МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інноваційних освітніх технологій

Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Савченко А.С.

"_____"_____20__ р.

ДИПЛОМНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"МАГІСТР"

Тема: «Захист інформації в комп'ютерних мережах»

Студент: Мельник Олексій Юрійович

Керівник: к.т.н., доцент, Моденов Юрій Борисович

Нормоконтролер: к.т.н., доцент, Райчев І.Е.

Київ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інноваційних освітніх технологій

Кафедра комп'ютерних інформаційних технологій
Освітній ступінь: Магістр
Спеціальність: 122 «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Савченко А.С.
"_____"_____ 20__р.

З А В Д А Н Н Я

на виконання дипломної роботи
студента Мельника Олексія Юрійовича

1. Тема: *Захист інформації в комп'ютерних мережа*

затверджена наказом ректора від 22.11.2019 р. *№ 2701/ст.*

2. Термін виконання: з 25.11.2019 р. до 20.02.2020 р.

3. Вихідні дані: проаналізувати інформаційну безпеку комп'ютерних систем і мереж; проаналізувати основні методи захисту інформації в комп'ютерних системах і мережах; на основі отриманих даних створити інформаційну (автоматизовану) систему для державної служби експертного контролю та створити на її основі комплексну систему захисту інформації.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):

1. Проаналізувати інформаційну безпеку комп'ютерних систем і мереж.
2. Проаналізувати основні методи захисту інформації в комп'ютерних системах і мережах
3. Створити інформаційну (автоматизовану) систему для державної служби експертного контролю.
4. Створити комплексну систему захисту інформації для даної інформаційної (автоматизованої) системи.

КАЛЕНДАРНИЙ ПЛАН

виконання магістерської роботи

№ п/п	Етапи виконання бакалаврської атестаційної роботи	Термін виконання етапів	Примітка
1.	*Уточнення постановки задачі*	*25.11.2019-26.11.2019*	
2.	*Аналіз літературних джерел*	*26.11.2019-01.12.2020*	
3.	*Обґрунтування вибору рішення*	*01.01.2020-15.01.2020*	
4.	*Збір інформації*	*01.01.2020-15.01.2020*	
5.	*Аналіз інформаційної безпеки комп'ютерних систем і мереж*	*15.01.2020-18.01.2020*	
6.	*Аналіз методів захисту інформації в комп'ютерних системах і мережах*	*18.01.2020-20.01.2020*	
7.	*Розробка інформаційної (автоматизованої) системи для державної службі експертного контролю*	*20.01.2020-22.01.2020*	
8.	*Розробка комплексної системи захисту інформації для інформаційної (автоматизованої) системи*	*22.01.2020-15.01.2020*	
10.	*Оформлення і друк пояснювальної записки*	*15.01.2020-10.02.2020*	
11.	*Оформлення презентації*	*10.02.2020-13.02.2020*	
12.	*Отримання рецензій від опонентів*	*13.02.2020-15.02.2020*	
13.	*Захист в ДЕК*	*15.02.2020-20.02.2020*	

Студент О.Ю. Мельник

(підпис, дата)

Науковий керівник Ю.Б. Моденов

(підпис, дата)

РЕФЕРАТ

магістерської роботи Мельника Олексія Юрійовича на тему

«Захист інформації в комп’ютерних мережах»

У магістерській роботі досліджується досліджується захист інформації, що циркулює та обробляється в комп’ютерних системах та мережах організації. Дана тема є актуальною, оскільки в сучасному інформаційному просторі відбувається безліч атак на інформаційну безпеку організацій, успішність дій яких відбувається за рахунок вразливостей, що пристутні в даних системах.

Метою роботи є проведення аналізу інформаційної безпеки комп’ютерних систем та мереж, аналіз основних методів захисту інформації, що циркулює та обробляється в них.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

ІС	Інформаційна система
АС	Автоматизована система
ІС (АС)	Інформаційна (автоматизована) система
КС	Комп’ютерна система
КМ	Комп’ютерна мережа
ТС	Телекомунікаційна система
ІТС	Інформаційно-телекомунікаційна система
ЗІ	Захист інформації
КСЗІ	Комплексна система захисту інформації
ДСЕР	Державна служба експертного контролю
АСЗЕ	Автоматизована система захисту експертизи
БД	Базза даних
НД ТЗІ	Нормативний документ технічного захисту інформації
ТКВ	Технічний канал витоку
ПЕМВН	Побічне електромагнітне випромінення та наводки

1. АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

1.1 Аналіз термінології, що пов'язана з інформаційною безпекою комп'ютерних систем і мереж

Для детального розуміння того, які загрози виникають в комп'ютерних системах та мережах, методів боротьби з ними та методів захисту інформації, потрібно чітко розібратися в термінології, що пов'язана з інформаційною безпекою будь-якої організації. Перш за все – необхідно зрозуміти, що таке «інформація», «комп'ютерна мережа», «комп'ютерна система» та розібратися в схемі «вразливість-загроза-атака».

Термін «інформація» має безліч визначень, в залежності від сфери її застосування. Найбільш точно «інформація» пояснена в Законі України «Про інформацію», згідно якого, інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Зазвичай, для належного отримання доступу до інформації та її використання, в залежності від цілей, створюються інформаційні системи, в яких вона циркулює.

Інформаційна (автоматизована) система являє собою організаційно-технічну систему, що об’єднує обчислювальну (комп’ютерну) систему (апаратне та програмне забезпечення), фізичне середовище (зовнішнє середовище та контрольована зона), персонал (керівництво, адміністратори і користувачі) і оброблювальну інформацію.

Комп’ютерна система – інформаційно-технічний комплекс (сукупність апаратного та програмного забезпечення), який призначений для обробки, модифікації, вводу та виводу інформації [1, 2]. Тобто, це складова інформаційної системи.

Комп’ютерна мережа – це сукупність кінцевих (термінальних) та проміжних (комутуючих) пристроїв, а також середовища передачі інформації (провідного, безпровідного), і вся ця сукупність призначена для обробки інформації шляхом передачі її у вигляді пакетів даних, що переносяться за допомогою електромагнітних сигналів [1, 2]. Тобто, це також елемент інформаційної системи, в якій, зазвичай, кінцеві пристрої входять до комп’ютерної системи, а проміжні та середовище передачі – до телекомунікаційної системи.

Телекомунікаційна система — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Тобто, інформаційно-телекомунікаційна система складається з двох компонентів – інформаційної та телекомунікаційної систем. В свою чергу, комп’ютерна система – складова інформаційної системи, а комп’ютерна мережа включає в себе елементи інформаційно-телекомунікаційної системи.

В процесі створення та функціонування (експлуатації) будь-якої системи, в якій циркулює чи/та обробляється інформація виникають або можуть вразливості, що можуть порушити процес нормального функціонування даної системи.

Вразливість системи – нездатність системи протистояти реалізації певної загрози або ж сукупності. Тобто, як було згадано раніше, в будь-якій інформаційній системі виникають або можуть виникнути вразливості. Як наслідок – виникає загроза інформаційної безпеки (далі – загроза), яка може перерости в здійснення атаки на дану систему (далі – атака).

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою[1]. У відповідності з цілями, які ставив перед собою зловмисник, атаку можна поділити вдалу (порушення інформаційної безпеки організації) та невдалу.

Дану схему типу «вразливість-загроза-атака» можливо пояснити на прикладі присадибної ділянки. Наприклад, на даній ділянці, яка оточена по периметру дерев'яною огороджею, вирощується морква. В даній огорожі наявна дірка, яка є вразливістю. Зловмисником може виступати заєць, який використовує може використати дірку (вразливість) для того, щоб потрапити до моркви (здійснити загрозу). В результаті використані ним загрози реалізовується атака (в даному випадку на моркву).

Проаналізувавши дані поняття, стає зрозумілим те, що основні загрози неналежного використання та незаконного отримання доступу до інформації пов'язані з:

- Вразливостями, що виникають в процесі обробки інформації в комп’ютерних системах та мережах. Тобто вразливості в апаратному та програмному забезпеченні;
- Вразливостями, що виникають в процесі передачі інформації в телекомунікаційних системах, комп’ютерних системах та мережах;
- Вразливості, що пов’язані з халатністю та неналежною роботою персоналу;
- Вразливості, що пов’язані з ненадійністю програмного та апаратного забезпечення та недосконалістю систем захисту інформації;
- Вразливості, що пов’язані з порушення організаційних заходів захисту.

Для належної обробки та циркуляції інформації в інформаційних системах потрібно організувати її належний захист.

захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [Закон України “про інформацію»].

Зазвичай, основні засади захисту інформації прописані в політиці безпеки інформації. Політика безпеки організації – це сукупність керівних принципів, правил, процедур і практичних прийомів в галузі безпеки, які регулюють управління, захист і розподіл цінної інформації. Якщо коротко, то це набір правил що реалізується в функціоналі певного програмного чи апаратного забезпечення, які необхідні для використання в певній інформаційній системі.

Для уникнення ситуацій незаконного ознайомлення, використання чи модифікації інформації, що циркулює в певній інформаційній системі організації,

та запобіганню її витоку за межі інформаційного середовища організації – створюються комплексні системи захисту інформації.

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. [Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних"]

1.2 Основні види загроз інформаційної безпеки комп’ютерних систем і мереж

У кожній інформаційній системі повинні бути забезпечені механізми (методи, засоби та способи) захисту інформації, що циркулює в системі, та процесів її обробки. Для здійснення належного захисту потрібно регулярно проводити пошук вразливостей, які можуть призвести до порушення основних властивостей інформації – її конфіденційності, цілісності та доступності.

Також, загрози безпеці комп’ютерних систем та мереж, а також інформації, що в ній циркулює, прийнято розрізняти за властивостями інформації, які може порушити певна загроза. Тобто, це:

- Загроза порушення конфіденційності інформації;
- Загроза порушення цілісності інформації
- Загроза порушення доступності інформації (порушення працездатності системи).

Конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення [**У К АЗ ПРЕЗИДЕНТА УКРАЇНИ Про Положення про технічний захист інформації в Україні]**

Порушення конфіденційності пов’язане з незаконним розголошенням інформації з обмеженим доступом (конфіденційної, службової чи таємної), що належить чи/та циркулює в комп’ютерних системах та мережах державних чи комерційних організацій. В результаті реалізації даних загроз (здійснення інформаційних атак) зловмисники отримують несанкціонований доступ до інформації, що зберігається та обробляється в комп’ютерній системі або ж передається між комп’ютерними системи за допомогою комп’ютерної мережі.

Цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення [**У К АЗ ПРЕЗИДЕНТА УКРАЇНИ Про Положення про технічний захист інформації в Україні].**

Порушення цілісності пов’язане з незаконною модифікацією інформації з обмеженим доступом чи відкритої інформації, що зберігається та обробляється в комп’ютерній системі або ж передається між комп’ютерними системи за допомогою комп’ютерної мережі. Дана властивість інформації може зазнати порушення у зв’язку з навмисними діями зловмисника, або ж в результаті впливу зовнішнього середовища, що оточує систему. Зазвичай, це одна з найбільш поширених загроз інформації та виникає у зв’язку неналежною передачею її за допомогою комп’ютерних мереж та телекомунікаційних мереж/систем.

Доступність – властивість інформації бути захищеною від несанкціонованого блокування [**У К АЗ ПРЕЗИДЕНТА УКРАЇНИ Про Положення про технічний захист інформації в Україні].**

Порушення доступності (працездатності системи) пов’язане з створення ситуацій, які погіршують працездатність інформаційних систем та/чи блокування

доступу до її ресурсі. Як приклад, під час вдалого здійснення атаки на доступність – користувач інформаційної системи не зможе отримати санкціонований доступ до інформації, що в ній зберігається та обробляється. Тобто, виникає ситуація відмови в обслуговувані. Атаки на доступність можуть мати постійний та тимчасовий характер, і зазвичай, здійснюються, як підготовчий етап перед здійсненням атак на цілісність та конфіденційність.

Порушення даних властивостей інформації може виникати за рахунок різноманітних небезпечних впливів на інформаційну систему. Зазвичай, це пов’язано з складністю ІС та вразливостями, що можуть виникнути при пошкодженні чи належній діяльності її елементів. Основними компонентами будь-якої інформаційної системи, в яких виникають вразливості, виступають:

- Програмне забезпечення;
- Апаратно-технічний комплекс;
- Персонал;
- Інформація, що циркулює та обробляється.

Небезпечні впливи, що виникають в комп’ютерних мережах та системах, можуть бути випадковими (природними) та створені зловмисниками (штучні). Випадкові впливи з’являються в процесі виникнення природних катаклізмів, надзвичайних ситуацій, що виникають в процесі діяльності апаратно-технічного комплексу, програмного забезпечення та персоналу, що обслуговує дані системи та мережі. Наприклад:

- помилки, що виникають в діяльності програмного забезпечення;

- помилки, що виникають в діяльності обслуговуючого персоналу та користувачів;
- аварійні ситуації, що виникають внаслідок стихійних лих та відключенням електричного живлення в приміщеннях, в яких працює інформаційна система;
- відмови в роботі та збої апаратури;
- завади в лініях зв'язку, що виникають внаслідок несприятливого впливу зовнішнього середовища.

Штучні впливи (загрози) виникають у результаті дій порушника. Порушниками можуть виступати, як санкціоновані особи (персонал, що обслуговує ІС) так і несанкціоновані особи (звичайний перехожий, відвідувач організації, конкурент, т.д.). Зазвичай атаки на основі штучної загрози виникають після детального аналізу всіх чи основних критичних елементів організації, на які можна здійснити успішну атаку. Наприклад:

- порушнику відомі організаційні та програмно-технічні принципи функціонування системи;
- порушник ознайомлений з логічною та/чи фізичною топологію комп'ютерної мережі організації. Як варіант, він може бути з числа обслуговуючого персоналу, що полегшує реалізацію атаки на інформаційну систему;
- порушник зміг підкупити чи залякати працівника організації з метою здійснення незаконних дій;
- і т.д.

Основними прикладами штучних загроз можуть бути: [130]:

- несанкціонований доступ сторонніх осіб, які не входять в число обслуговуючого персоналу
- ознайомлення обслуговуючого персоналу, адміністраторів системи чи її користувачів, з інформацією, до якої їм не надано доступ;
- несанкціоноване модифікування або ж копіювання програмних засобів та інформації;
- викрадення чи несанкціоноване створення/модифікація/знищення роздрукованих документів;
- викрадення матеріальних носіїв, що містять інформацію з обмеженим доступом;
- навмисне незаконне знищення інформації;
- відмова від авторства повідомлення, переданого каналом передачі даних;
- фальсифікація повідомлень, що передаються по каналах передачі даних;
- відмова від факту отримання інформації;
- незаконне знищення чи модифікація звітних, фінансових документів та баз даних;
- викрадення зразків апаратного забезпечення чи програмного забезпечення, що зберігається на матеріальних носіях;
- знищення чи модифікація інформації, яка розташована на змінних носіях даних.

1.3 Основні напрямки захисту інформації в комп’ютерних системах і мережах

Одним з основних напрямків захисту інформації в комп'ютерних системах та мережах є використання технічного захисту інформації (ТЗІ). Зазвичай, ТЗІ проектуються та створюються в комплексах технічного захисту інформації, які є складовими комплексних систем захисту інформації. Головне призначення ТЗІ – вирішувати наступних клас задач інформаційної безпеки організації:

- захист інформації від несанкціонованого доступу (НСД);
- захист інформації від витоку технічними каналами.

1.3.1. Несанкціонований доступ до інформації

Несанкціонований доступ – це доступ до інформації в інформаційних (автоматизованих) системах з використанням засобів, включених до складу комп’ютерних систем (КС), що порушує встановлені правила розмежування доступу (ПРД) [13].

Несанкціонований доступ може здійснюватися:

- З використанням штатних засобів, програмно-апаратного забезпечення, що внесені до складу комп’ютерних систем розробником під час розробки або системним адміністратором в процесі експлуатації;
- З використання програмно-апаратних засобів, включених до складу комп’ютерних систем зловмисником.

Як приклад використання штатних засобів комп'ютерної системи – є ситуація із несанкціонованим застосування зловмисником комп'ютера локальної мережі для доступу до чужих файлів.

До основних способів несанкціонованого доступу відносяться:

- Безпосереднє звертання до об'єктів з метою одержання певного виду доступу;
- Створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
- Модифікація засобів захисту, що дозволяє здійснити несанкціонований доступ;
- Впровадження в комп'ютерних системах програмних або апаратних механізмів, що порушують структуру і функції комп'ютерних систем і дозволяють здійснити несанкціонований доступ.

Під захистом від несанкціонованого доступу, слід розуміти діяльність, спрямовану на забезпечення додержання правил розмежування доступу шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації.

1.3.2. Технічні канали витоку інформації

Під час обробки інформації можуть виникати умови для неконтрольованого розповсюдження, що призводить до її несанкціонованого одержання сторонніми особами. Такі ситуації прийнято називати «витоком інформації». Під «технічним каналом витоку інформації» розуміють сукупність джерела носія інформації, середовища його поширення та засобу технічної розвідки [8]. В основі поширення інформації в просторі лежать фізичні процеси різної природи. При використанні таких процесів носієм інформації є сигнали.

Сигнал – це структурований фізичний процес, який здатний поширюватися через фізичне середовище та переносити інформацію в значеннях свої параметрів. З позицій забезпечення безпеки інформації доцільно розрізняти технологічні та небезпечні сигнали. Під технологічними сигналами слід розуміти такі сигнали, формування, розповсюдження і використання яких передбачено технологією обробки інформації. Під небезпечними сигналами розуміють такі сигнали, формування, розповсюдження і використання яких не передбачено технологією обробки інформації. Формування небезпечних сигналів, як правило, є результатом недоробки розробників ТОІ, або – порушенням правил експлуатації систем, які реалізують технології обробки інформації. Такий підхід до розгляду сигналів, існуючих під час обробки інформації, дозволяє представити технічний канал витоку інформацією структурою представленою на рис. 1.1

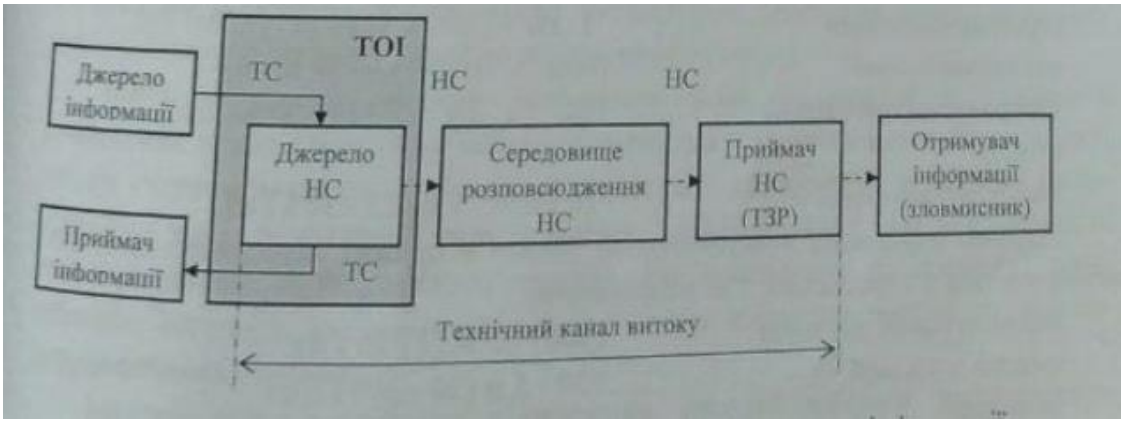


Рис 1.1. Структура технічного каналу витоку інформації

1.4 Висновок за розділом

У першому розділі було проведено аналіз інформаційної безпекою комп’ютерних систем і мереж. Було детально проаналізовано термінологію, що пов’язана з інформаційною безпекою комп’ютерних систем і мереж, розглянуто основні види загроз інформації та напрямки її захисту.

Даний аналіз потрібен для подальшого розуміння методів захисту інформації, які будуть описані в розділі 2.

2. АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

2.1 Аналіз основних принципів організації захисту інформації

Організація захисту інформації – це складний, комплексний та безперервний в часі процес, що пов'язаний із захистом інформаційного середовища організації, в якій циркулює інформація. Даний захист пов'язаний не лише з надійністю програмних та апаратних засобів, а й з організаційними процесами та належною роботою обслуговуючого персоналу. Слід пам'ятати наступні правила забезпечення захисту інформації:

- Завжди потрібно організовувати якісну підготовку користувачів та дотримання ними правил захисту;
- Безпека інформації в комп'ютерних системах та мережах організації може бути здійснена належним чином лише за умови комплексного використання засобів захисту;
- Безпека інформації безперервний в часі процес, що потребує постійного виявлення слабких (вразливих) місць в системі захисту, систематичного контролю захищеності та вдосконалення методів, засобів та способів, що використовуються в системах захисту;

- Завжди пам’ятайте, що жодна система захисту не вважається абсолютно надійною. Зловмисники завжди можуть знайти нові вразливості на які здійснять інформаційну атаку.

2.2 Канали витоку інформації

Технічний канал витоку інформації (який було згадано раніше) – це один із компонентів каналу витоку інформації. В свою чергу, канал витоку інформації – це сукупність джерела інформації, матеріального носія або середовища поширення, що несе цю інформацію у вигляді сигналу і засобів виділення інформації з сигналу або носія.

Найбільш поширені та відомі наступні канали витоку інформації:

1. Електромагнітний канал. Даний канал створюється внаслідок виникнення електромагнітного поля, яке пов’язе з проходженням електричного струму в технічних засобах обробки інформації. Також, дане поле створювати (індукувати) струми в неподалік розташованих дротяних лініях, так звані наводки. Основними видами електромагнітного каналу є:
   1.1. Низькочастотний канал.
   1.2. Мережевий канал (наводки на дроти заземлення).
   1.3. Радіоканал (високочастотні випромінювання).
   1.4. Канал заземлення (наведення на дроти заземлення).
   1.5. Лінійний канал (наводки на лінії зв'язку між ПЕОМ).
2. Акустичний канал. Він пов'язаний з поширенням звукових хвиль в повітрі або пружних коливань в інших середовищах, що виникають при роботі пристроїв відображення інформації.
3. Канал несанкціонованого копіювання.
4. Канал несанкціонованого доступу.

2.3 Організаційні та організаційно-технічні заходи захисту інформації в комп’ютерних системах та мережах

Організаці́йний за́хист інформа́ції — це захист інформації шляхом регулювання за допомогою організаційних заходів доступу до всіх ресурсів інформаційної системи [ ]. Тобто, даний вид захисту здійснюється за рахунок належного дотримання персоналом, що обслуговує інформаційні системи організації (комп’ютерні системи та мережі), правил експлуатації системи з метою забезпечення заданого рівня безпеки.

Основними організаційними заходами захисту інформації слугують:

1. Процес обмеження допуску та доступу в приміщення та установи, в яких здійснюється обробка інформації з обмеженим доступом (конфіденційна, службова, таємна). Допуск та доступ повинні надаватися спеціальними посадовими особами, на яких покладені дані функції, лише тим довіреним працівникам та при виникненні необхідності роботи з даною інформацією. В державних установах такі обов’язки покладені на режимно-секретні підрозділи;
2. Збереження матеріальних носіїв даних в спеціальних, захищених, вогнестійких металевих шафах чи приміщення;
3. Виділення однієї чи декількох персональних електронно-обчислювальних машин для роботи з інформацією із обмеженим доступом;
4. Встановлення пристроїв введення та виведення інформації таким чином, щоб виключити можливості несанкціонованого ознайомлення, використання та обробки інформації

5. Постійний контроль адміністратором безпеки організації чи окремого її підрозділу за роботою принтера та інших пристроїв виведення з метою захисту від захисту від витоку інформації за межі організації;
6. Здійснення процедури належної утилізації та знищення матеріалів, що містять фрагменти важливої для організації інформації. Наприклад, в державних організаціях використовують шредери для знищення непотрібних паперових документів. Після чого залишки паперу спалюються в спеціальних печах;
7. Заборона ведення переговорів про зміст інформації з обмеженим доступом;
8. Заборона використання незареєстрованих мобільних телефонів, планшетів, комп'ютерів та інших пристроїв зчитування інформації під час роботи з інформацією з обмеженим доступом

Організаційно-технічні захист інформації за своїм принципом схожий на організаційний. Відрізняються вони лише відсутністю використання технічних засобів захисту інформації в останнього.

Основними організаційно-технічними заходами захисту інформації слугують:

1. Процес обмеження доступу всередину корпусу персональних електронно-обчислювальних машин шляхом встановлення механічних запірних пристроїв;
2. Процедура знищення інформації на жорстких дисках персональних електронно-обчислювальних машин при необхідності відправлення їх в ремонт. Знищення інформації потрібно проводити з використанням засобів низькорівневого форматування;
3. Здійснювати живлення персональних електронно-обчислювальних машин від окремих джерел живлення. При їх відсутності – можна

використовувати загальну (міську електромережу) за умови наявності стабілізатора напруги (мережевого фільтру);

4. Використання лише рідкокристалічних або плазмових дисплеїв для відображення інформації, а для її друку – струменевих або лазерних принтерів;
5. Потрібно розміщувати системний блок, пристрої введення та виведення інформації не менше ніж 2,5-3,0 метрів від пристроїв освітлення, кондиціонування повітря, зв'язку (телефону), металевих труб, телевізійної та радіоапаратури, а також інших персональних електронно-обчислювальних машин, що не використовуються для обробки конфіденційної інформації;
6. Відключення персональних електронно-обчислювальних машин від глобальної мережі Інтеренет при обробці на них інформації з обмеженим доступом;
7. Установка принтера і клавіатури на м'які прокладки з метою зниження витоку інформації по акустичному каналу;
8. Під час обробки цінної інформації на персональних електронно-обчислювальних машинах рекомендується включати пристрої, що створюють додатковий шумовий фон (кондиціонери, вентилятори);
9. Потрібно знищувати інформацію після того, як відпала необхідність роботи з нею чи/та вона втратила свою актуальність.

2.4 Основні методи захисту ПЕОМ від витоків інформації по електромагнітному каналу

Основним джерелом високочастотного електромагнітного випромінювання – є монітори (екрани персональних електронно-обчислювальних машин).

Порушення політики безпеки організації може призвести до витоку через дані монітори інформації, яку можна перехоплювати на відстані сотень метрів. Повністю перешкодити витік з даних пристроїв можливо при встановлені на жалюзів на вікнах, випромінювачів акустичного шуму на вікнах та системах опалення, а також використання генератору шуму. Найпростіший спосіб захисту – використання плазмових або рідкокристалічних дисплеїв.

Іншим надійним способом захисту – є повне екранування приміщення сталевими алюмінієвими листами товщиною не менше 1 мм з надійним заземленням.

Основним джерелом низькочастотного електромагнітного випромінювання – є принтер. Дане джерело випромінювання також є небезпечним. Для боротьби з ним потрібно створювати потуний шумовий сигнал (наприклад, за допомого генератора шуму). Або ж використовувати струменеві чи лазерні принтери.

Також джерелом небезпеки можуть слугувати спеціально вбудовані в персональні електроно-обчислювальні машини передавачів та радіомаяків (закладок), що допомагають зловмиснику перехопити інформацію за допомогою технічного каналу витоку. Тому, забороняється обробляти інформацію на незахищених, незареєстрованих пристроях. Перед відправленням комп’ютера в ремонт потрібно впевнитись, що в ньому немає закладок.

Потрібно забезпечити уникнення ситуацій перетину зовнішніх провідників і кабелів комп’ютерів, на яких обробляється інформація з обмеженим доступом, з проводами, що виходять за межі приміщення.

Монтаж заземлення від периферійного обладнання потрібно проводити в межах контрольованої зони. Не можна допускати, щоб заземлення зустрічалося з іншими провідниками.

Основними сервісами, що забезпечують інформаційну безпеку організації є:

- Управління доступом,
- Протоколювання і аудит,
- Криптографія,
- Екранування.

2.5 Управління доступом

Управління доступом – це процес контролю дій, які користувачі інформаційної системи та процеси, що в ній виникають, можуть здійснюватися над інформаційними комп'ютерними ресурсами системи. Тобто, даний процес, виконується за допомогою спеціальних програмних засобів. Логічне управління доступом – це головний спосіб забезпечення конфіденційності та цілісності інформації в багатокористувацьких системах. Ціль логічного управління доступом – визначення допустимих операцій, які можуть виконувати користувачі чи процеси та контроль виконання встановленого порядку.

Даний вид контролю здійснюється завдяки різноманітним програмним компонентам інформаційного середовища. Наприклад, системою управління базами даних чи ядром операційної системи.

Для надання прав доступу до певного інформаційного ресурсу системи потрібно проаналізувати наступні параметри:

- Ідентифікатор суб'єкта (код користувача, мережеву адресу комп'ютера);
- Місце виникнення певної дії (системна консоль, надійний вузол мережі).
- Час виникнення дії;
- Внутрішні обмеження сервісу (кількість користувачів які можуть одночасно працювати з певним інформаційним ресурсом системи згідно з політики безпеки організації чи/та ліцензії на програмний продукт, який використовує користувач).

2.6 Протоколювання та аудит

Протоколювання – це процес збору та накопичення інформації про всі події, що відбуваються в інформаційній системі організації (в її комп’ютерних системах та мережах). В кожному сервісі виникає певний набір подій, які можна поділити на:

- Зовнішні – події, що створені діями інших сервісів;
- Внутріші – події, що створені діями самого сервісу;
- Клієнтські – події, що створені діями адміністраторів чи користувачі інформаційної системи.

Аудит – це процес накопичення інформації про стан інформаційної системи. Даний процес проводиться оперативно, в режимі реального часу, та/або періодично.

Причини використання протоколювання та аудиту наступні:

- Вчасне виявлення спроб порушень інформаційної безпеки організації;
- Надання можливості реконструкції послідовності подій;
- Належний контроль діяльності адміністраторів та користувачів інформаційної системи організації. Тобто, якщо персонал знає про те, що всі їхні дії фіксуються, вони будуть утримаються від незаконної діяльності. Також процедура даного контролю дозволє здійснювати відкат некоректних змін в системі;
- Забезпечення належного та своєчасного виявлення проблем в роботі інформаційної системи та причин їх виникнення. Це дозволяє поліпшити таку властивість інформації як доступність.

2.7 Криптографія

Найбільш популярним, потужним та надійним засобом захисту інформації, забезпечення її конфіденційності та контролю цілісності. Вона займає центральне місце серед програмно-технічних регуляторів безпеки.

Виділяють два основні методи шифрування – симетричні та асиметричні. При симетричному шифруванні використовується один і той самий ключ для шифрування та розшифрування повідомлення. Головним недоліком даного виду шифрування є те, що ключ одночасно повинен бути відомий як відправнику повідомлення, так і одержувачу. Як результат – виникає проблема в надійному та захищеному способі передачі даних ключів. Якщо зловмисник зуміє отримати ключ – він зможе використати його для отримання несанкціонованого доступу до шифрованої інформації, що передається в мережі. Звичайно, якщо знайде спосіб її перехоплення.

При асиметричній криптографії використовуються два ключа. Тобто, кожен користувач системи передачі повідомлень має два ключі – один, відкритий (несекретний), для шифрування повідомлення, а другий – закритий (секретний), який використовується для розшифрування повідомлення та відомий лише одержувачу. Найбільш популярними алгоритмами асиметричного шифрування, що використовуються навіть в мережі Інтернет, є алгоритм RSA та Діффі-Хелмана.

Ще однією позитивною стороною асиметричної криптографії – є можливість реалізації електронного цифрового підпису. Даний підпис використовується для належного встановлення (ідентифікації) особи чи пристрою в мережі. Тобто, підтвердження того факту, що пристрій чи особа насправді є тією, за кого себе видає.

Головним недоліком асиметричних методів криптографії є їх низька швидкодія. Як висновок, їх потрібно поєднувати належним чином з симетричними методами. Так, для вирішення завдання розсилки ключів повідомлення спочатку симетрично шифрують випадковим ключем, потім цей ключ шифрують відкритим асиметричним ключем одержувача, після чого повідомлення і ключ відправляються по мережі.

Також криптографічні методи надають змогу контролювати цілісність інформації, що передається по комп’ютерним мережам. Криптографічна контрольна сума (імітовставка), що обчислюється із застосування секретного ключа, знешкоджує всі можливості непомітної зміни даних.

2.8 Екранування

Процес екранування - це процес з використанням засобів розмежування доступу клієнтів з одного засобу обробки інформації чи групи засобів до іншої засобу чи групи засобів. Екран виконує функції контролю інформаційних потоків між двома множинами систем.

Екран може складатися з механізмів обмеження чи сприяння переміщення даних між засобами обробки інформації. Прикладом екранів можуть виступати фільтри, що виконують функції затримання чи переміщування інформації.

Екрани використовуються не лише для функцій розмежування доступу, але й для забезпечення протоколювання інформаційних обмінів.

Зазвичай, екрани використовуються для розмежування внутрішньої комп'ютерної мережі від загроз, що знаходяться в зовнішній, до якої організація може бути підключена. Міжмережеві екрани використовують для захисту локальної комп'ютерної мережі організації, що має вихід у відкрите середовище, наприклад, мережу Інтернет.

2.9 Висновок за розділом

У даному розділі було проаналізовано основні методи захисту інформації в комп’ютерних системах і мережах. Було отримано повну картину, що пов’язані з даними методами. А саме, отримано такі її компоненти, як основні принципи організації захисту інформації, канали витоку інформації, організаційні та організаційно-технічні заходи захисту та основні сервіси, що забеспечують інформаційну безпеку організації.

Дані результати, а також результати аналізу розділу 1, будуть використовуватися в якості фундаменту для практичної частини магістерської дипломної роботи.

3. РОЗРОБКА ІНФОРМАЦІЙНОЇ (АВТОМАТИЗОВАНОЇ) СИСТЕМИ ДЛЯ ОРГАНІЗАЦІЇ ДСЕР ТА СТВОРЕННЯ НА ЇЇ ОСНОВІ КСЗІ

3.1 Аналіз призначення ДСЕР та принципів її функціонування

У розділах 1 та 2 було проаналізовано основи інформаційної безпеки в комп’терних системах та мережах, а також методи захисту в даних системах та мережах, відповідно. На основі проаналізованих даних, додаткових відкритих джерел інформації, щодо інформаційного захисту, та нормативно-технічних документів технічного захисту інформації – потрібно створити інформаційну (автоматизовану) систему для Державної служби експертного регулювання, а також створити комплексну систему захисту інформації для даної оргнізації.

Для початку, слід проаналізувати постановку задачі на створення інформаційної (автоматизованої) системи. Тобто, проаналізувати сутність роботи та цілі діяльності організації.

Державна служба експертного регулювання (*ДСЕР*, далі - *Служба*) здійснює контроль у сфері експорту-імпорту товарів (технологій) військового та подвійного призначення. Контроль здійснюється шляхом експертизи заяв суб'єктів експорту-імпорту на предмет відповідності:

- державній системі нормативно-правового регулювання у цій сфері;
- міжнародним зобов'язанням держави.

З метою підвищення ефективності роботи Служби її керівництво прийняло рішення про створення інформаційної системи забезпечення експертизи (далі - ІСЗЕ), основними завданнями якої є:

- зниження часу підготовки документів експертизи;
- поліпшення якості контролю виконання функціональних завдань;
- підвищення оперативності управління підрозділами;
- інформаційно-аналітичне забезпечення керівництва Служби за рахунок організації доступу до ресурсів WWW;
- інформування клієнтів Служби про порядок оформлення матеріалів заяв шляхом створення свого інформаційного порталу в Інтернет;
- забезпечення безпеки інформаційних ресурсів Служби.

3.1.1 Аналіз процедур діяльності організації

Процедура експертизи складається з наступних етапів:

1) ***прийом та реєстрація формалізованих заяв*** від суб'єктів зовнішньоекономічної діяльності на предмет отримання державного дозволу на здійснення експорту-імпорту товарів (кожна заява має текстові і графічні додатки з опису товарів). По кожній заявці

формується формалізована ***контрольна картка***, якої присвоюється унікальний номер;

Примітка:

*a) етап здійснює **відділ 1;***

b)** заява та її додатки становлять **матеріали заяви;

c) заява містить наступну інформацію про експортну (імпортну) операцію:

- *назва товару;*
- *код товару;*
- *кількість товару;*
- *код операції (експорт/імпорт);*
- *країна призначення експорту (імпортер);*
- *фірма (компанія) призначення експорту (імпортер).*

2) ***тематична експертиза матеріалів заяви*** державними експертами ДСЕР (далі - «експертиза»). Результати експертизи відображаються в контрольній картці (відмітки «дозволяється» або «не дозволяється відповідно до пунктів № № ... нормативного акта № ...»; підписи державного експерта та начальника відділу);

*Примітка: етап здійснюють **відділи тематичної експертизи;***

3) ***затвердження результатів експертизи*** здійснюється шляхом підготовки ***зведених відомостей*** експертизи за місяць (у вигляді таблиці), які передаються в профільну комісію Кабінету Міністрів. Результати експертизи за кожною заявою затверджуються (не затверджуються).

Примітка:

a) *у таблиці* ***(зведені відомості)*** *для кожної заяви виділений 1 рядок, в полях якого відображені основні дані за матеріалами заяви та їх експертизі;*

b) *таблицю і супровідний лист формує* ***відділ інформаційно-аналітичного забезпечення*** *(ВІАЗ);*

c) *документи відправляє РСВ.*

4) ***підготовка і видача державних дозволів*** на право експорту-імпорту товарів здійснюється після прийняття рішення профільної комісії Кабінету Міністрів (далі - ПККП). Дозвіл оформляє *ВІАЗ* на стандартному нумерованому бланку суворої звітності, який підписує голова ДСЕР. Видачу дозволів здійснює *РСВ*. ***Матеріали архіву*** (тобто матеріали заяви, затверджена контрольна картка, копія оформленого дозволу) зберігаються в архіві служби.

Для ДСЕР визначена наступна ***організаційно-штатна структура*** (табл. 1):

Табл. 1

№ з/п	**Посада**	**Кіл.**	**Посадові обов'язки**
1	Голова служби	1	Організація роботи з органами державного управління, поточний контроль і управління
2	Заступник голови служби	1	Організація взаємодії підрозділів служби, поточний контроль и управління
	Реєстраційно-архівний відділ (відділ 1)		
3	Начальник відділу	1	Організація нетаємного документообігу в службі.
4	Провідний спеціаліст	3	Облік матеріалів заяв. Оформлення контрольних карток.
5	Спеціаліст	2	Облік вхідної та вихідної несекретної кореспонденції.

			Облік і ведення архіву.
	Відділ експертизи озброєння і військових технологій (відділ 2)		
6	Начальник відділу	1	Організація експертизи в відділі. Затвердження її результатів
7	Провідний спеціаліст	2	Державна експертиза матеріалів заяв.
	Відділ експертизи криптозасобів і спеціальної техніки (відділ 3)		
8	Начальник відділу	1	Організація експертизи в відділі. Затвердження її результатів
9	Державний експерт	3	Державна експертиза матеріалів заяв.
	Відділ експертизи хімічних товарів і технологій (відділ 4)		
10	Начальник відділу	1	Організація експертизи в відділі. Затвердження її результатів
11	Державний експерт	4	Державна експертиза матеріалів заяв.
	Відділ експертизи ядерних товарів и технологій (відділ 5)		
12	Начальник відділу	1	Організація експертизи в відділі. Затвердження її результатів
13	Державний експерт	1	Державна експертиза матеріалів заяв.
	Відділ інформаційно-аналітичного забезпечення (відділ 6)		
14	Начальник відділу	1	Організація роботи відділу і взаємодія з ПМКК
15	Провідний спеціаліст	2	Автоматизація процедур експертного контролю. Адміністрування безпеки інформації. Формування аналітичних матеріалів за запитом Голови служби. Інформування суб'єктів експортно-імпортної діяльності про діяльність ДСЕР
16	Спеціаліст	1	Підготовка зведених відомостей за матеріалами експертизи і супровідного листа.

	Режимно-секретний відділ (відділ 7)		
17	Начальник відділу	1	Організація таємного документообігу в службі.
18	Провідний спеціаліст	1	Прийом та видача таємних документів співробітникам ДСЕР. Організація підготовки таємних документів співробітниками служби. Реєстрація та облік вхідних і вихідних документів
19	Спеціаліст	2	Реєстрація та видача дозволів. Підготовка матеріалів експертизи для передачі до архіву.

ДСЕР розміщена в окремому одноповерховому будинку. *План приміщень організації* та порядок розміщення підрозділів в них представлений у ***додатку 1***. План розміщення будівлі представлений в ***додатку 2***.

У приміщеннях 122, 123, 124 відповідно розташовані Голова служби, його заступник і режимно-секретний відділ. У приміщенні 120 знаходиться робоче місце чергового по Службі. Тут же в години прийому здійснюється прийом заявок та видача дозволів.

Архів організації розміщений у окремому приміщенні відділу 1.

3.1.2 Особливості діяльності організації

Характеристики інформації за режимом доступу надаються в *таблиці 2*.

Всі приміщення обладнані:

- системою внутрішнього телефонного зв’язку (офісна АТС знаходиться в приміщенні 120). До АТС підключені три виділені лінії зв'язку до міської АТС. Телефони внутрішнього зв'язку мають вихід в міську телефонну мережу загального користування;

- системою протипожежної сигналізації. Центральний пульт розташований у приміщенні 120;
- системою централізованого опалення;
- системою електроосвітлення;
- системою електроживлення. Трансформаторна станція системи електропостачання розташована на території ДСЕР;
- системою заземлення. Контур заземлення розташований на території ДСЕР;
- системою охоронної сигналізації. Центральний пульт розташований у приміщенні 120. По периметру огорожі території ДСЕР розташовані камери відеоспостереження. Пульт керування системою відеоспостереження також розташований в приміщенні 120.

Кількість категорій співробітників в відділах експертизи

Таблиця 1

	Номера позицій організаційно-штатної структури								
	4	5	7	9	11	13	15	16	19
Кількість співробітників	3	2	2	3	4	1	2	1	2

Характеристики інформації за режимом доступу.

Таблиця 2

	Посадові особи, підрозділи							
	Голова, заступник голови	**Від. 1**	**Від. 2**	**Від. 3**	**Від. 4**	**Від. 5**	**Від. 6**	**Від. 7**
1. Матеріали заяв	**ВІ**	**ВІ**	**ВІ**	**ВІ**	**ВІ**	**ВІ**	**-**	**-**
2. Контрольні карточки	**-**	**ВІ**	**Т**	**ДСК**	**Т**	**Т**	**-**	**-**

3. Дозволи	**ВІ**	**-**	**-**	**-**	**-**	**-**	**ВІ**	**ВІ**
4. Зведені матеріали експертизи за місяць	**ЦТ**	**--**	**-**	**-**	**-**	**-**	**ЦТ**	**_**
5. Матеріали архіву	**-**	**Т**	**-**	**-**	**-**	**-**	**-**	**-**
6. Супровідні листи								**ЦТ, Т**

3. Відділ 1. Додаткове обладнання в приміщеннях.

Таблиця 4

	Найменування обладнання	Кількість в одному приміщенні	Номера приміщень
1.	Телефони та лінії міського телефонного зв'язку	1	102- 105, 122, 123, 124
2.	Телевізори	1	101-105, 122, 123, 120
3.	Копіювальні пристрої.	1	101, 120, 123,
4.	Холодильники.	1	101-104, 122, 123
5.	Системи кондиціювання.	1	101-103, 122
6.	Радіоприймач.	1	101-106, 122
7.	Центральний пульт і лінії системи ГГЗ.	1	122, 123
8.	Абонентський пульт и лінія системи ГГЗ.	1	101-103, 120, 123 124.

3.2 Створення ІС для організації ДСЕР

Тобто, потрібно створити інформаційну систему (до складу якої будуть входити комп’ютерні системи та мережі) що буде виконувати завдання, що покладаються на Службу. І на основі створеної ІС – створити комплексну систему захисту інформації для даної ІС.

3.2.1 Формалізовані результати аналізу інформаційного середовища установи

В результаті аналізу інформаційного середовища ДСЕР необхідно сформувати ряд інформаційних потоків організації ДСЕР, які представляються у виді вхідної, вихідної інформації та технології обробки інформації.

В загальному вигляді ІТС – це складна організаційно-технічна структура, що поєднує в собі Інформаційну систему (ІС) та Телекомунікаційну систему (ТС).

Складність такої структури полягає в тому, що не можливо однозначно (з 100% гарантією) описати процеси в цій системі. Якісний результат розробки нових та модернізація застарілих компонентів складних систем залежать від способів коректного опису їх внутрішніх процесів та зовнішніх факторів, що впливають на ці процеси.

Для аналізу інформаційного середовища організації ДСЕР було використано методику аналізу на основі інформаційно-функціональної структури.

Структура – це характеристика системи, яка описує систему в виді сукупності частин системи і зв’язків між ними.

Функціональна структура – це структура в якій частини системи представляються у вигляді функцій, перетворювань, дій.

Інформаційно-функціональна структура - це функціональна структура в якій зв’язки відповідають обміну інформацією між частинами.

Технологія обробки інформації – сукупність функцій і зв’язків між ними, що перетворюють вхідну інформації у вихідну.

Сутність методики:

- Визначення інформаційних потів, що описують всіх інформаційні процеси які відбуваються в організації ДСЕР;
- ТОІ організації за допомогою методу ієрархічних декомпозицій розкладається в вигляді сукупності внутрішніх інформаційних потоків (процедура опису “чорного ящика”);
- Кожний внутрішній інформаційний потік декомпозується у вигляді інформаційно-функціональної структури.

Ієрархічна декомпозиція – це розбиття системи на модулі і рівні:

1) Модуль вищого рівня реалізується функціями нижчого рівня.

2) Внутрішні інформаційні потоки рекомендують обмежувати вхідною (вихідною) інформацією підрозділу організації.

3) Рівень деталізації рекомендується обмежети функціями персоналу.

Інформаційний потік – це характеристика процесу обробки інформації, яка об’єднує: вхідну, вихідну інформацію обробки та сукупність функцій (дій), що реалізують цей вид обробки інформації.

3.2.1.1. Перелік інформаційних потоків

Перелік інформаційних потоків організації ДСЕР представлений в таблиці 1.1.1. Він складається з вхідної, вихідної інформації та технології обробки інформації.

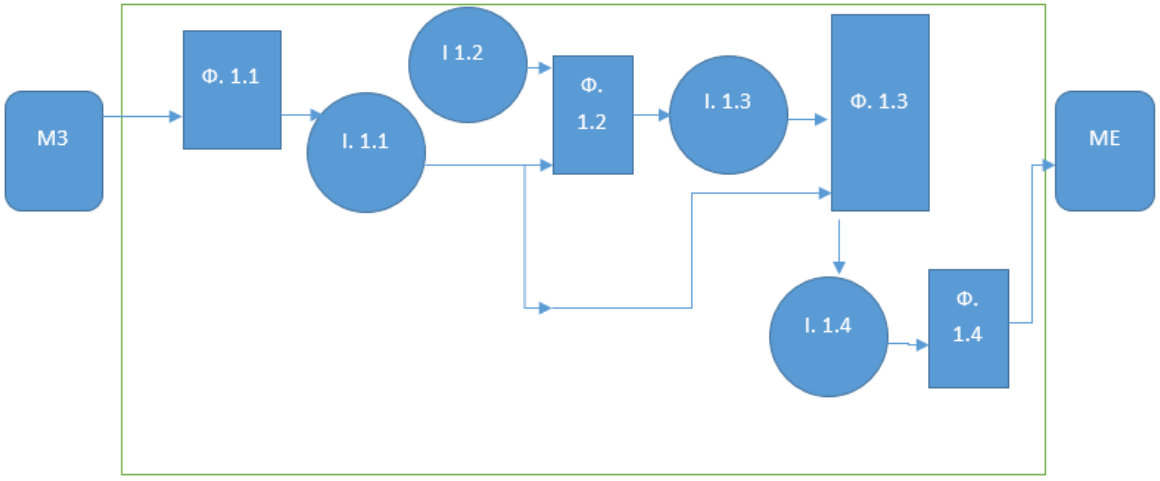
2 Таблиця 1.1.1 «Перелік інформаційних потоків організації ДСЕР»

№	Вхідна інформація	ТОІ	Вихідна інформація
1	Матеріали заяви	Технологія реєстрації та обробки заяв	Матеріали експертизи
2	Матеріали експертизи	Проведення тематичної експертизи	Контрольна картка з висновками експерта, Відомості експертизи
3	Відомості експертизи	Формування таблиць зведених відомостей та супровідних документів	Таблиці зведених відомостей, Супровідні листи
4	Зведені відомості	Підписання Головою	Підписані ЗВ
5	Підписані ЗВ	Технологія оформлення та обробки вхідних і вихідних документів	Зведені відомості для проведення комісії
6	Рішення комісії	Технологія оформлення та обробки вхідних і вихідних документів	Рішення комісії
7	Рішення комісії	Перевірка Головою і видача розпорядження на оформлення дозволів	Розпорядження Голови
8	Рішення комісії Розпорядження Голови	Оформлення дозволу	Заповнений бланк дозволу
9	Заповнений бланк дозволу	Підписання Головою ДСЕР	Підписаний дозвіл
10	Підписаний дозвіл	Технологія реєстрації та видачі дозволів Підготовка матеріалів експертизи для передачі в архів	Дозвіл Матеріали архіву
11	Матеріали архіву	Архівування	Архів
12	Запит Голови ДСЕР	Інформаційно-аналітичне забезпечення	Ресурси Інтернет
13	Запит клієнта служби	Інформаційно-аналітичне забезпечення	Інформація для клієнта

Далі, кожний ІП буде деталізований та описаний у вигляді ТОІ. Кожний ТОІ представлений у вигляді схеми, таблиці з проміжною інформацією та функціоналом ТОІ, а також його коротким описом (поясненням).

3.2.1.2. Інформаційно-функціональні структури потоків

ТОІ – 1 Технологія реєстрації та обробки заяв

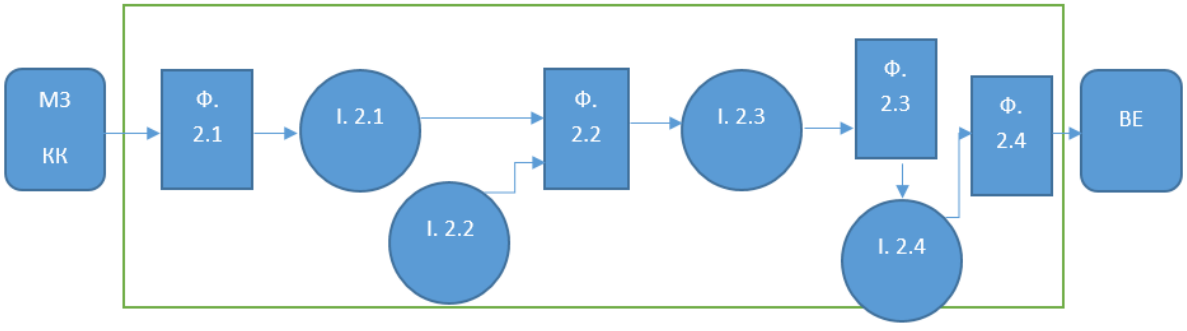


	Код	Найменування
	Функції технології	
.	Ф. 1.1	Перевірка МА та реєстрація
.	Ф. 1.2	Формування Контрольної картки
.	Ф. 1.3	Затвердження начальником відділу
	Ф. 1.4	Передача заяви до від. експертизи

	Проміжна інформація	
.	І. 1.1	Журнал реєстрації
.	І. 1.2	Бланк контрольної картки
.	І. 1.3	Контрольна картка
.	І. 1.4	Матеріали експертизи

Клієнт, заповнивши заяву та додавши до неї графічні і текстові додатки передає їх до Реєстраційно-архівного відділу. Ці матеріали заяви отримує Спеціаліст, який перевіряє і вносить їх до Журналу реєстрації. Далі ці матеріали передаються Провідному спеціалісту, який вирішує до якого відділу слід передати матеріали та оформлює Контрольну картку, яку додає до них, формуючи таким чином Матеріали експертизи. Далі матеріали експертизи подаються начальнику відділу на затвердження і після цього їх віддають у відповідний експертний відділ.

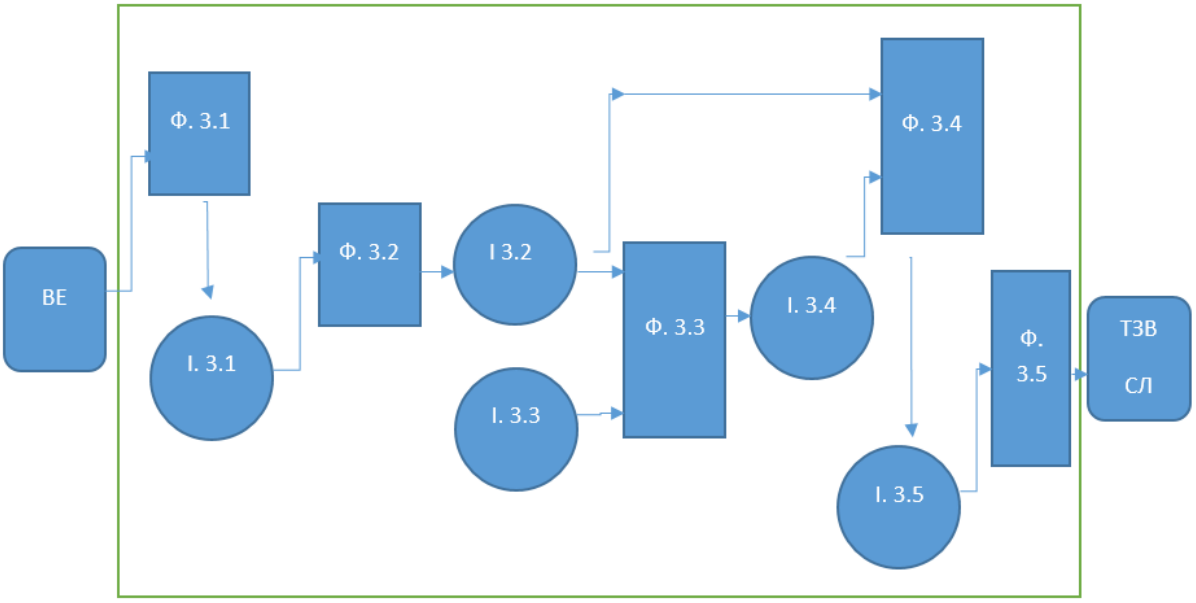
ТОІ -2 Проведення тематичної експертизи



	Код	Найменування
	Функції технології	
.	Ф. 2.1	Розгляд МЕ нач. відділу і передача експертам
.	Ф. 2.2	Отримання МЕ експертом та здійснення експертизи
.	Ф. 2.3	Підписання КК нач. Відділу
.	Ф. 2.4	Передача до ВІАЗ
	Проміжна інформація	
.	І. 2.1	Матеріали експертизи
.	І. 2.2	Нормативна документація для проведення експертизи
.	І. 2.3	КК з відміткою експерта
.	І. 2.4	Підписані Нач. відділу КК

Начальник відповідного відділу експертизи отримує на розгляд Матеріали експертизи та передає їх відповідному експерту. Експерт у свою чергу, керуючись потрібними нормативними документами вирішує дозволяти експорт чи ні і ставить відмітки «дозволяється» або «не дозволяється відповідно до пунктів № № ... нормативного акта № ...» та власний підпис на КК. Після цього матеріали подаються начальнику відділу, який їх перевіряє та ставить свій підпис на Контрольній картці і передає Відомості експертизи до ВІАЗ.

ТОІ – 3 Формування таблиць зведених відомостей та супровідних документів

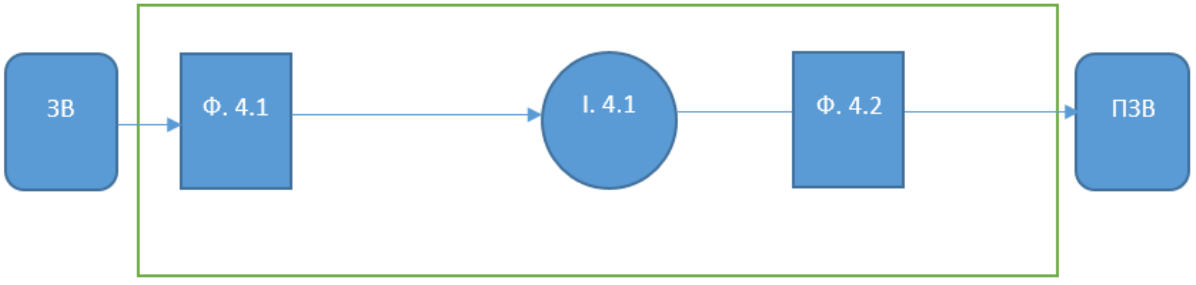


	Код	Найменування
	Функції технології	
.	Ф. 3.1	Розгляд ВЕ нач. відділу і передача їх спеціалісту
.	Ф. 3.2	Збір інформації по експертизам і формування її в таблицю ЗВ
.	Ф. 3.3	Формування Супровідного листа
.	Ф. 3.4	Підписання начальником відділу
.	Ф. 3.5	Передача документів на підпис Голові

	Проміжна інформація	
.	I. 3.1	Перевірені ВЕ
.	I. 3.2	Зведені відомості(таблиці)
.	I. 3.3	Бланк СЛ
.	I. 3.4	Супровідний лист
	I. 3.5	Підписані нач відділу ЗВ

Відомості експертизи отримує начальник відділу ВІАЗ, розглядає їх та передає Спеціалісту для формування Зведених відомостей у вигляді таблиць та оформлення супровідного листа. Після цього Спеціаліст передає ТЗВ і СЛ начальнику відділу, який перевіряє правильність оформлення, підписує СЛ та передає на підпис Голові ДСЕР.

ТОІ -4 Підписання Відомостей Головою ДСЕР

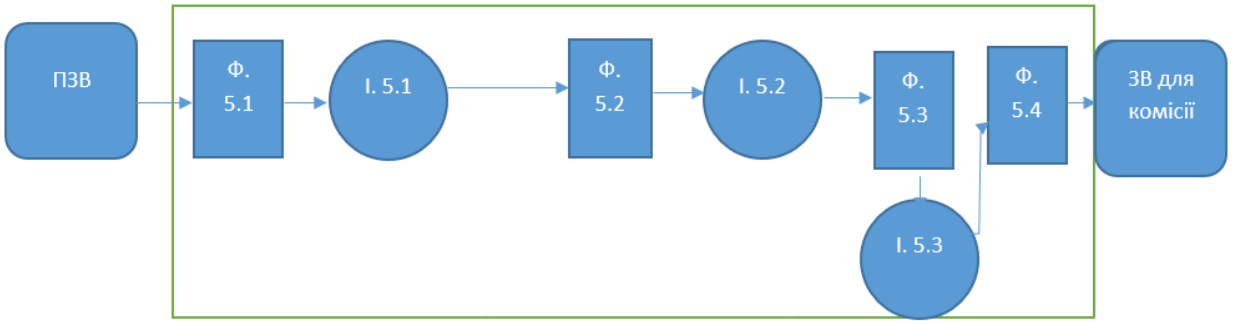


	Код	Найменування

	Функції технології	
.	Ф. 4.1	Перевірка і Підписання відомостей Головою ДСЕР
.	Ф. 4.2	Передача в РСВ
	Проміжна інформація	
.	І. 4.1	Підписані Головою ЗВ і СЛ

Голова ДСЕР, отримавши Зведені відомості, перевіряє їх та ставить свій підпис. Після цього передає їх до РСВ для відправки ПККМ.

ТОІ -5 Технологія оформлення та обробки вхідних і вихідних документів

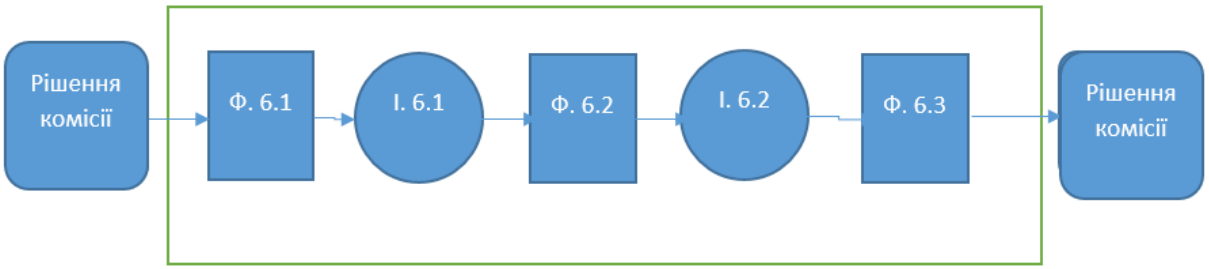


	Код	Найменування
	Функції технології	
.	Ф. 5.1	Отримання нач.РСВ Матеріалів комісії і передача їх провідному спеціалісту

.	Ф. 5.2	Формування пакету документів
.	Ф. 5.3	Передача фельд’єгерській службі
.	Ф. 5.4	Відправка до ПККМ
	Проміжна інформація	
.	І. 5.1	Документи на відправку до ПККМ
.	І. 5.2	Пакет документів
.	І. 5.3	Журнал реєстрації вихідних документів

Начальник РСВ отримує Підписані Головою зведені відомості перевіряє їх на наявність підпису Голови і передає їх Провідному спеціалісту для формування пакету документів, його реєстрації у журналі вихідних документів та передачі фельд’єгерській службі. Офіцер фельд’єгерської служби, отримавши пакет, розписується в журналі і передає Матеріали комісії до ПККМ.

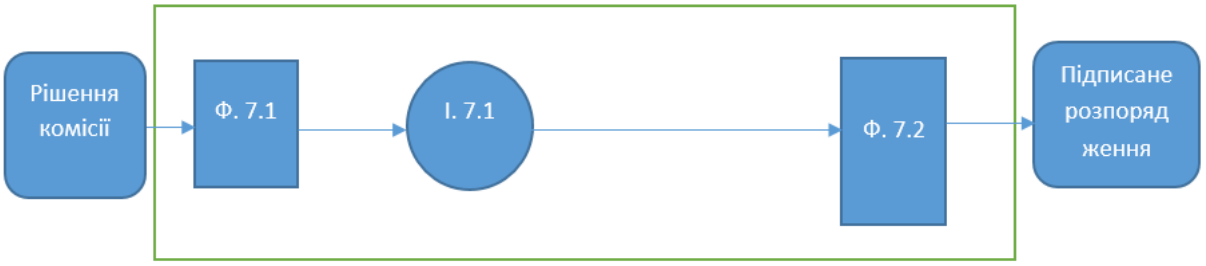
ТОІ -6 Технологія оформлення та обробки вхідних і вихідних документів



	Код	Найменування
	Функції технології	
	Ф. 6.1	Отримання Провідним спеціалістом Рішення комісії
.	Ф. 6.2	Облік та реєстрація документів
.	Ф. 6.3	Перевірка нач.РСВ і передача до Голови
	Проміжна інформація	
.	І. 6.1	Зареєстровані документи з ПККМ
.	І. 6.2	Журнал реєстрації вх. документів

Офіцер ФС передає пакет з Рішенням комісії Провідному спеціалісту, який у свою чергу вносить їх у журнал вхідних документів та несе на розгляд начальнику відділу. Начальник відділу перевіривши документи передає їх до Голови ДСЕР.

ТОІ -7 Перевірка та видача розпорядження Головою ДСЕР

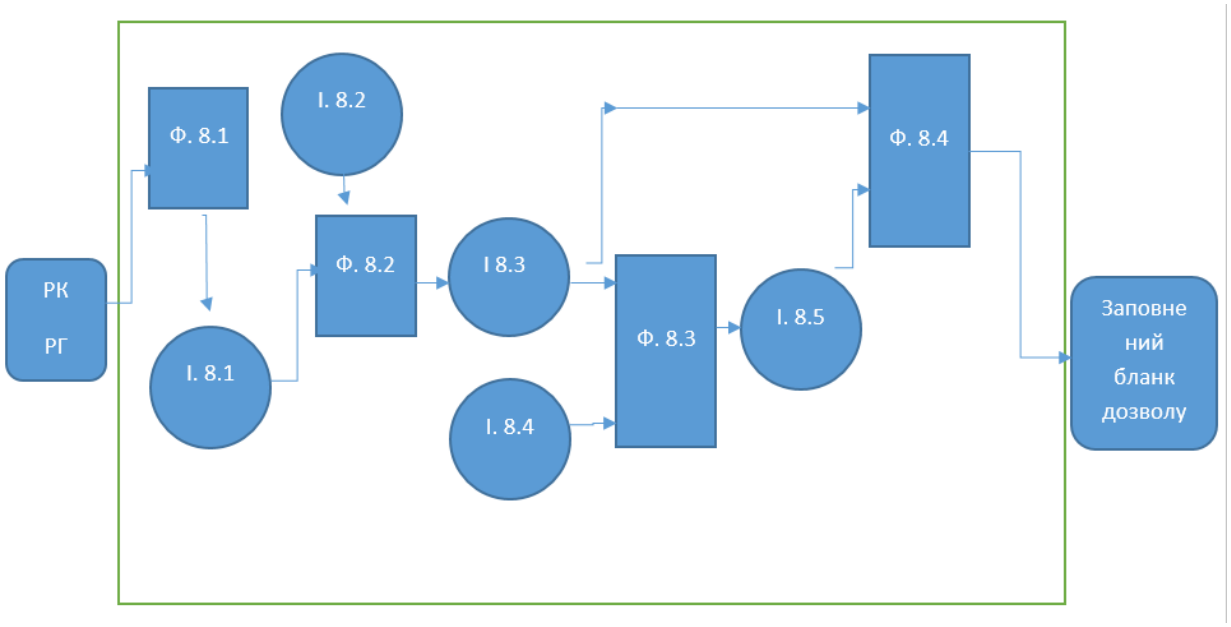


	Код	Найменування

	Функції технології	
.	Ф. 7.1	Перевірка Головою документів та видача розпорядження на оформлення дозволів
.	Ф. 7.2	Підписання розпорядження
	Проміжна інформація	
.	І. 7.1	Розпорядження

Отримавши Рішення комісії Голова ДСЕР видає розпорядження на видачу дозволів та підписує його. Далі йде передача розпорядження до ВІАЗ.

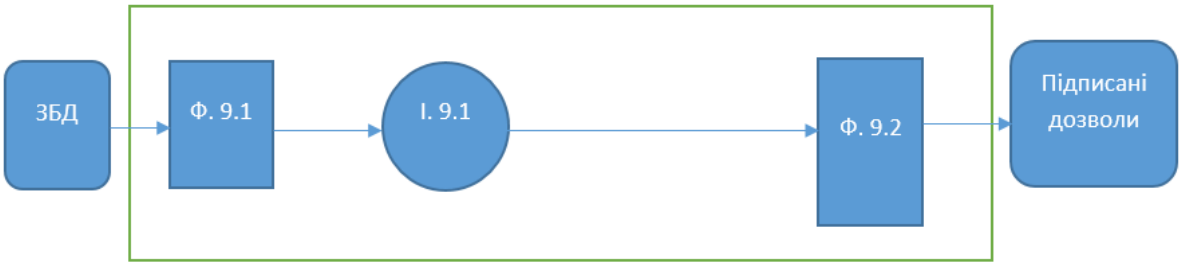
ТОІ – 8 Оформлення дозволів



	Код	Найменування
	Функції технології	
.	Ф. 8.1	Отримання розпорядження Голови начальником відділу і видача розпорядження нач. відділу
.	Ф. 8.2	Обробка рішень комісії спеціалістом
.	Ф. 8.3	Оформлення дозволів
.	Ф. 8.4	Підписання начальником відділу і відправка на підпис Голові
	Проміжна інформація	
.	І. 8.1	Розпорядження нач. відділу
.	І. 8.2	Рішення комісії
.	І. 8.3	Документи з ПККМ і МЗ
.	І. 8.4	Бланки дозволів
	І. 8.5	Заповнені дозволи

Начальник ВІАЗ, отримавши розпорядження Голови та Рішення комісії видає розпорядження на оформлення дозволів Спеціалістом відділу. Отримавши розпорядження начальника відділу Спеціаліст, на основі рішення комісії оформлює бланки дозволів на експорт/імпорт товарів. Після оформлення вони передаються начальнику відділу, який ретельно звіряє їх з рішенням прийнятим ПККМ і якщо вони вірні відправляє на підпис Голові ДСЕР.

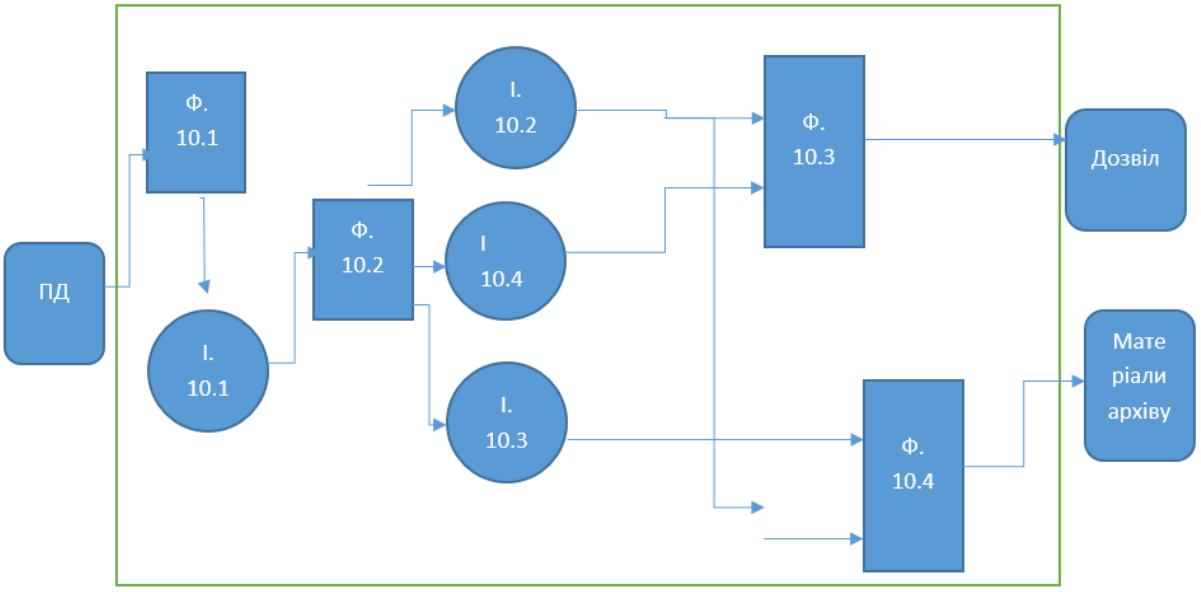
ТОІ -9 Перевірка та підписання дозволів Головою



	Код	Найменування
	Функції технології	
.	Ф. 9.1	Перевірка дозволів та підписання їх Головою
.	Ф. 9.2	Передача до РСВ
	Проміжна інформація	
.	І. 9.1	Підписані дозволи

Отримавши заповнені бланки дозволів Голова ДСЕР підписує їх і передає в РСВ.

ТОІ – 10 Оформлення дозволів

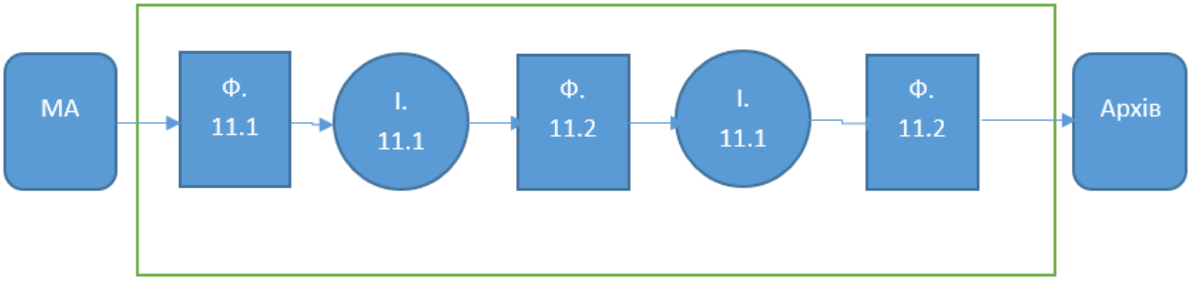


	Код	Найменування
	Функції технології	
.	Ф. 10.1	Отримання підписаних дозволів нач. РСВ і передача спеціалісту
.	Ф. 10.2	Обробка та реєстрація підписаних дозволів та копіювання дозволів і документів
.	Ф. 10.3	Перевірка нач. РСВ і видача дозволів
.	Ф. 10.4	Перевірка нач. РСВ і передача для архівування копій документів
	Проміжна інформація	
.	І. 10.1	Дозволи і МЗ
.	І. 10.2	Журнал реєстрації дозволів
.	І. 10.3	Копії дозволів та документів

.	I. 10.4	Дозвіл

Начальник РСВ, отримавши підписані Головою дозволи, передає їх Спеціалісту для внесення в Журнал реєстрації Дозволів та їх копіювання. Після прооблених операцій Спеціаліст передає Журнал і копії документів на перевірку начальнику РСВ. Після перевірки начальник РСВ передає одному із спеціалістів Дозволи для видачі їх клієнтам, а іншому Матеріали експертизи для підготовки їх до архівування. Після підготовки МЕ до архівування ці документи передаються до Реєстраційно-архівного відділу.

TOI -11 Архівування

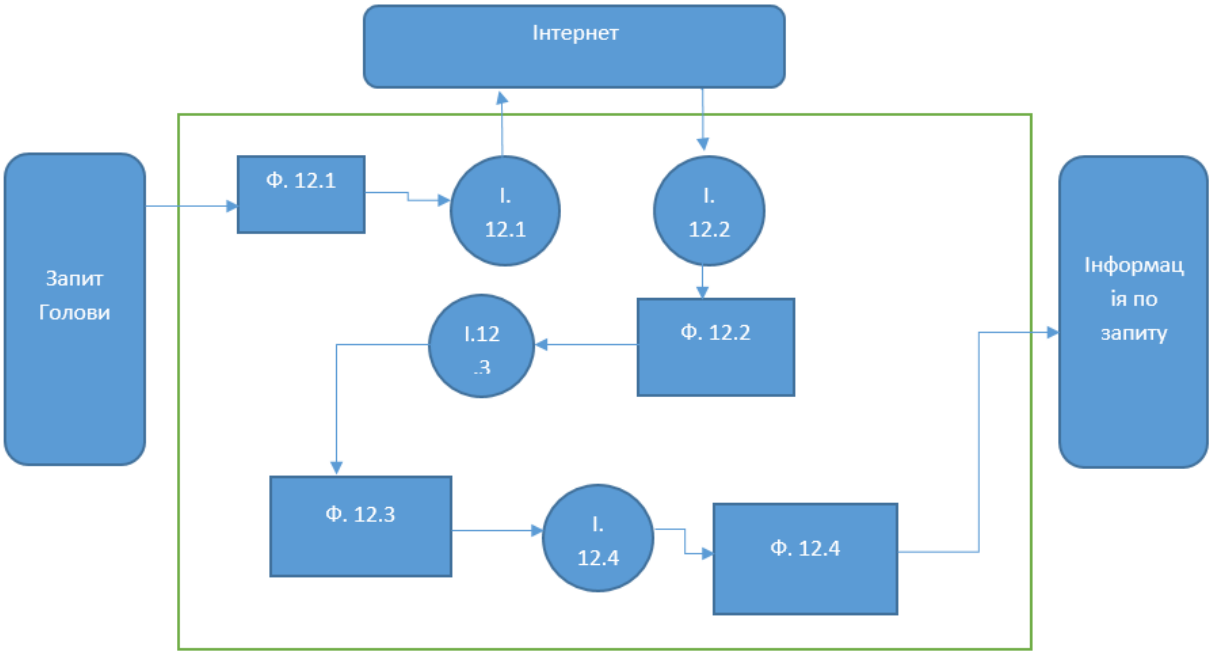


	Код	Найменування

	Функції технології	
	Ф. 11.1	Отримання нач.відділу документів і передача їх спеціалісту
.	Ф. 11.2	Заведення архівної папки для документів
.	Ф. 11.3	Складання папки з документами в архівну скриньку
	Проміжна інформація	
.	І. 11.1	Копії документів
.	І. 11.2	Папка архіву

Начальник РАВ отримує МЕ та копію Дозволу та передає їх спеціалісту. Спеціаліст отримавши Матеріали архіву заводить для них окрему папку і складує її в архівну скриньку.

ТОІ-12 Технологія Інформаційно-аналітичної роботи

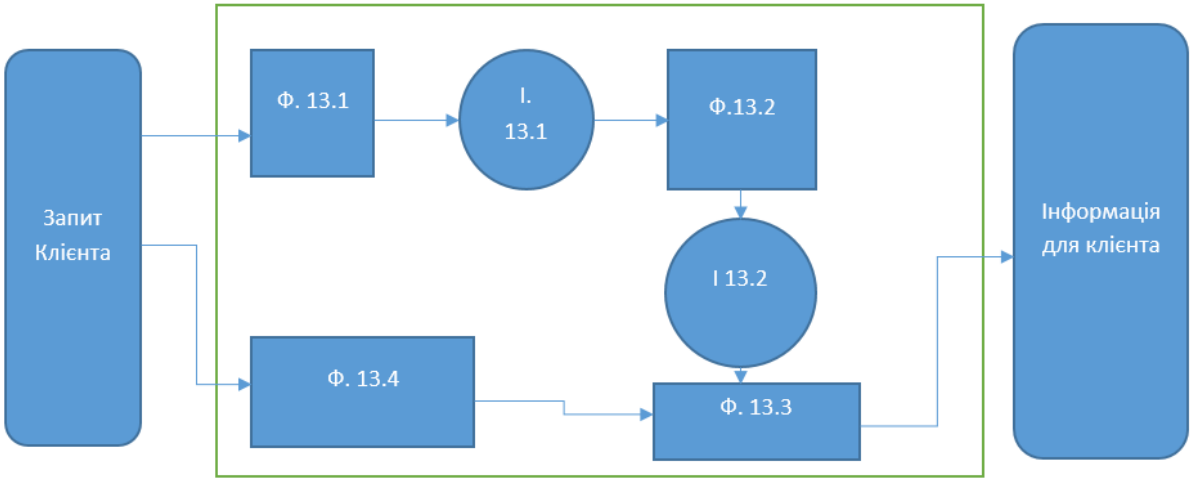


	Код	Найменування
	Функції технології	
.	Ф. 12.1	Формалізація запиту Голови

.	Ф. 12.2	Аналіз отриманих даних на правильність та достовірність
.	Ф. 12.3	Аналітична обробка
.	Ф. 12.4	Формування аналітичного продукту
Проміжна інформація		
.	І. 12.1	Формалізований запит
.	І. 12.2	Зібрані дані
.	І. 12.3	Аналітичні матеріали

Голова Служби робить запит до ВІАЗ, цей запит формалізується Провідним спеціалістом відділу, після чого ним же проводиться пошук за вже формалізованими даними в мережі Інтернет. Згодом проводиться перевірка знайденої інформації на достовірність, а потім її аналіз та обробка. Після всіх цих процедур дані формалізуються у вигляд звіту і подаються Голові Служби.

ТОІ – 13 Технологія сповіщення клієнта



	Код	Найменування
	Функції технології	
.	Ф. 13.1	Обробка заяви клієнта
.	Ф. 13.2	Звернення до БД
.	Ф. 13.3	Формування звіту
.	Ф. 13.4	Перегляд клієнтом зразків документів на подачу
	Проміжна інформація	
.	І. 13.1	Формалізований запит

.	I. 13.2	Зібрані дані

Клієнт робить запит у якому вказує потрібні йому дані. Цей запит оброблюється системою, вона робить звернення до Бази даних і формує звіт по інформації, що цікавить клієнта. Після цього цей звіт подається клієнту. Також на сайті ДСЕР містяться зразки Заяви та документи необхідні для подання разом із нею для розгляду державними експертами.

3.2.1.3. Інформаційно-функціональна структура організації.

Інформаційно-функціональна структура (далі – ІФС) – це функціональна структура в якій зв’язки відповідають обміну інформацією між частинами.

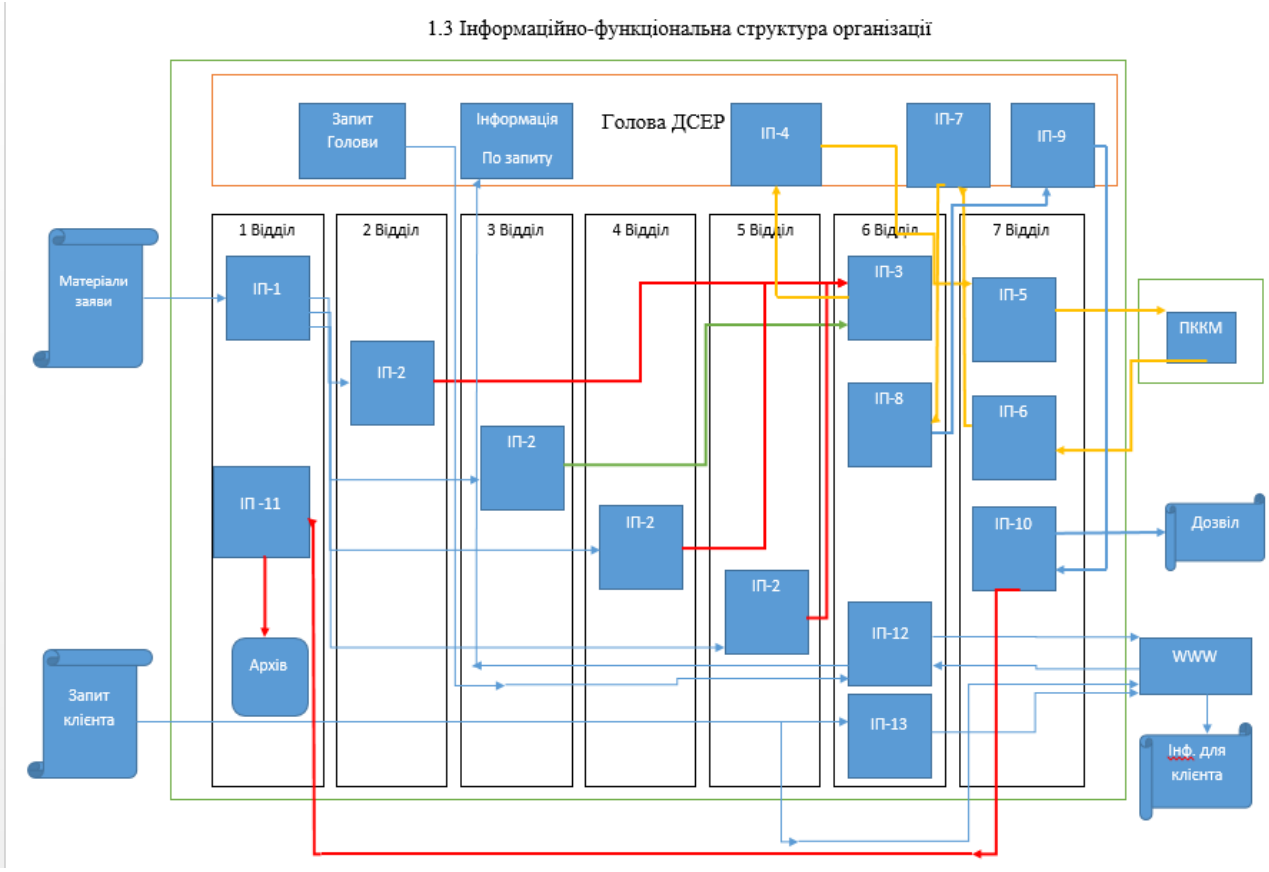
Тобто, ІФС організації ДСЕР буде представлена у вигляді вхідної інформації, вихідної інформації та проміжної інформації, що циркулює та обробляється в інформаційних потоках організації.

Вхідна інформація – це початкові відомості чи дані, які поступають в організацію ДСЕР, циркулюють та обробляються в ній. Вхідна інформація перетворюється в проміжну і в результаті в вихідну. В даному випадку – це Матеріали заяви, Запит Голови ДСЕР та Запит клієнта.

Вихідна інформація – кінцевий результат діяльності організації ДСЕР, що відбувається в процесі перетворення вхідної та проміжної інформації. В даному випадку – це Дозвіл, Заповнена заявка та Інформаційно аналітичний продукт.

Проміжна інформація – це інформація, що циркулює та обробляється в ІП. Кожний ІП описує процеси діяльності відділів організації ДСЕР.

На даній діаграмі показано як інформація циркулює всередині ДСЕР на основі проходження через інформаційні потоки.



- Відкрита інформація

- Інформація з грифом «Таємно»

- Інформація з грифом «Цілком Таємно»

- Інформація з грифом «ДСК»

3.2.2 Принципи роботи автоматизованої системи

Для роботи АСЗЕ буде використана електронно-паперова обробка інформації з використанням Баз даних. Це означає, що всі документи обробляються в паперовому вигляді, але відомості по цим документам зберігаються в електронному вигляді у базі даних. Електронно-паперова технологія обробки з використанням БД була вибрана бо вона дозволяє зменшити час підготовки документів, в порівнянні з паперовою технологією, яка була описана вище, та є дешевшою і не містить проблем з електронними ключами в порівнянні з технологією електронного документообігу.

В організації будуть створені 3 Бази даних:

- БД «Експертиза»(В подальшому БД)
- БД «Нормативні документи»
- БД «Архів»

Клієнт, заповнивши заяву та додавши до неї графічні і текстові додатки передає їх до Реєстраційно-архівного відділу. Ці матеріали заяви отримує Спеціаліст, який перевіряє і вносить їх в Журнал реєстрації. Далі ці матеріали передаються Провідному спеціалісту, який вирішує до якого відділу слід передати матеріали та оформлює Контрольну картку(Заповнює форму в БД і роздруковує її

зі свого АРМ), яку додає до них, формуючи таким чином Матеріали експертизи, інформація з цих матеріалів експертизи заносяться в БД «Експертиза», де їм присвоюється номер, що відповідає номеру Контрольної картки. Далі матеріали експертизи подаються начальнику відділу на затвердження, він у свою чергу перевіряє Журнал реєстрації та БД «Експертиза», підписує МЕ, і після цього їх віддають у відповідний експертний відділ. Також в кінці дня спеціаліст РАВ експортує дані з БД «Експертиза» в Exel-файли і переносить його на спеціальний зареєстрований флеш-накопичувач, який зберігається в сейфі Начальника РСВ, потім експортує ці файли в БД «Експертиза(Т)» для подальшої роботи з даними іншими працівниками.

Начальник відповідного відділу експертизи отримує на розгляд Матеріали експертизи та передає їх відповідному експерту, про що робить замітку в БД. Експерт у свою чергу, керуючись потрібними нормативними документами, які є в БД «Нормативні документи» і до яких він має доступ зі свого АРМ, вирішує дозволяти експорт чи ні і ставить відмітки «дозволяється» або «не дозволяється відповідно до пунктів № № ... нормативного акта № ...» та власний підпис на КК. Відомості про відмітки експерт заносить до БД. Після цього матеріали подаються начальнику відділу, який їх перевіряє у БД «Експертиза» та ставить свій підпис на Контрольній картці і передає Відомості експертизи до ВІАЗ.

Матеріали експертизи отримує начальник відділу ВІАЗ, розглядає їх та звіряє з інформацією, що була занесена до БД, після цього він передає їх Спеціалісту для формування Зведених відомостей у вигляді таблиць та оформлення супровідного листа. Спеціаліст, переходячи на потрібну вкладку БД «Експертиза», формує таблицю зведених даних, які згодом роздруковує і разом з тим оформлює супровідні листи, шляхом заповнення зі свого АРМ та роздрукування. Після цього Спеціаліст передає ТЗВ і СЛ начальнику відділу, який перевіряє

правильність оформлення, наявність СЛ, підписує СЛ та передає на підпис Голові ДСЕР.

Голова ДСЕР, отримавши СЛ та ТЗВ, звіряє їх з інформацією в БД та ставить свій підпис. Після цього передає їх до РСВ для відправки в ПККМ.

Начальник РСВ отримує Підписані Головою зведені відомості перевіряє їх на наявність підпису Голови і передає їх Провідному спеціалісту для формування пакету документів, його реєстрації у журналі вихідних документів та передачі фельд'єгерській службі. Офіцер фельд'єгерської служби, отримавши пакет, розписується в журналі і передає Матеріали комісії до ПККМ.

Офіцер ФС передає пакет з Рішенням комісії Провідному спеціалісту, який у свою чергу вносить їх у журнал вхідних документів та несе на розгляд начальнику відділу, перед цим занісши рішення комісії до БД. Начальник відділу, перевіривши документи та звіривши з занесеною до БД інформацією, передає їх до Голови ДСЕР.

Отримавши Рішення комісії Голова ДСЕР перевіряє БД, і видає розпорядження на видачу дозволів та підписує його. Далі йде передача розпорядження до ВІАЗ.

Начальник ВІАЗ, отримавши розпорядження Голови та Рішення комісії видає розпорядження на оформлення дозволів Спеціалістом відділу. Отримавши розпорядження начальника відділу Спеціаліст, на основі рішення комісії оформлює бланки дозволів на експорт/імпорт товарів, він заповнює інформацію на своєму АРМ і роздруковує його, в цьому випадку до БД заносять № дозволу і дата видачі розпорядження Голови ДСЕР. Після оформлення вони передаються начальнику відділу, який ретельно звіряє їх з рішенням прийнятим ПККМ, використовуючи БД, і якщо вони вірні відправляє на підпис Голові ДСЕР.

Отримавши заповнені бланки дозволів Голова ДСЕР підписує їх і передає в РСВ.

Начальник РСВ, отримавши підписані Головою дозволи, передає їх Спеціалісту для внесення в Журнал реєстрації Дозволів та їх копіювання. Після прооблених операцій Спеціаліст передає Журнал і копії дозволів на перевірку начальнику РСВ. Після перевірки начальник РСВ передає одному із спеціалістів Дозволи для видачі їх клієнтам, а іншому Матеріали експертизи для підготовки їх до архівування. Після підготовки МЕ до архівування ці документи передаються до Реєстраційно-архівного відділу. Після передачі документів в РАВ, інформація про них вилучається з БД «Експертиза»(щорічно проводиться скидання даних, але обов’язково після занесення в БД «Архів»), та в подальшому заноситься до БД «Архів»

Начальник РАВ отримує МЕ та копії Дозволів та передає їх спеціалісту. Спеціаліст отримавши Матеріали архіву заводить для них окрему папку, якій дається унікальний номер, який заноситься в БД «Архів» разом з описом документів, що знаходяться всередині, і складує її в архівну скриньку.

Забезпечення Голови ДСЕР інформаційно-аналітичним продуктом проходить наступним чином:

Голова Служби робить запит до ВІАЗ через своє АРМ, цей запит отримується і формалізується Провідним спеціалістом відділу, після чого ним же проводиться пошук за вже формалізованими даними в мережі Інтернет. Згодом проводиться перевірка знайденої інформації на достовірність, а потім її аналіз та обробка. Після всіх цих процедур дані формалізуються у вигляді звіту і подаються Голові Служби в роздрукованому вигляді.

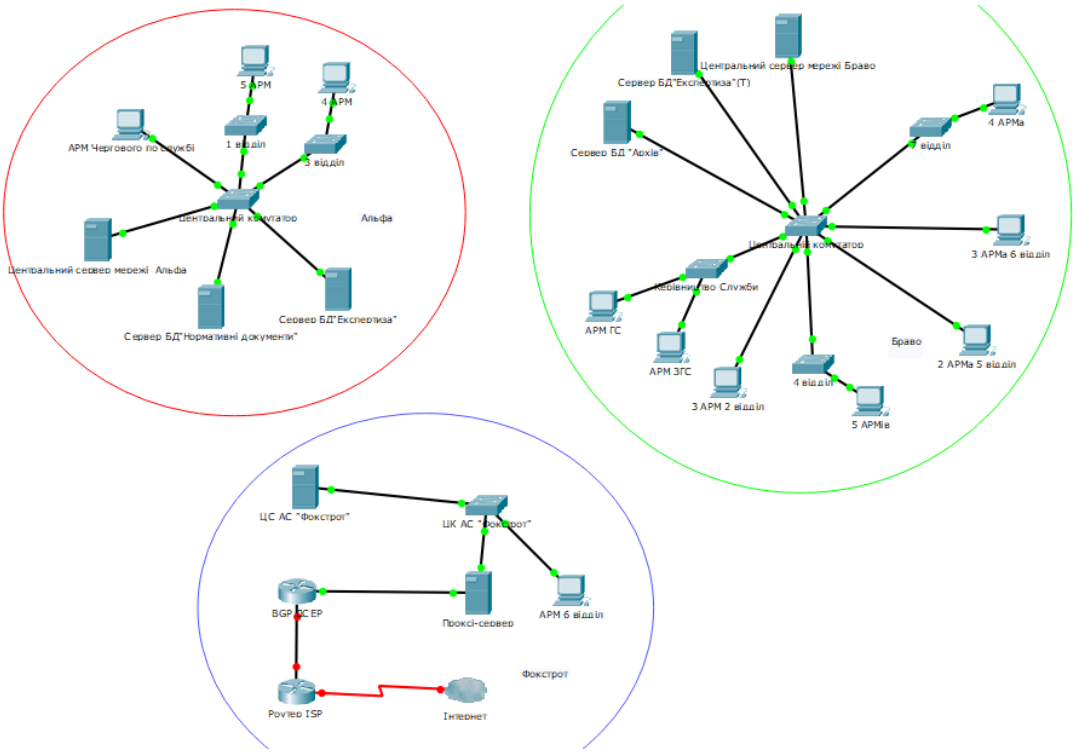
Інформування клієнтів ДСЕР проходить таким чином:

Клієнт робить запит у якому вказує потрібні йому дані. Цей запит оброблюється системою, вона робить звернення до Бази даних і формує звіт по інформації, що цікавить клієнта. Після цього цей звіт подається клієнту. Також на сайті ДСЕР містяться зразки Заяви та документи необхідні для подання разом із нею для розгляду державними експертами.

3.2.3 Структура АСЗЕ

Згідно з постановою КМУ №522 від 12.04.2002 «Про затвердження Порядку підключення до глобальних мереж передачі даних» - будь-якій організації забороняється підключати АС до глобальної мережі Інтернет, якщо в цій АС обробляється інформація, що є об'єктом державної власності і охороняється згідно із чинним законодавством.

Тому, доцільно зауважити, що для реалізація технології обробки інформації в майбутній АСЗЕ, буде складатися з трьох частин (трьох АС) – двох АС 2 класу – «Альфа», «Браво» та 1 АС 3 класу – «Фокстрот».



3.1 Схема структури АСЗЕ

В АС «Альфа» буде оброблятися відкрита інформація та інформація з грифом ДСК. Мережева топологія АС – зірка. Дана АС у своєму складі матиме 5 АРМ 1-го відділу, 4 АРМ 3-го відділу, АРМ Чергового по Службі, 3 Комутатори та 3 сервери (Центральний сервер АС, Сервер БД «Нормативні документи», Сервер БД «Експертиза». АС «Альфа» являє собою мережу типу «Клієнт - сервер» і знаходиться під управлінням Центрального сервера АС, що працює на ОС Microsoft Windows Server 2012. На сервері БД «Експертиза» інформація збирається протягом одного дня, потім експортується в Exel-файл, після чого за допомогою зареєстрованого флеш-накопичувача, ця інформація переноситься на АС «Браво» і імпортується в БД «Експертиза (Т)», де інформація зберігається за поточний рік.

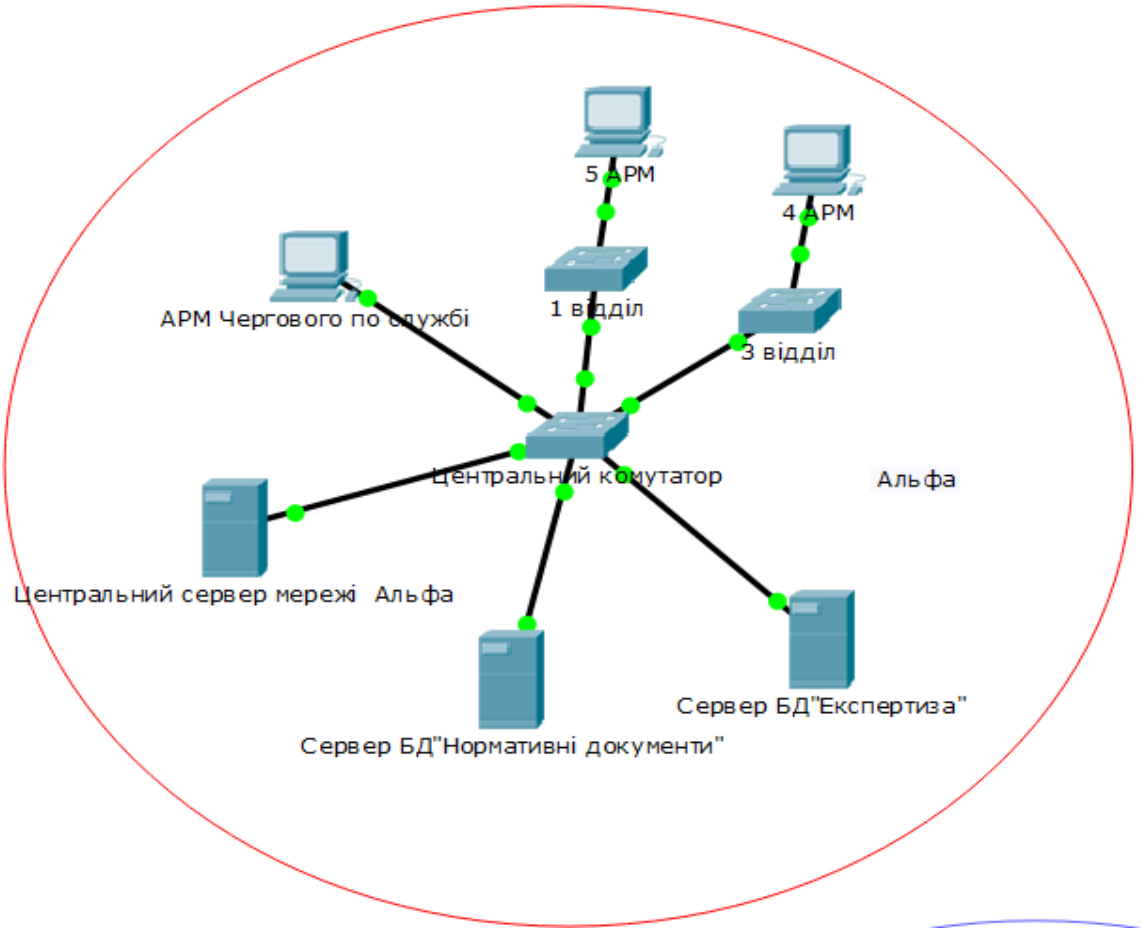


Рис 3.2 Топологія АС «Альфа»

АС «Браво» призначена для обробки Інформації з грифами «Таємно» та «Цілком таємно». Дана АС у своєму складі має : АРМ Голови ДСЕР, АРМ Заступника Голови, 2 АРМ 5-го відділу, 3 АРМ 6-го відділу, 5 АРМ 4-го відділу, 3 АРМ 2-го відділу, 4 АРМ 7-го відділу, 1 АРМ 1-го відділу, 4 комутатори (Центральний, комутатор керівництва Служби та комутатори в 4 та 7 відділах (для спрощення керування мережею)),Сервер БД «Експертиза (Т)», Сервер БД «Архів» та Центральний сервер АС «Браво» під управлінням ОС Microsoft Windows Server 2012.

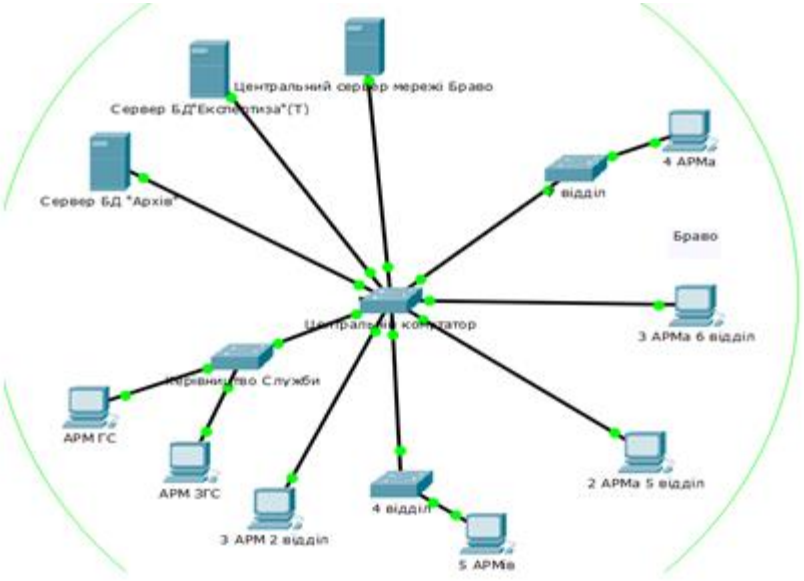
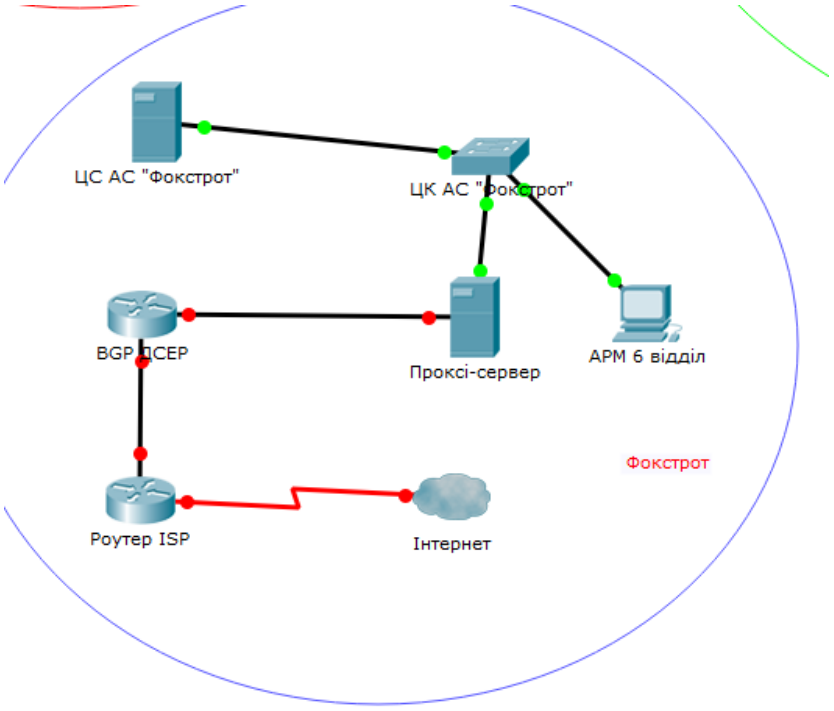


Рис. 3.3 Топологія АС «Браво»

АС «Фокстрот» являє собою АС 3-го класу. Вона має у своєму складі 1 АРМ 6-го відділу, Центральний комутатор АС, Центральний та проксі сервери, а також BGP-роутер ДСЕР та роутер Провайдера, який має доступ в мережу Інтернет. Дана АС призначена для виконання Спеціалістом ВІАЗ запитів Голови Служби(Після пошуку інформації на цьому ж АРМі формується звіт, роздруковується і подається Голові Служби), шляхом пошуку інформації в мережі Інтернет, а також для інформування клієнтів Служби.



3.4 Топологія АС «Фокстрот»

3.2.4 Перелік апартного та програмного забеспечення

В даному розділі буде розглянуто які апаратні та програмні засоби будуть встановлені на автоматизованих системах. Підбір засобів здійснюється на основі документу під назвою «**Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом**», що знаходиться на сайті Держспецзв'язку.

Таблиця 4.1 – Перелік АЗ та ПЗ для АС класу 2 «Альфа»

	№	Назва засобу	Призначення	Розміщення	Кількість
АЗ	1	Персональні комп'ютери із захистом інформації "EXPERT"(робочі станції) ТУ У 30.0-21503308.006-2001.	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідають вимогам ГОСТ 29339-92, НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-015-08, ОСТ 4.169.006-89 і ТУ в обсязі,	У 1, 3 відділі, у чергового по Службі	10

			зазначеному в сертифікаті		
	2	Комутатори «Cisco Catalyst серій WS-C2960» під керуванням операційної системи IOS 15.x,	Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі «Комутатори Cisco Catalyst серій WS-C2960 під керуванням операційної системи IOS 15.x. Технічні вимоги за критеріями технічного захисту інформації», сукупність яких визначається функціональним профілем: **КА-1,КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1,ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1** з рівнем гарантій **Г-2** оцінки коректності реалізації згідно з НД ТЗІ 2.5-004-99..	Центральний комутатор АС в серверній, інші в 1 та 3 відділах	3
	3	Персональні комп'ютери із захистом інформації "EXPERT" (сервери) ТУ У 30.0-21503308.006-2001	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідають вимогам ГОСТ 29339-92, НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-015-08, ОСТ 4.169.006-89 і ТУ в обсязі, зазначеному в сертифікаті	Серверна	3
	4	Кабельне обладнання UTP категорії 5е на основі витої пари	Створення каналів кабельної мережі на основі витої пари категорії 5е	Від комутатора до кожного АРМ і Серверів	17
ПЗ	1	Операційна система Microsoft Windows 10 Enterprise, виробництва Microsoft Corporation, США	Забезпечення конфіденційності, цілісності та доступності об’єктів захисту, що циркулюють в ОС.	На АРМ	10
	2	Операційна система Microsoft Windows Server 2012, виробництва Microsoft Corporation, США	Забезпечення конфіденційності, цілісності та доступності об’єктів захисту, що циркулюють в ОС.	На Серверах, Центральному Сервері та Шлюзі	4
	3	Система керування базами даних "Oracle Database 12c Enterprise Edition"	Призначена для зберігання і обробки інформації в базах даних.	На Сервері БД «Нормативні документи» та сервері БД «Експертиза»	2

Таблиця 4.2 - *Перелік АЗ та ПЗ для АС класу 2 «Браво»*

	№	Назва засобу	Призначення	Розміщення	Кількість
АЗ	1	Персональні комп'ютери із захистом інформації "EXPERT" (робочі станції) ТУ У 30.0-21503308.006-2001	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідають вимогам ГОСТ 29339-92, НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-015-08, ОСТ 4.169.006-89 і ТУ в обсязі, зазначеному в сертифікаті	Кабінети ГС та ЗГС, а також у 1,2,4,5,6,7 відділах	20
	2	Персональні комп'ютери із захистом інформації "EXPERT" (сервери) ТУ У 30.0-21503308.006-2001	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідають вимогам ГОСТ 29339-92, НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-015-08, ОСТ 4.169.006-89 і ТУ в обсязі, зазначеному в сертифікаті	Серверна – 2шт Архів - 1	3
	3	Комутатори «Cisco Catalyst серій WS-C2960» під керуванням операційної системи IOS 15.x,	Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі «Комутатори Cisco Catalyst серій WS-C2960 під керуванням операційної системи IOS 15.x. Технічні вимоги за критеріями технічного захисту інформації», сукупність яких визначається функціональним профілем: **КА-1,КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1,ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1** з рівнем гарантій **Г-2** оцінки коректності реалізації згідно з НД ТЗІ 2.5-004-99..	У серверній центральний ком-р та ком-р Керівництва, інші у 4 та 7 відділах	4
	4	Кабельне обладнання SF/UTP категорії 5е на основі витої пари	Створення каналів кабельної мережі на основі екранованої витої пари категорії 5е	Між АРМ, серверами та комутатором	26
ПЗ	1	Операційна система Microsoft Windows 10 Enterprise, виробництва Microsoft Corporation, США	Забезпечення конфіденційності, цілісності та доступності об’єктів захисту, що циркулюють в ОС.	На АРМ	20
	2	Операційна система Microsoft Windows Server 2012, виробництва Microsoft Corpo	Забезпечення конфіденційності, цілісності та доступності об’єктів захисту, що циркулюють в ОС.	На всіх серверах в АС	3

		ration, США			
	3	Система керування базами даних "Oracle Database 12c Enterprise Edition"	Призначена для зберігання і обробки інформації в базах даних.	На Сервері БД «Експертиза(Т)» та Сервері БД «Архів»	2

Таблиця 4.3 - *Перелік АЗ та ПЗ для АС класу 3 «Фокстрот»*

	№	Назва засобу	Призначення	Розміщення	Кількість
АЗ	1	Персональні комп'ютери із захистом інформації "EXPERT" (робочі станції) ТУ У 30.0-21503308.006-2001	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідають вимогам ГОСТ 29339-92, НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-015-08, ОСТ 4.169.006-89 і ТУ в обсязі, зазначеному в сертифікаті	У 6 відділі	1
	2	Персональні комп'ютери із захистом інформації "EXPERT" (сервери) ТУ У 30.0-21503308.006-2001	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідають вимогам ГОСТ 29339-92, НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-015-08, ОСТ 4.169.006-89 і ТУ в обсязі, зазначеному в сертифікаті	У 6 відділі	2
	3	Комутатори «Cisco Catalyst серій WS-C2960» під керуванням операційної системи IOS 15.x,	Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі «Комутатори Cisco Catalyst серій WS-C2960 під керуванням операційної системи IOS 15.x. Технічні вимоги за критеріями технічного захисту інформації», сукупність яких визначається функціональним профілем: **КА-1,КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1,ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1** з рівнем гарантій **Г-2** оцінки коректності реалізації згідно з НД ТЗІ 2.5-004-99..	У 6 відділі	1
	4	Маршрутизатори CiscoISRсерії 2900 (моделі Cisco 2901,Cisco 2911, Cisco	Призначені для створення корпоративної системи уніфікованих комунікацій в	У 6 відділі	1

		2921, Cisco 2951) під керуванням операційної системи CiscoIOS 15.x виробництва компанії "CiscoSystems", США	рамках єдиної платформи. Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі "Маршрутизатори Cisco ISR 2901, Cisco ISR 2911, Cisco ISR 2921, Cisco ISR 2951 під керуванням операційної системи Cisco IOS 15.x. Технічні вимоги за критеріями технічного захисту інформації", сукупність яких визначається функціональним профілем: **КА-1, КА-2, ЦА-1, ЦА-2, ЦО-2, ДР-1, ДС-1, ДЗ-1, ДЗ-2, ДВ-1, НР-1, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НТ-2**, НВ-1 з рівнем гарантій **Г-2** оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99.		
	5	Кабельне обладнання UTP категорії 5е на основі витої пари	Створення каналів кабельної мережі на основі витої пари категорії 5е	Між компонентами АС	7
ПЗ	1	Операційна система Microsoft Windows 10 Enterprise, виробництва Microsoft Corporation, США	Забезпечення конфіденційності, цілісності та доступності об’єктів захисту, що циркулюють в ОС.	На АРМ	1
	2	Операційна система Microsoft Windows Server 2012, виробництва Microsoft Corporation, США	Забезпечення конфіденційності, цілісності та доступності об’єктів захисту, що циркулюють в ОС.	На Проксі-Сервері та контролері	2

3.2.5 Схема розміщення обладнання АСЗЕ

Потрібно було розглянути схему розміщення обладнання реєстраційно-архівного відділу, як одного із основних відділі даної організації. Мною було вибрано приміщення №101, архів за умовами завдання розміщується в приміщенні №108. На схемі показані ОТЗ та ДТЗС для кожного з приміщень.

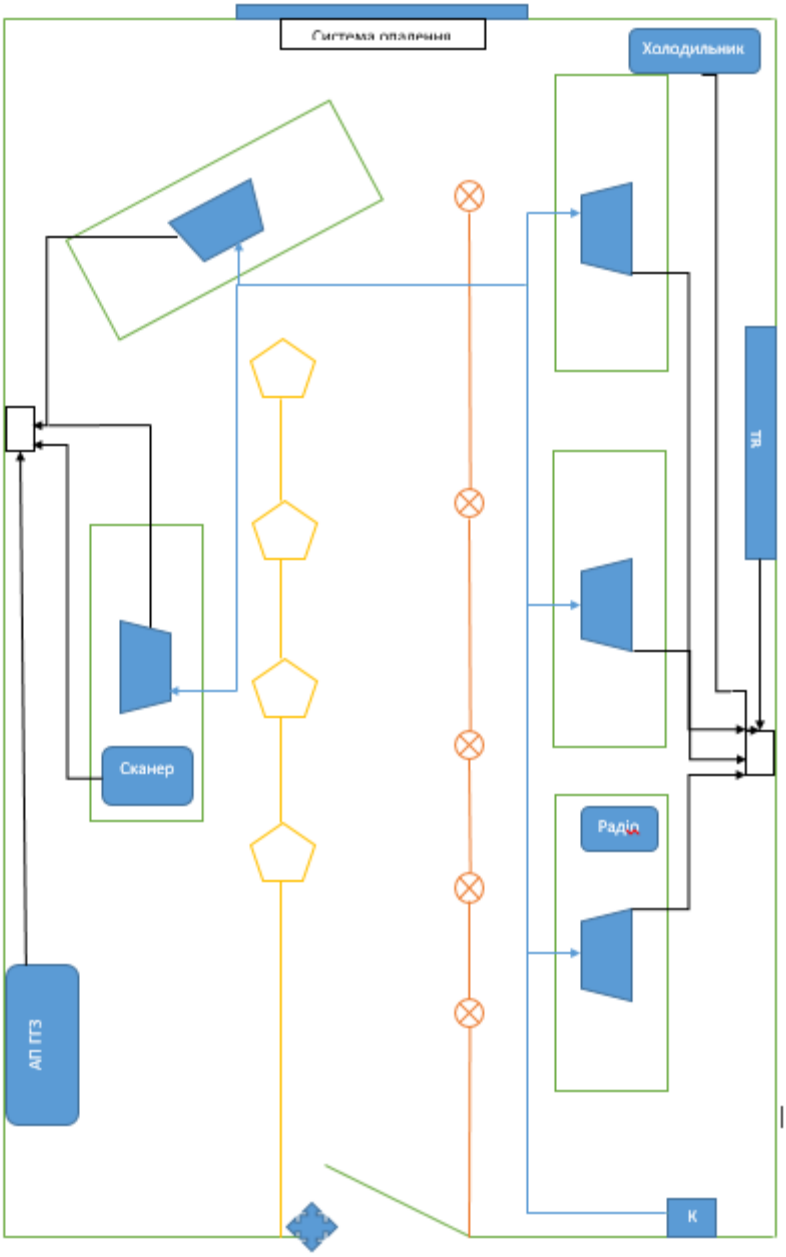


Рис. 5.1 Схема розміщення приміщення №101

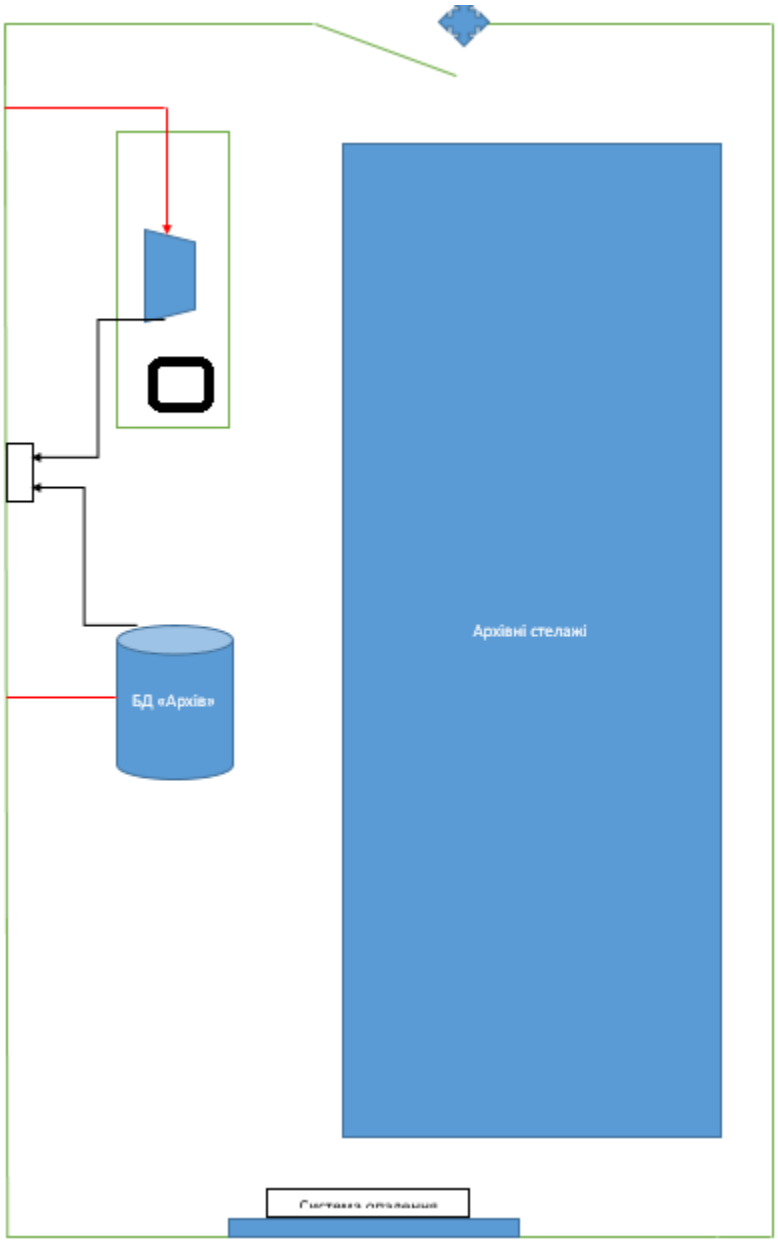
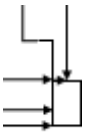


Рис. 5.2 Схема розміщення приміщення №108

 - пожежна сигналізація

 - Освітлення

 - Розетки та підключені до них пристрої

 - Ethernet

 - Сигналізація на двері

3.2.6 Схема даних для БД

Для зменшення часу підготовки документів співробітниками ДСЕР, а також для спрощення контролю за експортом-імпортом товарів, було розроблено реляційну Базу даних «Експертиза». В цій БД міститься інформація про контроль експорту-імпорту товарів військового та подвійного призначення, а саме: інформація з матеріалів заяв, інформація про проведення експертиз, інформація про видані дозволи та інформація про суб’єкта, що хоче ввезти-вивезти товар. Також БД «Експертиза» може будувати таблиці зведених даних за певний період часу та зразу формувати звіти по ним.

Схема БД розроблена в програмному продукті Microsoft Access. Її вигляд зображено нижче.

Перш за все проведемо аналіз необхідної інформації та виділимо сутності. На схемі відобразимо всі сутності, та відношення між ними.

Схема БД показана на рисунку 6.1

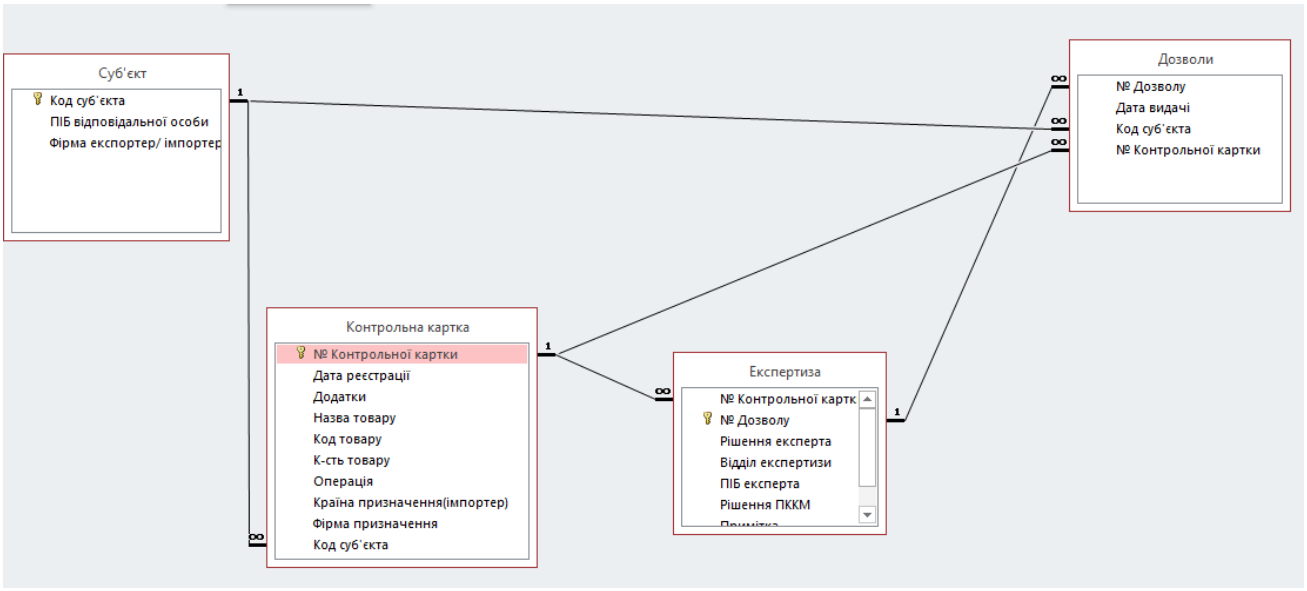


Рис. 6.1 Схема БД «Експертиза»

3.3 Створення (формування) вимог до КСЗІ

Відповідно до НД ТЗІ 1.4-001-2000 при створенні КСЗІ необхідно скласти вимоги до неї. Деталі до складених вимог викладені в НД ТЗІ 1.1-002-99. Ці два документи були використані при виконанні даного пункту завдання.

Під час складення вимог до КСЗІ було проаналізовано технологію обробки інформації та найбільш можливі загрози для неї. Під час цього аналізу було зроблено висновок, що загрози доступності та цілісності є найменш критичними для даної технології, через те, що всі документи дублюються в паперовому вигляді. Критичними загрозами для неї є порушення конфіденційності оброблюваної інформації.

3.3.1 Моделі порушників і загроз

Перед складанням моделей порушників було складено таблицю з напрямками захисту інформації для кожної з наявних АС.

№	АС	Обов'язкові напрямки захисту	Напрямки захисту	Пріоритетні властивості інформації
1	АС-1 «Альфа» (ВІ, ДСК)	НСД	НФСД, Аудит, Орг-захист	К
2	АС-2 «Браво» (Т, ЦТ)	НСД, ТКВ	НФСД, Аудит, Орг-захист	К
3	АС-2 «Фокстрот» (ВІ)	НСД	НФСД, Аудит, Орг-захист	Д

Табл. 7.1 Напрями захисту в АС

Також було визначено можливих порушників. Порушниками відносно АС можуть бути як особи з обслуговуючого персоналу, працівники ДСЕР, так і сторонні особи.

Можливі внутрішні порушники:

1. Працівники
2. Охорона установи
3. Системний адміністратор та обслуговуючий персонал

Можливі зовнішні порушники:

1. Клієнти
2. Обслуговуючі служби

№	Назва загрози	Порушники				
		Зовнішні		Внутрішні		
		1	2	1	2	3
1	НСД	+		+	+	+
2	НСФД	+	+	+	+	+
3	Виток через систему електроживлення		+			+
4	Виток через систему опалення		+	+		+
5	Виток за рахунок ПЕМВН		+			+

Табл. 7.2 Модель порушників

Для оцінки рівня загроз та можливих завданих збитків було використано оцінку експерта.

Шкала балів імовірності реалізації загроз наступна:

- малоймовірна загроза – 1 бал;
- можлива загроза – 2 бали;
- загроза, яка потребує особливої уваги – 3 балів.

Шкала балів величини збитків від реалізації загроз наступна:

- мінімальний збиток – 1 бал;
- середній збиток – 2 бали;
- максимальний збиток – 3 балів.

Обчислення величини ризику будемо за формулою

R=P*L

Де:

P - імовірність реалізації загрози;

L- величина збитку від реалізації загрози;

Загрози направлені на порушення конфіденційності, цілісності та доступності інформації наведені в таблиці**.**

№	Назва загрози	Можливі збитків	Ймовірність загрози	Ризик	Джерело загрози
Загрози пов’язані з НСД					
1	НСД до інформації, що зберігається на комп`ютерах відділу, іншими працівниками.	1	1	1	Зовнішні та внутрішні суб’єкти АС
2	НСД до серверів баз даних.	3	1	3	Зовнішні та внутрішні суб’єкти АС
3	Внесення Шкідливих програмних засобів через флеш-накопичувачі, або іншими шляхами.	2	2	4	Внутрішні об’єкти АС
4	Навмисне порушення цілісності інформації в АС іншими працівниками.	3	1	3	Внутрішні суб’єкти АС
Загрози пов’язані з НСФД					
1	Маскування під зареєстрованого співробітника з метою НСД до даних, які він обробляє.	3	1	3	Зовнішні суб’єкти АС
2	Використання незареєстрованих флеш-накопичувачів.	2	2	4	Внутрішні суб’єкти АС
3	Фізичний доступ і зчитування інформації	3	1	3	Зовнішні та

	з носіїв інформації співробітниками.				внутрішні суб’єкти АС

Табл. 7.3 Модель загроз для АС «Альфа»

№	Назва загрози	Можливі збитків	Ймовірність загрози	Ризик	Джерело загрози
Загрози пов’язані з НСД					
1	НСД до інформації, що зберігається на комп`ютерах відділу, іншими працівниками.	2	2	4	Внутрішні суб’єкти АС
2	НСД до серверів баз даних.	3	1	3	Внутрішні суб’єкти АС
3	Внесення Шкідливих програмних засобів через флеш-накопичувачі, або іншими шляхами.	3	1	3	Внутрішні та зовнішні суб’єкти АС
4	Навмисне порушення цілісності інформації в АС іншими працівниками.	2	2	4	Внутрішні суб’єкти АС
Загрози пов’язані з НСФД					
1	Маскування під зареєстрованого співробітника з метою НСД до даних, які він обробляє.	3	1	3	Зовнішні суб’єкти АС
2	Недотримання пропускного режиму до відділу співробітниками	3	2	6	Зовнішні та внутрішні суб’єкти АС
3	Використання незареєстрованих флеш-накопичувачів.	2	2	4	Внутрішні суб’єкти АС
4	Фізичний доступ і зчитування інформації з носіїв інформації співробітниками.	3	1	3	Внутрішні суб’єкти АС
Загрози пов’язані з ТКВ					
1	Утворення каналу витоку, обумовленого електричними і магнітними полями розсіяння ОТЗ	1	1	1	Внутрішні суб’єкти АС

2	Утворення каналів витоку, що виникають під час впливу електричних, магнітних або акустичних полів небезпечного сигналу на ДТЗС	2	2	4	Внутрішні суб'єкти АС
3	Підслуховування розмов, що ведуться в кабінетах, де працюють з таємною інформацією	2	1	2	Внутрішні, зовнішні суб'єкти АС
4	Встановлення вібродатчиків на опалювальні елементи будівлі.	3	1	3	Зовнішні суб'єкти АС
5	Підключення до електромереж для зняття ЕМ сигналів.	3	2	6	Зовнішні суб'єкти АС

Табл. 7.4 Модель загроз для АС «Браво»

№	Назва загрози	Можливі збитків	Ймовірність загрози	Ризик	Джерело загрози
Загрози пов'язані з НСД					
1	НСД до інформації, що зберігається на комп`ютері АС	1	1	1	Зовнішні та внутрішні суб'єкти АС
2	НСД до Web-серверу.	2	2	4	Зовнішні та внутрішні суб'єкти АС
3	Внесення Шкідливих програмних засобів через флеш-накопичувачі, або через Інтернет для подальшої атаки.	2	2	4	Внутрішні та зовнішні суб'єкти АС
Загрози пов'язані з НСФД					
1	Порушення роботи обладнання АС.	2	1	2	Зовнішні та внутрішні суб'єкти АС
2	Використання незареєстрованих флеш-накопичувачів.	2	2	4	Внутрішні суб'єкти АС

Табл. 7.5 Модель загроз для АС «Фокстрот»

3.3.2 Політика безпеки

Під політикою безпеки розуміється набір вимог, правил, обмежень, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Так у даному випадку було розроблено низку таких правил та вимог, що відповідають складеній моделі загроз. Були застосовані організаційні, фізичні заходи безпеки, захист від НСД та аудит.

До організаційних заходів, які відносяться до даної АС відносяться такі заходи:

1. Підбір кадрів для роботи з таємною інформацією, обов’язкове проходження співбесіди, психологічного та профвідборів.
2. Обмеження використання особистих мобільних та інших пристроїв, які можуть бути джерелом витоку інформації, у приміщеннях де працюють з ІзОД.
3. Заборона використання особистих засобів для накопичення інформації, особливо в приміщеннях де працюють з ІзОД.
4. Заборона розголошення інформації, що стала відомою під час роботи, поза ДСЕР.
5. Призначення відповідальних осіб за кожне АРМ.
6. При звільненні співробітників має підписуватись підписка про нерозголошення інформації.

До фізичних заходів безпеки можна віднести:

1. Облік друкованих документів.
2. Облік пристроїв накопичення.
3. Облік всіх технічних засобів, що задіяні в системі.

4. Опечатування технічних пристроїв, що використовуються, металевою печаткою відповідальної за ІБ особи.
5. Пропускний режим до будівлі ДСЕР та до відділів.
6. Приміщення у яких знаходяться засоби обробки інформації ДСК та вище обладнуються стальними дверима з автоматичними засовами та кодовими замками, охоронною сигналізацією. Безпека та контроль здійснюється за допомогою датчиків пожежної сигналізації, датчиків охоронної сигналізації, відеокамер з записом подій, моніторів відео спостереження.
7. Обмеження доступу співробітників до обслуговуючих приміщень.

Захист від НСД:

1. Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.
2. Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації

До заходів аудиту можна віднести:

1. Ідентифікація та аутентифікація користувачів в системі. Ведення журналів роботи з системою.
2. Контроль за програмним забезпеченням.

3. Контроль за використанням системи виключно у повноважної на це особи.

3.3.3 Стандартний функціональний профіль захищеності

Так як у системі наявні 3 АС для кожної з них потрібно вибрати стандартний профіль захищенності згідно з НД ТЗІ 2.5-005.99.

1. АС «Альфа» являє собою АС 2-го класу. Найбільш пріоритетними напрямками є захист конфіденційності. Доступність та цілісність не є критичними, так як документи дублюються в паперовому вигляді. Саме тому було вибрано наступний профіль:
2. 2.К.1 = { КД-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1 }
3. АС «Браво» також являє собою АС 2-го класу. Для цієї АС найбільш пріоритетними є напрями конфіденційності. Саме порушення цієї властивості може принести найбільші збитки для організації. Все через те, що в АС обробляється ІзОД з грифами Т і ЦТ. Властивість доступності та цілісності не є критичними через дублювання документції в паперовому вигляді, єдиний збиток від її порушення – затримка строків формування документів.

Для цієї АС було використано такий профіль захищенності:

2.К.4 = { КД-2, КА-2, КО-1, КК-1, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2 }

1. АС «Фокстрот» являє собою АС 3-го класу з можливістю виходу в мережу Інтернет. В ній не обробляється ІзОД, проте обробляється відкрита інформація, яка є власністю держави, саме тому потрібно будувати КСЗІ з підтвердженою відповідністю. Основною загрозою для цієї системи є порушення доступності, так як саме через цю АС

проходить інформування клієнтів ДСЕР та забезпечення керівництва ДСЕР доступом до мережі Інтернет.

Порушення конфіденційності та цілісності не є критичними, через відсутність ІзОД. Саме через це для даної АС було обрано наступний СФПЗ:

3.Д.1 = { ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1 }

3.3.4 Акт категоріювання відповідно до НД ТЗІ 1.6-005-13 і НД ТЗІ 1.6-006-15 для приміщень заданого відділу

ЗАТВЕРДЖУЮ

Керівник установи-власника (розпорядника, користувача) об’єкта

_____

(посада, підпис, ініціали, прізвище)

____. ____. 20___

М.П.

АКТ

категоріювання приміщення № 101

1. Підстава для категоріювання _____рішення про створення КСЗІ_____
2. Вид категоріювання _____первинне_____
3. На ОІД здійснюється обробка інформації технічними засобами та озвучування інформації
4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об’єкті ____таємна інформація_____

(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_____IV_____

Голова комісії _____ _____

(підпис) (ініціали, прізвище)

____.____. 20___

Члени комісії: _____ _____

(підпис) (ініціали, прізвище)

____.____. 20___

ЗАТВЕРДЖУЮ

Керівник установи-власника (розпорядника, користувача) об’єкта

_____

(посада, підпис, ініціали, прізвище)

____. ____. 20___

М.П.

АКТ

категоріювання приміщення № 108

1. Підстава для категоріювання _____рішення про створення КСЗІ_____
2. Вид категоріювання _____первинне_____
3. На ОІД здійснюється обробка інформації технічними засобами та озвучування інформації
4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об’єкті ____таємна інформація_____

(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_____II_____

Голова комісії _____ _____
(підпис) (ініціали, прізвище)

____.____. 20___

Члени комісії: _____ _____
(підпис) (ініціали, прізвище)

3.3.5 Перелік та склад можливих ТКВ на основі ПЕМВН

Було розглянуто відділ 1, він відповідає за реєстрацію та архівування матеріалів. У ньому обробляється ВІ та ДСК інформація. Також у відділі існує огороджена кімната для роботи з БД «Архів», інформація на якій йде з грифом Т. В цьому приміщенні потрібно організувати захист від ТКВІ.

Згідно схеми розміщення, можливими каналами витоку є витік через електромережу та через кабель Ethernet, який підключений до АС «Браво», також середовищем розповсюдження ПЕМВН можуть бути холодильник, телевізор і радіо, що є в кабінеті.

№	Назва, позначення засобу та його технічних умов	Призначення засобу	Виробник, місто
1	Фільтри мережеві протизавадні "ФМПЗ -1 – 3" ТУ У 02070921.186-99	Захист інформації, що обробляється засобами орг- та обчислювальної техніки, від витоку мережами електроживлення. Відповідає вимогам ТУ, зазначеним у сертифікаті	Технопарк "Перспектива " НТУУ "КПІ", м. Київ
2	Комплекс засобів захисту операційної системи MicrosoftWindows 10 Professional виробництва компанії MicrosoftCorporation, США	Призначений для використання в невеликих організаціях та сфері малого бізнесу. Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі "Державна експертиза за критеріями технічного захисту інформації операційної системи Microsoft Windows 10 Professional. Технічні вимоги", сукупність яких визначається функціональним профілем: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-	ТОВ "Майкрософт Україна", 01032, м. Київ, вул. Жилянська, 75

		99.	
3	Персональні комп'ютери із захистом інформації "EXPERT" (робочі станції) ТУ У 30.0-21503308.006-2001	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідають вимогам ГОСТ 29339-92, НД ТЗІ 2.2-005-08, НД ТЗІ 2.3-015-08, ОСТ 4.169.006-89 і ТУ в обсязі, зазначеному в сертифікаті	ТОВ "Епос", м. Київ,
4	Сервери "EXPERT" із захистом інформації ТУ У 30.0-21503308.006-2001	Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. Відповідає вимогам ГОСТ 29339-92 і ТУ в обсязі, зазначеному в сертифікаті	ТОВ "Епос", м. Київ,

7.6 Таблиця Засобів захисту від ПЕМВН

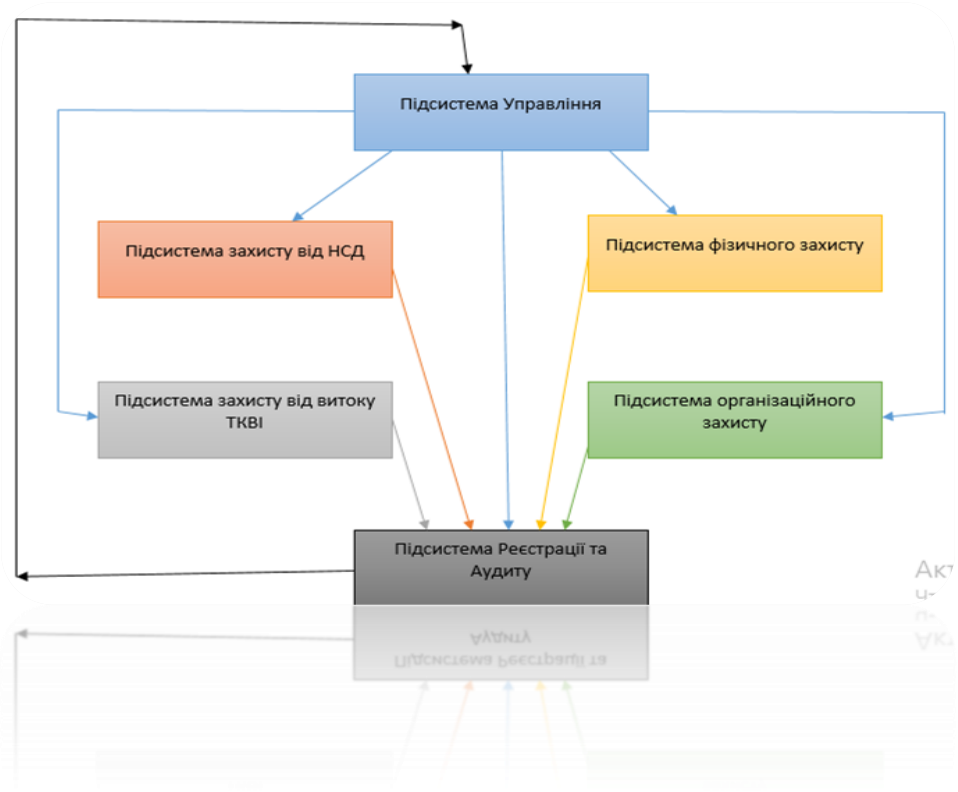
3.3.6 Перелік сертифікованих засобів захисту

№ з/п	Найменування	Призначення засобу	Перелік ф - х послуг захисту
1	Комплекс засобів захисту інформаційно-аналітичної системи „Кадри-Web” версії 8.х.х	Для реалізації автоматизованої технології обліку державних службовців та інших працівників в установах – суб’єктах владних повноважень та їх структурних підрозділах.	КА-2, КО-1, КВ-2, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-1, НИ-3, НК-1, НО-2, НЦ-1, НЦ-2, НТ-2, НВ-2 з рівнем Г-2 гарантій коректності їх реалізації згідно з НД ТЗІ 2.5-004-99
2	Комплекс засобів захисту системи „Мегаполіс. Документообіг-ДСК” версії 2.63	Для автоматизації процесів документообігу та діловодства документів, що містять відкриту, конфіденційну та службову інформацію. Відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі „Технічне завдання на створення комплексу засобів захисту системи	КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2, НА-2, НП-2 з рівнем гарантій Г-3 коректності їх реалізації згідно з НД ТЗІ 2.5-004-99
3	Комплекс засобів захисту	Призначений для використання в невеликих організаціях та сфері	КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1,

	операційної системи MicrosoftWindows 10 Professional виробництва компанії MicrosoftCorporation, США	малого бізнесу. Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі "Державна експертиза за критеріями технічного захисту інформації операційної системи Microsoft Windows 10 Professional.	ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99.
4	Комплекс засобів захисту програмної системи корпоративної електронної пошти “FossDocMail” версії 6.x	Для організації корпоративних систем обміну електронними поштовими повідомленнями. Відповідає вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі “Програмна система корпоративної електронної пошти “FossDocMail”.	КА-2, КО-1, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДР-1, ДЗ-1, ДВ-1, НР-2, НИ-1,НО-1, НЦ-1, НТ-2, НА-1, НП-1 з рівнем Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99

3.3.7 Компоненти КСЗІ

Схема 10.1 «Компоненти КСЗІ та їх взаємозв'язок



Підсистема управління – здійснює управління системою та реагування на помилки, збої.

Підсистема Реєстрації та Аудиту – реєструє усі події, що трапляються у системі, та повідомляє підсистему управління про помилки та збої.

Підсистема фізичного захисту – здійснює контроль фізичного доступу до обладнання, приміщень.

Підсистема організаційних заходів – описує загальні правила роботи системи.

Підсистема захисту від НСД – відповідає за доступ до інформаційного середовища та інформаційних ресурсів.

Підсистема захисту від витоку ТКВІ – відповідає за захист інформації від витоку ТКВІ.

3.4 Висновок за розділом

У даному розділі було проаналізовано призначення ДСЕР, приципів її функіонування та особливостей діяльності даної організації. На основі цих даних було отримано змогу якісного аналізу інформаційного середовища установи та принципів роботи майбутньої автоматизованої системи. Кінцевим результатом даного розділу –створення інформаційної (автоматизованої) системи для державної служби експертного регулювання, та на її основі комплексної системи захисту інформації.

ВИСНОВКИ

В роботі були розглянуті та досліджені методи та підходи в задачах класифікації зображень за допомогою нейронних мереж. Було описано вибір моделей, метрик якості, методів оцінки моделей та підбір гіперпараметрів, виконано порівняння різних моделей та відповідних підходів.

Вхідними даними для даної задачі були відкриті дані. Набір вхідних зображень не збалансований. Проблему дизбалансу класів було вирішено за допомогою методу аугументації.

Було проаналізовано наступні архітектури і проведено порівняльний аналіз наступних моделей:

- MobileNet.
- Dense Net
- Inception V3
- Sqeeze Net;

Найкращу точність показала модель DenseNet, яка підвищила точність початкової моделі більш ніж на 20%. Якщо ви хочете використовувати систему з обмеженими ресурсами, ви можете скористатися моделлю SqeezeNet, яка дає вам трохи більше точності, але розмір моделі менший.

Також у роботі описано алгоритмічну частину, які можливі для побудови нейронних мереж та побудови математичних моделей. Також було викладено суть методів обробки вхідних даних, вибір архітектур, функцій активації, метрик оцінки якості та методу оцінки моделі. Після чого було проведено підбір гіперпараметрів і проаналізовано отримані результати. Також було виконано порівняння чотирьох різних моделей, які були в процесі розроблено для конкретної задачі.

Якщо на одному зображені присутні два предмети, погана якість зобрадена або сам предмет зливається з фоном модель буде давати не правильні передбачення.

У розділі розробки проекту було визначено характеристики розроблюємого ПЗ з класифікації зображень. Також в цьому розділі було проаналізовано вибір фреймворку, мови написання і тд з аналогів. Було розроблено стратегії, на різні випадки розвитку ринку, описано вихід на ринок та залучення інвестицій.

Описаний продукт є корисним для підприємств, які потребують швидкої автоматичної класифікації зображень.

Отже, в роботі розрита науково-прикладна проблема: розробка методу автоматичної багатокласової категоризації зображень за допомогою систем штучного інтелекту.

Щоб досягти ці єї мети, було отримано:

1. набі р вхі дних даних дослі джений, очищений та вдосконалений;

2. Вибрані та спроектовані архі тектури нейронної мережі ;

3. обраний з метрики оці нки алгоритму, вибі р ві дпові дно до валі даці ї;

4. Дослі джено вплив компоненті в нейронної мережі на точні сть

класифі каці ї;

5. Гі перпараметри класу були дослі джені на предмет точності класифі каці ї.

Отримані результати призначені для впровадження в реальних системах, нижче - потенційні програми та практична цінність результатів в диплому:

1. Модель може використовуватись на будь-якому сайті чи мобільному додатку, де потрібна автоматична категоризація зображень;
2. Сформульовано основні концепти, на які потрібно звернути увагу при проектуванні архітектури нейронної мережі, описано метод та підходи, які дозволяють майже без втрат точності зменшити розміри моделі та швидкість отримання передбачень;
3. Розширивши набір даних та дотренувавши систему, можна використовувати для більшої кількості категорій, також можна взяти інший набір даних і спробувати застосувати ці ж методи та архітектури, можливо, трохи змінити параметри мережі і отримати іншу готову систему для класифікації зображень.

Отже, дана робота є актуальною і містить наукову новизну, в подальшому її можна вдосконалити таким чином, щоб її можна було використовувати в реальному часі, та спробувати зробити її більш універсальною для різних наборів даних.