементом середовища поширення потенційних каналів витоку інформації.

Звукоізолюючі властивості вікон підвищуються за рахунок встановлення двокамерного склопакета.

2.3.2 Розробка інженерно-технічних заходів захисту акустичної (мовної) інформації у залі засідань

Для захисту мовної інформації застосовується комплекс активних і пасивних засобів:

1 Енергетичне приховування інформації шляхом:

- звукоізоляції акустичного сигналу;
- звукопоглинання акустичної хвилі;
- глушіння акустичних сигналів;
- зашумлення приміщення або твердого середовища розповсюдження іншими широкосмуговими звуками, які забезпечують маскування акустичних сигналів.

Витік інформаційного акустичного сигналу може здійснюватися за рахунок повітряної акустичної хвилі. У цьому випадку в якості технічного засобу перехоплення може служити людське вухо, мікрофон, спрямований мікрофон.

Для захисту інформації від витоку прямим акустичним каналом було обрано пасивний метод, а саме звукоізоляцію.

Основна вимога до звукоізоляції приміщень полягає в тому, щоб за його межами співвідношення акустичний сигнал/шум не перевищувало деякого допустимого значення, що виключає виділення мовного сигналу на тлі природних

шумів засобом розвідки. Тому до приміщень, в яких проводяться закриті заходи, пред'являються певні вимоги до звукоізоляції.

Зал засідань віднесено до 4 категорії приміщень. Для даної категорії норм по звукоізоляції не встановлено, тому за нормовані значення прийнято значення для приміщення 3 категорії.

Необхідний мінімальний рівень затухання звукового сигналу для даної категорії приміщення наведено у таблиці 2.4[3].

Таблиця 2.4 – Мінімальний необхідний рівень затухання для залу засідань

Частота, Гц	Рівень затухання, дБ
500	43
1000	46
2000	46
4000	45

Для підвищення звукоізоляції приміщення необхідне встановлення дверей з більшим рівнем звукоізоляції.

Порівняльна характеристика дверей від різних виробників представлена у таблиці 2.5.

Таблиця 2.5 – Порівняльна характеристика дверей

№ п/п	Виробник	Звукоізоляція, дБ	Ціна, грн.
1	Звукоізоляційні двері HS75-1, Hormann	50-53	50000
2	Porta-двері	42	25000
3	Бастіон	40	17000
4	СКМ EI 30 RW	42	18500

Для встановлення було обрано двері марки СКМ EI 30 RW 42 db, дверне полотно якого заповнене комбінованим ДСП, тобто листів ДСП, які мають різну щільність. Вибір обґрунтований тим, що двері забезпечують необхідний рівень звукоізоляції в поєднанні із порівняно невисокою ціною.

Підвищення звукоізоляції дверей проводиться шляхом застосування додаткових ущільнюючих прокладок по периметру притвору дверей.

Схематичне зображення установки ущільнюючих прокладок на двері зображено на рисунку 2.1

Отже, для захисту інформації у залі засідань доцільно застосовувати спеціально розроблені звукоізолюючі двері. Для встановлення обрано двері марки СКМ, модель EI 30 RW 42 db.

Рисунок 2.1 – Розташування ущільнюючих прокладок на дверях

Для захисту акустичної(мовної) інформації також необхідна заміна вікна у залі засідань, адже вікно може послужити джерелом витоку акустичної(мовної) інформації під час проведення закритих заходів у залі засідань.

Порівняльна характеристика вікон від різних виробників представлена у таблиці 2.6

Таблиця 2.6 – Порівняльна характеристика вікон

№	Виробник	Кількість камер	Звукоізоляція, дБ
1	KBE – Еталон	2	42
2	BRUGMANN AD	1	40
3	Rehau 86plus	2	46
4	Winbau	2	46

У приміщенні обрано для встановлення двокамерні склопакети за формою(товщина перегородок і відстань між ними) марки Rehau 86plus 4-12-4-8-4. Вибір обґрунтований достатнім рівнем звукоізоляції та порівняно невисокою ціною.

Такі вікна забезпечують ослаблення звукового сигналу на 46 дБ. На рисунку 2.2 наведено схематичне зображення двокамерного склопакету, обраного для встановлення в залі засідань.

Рисунок 2.2 - Двокамерний склопакет

Таким чином, для захисту від витоку інформації прямим акустичним каналом було запропоновано для встановлення:

- двокамерний склопакет на вікно;
- звукоізольовані двері;
- ущільнюючі прокладки на двері.

2.3.3 Обґрунтування вибору технічних засобів захисту акустичної (мовної) інформації у залі засідань

Мова являє собою модульовані по амплітуді і частоті акустичні коливання, основна енергія яких укладена в діапазоні частот 70 Гц - 7 кГц, а більше 95% смислової інформації передається в діапазоні 200 Гц - 5 кГц.

Акустичні коливання, впливаючи на огороджувальні конструкції приміщення, в основному відбиваються від них. Однак часткові взаємодії звукових хвиль з конструкціями викликають коливання останніх, що поширюються далі у вигляді вібрацій. Внаслідок пружних властивостей будівельних матеріалів вібрації, викликані акустичними сигналами, можуть прийматися на значній відстані від місця виникнення.

Ефективність систем і пристроїв віброакустичного зашумлення визначається властивостями застосовуваних електроакустичних перетворювачів (вібродатчиків), трансформують електричні коливання в пружні коливання (вібрації) твердих середовищ. Якість перетворення залежить від реалізованого фізичного принципу, конструктивно-технологічного рішення та умов погодження вібродатчика з середовищем.

Таким чином, можна зробити висновок, що поява віброакустичного каналу витоку ІзОД відбувається завдяки вібраційним коливанням, спричиненим акустичним полем мови, що розповсюджуються будівельними конструкціями та жорсткими інженерними комунікаціями, елементи яких виходять за межі КЗ, шибок віконних отворів у залі засідань, дверей та труб системи опалення.

Приймання таких коливань може здійснюватися шляхом застосування портативних засобів акустичної розвідки (стетоскопів), в тому числі із записом

інформативних сигналів на магнітні носії. Ці засоби ТР можуть бути приховано встановлені на труби системи опалення, які виходять за межі КЗ.

Оптикоелектронний канал витоку ІзОД утворюється за рахунок дистанційного перехоплення вібраційних коливань відбиваючих поверхонь, що виникають під впливом акустичного поля мови.

Ймовірними місцями витоку інформації у залі засідань є поверхні дверей, труби системи опалення, поверхні вікон та відбиваючі поверхні.

Для захисту інформації від витоку віброакустичним та оптико-електронним каналом запропоновано застосувати активний метод захисту.

Система активного захисту реалізована на базі генератора «білого шуму» і дозволяє виключити просочування мовної інформації з приміщень по віброакустичному і оптикоелектронному каналах через елементи будівельних конструкцій (стіни, стеля) , поверхні вікон та інші.

У таблиці 2.7 наведені експлуатаційно-технічні параметри сучасних генераторів віброакустичного зашумлення.

Таблиця 2.7 - Технічні характеристики генераторів віброакустичного зашумлення

Параметр	**Прилад віброаку-стичного захисту інформації "ОЦЗІ-ВА"**	**Генератор шумових сигналів МАРС-ТЗО-4-2**	**Генератор шуму акустичний "Топаз ГША-4"**	**Генератор шуму „DNG-2300”**
Кількість каналів	2	2	2	3 (1-акустичні, 2 -вібровипр.)
К-сть вібро-випромінюва-чів на 1 канал, шт	До 25	До 20	До 16	Для стін – 12 Для вікон-18
Робочий діапазон частот, Гц	117-5600	180-5600	170-5700	250—5000
Потужність споживання	Не більше 75 ВА	Не більше 40ВА		
Габаритні розміри, мм	140x230x85	225x142x48	180x160x70	60×175×254

Генератори віброакустичного зашумлення використовуються в комплекті із акустичними та вібраційними випромінювачами.

В таблиці 2.8 наведені характеристики вібраційних випромінювачів.

Таблиця 2.8 – Основні технічні характеристики вібраційних випромінювачів

Параметр	**ВИ-3**	**ВИ-4**	**Топаз ВВ-1**
Робочий діапазон частот, Гц	180-5600	180-5600	170-5700
Потужність розсіювання, ВА	1	2	2
Розміри ,мм	∅47.5х20	∅60х22	∅42х20
Можливе місце встановлення	Для вікна	Стіни, стеля, система опалення	Всі поверхні кімнати

Для встановлення у залі засідань було обрано систему віброакустичного захисту у складі генератора Топаз ГША-4 та вібровипромінювачів Топаз ВВ-1. Вибір обґрунтований тим, що технічні характеристики задовольняють вимогам для даного об'єкту, а саме порівняно невелика потужність споживання, необхідний діапазон частот .

Також вартість даної системи задовольняє ціновій політиці організації. Генератор та вібровипромінювачі наявні у переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України.

Кількість вібровипромінювачів: 2-на вікно, 1-на вхідні двері у зал засідань, 1- на батарею системи опалення.

Для захисту акустичної (мовної) інформації також рекомендовано встановити пригнічувач мобільних телефонів у залі засідань. Порівняльна характеристика деяких пригнічувачів наведена у таблиці 2.9.

Таблиця 2.9-Основні технічні характеристики пригнічувач мобільних телефонів

Параметр	**Стаціонарний пригнічувач мобільних телефонів «Алігатор Super-60»**	**Deception - пригнічувач мобільних сигналів**	**Пригнічувач Cellbuster GSM,3G,DCS,CDMA**
Радіус дії, м	до 60	до 40	до 10
Стандарти зв'язку, на які впливає	WCDMA-2000, SCDMA-2100, GSM-900 та GSM-1800, PHS-1900,	GSM, 3G, CDMA, DCS	GSM, 3G, CDMA, DCS
Ціна, грн	6700	5400	1075

Для встановлення у залі засідань було обрано пригнічувач Cellbuster, оскільки дальність його дії задовольняє розмірам кімнати, також він має невисоку вартість.

Встановлення технічних засобів захисту акустичної (мовної) інформації проводиться згідно схеми, яка наведена у Додатку.

2.3.4 Розробка організаційних заходів захисту акустичної (мовної) інформації у залі засідань

Розробка організаційних заходів захисту інформації від витоку акустичним каналом під час проведення закритих заходів, нарад та інших заходів передбачає розроблення правил проведення переговорів у залі засідань та застосуванню системи активного захисту інформації.

З метою запобігання знімання інформації за допомогою закладних пристроїв необхідно проводити планові обстеження залу засідань на наявність закладних пристроїв за допомогою спеціалізованих пошукових пристроїв.

Для захисту акустичної (мовної) інформації у залі засідань в якості організаційного заходу захисту були розроблені правила проведення переговорів та закритих заходів у залі засідань.

Правила проведення закритих заходів у залі засідань

1 Перед проведенням заходу необхідно провести візуальний огляд приміщення на предмет виявлення закладних пристроїв. Огляд повинен проводитися співробітником СЗІ.

1 Перед проведенням переговорів щільно закриваються вікна та штори для запобігання знімання інформації шляхом прямого акустичного та оптико-електронного каналів.

2 Перевірити справність апаратури системи віброакустичного захисту.

3 Увімкнути в мережу електроживлення генератор "Топаз ГША-4" та переключити вимикач «Мережа» в активний режим, увімкнути пригнічувач мобільних телефонів.

4 Кількість осіб, що задіяна у переговорах повинна бути обмежена до мінімуму.

5 Протягом всього часу, який триває закритий захід, біля дверей кімнати повинен чергувати охоронець, який здійснює контроль за дверима і коридором біля входу в зал засідань, а також стежити за тим, щоб ніхто зі сторонніх осіб не проник всередину.

6 По завершенні закритого заходу співробітник СЗІ вимикає пригнічувач мобільних телефонів та генератор та від'єднує їх від мережі електроживлення.

7 Після вимкнення апаратури кімната повинна ретельно оглядатися, закриватися і опечатуватися.

8 Ключі від залу засідань повинні бути передані черговій зміні охорони під розписку і зберігатися в кімнаті охорони, доступ до якої регламентується керівництвом.

Виконання цих правил дозволить мінімізувати ризик встановлення ЗП та витік ІзОД акустичними каналами витоку інформації.

2.4 Розробка заходів захисту інформації від витоку колами електроживлення

Кола електроживлення є одним з основних електричних каналів витоку інформації із засобів обчислювальної техніки, призначених для обробки інформації з обмеженим доступом.

Трансформаторна підстанція, від якої відбувається електроживлення технічних засобів на ОІД, розташована за межами контрольованої зони . Для захисту кіл електроживлення повинні використовуватися технічні засоби, що забезпечують фільтрацію небезпечних сигналів, або системи активного лінійного зашумлення.

Електричні канали витоку інформації включають:

- зйом наведень ПЕМВ ТЗПІ з сполучних ліній ДТЗС і сторонніх провідників;

- зйом інформаційних сигналів з ліній електроживлення ТЗПІ;

- зйом інформації шляхом установки в ТЗПІ електронних пристроїв перехоплення інформації.

Для захисту інформації від витоку колами електроживлення використовують наступні методи:

-пасивні (фільтрація, встановлення роздільних трансформаторів;)

-активні (встановлення генераторів лінійного зашумлення).

Фільтрація

Фільтрація небезпечних сигналів здійснюється з метою запобігання розповсюдження високочастотних інформаційних сигналів за межі контрольованої зони.

Для фільтрації сигналів в ланцюгах електроживлення використовують протизавадні фільтри. В даний час існує велика кількість різних типів протизавадних фільтрів, що забезпечують ослаблення небажаних сигналів в різних ділянках частотного діапазону.

Для виключення проникнення інформаційних сигналів у колі електроживлення використовуються фільтри нижніх частот, які пропускають

сигнали з частотами нижче граничної частоти ($f \leq fгр$) і пригнічують - з частотами вище граничної частоти.

Фільтри, які встановлюються в ланцюзі живлення окремих технічних засобів безпосередньо в приміщеннях, де проводиться обробка інформації, що захищається, або ж поруч з цими приміщеннями, класифікуються як «фільтри для локальних ланцюгів». Вони розраховані на електроживлення одного або ряду технічних засобів і забезпечують придушення інформативних сигналів у фазному, нульовому і заземлювальному проводах однофазної мережі.

Інша група фільтрів, що класифікується як «об'єктові фільтри», встановлюється в ланцюзі електроживлення групи технічних засобів або об'єкта в цілому і забезпечує придушення інформативних сигналів в кабелях живлення трифазної мережі. Залежно від числа фільтрованих ліній фільтри можуть бути двопровідними, трипровідними і чотирипровідними.

Вибір фільтра визначається величиною робочої напруги, номінального робочого струму кола, в яке він включається, і необхідної величиною внесеного загасання в смузі частот придушення з урахуванням рівнів спектральних складових інформативного сигналу.

Зашумлення

Для захисту кіл електроживлення також використовуються системи лінійного зашумлення.

У загальному випадку система лінійного зашумлення являє собою генератор шуму, що формує маскуючу напругу з заданими спектральними, часовими і енергетичними характеристиками, який підключається до лінії.

До системи лінійного зашумлення, застосовуваної для створення маскуючих електромагнітних перешкод у ланцюгах електроживлення, висуваються такі вимоги:

- система повинна створювати електромагнітні завади в діапазоні частот можливих наведень побічних електромагнітних випромінювань (150 кГц- 300 МГц);

- створювані завади не повинні мати регулярної структури (ентропійний коефіцієнт якості шуму повинен бути не менше 0,6).

У системах лінійного зашумлення в основному використовуються завади типу «білого шуму» з рівномірно розподіленим енергетичним спектром у всьому робочому діапазоні частот.

Генератори шуму виконуються у вигляді окремого блоку з живленням від мережі 220 В.

Для забезпечення захисту інформації від витоку колами електроживлення на ОІД було обрано для використання пасивний метод, а саме фільтрацію.

Даний вибір обґрунтований наступними чинниками:

- фільтрація у даному випадку є більш доцільною, оскільки система захисту повинна працювати цілодобово;
- фільтр не потребує окремого джерела живлення, так як він встановлюється в розрив кабелю.

Споживана потужність усіх приладів на об'єкті становить 16-17 кВт. Це значить, що номінальний струм фільтра повинен бути не менше 60 А.

У таблиці 2.10 наведені деякі з варіантів фільтрів типу ФП, які можуть бути застосовані.

Таблиця 2.10 – Технічні характеристики деяких мережевих протизавадних фільтрів

Параметр	**ФП-15**	**ФП-15Ма**	**ФП-14**
Кількість проводів	4	4	2
Номінальний струм, А	70	200	40
Номінальна напруга, В: -при постійному токові -при перемінному токові 50 Гц -при перемінному токові 400 Гц	 500 220 110	 500 220 115	 1000 500 220
Маса, кг	20	26	10
Різьба патрубка, дюйм	1,5	1,5	1

З наведених у таблиці варіантів встановлення обрано фільтр мережевий протизавадний ФП-15. Даний фільтр забезпечує загасання (R=50 Ом):

- на частотах 20-150 КГц не менше 30 дБ;

- на частотах 0,15-1000 МГц не менше 100 дБ.

На рисунку 2.3 Зображений фільтр ФП-15.

Рисунок 2.3 - Фільтр ФП-15

Фільтр ФП-15 рекомендовано встановити на вході лінії електроживлення до електричної щитової, що відфільтрувати інформативні сигнали в полосі частот від 20 кГЦ до 1ГГц.

2.5 Висновок

Таким чином, у даному розділі було розроблено комплекс технічного захисту інформації на ОІД ТОВ «Готік» , який включає в себе організаційні, інженерно-технічні та технічні заходи захисту.

Організаційні заходи захисту включають в себе

- правила доступу на КЗ;
- правила роботи з ІзОД;
- правила проведення закритих заходів у залі засідань.

У якості інженерно-технічних рішень було запропоновано:

а) для запобігання витоку акустичної мовної інформації у залі засідань:

- демонтування телефонної лінії та телефонного апарата;
- заміну вікон і дверей на ті, що мають більш високий рівень звукоізоляції;

- встановлення системи віброакустичного захисту акустичної(мовної) інформації та пригнічувача мобільних телефонів.

б) для захисту ліній електроживлення від витоку інформації встановлення мережевого протизавадного фільтра на вході лінії електроживлення до електричної щитової.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Обґрунтування витрат на реалізацію комплексу технічного захисту інформації

Метою даного розділу є визначення витрат на розробку комплексу технічного захисту інформації ТОВ «Готік».

У даному розділі у грошовому вираженні доводиться необхідність створення КТЗІ, як необхідної міри боротьби проти витоку інформації.

Для визначення витрат на розробку комплексу та економічної доцільності даного комплексу необхідно провести наступні розрахунки:

1) Розрахунок капітальних витрат на проєктування та впровадження комплексу технічного захисту інформації;

2) Розрахунок річних експлуатаційних витрат на функціонування комплексу технічного захисту інформації;

3) Розрахунок капітальних витрати при втраті інформації, за відсутності даного комплексу (розрахунок збитків).

3.2 Розрахунок капітальних витрат

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

Для розрахунку капітальних витрат на проєктування та впровадження комплексу технічного захисту інформації використаємо формулу:

$$K = K_{áóä} + K_{iá} + K_{àï},$$

де $К_{буд}$ – вартість будівельних робіт і матеріалів;

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

$К_{вс}$ – витрати на встановлення обладнання, грн.

3.2.1 Будівельні роботи

Витрати на будівельні роботи, як інженерні рішення, призначені для розробки комплексу технічного захисту інформації представлені в таблиці 3.1.

Таблиця 3.1 – Будівельні роботи

№	Будівельна робота та матеріали	Вартість, грн
1	Вікно двокамерне	14200
2	Двері звукоізольовані	18500
3	Демонтаж дверей	3000
4	Демонтаж вікна	3000
5	Встановлення дверей	3000
6	Встановлення вікна	3000
8	Додаткові витрати (матеріали)	7500
ВСЬОГО		52200

3.2.2 Апаратна частина витрат

Витрати на обладнання, призначеного для розробки комплексу технічного захисту інформації представлені в таблиці 3.2.

Таблиця 3.2 – Вартість обладнання

Назва	Ціна, за одиницю, грн.	Кількість, од.	Загальна ціна, грн.
Генератор шуму "Топаз ГША-4"	25925	1	25925
Вібровипромінювач Топаз ВВ-1	1000	13	13000
Фільтр протизавадний	5400	1	5400
Загальна вартість, грн.			44325

Отже витрати на обладнання, призначеного для розробки комплексу технічного захисту інформації становлять 44325 грн.

Монтажні роботи на встановлення усієї системи складають 27% від загальних витрат на обладнання, що дорівнює 11967,75 грн, а також витрати на налагодження складають 10% від загальних витрат на обладнання, що дорівнює 4432,5 грн.

Тобто, загальна сума апаратної частина витрат складатиме 60725,25 грн.

Таким чином, капітальні витрати на проєктування комплексу технічного захисту інформації:

$$К = 52200 + 60725,25 = 112925,25 \text{ грн.}$$

3.3 Розрахунок експлуатаційних витрат

Річні експлуатаційні витрати на комплекс технічного захисту інформації визначаються за формулою:

$$C = C_r + C_e + C_a$$

де C_r – вартість поточних ремонтних робіт, грн.;

C_e – вартість електроенергії, що споживається апаратурою комплексу технічного захисту інформації протягом року, грн;

C_a - річний фонд амортизаційних відрахувань, грн.

Витрати на поточний ремонт становлять 10% від капітальних витрат на обладнання.

$$C_r = 11292,53 \text{ грн.}$$

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів.

Річний фонд амортизаційних відрахувань:

$$C_a = Ф_{пер} * Н_a / 100$$

Річний фонд амортизаційних відрахувань для будівельних робіт:

$$C_a = 52200 * 0,05 / 100 = 26,1 \text{ грн.}$$

Річний фонд амортизаційних відрахувань для апаратної частини:

$$C_a = 44325 * 0.2 / 100 = 88,65 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою комплексу технічного захисту інформації протягом року, визначається за формулою:

$$C_{ел} = P \times F_p \times Ц_e$$

де Р – встановлена потужність апаратури комплексу технічного захисту інформації, кВт;

$F_р$ – річний фонд робочого часу комплексу технічного захисту інформації, годин;

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

Вартість електроенергії, що споживається апаратурою комплексу технічного захисту інформації протягом року:

$$С_е = 0,235 \text{ x } 8760 \text{ x } 6 = 12351,6 \text{ грн.}$$

Річні експлуатаційні витрати на функціонування комплексу технічного захисту інформації:

$$С = 11292,53 + 26,1 + 88,65 + 12351,6 = 23758,88 \text{ грн.}$$

3.4 Оцінка величини збитку

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Місячний фонд робочого часу складає 176 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 3 год.

$$Пп = (Зс/Fр) * tп = (350000/176) * 3 = 5965,91 \text{ грн.},$$

де Зс – сумарна заробітна плата персоналу, 350000 грн.

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн.;

Ппв – витрати на відновлення системи, грн.;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу тви = 3 год.:

$$Пви = (100000/176) * 3 = 1704,55 \text{ грн.}$$

Витрати на відновлення системи визначаються часом відновлення після атаки тв = 3 год. і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = 250 * 3 = 750 \text{ грн.}$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 1704,55 + 750 + 0 = 2454,55 \text{ грн.},$$

де Пзч = 0 грн. - вартість для витрат на заміну частин.

О = 5000000 грн. - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = O/Fp * (tп + tв + tви) = 5000000/1920 * (3 + 3 + 3) = 23437,5 \text{ грн.}$$

Fp – це річний фонд часу роботи офісу, 1920 годин;

tп – 3 годин простою після атаки;

тв – 3 годин відновлення після атаки;

тви – 3 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на інформаційну систему при реалізації загрози складе:

$$U = Пп + Пв + V = 5965,91 + 2454,55 + 23437,5 = 31857,96 \text{ грн.}$$

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

$$B = \sum i \sum n * U = 8 * 2 * 31857,96 = 509727,36 \text{ грн.},$$

де: i- число атакованих вузлів, 8 комп'ютерів;

n – середнє число атак на рік, 2 рази.

3.6 Загальний ефект від впровадження комплексу технічного захисту інформації

Загальний ефект від впровадження комплексу технічного захисту інформації визначається з урахуванням B – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; C – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R – C = 509727,36 * 0,25 – 23758,88 = 103672,96 \text{ грн.}$$

3.7 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності комплексу технічного захисту інформації, розглянутого у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій To.

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

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

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

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

$$ROSI = E/K = 103672,96 \ / \ 112925,25 = 0,91$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/ROSI = 1/0,91 = 1,1 \text{ року} = 13 \text{ місяців}.$$

3.8 Висновок

У цьому розділі обґрунтована економічна доцільність впровадження комплексу технічного захисту інформації. Для обґрунтування доцільності були визначені наступні фактори:

– загальні витрати на впровадження комплексу технічного захисту інформації на підприємстві;

– передбачувані збитки за умови успішної інформаційної атаки на підприємство.

За отриманими результатами можна зробити висновок, що при атаці загальна сума збитків буде складати 509727,36 грн. При цьому поточні експлуатаційні витрати складають 23758,88 грн, а капітальні інвестиції - 112925,25 грн., що за підрахунком окупиться за 13 місяців.

Відповідно до розрахунків, виконаних в даному розділі, запропонований комплекс технічного захисту інформації є економічно вигідним.

ВИСНОВКИ

В даній кваліфікаційній роботі був розроблений комплекс технічного захисту інформації ТОВ «Готік».

У результаті проведення обстеження на ОІД та побудови моделі загроз було виявлено найбільш небезпечні канали витоку інформації, що циркулює на ОІД. Проведено аналіз стану захищеності ОІД ТОВ «Готік» та розроблено заходи захисту інформації від витоку технічними каналами. Розроблені інженерні, технічні та організаційні заходи захисту, які складають комплекс технічного захисту інформації для об'єкту інформаційної діяльності ТОВ «Готік».

В економічному розділі була розрахована економічна доцільність впровадження комплексу технічного захисту інформації, яка циркулює на ОІД ТОВ «Готік». Порівнявши збитки від реалізації можливих загроз підприємству з витратами на впровадження комплексу технічного захисту інформації, можна зробити висновок, що затрати на дане впровадження виправданими у порівнянні зі збитками від витоку інформації.

Таким чином, розроблений комплекс технічного захисту інформації для ОІД ТОВ «Готік» дозволить забезпечити захист інформації з обмеженим доступом від її витоку технічними каналами.

ПЕРЕЛІК ПОСИЛАНЬ

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

2 Закон України «Про інформацію».

3 Закон України «Про телекомунікації».

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

5 НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

6 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

7 Захист інформації в інформаційних системах [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/13670622/informatika/zahist_informatsiyi_informatsiynih_sistemah. Назва з екрана.

8 НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

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

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

11 «Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України» / Спосіб доступу: URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=78319&cat_id=39181 – Назва з екрана.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1	20	
6	А4	Розділ 2	20	
7	А4	Розділ 3	7	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	2	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	
15	А4	Додаток Д	4	
16	А4	Додаток Е	1	
17	А4	Додаток Є	1	
18	А4	Додаток Ж	1	
19	А4	Додаток З	4	
20	А4	Додаток И	1	
21	А4	Додаток І	2	

ДОДАТОК Б. Перелік документів на оптичному носії.

1. Презентація_Лєвін.ppt
2. Кваліфікаційна робота_ Лєвін.doc

ДОДАТОК В. Наказ про створення служби захисту інформації

ТОВ «Готік»

02 січня 2024 р.

м. Дніпро

Наказ №120

про створення служби захисту інформації (СЗІ)

З метою забезпечення захисту інформації з обмеженим доступом, яка циркулює на ОІД від витоку технічними каналами

НАКАЗУЮ:

1 Створити в ТОВ «Готік» службу захисту інформації.

2 Передбачити в штатному розкладі посади:

- адміністратора СЗІ - 1 чол.;
- спеціаліст із безпеки інформації- 2 чол.

3 Покласти наступні обов'язки на службу захисту інформації:

- визначення переліків відомостей, які підлягають захисту в процесі обробки, класифікація інформації за вимогами до її конфіденційності або важливості для організації;

- розробка моделі загроз і моделі порушника інформації, яка циркулює на ОІД;

- визначення і формування вимог до КТЗІ;

- організація і координація робіт з проєктування та розробки КТЗІ, безпосередня участь у проєктних роботах з створення КТЗІ;

- підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами під час створення КТЗІ;

- вибір організацій-виконавців робіт з створення КТЗІ, здійснення контролю за дотриманням порядку проведення робіт з захисту інформації, у взаємодії з службою охорони організації, погодження основних технічних і розпорядчих документів, що супроводжують процес створення КТЗІ;

- розробка нормативних документів щодо технічного захисту інформації на

ОІД.

4 Призначити на посаду:

адміністратора СЗІ - Прокопенко В.І.;

спеціалістів із безпеки інформації - Пінчук А.Д та Шаповал В.В.

Директор _____ Коваленко О.О.

(підпис)

ДОДАТОК Г. Наказ про створення комісії по категоріюванню та обстеженню ОІД

ТОВ «Готік»

03 січня 2024 р.

м. Дніпро

Наказ №120

про створення комісії по категоріюванню та обстеженню ОІД

З метою розробки окремої моделі загроз інформації, яка циркулює на ОІД та проведення робіт з ТЗІ

Наказую:

1 Для проведення категоріювання приміщень та обстеження ОІД ТОВ «Готік» створити комісію у складі:

Голови комісії: Прокопенко С.С.

Членів комісії: Антоненко В.О, Кірлаш О.Д.,

2 У відповідності з документом НД ТЗІ 1.6-005-2013 “Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці” здійснити категоріювання приміщень, де обробляється ІзОД та надати на затвердження акти категоріювання.

3 Згідно з вимогами документу НД ТЗІ 3.1-001-07 “Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроєктні роботи” провести обстеження ОІД та надати на затвердження “Акт обстеження ”.

Термін виконання з 26 січня по 02 лютого 2024р.

Директор _____ Коваленко О.О.

(підпис)

ДОДАТОК Ґ. Наказ про встановлення контрольованої зони

ТОВ «Готік»

04 січня 2024 р.

м. Дніпро

Наказ №124

«про встановлення контрольованої зони в межах приміщення, у якому розташований ОІД та внутрішнього двору»

Причиною для створення цього документу послужило те, що комплекс ТЗІ для даного ОІД розробляється і впроваджується вперше. Цей документ є необхідним для створення КТЗІ на ОІД.

Цей наказ розробляється виходячи з актів №2-5 «категоріювання приміщень ОІД», та акту №1 «Обстеження ОІД».

Межі контрольваної зони вказані у ситуаційному плані.

НАКАЗУЮ:

1 Встановити контрольовану території в межах приміщення, у якому розташований ОІД та суміжного з ним внутрішнього двору.

2 Відповідальним за створення контрольованої території призначити адміністратора СЗІ Іванова П. П.

Директор Коваленко О.О.

_____(підпис)

Наказ довести адміністратору СЗІ Прокопенко В.І.

ДОДАТОК Д. Акти категоріювання приміщень

ЗАТВЕРДЖУЮ

Директор ТОВ «Готік»

Коваленко О.О.

05 січня 2024 р.

АКТ №1

категоріювання приміщення № 3 (зал засідань)

1. Підстава для категоріювання – наказ про створення КТЗІ від 02 січня 2024 р.;

2.Вид категоріювання – первинне;

3. На ОІД здійснюється озвучування інформації під час проведення переговорів.

4. Ступінь обмеження доступу до інформації, що озвучується на об'єкті – комерційна таємниця;

5. Для приміщення № 3 (зал засідань) встановлена IV категорія

Голова комісії _____ Прокопенко С.С.

Члени комісії: _____ Антоненко О.Д.,

_____ Кірлаш О.Ю

ЗАТВЕРДЖУЮ

Директор ТОВ «Готік»

Коваленко О.О.

03 вересня 2012 р.

АКТ №2

категоріювання приміщення № 1 (кабінет директора)

1 Підстава для категоріювання – наказ про створення створення КТЗІ від 02 січня 2024 р.;

2 Вид категоріювання – первинне;

3 На ОІД здійснюється обробка інформації технічними засобами.

4 Ступінь обмеження доступу до інформації, що обробляється на об'єкті – комерційна таємниця;

5 Для приміщення №1 (кабінет директора) встановлена IV категорія .

Голова комісії _____ Прокопенко С.С.

Члени комісії: _____ Антоненко О.Д.,

_____ Кірлаш О.Ю

ЗАТВЕРДЖУЮ

Директор ТОВ «Готік»

Коваленко О.О.

03 січня 2024 р.

АКТ №3

категоріювання приміщення № 6 (серверна)

1 Підстава для категоріювання – наказ про створення КТЗІ від 02 січня 2024 р.;

2 Вид категоріювання – первинне;

3 На ОІД здійснюється обробка інформації технічними засобами;

4 Ступінь обмеження доступу до інформації, що обробляється на об’єкті – комерційна таємниця;

5 Для приміщення № 6 (серверна) встановлена IV категорія .

Голова комісії _____ Прокопенко С.С.

Члени комісії: _____ Антоненко О.Д.,

_____ Кірлаш О.Ю

ЗАТВЕРДЖУЮ

Директор ТОВ «Готік»

Коваленко О.О.

03 січня 2024 р.

АКТ №4

категоріювання приміщення № 12 (приміщення старших спеціалістів)

1 Підстава для категоріювання – наказ про створення КТЗІ від 02 січня 2024 р.;

2 Вид категоріювання – первинне;

3 На ОІД здійснюється обробка інформації технічними засобами;

4 Ступінь обмеження доступу до інформації, що обробляється на об’єкті – комерційна таємниця;

5 Для приміщення № 12 (приміщення старших спеціалістів)встановлена IV категорія .

Голова комісії _____ Прокопенко С.С.

Члени комісії: _____ Антоненко О.Д.,

_____ Кірлаш О.Ю

ДОДАТОК Е. Наказ про встановлення контрольованої зони

ТОВ «Готік»

04 січня 2024 р.

м. Дніпро

Наказ №124

«про встановлення контрольованої зони в межах приміщення, у якому розташований ОІД та внутрішнього двору»

Причиною для створення цього документу послужило те, що комплекс ТЗІ для даного ОІД розробляється і впроваджується вперше. Цей документ є необхідним для створення КТЗІ на ОІД.

Цей наказ розробляється виходячи з актів №2-5 «категоріювання приміщень ОІД», від 3.01.24, та акту №1 «Обстеження ОІД» від 3.01.24.

Межі контрольваної зони вказані у ситуаційному плані

НАКАЗУЮ:

1 Встановити контрольовану території в межах приміщення, у якому розташований ОІД та суміжного з ним внутрішнього двору.

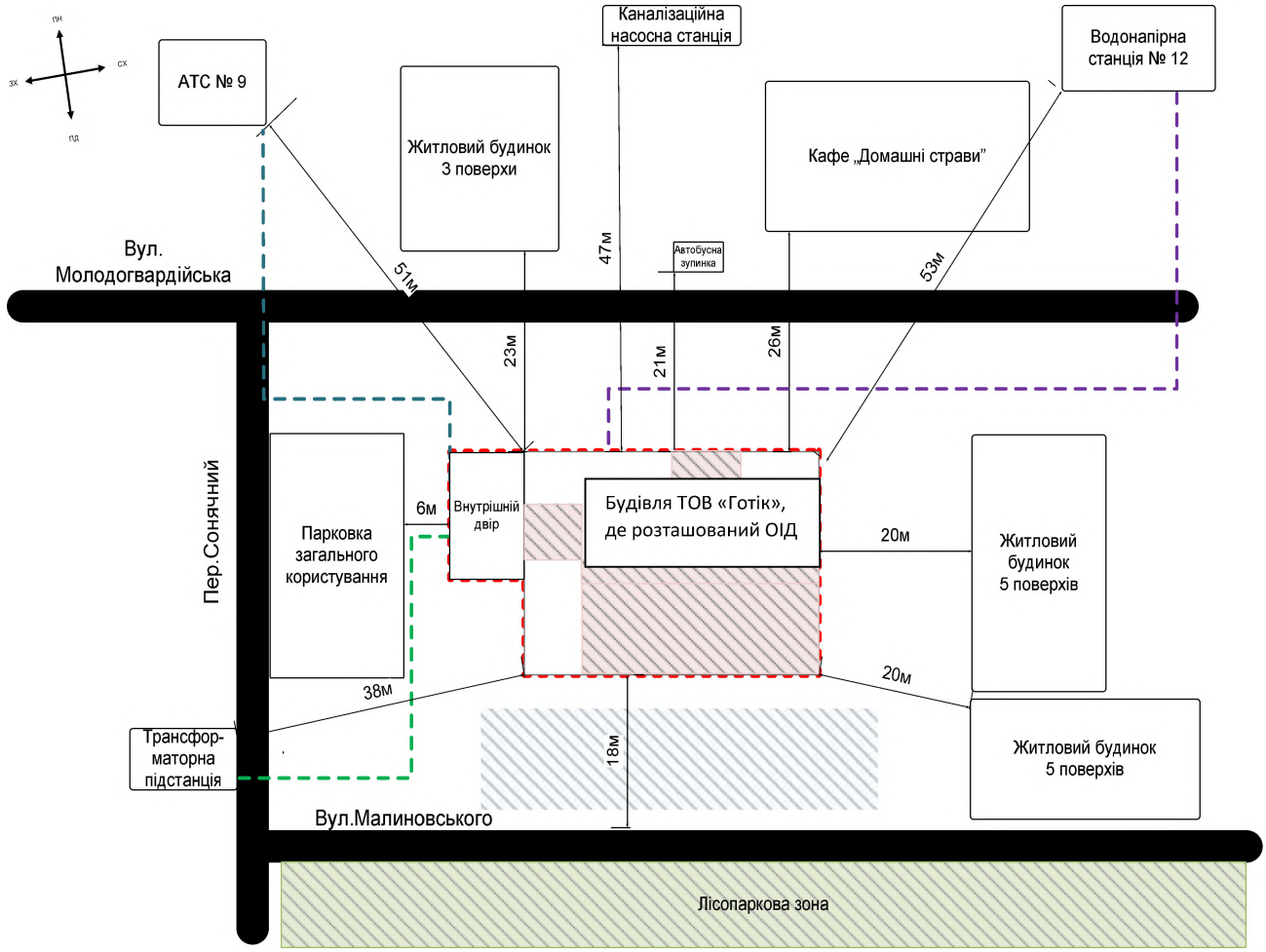
2 Відповідальним за створення контрольованої території призначити адміністратора СЗІ Іванова П. П.

Директор Коваленко О.О.

_____(підпис)

Наказ довести адміністратору СЗІ Прокопенко В.І.

ДОДАТОК Є. Ситуаційний план ОІД ТОВ «Готік»

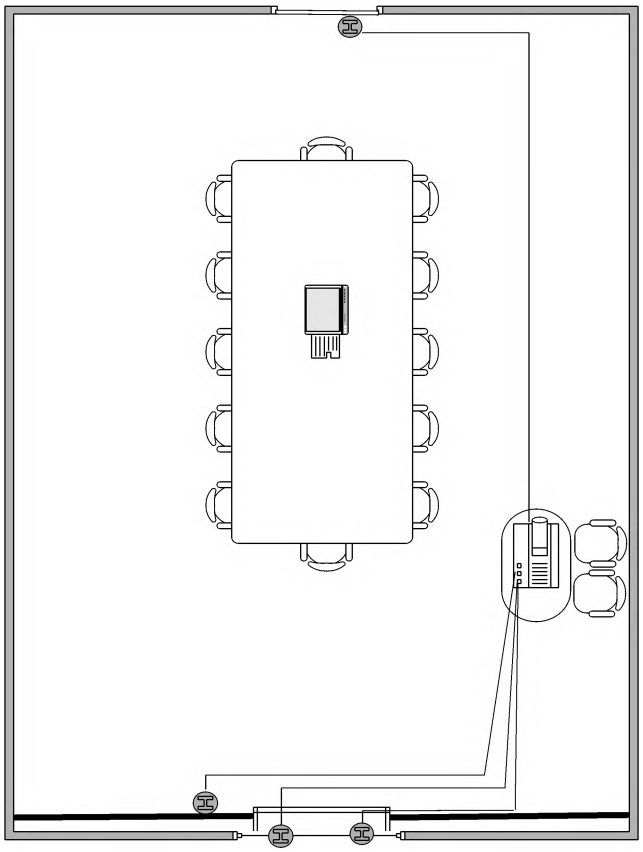


Умовні позначення:

- Роташування ОІД
- Можливі місця розташування ТР
- Межі КЗ
- Телефонна лінія
- Лінії електроживлення
- Канал водопостачання

Рисунок Є.1-Ситуаційний план ОІД

ДОДАТОК Ж. План розміщення технічних засобів захисту акустичної (мовної) інформації в залі засідань



Умовні позначення:

- Вібровипромінювач
- Генератор
- Труба системи опалення
- Пригнічувач мобільних телефонів

Рисунок Ж.1- План розміщення технічних засобів захисту акустичної (мовної) інформації у залі засідань

ДОДАТОК З. Плани комунікацій на ОІД

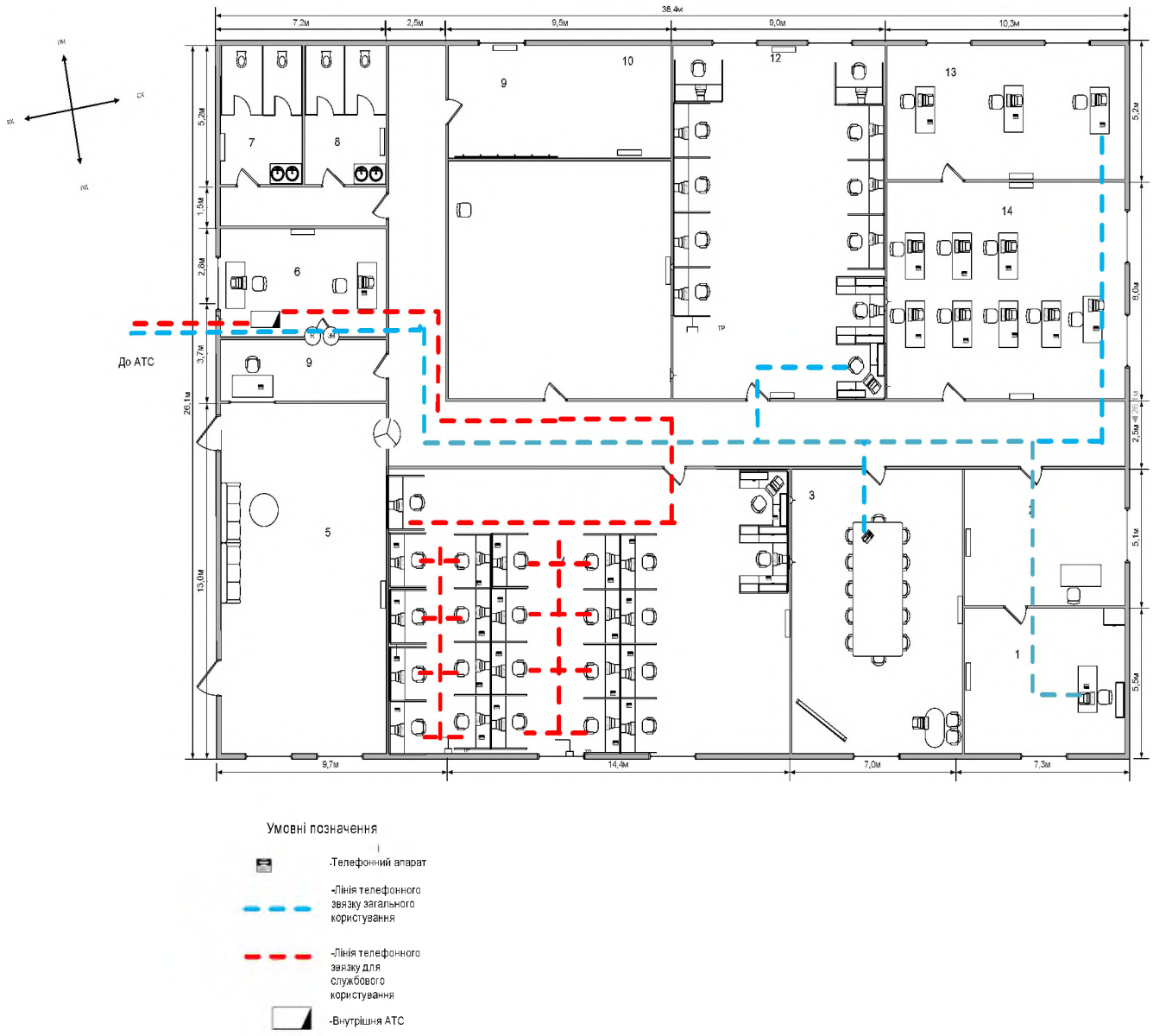


Рисунок 3.1 -План розташування телефонних ліній

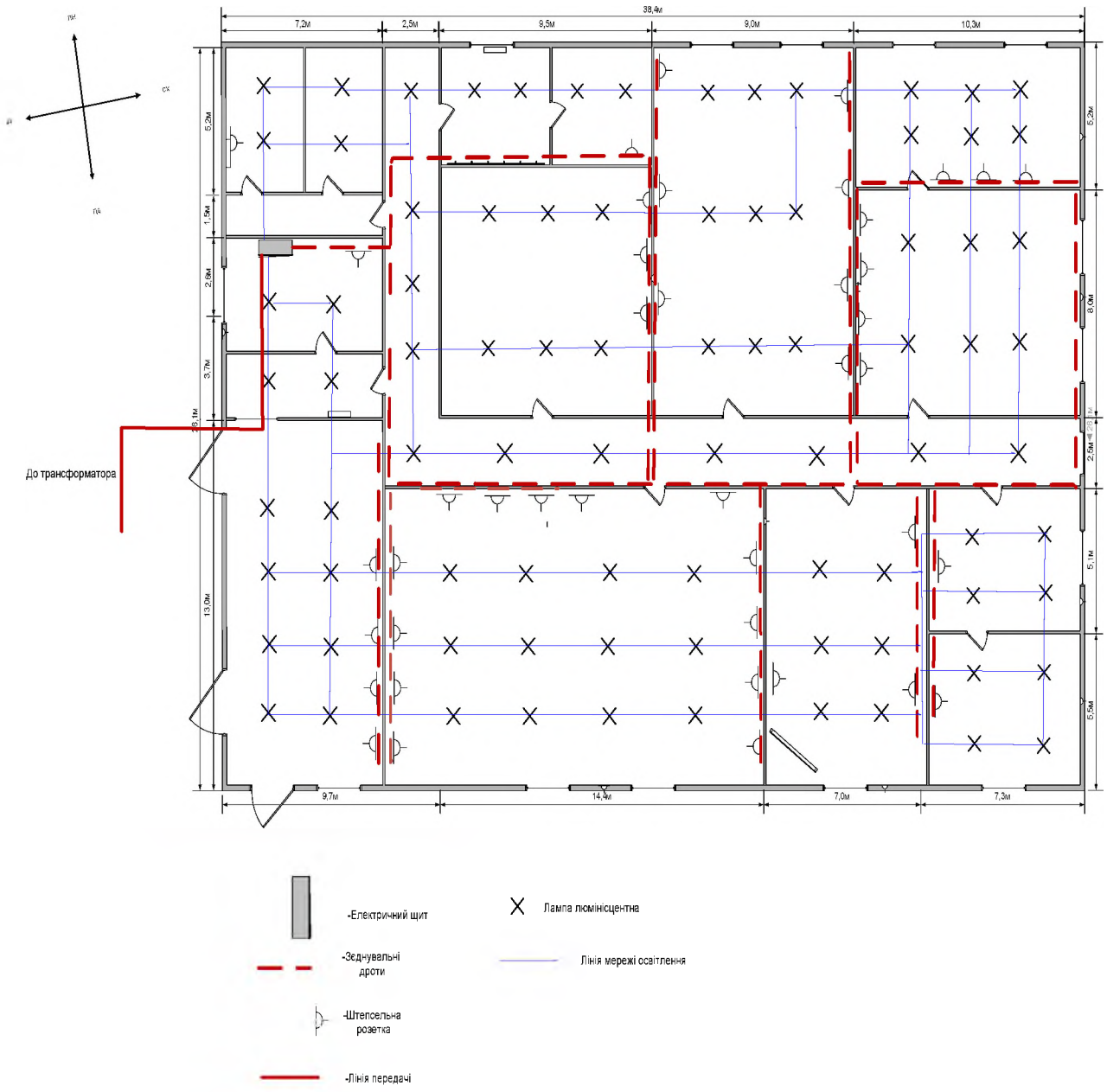
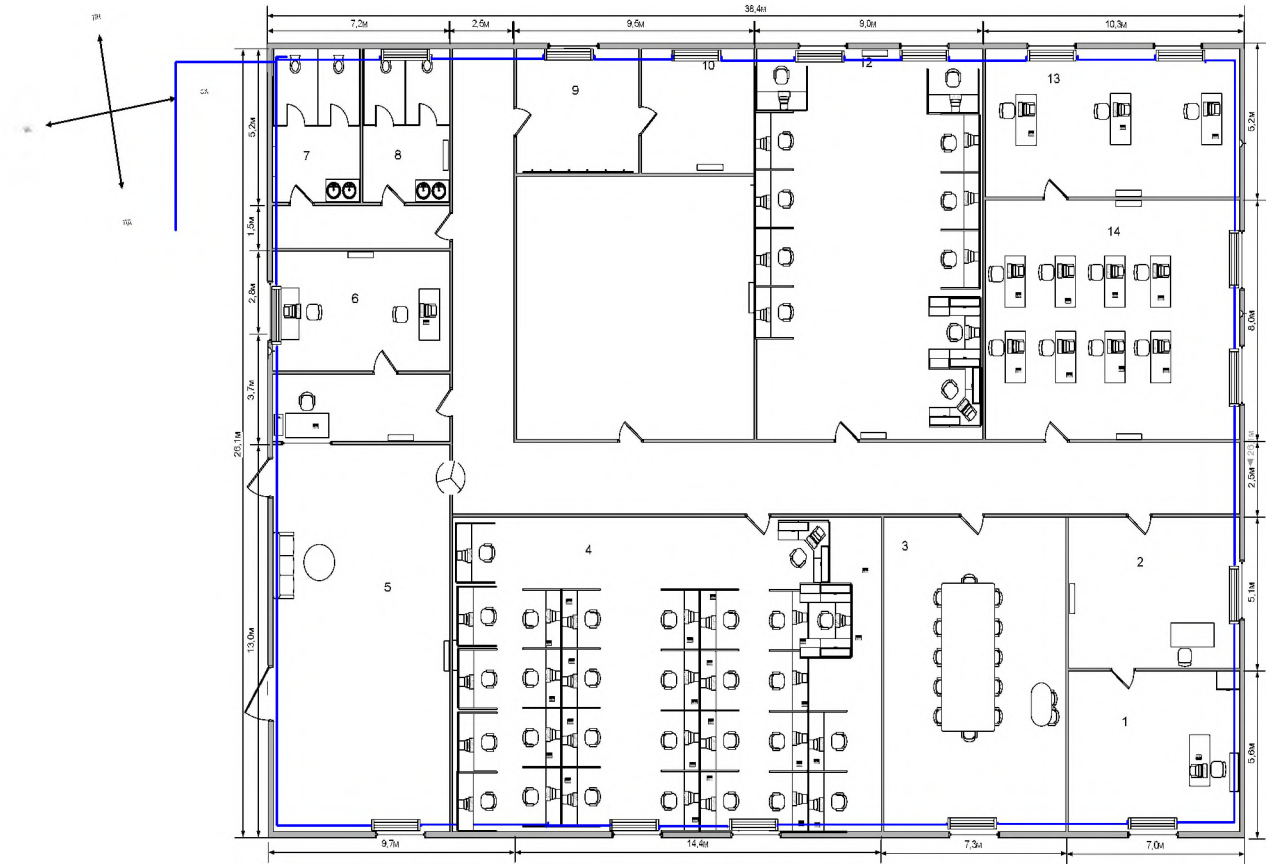


Рисунок 3.2 -План розміщення системи електроживлення та освітлення



1) Директор;
2) Приймальня директора;
3) Зал Засідання ;
4) Оператори
5) Хол;
6) Охорона і серверна;
7) Жіночий туалет ;

8) Чоловічий туалет ;
9) Роздягалка для всіх працівників;
10) Підсобне приміщення;
11) Оператори
12) Оператори;
13) Бухгалтери
14) Відділ кадрів

- Труба системи опалення
- Батарея

Рисунок 3.3 -Генеральний план ОІД

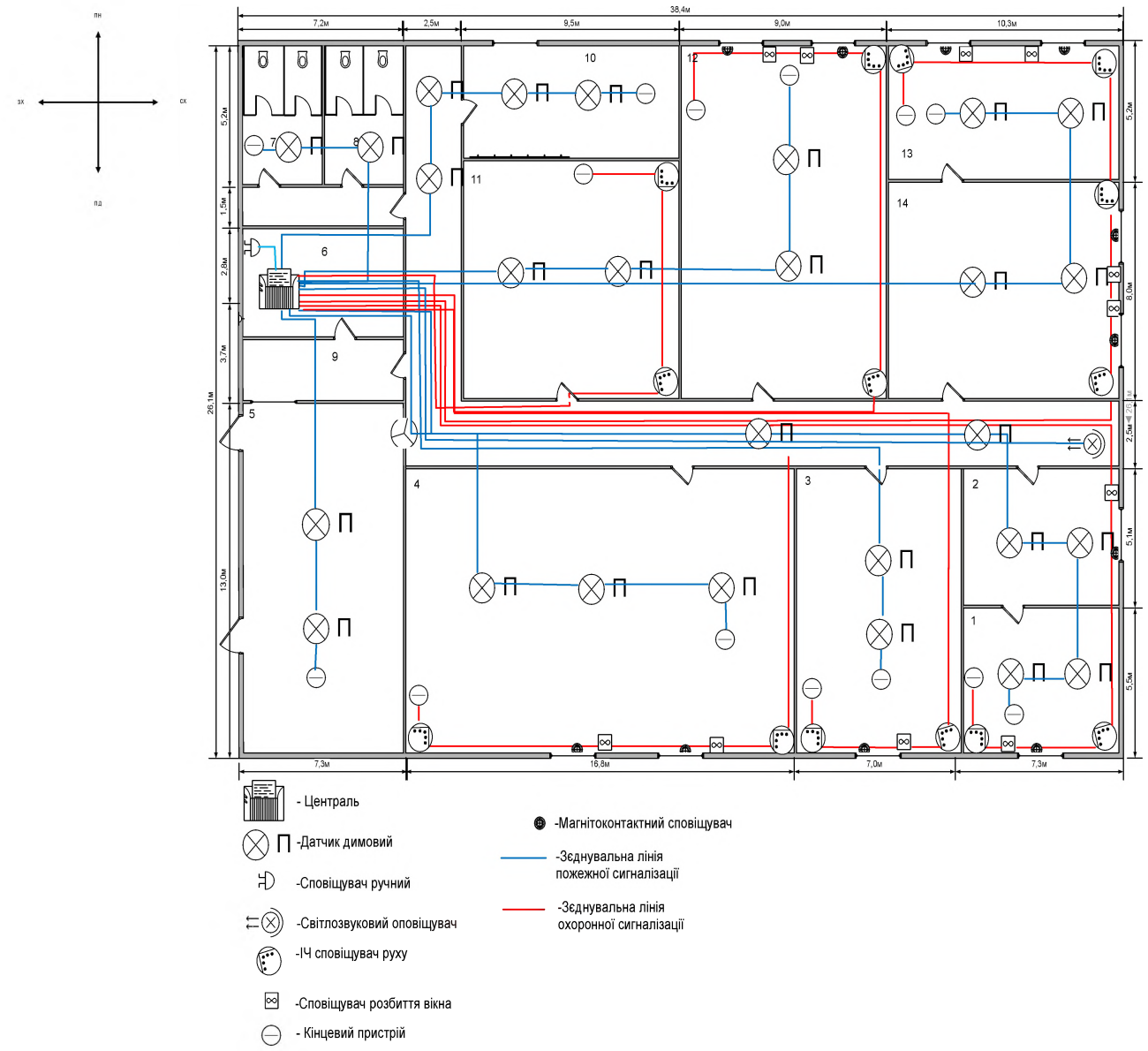


Рисунок 3.4 -План розташування системи пожежноохоронної сигналізації на ОІД

ДОДАТОК И. Відгук керівника економічного розділу

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК І. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-3 Лєвіна Є.Г. на тему: «Розробка комплексу технічного захисту інформації на об'єкті інформаційної діяльності ТОВ «Готік»

Пояснювальна записка містить 77 сторінок, 10 рисунки, 18 таблиць, 12 додатків, 11 джерел.

Метою даної кваліфікаційної роботи є підвищення рівня захищеності інформації з обмеженим доступом, що циркулює на ОІД ТОВ «Готік».

У першому розділі кваліфікаційної роботи проведено обстеження ОІД підприємства, проаналізовані існуючі канали витоку інформації, створені моделі загроз та порушника, а також сформульовані основні задачі даної кваліфікаційної роботи.

У спеціальній частині проведена оцінка стану захищеності на ОІД, в рамках розробки комплексу технічного захисту інформації запропоновані організаційні, інженерні та технічні заходи щодо захисту інформації від витоку акустичними та електричними каналами витоку інформації.

В економічному розділі визначені витрати на розробку і впровадження системи захисту інформації та проведено аналіз її економічної ефективності.

Практичне значення результатів кваліфікаційної роботи полягає у забезпеченні захисту інформації з обмеженим доступом на ОІД ТОВ «Готік» при впровадженні розроблювального КТЗІ на цьому підприємстві.

Серед недоліків проєкту слід відзначити: незначні відхилення від стандартів при оформленні пояснювальної записки; недостатньо обґрунтовано виключення захисту інформації від її витоку каналами ПЕМВН на ОІД ТОВ «Готік».

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Лєвін Є.Г. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Мацюк С.М.**