КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

До захисту допущено: «На правах рукопису»
Завідувач кафедри _____ Ігор АНІСІМОВ
« __ » червня 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«ЗАХИСТ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ТА ВІДЕОСПОСТЕРЕЖЕННЯ В ДЕРЖАВНІЙ УСТАНОВІ»

Виконав:
студент 4-го курсу
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОП «Інформаційна безпека телекомунікаційних систем і мереж»
Горський Олег Олексійович _____

Науковий керівник:
к.в.н., доц. Довбня Сергій Якович _____

Рецензент:
к.в.н., доц. Шульга Владислав Сергійович _____

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____

Робота допущена до захисту в ЕК рішенням кафедри радіотехніки та радіоелектронних систем від «23» червня 2023 р., протокол № 22.

Завідувач кафедри радіотехніки та радіоелектронних систем,
доктор фіз.-мат. наук, професор
Анісімов Ігор Олексійович _____

Київ – 2023

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

СКД – система контролю доступу

ВС – відеоспостереження

ДУ – державна установа

НСД – несанкціонований доступ

ТКВІ – технічні канали витоку інформації

КСЗІ – комплексна система захисту інформації

ТЗІ – технічний захист інформації

ТКВІ – технічний канал витоку інформації

ЗІ – захист інформації

ТЗ – технічне завдання

ВСТУП

Інформаційна сфера відіграє все більшу роль у забезпеченні безпеки держави і суспільства. Саме через цю сферу реалізується значна частина загроз національній безпеці держави. Основними джерелами загроз інформаційної безпеки є діяльність іноземних спецслужб, кримінальних угруповань та організацій, а також протизаконна діяльність окремих осіб, спрямована на збір, викрадення та розповсюдження (продаж) цінної інформації, закритої для доступу сторонніх осіб [1-5]. Тому проблема надійного захисту інформації в різних організаціях та установах в сучасних умовах є досить актуальною.

За останні роки, завдяки стрімкому розвитку сучасної науки та техніки, з’явилася велика кількість пристроїв, які використовуються в системах контролю доступу та відеоспостереження (далі СКД ВС).

Також лля державних закладів існують вимоги щодо обмеження доступу до структури та характеристик таких систем захисту інформації та захисту від спеціального впливу [6-8].

Створення систем захисту інформації передбачає проведення визначеної послідовності робіт щодо обстеження, оцінки ризиків, проектування системи та оцінки ефективності методів та заходів захисту інформації від несанкціонованого доступу, витоку технічними каналами та спеціального впливу [9-12]– тому потрібно обрання моделі та методики такої оцінки.

РОЗДІЛ 1. АНАЛІЗ СТАНУ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз завдання на створення СКД ВС в державній установі

Вихідні дані для створення системи контролю доступу та відеоспостереження наведено в Додатку А.

На підставі [13-18], СКДВС є інформаційно-комунікаційною системою класу 2 (локальна автоматизована система). В цій системі передбачається обробка службової інформації, тому потрібно створити систему захисту інформації.

Для подальшого створення СКД ВС, нам потрібно розібрати та проаналізувати, що повинно використовуватися в фінальному варіанті.

В аналізі будуть враховані недоліки, переваги наявних СКД ВС, будуть запропоновані нові варіанти СКД ВС, які в подальшому замінять наявні системи.

- Недоліки наявних СКД та ВС:
  - Застарілість систем;
  - Залежність від старого ПЗ;
  - Складність технічної підтримки;
  - Високий рівень енергоспоживання;
  - Низька кількість спеціалістів, які знайомі з наявним СКД та ВС;
  - Висока вразливість до хакерських атак;
- Переваги наявних СКД та ВС:
  - Низька ціна на придбання системи;
  - Простота у встановленні приладдя;
  - Довготривала дія приладдя;

Як бачимо, згідно проведеного аналізу – ми маємо шість масштабних недоліків існуючих СКД та ВС, які шкодять безпеці державної установи та мають бути вирішені.

Найбільш поширеним недоліком нинішніх СКД та ВС – те що, вони використовують застарілі приладдя та програмне забезпечення, яке ймовірно не оновлюється роками. Завдяки цьому зловмисники можуть спробувати та цілком успішно обійти СКД та ВС, задля незаконного проникнення на територію об’єкта державного значення.

Виходячи з цього аналізу, ми можемо створити нову, сучасну та більш забезпечену систему контролю доступом та функціональну систему відеоспостереження.

Для потрібно, щоб нова система підходила під бажані параметри, які будуть зазначені нижче:

- Найдовший термін придатності;
- Висока якість запису та зображення;
- Використання сучасного ПЗ;
- Можливість збереження інформації у хмарних/фізичних носіях;
- Низька або нульова вразливість до хакерських атак з боку зловмисників;
- Використання абсолютно нового приладдя;
- Підвищення кваліфікації спеціалістів з безпеки;

Маючи на руках такі умови, ми маємо змогу створювати абсолютно нові СКД та ВС у державних установах.

1.2 Аналіз та обрання засобів для створення СКД ВС

Для обрання засобів щодо створення СКД ВС, було проведено аналіз [27-30] ринку засобів та прийшли до логічного висновку стосовно умови задачі.

Щодо самого обрання засобів – треба зрозуміти, що є декілька засобів створення, які суттєво відрізняються між собою.

Самі СКД ВС можуть мати один з двох типів з’єднань: провідне та безпровідне. Стосовно самих систем вони можуть бути або сумісні між собою, або різні, але з’єднанні на різних системах.

Порівняльний аналіз переваг та недоліків бездротових та провідних технологій наведено в таблиці 1.

Таблиця 1.

Безпровідні пристрої та камери	Провідні пристрої та камери
Використання автономних блоків живлення	Можуть живитися по лінії, та з’єднуватися по інтернет-з’єднанню
Завантажує відео у хмару чи локальний накопичувач	Дані, які записує камера зберігаються у відеореєстраторі
Не потребує створення структурованої кабельної системи (СКС)	Потребує з’єднання по кабелю та монтаж СКС
Можуть працювати в автономному режимі з подальшим збереженням інформації на карті пам’яті	Можуть працювати в автономному режимі з подальшим збереженням інформації на карті пам’яті (якщо воно встановлено)
Працюють з використанням Wi-Fi мережі	Працюють з використанням СКС (кабельні, ВОЛЗ)
Не потребує кабельного з’єднання, але знижена дальність передачі інформації сягає до 15-25 метрів	Довжина з’єднувальних ліній від 200 до 2000 метрів
Швидкість передачі інформації віл 54-100 Мбіт/с	Швидкість передачі інформації сягає від 100 Мбіт/с

Виходячи з даного аналізу вигідно було би взяти пристрої безпровідного з’єднання, але основними мінусом таких пристроїв є те, що вони вразливі до хакерських атак (незахищені протоколи). Також до головного плюсу провідних пристроїв можна віднести, те що флеш-порт, який використовується для запису пам’яті опечатується, що зумовлює підвищення безпеку записаних даних з камер спостереження. Тому оптимальним варіантом може бути обрання провідних пристроїв.

1.3 Методика створення СКД ВС

Під методикою створення СКД ВС розуміється, що саме створення такої комплексної системи має на собі комплексну методику, яка на виході допомагає повноцінно створити вищезазначені системи.

У даному підрозділі буде описана дана методика та її імплементація в нашому проекті.

Важливо розуміти, що методика створення СКД та ВС є невід’ємною частиною в розробці системи безпеки будівель, територій та приміщень загалом й без цієї методики неможливо розробити якісну систему, яка буде діяти у довготривалий термін.

Згідно з [16-25] основними складовими створення створення СКД ВС є:

- Визначення потреб СКД та ВС;
- Вибір компонентів вищезазначених систем;
- Розробка схеми системи;
- Інсталяція компонентів системи;
- Конфігурація системи;
- Тестування системи;
- Фіналізація та ввід у експлуатацію;

Під визначенням потреб СКД та ВС мається на увазі, що розробники повинні визначити мету створення необхідної системи, визначення дислокації, де буде розміщена система з потребою в захисті. Для цього виникає потреба визначення необхідного рівня безпеки та тип приміщення, який має бути під захистом – також враховуються подальші ризики безпеки.

Після визначення потреб, йде етап вибору компонентів. Вони повинні відповідати потребам безпеки та особливостям території, яка буде

охоронятися. До компонентів, які будуть використані відносяться камери, системи контролю доступу, сирени, електронні замки і тд., але про компоненти згадка буде в подальших розділах даного проекту.

Маючи готові потреби та визначені компоненти, далі можна приступити до розробки схеми проекту. У даній схеми повинні бути зазначені місцезнаходження камер з радіусом їх дій, розміщення систем контролю доступу, перелік програмного забезпечення, яке буде інстальовано у систему, мережеве обладнання, яке вмонтоване у приміщенні та інші потрібні для проекту компоненти.

Інсталяція компонентів системи – має за собою мету фізичне встановлення обраних компонентів системи по заданих на схемі місцях. Наприклад, встановлення систем відеоспостереження буде вимагати додаткового проведення кабелів в приміщенні, що є головною частиною побудови кабельної інфраструктури.

Налаштування системи проходить вже після інсталяції системи, і в даному етапі вже проводять систему конфігурацію системи, а саме: встановлення програмного забезпечення, налаштування камер та систем контролю доступом, проведення конфігурації мережі до яких будуть з’єднанні камери, контролери доступу та інші компоненти.

Тестування системи – після інсталяції та налаштування системи, настає етап тестування. У даному етапі проводиться тестовий запуск системи, де розробники визначають технічні, програмні та ймовірні фізичні проблеми, які можуть виникнути під час тестового запуску. В разі негативних результатів, розробники переглядають компоненти системи, де вирішують або їх замінити на більш нові, або спробувати їх полагодити до стану, що ввести у режим експлуатації.

Фіналізація та ввід у експлуатацію – на даному етапі завершуються усі приготування, тестування та ведеться підготовка до введення системи в стан експлуатації. Фіналізація є обов’язковою частиною в даній методиці.

1.4 Розробка та обґрунтування варіанту СКД ВС ДУ

Обладнання, яке буде далі обрано треба розмістити таким чином, щоб їх ефективність була на максимумі під час експлуатації. В даному проекті буде використано два поверхи умовної державної установи, в якій розташують обране обладнання. Схема нижнього поверху присутня в Додатку А.

Згідно схеми нижнього поверху, ми розташувати камери безпеки на вході поверху та посередині коридору, який простягається вздовж поверху. Також на вході до поверху варто розмістити сканери відбитків пальці або сканер, який призначений для сканування карток.

Камери спостереження на поверсі для повного радіусу спостереження повинні бути виключно купольними з можливістю повороту на 360 градусів.

Як й з верхнім поверхом ДУ, уся ця система буде централізованою та матиме керування з окремої кімнати, яка розташовуватиметься на верхньому поверсі. Схема верхнього поверху присутня в Додатку Б.

Верхній поверх відрізняється тим, що до нього є невеликий прохід з нижнього поверху, і там в коридорі можна розмістити декілька купольних камер, які зможуть охопити повністю весь коридор. Також можна розмістити турнікет або замок з розпізнаванням особливих карток пропуску.

Окремо варто додати до кожного входу в кімнату спеціальні системи розпізнання відбитків пальців (як на нижньому).

На верхньому поверсі можна побачити невелику кімнату, де можна розмістити кімнату оператора, який буде контролювати систему безпеки.

Варто уточнити, що вибір купольних камер пояснюється тим, що камери, які не мають поворот - не зможуть повністю охопити увесь коридор приміщення.

Окремо треба додати, що кімната оператора буде поряд із серверною, яка буде також мати власну роль в організації системи безпеки. Так як наявність деяких програм та працездатність самої ВС та СКД потребують того, щоб був сервер.

Також саме розташування обладнання залежить від потреб організації або державної установи. Особливо воно повинно дотримуватися зазначених вимог безпеки та конфіденційності даних, які будуть оброблюватися.

Сама СКД та ВС складається з наступних елементів:

1) Підсистема контролю доступу: Картки; спеціальні пропускні браслети; сканер відбитків пальців і тд;
2) Підсистема відеоспостереження: Відеокамери (будь-яких видів), кабелі і тд;

Під час обрання обладнання, враховувалося технічні характеристики (їх переваги), що унеможливить або зменшить ризик проникнення на територію ДУ.

До обрання належного варіанту треба орієнтуватися згідно технічного облаштування даних систем. Як можемо спостерігати, потрібно обрати спеціальні пропускні картки та сканери карток, так й купольні відеокамери для ВС.

Відеокамера було обрано за наступними показниками:

- Можливість повороту;
- Якість зображення;
- Можливість запису відео;
- З’єднання за дротом;
- Роздільна здатність камери;

Перед вибором з’явились дві камери: одна IP-камера купольна, друга HDTVI-камера купольна. Характеристики наведено в додатку Б.

Суттєва відмінність цих камер між собою полягає в їх конструкції, та їх особливостях наприклад в наявності інфрачервоної підсвітки або можливості нічної зйомки.

Враховуючи переваги та недоліки характеристик, більш оптимальним та вигідним вибором буде **IP-відеокамера Hikvision DS-2CD1121-I(F)**.

За таким же принципом було обрано інше устаткування: комп’ютери для керування СКД та ВС, електромагнітний замок, контролер доступу, блок безперебійного живлення, жорсткий диск для збереження інформації, яка буде оброблена в ВС та разом з цим відеореєстратор, який буде обробляти цю інформацію.

Специфікацію обладнання їх основні технічні характеристики наведено в Додатку Б.

Наступними будуть комп’ютери з моніторами як для СКД так й для ВС, вони потрібні для оперування та системним оглядом території, яка оглядається системами безпеки.

Основні засоби, які обробляють інформацію в СКД ВС наведено в таблиці 2.

Таблиця 2.

Тип приладу	Найменування	Кількість
Монітор	24.5 AOC 25G3ZM/BK	2
Зчитувач	Mifare ATIS PR-08 MF-W (black)	4
Контролер	NDC F18IP (U-Prox IP400)	1
Комутатор	TP-LINK TL-SF1008D	1
Комп’ютер	ARTLINE Business B29 v31Win	2
Жорсткий диск	Western Digital Red SA500 SSD 2TB 2.5” SATA III	1
Камера відеоспостереження	IP-відеокамера Hikvision DS-2CD1121-I(F)	3

Відеореєстратор	GreenVision GV-N-I017/16 12MP	1

Повну специфікацію засобів та послуг для створення СКД ВС ДУ наведено в таблицях Б.1, Б.2 Додатку Б.

Запропонований варіант СКД ВС ДУ

Для повноцінної роботи СКД ВС ДУ треба виокремити наявність функціональної схеми, яка буде пояснювати як працюватиме дана система та з чого вона складається. Фукнціональна схема СКД ВС ДУ представлена на рис. 3 в Додатку Б.

На даній схемі зображено наступні елементи: підсистем СКД та ВС, що контролюються окремо на двох комп’ютерах, та з’єднані до одного сервера (в майбутньому).

ВС працює наступним чином: камери передають інформацію на мережу по зашифрованому відео-ефіру. Оброблена інформація йде до декодеру, яка дешифрується та відправиться до пул зображень. Звідти відео направляється до системи обробки, де воно після процесу йде до логічної одиниці та на вихід. З виходу воно йде до першого персонального комп’ютера, де після воно зберігатиме на першому виділеному сервері для даного комп’ютера.

СКД складається та працює за таким принципом дії: працівник установи прикладає відбиток або пропускну картку до зчитувача, де останній передає сигнал до другого СКД. Другий СКД з отриманої інформації передає сигнал, щоб відкрити замок на двері та впустити робітника – другий персональний комп’ютер, що з’єднаний з другим виділеним сервером має інформацію про всіх працівників, таку як відбитки пальця або спеціальні пропускні картки.

У випадку з першим СКД, воно відрізняється тим, що воно має кнопку зі сторони виходу, для того аби оператор міг відкрити двері у випадку, якщо зчитувач не зміг розпізнати відбиток пальця/картку пропуску, або якщо працівник є новим в установі та немає пропуску. За принципом дії воно працює так само як й другий СКД. Усі вони з’єднанні з другим комп’ютером.

Опис функціонування СКД ВС ДУ

СКД ВС ДУ є комплексною системою, яка складається з багатьох компонентів у яких є головна особистість – повна взаємодія підсистем СКД та ВС між собою. Ця взаємодія випливає з того, що оператор безпосередньо керує як СКД, так й ВС.

Сам СКД ДУ складається з декількох частин, таких як:

- Електромагнітні замки;
- Безперебійний блок живлення;
- Ідентифікатор відбитків/карток;
- Картки для пропуску;
- Кнопка тривоги;
- Сирени;

Електромагнітні замки є ефективними та доцільним елементом в будь-якій системі безпеки. За принципом роботи вони отримують сигнал з ідентифікаторів відбитків або карток, які розташовані біля самих дверей – якщо пропуск або відбиток пальця розпізнається в базі даних, то відповідна команда буде подаватися на контролер замка, який дасть людині доступ до установи. В противному випадку, людина не отримує доступу до приміщення.

Безперебійний блок живлення потрібний для того, щоб в разі екстреного вимкнення енергії апаратне забезпечення могло працювати й далі допоки не відновиться електропостачання в будівлі. У разі відсутності такого

блока живлення система безпеки вийде з ладу та підвищить шанси проникнення зловмисниками.

Ідентифікатори відбитків або карток потрібні для того аби зменшити ризик проникнення на територію установи небажаними особами. По принципу дії такі ідентифікатори зв’язані з серверною частиною СКУД, де зберігається потрібна інформація для пропуску (тобто відбиток пальця або відсканована картка пропуску) – при розпізнаванні відбитка або картки, буде подаватися команда на контролер електромагнітного замка, яка відповідає за відкриття дверей.

Кнопка тривоги виконує функцію подачі сигналу аби сповістити персонал установи про надзвичайну ситуацію. Сигнал з кнопки передається на пристрій, який надає сповіщення у вигляді гучного звуку (на кшталт сирени) усьому персоналу та передати непомітно інформацію про порушення до органів правопорядку.

Сирени виконують роль пристрою сповіщення, які отримують сигнал з кнопки тривоги та подають сповіщення до всіх людей, що знаходяться на даний момент у приміщенні.

ВС також складається з декількох частин та безпосередньо, як й СКД керуються оператором. До ВС ДУ входять такі прилади:

- Відеокамери;
- Відеореєстратори;
- Комп’ютер;
- Жорсткий диск;

Відеокамери виконують роль спостереження за приміщенням та передають інформацію на комп’ютер оператора, де він власне аналізує в реальному часі стан безпеки кімнати/коридору тощо.

Відеореєстратор зберігає в своїй пам’яті запис з відеокамери та в разі чого усю інформацію збережену там можна викачати до жорсткого диску.

Комп’ютер виконує задачу керування камер спостереження та відеореєстраторів, разом з цим він з використанням жорсткого диску зберігає та оброблює інформацію, яка надходить з камер та реєстратора. Це дозволяє оператору сортувати, корегувати та зберігати отриману інформацію.

Жорсткий диск обробляє отриману інформацію та зберігає її для подальшого використання.

Висновки

Проведений аналіз вихідних даних, різних технологій побудови сучасних систем контролю доступу та відеоспостереження а також особливих умов експлуатації даної системи в державній установі дозволів надати пропозиції щодо створення системи контролю доступу та відеоспостереження, а саме:

- обґрунтувати функціональний склад СКД та ВС;
- обрати пристрої та засоби для побудови СКД ВС ДУ.

При забезпеченні особливих умов:

- обмеження доступу до структури та характеристик реальних систем;
- забезпечення захисту інформації від витоків технічними каналами, несанкціонованого доступу та спеціального впливу.

1. Для обґрунтування функціонального складу СКД та ВС, було проведено порівняльний аналіз технологій використання бездротових та провідних датчиків та камер, для подальшого ескізного проектування СКД ВС ДУ.
2. Було визначено основні технічні вимоги до варіанту СКД ВС ДУ. Технічні вимоги поділяються на два напрямки: вимоги програмного забезпечення та вимоги до технічних засобів. З врахуванням

цього здійснювалось обрання комплектуючих та програмного забезпечення для створення захищеної СКД ВС.

3. В подальших розділах потрібно провести оцінку ризиків захисту Системи контролю доступу та відеоспостереження державної установи та розробити рекомендації щодо захисту інформації від несанкціонованого доступу, витоку технічними каналами та спеціального впливу.

РОЗДІЛ 2. ПЕРЕДПРОЄКТНІ ДОСЛІДЖЕННЯ СКД ВС ДУ

У зв’язку з необхідністю створення захищеної системи контролю доступу та відеоспостереження державної установи - обрано загальний порядок проведення робіт при створенні комплексної системи захисту інформації в інформаційно-комунікаційних системах.

Особливості створення КСЗІ СКД ВС наведено в Додатку В. При цьому враховано вимоги щодо оцінки ризиків функціонування підсистем контролю доступу та відеоспостереження.

Методика оцінки ризиків є ключовою стадією в розробці будь-якої інформаційно-комунікаційної системи, так як вона допомагає передбачити ймовірні ризики та вчасно попередити.

Методики оцінки ризиків обрано згідно з рекомендаціями ДСТУ IEC/ISO 31010:2013 «Методи загального оцінювання ризику. Керування ризиком».

Треба враховувати, що сама система контролю доступу може бути розміщена як назовні, так й всередині будівлі, де вона буде експлуатуватися. В нашому випадку СКД буде розміщено всередині будівлі. Варто також врахувати, що загальною задачею методики оцінки ризиків є попередній аналіз небезпечних чинників (будь-то особа, чи небезпечне ПЗ або інші чинники спеціального впливу).

Для подальшого оцінювання ризиків, ми повинні передбачати те, які можуть бути ймовірні технічні проблеми в функціонуванні системи, умисна несправність технічного обладнання, спричинення несправності через особливі чинники (в даному випадку перепади напруги на генераторі, тощо).

Оцінка ризиків здійснюється з метою, аби мати впевненість та провести деякі підготовчі дії внаслідок виникнення подібної проблеми, яка мала місце в даній оцінці.

На даний момент, ми можемо позначити п’ять класів ризиків, які можуть статися під час експлуатації нашої системи.

- Клас 1: Загрози, що пов’язані зі терористичною діяльністю;
- Клас 2: Загрози, що пов’язані з технічними проблемами;
- Клас 3: Загрози, що мають техногенний характер;
- Клас 4: Загрози з боку зовнішніх порушників;
- Клас 5: Загрози з боку внутрішніх порушників;

Оцінка ризиків в основному приводиться у вигляді таблиці, якаи зображує ту чи іншу загрозу.

Також ризики несанкціонованого доступу визначаються методом Дельфі, який передбачає собою системний збір інформації про об’єкт, та прогнозування експертів з безпеки й подальшого узагальнення отриманих даних.

До ризиків НСД, варто додати ризики витоку технічними каналами, що являють собою сукупність джерел небезпечних сигналів та середовищ, які поширюють небезпечні сигнали, які можуть бути отримані засобами технічної розвідки. Їхнім аналізом займаються за допомогою НАССР, який ще передбачає аналіз та попередження ризиків, що спричинені спеціальним впливом.

Загальна оцінка ризиків проводиться створенням та внесенням в модель загроз, модель порушників, політику безпеки усіх показників ризиків разом із з їх чинниками та рекомендаціями щодо прийняття ризиків, що є підгрунтям до формування вимог до захисту інформації в СКД ВС. Детальний порядок створення КСЗІ СКД ВС наведено в Додатку В.

2.1 Розробка моделі загрози

Розробка моделі загрози є однією з трьох ключових моментів в розробці захищеної системи безпеки. Завдяки цієї моделі компанія може створити надійну та якісну систему захисту, яка матиме низький або нульовий ризик обходу зловмисниками.

Сама побудова моделі загрози вимагає уточнювати такі деталі як: персонал організації, технічні умови, спеціальні умови, тощо. Враховуючи, що моя задача в даній роботі є створенням більш нової та захищеної системи безпеки в державній установі, треба враховувати усі можливі чинники.

Розроблену модель загроз (за методом Делфі) наведено в таблиці 3.

Таблиця 3.

Позначення	Назва загрози	Рівень загрози
П1	Порушення конфіденційності	5
П2	Порушення доступності інформації	4
П3	Порушення цілісності	4
П4	Порушення керованості та спостереженості ВС	3
П5	Порушення керованості СКД	3

Дана модель загрози показує, що порушення конфіденційності є першим пріоритетом в цілях зловмисників, окрім цього в другому пріоритеті стоять порушення доступності інформації та цілісності системи – що буде ускладнювати подальшу роботу системи безпеки та наявної інформації, яка зберігається в цілому. Останнім пріоритетом вже йде порушення керованості системи відеоспостереження та СКД – ця ціль полягає в тому, що зловмисники планують обійти усі можливі системи аби дійти до самої мети – порушення конфіденційності інформації, яка зберігається в державній установі.

Моделі загрози допомагають розробникам системам безпеки вдосконалити свої ідеї, переглянути можливі прогалини в самій системі та докорінно їх усунути, аби вийшла повноцінна система безпеки.

Маючи готову модель загрози вже можна перейти до розробки моделі порушника.

2.2 Розробка моделі порушника

Разом з розробкою моделі загрози, повинна також розроблюватися модель порушника.

Модель порушника показує умовний портрет зловмисника, який намагатиметься обійти систему захисту задля своєї мети. При розробці даної моделі треба враховувати такі чинники: перевірка бази даних співробітників, моніторинг зв’язку співробітників під час роботи у державній установі, тощо.

Порушники згідно моделі поділяються на дві категорії: **зовнішній** та **внутрішній**. Ці категорії дуже сильно відрізняються між собою, і нижче буде їх детальний опис.

Зовнішній порушник – це порушник, який не має відношення до установи, до якої він хоче проникнути та вчинити злочин. Але він має змогу нанести фізичної та/або технічної шкоди встановленому обладнанню. На відміну від **внутрішнього порушника** він не має доступу до програм керування обладнанням та не може звідти вимкнути усю систему безпеки.

Внутрішній порушник – це порушник, який має безпосереднє відношення до систем безпеки та має змогу отримати контролю даної установки. Такий порушник здатен або вимкнути систему, або передати її під дистанційний контроль зловмисників.

В даній моделі ці типи порушники розглядаються таким чином:

- Зовнішній порушник не має доступу до внутрішнього керування системою, але має можливість взаємодіяти з елементами системи (камери, турнікети тощо);

- Внутрішній порушник має доступ до внутрішнього керування, а також здатний передати контроль над всією системою, або взагалі її вимкнути на деякий період часу, який потрібен зловмисникам;

Згідно такої класифікації, ми можемо з впевненістю сказати, що рівень загрози однаковий, як від внутрішнього так й від зовнішнього порушника. Враховуючи, що система розробляється під використання в державній установі, то в даному випадку – зовнішній порушник має більш високу ймовірність мати високий рівень загрози.

Таблиця 4. модель порушника

Позначення	**Визначення категорії**	**Потенційний рівень загрози**
П1	Системний адміністратор	4
П2	Адміністратор безпеки	4
П3	Охоронці	3
П4	Персонал, який обслуговує будівлю та приміщення в якій розташовано систему	5
П5	Технічний персонал (інженери)	5
П6	Представники організації	1
П7	Сторонні особи	5

На даній таблиці ми бачимо, що найвищий рівень потенційної загрози несуть як технічний персонал, так й персонал, що обслуговує будівлю та приміщення, разом зі сторонніми особами.

2.3 Результати оцінки ризиків функціонування СКД

Нижче буде зображено приклад таблиці на якій буде зображено можливу загрозу та чинники, які будуть з нею пов’язані.

Таблиця 5. Оцінка ризиків функціонування СКД та ВС в ДУ

Клас загрози	Чинники загрози
Клас 1. Загрози, що пов’язані з терористичною діяльністю	Збройний напад на державну установу;
Клас 2. Загрози, що пов’язані з технічними проблемами	Перевантаження напруги на живленні; Коротке замикання на деяких приладах СКД та ВС;
Клас 3. Загрози, що мають техногенний характер	Помилка проектування СКД та ВС; Порушення правил експлуатації СКД та ВС в ДУ;
Клас 4. Загрози з боку зовнішніх порушників	Несанкціоноване проникнення на територію ДУ; Пошкодження СКД та ВС в ДУ;
Клас 5. Загрози з боку внутрішніх порушників	Несанкціонований доступ до секретної інформації; Крадіжка секретної інформації;

Згідно цієї таблиці, ми будемо в змозі розробити досконалу систему безпеки та унеможливити, як саме НСД до державної установи, так й до самої СБ.

2.4 Обрання засобів радіомоніторингу та вимірювальних засобів

Засоби радіомоніторингу потрібні для створення СКД та ВС в державній установі аби запобігти появі закладних пристроїв у будь-якому елементі СКД ВС ДУ, починаючи від камер та закінчуючи електромагнітними замками.

Засоби радіомоніторингу поділяються на три типи: портативні, стаціонарні та мобільні. Вони дуже суттєво відрізняються собою, як за назвою, так й за характеристиками функціоналу.

- Портативні – їх можна створити з будь-якого пристрою, який використовується в повсякденному житті, буцімто телефон чи планшет, СПЗ та SDR приймача.
- Стаціонарні – відрізняються тим, що вони є цілим комплексом, ціль яких полягає в тому, що застосовуються для проведення спеціальних досліджень радіоелектронних засобів.
- Мобільні – є більш переносними та ефективними завдяки власній мобільності, вони бувають як радіовиявлячами, аналізаторами спектру, так й засобами виявлення закладних пристроїв.

Для виявлення ТКВІ в організаційних установах використовувались портативні та мобільні засоби радіомоніторингу, також дані пристрої дозволяють виявляти електромагнітні випромінювання та наведення, які видають закладені засоби.

Для нашої задачі ми використовували мобільний комплекс радіомоніторингу Delta4G з наступними характеристиками:

Призначення	Виявлення ІЧ, радіо-, проводових закладних пристроїв (СПЗ – Didgiskan), вимірювання ПЕМВН (СПЗ – Spice)
Склад комплексу	USB- спектраналізатор SA44BB Комплект пошукових та вимірювальних антен, струмознімач, пробник напруги (калібровані та з метрологічною повіркою)
Діапазон частот	50 кГц – 4.4 ГГц
Швидкість аналізу	75 МГц/с
Режими роботи	РЧ Пошук, Детектор-Локалізація

Таблиця 6. Характеристики обраного засобу радіомоніторингу

2.5 Вимоги до створення КСЗІ СКД ВС ДУ

Для створення самого КСЗІ СКД ВС ДУ, треба розуміти що значить саме КСЗІ.

КСЗІ – це комплексна система захисту інформації, яка є взаємопов’язаною сукупністю інженерно-технічних, організаційних заходів, методів та засобів ЗІ (захист інформації).

В даному випадку, КСЗІ СКД ВС ДУ полягає в тому, що буде ставити за питання інформаційну та фізичну безпеку державної установи у якій буде вмонтована дана система. Це пояснюється наступним чином: будь-яка технологічна інформація повинна підлягати захисту в категоріях конфіденційності, цілісності системи – оскільки від цього залежить керованість СКД та ВС.

Також фізичний захист має за собою наступне обґрунтування: система живлення СКД та ВС, а й взагалі усієї ДУ залежить від умовних електричних щитків, трансформаторів – такі об’єкти повинні мати деяку посилену охорону та систему спостереження, так як вони є ціллю вищого пріоритету для знешкодження працездатності самих СКД та ВС.

Тому до основних вимог КСЗІ даного проекту повинні відноситися такі аспекти:

- СКД ВС повинні забезпечувати захист від несанкціонованого проникнення у ДУ;
- Захист СКД ВС від фізичної взаємодії з боку порушників;
- Захист ДУ від діяльності внутрішніх порушників;
- ВС повинні забезпечувати повноцінний захист ДУ, як ззовні, так й всередині самої організації;
- Захист від несанкціонованого отримання інформації, яка зберігається в ДУ;

- Контроль та цілісність працездатності СКД та ВС в межах ДУ;
- Мінімізація можливих наслідків в разі загрози, яка несе характер кібератаки (на сервер і тд.);
- Реєстрацію спроб несанкціонованого проникнення на територію ДУ;
- Реєстрація подій, які пов’язані із доступом до ресурсів активного мережного обладнання, та реакцію на факти порушення;
- Мережеве та фізичне розділення СКД та ВС, й внутрішньої мережі передачі даних (сервер);

Також КСЗІ СКД ВС ДУ повинен мати рівень забезпечення прав доступу до контролю та подальших маніпуляцій з обладнанням:

- Оператор;
- Адміністратор бази даних;
- Адміністратор системи безпеки;
- Системний адміністратор;
- Мережевий адміністратор;

Функціонування СКД ВС ДУ залежить в першу чергу від того, чи відповідає воно умовам функціонування КСЗІ СКД ВС ДУ.

Робота вищезазначених адміністраторів здійснюватися повинна в окремому середовищі, яке розміщено в межах захищених інформаційних об’єктів, місць, які грають критичну роль в функціональності СКД та ВС. Вона повинна забезпечуватися в обсязі, які необхідні для виконання службових зобов’язань даних працівників, та у межах розташування доступу до СКД, ВС. Також періодичність контролю повинно визначатися загальним календарним планом захисту інформації.

КСЗІ СКД ВС ДУ обов’язково повинно пройти державну експертизу, які відповідають чинному законодавству України. Під час проведення експертизи, засоби захисту, які на момент проектування КСЗІ не мали тоді

експертних висновків або сертифікатів відповідності, повинні бути оцінені належним чином.

РОЗДІЛ 3. ПРОЕКТУВАННЯ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ОБ'ЄКТІВ СКД ВС ДУ

3.1 Оцінка захисту інформації СКД ВС ДУ без впровадження методів та заходів технічного захисту

Оцінку захисту інформації проведено для варіанту СКД ВС ДУ наведеному в розділі 1.

На сьогодні рівень ефективності систем і комплексів технічного захисту інформації (КТЗІ) на об'єктах інформаційної діяльності (об'єктах електронної техніки) напряму залежить від забезпечення заданого рівня захисту за мінімальних матеріально-технічних витрат. Створення зазначених систем і комплексів на об'єктах фактично відбувається за результатами їх обстеження без проведення попередніх оцінок загроз і шкоди (втрат) від їх можливої реалізації, які складають основу моделі загроз інформації від витоку технічними каналами та спеціального впливу. На підставі рекомендацій [23, …..] визначено, що побудова МЗ складає основну частину передпроектних досліджень з ТЗІ і забезпечує прийняття первинних проектних рішень, розробку проекту технічного завдання на створення комплексних систем (комплексів) захисту інформації і визначення попередньої вартості цих заходів.

Для розробки адекватної моделі загроз від витоку інформації технічними каналами або для захисту від спеціального впливу – рекомендовано проводити ряд заходів, а саме:

- Обстеження об'єктів інформаційної діяльності (фізичного середовища ОІД);
- інженерно-технічний аналіз та Спеціальні дослідження основних технічних засобів, що обробляють інформацію (ОТЗ) ;

- Спеціальні дослідження ОІД (виток мовленнєвої інформації, властивості захисту від спеціального впливу);
- Інженерний аналіз та Спеціальні дослідження допоміжних технічних засобів та систем (ДТЗС).

По-перше потрібні дані сигнали, що циркулюють як у зовнішніх (міжблокових), так і внутрішніх (між вузлових) інтерфейсах передачі інформації СКД ВС (функціональна схема наведена на рис. 3, специфікація у Додатку Б). При цьому, відповідно до різновидів сигналів та особливостей побудови інтерфейсів спряження, ступені загроз (від вищого до нижчого) утворенню каналів витоку інформації розподіляються таким чином:

- сигнали відеозображень;
- сигнали передавання даних зі зчитувача;
- сигнали обміну даними через кабельні з’єднання та мережеве обладнання;
- сигнали обміну даними через інтерфейс SAS;
- сигнали обміну даними через інтерфейс HDMI;
- сигнали обміну даними через інтерфейс НЖМД SATA III.

По-друге показники захищеності мають бути визначені для всієї номенклатури інформаційних сигналів передавання. З урахуванням положень методики оцінки ризиків НАСР - таким показником обрано Ймовірність витоку інформації при наявності технічного каналу за результатами інженерно-технічного аналізу Ртк=1, та з урахуванням обмежень Рсв=Ртк=1.

Для подальшого проведення спеціальних досліджень ОТЗ в роботі на підставі даних інженерно-технічного аналізу визначено загальні вимоги до вимірювальних засобів.

За результатами проведення інженерно-технічного аналізу електронних засобів СКД ВС отримано параметри небезпечних сигналів – несуча частота, смуга, рівень передачі, час передачі для основних технічних засобів, що

обробляють інформацію (яка підлягає захисту). Характеристики небезпечних сигналів наведено в таблиці 7.

Таблиця 7. Дані інженерно-технічного аналізу СКД ВС ДУ

Зчитувач Mifare ATIS PR-08 MF-W – Контролер доступу NDC F18IP (U-Prox IP400) інтерфейс Wiegand.						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
50-500	5-0 В	500	300…3000 мкс	1	1	+
Контролер доступу NDC F18IP (U-Prox IP400) – Кабель КПВЕ-ВП (200) 4х2х0,51 – Комутатор TP-LINK TL-SF1008D (8 портів) Ethernet 100Mbit(RJ45).						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
17,5-500	2.8 3.3 В	500	0,5 – 2 с	1	1	+
Комутатор TP-LINK TL-SF1008D (8 портів) – Кабель КПВЕ-ВП (200) 4х2х0,51 – Комп'ютер ARTLINE Business B23v24 Ethernet 100Mbit(RJ45).						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
17.5-500	2.8 - 3.3 В	500	0,5 – 2 с	1	1	+
Комп'ютер ARTLINE Business B23v24 – HDMI – Монитор 23.6" Acer K242HQLCbid (UM.UX6EE.C01) HDMI 1080x1094 60 Гц						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
750	-0,5 +0,5 В	1500	Від 0,1 с до 2 хвл.	1	1	+
Комп'ютер ARTLINE Business B23v24 – 120 GB SSD інтерфейс SAS						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
1500	-0.5 0.5 В	3000	300 мкс	1	1	+
IP-відеокамера 2 Мп Hikvision DS-2CD1321-I(F) (2.8mm) – Кабель КПВЕ-ВП (200) 4х2х0,51 – IP-відеореєстратор 4-канальний Hikvision DS-7104NI-Q1/4P© 2.5 GBASE-T						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційного сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціального впливу Рсп	Необхідність в блокуванні технічного каналу
17,4-517,5	2.8 – 3.3 В	500	0,5-2 с	1	1	+
IP-відеореєстратор 4-канальний Hikvision DS-7104NI-Q1/4P© - Жорсткий диск 2TB Western						

Digital WD22PURZ SATA III						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційног о сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціальног о впливу Рсп	Необхідність в блокуванні технічного каналу
3000	-0.5 0.5 В	6000	100 мкс	1	1	+
IP-відеореєстратор 4-канальний Hikvision DS-7104NI-Q1/4P© - Кабель КПВЕ-ВП (200) 4х2х0,51 – Комп'ютер ARTLINE Business B23v24 100 Ethernet 100Mbit(RJ45).						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційног о сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціальног о впливу Рсп	Необхідність в блокуванні технічного каналу
17,4 - 500	2.8 – 3.3 В	500	0,5-2 с	1	1	+
Комп'ютер ARTLINE Business B23v24 – HDMI – Монитор 23.6" Acer K242HQLCbid (UM.UX6EE.C01) HDMI 1080x1094 60 Гц						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційног о сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціальног о впливу Рсп	Необхідність в блокуванні технічного каналу
1500	0 0.7 В	3000	Від 0.1 с до 2 хвл.	1	1	+
Комп'ютер ARTLINE Business B23v24 – 120 GB SSD інтерфейс SAS						
Частота (МГц)	Рівень	Смуга перехоплення (мгц)	Середній час передачі інформаційног о сигналу	Ймовріність витоку інформації Ртк	Ймовірність спеціальног о впливу Рсп	Необхідність в блокуванні технічного каналу
1500	-0.5 0.5 В	3000	300 мкс	1	1	+

Таким чином в СКД ВС наявно 9 основних технічних каналів витоку інформації за рахунок побічних електромагнітних випромінювань та наведень по яких також може бути здійснено електромагнітне нав’язування хибної інформації, або блокування передачі інформації.

Загальна характеристика небезпечного електромагнітного поля та сигналів СКД ВС:

- **смуга випромінювання небезпечних сигналів - 17,5 – 3000 МГц;**
- **можливість створення електромагнітних наводив в лініях електроживлення та заземлення – токи до 500 МГц та напруга до 1200 МГц;**
- **при використанні кручених пар крім електричної складової (17,5 – 517 МГц) буде магнітна складова електромагнітного поля – до 30 МГц.**

Розрахуємо загальну імовірність захисту інформації від витоку технічними каналами в СКД ВС (без застосування методів та засобів технічного захисту інформації), при цьому враховуємо, що виток інформації може бути хоча би по одному каналу

$Р_{тк}$ скдвс = $(1-Р_{ткі}) = (1-1) = 0$

Загальна імовірність спеціального впливу технічними каналами в СКД ВС (без застосування методів та засобів захисту інформації від спеціального впливу), при цьому враховуємо, що нав'язування хибної інформації або її блокування може бути хоча би по одному каналу

$Р_{св}$ скдвс = (1-Рткі) = (1-1) = 0

Висновок – розроблений варіант СКД ВС без застосування методів та засобів технічного захисту інформації є незахищеним від витоку технічними каналами та спеціального впливу.

Розрахуємо імовірність захисту інформації за трьома складовими:

- Несанкціонований доступ – обрано 0,8 (КСЗІ не має);
- Виток інформації технічними каналами ПЕМВН можливий;
- Спеціальний вплив технічними каналами можливий.

$Р_{зі} = Р_{нсд} \times Р_{тк} \times Р_{св} = 0,8 \times 0 \times 0 = 0$

Висновок.

Оцінка захисту інформації варіанту СКД ВС показала, що використання дозволених електронних засобів, програмного забезпечення, будова системи з використанням проводових ліній, без застосування методів та засобів технічного захисту інформації від витоку технічними каналами та спеціального впливу може забезпечити захист на рівні 0,8 (так званий базовий рівень) від несанкціонованого доступу, але не забезпечує захист від витоку технічними каналами та спеціального впливу, що для спеціальних умов експлуатації таких систем в державних установах не відповідає вимогам.

Потрібно розробити комплекс організаційно-технічних заходів щодо забезпечення захисту СКД ВС та максимізації блокування всіх технічних каналів витоку інформації та спеціального впливу, шляхом створення комплексу технічного захисту інформації в складі комплексної системи захисту інформації, з метою досягнення рівня захисту не менш 0.8 для проведення дослідної експлуатації та 1 при підтвердженні відповідності КСЗІ СКД ВС шляхом проведення державної експертизи, отриманні атестату відповідності та введенні в промислову експлуатацію. $K_{зі} = P_{зі} (max \rightarrow 1 = 1$

3.2 Рекомендації щодо захисту СКД ВС ДУ

На підставі аналізу вимог та рекомендацій [23? 26] для варіанту СКД ВС розроблено наступні рекомендації щодо захисту інформації від витоку технічними каналами та спеціального впливу:

- СКД ВС передбачає обробку службової інформації, та згідно вимог НД ТЗІ 1.6-005-2013.Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, даній системі може бути надана 4 категорія, яка передбачає захист тільки від несанкціонованого доступу, але Власник системи – ДУ має право встановити 3 категорію та висунути вимоги щодо створення КТЗІ на об’єктах ЕОТ (захист від витоку інформації за рахунок ПЕМВН та спеціального впливу);
- Вимоги до захисту інформації від витоку за рахунок ПЕМВ та методики проведення спеціальних досліджень, оцінки захисту в разі присвоення СКД ВС категорії 3 – повинні використовуватися прийняти в Україні для захисту секретної інформації (в роботі не розглядаються);
- Вимоги для захисту інформації від спеціального впливу шляхом формування електромагнитних полів та сигналів згідно з [3/ 22] повинні

бути розроблені Власником системи та узгоджені з Адміністрацією Держспецзв’язку (в роботі не розглядаються);

- З урахуванням положень методики оцінки ризиків НАСР – показником блокування технічних каналів витоку інформації ПЕМВН прийнято досягнення Ймовірності витоку інформації при наявності технічного каналу за результатами інженерно-технічного аналізу Ртк=0, та з урахуванням обмежень Рсв=Ртк=0;
- При побудові КТЗІ об’єктів ЕОТ СКД ВС рекомендовано використовувати методи пасивного та активного захисту від витоку інформації ТКВІ та пасивного захисту ввід спеціального впливу.
- Для варіанту СКД ВС розроблено рекомендацій за наступними напрямами:
- Розміщення складових СКД ВС всередині контрольованої зони ДУ, встановлення додаткових зон безпеки для ОТЗ що розміщуються між поверхами будівлі;
- Використання тільки проводових з'єднань;
- Проводове з'єднання повинно бути екранованим, екрани заземлені на контур захисного заземлення опором не більш 4 Ом.;
- Екрановані кабельні з'єднання, кінцеві засоби (камери, зчитувачі) повинні бути прокладені в коробах (додатково обладнані захисники кожухами) які обладнані засобами контролю розкриття (порушенням ізоляції) та виведені на пристрої сигналізації на пост охорони;
- Електроживлення СКД ВС повинно забезпечуватися безперебійно з використанням фільтрів, які мають діючий експертний висновок в галузі ТЗІ, розподільчі щитки, повинні бути під сигналізацією;
- Кабельні з'єднання та захисні бокси повинні бути розміщені в радіусі дії генератора шумів, або використовуватися лінійне зашумлення;
- Активне мережеве обладнання СКД ВС та системні блоки ПЕОМ потрібно встановити в монтажних шафах (бажано екранованих з

коефіцієнтом екранування не менш 20 дб в смузі частот 150 кГц – 3000 МГц) та застосувати систему активного захисту – пристрій електромагнітного випромінювання в смузі 9 кГц – 3000 МГц;

- Розміщення СКД та ВС повинно бути влаштовано таким чином, щоб технічний спеціаліст мав змогу періодичного огляду на предмет встановлення закладних пристроїв, контролю опечатування та сигналізації;
- Комплекс технічного захисту інформації на об’єктах ЕОТ СКД ВС повинен пройти випробування та атестацію з реєстрацією Акту атестації в Адміністрації Держспецзв’язку – це обов’язкова умова надання Атестату відповідності на КСЗІ СКД ВС ДУ.

3.3 ***ТЕХНІЧНИЙ ПРОЕКТ*** створення комплексу технічного захисту інформації об’єкта електронної техніки СКД ВС ДУ

ЗМІСТ

ЗАТВЕРДЖУЮ

Керівник ДУ

«___» _____ 202_ року

КОМПЛЕКС ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ПОЯСНЮВАЛЬНА ЗАПИСКА З ТЗІ

Об’єкт електронно-обчислювальної техніки СКД ВС ДУ

(Шифр – КТЗІ – СКД ВС ДУ)

ПОГОДЖЕНО	ПОГОДЖЕНО

Київ – 2023

ЗМІСТ

Перелік скорочень

АБЗ	–	архітектурно-будівельні заходи;
АС	–	автоматизована система;
ГШ	–	генератор шуму;
ІзОД	–	інформація з обмеженим доступом;
КЗ	–	контрольована зона;
КТЗІ	–	комплекс технічного захисту інформації;
ОІД	–	об’єкт інформаційної діяльності;
ОК	–	огороджувальні конструкції;
ПЗ	–	пояснювальна записка;
ТЗ	–	технічне завдання на КСЗІ;
ТЗІ	–	технічний захист інформації;
ПЕМВН	–	побічні електромагнітні випромінювання та наведення.

1. Терміни та визначення

В цьому документі використовуються терміни та визначення, наведені в ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

2. Загальні відомості

Дана Пояснювальна записка (ПЗ) визначає основні проектні рішення щодо модернізації комплексу технічного захисту інформації (КТЗІ) СКД ВС ДУ.

Умовне позначення комплексу ТЗІ: КТЗІ – СКД ВС ДУ.

Замовник – ДУ.

Виконавець – студент 3 курсу Горський О.О.

Планові терміни початку та закінчення робіт зі створення КТЗІ – СКД ВС ДУ та фінансування цих робіт визначаються Замовником.

3. Призначення комплексу технічного захисту інформації

Основним призначенням КТЗІ є забезпечення захисту інформації, що становить державну або іншу передбачену законом таємницю, які циркулюватимуть в СКД ВС ДУ, від витоку технічними каналами.

Результатом створення КТЗІ буде блокування можливих технічних каналів витоку ІзОД, визначених у документі «Окрема модель загроз для інформації, яка циркулює на об’єкті ЕОТ СКД ВС ДУ.

4. Нормативні посилання

Створення КТЗІ – СКД ВС ДУ буде проведено на підставі та відповідно до вимог наступних нормативно-правових актів і нормативних документів з питань ТЗІ та охорони державної таємниці:

- Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 209229/99;
- ТР ЕОТ-95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, АС і мережах від витоку каналами побічних електромагнітних випромінювань та наведень. Затверджено наказом ДС ТЗІ від 09 червня 1995 року № 25;
- Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначена законодавством України.

5 Опис проектних рішень та схем активного захисту інформації від витоку каналами ПЕМВН

5.1 Ефективність проектних рішень активного захисту ІзОД від витоку каналами ПЕМВН забезпечено обґрунтованим вибором системи активного захисту - генератора шуму, місця його встановлення, а також розгортання антенної системи на поверхні конструкцій ОІД відповідно до техніко-експлуатаційної документації.

5.2 Вибір генератору електромагнітного шуму, монтаж його антенної системи, підключення до АС СКД ВС ДУ наведено в документі:

«Акт проведення ініціалізації системи активного захисту, що вперше розгортається в приміщенні охорони ДУ…».

5.3 Застосування системи активного захисту

5.3.1 Для захисту ІзОД від витоку каналами ПЕМВН застосовано Прилад високочастотного шуму мобільний РІАС–1М (5 Вт), призначений для створення електромагнітних перешкод в ефірі в діапазоні частот від 180 Гц до 3 ГГц.

До складу приладу входять генератор високочастотного шуму мобільний „РІАС–1ГМ”, антени дипольні телескопічні „РІАС–1АД” (3 шт.), антени рамкові м’які РІАС–1АМ (2 шт.).

Коефіцієнт якості шуму - не менше 0,8. Коефіцієнт міжспектральних кореляційних зв’язків - не менше 2,0. Нормований рівень спектральної

щільності напруженості електричного і магнітного компонентів нормованого електромагнітного поля шуму - не менше 30 дБ. Максимальне інтегральне значення вихідної потужності - не менше 5 Вт.

5.3.2 Також для захисту ІзОД від витоку каналами:

- побічних електромагнітних випромінювань основних технічних засобів;

- побічних електромагнітних наведень на лінії електроживлення та заземлення;

- побічних електромагнітних наведень на лінії допоміжних технічних засобів та систем

Розгорнути три телескопічні антени (одну вертикально, другу з нахилом 45^0 праворуч, третю з нахилом 45^0 ліворуч) та 2 низькочастотні (одну у вертикальній, другу у горизонтальній площині).

5.3.3 Монтаж та підготовку до роботи «РІАС-1М» виконано відповідно до техніко-експлуатаційної документації.

5.3.4 Місце монтажу САЗ наведено у Комплекті робочих креслень (рис. 2 Генеральний план ОІД).

5.3.5 Для захисту ІзОД від витоку Візуально-оптичний каналом (утворюється за рахунок отримання технічними засобами візуальної розвідки, що встановлюються в зоні прямої видимості з вікон ОІД, видової інформації у вигляді друкованих документів з ІДТ та ІДТ, яка виводиться на монітор засобу ЕОТ, отримання вказаної інформації може здійснюватися шляхом дистанційної зйомки та спостереження з використанням залежно від умов спостереження (відстані до ОІД, освітленості тощо) засобів оптико-електронної та візуально-оптичної технічної розвідки) здійснено наступне:

- вікно обладнано металевими ролетами, які мають запірні замки, та вертикальними полістироловими офісними жалюзі, які опускаються під час циркуляції ІДТ;

- АС – 1 СКД ВС ДУ та монітори розміщено в куту між стінами, бар’єром та столом чергового охоронця, що унеможливлює стороннє спостереження за видовою інформацією.

5.4 Склад засобів ТЗІ

Виходячи з умов розташування ОІД, враховуючи характеристики

системи активного захисту інформації від витоку каналами ПЕМВН та результати попереднього контролю радіочастотної обстановки на ОІД, проведено монтаж технічних засобів, склад яких наведено в таблиці 1.

Таблиця 1

№ з/п	Найменування засобу ТЗІ*	Кіль-кість, шт.	Місце встановлення (монтажу)	Паспорт (етикетка)	Наявність сертифікату	Схема встановлення (монтажу)
1	Прилад високочастотного шуму мобільний PIAC – 1M (5Вт)	1	Прим. № 605 В складі АС-1 СРСР	Зав. №_____ 15.07.21 року, термін служби не менш 10 років	ЕВ № 969 04.06.2019.	Рис. 1 кресленння

* – засіб ТЗІ входить до Переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначена законодавством України.

Рекомендації щодо проведення монтажу АС з системою активного захисту PIAC-1M:

1. З’єднання комплектуючих АС виконати в наступному порядку:

- Електроживлення однофазне 240 вольт, 50 Гц забезпечити від двох трьох контактних розеток. (згідно з п.5.3.2, 5.3.6 документу «Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок» (ТР ЕОТ – 95), **з**аземлювальні проводи повинні бути виконані з мідного дроту (кабеля) з перехідним опором з'єднань не більше 600 мкОм. Опір заземлення не повинен перевищувати 4 Ом. При неможливості провести заземлення ТЗ ЕОТ допускається їх "занулення".

- *Виконання цих вимог підтверджується щорічними актами випробувань електромереж в будівлі та актами перевірки контурів зазамлення трансформаторних підстанцій РУ 10кв/400 в.*

- До першої розетки підключити ДБЖ з фільтром мережевим на 5 розеток (системні блоки, монітори, PIAC- 1M), для забезпеченння роботти АС- з системою активного захисту в разі знеструмлення.

- До другої розетки підключити контролер та роутер.

2. Роз’єми Системних блоків розподілити наступним чином:

- на передній панелі порт USB Type-C та USB 3.2 – для підключення USB Флеш-накопичувачів.

- на задній панелі відеовиход HDMI – монітор який встановлюється на посту чергового, DisplayPort і VGA – монітор в кімнате чергового, а також по два інтерфейси USB 2.0 – миша, клавіатура і USB 3.2 – вільний.

3. З метою забезпечення гарантованого, безперервного активного захисту об’єкту ЕОТ – прилад PIAC-1M рекомендовано підключити до мережевого фільтру на виході ДБЖ та встановити зверху на корпус системного блоку.

Розгорнути три телескопічні антени (одну вертикально, другу з нахилом 45^0 праворуч, третю з нахилом 45^0 ліворуч) та 2 низькочастотні (одну у кабельний канал підсистеми контролю доступу, другу у кабельний канал підсистеми відеоспостереження).

6. Опис заходів щодо недопущення встановлення закладних пристроїв під час створення КТЗІ

Провести роботи з виявлення закладних пристроїв в основних технічних засобах, зі складанням наступних документів:

- План проведення робіт з виявлення закладних пристроїв в основних технічних засобах, що вперше розгортаються в приміщенні №_____.

- Акт за результатами проведення робіт з виявлення закладних пристроїв в основних технічних засобах, що розгортаються вперше в складі об’єкту ЕОТ у складі СКД ВС категорії 3.

Під час виконання монтажно-налагоджувальних робіт, прокладення нових інженерних комунікацій, встановлення технологічного обладнання, засобів оргтехніки, елементів інтер’єру, меблів тощо, будуть вживатися заходи щодо недопущення встановлення закладних пристроїв несанкціонованого отримання інформації.

Від замовника: _____

Від виконавця: _____Сергій ДОВБНЯ

_____Олег ГОРСЬКИЙ

3.4 Оцінка впровадження рекомендацій захисту інформації в СКД ВС ДУ

При створенні КТЗІ об’єкту ЕОТ СКД ВС, проведенні випробувань та атестації можна буде гарантовано блокувати методами пасивного та активного технічного захисту 9 основних технічних каналів витоку інформації за рахунок побічних електромагнітних випромінювань та наведень.

В виконанням вимог до захисту небезпечного електромагнітного поля та сигналів СКД ВС:

-електромагнитне поле шума в смцзі 180 Гц – 3000 МГц, що перекриває смугу випромінювання небезпечних сигналів - 17,5 – 3000 МГц;

- створення електромагнітних шумів наводив в лініях електроживлення та заземлення, що маскують небезпечні токи до 500 МГц та напругу до 1200 МГц;

- електромагнитне зашумлення (лінійне та наводами) при використанні кручених пар - електричної складової (17,5 – 517 МГц) та магнітної складової електромагнітного поля – до 30 МГц.

Розрахуємо загальну імовірність захисту інформації від витоку технічними каналами в СКД ВС (при застосуванні рекомендацій наведених у п.____ даної роботи), при цьому враховуємо, що виток інформації буде блокуватися по кожному каналу наведеному у таблиці____.

Ртк скдвс = 1- (1-Ртк1) (1-Ртк2) (1-Ртк3) (1-Ртк4) (1-Ртк5) (1-Ртк6) (1-Ртк7) (1-Ртк8) (1-Ртк9) =1- (1-1) = 1-0=1

Загальна імовірність спеціального впливу технічними каналами в СКД ВС (при застосуванні рекомендацій наведених у п.____ даної роботи), при цьому враховуємо, що нав’язування хибної інформації або її блокування буде унеможливлено по кожному каналу наведеному у таблиці ____.

Рсв скдвс = 1- (1-Ртк1) (1-Ртк2) (1-Ртк3) (1-Ртк4) (1-Ртк5) (1-Ртк6) (1-Ртк7) (1-Ртк8) (1-Ртк9) =1- (1-1) = 1-0=1

Висновок – розроблений варіант СКД ВС (при застосуванні рекомендацій наведених у п.____ даної роботи) з використанням пасивних та

активних методів та засобів технічного захисту інформації при створенні КТЗІ об’єкту ЕОТ (в разі проведення інструментальної оцінки захищеності інформації та атестації комплексу) є захищеним від витоку технічними каналами та спеціального впливу.

Розрахуємо імовірність захисту інформації за трьома складовими:

Несанкціонований доступ – обрано 0,8 (заначаємо, що КСЗІ СКД ВС ДУ знаходиться в дослідної експлуатації);

Виток інформації технічними каналами ПЕМВН унеможливлено;

Спеціальний вплив технічними каналами унеможлилено.

Рзі = Рнсд х Ртк х Рсв = 0,8 х 1 х 1 = 0,8

Висновки:

1. Оцінка захисту інформації варіанту СКД ВС показала, що використання дозволених електронних засобів, програмного забезпечення, будова системи з використанням проводових ліній, при застосування методів та засобів технічного захисту інформації від витоку технічними каналами та спеціального впливу може забезпечити захист на рівні 0,8 (так званий базовий рівень) від несанкціонованого доступу, що для спеціальних умов експлуатації таких систем в державних установах відповідає вимогам для дослідної експлуатації.
2. З метою досягнення рівня захисту Кзі = Рзі ($\max \rightarrow 1$) = 1 для промислової експлуатації потрібно завершити створення КСЗІ СКД ВС ДУ шляхом проведення державної експертизи, отриманні атестату відповідності та введенні в промислову експлуатацію.

ВИСНОВКИ

В ході виконання роботи було створено функціональну схему СКД ВС ДУ, проведено оцінку ризиків та розроблено рекомендації щодо захисту інформації, а саме:

1. Проведений аналіз вихідних даних, різних технологій побудови сучасних систем контролю доступу та відеоспостереження а також особливих умов експлуатації даної системи в державній установі дозволів надати пропозиції щодо створення системи контролю доступу та відеоспостереження, а саме:

- обґрунтувати функціональний склад СКД та ВС;
- обрати пристрої та засоби для побудови СКД ВС ДУ.

При забезпеченні особливих умов:

- обмеження доступу до структури та характеристик реальних систем;
- забезпечення захисту інформації від витоків технічними каналами, несанкціонованого доступу та спеціального впливу.

2. Для обґрунтування функціонального складу СКД та ВС, було проведено порівняльний аналіз технологій використання бездротових та провідних датчиків та камер, для подальшого ескізного проектування СКД ВС ДУ.

3. Було визначено основні технічні вимоги до варіанту СКД ВС ДУ. Технічні вимоги поділяються на два напрямки: вимоги програмного забезпечення та вимоги до технічних засобів. З врахуванням цього здійснювалось обрання комплектуючих та програмного забезпечення для створення захищеної СКД ВС.

4. Розроблено рекомендації та проведено оцінку їх впровадження щодо забезпечення захисту інформації в СКД ВС ДУ.

5. Оцінка захисту інформації варіанту СКД ВС показала, що використання дозволених електронних засобів, програмного забезпечення, будова системи з використанням проводових ліній, при застосування методів та засобів технічного захисту інформації від витоку технічними каналами та спеціального впливу може забезпечити захист на рівні 0,8 (так званий базовий рівень) від несанкціонованого доступу, що для спеціальних умов експлуатації таких систем в державних установах відповідає вимогам для дослідної експлуатації.

6. З метою досягнення рівня захисту Кзі = Рзі ($\max \rightarrow 1$) = 1 для промислової експлуатації потрібно завершити створення КСЗІ СКД ВС ДУ шляхом проведення державної експертизи, отриманні атестату відповідності та введенні в промислову експлуатацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію».
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах».
3. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.
4. Постанова Кабінету Міністрів України від 29 березня 2006 року №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».
5. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення.
6. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
7. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
8. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
9. НД ТЗІ 1.6-005-2013.Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. Затверджено наказом ДСТСЗІ СБ України від 15.04.2013 року № 215.
10. Інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, в Бюро економічної безпеки України та територіальних управліннях Бюро економічної безпеки України,

затверджена Наказом Бюро економічної безпеки України від 21.11.2022 року №341.

11. Перелік відомостей, що становлять службову інформацію в Бюро економічної безпеки України, затверджений Наказом Бюро економічної безпеки України від 01.02.2022 № 27 (із змінами, внесеними згідно із наказом Бюро економічної безпеки України від 05.08.2022 № 178).

12. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем. Стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

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

14. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

15. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

16. ТР ЕОТ-95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, АС і мережах від витоку каналами побічних електромагнітних випромінювань та наведень.

17. Безпека електрозв’язку та інформаційних технологій. Огляд, зміст та застосування діючих Рекомендацій МСЕ-Т для забезпечення захищеного електрозв'язку. МСЕ-Т – Бюро стандартизації електрозв'язку (БСЕ). Place des Nations – CH-1211 Geneva 20-Switzerland, 2009. – 162 с. Веб сайт: www.itu.int/ITU-T, ел. Пошта: tsbmail@itu.int.

18. Г.Ф. Конахович та інші. Захист інформації в телекомунікаційних системах: Навчальний посібник. – К.: НАУ, 2009.-380 с.

19. Основи інформаційної безпеки. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.

20. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем.-К.: Видавнича група BHV, 2009 – 608с.:іл.

21. Педагогічний програмний засіб (ППЗ) «Телекомунікаційні системи та мережі. Структура й основні функції. Том 1». Автори: Поповський В.В, Лемешко О.В.; Ковальчук В.К.; Плотніков М.Д.; Картушин Ю.П.; Попонін О.М.; Агєєв Д.В.; Сабурова С.О., Олійник В.Ф., Персиков А.В.; Лошаков В.А. Селіванов К.О. Друге видання. Виправлено та доповнено. 2018.

22. Голев Д.В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / Голев Д.В., Кононович В.Г., Хомич С.В.; за ред. чл.-кор. МАЗ В.Г. Кононовича. - Одеса: ОНАЗ ім. О.С. Попова, 2013. - 218 с.

23. С.Я. Довбня. Методи (моделі) розробки комплексів технічного захисту інформації на об’єктах інформаційної діяльності та радіоелектронної техніки: Навчальний посібник. – К.: ДП «Український центр «Безпека», 2019. – 95 с.

24. С.Я. Довбня, П.П. Наталенко. Основи використання, адміністрування та забезпечення захисту інформації в автоматизованих системах: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2017. – 164 с.

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

26. Анохін А.М. Методи виявлення важливості критеріїв// Автоматика та телемеханіка

27. Герасимов Б.М., Домарев В.В. Вибір оптимального варіанту системи захисту інформації на основі застосування методів нечіткої багатокритеріальної оптимізації// Захист інформації. №3.

28. Висоцька Е., Давиденко А. Сучасний стан методології аналізу ризиків при забезпеченні інформаційної безпеки комп’ютерної системи // Правове. нормативне та метрологічне забезпечення системи захисту інформації в Україні

29. Василевич Л.Ф., Проскурин В.М. Вибір способів та пристроїв захисту інформації на основі теорії ігор// Праці КВІУЗ. Випуск 2. 1998. С.95-100.

Додаток А

Вихідні дані для розробки варіанту СКД ВС

Задум організації контролю доступу та відеоспостереження

Потрібно встановити систему контролю доступу на два поверхі, камери відеоспостереження за основними та запасними виходами, коридорами на поверхах з виведенням інформайції в кімнату чергового та на пост четвертого поверху. Загальна вартість обладнання та робіт не більше 150 000 гривень.

Схеми розміщення приміщень по поверхах

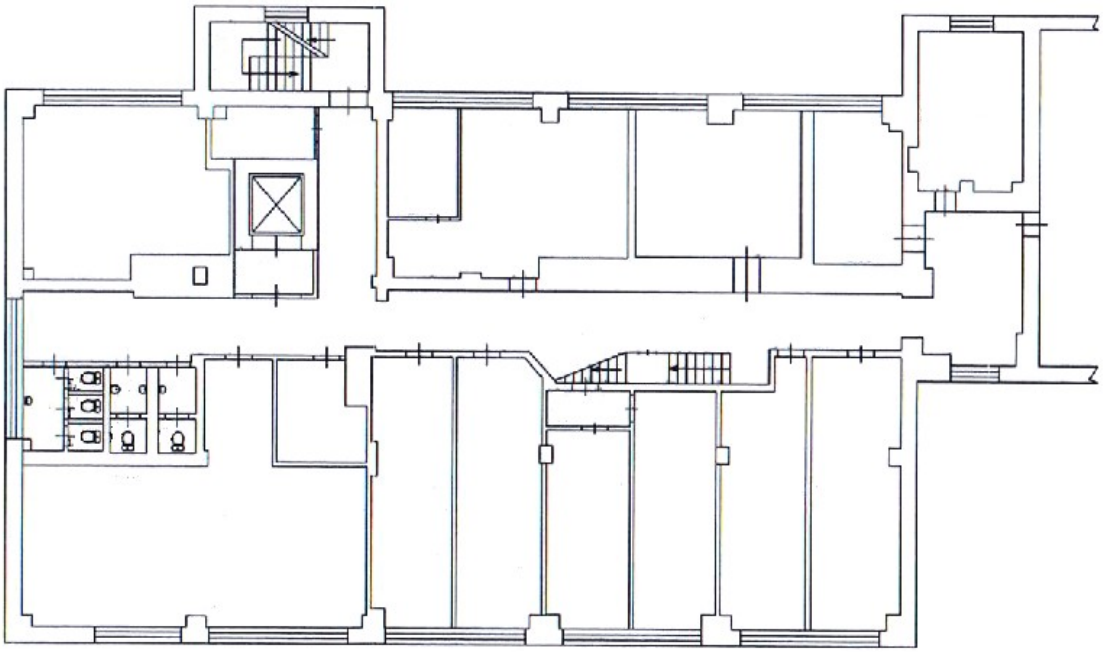

Рис. 1. Схема нижнього поверху в державній установі

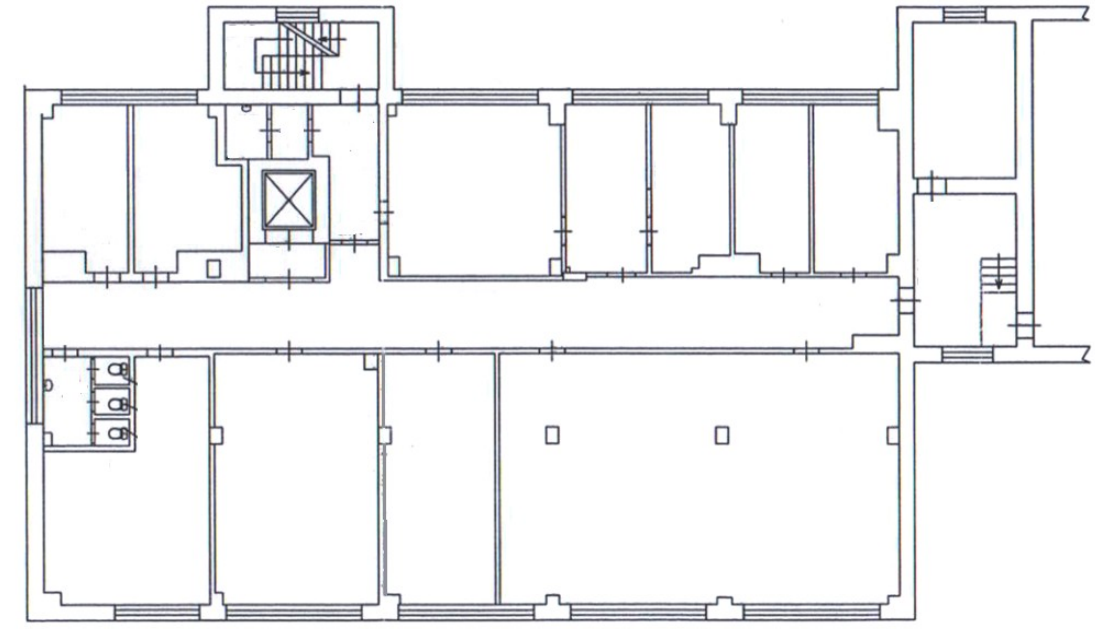

Рис. 2. Схема верхнього поверху в державній установі

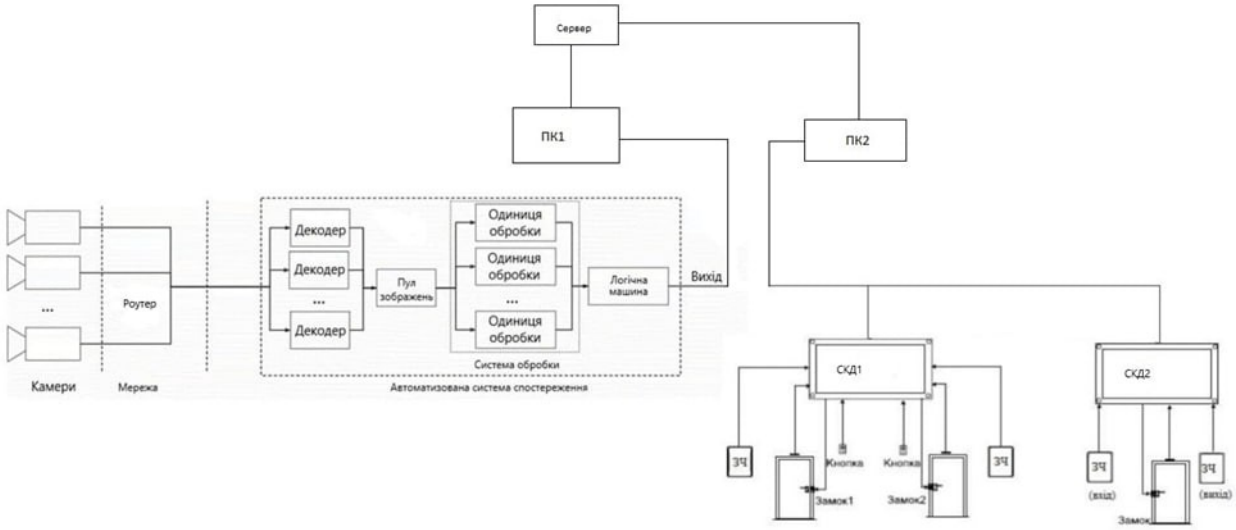

Рис. 3. Функціональна схема СКД ВС ДУ

Додаток Б.

Специфікація засобів та послуг для створення СКД ВС ДУ

Таблиця Б.2 Система відеоспостереження

	Назва	***Од. вим.***	***Кіль-кість***	***Вар-ть од. грн.***	***Сума грн.***
1	*IP-відеокамера 2 Mn Hikvision DS-2CD1321-I(F) (2.8mm)*	*шт.*	*2*	*2 588,00*	*5 176,00*
2	*IP-відеореєстратор 4-канальний Hikvision DS-7104NI-Q1/4P©*	*шт.*	*1*	*4 715,00*	*4 715,00*
3	*Жорсткий диск 2TB Western Digital WD22PURZ*	*шт.*	*1*	*2 349,00*	*2 349,00*
4	*Комп'ютер ARTLINE Business B23v24 без опер.сист.*	*шт.*	*1*	*5 958,00*	*5 958,00*
5	*Монитор 23.6" Acer K242HQLCbid (UM.UX6EE.C01)*	*шт.*	*2*	*4 399,00*	*8 798,00*
6	*Комплект дротовий Esperanza Titanum TK106 USB UA*	*шт.*	*1*	*183,00*	*183,00*
7	*Кабель КПВЕ-ВП (200) 4х2х0,51*	*м*	*305*	*23,82*	*7 265,10*
8	*Монтажний набір*	*шт.*	*1*	*1 400,00*	*1 400,00*
9	*Монтажні та налагоджувальні роботи*		*1*	*21 500,00*	*21 500,00*
10	*Техічна документація на систему*		*1*	*2 400,00*	*2 400,00*
	РАЗОМ, грн. з ПДВ				***59 744,10***

Характеристики обладнання.

Перша камера: IP-відеокамера Hikvision DS-2CD1121-I(F), яка має наступні характеристики:

- Дротове з’єднання;
- Можливість нічної зйомки;

- Можливість повороту до 355 градусів;
- Якість зображення 1920x1080 пікселів;
- Роздільна здатність 2.8 мегапікселів;
- Частота кадрів дорівнює 25 кадрів на секунду;

Основними плюсами є те, що подається найвища якість зображення та присутня можливість повороту до 360 градусів, також наявність дротового з'єднання підходить нам для з'єднання з серверним обладнанням та знижується ризик злому на відміну камер, які з'єднуються за допомогою технології Wi-Fi.

Друга камера: Turbo HD-відеокамера Hikvision DS-2CE56D0T-IRMFF вже суттєво відрізняється від першою завдяки деяким моментам у власних характеристиках.

- Відсутність повороту на потрібний градус;
- Роздільна здатність 2.8 Мп;
- Наявність інфрачервоної підсвітки;
- Дротове з'єднання;

Блок живлення

У даного блока живлення наступні характеристики, які роблять його хорошим вибором:

- Імпульсний блок живлення;
- Вхідна напруга має діапазон від 100 до 240 В;
- Вихідна напруга дорівнює 12 В;
- Вихідний струм 1 А;
- Робочі температури: від 0 до +45 градусів за Цельсієм;

Основними критеріями для вибору комп'ютера та монітора повинні бути такими:

- Максимальний розмір екрану – 1920x1080 пікселів;
- Сучасні процесори (оптимально починаючи з 9-го покоління Intel або останні серії сімейства AMD Ryzen);
- Оперативна пам'ять, яка буде задіяна повинна мати мінімум в 16 Гб;
- Наявність встановленої ОС (в даному випадку Windows 11, але можна паралельно встановити один з дистрибутивів Linux);

Ідеальним варіантом буде ARTLINE Business B29 v31Win завдяки його відмінним характеристикам:

- Шестиядерний процесор виробництва Intel Core i5-10400F;
- 16 гб оперативної пам'яті;
- Наявність твердотілого накопичувача в розмірі 480 гб (також можливим буде розширення пам'яті з додаванням додаткового диску);
- Присутня операційна система Windows 11;

В якості монітора виступатиме: 24.5 дюймовий AOC 25G3ZM/BK з наступними характеристиками:

- Роздільна здатність дисплею: 1920x1080 пікселів;
- Частота оновлення кадрів: 240 Гц;
- Діагональ дисплея: 24.5 дюймів;
- Порт інтерфейсу: HDMI;
- Відношення сторін: 16:9;

Далі, ми повинні обрати електронний замок, який повинен бути надійним в будь-яких випадках починаючи від перепадів електроживлення, так й витримати спробу зламу з боку зловмисників. Для нашого проекту підходить замок MS-280LED, який завдяки своїм якостям дуже добре підходить:

- Напруга дорівнює 12В;
- Відсутня світлодіодна індикація;

- Діапазон робочих температур варіюється від -10 до +50 градусів за Цельсієм;
- Алюмінієвий сплав та оцинкований метал;

Після цього треба вибрати контролер доступу, який є невід'ємною частиною будь-якої СКД, як й в нашому проекті воно відіграє свою роль. Його характеристики дозволяють обрати для нашої системи:

- Мережевий контролер;
- Дротове з'єднання;
- Напруга живлення дорівнює 12В;
- Обсяг пам'яті сягає до 30 тисяч унікальних ідентифікаторів;
- Робочі температури дорівнюють від 0 до 50 градусів за Цельсієм;

Жорсткий диск є необхідною частиною для будь-якого комп'ютера, в нашому випадку на ньому буде встановлено програмне забезпечення та зберігатися оброблена інформація з відеокамер. Диск повинен відповідати таким вимогам: надійність, обсяг пам'яті від 2 терабайтів, твердотілий (бажано), швидкість обробки інформації.

В якості жорсткого диску підходить: Western Digital Red SA500 SSD 2TB 2.5" SATA III. Його особливості дозволяють обрати саме цей диск для подальшої експлуатації:

- Обсяг пам'яті: 2 ТБ;
- Швидкість зчитування сягає 560 Мб/с;
- Швидкість запису досягає до 530 Мб/с;
- Енергоспоживання дорівнює 6 Вт;

Останнім, і ключовим пристроєм, який залишилось обрати – це відеореєстратор, для нього вимоги такі: підтримка IP-камер, роздільна здатність 1920x1080, здатність підтримувати управління камер кількістю до 16 шт., максимальний обсяг збереженої пам'яті сягає 10 Тб.

Для цього ідеально підходить GreenVision GV-N-I017/16 12MP, його характеристики також добре пояснюють даний вибір:

- Підтримка 4K формату;
- Максимальний обсяг пам'яті дорівнює 10 Тб;
- Наявність двох USB-виходів;
- Підтримує до 16 відеокамер;
- Швидкість Ethernet сягає від 10 до 1000 Мб;
- Підтримка Linux OS;
- Наявне управління поворотними камерами;

Додаток В.

В.1 Завдання та функції КСЗІ

Завдання КСЗІ полягають у захисті конфіденційності інформації, забезпеченні безпеки самої інформації, а також в цілісності та доступності даних. Основними завданнями КСЗІ є: аутентифікація, шифрування, контроль доступу, виявлення загроз та захист від них, аудит та моніторинг, резервне копіювання та відновлення даних, сертифікація та валідація інформації.

- Аутентифікація: КСЗІ має за собою мету, що обов'язково потрібно встановлювати та перевіряти ідентичність усіх користувачів та систем, аби було повноцінне забезпечення доступу тільки для авторизованих осіб в межах державної установи;
- Шифрування: КСЗІ повинно на цьому етапі захищати конфіденційність наявної інформації шляхом застосування сучасних алгоритмів шифрування.
- Контроль доступу: в даному завданні КСЗІ повинно керувати доступом до інформації, яка маю класифікацію секретності різних рівнів на основі прав доступу, ролей працівників та інших вимог безпеки.
- Виявлення загроз та захист: КСЗІ обов'язково повинно мати механізми для виявлення ймовірних загроз (віруси, фішингові програми тощо), аби при можливій загрозі системі безпеки був наявний механізм захисту (такі як антивіруси, сучасне ПЗ, брандмауери та інше).
- Аудит та моніторинг: дана задача являє собою те, що КСЗІ повинно виконувати моніторинг усіх користувачів та їх діяльності, а також системи, що були встановлені на предмет підозрілої активності.
- Резервне копіювання та відновлення даних: цей етап має таке обґрунтування – КСЗІ має на собі мету забезпечувати збереження важливої інформації та в разі чого зробити резервну копію, аби після технічної проблеми мати можливість відновити втрачені дані.
- Сертифікація та валідація: КСЗІ обов'язково має пройти етап сертифікації та валідації, щоб воно могла підтвердити відповідність захисних властивостей, які встановлені вимогами стандартів безпеки;

Функції КСЗІ має більш широкі повноваження, але відповідає вищезазначеним завданням. До функцій КСЗІ можна віднести: виявлення загрози, захист від НСД, конфіденційність, цілісність даних, автентифікація та ідентифікація, аудит та моніторинг, управління ключами, відновлення системи після інцидентів.

- Виявлення загрози: система КСЗІ повинна обов'язково виявляти можливі загрози безпеці інформації, такі як вірусні програми, фішингові програми з метою злому бази даних;
- Захист від НСД: КСЗІ має забезпечувати повноцінний захист від несанкціонованого доступу до системи безпеки та мережі, що включає в собі захист від хакерських атак, НСД через мережу або зламу паролів бази даних;
- Конфіденційність: КСЗІ за допомогою криптографічних методів, алгоритмів та механізмів шифрування здатне забезпечити збереження конфіденційності інформації від НСД.
- Цілісність даних: КСЗІ має гарантувати, що дані, які зберігаються не будуть змінені без дозволу адміністратора, цілісність інформації забезпечується завдяки хеш-функціям та цифровими підписами.

- Автентифікація та ідентифікація: КСЗІ забезпечує перевірку ідентичності працівників, їх діяльність в межах ДУ, перевіряє доступ працівників до ресурсів та проводить контроль прав доступу працівників.
- Аудит та моніторинг: дана функція передбачає, що КСЗІ реєструє усі дії працівників в межах ДУ, а також використання працівниками ресурсів та проводить обов'язкову перевірку з метою виявлення порушень вимог безпеки та подальшого аналізу подій.
- Управління ключами: КСЗІ на цьому моменті включає в собі механізми зберігання криптографічних ключів, їх генерацію та керування, що використовуються для подальшого шифрування та розшифрування отриманих даних, або тих даних, що є наразі.
- Відновлення системи після інцидентів: КСЗІ повинно мати такі механізми, аби воно могло відновити власну роботу після неблагополучних інцидентів з системою безпеки. В даному випадку відновлення даних з резервних копій, або відновлення системи після НСД.

Загалом, КСЗІ має за собою мету забезпечувати цілісність, конфіденційність та доступність важливої інформації в комп'ютерних системах, а також забезпечити повноцінний захист системи, до якої воно закріплено від можливих хакерських атак та НСД.

В.2 Етапи створення КСЗІ

Етапи створення КСЗІ поділяються на декілька кроків, враховуючи, що даний процес є досі комплексним та найбільш важливою частиною в розробці до будь-якої СКД ВС ДУ. Нижче будуть представлені дані етапи з подальшим поясненням:

1. Формування загальних вимог до КСЗІ СКД ВС ДУ
2. Розробка політики безпеки інформації СКД ВС ДУ
3. Розробка технічного завдання на створення СКД ВС ДУ
4. Розробка проекту КСЗІ
5. Введення до експлуатації КСЗІ та оцінка захищеності СКД ВС ДУ
6. Супроводження КСЗІ

Формування загальних вимог є початковою фазою в створенні КСЗІ, так як на даному етапі обговорюється обґрунтування вимог, а потім формується завдання до створення КСЗІ. В позитивному вирішенні усіх початкових питань при формуванні загальних вимог вже можна прийняти рішення про створення КСЗІ.

До **розробки політики безпеки інформації** відноситься такий план дій, як: вивчення об'єкта, який буде створюватися; вибір варіанту КСЗІ; і в кінцевому рішенні оформлюється власне політика безпеки.

Розробка технічного завдання на створення являє собою комплексний план, в якому створюється власне саме ТЗ, яке є організаційно-технічним документом, що визначає вимоги із захисту СКД ВС ДУ. ТЗ на створення КСЗІ виконується таким чином, що на відповідній стадії робіт з розробки СКД ВС ДУ з подальшим урахуванням комплексних підходів до побудови КСЗІ, яке власне передбачає об'єднання у єдину систему всіх необхідних заходів та засобів захисту інформації від різноманітних загроз безпеки на всіх етапах життєвого циклу СКД ВС ДУ.

Також оформлення ТЗ має три варіанти: у вигляді окремих розділів ТЗ на створення СКД ВС ДУ; у вигляді окремого (часткового) ТЗ; у вигляді доповнення до ТЗ на створення СКД ВС ДУ.

Розробка проекту КСЗІ складається з простого порядку розробки, яка ділиться на три частини – перша частина відводиться до розробки на підставі та відповідності з ТЗ на створення СКД ВС ДУ; друга частина полягає в тому, що під час розробки КСЗІ обґрунтовуються та приймаються проектні рішення, що дають змогу реалізувати вимоги ТЗ, забезпечити сумісність та взаємодію різних компонентів КСЗІ, а також різних заходів,

методів та способів захисту інформації. Після цього відводиться на ескізний проект, розробка проектних рішень КСЗІ, технічний проект та остаточна розробка робочого проекту.

Введення до експлуатації КСЗІ та оцінка захищеності СКД ВС ДУ складається з декількох етапів: підготовки до введення КСЗІ в дію; навчання операторів КСЗІ; комплектування КСЗІ; будівельно-монтажні роботи; пусконалагоджувальні роботи; проведення попереднього випробування; дослідної експлуатації; державна експертиза КСЗІ.

Супроводження КСЗІ має на увазі, що на цьому етапі виконуються остаточні роботи з організаційного забезпечення функціонування КСЗІ та подальшого управління засобами захисту інформації, що відповідає згідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному та післягарантійному технічному обслуговуванню засобів захисту інформації.

В.3 Вимоги до випробувань КСЗІ

При випробуванні КСЗІ створюються такі вимоги, аби в подальшому дана система могла їх пройти та в разі деяких технічних проблем була можливість доопрацювати саму КСЗІ, щоб після повторного випробування можна було би завершити повністю створення системи та ввести її у повноцінну експлуатацію.

До вимог випробувань КСЗІ відносяться: функціональність; безпека; надійність; відповідність до стандартів; тестування на прохідність; документація.

- Функціональність: система повинна виконувати закладені у неї функції захисту інформації, які відповідають згідно встановлених вимог – до функцій можна віднести шифрування, аутентифікація, контроль доступу, моніторинг тощо. Випробовування перевіряють якість виконання поставлених функцій;
- Безпека: КСЗІ повинна на меті підтримувати високий рівень безпеки інформації шляхом захисту від НСД, зламу, або втрати важливих даних. Дане випробовування включає в собі мету оцінити стійкість системи до атак будь-якого роду.
- Надійність: система повинна бути надійною та стабільною під час роботи. Випробовування на надійність перевіряє та оцінює стійкість системи до можливих помилок в роботі, відновлення після збоїв як на програмному рівні, так й на рівні живлення.
- Відповідність до стандартів: КСЗІ обов’язково повинно відповідати встановленим стандартам безпеки та регуляційним вимогам. Ці стандарти можуть бути як вітчизняні, так й закордонні, або взагалі внутрішніми стандартами установи. Це випробування перевіряє, чи відповідає система вимогам стандартів.
- Тестування на прохідність: дане тестування проводиться з ціллю перевірки КСЗІ на вразливість до хакерських атак. На цьому етапі проводять етичний хакінг, пенетраційні тести та будь-які інші методи з метою виявлення вразливості системи.
- Документація: вимоги випробувань повинні включати в собі ведення документації, яка буде описувати архітектуру, принцип роботи системи, інструкцію з використання та інші відповідні документи.

Власне ми складаємо такі етапи до вимог:

- Створення тестових завдань;
- Перевірка та контроль тестових завдань;
- Навчання працівників роботою з системою;
- Проведення тестової експлуатації з метою дослідження;

Тестові завдання створюються для того, аби визначити в якому напрямку буде працювати КСЗІ. Після створення завдань, проводиться подальший контроль з перевіркою завдання для того, щоб система пройшла тестові завдання для подальшого навчання працівників.

Після успішних проведень тестових завдань, для подальшої експлуатації установа повинна провести курс підготовки працівників для роботи із системою, аби отримати практичні навички з використання програмно-апаратного забезпечення, яке є наявне в установі. А також працівники засвоять потрібні вимоги до організаційних та розпорядливих документів, які відносяться до питання розмежування доступу до інформаційних ресурсів, так й технічних засобів.

Фінальним етапом випробування КСЗІ є тестова експлуатації з метою дослідження. На даному етапі відпрацьовуються технології обробки інформації та усього наявного технічного обладнання, також опрацьовуються програмні забезпечення та додаткове налагодження системи для зменшення ризику НСД. Також проводять коректування робочих та експлуатаційних документацій на цьому етапі.

Після завершення виконання вимог та за результатами даних вимог, КСЗІ відправляють на державну експертизу в разі повної готовності.

В.4 Приймання КСЗІ до проекту

Дана процедура є суто формальною, але відіграє свою роль в створення КСЗІ як повноцінної системи, так як вимагає відповідних вимог та процедур, які слідують цьому. Саме приймання КСЗІ має декілька етапів, таких як: визначення критеріїв проекту; оцінка відповідності; тестування; аудит безпеки; документування; прийняття до проекту.

- Визначення критеріїв проекту: даний етап показує, що для прийняття проекту потрібно вибудувати низку критеріїв, які повинні буть виконані перед прийняттям проекту. Ці критерії можуть бути від функціональності до відповідності стандартам, тощо.
- Оцінка відповідності: дана оцінка потрібна для того, щоб КСЗІ міг відповідати встановленим критеріям та вимогам. Ця перевірка може включати в себе, як перевірку документації, результатів проведених випробувань, аудитів безпеки та іншої відповідної діяльності до переліченого.
- Тестування: КСЗІ обов’язково повинно бути підданим до тестування задля перевірки його функціональності, надійності під час роботи та його безпеки. До таких тестувань можна віднести: пенетраційні тести; функціональні тести; тести на відновлення інформації після збоїв або зламу; тести на прохідність.
- Аудит безпеки: КСЗІ також повинно пройти обов’язковий аудит безпеки для максимальної оцінки стійкості, вразливості системи до атак та забезпечення найвищого рівня захисту. Аудит безпеки може перевірятися як зовнішніми установами, так й внутрішніми відділами.
- Документація: цей етап є формальною частиною серед вимог, але завдяки цьому є наявне підтвердження відповідності КСЗІ до усіх поставлених вимог та критеріїв. До видів документації відносять: нормативні документи, технічно-організаційні документи, протоколи тестування, звіти з аудиту безпеки, сертифікати та інші документи.
- Прийняття до проекту: після виконання усіх вимог та проходження відповідних процедур, КСЗІ тільки після цього може бути прийнятим до проекту. Таким чином, це означає, що система є придатною до експлуатації та відповідає всім вимогам захисту та безпеки інформації.

Обов’язково варто додати, що при прийнятті КСЗІ до проекту треба керуватися відповідними стандартами, політикам та регуляційним вимогам установи.

В.5 Склад документації КСЗІ

Склад документації КСЗІ варіюється в залежності від конкретних стандартів та вимог, а також від складності та типу власне самої системи, до якої буде застосована документація. Але, в нашому випадку в документації є декілька ключових елементів, які є основними її складовими: опис системи, технічна специфікація, інструкція з експлуатації,

планування безпеки, результати проведених випробувань, декларації відповідності, план реагування на інциденти.

Також загальна документація КСЗІ, може включати в себе ліцензійні угоди, відповідні сертифікати, рекомендації з розвертання КСЗІ та інші відповідні документи згідно документації. Одним з важливих моментів у веденні документації, це те що потрібно забезпечувати постійну актуалізацію та оновлення складових самої документації в разі змін у КСЗІ та відповідно вимог інформаційної безпеки.

Нижче буде опис складових елементів документації КСЗІ:

- Опис системи: даний документ містить в собі детальну інформацію про систему, яка буде встановлюватися на території державної установи або в її приміщенні. Сам документ пояснює, як працює власне сама система та які задачі, ця система виконує.
- Технічна специфікація: дана специфікація, визначає технічні властивості та характеристики КСЗІ, такі як шифрувальні алгоритми, протоколи комунікації, вимоги до програмно-апаратного забезпечення, системні вимоги, тощо. Власне, даний документ допомагає краще зрозуміти технічні деталі та аспекти КСЗІ.
- Інструкція з експлуатації: інструкція допомагає користувачам інформацію про встановлення, використання та конфігурацію КСЗІ під час експлуатації. Також дана інструкція включає в собі, параграфи про управління системою, її налагодження, резервне копіювання збереженої інформації, її відновлення після збою та інші важливі деталі.
- Планування безпеки: планування безпеки описує собою політику та заходи безпеки, що використовуються в КСЗІ. Воно включає в себе такі елементи, як заходи з авторизації, аутентифікації, шифрування, контролю доступу, захисту від вразливостей системи, аудиту та інші ключові аспекти безпеки.
- Результати проведених випробувань: в кожній документації по КСЗІ повинно бути присутніми результати усіх проведених випробувань, які були під час проектування КСЗІ включаючи в собі аналіз результатів випробувань, виявлення вразливостей системи, та власне заходів для їх вирішення.
- Декларації відповідності: документація має в собі включати декларації відповідності до відповідних стандартів та регуляційних вимог, які потребують під час проектування КСЗІ. Дані декларації підтверджують, що КСЗІ відповідає усім встановленим стандартам та вимогам установи.
- План реагування на інциденти: КСЗІ повинно містити в собі план реагування на інциденти, які можуть статися під час її експлуатації, такі як збій електроживлення або ураження кібератаками. План повинен в собі містити процедури та кроки вирішення, які слід виконувати під час виникнення небажаних подій.

В даному проекті буде використаний склад документації, що приведений вище. Так як в більшості випадків, зустрічаються саме такий склад документації. В деяких ситуаціях, склад документації може розширюватися або зменшуватися в залежності від рішення експертної комісії або інженерно-технічної команди, яка проектує дане КСЗІ.

Додаток Г

Склад засобів радіомоніторингу та вимірювання для проведення оцінки захищеності інформації від витоку за рахунок ПЕМВ та закладних пристроїв

№ з/п	Найменування	Тип	Заводський та/або інвентарний номер
1	Пошукова система З ПЕОМ (СПЗ)	DigiScanEx Samsung	інв. 1/1
2	Пристрій пошуку відеокамер та джерел радіовипромінювань	PIAC – 5 BM	B2487, інв.3
3	Індикатор поля - Частотомір	SC-1PLUS	1411-C-8683 Інв. 4
4	Детектор неоднорідностей	STANLEY S150	14W16 Інв. 6
5	Мультіметр	M-830B	Інв. 7
6	Спектраналізатор (9 кГц – 1,5 ГГц)	Agilent E7401A	US39150130 s/n 279
7	Аналізатор спектра (1 Гц – 4,4 ГГц) з комплектом антен	Signal Hound USB-SA44B	18339712
8	Антена вимірювальна дипольна (перетворювач дипольний активний ПДА 5-0) (0,009 – 1000 МГц)	АИ 5-0	К - 007
9	Пристрій розв’язуючий	УР 1,6	К - 007
10	Кабель (L=6 м.)	ВЧ	б/н
11	Кабель (L =0.25 м.)	ВЧ	б/н
12	Блок живлення стабілізований (12в.)	Panasonic	0421
13	Антена вимірювальна рамочна (0,009 – 30 МГц)	АВР-30	10649
14	Кабель	РК50-СР50	б/н
15	Струмознімач (0,009 –500 МГц)	ТИ 2-3	0056
16	Кабель	РК50-СР50	б/н
17	Допоміжні технічні засоби та інструменти	-	б\н

Роботи проводяться відповідно до документу «Методика виявлення закладних пристроїв (власної розробки з урахуванням апаратурного забезпечення), погоджена Адміністрацією Держспецзв’язку 13.03.2023 р. (№04/01/01-737ВС від 15.03.2023 р.)».