Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет інформаційних радіотехнологій та технічного захисту інформації
(повна назва)
Кафедра Комп'ютерної радіоінженерії та систем технічного захисту інформації
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Комплекс технічного захисту інформації для об'єкта інформаційної діяльності
(тема)

Виконала:
студент 2 курсу, групи СТЗІАм-22-1
Алфьорова М.О.
(прізвище, ініціали)

Спеціальність 125 «Кібербезпека»
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Системи технічного захисту інформації, автоматизація її обробки
(повна назва освітньої програми)

Керівник проф. Олейніков А.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Антіпов І.Є.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій та технічного захисту інформації
Кафедра_Комп'ютерної радіоінженерії та систем технічного захисту інформації_
Рівень вищої освіти __другий (магістерський)_____
Спеціальність _____125____Кібербезпека _____
Тип програми _____освітньо-професійна_____
Освітня програма _____Системи технічногозахисту інформації,_____
_____автоматизація її обробки_____

ЗАТВЕРДЖУЮ:
Зав. кафедри КРіСТЗІ
Антіпов І.Є._____
(підпис)
«____»_____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентці _____Алфьоровій Марії Олександрівні_____
(прізвище, ім'я, по батькові)

1. Тема роботи «Комплекс технічного захисту інформації для об'єкта інформаційної діяльності»
затверджена наказом по університету *№1281 Ст від 03.11.2023*
2. Термін подання студентом роботи _____10.01.2024_____
3. Вихідні дані до проекту (роботи) _____

Предметом дослідження є:
- організаційно-правові засади захисту інформації в Україні
- огляд можливих технічних каналів витоку інформації для об'єкту інформаційної діяльності
- методологія створення комплексу технічного захисту інформації
- практична побудова комплексу технічного захисту

4. Перелік питань, що потрібно опрацювати в роботі
1 Організаційно - правові засади захисту інформації в Україні
2 Технічні канали витоку інформації
3 Створення комплексів технічного захисту інформації
4 Побудова системи безпеки у складі комплексу технічного захисту інформації
5 Практична побудова комплексу технічного захисту інформації на прикладі об'єкту інформаційної діяльності
5. Перелік графічного матеріалу із зазначенням обов'язкових креслеників, схем, плакатів, комп'ютерних ілюстрацій: кількість слайдів 20 , основні з них:
1) Слайд 1 Титульний аркуш презентації;
2) Слайд 2 Завдання на кваліфікаційну роботу
3) Слайд 3 Організаційно - правові засади захисту інформації в Україні;
4) Слайд 4 Інформація як об'єкт захисту;
5) Слайд 5 Технічний захист інформації;

6) Слайд 6 Технічні канали витоку інформації та їх класифікація;
7) Слайд 7 -8 Створення комплексів технічного захисту інформації;
8) Слайд 9 Побудова системи безпеки у складі комплексу технічного захисту інформації;
9) Слайд 10-19 Практична побудова комплексу технічного захисту інформації на прикладі об'єкту інформаційної діяльності;
10) Слайд 20 Висновки .

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд літературних джерел	05.11-06.12.2023	
2	Розділ 1	07.12-14.12.2023	
3	Розділ 2-3	15.12-22.12.2023	
4	Розділ 4-5	23.12-09.01.2024	
5	Перевірка керівником роботи		
6	Перевірка нормо контролем, перевірка академічної доброчесності		
7	Перевірка зав. кафедрою, рецензування		

Дата видачі завдання 05.11.2023

Студент _____ _____
(підпис)

Керівник роботи _____ проф. Олейніков А.М.
(підпис)
(посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 95 с., 13 рисунків, 5 таблиць, 14 джерел, 9 додатків

КСТЗІ, МОДЕЛЬ ЗАГРОЗ, ОТЗ, ДТЗС, СИСТЕМА БЕЗПЕКИ, ОІД, ВІДЕОСПОСТЕРЕЖЕННЯ, СКУД, СКС

Об’єкт розробки - Комплекс технічного захисту інформації

Мета кваліфікаційної роботи: подальша систематизація, засвоєння і поглиблення теоретичних знань з ТЗІ та набуття умінь самостійно проводити практичні роботи з аналізу ТКВІ, розробляти пропозиції по захисту інформації, їх документально оформляти.

Задача кваліфікаційної роботи: практично та теоретично дослідити процес побудови комплексної системи технічного захисту інформації на об’єкті інформаційної діяльності.

Метод дослідження: розгляд нормативно-правової бази, теоретичних аспектів в області ТЗІ, практичне застосування знань з побудови КСТЗІ.

ABSTRACT

The explanatory note contains: 95 pages, 13 figures, 5 tables, 9 appendices, 14 sources.

COMPREHENSIVE TECHNICAL PROTECTION SYSTEM, THREAT MODEL, BASIC TECHNOLOGY AND SYSTEMS, ASSISTIVE TECHNOLOGY AND SYSTEMS, SECURITY SYSTEMS, THE FIELD OF INFORMATION ACTIVITIES, CCV, ACMS, SKS

The goal of the qualification work is to further systematize, assimilate, and deepen theoretical knowledge in the field of technical information security, as well as acquire the skills to independently perform practical tasks related to the analysis of technical channels of information leakage, develop proposals for information protection, and document them

The task of the qualification work is to theoretically and practically investigate the process of building a comprehensive information security system in the field of information activities.

Research method: examination of the regulatory framework, theoretical aspects in the field of technical information security, and practical application of knowledge in building a comprehensive technical protection system.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

АТС — автоматична телефонна станція

АС — автоматизована система

ДБН —державні будівельні норми

ДТЗС — допоміжні технічні засоби

ІзОД — інформація з обмеженим доступом

КЗ — контрольована зона

КСТЗІ — комплексна система технічного захисту інформації

ЛСАР — лазерна система акустичної розвідки

НД ТЗІ — нормативний документ технічного захисту інформації

НСД — несанкціонований доступ

ОІД — об'єкт інформаційної діяльності

ОТЗ — основні технічні засоби

ПЕМВН — побічні електромагнітні випромінювання і наводки

ПЕОМ — персональна електронно-обчислювальна машина

СКС—структурована кабельна система

СКУД — система контролю та управління доступом

СТЗІ — системи технічного захисту інформації

ТЗ — технічне завдання

ТЗІ — технічний захист інформації

ТКВІ — технічні канали витоку інформації

ЗМІСТ

ВСТУП

Метою кваліфікаційної роботи є систематизація, засвоєння і поглиблення теоретичних знань з ТЗІ та набуття умінь самостійно проводити практичні роботи з аналізу ТКВІ, розробляти пропозиції по захисту інформації, їх документально оформляти. Комплекс ТЗІ – сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об’єкті інформаційної діяльності (ОІД).

Інформація у 21 столітті є найголовнішим ресурсом. Створення комплексів ТЗІ на ОІД є однією з найголовніших частин для забезпечення безпеки інформації, тому дуже важливо звертати увагу на правильність їх побудови та деталі.

У пояснювальній записці кваліфікаційної роботи наведено аналіз досліджуваної нормативно-правової бази для побудови комплексу ТЗІ на ОІД, теоретичної бази з ризиків для інформації.

На основі здобутих теоретичних навичок було проведено огляд та аналіз реального об’єкта в Україні. Після узгодження з установою-замовником, у пояснювальній записці наведено результати проєктно-документальної діяльності. Задля забезпечення безпеки об’єкту його назву, місце та діяльність у роботі змінено.

Таким чином у пояснювальній записці наведено опис реального об’єкту і на базі його наведені дослідження моделі загроз.

Після аналізу моделі загроз описано процес розроблення технічного та фінансового проєкту комплексу технічного захисту інформації на об’єкті інформаційної діяльності.

Для наочного розуміння процесів та необхідності моделі загроз, як етап проєкту комплексу технічного захисту інформації, наведено описи та схеми КСТЗІ.

У кваліфікаційну роботу було включено повний комплекс досліджень з теми «Комплекс технічного захисту інформації для об’єкту інформаційної діяльності» разом з практичними прикладами реалізації такого комплексу.

1 ОРГАНІЗАЦІЙНО - ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Як було сказано раніше інформація у 21 столітті є одним з найважливіших ресурсів. І в часи інформаційної війни однією з найважливіших задач держави є збереження безпеки інформації не тільки цілком таємного рівня, а і будь якої, яка стосуватиметься громадян. Тому з початком інформатизації були створені організаційно - правові засади захисту інформації, які є невід’ємною частиною побудови комплексів технічного захисту інформації. Наразі у всій сфері інформаційної безпеки тривають зміни по покращенню, але це не заважає Україні першою в світі стати цифровою державою, тобто майже всі сфери перенести у цифровий формат, яскравий приклад єдиний портал державних послуг «Дія».

Навіщо ж проводити зміни в сфері інформаційної безпеки, якщо Україна вже є першою цифровою державою? Як раз через цифрову державу з’являються більші ризики, що інформація про громадян, підприємства та усі сфери держави потраплять у руки зловмисника. Наразі також ведеться робота по вдосконаленню організаційно-правових засад захисту інформації в Україні, для того щоб вони відповідали міжнародним стандартам. Розходження в нормах національних правових систем суттєво перешкоджають розвитку та поглибленню широкого міжнародного співробітництва з багатьох суттєвих питань. Зокрема, країни Північноатлантичного договору вимагають від своїх партнерів, і передусім абітурієнтів, ретельного дотримання стандартів та вимог Альянсу щодо захисту інформації. Безумовно, це неможливо без врахування країнами-кандидатами основних принципів політики НАТО. Це пов’язано в першу чергу з тим, що країна партнер почне нести відповідальність вже не тільки про свою інформацію, а й про інші країни, які входять у об’єднання. Але на мою думку усі ці стандарти,

не повинні відповідати рівню заявлених, а навпаки бути кращими і постійно вдосконалюватися, бо час не стоїть на місці як і технології.

Наразі в Україні діє низка законів, постанов та нормативно-правових документів, як регулюють інформаційну безпеку в країні, основними з яких являються:

- Конституція України;
- Закон України «Про інформацію» від 02.10.1992 № 2657-XII
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI
- Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

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

1.1 Інформація як об’єкт захисту

Що ж таке інформація і навіщо її захищати, ще й створювати цілю нормативну базу і комплекси для цього? В цьому розділі ми це розглянемо більш детально.

Правильного визначення як такого для інформації не існує, можна рахувати його більш філософським. Але ми завжди можемо описати, що саме собою представляє інформація.

Розглянемо на прикладі: якщо студенти прийшли на заняття і викладач повідомив, що на наступному занять буде захист лабораторних наприклад, то ми вважатимемо, що студентів проінформували, тобто надали інформацію, яка буде важливою для успішного складання заліку. Отже інформацію ми можемо представити як сукупність відомостей про об’єкти, явища, події і так далі, які дозволяють краще їх пізнати. Але при цьому реакція різних людей на ці відомості буде різною. Так, в доповнення до прикладу, частина студентів буде спокійною, бо вже готові до захисту лабораторних, а частина навпаки буде в паніці, бо навіть не починали готуватися. Або якщо дві людини з різним рівнем знань будуть розглядати одні й ті самі закони наприклад (вони єдині для всіх громадян), то трактувати їх вони можуть зовсім по різному. Тому підвівши підсумки я можу навести наступне описове визначення інформації.

Інформація — це результат сприйняття й опрацювання повідомлень, які людина отримала від інших людей чи результатів спостережень за навколишнім світом, що також залежить від особливостей самої людини, її життєвого досвіду, бази знань, кмітливості тощо.

Інформаційна безпека, в широкому розумінні цього слова, в свою чергу, є сукупністю технічних та організаційних заходів, а також розроблених документів, основною метою яких є захист та збереження інформації, якою володіє людина, компанія чи держава. Разом з тим, інформаційна безпека все ж

залишається складовою частиною кібербезпеки, що є значно ширшою категорією та включає в себе не лише захист інформації та даних, а й захист систем, мереж та інше.

Успішність побудови комплексу ТЗІ ґрунтується на деталях які з’ясовуються в першу чергу після категоріювання ОІД згідно з нормативними документами. Після огляду ОІД, а саме складання ситуаційного та генерального планів ОІД з детальним описом, схем розташування ОТЗС та ДТЗС, а також розгляд усіх можливих каналів витоку інформації, на їх основі розробляється технічне завдання на створення комплексу ТЗІ, від детальності якого прямопропорційно залежитиме результат виконаних робіт.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об’єкті.

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

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (військова, комерційна, банківська, професійна, лікарська, адвокатська таємниця тощо), розголошення якої завдає шкоди особі, суспільству і державі.

Інформація, що становить військову таємницю – це вид таємної інформації, який охоплює відомості в сфері оборони, державної безпеки та охорони правопорядку, розголошення якої може завдати шкоди інтересам державної безпеки, бойової готовності Збройних Сил України та інших військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно з законодавством України.

Інформація, що становить комерційну таємницю – це відомості науково-технічного, технічного, виробничого, фінансово-економічного або іншого характеру (в тому числі секрети виробництва – так зване ноу-хау), що мають дійсну або потенційну комерційну цінність у силу її невідомості третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим комерційної таємниці.

Порядок обігу таємної інформації, що не становить державної таємниці, та її захист визначається відповідними державними органами за умов додержання вимог Закону України "Про інформацію".

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо вона є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Особливим видом таємної інформації є державна таємниця. Вона охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і

органів правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені у порядку, встановленому законом, державною таємницею та підлягає охороні з боку держави.

Віднесення інформації до категорії відомостей, що становлять державну таємницю, порядок її захисту та обігу, доступ до неї визначається Законом України “Про державну таємницю”, яким закладено правову основу створення та функціонування системи охорони державної таємниці в Україні.

Ступень таємності інформації визначається наданим грифом таємності "Таємно", "Цілком таємно" та "Особливої важливості". Гриф надається на певний термін, який залежить від ступеня таємності: для грифу "таємно" – 5 років, "цілком таємно" – 10 років, "особливої важливості" – 30 років. [1]

У роботі розглядатиметься об’єкт який відноситься до категорії конфіденційної інформації, так як вона є однією з найрозповсюджених.

На рисунку 1.1 наведено форму акту про категоріювання, який є обов’язковим у технічній документації.

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об'єкта
_____
(посада, підпис, ініціали, прізвище)
___.___.20__

М. П.

АКТ
категоріювання _____
(найменування об'єкта категоріювання)

1. Підстава для категоріювання _____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об'єкта тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання _____
(первинне, чергове, позачергове)

(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється _____
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті
_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія _____

Голова комісії _____ _____
(підпис) (ініціали, прізвище)
Члени комісії: _____ _____
(підпис) (ініціали, прізвище)
. .20

Рисунок 1.1 – Форма заповнення акту про категоріювання

1.2 Технічний захист інформації

Технічний захист інформації – це діяльність, спрямована на забезпечення організаційними і інженерно-технічними заходами конфіденційності, цілісності і доступності інформації, яка визначена власником або уповноваженою ним особою як об'єкт захисту.

Спираючись на вище приведене визначення інформації і суть технічного захисту інформації, можна сформулювати парадигму захисту інформації -

інформація вважається захищенною, якщо при переміщенні інформації дотримується режимна адекватність комунікабельних носіїв інформації.

Правову основу технічного захисту інформації в Україні становлять Конституція України, закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, з питань технічного захисту інформації, а також безпосередньо Положенням про технічний захист інформації в Україні.

Згідно з останнім нормативним документом ТЗІ здійснюється щодо усіх органів державної влади, органів управління, та місцевого самоврядування, а також усіх органів управління військовими формуваннями. Але також в цей перелік входять усі підприємства, установи та організації утворенні згідно із чинного законодавства України.

За організацію ТЗІ на об’єкті інформаційної діяльності в першу чергу відповідає керівник. Також організаційно-технічні принципи, порядок здійснення заходів з ТЗІ та контролю цієї сфери, разом з атестацією, так само як і усі характеристики загроз норми та вимоги, повинні визначатися нормативно-правовими актами.

Нормативно-правові акти з ТЗІ на ОІД повинні бути прийняті відповідними установчими органами, і являються обов’язковими до виконання кожним суб’єктом інформаційної діяльності. [2,8]

Отже нормативно-правову базу в Україні можна представити наступною схемою (Рис.1.2 – Нормативно-правова база України в сфері ТЗІ)

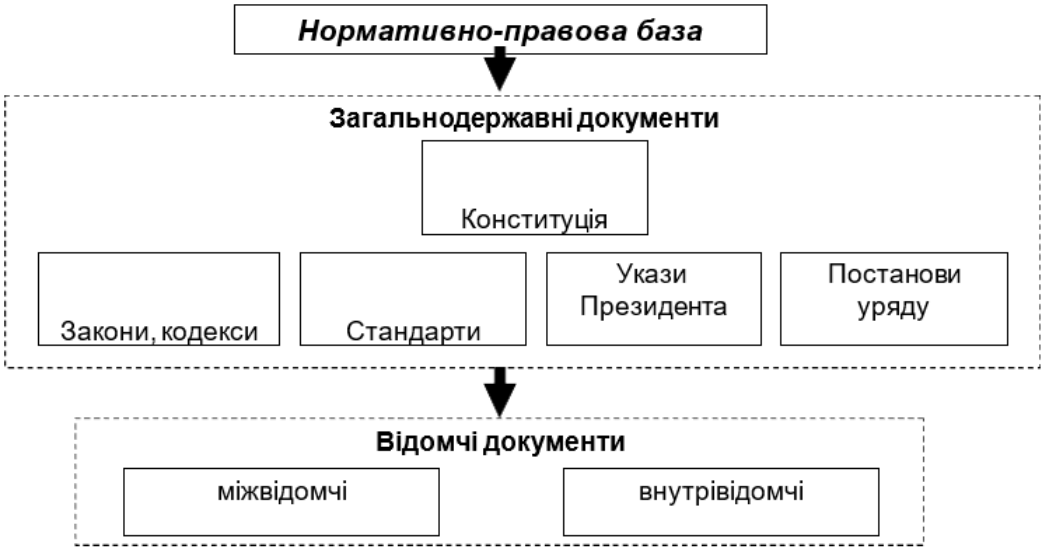

Рисунок 1.2 – Нормативно-правова база України в сфері ТЗІ

В наступних розділах ми більш детально розглянемо принцип побудови комплексних систем технічного захисту інформації на ОІД.

2 ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

Одним з найбільших ризиків для інформації, яка циркулює на об’єкті інформаційної діяльності, являється її витік по технічним каналам.

Саме неконтрольоване поширення інформації, яке призводить до несанкціонованого оволодіння нею третіми особами називається витоком інформації.

Усі витоки відбуваються відповідними каналами і так як зловмисники використовують за правило технічні засоби розвідки, то і канали називаються технічними.

Загальне означення технічних каналів витоку інформації представляє собою сукупність джерела небезпечного сигналу (носія інформації), середовища поширення цього сигналу, засобу технічної розвідки та звісно ж завади які впливають на сигнал у середовищі поширення (Рис. 2.1 – Технічний канал витоку інформації)

Рисунок 2.1 – Технічний канал витоку інформації

В загальному вигляді витік інформації можна розглянути на прикладі. Якщо на ОІД передбачаються усі види робіт з інформацією, що найчастіше так і відбувається: озвучування інформації (проведення нарад, обговорення робочих процесів і так далі), візуалізація інформації (показ презентацій, креслення, роздрукування документів), а також усі види обробки технічними засобами та

системами, включаючи зберігання на носії, то схематично можливість витоку інформації матиме наступний вигляд (Рис.2.2- Витік інформації на ОІД):

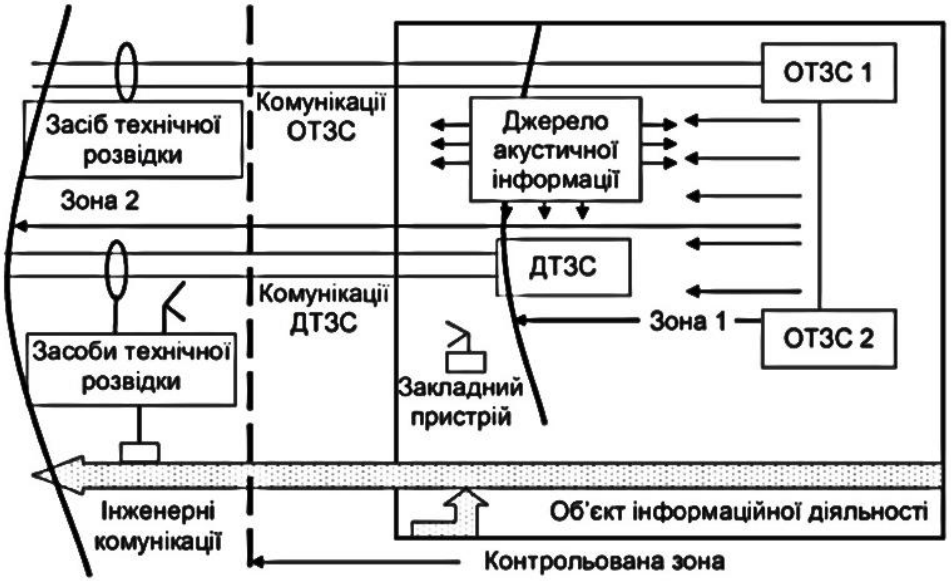

Рисунок 2.2- Витік інформації на ОІД

На даній схемі зображено дві основні зони які обов’язкові до розглядання під час побудови КСТЗІ, а саме:

- Зона 1 - територія навколо основних технічних засобів, в межах якої здійснюється наведення небезпечних сигналів на інші технічні засоби, системи та їх комунікації, характеризується радіусом R1, що визначає граничну відстань від основних технічних засобів до межі, за якою вважається неможливим наведення небезпечних сигналів на технічні засоби.
- Зона 2 - територія навколо технічних засобів обробки інформації, за межами якої вважається неможливим перехоплення небезпечного сигналу з метою відтворення інформації, характеризується радіусом R2, що визначає найбільшу відстань від технічних засобів обробки інформації до межі, за якою напруженості електричного та магнітного полів небезпечного сигналу відносно шумових завад не перевищують нормованого значення. Саме у цій зоні можливе перехоплення інформації.

Найчастіше Зона 1 менша за Зону 2, але бувають і виключення які необхідно обов’язково врахувати при побудові КСТЗІ.

Далі ми розглянемо детальніше класифікацію ТКВІ.

2.1 Класифікація технічних каналів витоку інформації

Кожен канал витоку інформації ми будемо характеризувати за допомогою основних показників, які дозволяють оцінити ризики витоку інформації, до таких відносяться:

- пропускна спроможність ТКВІ;
- довжина ТКВІ;
- відносна інформативність ТКВІ.

Пропускну спроможність технічних каналів витоку інформації ми можемо представити у вигляді наступної формули 2.1:

$$C = \Delta F \log(1 + \frac{P_c}{P_ш}) \text{ , біт/с} \quad (2.1)$$

де ΔF – ширина смуги пропускання каналу, Гц;

$P_с$ - потужність сигналу дБ;

$P_ш$ - потужність шумів дБ.

Усі технічні канали витоку інформації можна прокласифікувати по 4 критеріям, а саме:

- по інформативності;
- по часу прояву;
- по структурі;
- по фізичній природі.

Зупинимося на кожному критерії і розглянемо трохи детальніше з чого вони складатимуться.

Почнемо з першого, а саме інформативності. В даній класифікації все дуже просто: є інформативний канал витоку, а є малоінформативний. Якщо наприклад встановлюється радіозакладний пристрій в буфеті то ймовірність отримати цінну інформацію там буде набагато менша, ніж якщо цей же пристрій буде встановлено в залі нарад.

За другою класифікацією ми розрізняємо 3 підвиди каналів витоку. Якщо витік інформації відбувається цілодобово і кожен день, то такі канали ми будемо називати постійними. Якщо наприклад радіоелектронний закладний пристрій вмикається о 8 ранку і працює до кінця робочого дня, після чого вимикається, то такий канал буде періодичний. І якщо в перших двох закладні пристрої можна легше демаскувати, то з останнім буде трохи складніше, бо епізодичні канали спрацьовують лише на запрограмований чинник, наприклад якщо під час наради хтось скаже слово ключ.

Усі абсолютно класифікації не мають чітких меж, бо канали завжди можуть бути окремими і це буде називатися одноканальними по структурі і якщо витік інформації відбувається одразу по декільком каналам, то це вже буде складений канал витоку по класифікації структури.

Основним поділом технічних каналів витоку інформації являється по фізичній природі, тут 4 основних класифікації:

- візуально-оптичний;
- вібро-акустичний;
- радіоелектронний;
- матеріально-речовий.

Дана класифікація є узагальненою, бо найчастіше ці канали об’єднані між собою. Яскравим прикладом є акустооптоелектронний канал який складається одразу з 3 вищенаведених класифікацій. Наприклад лазерна система акустичної розвідки має характеристики притаманні одразу 3 класифікаціям: вид інформації який дізнаються мовний, що відноситься до вібро-акустичного каналу, методом дізнавання являється лазерна система, тобто застосовується візуально-оптичний канал, а відбитий промінь цієї системи зчитується приймачем та перетворюється у електричний сигнал, який вже можна розшифровувати. Або ж за допомогою радіоелектронних закладних пристроїв ми в першу чергу дізнаємося мовну інформацію. Тому об’єднання дуже розповсюджене у даній сфері.

Про кожен з каналів витоку інформації за вище вказаними класифікаціями далі ми розглянемо детальніше. [12]

2.2 Візуально-оптичний канал витоку інформації

Основою для даного каналу є оптичне випромінювання, або ж світло. Носієм інформації в оптичному каналі є електромагнітне поле (фотони) в діапазоні 0,46-0,76 мкм (видиме світло) і 0,76-13 мкм (інфрачервоні випромінювання).

Для того щоб докладніше розглянути візуально-оптичний канал витоку інформації, необхідно в першу чергу розібратися зі структурою цього каналу (Рис.2.3 – Структура візуально-оптичного каналу)

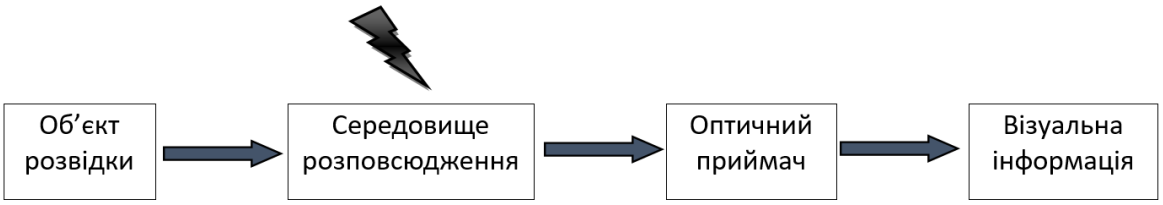

Рисунок 2.3 – Структура візуально-оптичного каналу

Джерелом оптичного каналу витоку інформації являється об’єкт нагляду, який відбиває сигнал (відбивання світла іншими джерелами), або ж випромінює сигнал або теплове поле.

Середовищами розповсюдження будуть усі в яких розповсюджується світло:

- атмосфера;
- безповітряний простір;
- вода;
- оптичне волокно.

Довжина даного каналу витоку інформації буде залежати від потужності світла, об’єкту спостереження, середовища розповсюдження та чутливості фотоприймача.

До останнього входитимуть усі оптичні пристрої, які розширюють можливості людського зору: біноклі, телескопи, фото-кіноапарати, відеокамер, тепловізори, пристрої нічного бачення та багато інших.

2.3 Вібро-акустичний канал витоку інформації

Як вже було сказано найчастіше канали витоку є складеними, тобто відбувається по декільком каналам одночасно, або по паралельним.

Як на мою думку саме вібро-акустичний канал, а точніше канал витоку мовної інформації є найрозповсюдженим серед усіх. У 2021 році вже мною була написана ціла кваліфікаційна робота пов’язана саме з даним типом ТКВІ. У цьому ж розділі ми згадаємо основні аспекти.

Для кращого розуміння, розглянемо загальні схеми способів та засобів зняття мовної інформації, і саме з неї ми можемо побачити, що саме складені ТКВІ несуть більшу загрозу (Рис.2.4 – 2.6).

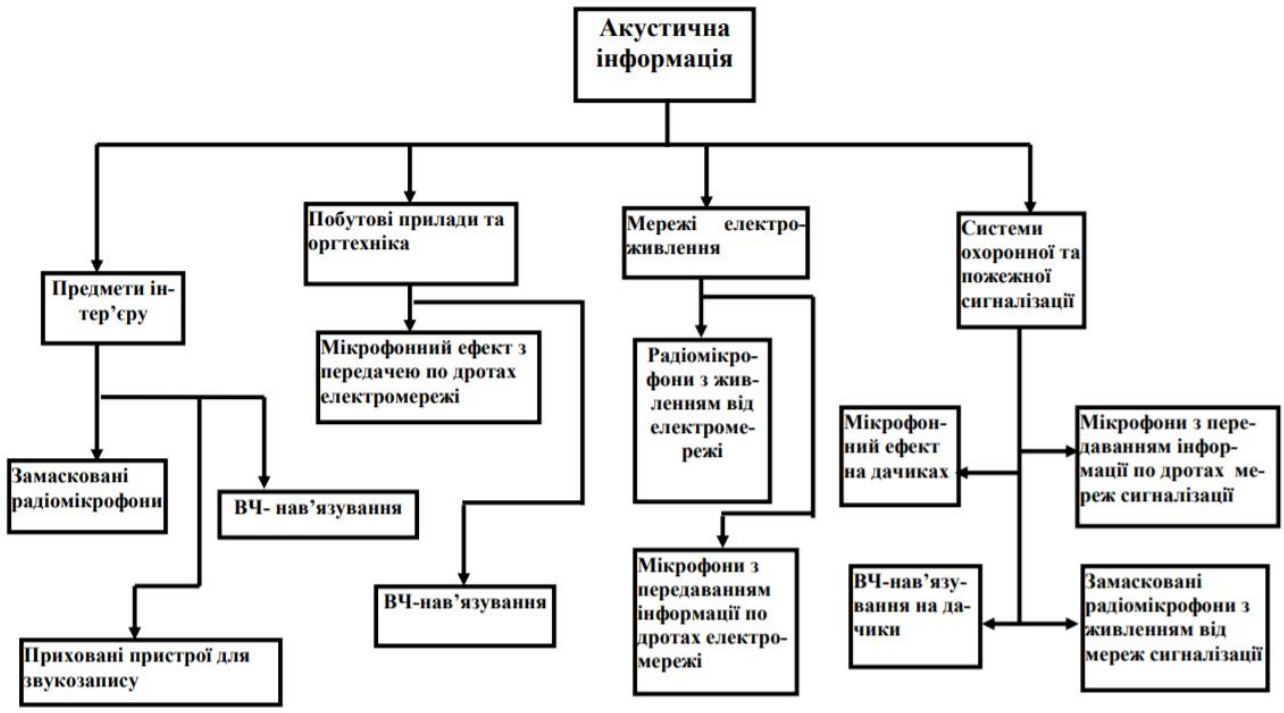

Рисунок 2.4 – Комбіновані способи зняття акустичної інформації

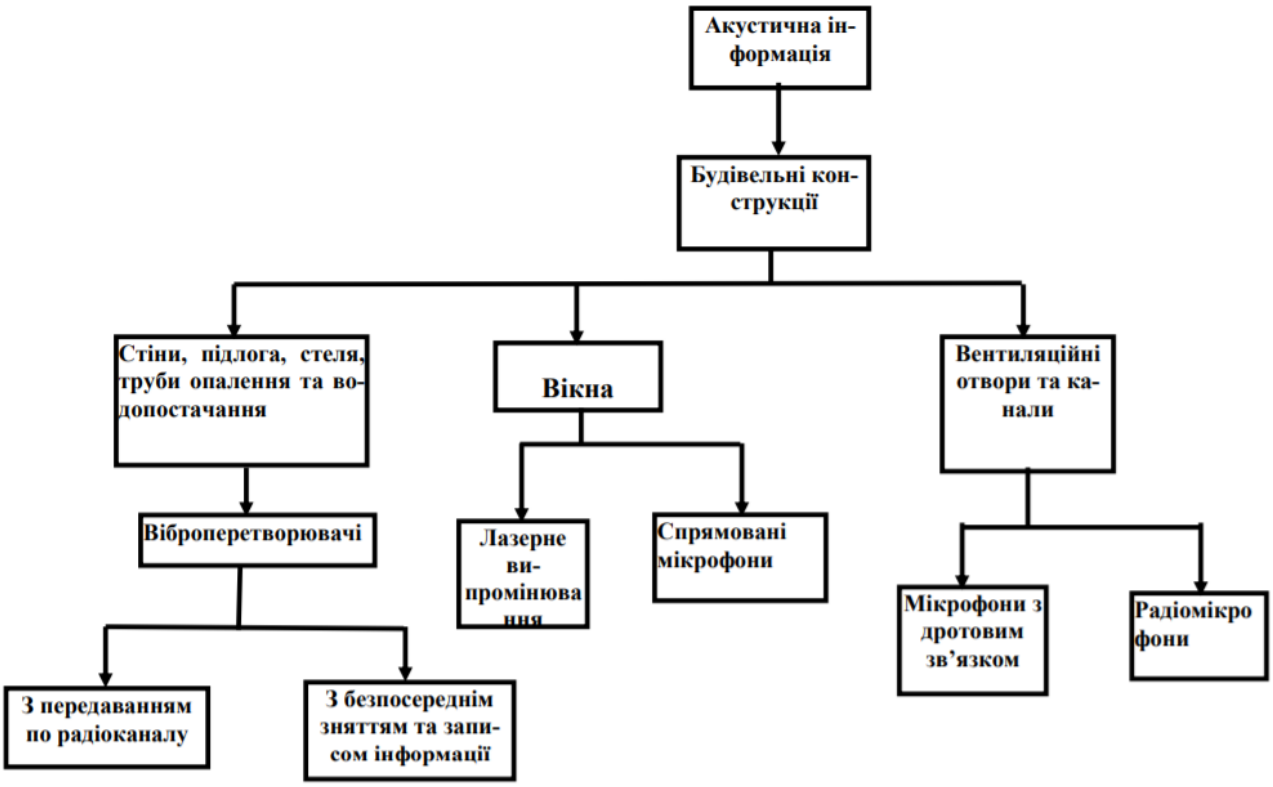

Рисунок 2.5 – Способи зняття акустичної інформації з будівельних конструкцій

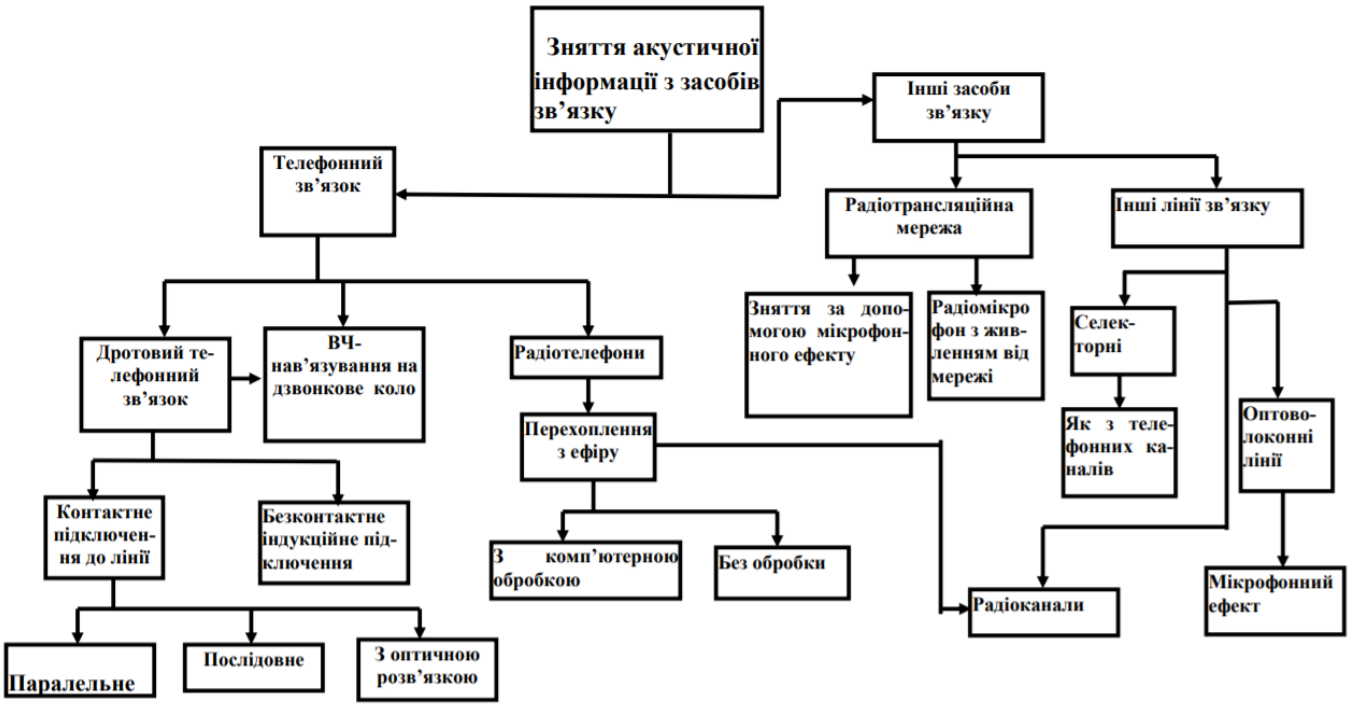

Рисунок 2.6 – Способи зняття акустичної інформації з засобів та ліній зв'язку

2.4 Радіоелектронні канали витоку інформації

Один з найбільших каналів витоку інформації, саме він є основним у складених каналів. Це зумовлено саме носієм інформації в даному каналі, а саме електричним струмом та електромагнітним полем з частотами від десятків Гц до десятків ГГц.

Розглянемо радіоелектронний канал на прикладі схеми (Рис.2.7 – Структурна схема радіоелектронного каналу):

Рисунок 2.7 – Структурна схема радіоелектронного каналу

Джерелом сигналу у цьому випадку можуть виступати:

- передавачі функціональних каналів зв’язку (рації, телефони і так далі);
- джерела небезпечних сигналів, до них входять майже усі засоби які використовуються на об’єкті, навіть засоби протипожежної та охоронної сигналізації;
- об’єкти які відображають електромагнітні хвилі;
- об’єкти які відображають особистий тепловий фон у радіодіапазоні;
- ланцюги заземлення.

Передумовами для виникнення небезпечних сигналів являється конструктивне недоопрацювання при розробці радіоелектронних систем на об’єкті, порушення правил експлуатації та не врахування полей навколо засобів, або ж невідповідність стандартам структурованої кабельної системи.

Окремо хотілося б виділити два витоки інформації каналом побічних електромагнітних випромінювань та побічних наведень на лінії електроживлення (заземлення). Перший утворюється шляхом перехоплення приймачами засобів технічної розвідки за межами контрольованої зони небезпечних сигналів у вигляді побічних електромагнітних полів ОТЗС, які перевипромінюються допоміжними технічними засобами та системами, а також

сторонніми провідниками, а другий утворюється безпосереднім зняттям інформації з ліній електроживлення, за допомогою засобів технічної розвідки за межами КЗ небезпечних електричних сигналів, що наводяться в цих лініях побічними електромагнітними полями ОТЗС та/або просочуються (стікають) в ці лінії (Рис. 2.8 –2.9). [3]

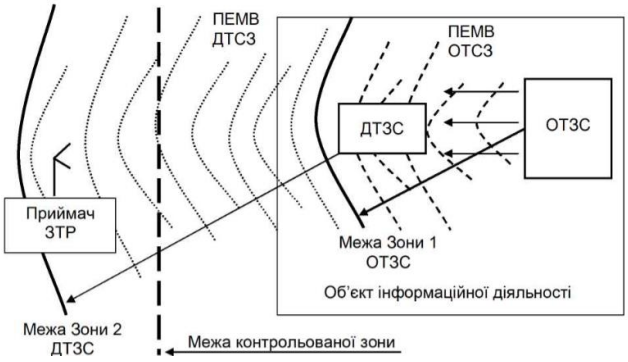

Рисунок 2.8 – Канал ПЕМВ

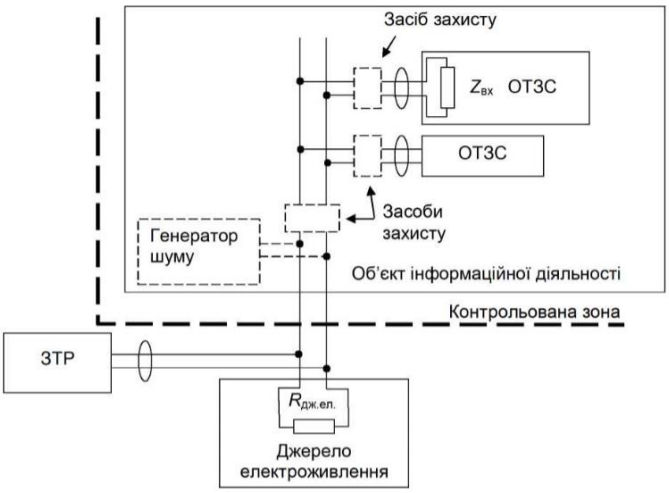

Рисунок 2.9 – Канал ПЕМН на лінії електроживлення

Отже які ж особливості в даному каналі? По-перше незалежність функціонування каналу від часу та низька залежність від метеоумов (звісно ж в порівнянні з іншими). Також виділяють високу достовірність інформації, яку дізнаються, особливо при перехоплені її у функціональних каналах зв'язку. Не можна пропустити й великий об'єм інформації який можна перехопити за допомогою даного каналу дуже швидко і навіть у реальному часі. І даний канал є менш демаскуючим, тобто перехват сигналу та радіотепловий нагляд ми зможемо виявити найчастіше лише за допомогою регулярного радіомоніторингу усього об'єкту інформаційної діяльності.

2.5 Матеріально-речовинні канали витоку інформації

Ми дійшли до розгляду останнього каналу витоку інформації по фізичній природі. Якщо до цього джерелом являлися сигнали, хвилі та частинки, то тут будуть результати діяльності людини зафіксовані на будь яких носіях.

Даний канал є важливим для розгляду, так як на будь якому об’єкті завжди залишатиметься ризик людського фактору, який найчастіше використовує звичайний спосіб дізнавання інформаії, а саме викрадення матеріалів, записів чи чернеток.

Розглянемо загальну класифікацію матеріально-речового каналу (Рис. 2.10 - Класифікація матеріально-речовинних каналів витоку інформації)

Рисунок 2.10 - Класифікація матеріально-речовинних каналів витоку інформації

Втрата носіїв коштовної інформації можлива при відсутності в організації чіткої системи їхнього обліку та відсутності правил знищення. Наприклад через неуважність працівника офісу, чернетка з важливими записами, або навіть печатями, не були належним чином знищенні, що може привести до потрапляння цінної інформації до зловмисника. Далі ми розглянемо правила побудови КСТЗІ де будуть враховані усі ризики ТКВІ.

3 СТВОРЕННЯ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Створення комплексів технічного захисту інформації. Загальні положення.

Ми вже з’ясували що існує безліч ризиків витоку інформації. Аби захистити її, було створено цілу нормативно-правову базу на державному і навіть міжнародному рівні. Так само було створено купу технічних засобів, головною ціллю яких є забезпечення безпеки. Але яке все це застосувати на об’єкті інформаційної діяльності? Для того щоб кожен метод був більш ефективним, необхідно створити систему, в якій кожен механізм попередження витоку буде доповнювати один одного, утворюючи єдиний повноцінний захист. Такою системою є комплекс технічного захисту інформації.

Комплекс ТЗІ – сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об’єкті інформаційної діяльності.

Створення комплексів ТЗІ на ОІД є однією з найголовніших частин для забезпечення безпеки інформації, тому дуже важливо звертати увагу на правильність їх побудови та деталі.

Розглянемо правила створення таких комплексів більш детально.

Як і будь який механізм комплекс ТЗІ є виходом з логічного ланцюжка дій, у кожній одиниці якого є відповідальні суб’єкти та алгоритми дій.

Комплекси ТЗІ створюють на ОІД, де передбачається:

- озвучення інформації, під час нарад, засідань і навіть під час відеоконференцій, яка буде цікава для зловмисника;

- якщо здійснюється будь яка обробки ІзОД технічними засобами (отримання, збирання, записування, введення, зберігання, передавання тощо);

- обіг іншої ІзОД при проектуванні, будівництві, експлуатації об’єктів, виробництві технічних засобів тощо.

Розібравшись на яких об’єктах будується комплекс ТЗІ розглянемо хто здійснює відповідні роботи в кожній одиниці ланцюжка та який юридичний розподіл між ними.

Виділяють наступних суб’єктів створення комплексу ТЗІ:

- установа-замовник - установа, яка є замовником та в інтересах якого створюється комплекс ТЗІ;
- підрозділ-заявник - структурний підрозділ в установі, що обґрунтовує необхідність і заявляє про створення комплексу ТЗІ;
- підрозділ ТЗІ (організатор) - підрозділ (фахівець, або найчастіше група фахівців), якому доручено організацію і супроводження робіт зі створення комплексу ТЗІ в установі (можливо суб’єкт господарської діяльності);
- виконавець спеціальних досліджень технічних засобів системи-підрозділ, який здійснює спеціальні дослідження технічних засобів системи;
- виконавець робіт - підрозділ, який здійснює упровадження комплексу ТЗІ;
- виконавець атестації - підрозділ (суб’єкт господарювання), який виконує атестацію комплексу ТЗІ.

Слід відмітити, що суб’єкти господарської діяльності, які залучаються для атестації комплексів ТЗІ, повинні мати відповідну ліцензію для надання послуг у галузі ТЗІ.

Відповідним рішенням керівник установи-замовника, повинен дати підстави для створення комплексу ТЗІ, що запускає повний механізм. При цьому, споруді, де планується створення комплексу ТЗІ, розпорядчим документом надається статус ОІД та призначається відповідальна особа для організації, супроводження та координації робіт на всіх етапах цього створення.

При цьому враховуються:

- пропозиції від заявників щодо організації створення комплексів захисту;

- відомості про діючі ОІД та створені в установі комплекси ТЗІ;

- перспективи подальших робіт з ТЗІ в установі;

- технічні та економічні можливості установи щодо впровадження інженерно-технічних заходів з ТЗІ.

Виходячи з того, що технології не стоять на місці будь який КСТЗІ повинен створюватися, виходячи із перспектив модернізації і розвитку інших компонентів. Наприклад у зв'язку з воєнними діями стали частіші та триваліші випадки вимкнення світла, отже необхідно враховувати можливість безперебійного переходу живлення на альтернативне джерело енергії, при чому необхідно забезпечувати виконання норм ефективності захищеності інформації, відповідати експлуатаційним вимогам щодо необхідності та періодичності перевірок цієї захищеності.

Для того щоб побудувати відповідний КСТЗІ необхідно використовувати тільки сертифіковане обладнання, або з експертним висновком, що підтверджує відповідність засобу у сфері технічного захисту інформації відповідно до законодавства України.

Застосування засобів ТЗІ іноземного виробництва можливе за умови відсутності вітчизняних аналогів при наявності відповідних техніко-економічних обґрунтувань і проведення їх сертифікації або державної експертизи у сфері ТЗІ.

Щоб створити якісний КСТЗІ необхідно пройти три основних етапи створення:

1) розробка комплексу ТЗІ;
2) упровадження розробленого комплексу;
3) проведення атестації комплексу ТЗІ по завершенню робіт.

Зміст та порядок робіт на етапах створення комплексу ТЗІ визначається нормативними документами системи ТЗІ.

Вимоги до захищеності інформації від витоку технічними каналами та норми захищеності інформації визначаються нормативно-правовими актами та нормативними документами системи ТЗІ.[4]

3.2 Розроблення комплексу ТЗІ

Як вже було сказано у попередньому розділі, створення комплексу ТЗІ це логічний ланцюжок, кожна одиниця якого відіграє свою роль. Дуже важливо при створенні дотримуватися порядку і правил.

В цьому підрозділі розглянемо сам процес розроблення всього комплексу технічного захисту, який в свою чергу складається з двох одиниць ланцюжка:

- передпроєктні роботи;
- розробка технічного проєкту.[5]

3.2.1 Передпроєктні роботи

Передпроектні роботи складаються з комплексу заходів, необхідних для детального дослідження об’єкту і визначення усіх ризиків для інформації, щоб врахувати їх у розробці технічного проєкту.

Всього існує 7 основних заходів передпроєктних робіт: категоріювання, обстеження, спеціальні дослідження основних технічних засобів та самого об’єкту інформаційної діяльності (у разі створення комплексу ТЗІ для захисту мовної інформації), інженерний аналіз додаткових технічних засобів, розробка моделі загроз для інформації і останнє розробка технічного завдання на створення комплексу ТЗІ.

Розглянемо трохи детальніше кожен вид робіт:

- категоріювання – як вже писала у пункті 1.1 перед початком побудови системи захисту інформації, необхідно розуміти яка саме інформація обробляється на об’єкті і до якої категорії відноситиметься. Даний процес відбувається згідно нормативно-правових документів і по закінченню складається відповідний акт про категоріювання.

- обстеження - передбачає аналіз обє’кту інформаційної діяльності, визначення його параметрів та розміщених на ньому технічних засобів, усіх комунікацій, побутових засобів, предметів інтер’єру, що обумовлюють можливість створення технічних каналів витоку інформації, а також підготовку

вихідних даних для розробки моделі загроз для інформації та формування вимог до комплексу ТЗІ. За результатами складається акт обстеження ОІД згідно нормативним документам. Наголошу, що без ретельного обстеження модель загроз може бути не повною, в наслідок чого ризики для інформації зростають прямопропорційно.

- спеціальні дослідження - передбачають комплекс аналітичних, експериментальних та вимірювальних робіт з визначення можливості створення технічних каналів витоку інформації через ОТЗС та в цілому витоку мовної інформації на ОІД.

- інженерний аналіз – проводиться аналіз усіх ДТЗС на ОІД, їх призначення, принцип дії, склад, взаємозв'язки складових ДТЗС тощо для визначення можливості (або неможливості) створення допоміжними технічними засобами та системами технічних каналів витоку інформації при розташуванні їх на ОІД. У разі недостатності інженерного аналізу здійснюються спеціальні дослідження ДТЗС.

- розробка моделі загроз для інформації – на основі усіх обстежень та досліджень об'єкту складається повний формалізований опис методів та засобів здійснення загроз для інформації і схематичне подання шляхів їх здійснення згідно з нормативно-правовими документами. У склад моделі загроз повинні входити: ситуаційний план ОІД та його опис; генеральний план ОІД та його опис; схему розташування та опис ОТЗС; схему розташування та опис ДТЗС; обґрунтування можливості створення технічних каналів витоку інформації, властивих даному ОІД і звісно ж висновки, а саме перелік технічних каналів витоку інформації, які можуть бути утворені на даному ОІД.

- розробка технічного завдання на створення ТЗІ – це вирішальний процес передпроєктних робіт, на якому базуватиметься подальша побудова. Це підсумок усіх обстежень та досліджень з урахуванням моделі загроз, в якому прописуються усі норми та правила побудови прораховані саме для даного об'єкту інформаційної діяльності. Саме тут вказуються абсолютно усі вимоги як технічні так і документальні.[6]

3.2.2 Будівельні норми на приміщення де будується ТЗІ

Основними будівельними нормами які регулюють процес побудови КСТЗІ є ДБН А.2.2-2-96 та ДБН А.2.2-3-2004, але нажаль офіційно вони є недійсними з 2018 року.

При проведенні будівельно-монтажних робіт враховуються вимоги технічного завдання на створення КСЗІ.

Будівельні роботи здійснюються силами установи-замовника або будівельно-монтажними організаціями згідно з проектною документацією на будівництво, яка розробляється проектною організацією у відповідності до вимог нормативних документів.

Але під час побудови КСТЗІ повинні враховуватися абсолютно усі будівельні конструкції на ОІД.

До будівельних конструкцій приміщення відносять перегородки (стіни), перекриття (стелю, підлогу), двері та вікна.

Наприклад згідно будівельних норм перегородки та перекриття, які відокремлюють режимні приміщення від інших приміщень, повинні бути бетонними, залізобетонними (монолітними або збірними) товщиною не менше ніж 80 мм або цегляними товщиною не менше ніж 120 мм.

Опорядження стін і підвісних стель (якщо вони необхідні) повинні бути із негорючих матеріалів.

Кожна будівельна конструкція повинна бути врахована під час побудови КСТЗІ. Нажаль через відміну більшості будівельних норм дуже складно дотримуватися виведених стандартів для захисту інформації, але якщо це режимний об’єкт і будується з нуля, то все рівно усі норми дотримуються як і раніше. Якщо ж ми говоримо про комерційні ОІД, то тут ситуація трохи інакша, бо установа-замовник може не мати змоги перебудувати приміщення і тоді треба вводити додаткові конструкції і заміни існуючих для того щоб знизити ризики виникнення нових каналів витоку інформації.

Після завершення будівельних робіт створюється комісія з прийняття робіт, до складу якої входять представники організації-замовника будівельних

робіт, проектної та будівельно-монтажної організацій. За результатами роботи комісії складається за довільною формою акт приймання робіт з оцінкою їх відповідності вимогам ТЗІ, який затверджується керівником організації-замовника будівництва.[7]

3.2.3 Розроблення технічного проєкту комплексу ТЗІ

Технічний проєкт на комплекс технічного захисту або комплексну систему захисту інформації полягає в розробці організаційних і технічних заходів захисту інформації з обмеженим доступом, котрі відповідають моделі загроз і забезпечують заплановані технічні та економічні показники для встановлених рівнів захисту інформації.

Під час розробки проєкту КСЗІ обґрунтовуються і приймаються проєктні рішення, які дають змогу реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. Проєкт КСЗІ розробляється відповідно до НД ТЗІ 3.7–003-05.

Форма та зміст технічного завдання на створення КТЗІ мають відповідати Додатку Б НД ТЗІ 3.6–003-2016. В технічному завданні також мають бути вказані характерні особливості ОІД, які можуть впливати на вибір проєктних рішень з ТЗІ, орієнтовний вибір основних проєктних рішень з ТЗІ та їх економічне обґрунтування, оцінка умов реалізації заходів ТЗІ.

Особливу увагу замовник має приділити розділу технічного завдання «Вимоги до документації», в якому має бути наведений перелік необхідної проєктної та експлуатаційної документації КТЗІ з наведенням основних вимог до неї (можливо у вигляді посилань на НПА та НД ТЗІ), оскільки від наповнення робочої документації та експлуатаційних документів залежить якість подальшого обслуговування КТЗІ в процесі його експлуатації.

Форма та зміст Пояснювальної записки з ТЗІ, що є ключовим документом проєкту КТЗІ, мають відповідати Додатку В НД ТЗІ 3.6–003-2016.

На основі обґрунтування необхідності у технічному завданні, підрозділ ТЗІ, створює проєкт і план робіт з створення комплексу ТЗІ враховуючи:

- модель загроз для ОІД, неведеним підрозділом-замовника;

- пропозиції від заявника щодо організації створення комплексу захисту;

- відомості про ОІД та вже існуючі в установі комплекси ТЗІ, враховуючи всі існуючи структурні кабельні системи;

- вимоги до будівельних конструкцій режимних об’єктів;

- необхідність впровадження системи контролю доступу, врахувавши його вид та можливості підключення;

- технічні та економічні можливості установи щодо впровадження інженерно-технічних заходів з ТЗІ.

Також повинно враховуватись всі ситуації, які можуть вплинути на працездатність комплексу, щоб мінімізувати їх наслідки (вимкнення електроживлення, пожежа, затоплення і т.д.).

Згідно проєкту виконавець робіт повинен упровадити комплекс ТЗІ, врахувавши усі деталі на ОІД, які можуть вплинути на рівень безпеки інформаційної діяльності, і повідомивши про них підрозділ ТЗІ та підрозділ-замовника.

На основі технічного проєкту комплексу технічного захисту інформацій на об’єкті та обраного технічного обладнання розпочинається складання фінансового проєкту реалізації комплексу технічного захисту інформації.

3.2.4 Розроблення фінансового плану проєкту комплексу ТЗІ

Обов’язковим при створені комплексу ТЗІ є ведення проєктно-кошторисної документації, згідно з вимогами ДБН А.2.2-2 і ДБН А.2.2-3, та створення можливості удосконалення і розвитку інших комплексів ТЗІ установи.

Тому після технічного проєкту розробляється фінансовий план. Саме на цьому етапі виконавець та замовник знаходять фінансове рішення для технічного плану. Під час розроблення фінансового плану усі матеріали та роботи які

зазначені у технічному проєкті, повинні бути перераховані у фінансову складову з урахуванням кількості необхідних робочих та часу виконання робіт.

Для розробки фінансового плану необхідно зробити наступні кроки:

- проаналізувати ринок, а саме дослідити усі пропозиції, які задовольнятимуть технічний проєкт;
- згідно проєктної документації необхідно визначитися з потребами в людській силі, матеріалах та часі;
- регулярно проводити моніторинг і корекції за необхідності.

Планування проєкту гарантує, що результати перевіряються на якість та терміни виконання на кожному кроці.

Крім того, планування проєкту допомагає визначити пріоритети, проаналізувати та розробити правильний план дій для всіх можливих ризиків. Правильна реалізація означає, що якщо під час виконання плану проєкту є пов’язані з ним ризики, вони встановлюються за пріоритетністю та своєчасно розглядаються.

3.3 Упровадження комплексу ТЗІ

Після усіх узгоджень згідно технічного та фінансового плану починається етап упровадження комплексу ТЗІ.

В першу чергу цей процес передбачає придбання засобів ТЗІ та іншого необхідного обладнання згідно фінансового плану . Також в цей етап входить:

- монтаж та пусконалагоджувальні роботи з КСТЗІ;
- розробка технічної та експлуатаційної документації на увесь комплекс.

Впровадження на ОІД заходів та встановлення і налагоджування (настроювання) засобів ТЗІ здійснюється відповідно до технічного проєкту комплексу ТЗІ та іншої проєктної документації, плану робіт з впровадження заходів із захисту інформації на ОІД, а також відповідно до технічної та експлуатаційної документації засобів ТЗІ.

Після проведення усіх монтажних та пусконалагоджувальних робіт проводиться тестовий запуск для перевірки працездатності системи і у випадках виявлення несправностей швидко та якісно їх усунути, не допустивши виникнення нових ризиків для об’єкту інформаційної діяльності.

Також головним кроком в етапі упровадження є проведення уадитів безпеки та навчання користувачів новою системою.

3.4 Атестація комплексу ТЗІ

Останнім етапом побудови КСТЗІ є її атестація.

Атестація комплексу ТЗІ передбачає:

- здійснення інструментального контролю захищеності інформації;

- проведення перевірки повноти і відповідності реалізованих на ОІД заходів із захисту інформації від витоку властивими конкретному ОІД технічними каналами вимогам ТЗ на створення комплексу ТЗІ та вимогам НД ТЗІ;

- оформлення, затвердження та організація реєстрації Акта атестації комплексу ТЗІ.

Атестація комплексу ТЗІ буває первинною, черговою та позачерговою. Первинна атестація проводиться при завершенні створення комплексу ТЗІ. Чергова атестація проводиться при завершенні строку дії акта попередньої (первинної або чергової) атестації. Термін проведення чергової атестації вказується в акті атестації та паспорті на комплекс ТЗІ. Позачергова атестація проводиться у разі змін умов функціонування ОІД, що призводять до змін загроз для інформації. Позачергова атестація також проводитися, якщо така необхідність визначена за результатами державного контролю за станом ТЗІ.

Атестація комплексу ТЗІ включає такі роботи:

- розроблення, погодження та затвердження програми та методики атестації комплексу ТЗІ;

- інструментальний контроль захищеності інформації від витоку властивими даному ОІД технічними каналами та оформлення протоколу інструментального контролю захищеності інформації;
- перевірку правильності встановлення категорії ОІД;
- перевірку виконання етапів створення комплексу ТЗІ, що визначені НД ТЗІ;
- перевірку наявності, чинності та оцінку відповідності проектної, конструкторської, експлуатаційної та іншої технічної документації на комплекс ТЗІ вимогам НД ТЗІ та ТЗ на створення комплексу ТЗІ;
- перевірку правильності визначення загроз інформації (технічних каналів витоку інформації, що властиві даному ОІД) в Моделі загроз для інформації;
- перевірку коректності визначених в ТЗ на створення комплексу ТЗІ вимог до захисту інформації від витоку технічними каналами;
- перевірку відповідності складу та реального розміщення ОТЗ, ДТЗС та сторонніх комунікацій на ОІД даним, зазначеним в моделі загроз для інформації та наведеним у паспорті на комплекс ТЗІ;
- перевірку відповідності складу та розміщення комплексу ТЗІ;
- перевірку наявності сертифікатів відповідності або експертних висновків у сфері ТЗІ на засоби ТЗІ, що входять до складу комплексу ТЗІ;
- перевірку відповідності монтажу та умов експлуатації засобів ТЗІ
- вимогам проєктної, конструкторської, експлуатаційної та іншої технічної документації;
- аналіз результатів (протоколів) інструментального контролю захищеності інформації стосовно інструментального підтвердження відповідності показників захищеності інформації від витоку технічними каналами нормам захищеності інформації;
- оцінку відповідності комплексу ТЗІ вимогам НД ТЗІ та ТЗ на створення комплексуТЗІ;

- оцінку відповідності рівня створеного комплексу ТЗІ сучасному стану науки і техніки у сфері ТЗІ;
- оформлення, затвердження та організація реєстрації Акта атестації комплексу ТЗІ.

В свою чергу Акт повинен містити наступну інформацію:

- загальні відомості про ОІД та інформаційну діяльність на ньому;
- перелік документів нормативно-правових актів та НД ТЗІ, згідно з якими проводилась атестація комплексу ТЗІ;
- перелік проєктних, конструкторських, експлуатаційних та інших технічних документів, наданих для проведення атестації комплексу ТЗІ;
- результати перевірок, які здійснювалися при атестації комплексу ТЗІ;
- висновки щодо відповідності показників захищеності інформації від витоку кожним з технічних каналів, які властиві даному ОІД, нормам захищеності інформації;
- висновки за результатами атестації щодо відповідності комплексу ТЗІ вимогам ТЗ на цей комплекс та вимогам НД ТЗІ;
- термін проведення чергової атестації (строк дії акта атестації);
- рекомендації з експлуатації комплексу ТЗІ (за необхідністю);
- умови проведення позачергової атестації комплексу ТЗІ.

Розглянувши у всіх попередніх розділах основну теоретичну частину, яка включала нормативно-правову базу та класифікацію можливих загроз, цим розділом ми завершуємо розгляд алгоритму побудови комплексної системи захисту інформації, відповідно до чинного законодавства України. В наступних розділах ми ознайомимося з технічними системами які використовуються для побудови систем безпеки, та в останньому розділі буде наведено практичне застосування знань описаних раніше.[9]

4 ПОБУДОВА СИСТЕМИ БЕЗПЕКИ У СКЛАДІ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

З давніх давен люди хотіли зберегти те що їм належить і якщо раніше це були найчастіше предмети, то зараз це вже і речі які ми не можемо просто взяти у руки. Задля забезпечення безпеки наймали охорону, проводили постійні нагляди і так далі, але людський організм не взмозі якісно контролювати 24/7 навіть і 1 приміщення. А коли мова заходить про цілу будівлю, то що робити? Через необхідність зберегти інформацію та убезпечити об'єкти, люди почали розробляти системи безпеки, які будуть працювати автономно і сповіщати людей у разі загроз.

Якщо ми уявимо систему безпеки як організм, то ми можемо виділити і основні органи: мережне обладнання (зв'язок між усіма органами, як у людському тілі кровоносна система та мозок), системи відеоспостереження (наш зір на об'єкті, а точніше в будь якому його куточку), сигналізація (сповіщає про всі небезпечні ситуації, які виникають, тут можна порівняти з нервовою системою) та багато іншого.

Цей розділ буде присвячений технічним засобами без яких уявити сучасний комплекс системи технічного захисту неможливо. Наразі в Україні дана сфера стрімко розвивається, з'являються нові представники на ринку систем безпеки, як національні так і закордонні. Але не кожне обладнання може підійти для побудови якісного КСТЗІ. Тому саме в цьому розділі буде розглянуто основну схему побудови системи безпеки та основних представників на ринку на момент написання даної роботи.

4.1 Мережне обладнання

Як було сказано раніше мережне обладнання можна порівняти з кровоносною системою та мозком людини. Чому? Бо саме у цьому вузлі відбувається обмін інформацією між усіма компонентами системи. Виникла

пожежа? Датчики диму передають цю інформацію по кабельній системі, яка в свою чергу через комутатор дає сигнал на контролер , який сповіщає всіх про небезпеку. І так відбувається з кожним компонентом. Тому дуже важливо щоб кожна складова мережного обладнання була якісна і виконувала свою функцію як слід.

Усе мережне обладнання можна розділити на пасивне та активне. В пасивне входитимуть усі прилади які просто передають інформацію, в активне ж входитиме обладнання яке вже в змозі обробляти і перенаправляти інформацію до необхідних вузлів.

4.1.1 Структурована кабельна система

Основним представником пасивного мережного обладнання є структурована кабельна система (СКС). Ми в першу чергу розглянемо самі види кабелю, але також до кожного з них під час побудови КСТЗІ підбриються свої відповідні конектори, з'єднувачі, схеми обжиму і так далі.

Усі системи можна розділити в першу чергу на силову та слабострумну.

Основні елементи силової мережі – це електророзетки (з автоматами, пристроями захисного вимкнення, лічильником), дроти, з'єднувальні коробки (які зараз майже вже не застосовують), електророзетки, різні лампи і світильники.

Правильно зібрати електрощиток зможе не кожен електрик, хоча кожен буде говорити що це не складно і він зможе це зробити. Тут приховано дуже багато підводних каменів, які здаються простими на перший погляд, але насправді це не так. Простір в електрощитку, найчастіше, обмежений і мало того, що необхідно "запхати" туди автомати й інші прилади, підключити їх і розвести дроти – але також і необхідно зробити щоб не виникло коротких замикань, шумів і також забезпечити недоступність до нього третім особам.

В системах безпеки використовується три типи структурованих кабельних систем на базі слабострумних, так як при роботі використовується низькі напруги:

- з кабелем типу вита пара;

- з коаксіальним кабелем;

- з оптоволоконним кабелем.

Почнемо розгляд з першого типу, а саме кабелю типу вита пара. Наразі в Україні розповсюджено тип даного кабелю категорії 5Е, в яких діаметр однієї жили не більше 0,51 мм. Але з розвитком технологій виникає потреба в якіснішій та швидшій передачі інформації, тому вже почали використовувати і більш сучасні категорії наприклад 6 та 6А (діаметр жили збільшений в середньому до 0,54 мм) і навіть з'явилася 7 та 7А категорії (діаметр жили 0,56).

Чому ж збільшують діаметр жил і навіть змінюють склад сплаву (наприклад, якщо раніше жила складалася з сплаву алюмінію та міді, то зараз використовують жили з міді)?

Звісно це все пов'язано з покращенням передачі сигналу і розширенням діапазону хвильового опору. Наразі дуже багато виробників, але лідером на ринку наразі являється Одесакабель.

У них представлено дуже велику різноманітність кабелю як по категоріям так і по застосуванню: внутрішні, зовнішні, екрановані, протипожежні і навіть армовані та багато інших. Тому саме на їх прикладі буде наведено порівняльні таблиці з характеристиками внутрішніх неекранованих кабелів категорії 5Е, 6 та 7 (Таблиця 4.1 – Порівняльна таблиця кабелю типу вита пара).

Таблиця 4.1 – Порівняльна таблиця кабелю типу вита пара

Категорія	Діаметр жили, мм	Модуль хвильового опору, в діапазоні від 1 до 100 МГц, Ом	Номінальна швидкість поширення сигналу, %	Застосування
5Е	0,51	100 +\-15	68	PBX, V.11, X.21, ISDN, Ethernet (10Base-T), ATM-25/52/155 Mbit/s, 100VG-AnyLAN, Fast Ethernet (100BASE-TX), Token Ring 16/100 Mbit/s, Firewire 100 Mbit/s, PoE (IEEE 802.3af), PoE+ (IEEE

				802.3at), PoE++ (IEEE 802.3bt), HDBaseT, 1000BASE-T, 2.5GBASE-T, 5GBASE-T (до 55 метрів)
6	0,54	100 +\-15 Також додається в діапазоні від 101 до 250 МГц 100 +\-22	68	PBX, V.11, X.21, ISDN, Ethernet (10Base-T), ATM-25/52/155 Mbit/s, 100VG-AnyLAN, Fast Ethernet (100BASE-TX), Token Ring 16/100 Mbit/s, Firewire 100 Mbit/s, PoE (IEEE 802.3af), PoE+ (IEEE 802.3at), PoE++ (IEEE 802.3bt), HDBaseT, 1000BASE-T, 2.5GBASE-T, 5GBASE-T, 10GBASE-T (до 55 метрів)
7	0,565	100 +\-15 Також додається в діапазоні від 101 до 250 МГц 100 +\-22 Та в діапазоні від 251 до 600 МГц 100 +\-25	80	PBX, V.11, X.21, ISDN, Ethernet (10Base-T), ATM-25/52/155 Mbit/s, 100VG-AnyLAN, Fast Ethernet (100BASE-TX), Token Ring 16/100 Mbit/s, Firewire 100 Mbit/s, PoE (IEEE 802.3af), PoE+ (IEEE 802.3at), PoE++ (IEEE 802.3bt), HDBaseT, 1000BASE-T, 2.5GBASE-T, 5GBASE-T, 10GBASE-T

Наступним на розгляді коаксіальний кабель.

Коаксіальний кабель, він же антенний або телевізійний кабель - застосовується для передачі радіочастотних сигналів і використовується у роботі з телевізійними системами, кабельним і супутниковимм телебаченням, в системах відеоспостереження і радіомовлення. Коаксіальний кабель відмінно підходить для стійкої передачі сигналу на достатньо великі відстані. За рахунок екрану з металевого обплетення та фольги телевізійний кабель добре захищений від зовнішніх електромагнітних перешкод. Особливості конструкції кабелю дозволяють забезпечити передачу сигналу високої якості та без спотворень.

Основною характеристикою є хвильовий опір, по якому можна створити наступну класифікацію:

- 50 Ом. В основному областю застосування є радіоелектроніка. Передача сигналу здійснюється з малими втратами, також має високу електричну міцність і передачу потужності.

- 75 Ом. Особливо поширений в передачі зв'язку, тобто як антенний кабель. Радіотехніка та телевізійна сфера - основні області його використання. Він має менші втрати, і має добре узгодження з хвильовим опором у порівнянні з попереднім кабелем.

- 100 Ом. Його використання досить рідко для спеціалізованих цілей або в техніці імпульсної.

- 150 Ом. Даний коаксіальний провід не є передбаченим міжнародними стандартами і в основному застосовується в імпульсній техніці.

Крім даних видів існують і інші, мають ненормований хвильовий опір. Вони зарекомендували себе в аналоговій звуковій техніці.

І третій тип це на основі оптоволоконного кабелю. Даний тип принципово відрізняється від двох попередніх своєю будовою.

Основним елементом оптоволоконного провідника є скловолокно. Тому на відміну від кабелів з мідними та алюмінієвими сердечниками передача сигналу здійснюється за допомогою світлових, а не електричних імпульсів. Це дає кілька суттєвих переваг.

Перша перевага: на сигнал не впливають електромагнітні хвилі та зовнішні наведення, що проявляється у виключній дальності передачі світлового імпульсу без спотворення, яке може становити кілька десятків кілометрів.

Другою перевагою є будова волокон оптичного кабелю чимось нагадує принципову структуру коаксіального. Однак для “оптики” використовується зовсім інші матеріали. Замість мідної струмопровідної жили – скловолокно діаметром 1-10 мкм. Внутрішня ізоляція зі спіненого поліетилену замінюється склопластиковою оболонкою, яка перешкоджає поширенню світлових хвиль за межі скловолоконного провідника.

Як ми можемо побачити існує безліч кабелів і всі вони можуть використовуватися у системі, але важливо прокладати СКС згідно правил

вказаними виробником і характеристикам кабелю. Інакше в кращому випадку ми матимемо шуми та згасання сигналу на меншій відстані ніж можливо.

4.1.2 Активне мережне обладнання

Другою складовою мережного обладнання після СКС являється активне мережне обладнання. Воно виконує роль координатора інформації, яка поступає по СКС.

Активне обладнання — це сукупність апаратно і програмно сумісного обладнання, об’єднаного в єдину систему з метою передачі даних між пристроями різного типу.

До активного обладнання належать всі пристрої, які забезпечують передачу і прийом мережного трафіку, а також зв’язок одних телекомунікаційних систем з іншими.

Основними пристроями і компонентами, які входять в дану групу є:

- Сервери, що зберігають і обробляють інформацію.
- Модеми, мережні адаптери, концентратори, комутатори, маршрутизатори та ін. Ці пристрої необхідні для передачі і прийому даних.
- Мережне програмне забезпечення, що керує процесом передачі і прийому даних і контролює роботу окремих частин комунікаційної системи.

Дуже важливо встановлювати активне обладнання згідно плану враховуючи усі можливі ризики. Необхідно обов’язково забезпечити програмний захист мережі за допомогою криптографічних шифрувань та фаєрволи, який в свою чергу контролює весь вхідний та вихідний мережний трафік, дозволяючи або забороняючи (на основі заданих правил) ті чи інші мережне підключення.

Саме файервол забезпечує захист від атак з віддалених комп’ютерів та дозволяє блокувати деякі потенційно небезпечні служби.

Також дуже важливо розділяти за допомогою активного обладнання усі мережі на ОІД: користувачі, відеоспостереження, сигналізація, бази даних і так далі.

Про основні мережі які використовуються в сучасних системах безпеки поговоримо в наступних підрозділах.

4.2 Системи охоронно-тривожної сигналізації

Після «з'єднувальних» у системі безпеки відбувається, так би мовити розділення: реагування, нагляд, доступ.

Одним з методів реагування на об'єкті є сигналізація. Існує два основних поділи: тривожна сигналізація та пожежна (про неї поговоримо трохи пізніше).

Що стосується тривожної сигналізації, то існує безліч датчиків з яких вона складається, як провідних так і безпровідних, але з початку розберемося з поняттями.

Тривожна сигналізація — це система охоронних приладів, які передають сигнал тривоги непомітно для сторонніх очей.

Одним з основних приладів являється тривожна кнопка. При натисканні кнопки, сигнал тривоги надходить на пульт охоронної служби. За допомогою цього пристрою, потерпілий попереджає черговий підрозділ про напад, закликаючи про допомогу.

Тривожна сигналізація складається з прихованої стаціонарної клавіші, датчиків та централі (ППК).

Які ж датчики входять до тривожної сигналізації? В першу чергу це датчики руху та розбиття скла (при правильному налаштуванні датчика, він може реагувати не тільки на сам факт розбиття, а й на намагання, так як зчитує вібрації на склі), датчик відкриття дверей, або ж геркон. Також існують допоміжні датчики, наприклад затоплення.

Усі тривожні сигнали поступають на централь, яка в свою чергу сповіщає відповідальних про небезпеку. Також ця система найчастіше включає в себе і

контролер, який у разі спрацювання датчиків може передавати сигнал і будуть виконуватися захисні дії.

Так на одному з об’єктів було впроваджено систему тривожної сигналізації було проєктовано цілий алгоритм який виконувався під того чи іншого сценарію. Наприклад, якщо спрацьовував датчик розбиття скла, то автоматично опускалися металеві жалюзі, які в звичайному режимі закривалися лише в неробочий час. Також прикладом є сценарій з спрацювання геркону, при якому в основних приміщеннях блокувалися двері і відкрити можна було лише за допомогою ключа у відповідального служби безпеки.

Як вже і писала раніше кожна одиниця ланцюжка тісно пов’язана з іншими і утворюють один єдиний механізм. Далі у розділах про відеоспостереження та системи контролю доступу ми ще поговоримо про ці зв’язки.

Найбільшими представниками провідних систем в Україні є системи «Лунь», до централі яких можна підключити майже будь який датчик.

Але наразі стають дуже популярними бездротові системи. Чому так? Ну в першу чергу це зручно, бо не потрібно прокладати додатковий кабель, але з’являються тоді ризики при передачі сигналу бездротовим шляхом. Українські спеціалісти вже почали вирішувати дану проблему, зменшуючи ризики як від впливу третіх осіб, так і погодних умов.

Наразі українські системи бездротового реагування є провідними у світі, так як саме наші спеціалісти ведуть активну роботу з представлення не тільки внутрішніх датчиків, але і зовнішніх. Звісно основою в таких датчик вже є штучний інтелект.

Але на об’єктах в залежності від площи я раджу використовувати провідні системи, або ж комбіновані.

В Україні основним виробником безпровідних систем став «Ajax» (хоча і провідні системи в них також є), так як вони одні з найперших почали вводити безпровідні системи у обіг і займаються найбільшими розробками у цій сфері.

Станом на 2023 рік на ринку також було представлено одні з найперших систем охоронної сигналізації від «U-prox», з ним ми познайомимося ще як з виробником систем контролю доступу.

Як і з іншими пристроями існують свої правила для встановлення датчиків. В першу чергу потрібно врахувати раціональність встановлення і визначити порогові значення, а після згідно рекомендацій виробника та проєктного плану встановлювати. Наприклад встановлення датчику руху на вході без правильного програмування, призведе до постійних хибних спрацювань.

4.3 Системи контролю та управління доступом

Щоб запобігти несанкціонованому доступу на об’єкт необхідно забезпечити правильний процес роботи системи контролю доступу.

Системи контролю доступу (СКУД) – це сукупність спеціалізованих пристроїв та програмного забезпечення, для запобігання проникнення сторонніх людей та безперешкодного пересування при цьому людей з відповідним доступом.

Саме система контролю доступу є ідеальним рішенням для розділення об’єкту по зонам з відповідними доступами.

До СКУД відносяться:

- ідентифікатор — ключ або картка, що містить мікросхему з даними, необхідними для розпізнавання. Крім того, ідентифікатором може виступати код, що вводиться на клавіатурі, райдужна оболонка, відбиток пальця або навіть голос відвідувача;
- зчитувач — прилад, що містить електронну плату. Пристрій зчитує інформацію з ідентифікатора і передає її на контролер. У сучасних зчитувачах використовуються технології, що розпізнають біометричні параметри;
- контролер — «ядро» СКУД, в якому зберігаються коди ідентифікаторів. Саме цей прилад «приймає рішення» про допуск або заборону допуску власника ідентифікатора;

- електромагнітні або електромеханічні замки, турнікети, біометричні замки;
- кодова клавіатура і кнопка виходу;
- програмне забезпечення — встановлюється на один або кілька комп'ютерів, об'єднаних в єдину мережу. При необхідності створення звітів і систематизації інформації використовуються модулі фотоверифікації та обліку робочого часу;
- додаткове обладнання: броньовані двері, металорамки, лічильники відвідувачів та інші.

Добрим прикладом СКУД з практики була організація перевірки особи з доступом на наявність заборонених металевих предметів. В цьому випадку встановлювався зчитувач (ідентифікатор особи), після якого людина проходила через металорамку і при її спрацьовуванні відкритий до цього прохід через турнікет закривався. Таким чином усувалася не лише загроза проникнення з забороненим предметом, а й одразу з’ясовувалася особа, яка намагалася це зробити.

Набувають популярності різні ідентифікатори, особливо біометричні.

До біометричних ідентифікаторів ми можемо віднести як і звичайні зчитувачі відбитків пальців, сітківки ока, чи загалом обличчя, так і цілі контролери з вбудованими біометричними зчитувачами. Це все вже не є таким фантастичним порівняно з ситуацією наприклад 5 років назад.

В будь якому випадку необхідно завжди мати другий варіант для ідентифікації, наприклад карту MIFARE. Це необхідно для випадків, коли неможливо ідентифікувати людину за допомогою біометричного зчитувача.

Подібна ситуація виникла на одному з об’єктів на якому була ідентифікація по відбитку пальця, коли працівник, нажаль, обпік палець яким мав доступ, то система не змогла його впізнати. В цьому випадку прийшло на виручку як раз картковий ідентифікатор.

Як говорили в розділі про тривожну сигналізацію, можна зробити відповідну зв’язку її з іншими системами і СКУД не є виключенням.

При спрацюванні тривожної сигналізації, можуть блокуватися виходи, а якщо виникає пожежа, то навпаки розблоковуються усі виходи.

Важливими етапами упровадження СКУД на об’єкті є дотримання правил встановлення та пусконалагоджувальних робіт.

За допомогою програмного забезпечення у сучасних системах можна контролювати пропускну систему кожного включаючи обмежувати доступ до приміщенні в залежності від часу.

4.4 Системи відеоспостереження

Відеоспостереження використовується у системах безпеки дуже давно. Але зараз воно виходить на абсолютно новий рівень, так як починає базуватися на елементах штучного інтелекту.

Раніше використовували аналогове відеоспостереження, але через незручності і застарілість технології, даний тип відійшов на другий план. Зараз основою для відеоспостереження є IP технології.

Які основні переваги? Розглянемо це питання трохи детальніше:

- по-перше доступ до кожної IP камери при правильному налаштуванню можна мати з будь якої точки світу, головне щоб був доступ до інтернету.
- по-друге простіша і більш універсальна система встановлення, а саме: якщо для аналогових камер потрібно було тягнути 2 кабелі (аналоговий та силовий), або ж комбінований який на порядок дорожчий, то для IP найчастіше вже достатньо прокласти один кабель типу вита пара, який в сучасному світі є більш універсальним у використанні (навіть аналогову камеру можна підключити за допомогою нього та використовуючи спеціальні балуни на обох кінцях). Все найчастіше виробник використовують для живлення IP камер технологію POE, яка значно полегшує монтаж та підключення, бо в такому випадку живлення як і інформаційний обмін відбувається завдяки відповідним жилам кабелю типу вита пара.

- по-третє IP системи як і аналогові ведуть послідовну передачу даних, але швидкість набагато більша. Це пов’язано з тим, що дані можна розділити. Це можна розглянути на прикладі: якщо ми візьмемо 10 кольорів фарби та змішаємо це в один потік, як це відбувається в аналоговому відеоспостереженні, то розділити ми не зможемо, а якщо в нас 10 фломастерів різних кольорів, то ми завжди можемо дістати окремий колір, так і в IP відеоспостереженні, бо в цьому випадку сигнал цифровий, тобто представлений послідовністю «0» та «1».
- четверте це мала помітність збоїв. Це пов’язано з попереднім пунктом. Якщо на аналогове відеоспостереження діє якась перешкода, то ми побачимо лише шуми і обробити зображення не зможемо, в той самий час IP відеоспостереження, намагаючись виправити помилку «заморозить» кадр або встигне виправити і збої будуть непомітними

Схеми підключення системи відеоспостереження можна побачити на Рисунках 4.1-4.2.

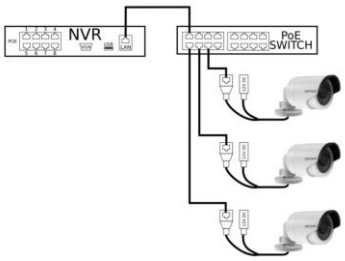

Рисунок 4.1 – Схема підключення системи відеокамер з підтримкою POE

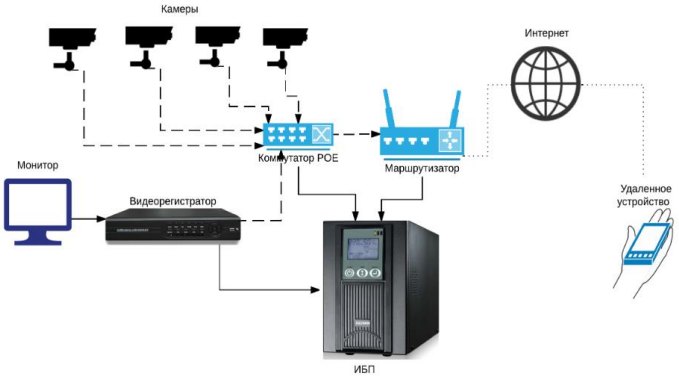

Рисунок 4.2 – Загальна схема підключення системи відеоспостереження

4.5 Системи протипожежного захисту

Абсолютно усі системи на об’єкті повинні будуватися з дотриманням протипожежних правил і обов’язково повинна бути запроваджена система протипожежного захисту.

Системи протипожежного захисту - це комплекс організаційних та технічних засобів, встановлений на ОІД, який призначений для виявлення, локалізації та ліквідації пожежі без втручання людини, захисту людей, матеріальних цінностей та довкілля від впливу небезпечних факторів пожежі.

Системи протипожежного захисту в усьому світі та в Україні зокрема строго регламентуються. Вимоги до них описані нормативними документами (ДБН, ДСТУ і ін.) а також Законами України. З кожним роком норми щодо пожежної безпеки об'єктів все більше посилюються, приводяться у відповідність європейським EN. Абсолютно вся діяльність у даній сфері є стандартизованою та сертифікованою і регулюється безпосередньо ДСНС та службами ліцензіювання.

До складу систем протипожежного захисту входять:

- система пожежної сигналізації
- автоматична / автономна система пожежогасіння
- система оповіщення про пожежу та управління евакуацією
- система протидимного захисту
- система централізованого пожежного спостереження

Також до складу систем протипожежного захисту можна віднести:

- грозозахист
- пожежні ліфти
- пожежні крани і кран-комплекти
- протипожежні двері, ворота, завіси та інше.

Дуже важливе значення має найбільш раннє виявлення пожежної небезпеки на об'єкті, для цього повинні використовуватися сучасні засоби виявлення загорянь, такі наприклад як аспіраційна система пожежної

сигналізації, що дозволяє виявляти продукти горіння на самій ранній стадії (до появи видимого диму або вогню).

Весь комплекс протипожежного захисту повинен працювати як єдина система, всі системи повинні взаємодіяти на апаратному рівні, мати певний запас міцності для надійної роботи в екстремальних умовах і тривалу автономність по електроживленню.

5 ПРАКТИЧНА ПОБУДОВА КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПРИКЛАДІ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Задля кращого розкриття теми кваліфікаційної роботи, мною було проведено практичну побудову комплексної системи технічного захисту. До мене звернулася установа-замовник з проханням зпроєктувати та упровадити комплексну систему на їх об'єкті. Дотримуючись усіх правил, стандартів та алгоритмів побудови наведених в попередніх розділах, я взялася за роботу. Результати цієї роботи наведені у цьому розділі, але зі зміненими назвами, місцем знаходження та описом, задля забезпечення конфіденційності.

5.1 Опис об'єкту

Як зазначалося раніше після узгодження з представником-замовником об'єкт був взятий за основу, для наочного відображення процесу побудови комплексу технічного захисту інформації на об'єкті інформаційної діяльності.

Об'єкт ЦСД«Промінь» знаходиться в Україні за адресою: м. Харків, вул. Архітекторів, 358. На території об'єкту знаходиться три будівлі. Основна будівля, в якій проводяться усі основні робочі процеси, двоповерхова з підвальним приміщенням. Поряд з нею розміщується одноповерхова будівля з актовою залою та власною котельнею. Також розміщенно невелике КПП на в'їзді до території.

Основна діяльність ЦСД«Промінь» направлена на процеси психологічно-соціальної безпеки мирного населення яке знаходиться у місті, або евакуювалося з більш небезпечних районів.

Об'єкт поділено на дві основні зони роботи (по поверхам) і в кожній знаходиться 2 головних приміщення для неї: кабінет для нарад та комутаційне приміщення. В тому числі на другому поверсі захисту підлягає додаткове приміщення з розташованими у ньому серверами.

Мета, яку поставив представник-замовник, заключається в побудові комплексу який забезпечуватиме безпеку відвідувачів, персоналу та інформації яка зберігається та циркулює на об’єкті.

Після огляду ЦСД«Промінь» було складено модель загроз на основі якою буде будуватися комплекс технічного захисту інформації. Також було проведено огляд об’єкту на відповідність вже існуючої системи ТЗІ до ДБН А.2.2-2-96 та ДБН А.2.2-3-2004. В результаті чого було виявлено порушення та невідповідність системи вимогам представника-замовника, тому було вирішено провести демонтаж старого комплексу ТЗІ разом з структурованою кабельною системою та побудувати нову більш сучасну систему з обов’язковою можливістю розширення.

Також було оглянуто територію за межами контрольованої зони та виявлено декілька можливих канали витоку, які в подальшому будуть враховані у моделі загроз та технічному проєкті. Це пов’язано з близьким розташуванням до ОІД 2 будівель в які потенційно може потрапити зловмисник.

З ситуаційним та генеральними планами кожної зони можна ознайомитися у Додатках Б-Д

5.2 Модель загроз для об’єкту інформаційної діяльності

Для надійної охорони ОІД , як вже зазначалося, в першу чергу треба проаналізувати всі можливі технічні канали витоку інформації: вібро-акустичний, візуально-оптичний, електромагнітний та матеріально речовий.

Модель загроз включає в себе розгляд актів обстеження, ситуаційний і генеральний та план розміщення основних технічних засобів та допоміжних технічних засобів.

Перед побудовою моделі загроз технічними каналами витоку інформації, треба розуміти кому буде потрібна інформація, тому складається, в першу чергу, модель зацікавленої сторони.

У ролі порушника для ЦСД«Промінь» може виступати як сторонні особи, наприклад зацікавлені в конфіденційній інформації бенефіціарів, так і персонал самого об’єкту.

Інформація в ОІД передається і обробляється за допомогою різних носіїв:

- акустичні, аналогові та цифрові сигнали;
- документація, чернетки та графічні матеріали; макети, готові пристрої та їх елементи.

Наведемо можливі КВІ в ЦСД«Промінь»:

1. Вібро-акустичний

   Так як на територію ЦСД«Промінь» мають право заходити відвідувачі, без доступу до конфеденційної інформації, то витік інформації через прослуховування стін або дверей можливий. Також є варіанти: прослуховування за допомогою закладних пристроїв, ЛСАР, вузьконаправлених мікрофонів та через комунікаційні конструкції будівлі (труби).

   Підслуховування інформації через ЛСАР чи вузьконаправлені мікрофони можливе з двох приміщень за межами контрольованої зони.

   Через достатню ймовірність зняття інформації через комунікаційні конструкції є необхідність взяття під контроль усі вузли комінкаційних систем.

2. Візуально-оптичний

   Інформація зчитується за допомогою оптичних пристроїв. За допомогою засобів оптичної розвідки (біноклі, підзорні труби та ін.) інформацію можна дізнатися, розміщуючись навпроти вікон. Нажаль на даному об’єкт є ймовірність підглядання з вулиці.

   Застосовуючи закладні оптичні пристрої (фото- відеокамер) та підключення до внутрішнього відеоспостереження можливий витік інформації з середини приміщення.

3. Електромагнітний

Це найбільший канал витоку інформації: ПЕМВН, заземлення, зчитування інформації з електромереж.

Ризики присутні в першу чергу через те що електромережа підведена з теритрої за межами контрольованої зони.

Також на території відсутнє заземлення, що несе за собою небезпеку виведення з ладу обладнання. Тому було вирішено прокласти заземлення на території об’єкту під вікном приміщення служби безпеки, яке опускається по зовнішній стороні будівлі на 3 метра в ґрунт до контуру заземлення у вигляді рівностороннього трикутника з ребрами по 1,5 м, але під час робіт виникли складнощі з прокладанням такої схеми через виявлені комунікаційні споруди під землею, які не були вказані у технічній документації наданій установою-замовником. Тому схему було змінено з трикутника на пряму довжиною 6 метрів.

4. Матерільно-речовий

Витік інформації відбувається за рахунок потрапляння матеріальних носіїв інформації до злочинця. Даний канал витоку інформації є абсолютно людським фактором.

Нажаль у ЦСД«Промінь» було виявлено велику кількість документації, яка несе конфіденційну інформацію в тому числі персональні дані.

5.3 Розроблення комплексу ТЗІ для заданого об’єкту з урахуванням будівельних норм

Після першого огляду ЦСД«Промінь» було з’ясовано, що приміщення не підпадає під будівельні норми для комплексної системи захисту інформації і змога перебудовувати звісно відсутня.

Нажаль такі ситуації дуже поширені і треба вміти вирішувати задачі побудови якісної КСТЗІ з урахуванням таких недоліків.

Що ж саме не підпадало під норми:

1. Стіни. Окрім того, що в приміщеннях де будуть проводитися наради зовсім відсутнє екранування, стіни в деяких приміщеннях зроблені з гіпсокартонних конструкцій без наповнювача, товщиною менш ніж 15 см;
2. Вікна. На першому поверсі відсутні будь які захисні споруди для вікон. Окрім того усі склопакети виявилися однокамерними;
3. Не якісна електромережа з відсутнім заземленням;
4. Відсутність телекомунікаційних ніш для кабельних систем;
5. Повна відсутність протипожежних систем.

Тому було обговорено з представником-замовником та затверджено план по покращенню умов для якісної побудови КСТЗІ.

5.4 Передпроєкті роботи на об’єкті інформаційної діяльності

Таким чином після попереднього огляду ЦСД«Промінь» і обговорення невідповідності будівлі будівельним нормам для побудови КСТЗІ, було розпочато етап передпроєктних робіт на об’єкті інформаційної діяльності.

Першим кроком було з’ясовано, що на даному ОІД циркулює як відкрита інформація так і з обмеженим доступом. Уся інформація з обмеженим доступом є конфіденційною. Тому було складено відповідний Акт про категоріювання з яким можна ознайомитися на наступній сторінці:

Розпорядженням директора
ЦСД«Промінь» № 546 від 06 серпня 2023 року

АКТ
категоріювання приміщень, в яких розташовані та функціонують компоненти обчислювальної системи ЦСД«Промінь»

1. Підстава для категоріювання: розпорядження директора ЦСД«Промінь» №546 від 06 серпня 2023 року «Про категоріювання приміщення».

2. Вид категоріювання: первинне, актом від 14 серпня 2023 року встановлено 4 категорія.

3. На ОІД здійснюється обробка конфіденційної інформації про особу, вимоги щодо захисту якої встановлюється законодавством.

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об’єкті: конфіденційна інформація.

5. Встановлена категорія: 4 (четверта) категорія.

6. Приміщення розташоване за адресою: м. Харків, вул. Архітекторів, 358.

Голова комісії

Марія Алфьорова

_____

Члени комісії

_____ Віталій Сохніч

_____ Марина Петрова

14.08.2023 р.

Після огляду ЦСД«Промінь» на відповідність будівельним нормам було з’ясовано розміщення та характеристики усіх ОТЗС та ДТЗС (Додаток Е). З їх описом можна ознайомитися у Таблиці 5.1-2

Таблиця 5.1 – ОТЗС на ОІД ЦСД«Промінь»

№	Назва ОТЗС	Опис	Серійний номер	Інвентарний номер
ОТЗС у першій зоні (перший поверх)				
1	ПЕОМ	HP Victus 15-fb1013dx Процесор: AMD Ryzen 5 7535HS, 3,3-4,55 ГГц	6TG4563YTU	№SX10098761
2	Сканер	Plustek OpticSlim 550 Plus	GHFD7658	№SX10097682
3	Копіювальний апарат	МФУ Xerox WC 3025NI	VB45KJL678	№SX10096873
ОТЗС у другій зоні (другий поверх)				
4	ПЕОМ	HP Victus 15-fb1013dx Процесор: AMD Ryzen 5 7535HS, 3,3-4,55 ГГц	9TK4398YBN	№SX20098761
5	Сканер	Plustek OpticSlim 550 Plus	LKJU5645	№SX20097682
6	Копіювальний апарат	МФУ Xerox WC 3025NI	MJ89HGF908	№SX20096873

Таблиця 5.2 – ДТЗС на ОІД ЦСД«Промінь»

№	Назва ДТЗС	Опис	Серійний номер	Інвентарний номер
ДТЗС у першій зоні (перший поверх)				
1	Проєктор	BenQ MS550	KL453GHF	№SX10089761

2	Телевізор	Samsung UE50NU7090UXUA, 60”	GHJK8907HG	№SX10086792
3	Внутрішня АТС	Panasonic KX-TS2350UAB	HJKG0987678	№SX10087693
ДТЗС у другій зоні (другий поверх)				
4	Проектор	BenQ MS550	MN678UY	№SX20089761
5	Телевізор	Samsung UE50NU7090UXUA, 60”	FGHD4563LK	№SX20086792
6	Внутрішня АТС	Panasonic KX-TS2350UAB	GDSE4562348	№SX30087693

Після розгляду усіх ОТЗС та ДТЗС та проаналізувавши модель загроз, було складено технічне завдання, яке ґрунтується на основному завданні від представника-замовника: забезпечення безпеки відвідувачів, персоналу та інформації яка зберігається та циркулює на об’єкті.

На основі моделі загроз можна скласти наступне ТЗ:

1) фіксація відвідувачів за допомогою електронно-пропускної системи з турнікетом , а для уникнення небезпечних ситуацій зі зброєю, так як об’єкт знаходиться в близкості до територій на яких ведуться бойові дії, на КПП необхідно встановити металодетектор який при виявлені потенційно небезпечних предметів блокує турнікет на вході.
2) проведення аудитів з безпеки з кожним працівником, по результату якого він повинен підписати відповідальні договори про нерозголошення комерційної інформації.
3) необхідно встановити СКУД з відповідним розділенням об’єкту на зони з відповідними доступами.
4) задля запобігання витоку інформації по вібро-акустичному каналу усі переговори які будуть нести ризик витоку інформації будуть

проводитися у окремих кімнатах, також потрібно проводити регулярні радіомоніторинги, вікна повинні бути двокамерними, з шумоізоляцією та завішені спеціальними жалюзями. В якості захисту інформації також можна використовувати зашумлення під час переговорів, щоб уникнути витоку за допомогою ЛСАР та усіх видів вузьконаправлених мікрофонів.

5) для запобігання витоку інформації по візуально-оптичному КВІ потрібно на час нарад закривати вікна шторами, щоб уникнути зовнішнього підглядання; проводити радіомоніторинг та безконтактну перевірку відвідувачів; захистити канали передачі відео зображень з камер спостережень і не залишати без нагляду приміщення служби безпеки.
6) для уникнення витоку інформації через ПЕМВН у ОІД необхідно встановити екранування в приміщенні де ведуться переговори. Враховуючи, що електромережа підведена з теритрої за межами контрольованої зони, необхідно екранувати загальний трьохфазний кабель та взяти під контроль охорони вузол електричного з’єднання.
7) для уникнення витоку інформації через заземлення, необхідно використати багато точкову схему заземлення пристроїв. Так як заземлення на глибині 3 метрів, щоб уникнути витоку інформації через небезпечні сигнали у ґрунті, потрібно проводити регулярний моніторинг заземлення та підвищити опір на поверхні землі, наприклад розсипати пісок.
8) для контролю пересування відвідувачів необхідно встановити систему відеоспостереження з найменшими сліпими зонами.
9) для попередження пожеж, необхідне встановлення протипожежної системи.
10) для збереження безпеки людей, необхідно врахувати оповіщення про повітряну тривогу, щоб люди могли спуститися в укриття, яким виступає підвальне приміщення.

5.5 Розроблення технічного проєкту комплексу ТЗІ для ОІД

Розглянувши детально ТЗ, було розроблено детальний проєкт комплексу ТЗІ у ЦСД«Промінь», з урахуванням необхідності вдосконалення будівельних конструкцій.

З загальним планом розміщення технічних засобів можна ознайомитися на генеральних планах (Додаток Г-Д).

Опишемо технічний план згідно кожного пункту ТЗ.

1) у якості пропускної системи на КПП було обрано СКУД від українського виробника «U-Prox», а саме контролер IP-400 та зчитувачі SE mini та стійка для нього, турнікет триштанговий Tiso та металодетектор арочний ZKTeco ZK-D1065, уся схема працює за допомогою інтерфейсу RS-485, що являє собою двохпровідну лінію зв’язку. Алгоритм даної пропускної системи такий: відвідувач реєструється у охоронця (персонал має власні вже зареєстровані картки), після чого сканує картку зчитувачем і відкривається турнікет. Зчитувач знаходиться на стійці біля металодетектору, який відвідувач повинен пройти після зчитування картки, якщо спрацювання не відбулося, то турнікет залишається відкритий і людина спокійно проходить, якщо ж відбулося спрацювання, турнікет блокується і охоронець починає діяти згідно інструкцій в даній ситуації.
2) разом з установою-замовником було обговорено усі безпекові міри і складений календарний план аудитів з персоналом. Також на етапі упровадження буде складено відповідну документацію про нерозголошення інформації персоналом.
3) в доповнення до першого пункту до відповідних кімнат, а саме кімнат для наради та сервісних, буде також застосовано СКУД на основі додаткових контролерів та зчитувачів.
4) на об’єкті необхідно провести встановлення більш кращих вікон, а саме двокамерних і встановити металеві жалюзі, котрі закриваються у 3-х

основних випадках: у не робочий час, під час переговорів та якщо спрацьовуватиме датчик розбиття скла. Враховуючі сумнівні конструкції стін вирішено встановити звукоізоляцію в кабінетах для нарад. Також необхідно організувати міри з радіомоніторингу та регулярні перевірки ОІД на наявність прослуховуючих елементів.

5) для уникнення витоку по візуально-оптичному каналу, у всіх приміщеннях будуть присутні непрозорі штори, які обов'язково закриваються під час нарад. Перед кожною нарадою, проводитиметься аудит безпеки з персоналом. Усі записи з відеокамер надійно зберігаютимуться у окремому приміщенні, доступ до якого має лише служба безпеки, а до записів лише особи з відповідним доступом. Усі мережі надійно забезпечаться криптографічним захистом та файерволами.
6) проведеться робота для уникнення витоку по ПЕМВН, а саме: організаційна, екранування металевою сіткою кімнат для нарад та загальний трьохфазний кабель.
7) через труднощі які виникли при повторному огляді об'єкта і які були відсутні у наданій документації, заземлення вирішено було змінити зі схеми трикутник на пряму довжиною 6 метрів з оцинкованої стрічки на глибині 0,5 м та 3-х стержнів довжиною 3 м, які були вкопані в землю через кожні 2 м. Також регулярно проводитиметься радіомоніторинг.

8-10) у додатках наведено схему розміщення пожежної системи (для встановлення необхідно заключити договір з службою ДСНС, щоб все було встановлено згідно норм і мало ліцензію), систему відеоспостереження на основі українського виробника GreenVision та його комутацію, яка повинна бути прокладена в кабельканали. За допомогою відеоспостереження в якому використовується штучний інтелект необхідно організувати сповіщення про повітряну тривогу та необхідність переміщення людей в укриття. Також необхідно встановити систему тривожної сигналізації, а саме :датчики руху та розбиття скла, при спрацьовуванні яких, блокуються основні зони та закриваються жалюзі.

5.6 Розроблення фінансового проєкту

Фінансовий проєкт включає в себе два етапи: перший матеріали (Таблиця 5.3), другий роботи з урахуванням 5 робочих та часу в 1 місяць (Таблиця 5.4). Так як будівельні роботи та пожежну систему встановлюватимуть відповідні ліцензійовані організації окремо, то у даному фінансовому плані пункти які відносяться до них прописані загальними рядками. Також усі довжини та ціни в наведеному нижче плані є приблизними, тільки для прикладу. В усіх етапах додано фінансовий буфер, розрахунок якого ведеться з урахуванням податків, доставки матеріалів та бюджету на випадок виникнення проблем.

Таблиця 5.3 – Приклад фінансового проєкту на закупку матеріалів

Назва	Одиниця виміру	Кількість	Ціна за 1 одиницю	Ціна загальна	Коментар
Комутатор мережевий POE GV-016-D-09+2P	шт	2	1504,00	3008,00	Встановлюється на 1 та 2 поверсі, живлення камер
Маршрутизатор MikroTik hEX RB750Gr3	шт	1	2500,00	2500,00	Структурована організація мережі робочої та безпекової
Автономне ДБЖ Full Energy	шт	2	4 000	8 000	При відключенях світла приблизно година на резервному живлені, для коректного вимкнення
КАБЕЛЬ КПВ-ВП 4Х2Х0,51 (UTP 5E CAT) «ОК-NET»	м	610	13,61	8302,10	
Відеореєстратор NVR GV-N-I017/16 12MP	шт	1	4998,00	4998,00	Підтримка 16 камер , з інтелектуальними можливостями
Жорсткий диск 4TB Western Digital Purple WD43PURZ для відеоспост	шт	1	4273,00	4273,00	Запис з відеокамер на 2 тижня
Відеокамера GV-164-IP-FM-DOA50-15 (Pro)	шт	11	3000,00	33000,00	Камери антивандальні з кутом 130 градусів та нічним режимом підсвітки (8 у приміщення та 3 на території)
Мережевий фільтр PowerPlant 7 м білий 5 розеток	шт	3	360,00	1080,00	
Шафа настінна 10" 6U глибина 300 мм чорна UA-ШТК-6U-BK	шт	1	2 560	2 560	
КОРОБ ПЛАСТИКОВЫЙ 15Х10 ТЕМНО-КОРИЧНЕВЫЙ SOKOL	м	100	15,50	1550,00	
Монтажний комплект	шт	1	2000,00	2000,00	конектори RJ-45,дюбелі та саморізи, цвяхи, стяжки, гвинти, шайби,гайки
Комплект заземлення (провідник плоский 10 м, 3 стержня заземлення по 3 м, з'єднувальні елементи та Провод ПВ3 1 * 10 для заземленя 10 м)	шт	1	5500,00	5500,00	
Комплект для будівельних робіт	шт	1	100000,00	100000,00	
Комплект для протипожежної системи	шт	1	20000,00	20000,00	
			ВСЬОГО:	176771,10	
			З урахуванням буферу всього:	441 927,75	

Таблиця 5.4 – Приклад фінансового проєкту на роботи

Роботи	Ціна за одиницю	Коефіфцієнт висоти	Кількість	Сума	Коментар
Прокладання кабелю	6,00 UAH	1,5	610	5 490,00 UAH	У зв'язку з тим що стеля більше 2,5 м, то додається коефіцієнт висоти
Налаштування активного обладнання	250,00 UAH	1,0	6	1 500,00 UAH	
Збір та монтаж шафи	350,00 UAH	1,0	1	350,00 UAH	
Встановлення камери	250,00 UAH	1,0	5	1 250,00 UAH	
Встановлення реєстратора	250,00 UAH	1,0	1	250,00 UAH	
Пуско наладка відео (в годинах)	200,00 UAH	1,0	3	600,00 UAH	
Встановлення ПЗ (в годинах)	300,00 UAH	1,0	3	900,00 UAH	
Встановлення СКУД	500,00 UAH	1,0	4	2 000,00 UAH	
Пуско наладка СКУД (в годинах)	300,00 UAH	1,0	3	900,00 UAH	
Встановлення колонки	110,00 UAH	1,0	1	110,00 UAH	
Встановлення металодетектора	500,00 UAH	1,0	1	500,00 UAH	
Додаткові роботи монтажної групи (в годинах)	200,00 UAH	1,0	20	4 000,00 UAH	
Транспорт	1 100,00 UAH	1,0	10	11 000,00 UAH	
Роботи з будівництва	50 000,00 UAH	1,0	1	50 000,00 UAH	
Роботи по встановленню протипожежної систем	50 000,00 UAH	1,0	1	50 000,00 UAH	
			ВСЬОГО:	128 850,00 UAH	
			З урахуванням буферу всього:	322 125,00 UAH	

5.7 Опис упровадження та атестації комплексу ТЗІ

Закінчивши передпроєктні роботи та усі плани, було розпочато упровадження системи у ЦСД«Промінь».

Так як цей процес передбачає придбання засобів ТЗІ та іншого необхідного обладнання згідно фінансового плану , то це було першим кроком. Отримавши усі необхідні матеріали, почалися роботи з монтажу згідно ДБН та технічного плану. Процеси покращення умов у кабінетах для нарад, встановлення протипожежної системи відбувалися паралельно, разом з цими роботами упроваджувалася система СКУД на КПП та прокладався кабель у кабельний канал.

Впровадження на ОІД заходів та встановлення і налагоджування (настроювання) засобів ТЗІ здійснювалося відповідно до технічного проєкту комплексу ТЗІ та іншої проєктної документації, плану робіт з впровадження заходів із захисту інформації на ОІД, а також відповідно до технічної та експлуатаційної документації засобів ТЗІ.

Після проведення усіх монтажних та пусконалагоджувальних робіт провівся тестовий запуск для перевірки працездатності системи, під час яких виявили декілька несправностей, які змогли швидко та якісно усунути, не допустивши виникнення нових ризиків для об’єкту інформаційної діяльності.

Після завершення усіх монтажних та пусконалагоджувальних робіт провели процес розробки технічної документації на увесь комплекс. Саме на базі цих документів провівся аудит безпеки та навчання користувачів нової системи.

Для завершення створення КСТЗІ провели атестацію разом з установою-замовником, під час якої було перевірено повноту і відповідність реалізованих на ОІД заходів із захисту інформації від витоку технічними каналами, вимогам ТЗ на створення комплексу ТЗІ та вимогам НД ТЗІ. По результатам було оформлено та затверджено акт атестації комплексу ТЗІ.

Обговорено та зафіксовано у акті, що атестаційні роботи проводитимуться кожні два місяці з заповненням відповідного табелю про кожну таку перевірку і складанням акту атестації після кожної.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено нормативно-правову базу для побудови комплексу ТЗІ на ОІД та теоретичну базу ризиків для об’єкту. Також було проведено аналіз сертифікованого в Україні технічного обладнання яке можна застосовувати у КТЗІ згідно чинного законодавства.

На основі здобутих теоретичних навичок було проведено огляд та аналіз реального об’єкта в Україні. Після узгодження з установою-замовником, у пояснювальній записці наведено результати проєктно-документальної діяльності. Задля забезпечення безпеки об’єкту його назву, місце та діяльність у роботі змінено.

На основі отриманої інформації було створено проєкт і план робіт з створення комплексу ТЗІ, враховуючи:

- модель загроз для ОІД, складеної після огляду об’єкту;
- пропозиції від заявника щодо організації створення комплексу захисту;
- відомості про ОІД та вже існуючі структурні кабельні системи;
- вимоги до будівельних конструкцій режимних об’єктів;
- необхідність впровадження системи контролю доступу, врахувавши його вид та можливості підключення;
- технічні та економічні можливості установи щодо впровадження інженерно-технічних заходів з ТЗІ.

Після усіх узгоджень було проведено упровадження та атестація КСТЗІ на обраному ОІД, згідно з складеними технічним та фінансовим планом. Створений повний комплект документації в якій наведена вся інформація про упроваджений КСТЗІ.

Задачею кваліфікаційної роботи було практично та теоретично дослідити процес побудови КСТЗІ на ОІД. Навчитися аналізувати обстановку на ОІД та виявляти ТКВІ. Засвоїти навички розробки технічних пропозицій по побудові КСТЗІ з складанням технічної документації згідно нормативно-правової бази. Усі задачі кваліфікаційної роботи успішно виконані.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. ТПКО – 95. Тимчасове положення про категорювання об'єктів.
2. ДСТУ 3396.1–96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
3. ТР ТЗІ–ПЕМВН–95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань та наводок.
4. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»
5. НД ТЗІ 3.7- 001- 99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»
6. НД ТЗІ 3.1-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи»
7. ДБН А.2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва
8. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27 вересня 1999 року №1229.
9. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інфоромації. Навч. посібник / С. Іванченко та ін. Київ : ІСЗЗІ НТУУ«КПІ», 2016. 104 с.
10. Носов В., Манжай О. . Організація та забезпечення безпеки інформації. Навч. посібник. Харків : ХНУВС, 2007. 155 с.
11. Конспект лекцій по курсу «Методи та засоби захисту інформації»
12. Конспект лекцій по курсу «Технічні канали витоку інформації»
13. Конспект лекцій по курсу «Нормативно-правове забезпечення інформаційної безпеки»
14. Конспект лекцій по курсу «Технічні засоби охорони об’єктів»