ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ПОБУДОВА ЗАХИЩЕНОГО ПРИМІЩЕННЯ ЗГІДНО НОРМАТИВНИХ ДОКУМЕНТІВ»

на здобуття освітнього ступеня магістра

зі спеціальності 125 Кібербезпека та захист інформації
(код, найменування спеціальності)

освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ СКРЕБКОВ А.О.
(підпис) *(прізвище та ініціали)*

Виконав: здобувач вищої освіти гр. СЗДМ-61
СКРЕБКОВ А.О.
(прізвище та ініціали)

Керівник: к.т.н., доцент ПЕПА Ю.В.
науковий ступінь, вчене звання *(прізвище та ініціали)*

Рецензент: _____
науковий ступінь, вчене звання *(прізвище та ініціали)*

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра систем інформаційного та кібернетичного захисту

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедрою СІКЗ
_____ д.т.н. Туровський О.Л.
«_____» _____ 20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Скребкову Антону Олександровичу

(прізвище, ім'я, по-батькові здобувача)

1. Тема кваліфікаційної роботи: Побудова захищеного приміщення згідно нормативних документів

керівник кваліфікаційної роботи к.т.н., доцент Пепа Ю.В.

(прізвище та ініціали, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «_____» _____ 20__ р. № ___

2. Строк подання кваліфікаційної роботи «_____» _____ 20__ р.

3. Вихідні дані до кваліфікаційної роботи: _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. _____
2. _____
3. _____

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «_____» _____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Загрози інформації та засоби протидії у захищеному приміщенні		
2	Етапи створення захищеного приміщення		
3	Побудова захищеного приміщення банку		
4	Реферат, вступ, висновки		
5	Підготовка презентації до захисту		

Здобувач вищої освіти _____ Скребков А.О.
(підпис) *(прізвище та ініціали)*

Керівник кваліфікаційної роботи _____ Пепа Ю.В.
(підпис) *(прізвище та ініціали)*

РЕФЕРАТ

Текстова частина магістерської роботи: 88 сторінок, 5 рисунків, 4 таблиці, 17 джерел.

Об'єкт дослідження – процеси та способи захисту інформації у захищених приміщеннях, зокрема у серверних приміщеннях банківських установ.

Предмет дослідження – аналіз і проектування захищеного серверного приміщення банку, відповідно до чинних нормативних документів у галузі інформаційної безпеки.

Мета роботи – розгляд поняття захищеного приміщення, існуючих загроз, способів і засобів захисту від них, а також проектування захищеного серверного приміщення банку.

Методи дослідження – аналітичні методи, теорія електрозв'язку, теорія інформації, системний аналіз.

В кваліфікаційній роботі магістра було проведено розгляд і аналіз нормативних документів щодо захисту інформації у захищених приміщеннях. В проектній частині кваліфікаційної роботи, було розглянуто види та приклади інформації, яка обробляється та зберігається на серверах у серверному приміщенні банку, можливі загрози для цієї інформації, а також були сформовані рекомендації та вимоги для побудови захищеного приміщення та організації комплексного захисту, дотримування яких зменшить ступінь вразливості інформації.

Галузь використання – інформаційна безпека.

КЛЮЧОВІ СЛОВА: ЗАХИЩЕНЕ ПРИМІЩЕННЯ, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, КОМПЛЕКС ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КСЗІ – комплексна система захисту інформації

СЗІ – система захисту інформації

ІТС – інформаційно-телекомунікаційна система

КЗЗ – комплекс засобів захисту

ОІД – об'єкт інформаційної діяльності

ПК – персональний комп'ютер

АС – автоматизована система

КС – комп’ютерна система

ТЗІ – технічний захист інформації

ПЕМВН – побічні електромагнітні випромінювання і наведення

ЄСКД – єдина система конструкторської документації

ЄСПД – єдина система програмної документації

КТЗІ – комплекс технічного захисту інформації

ОТЗ - основні технічні засоби

КЗ – контрольована зона

НСД – несанкціонований доступ

ІзОД – інформація з обмеженим доступом

ОС – операційна система

ПЗ – програмне забезпечення

ОТЗС – основні технічні засоби і системи

ДТЗС – допоміжні технічні засоби системи

DDoS – Distributed Denial-of-service

ВСТУП

У сучасному світі, коли інформація стала найціннішим активом, питання забезпечення її надійного та ефективного захисту набуває особливої важливості. Одним із ключових аспектів цього процесу є побудова захищеного приміщення, що є фундаментальною ланкою в системі захисту конфіденційної інформації.

Побудова захищеного приміщення є складним завданням, яке вимагає глибокого розуміння технічних, організаційних та юридичних аспектів. Для ефективного вирішення цього завдання необхідно дотримуватися визначених стандартів та нормативів, які визначають вимоги до будівельної конструкції, систем безпеки та управління доступом.

У цьому контексті, важливо вивчати та впроваджувати нормативні документи, які регламентують побудову захищених приміщень. Це не лише сприяє забезпеченню безпеки інформації, але й забезпечує відповідність стандартам та уніфікованим вимогам. Дана тема є актуальною у зв'язку з постійними змінами у сфері технологій та зростанням загроз кібербезпеки. У цьому контексті, розгляд аспектів побудови захищеного приміщення згідно з нормативними документами визначається як критичний етап у забезпеченні цілісності та конфіденційності важливої інформації.

Мета роботи – розгляд поняття захищеного приміщення, існуючих загроз, способів і засобів захисту від них, а також проектування захищеного серверного приміщення банку.

Об’єкт дослідження – процеси та способи захисту інформації у захищених приміщеннях, зокрема у серверних приміщеннях банківських установ.

Предмет дослідження – аналіз і проектування захищеного серверного приміщення банку, відповідно до чинних нормативних документів у галузі інформаційної безпеки.

1. ЗАГРОЗИ ІНФОРМАЦІЇ ТА ЗАСОБИ ПРОТИДІЇ У ЗАХИЩЕНОМУ ПРИМІЩЕННІ

1.1. Визначення захищеного приміщення

Інформаційні ресурси, що належать державі, громаді або окремим організаціям та особам, представляють собою значущу цінність, мають відповідне матеріальне вираження і потребують захисту від різноманітних впливів, які можуть призвести до зменшення їхньої цінності. Такі впливи, спрямовані на зниження цінності інформаційних ресурсів, називаються несприятливими, а потенційно можливий негативний вплив отримує назву загрози [1].

Захищене приміщення - це спеціально обладнане і забезпечене приміщення, яке відповідає певним нормативам та вимогам, спрямованим на забезпечення безпеки і захисту від загроз інформаційних ресурсів та обладнання на якому створюються, зберігаються або обробляються такі інформаційні ресурси з обмеженим доступом.

Основні характеристики захищеного приміщення можуть включати:

- фізична безпека: забезпечення стійкості будівлі до впливу різних небезпечних чинників, таких як землетруси, пожежі, затоплення та інші чинники, що можуть пошкодити або знищити інформацію з обмеженим доступом;
- контроль доступу: використання систем контролю доступу, для фільтрації людей, які можуть потрапити в приміщення, і таким чином, забезпечення захисту від несанкціонованого вторгнення;
- системи безпеки інформації: захист конфіденційної інформації від несанкціонованого доступу, кібератак і інших загроз;
- аварійна готовність: наявність процедур для ефективної реакції на аварійні ситуації та загрози безпеці;
- енергозабезпечення: забезпечення стійкості електропостачання та інших енергетичних ресурсів;

- відповідність нормативам: проектування та будівництво приміщення відповідно до чинних будівельних і безпекових нормативів.

Розглянемо детальніше захист від потенційних загроз:

Щодо фізичної безпеки, а саме захисту від таких загроз як землетрус, пожежа або затоплення. Від землетрусів, які за 2023 рік відбувалися в межах Європи та навіть в Україні, а саме в Ужгороді, Львові, Полтаві, Словаччині, Туреччині та у Чорному морі, зможе захистити лише правильна будівельна конструкція приміщення, яка може бути спроектована таким чином, щоб витримувати землетруси.

Від пожеж захист можливий за допомогою використання при будуванні приміщення пожежостійких матеріалів, які не підтримують горіння або мають високий рівень пожежостійкості, прикладом таких матеріалів може слугувати:

- гіпсокартон (для стін, стель і перегородок), який має високий рівень пожежостійкості і може витримувати високі температури протягом певного часу без пошкодження;
- вогнеупорна цегла, яка виготовлена з вогнеупорних матеріалів, таких як шамот (вогнетривка глина), що робить цеглу стійкою до високих температур;
- вохнеупорний бетон, який містить вогнеупорні добавки, які забезпечують йому стійкість до вогню;
- вогнеупорні фарби, які містять вогнетривкі речовини і можуть захищати поверхні від впливу вогню.

Також від пожеж є технічний захист, а саме автоматичні системи газового, рідкого, пінного, порошкового, аерозольного вогнегасіння для швидкої реакції на виникнення пожежі у парі з розташуванням детекторів пожежі для раннього виявлення і сповіщення про вогонь, основні задачі яких – виявляти ознаки пожежі на ранній стадії, передавати тривожні повідомлення до пристроїв передачі пожежної тривоги та інформації про несправність та генерувати сигнали управління для систем протипожежного захисту та іншого інженерного обладнання, що активується під час пожежі. Головна мета такого обладнання – це

згасити пожежу, що почалася до того, як пожежний розрахунок затопить всю кімнату, для того, щоб уникнути великих збитків вже не від самої пожежі, а від піни чи іншої рідини, яка може залити важливе обладнання на якому зберігається або обробляється інформація, що навіть могло б і не постраждати через саму пожежу. Розглянемо детальніше типи систем автоматичного вогнегасіння:

- спосіб дії рідкого вогнегасіння полягає у використанні рідких хімічних реагентів, таких як водний розчин, щоб охолоджувати інфіковану зону і покривати поверхню вогню, щоб заборонити доступ кисню. Такі комплекси є найбільш поширеними на ринку;
- спосіб дії пінного вогнегасіння полягає у використанні піни, яка покриває поверхню горіння, утворюючи бар'єр, який пригнічує пожежу, і запобігає повторному запаленню. Зазвичай така автоматична система вогнегасіння використовується в приміщеннях де є висока вірогідність осередків займання легкозаймистих речовин і рідин для їх подальшого придушення;
- спосіб дії аерозольного вогнегасіння полягає у використанні часток твердого вогнегасного матеріалу, який перетворюється в аерозольну хмару в разі виявлення пожежі. Ця хмара ефективно загасає вогонь, витрачаючи кисень та охолоджуючи зону горіння. Зазвичай така автоматична система вогнегасіння використовується в приміщеннях з електронним обладнанням;
- спосіб дії газового вогнегасіння полягає у використанні газів, таких як хладон, CO2 (вуглекислий газ), азот або інші, щоб зменшити концентрацію кисню, необхідного для горіння, або для видалення тепла від зони вогню. Зазвичай така автоматична система вогнегасіння використовується в приміщеннях з цінним майном та де важко, ризиковано або неможливо застосувати рідкі реагенти бо це завдасть велику матеріальну шкоду (наприклад, бібліотеки, архіви, комп’ютерні центри);
- спосіб дії порошкового вогнегасіння полягає у використанні подачі у вогнище дрібнодисперсного порошкового гасячого речовини. Зазвичай

така автоматична система вогнегасіння використовується у складських і промислових приміщеннях (у томи числі, через невелику вартість) для придушення області загоряння, що виникла через електрообладнання або нафтопродуктів.

Від потопів захист може здійснюватися також як інженерно, так і технічно. Наприклад, до інженерних рішень для захисту від затоплень можна віднести:

- ущільнення підлоги, стін та стелі шляхом використання спеціальних герметизуючих матеріалів для підлоги, стін та стелі може допомогти запобігти проникненню води;
- використання систем піднятих підлог для створення додаткового простору, де можна розмістити дренажні труби або системи відведення води. Також рекомендується робити незначний нахил підлоги у бік дренажного отвору або отворів, якщо їх декілька, для того, щоб у випадку попадання води на підлогу, вона якнайшвидше потрапила до системи водовідведення;
- використання автоматичних систем відкачування води, які встановлюються для відведення води, яка може накопичуватися під будівлею або в приміщенні.

До технічних рішень для захисту від затоплень можна віднести:

- системи раннього виявлення затоплень використовують датчики, які реагують на підвищення вологості та якщо виявляється підозра на витік води, система негайно повідомляє про відповідний персонал;
- системи автоматичного відключення електропостачання при виявленні затоплення можуть автоматично відключити електропостачання для запобігання короткого замикання та пошкодження обладнання;
- системи автоматичного відключення водопостачання при виявленні прориву труб можуть автоматично відключити водопостачання для запобігання подальшому розповсюдженню води.

Для забезпечення контролю доступу та фільтрації людей, які можуть потрапити в приміщення, можна використовувати різноманітні системи контролю доступу. Детальніше розглянемо приклади деяких з них:

- використання сучасних електронних ключів або карток, які мають інформацію про права доступу користувача;
- безконтактні картки, які можуть бути зчитані безпосередньо або через невеликий зчитувач;
- біометричні системи, які використовують біометричні дані, такі як відбитки пальців, розпізнавання обличчя або сканування радужок для ідентифікації користувачів;
- кодові замки, які відкриваються за допомогою введення правильного коду на клавіатурі;
- системи розпізнавання RFID (Radio-Frequency Identification) використовують RFID-технологію для ідентифікації та відстеження об'єктів та осіб;
- системи відеоспостереження, що включають в себе встановлення камер спостереження для відстеження та запису дій осіб, які намагаються потрапити в приміщення;
- системи двохфакторної ідентифікації забезпечують використання двох або більше методів ідентифікації, наприклад, комбінації пароля і відбитка пальця;
- системи електронних браслетів, які містять інформацію про доступ та можуть взаємодіяти з системою контролю доступу.

Для забезпечення безпеки інформації, існує безліч систем безпеки інформації, які можуть використовуватися окремо або в поєднанні для комплексного захисту інформації від різних видів загроз, тож розглянемо деякі з них:

- системи шифрування даних використовуються для захисту інформації шляхом перетворення її в незрозумілу форму, яку можна розкодувати тільки з допомогою правильного ключа;
- системи виявлення та захисту від вторгнень займаються моніторингом мережі чи системи на предмет надзвичайних або підозрілих активностей і реагують для запобігання або обмеження потенційно шкідливих подій;
- системи антивірусного захисту сканують та виявляють шкідливі програми, віруси та інші загрози, які можуть завдати шкоди інформації;
- системи резервного копіювання та відновлення забезпечують регулярне створення резервних копій даних для відновлення інформації у випадку втрати або пошкодження;
- системи моніторингу та аудиту забезпечують ведення журналів подій, аналізують та реєструють активності користувачів для виявлення можливих загроз;
- екранування приміщення спрямоване на зменшення або блокування впливу електромагнітних полів на обладнання чи інформацію в середині, це може бути важливим для забезпечення конфіденційності і захисту від електромагнітних перешкод чи шпигунства. Екранування приміщення включає в себе блокування зовнішніх джерел, глушники, електромагнітні фільтри, екрановані матеріали для оздоблення приміщення, екрановані шафи, коробки або камери для розміщення чутливого обладнання чи інформації.

Для забезпечення аварійної готовності може використовуватися чіткий план дій, який може містити у собі, наприклад, наступні пункти:

- використання систем моніторингу та виявлення вторгнень для розпізнавання аномальних активностей або змін, які можуть свідчити про кібератаку;
- вживання заходів для призупинення або обмеження дії атаки, якщо це можливо, з метою запобігання подальшим збиткам;

- відокремлення та ізоляція інфікованих або компромітованих систем від мережі для запобігання поширенню атаки;
- проведення детального аналізу інциденту для визначення обсягу атаки, методів вторгнення та виявлення потенційних слабкостей;
- сповіщення внутрішніх служб безпеки, адміністраторів систем та інших зацікавлених сторін про інцидент;
- взаємодія з зовнішніми службами безпеки, якщо це необхідно, і відправлення звіту про інцидент в компетентні органи;
- зберігання журналів подій та інших доказів, які можуть допомогти при подальшому розслідуванні;
- проведення аудиту інциденту для визначення причин та уроків із вчинених помилок для подальшого покращення систем безпеки.

Важливо, щоб персонал, який відповідає за безпеку інформації, був добре підготовлений та регулярно тренувався з метою ефективної реакції на інциденти та відновлення нормального функціонування систем.

Забезпечення енергозабезпечення для захищеного приміщення на сьогоднішній день є дуже актуальною темою для України та включає в себе ряд заходів та технічних рішень для стійкості електропостачання та інших енергетичних ресурсів, втрата яких, навіть на секунду, здатна принести чималої шкоди. Ось кілька ключових аспектів, які можна врахувати:

- встановлення систем резервного електропостачання, таких як генератори електроструму, які можуть автоматично активуватися у випадку відмови основного джерела електропостачання;
- використання акумуляторних систем для тимчасового живлення в разі перерв у постачанні електроенергії. Це може забезпечити час на переключення на резервне джерело енергії;
- встановлення систем неперервного живлення для захисту від коротких перерв у подачі електроенергії та стабілізації напруги;

- використання енергоефективного обладнання та технологій для зменшення енергоспоживання і забезпечення більш ефективного використання електроенергії;
- впровадження систем моніторингу енергоспоживання та автоматизації, що дозволяє ефективно керувати електроживленням та автоматично реагувати на відмови;
- врахування географічного розташування при виборі місця для захищеного приміщення, з урахуванням наявності альтернативних джерел енергії, таких як сонячні батареї або вітрогенератори;
- впровадження заходів захисту від енергетичних загроз, таких як електромагнітні перешкоди;
- створення планів резервних джерел енергії та їхнього підтримання, зокрема, регулярна перевірка та обслуговування обладнання;
- тренування персоналу з питань взаємодії з резервними системами та енергозабезпеченням в аварійних ситуаціях.

Вище перелічені заходи сприятимуть забезпеченню стійкості електропостачання та енергетичних ресурсів для захищеного приміщення в умовах різних ситуацій.

Забезпечення відповідності будівництва і проектування приміщення чинним будівельним і безпековим нормативам включає в себе кілька ключових етапів:

- проведення детального аналізу чинних будівельних, пожежних, електротехнічних та інших відповідних нормативів. Це включає ознайомлення зі специфічними вимогами до будівель та приміщень для конкретного типу діяльності;
- залучення кваліфікованих фахівців, таких як інженери, архітектори та інші спеціалісти, які мають досвід у роботі з відповідними нормативами та стандартами;

- отримання всіх необхідних ліцензій і дозволів від відповідних органів влади. Це може включати ліцензії на будівництво, використання земельної ділянки, пожежну безпеку тощо;
- створення проекту будівлі або приміщення, який враховує всі вимоги та нормативи. Це включає в себе правильне розташування приміщення, дотримання будівельних матеріалів, систем безпеки, інженерних мереж та інших важливих параметрів;
- проведення регулярних інспекцій та аудитів, щоб переконатися, що будівля відповідає всім чинним нормативам. Це може включати технічні інспекції, огляди безпеки та інші процедури;
- налагодження ефективного зв'язку із земельними, будівельними і пожежними органами для вирішення питань відповідності та виправлення недоліків, якщо такі виявляються;
- внесення відповідних змін та модифікацій у будівельний проект та приміщення, якщо відбулись зміни у чинних нормативах або стандартах безпеки.

Забезпечення відповідності нормативам - це процес, що вимагає уважного слідкування за змінами у відповідних законодавчих актах та стандартах та невпинного вдосконалення систем безпеки та будівельних рішень.

Захищені приміщення можуть використовуватися у різних галузях, включаючи військову, комерційну, наукову та інші, в залежності від специфіки застосування і вимог їхнього використання.

Інформаційно-телекомунікаційна система (ІТС) – це комплекс взаємопов'язаних елементів, які об'єднують технічні та організаційні засоби для збору, обробки, зберігання, передачі та використання інформації. ІТС включає в себе апаратні засоби (сервери, комунікаційне обладнання, комп'ютери тощо), програмне забезпечення (операційні системи, програми для обробки інформації), мережеві з'єднання та людей, які взаємодіють з системою.

Зв'язок інформаційно-телекомунікаційної системи з захищеним приміщенням полягає в тому, що ІТС може бути розміщена або обслуговуватися в

захищеному приміщенні з метою забезпечення високого рівня фізичної та технічної безпеки інформації.

У березні 2006 року були ухвалені "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах". У цих правилах визначено, що для захисту інформації в системі створюється КСЗІ (комплексна система захисту інформації). Головна мета КСЗІ полягає в захисті інформації від таких подій, як:

- витік технічними каналами, включаючи канали ПЕМВН, які утворюються через фізичні процеси;
- несанкціоновані дії з інформацією;
- вплив на засоби обробки інформації, який може призвести до порушення цілісності, здійснюючись за допомогою формування фізичних полів і сигналів [2].

Згідно з Законом України "Про захист інформації в інформаційно-телекомунікаційних системах", термін "комплексна система захисту інформації" визначається як взаємопов'язана сукупність організаційних, інженерно-технічних заходів, засобів і методів, спрямованих на забезпечення безпеки інформації [3].

Згідно з восьмою статтею цього закону, яка стосується "Умов обробки інформації в системі", вказується, що інформація із обмеженим доступом чи та, яка є власністю держави, повинна оброблятися в системі застосуванням комплексної системи захисту інформації з підтвердженою відповідністю, яка проходить державну експертизу. Для створення такої системи захисту інформації, яка є власністю держави, використовуються засоби захисту інформації, що мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи [3].

У випадку обробки інформації в системі, яка є державною таємницею або обраною власником інформації, здійснюється захист від витоку через технічні канали. Закон України "Про інформацію" підтверджує, що публічна або задокументована інформація в різних сферах, таких як політика, економіка і т.д., є об'єктом інформаційних відносин [4].

Існує кілька основних видів інформаційної діяльності, які включають отримання, використання, поширення та зберігання інформації:

- отримання інформації передбачає набуття, накопичення або придбання неї суб’єктами (громадянами, державою або юридичними особами);
- використання інформації включає задоволення інформаційних потреб суб’єктів;
- поширення інформації означає розповсюдження публічно оголошуваної чи документованої інформації;
- зберігання інформації включає забезпечення належного стану інформації.

Об'єднання обчислювальної системи, фізичного середовища, персоналу та оброблювальної інформації утворює автоматизовану систему, яка включає в себе організаційно-технічну структуру для реалізації інформаційної технології. В сучасному світі використовується така класифікація автоматизованих систем:

- АС-1: обробка інформації однієї або декількох категорій конфіденційності, за допомогою одномашинного комплексу для одного користувача, наприклад, автономний ПК із забезпеченням доступу через організаційні засоби безпеки.
- АС-2: обробка інформації різних категорій конфіденційності, використання локалізованого багатомашинного багатокористувацького комплексу, такого як локальна обчислювальна мережа.
- АС-3: обробка інформації різних категорій конфіденційності за допомогою розподіленого багатомашинного багатокористувацького комплексу, такого як глобальна мережа. Відмінність від АС-2 полягає в необхідності передачі інформації через незахищене середовище [5].

Збереження інформації, яка обробляється в автоматизованих системах, включає в себе впровадження та підтримку ефективних заходів як технічного (інженерно-технічного, програмно-апаратного), так і нетехнічного (правового, організаційного) характеру. Ці заходи призначені для запобігання або ускладнення можливості виконання загроз і зменшення можливих збитків. Або ж

можна сказати, що для успішного збереження інформації необхідно націлитися на забезпечення безпеки оброблюваної інформації та автоматизованої системи загалом. Це означає досягнення стану, що гарантує збереження визначених властивостей інформації та автоматизованої системи, якою вона обробляється. Сукупність заходів, спрямованих на захист інформації в автоматизованій системі, називається комплексною системою захисту інформації (КСЗІ).

Організаційні заходи мають важливе значення у забезпеченні безпеки інформації в автоматизованій системі. Проте, з розвитком інформаційних технологій спостерігається тенденція до зростання потреби в застосуванні технічних засобів та заходів захисту для вирішення істотної частини проблем у цій сфері.

Сама ж класифікація автоматизованих систем базується на вимогах до забезпечення властивостей інформації, таких як конфіденційність, цілісність та доступність. Кожен клас автоматизованих систем має підкласи з підвищеними вимогами для забезпечення вказаних властивостей інформації.

Розглянемо детальніше підкласи, що формуються в кожному класі автоматизованої системи відповідно до підвищених вимог щодо забезпечення інформаційної:

- конфіденційності (х.К);
- цілісності (х.Ц);
- доступності (х.Д);
- конфіденційності та цілісності (х.КЦ);
- конфіденційності та доступності (х.КД);
- цілісності та доступності (х.ЦД);
- конфіденційності, цілісності та доступності (х.КЦД) [5].

Для кожного підкласу у межах кожного класу визначається конкретна кількість ієрархічних функціональних профілів. Ці профілі можуть відрізнятися для різних класів і підкласів автоматизованих систем (АС). Важливо відзначити, що профілі розглядаються як ієрархічні, оскільки їхнє впровадження забезпечує

поетапне збільшення рівня захищеності від загроз конфіденційності, цілісності та доступності відповідного типу. Це зростання рівня захисту може бути досягнуте як посиленням існуючих послуг через включення більш високорівневих елементів, так і шляхом введення нових послуг у структуру профілю.

Стандартний функціональний профіль захищеності представляє собою перелік мінімально необхідних рівнів послуг, які повинен надавати комплекс засобів захисту автоматизованої системи для відповіді конкретним вимогам щодо захищеності інформації, що обробляється або зберігається в даній системі.

Стандартні функціональні профілі формуються на основі наявних вимог щодо захисту конкретної інформації від певних загроз, а також використання відомих на сьогоднішній день функціональних послуг для протидії цим загрозам та забезпечення виконання встановлених вимог.

Для стандартних функціональних профілів захищеності не встановлюється жодна зв'язана з ними політика безпеки або рівень гарантій. Політика безпеки комплексу засобів захисту, що реалізує певний стандартний профіль, повинна бути узгоджена з відповідними документами, що встановлюють вимоги до обробки конкретної інформації в межах автоматизованої системи. Отже, один і той же профіль захищеності може використовуватися для опису функціональних вимог з захисту оброблюваної інформації як для операційних систем, так і для систем управління базами даних (СУБД), при цьому їх політика безпеки, зокрема визначення об'єктів, може відрізнятися [5].

Профіль містить у собі три складові: буквено-цифровий ідентифікатор, символ рівності та перелік рівнів послуг, розташованого у фігурних дужках. Ідентифікатор включає в себе позначення класу АС – перший, другий або третій, також буквену частину, що описує види загроз, що потребують захисту – конфіденційність, доступність, цілісність або комбінація, і номер профілю та, за необхідності, буквене позначення версії. Усі частини ідентифікатора розділяються крапкою. Візьмемо за приклад профіль 3.Ц.2 – профіль номер два, який встановлює вимоги до автоматизованої системи третього класу, призначеного для забезпечення цілісності, що і є основною вимогою при обробці інформації.

Використані система класифікації та профілі захищеності мають за мету спростити вибір необхідних функцій для комплексу засобів захисту автоматизованої системи (АС) і забезпечити економію витрат на початковому етапі створення системи засобів захисту інформаційно-комунікаційної системи. Однак перед прийняттям рішення необхідно провести ретельний аналіз потенційних загроз і оцінити ризики для створення КЗЗ, який належним чином врахує особливості конкретної автоматизованої системи.

Термін "режим доступу до інформації" визначає порядок отримання, використання, поширення та зберігання інформації відповідно до чинного законодавства. У цьому контексті інформацію можна розділити на дві категорії: відкриту та ту, до якої обмежується доступ (ІзОД). Згідно з законодавством України, а саме закону України "Про інформацію", усю інформацію класифікують за режимом доступу, враховуючи встановлені правові норми (рис 1.1) [6].

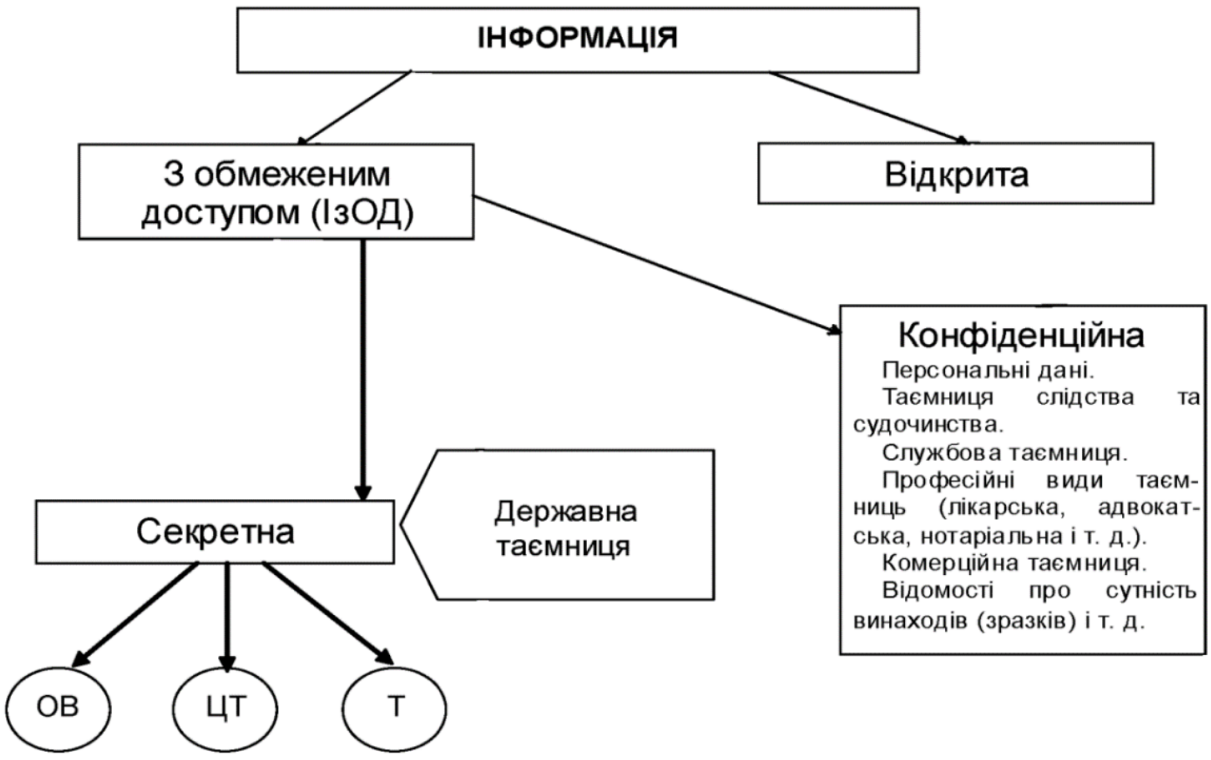

Рис. 1.1 – Види інформації в Україні згідно чинного законодавства

Інформація з обмеженим доступом (ІзОД) поділяється на конфіденційну та секретну, і не є загальнодоступною. Конфіденційною вважається інформація, яка

перебуває у власності окремих осіб і може розголошуватися відповідно до їхнього бажання.

Секретною визначається інформація, яка охоплює сфери науки, оборони, державної безпеки і т. д. Розголошення такої інформації може завдати шкоди національній безпеці України. Така інформація визнається державною таємницею та підлягає захисту з боку держави. Секретна інформація поділяється на особливо важливу, таємну та цілком таємну.

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», забезпечення цілісності при обробці відкритої інформації передбачає захист від несанкціонованих дій, що можуть спричинити пошкодження або знищення інформації. Обробка інформації з обмеженим доступом вимагає захисту від неконтрольованого та несанкціонованого доступу, модифікації, знищення, копіювання та поширення [2].

1.2. Шляхи втрати інформації

Для забезпечення конфіденційності, цілісності і доступності інформації необхідно вжити заходів щодо захисту від витоку та упередження втручання в систему чи об'єкт, де зберігається інформація.

Найчастіше помилки виникають від користувачів або обслуговуючого персоналу системи, і ці помилки є ненавмисними та потенційно небезпечними. Інколи їх можна розглядати як загрозу, що може призвести до колапсу системи. У випадках, коли помилка стає безпосередньою загрозою для безпеки об'єкта, це може трапитися навіть без зловмисницьких дій. Наприклад, швейцарський оператор, введучи невірну інформацію в комп'ютер, спричинив зіткнення двох літаків у повітрі.

Результати досліджень в галузі інформаційної безпеки свідчать, що шкода, завдана інформаційним ресурсам, в більшій мірі є наслідком ненавмисних помилок, а саме 65% загальної шкоди. Загрози природного характеру, такі як пожежа чи землетрус, виникають значно рідше.

Загальну класифікацію загроз можна представити наступним чином (див. рис. 1.2):

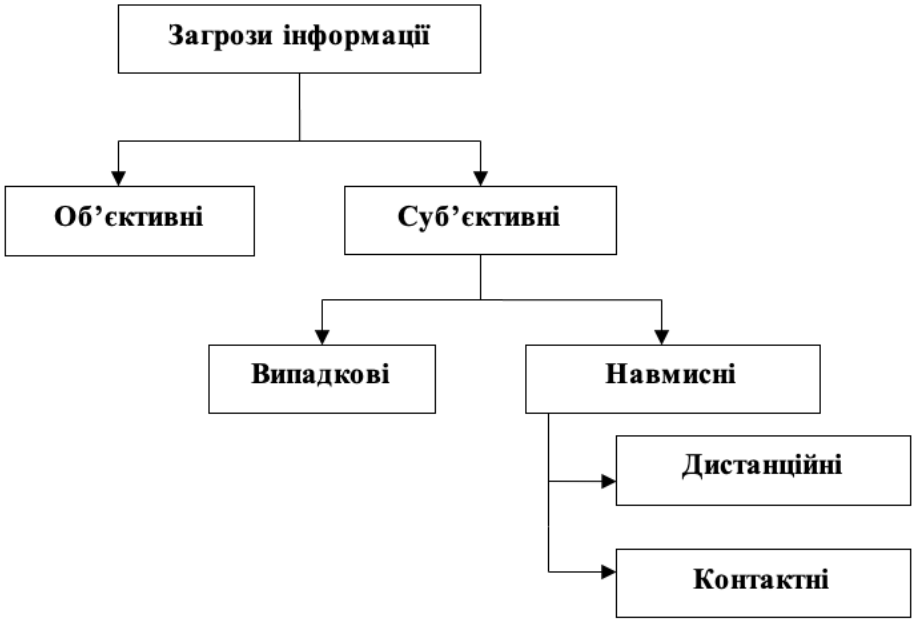

Рис. 1.2 – Загальна класифікація загроз інформації

Суб’єктивні загрози, залежно від походження, розподіляються на випадкові та навмисні. Випадкові загрози виникають внаслідок помилок у проектуванні автоматизованих систем, систем захисту інформації та захищених приміщень, таких як програмні помилки, збої систем забезпечення та апаратури, нехтування нормативам будування захищених приміщень або людські помилки, допущені персоналом, який обслуговує систему. Навмисні загрози виникають в результаті цілеспрямованих дій людей, тоді як ненавмисні загрози виникають внаслідок випадкових подій, помилок проектування або несприятливих умов, які не мають свідомого наміру завдати шкоду інформаційній системі чи об'єкту.

За розташуванням, навмисні загрози поділяються на дистанційні та контактні. Дистанційні загрози є тими, що виникають на відстані від контрольованої території, і можуть включати такі сценарії, як зовнішні кібератаки чи електронне шпигунство, що здійснюється віддалено. Ці загрози можуть стати особливо небезпечними через використання віддалених технологій, таких як хакерські атаки чи атаки через мережу Інтернет.

Навпаки, контактні загрози виникають всередині зони контролю, включаючи фізичний доступ до об'єкта або приміщення. Це може включати в себе несанкціонований вхід у приміщення, де зберігається інформація, використовуючи методи фізичного вторгнення або отримання доступу до компрометованого обладнання прямим контактом.

Враховуючи різноманіття та складність сучасних загроз, важливо розробляти імовірні сценарії та заходи безпеки для ефективного управління як дистанційними, так і контактними загрозами на всіх рівнях захисту.

За видом основного засобу, що використовується для реалізації загроз, джерела загроз поділяються на категорії, які включають в себе різні аспекти, які можуть впливати на безпеку інформації та інформаційних систем. Ці категорії мають наступний вигляд:

- людина – це можуть бути як зловмисники та хакери, тобто особи, які мають намір несанкціоновано отримати доступ до інформації з метою викрадення, руйнування чи модифікації, так і персонал організації, через який внутрішні загрози можуть виникати через недбалість, недостатню освіту з питань безпеки, або навіть умисні дії зсередини;
- апаратура – це можуть бути пристрої, які використовують певні технічні або інженерні вади, а саме дефекти в автоматизованих системах, програмному забезпеченні або недостатню захищеність приміщення, де фігурує інформація з обмеженим доступом, які можуть створювати точки вразливості;
- шкідливе програмне забезпечення, що розроблене для завдання шкоди, таке як видалення, модифікація чи перехоплення інформації;
- фізичне середовище – наприклад, формування фізичних полів і сигналів що можуть призвести до порушення цілісності інформації.

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99), існує чотири класи, що поділяють загрози за наслідками їх впливу на інформацію або систему обробки, представляючи різні сценарії вразливостей та можливих порушень, розглянемо їх детальніше:

- порушення конфіденційності – загрози, які відносять до несанкціонованої взаємодії з інформацією і, як результат, витік чутливої інформації, тобто отримання інформації без дотримання встановлених правил доступу, що може призвести до неправомірного використання або розголошення конфіденційної інформації;
- порушення цілісності – зміна (модифікація) чи видалення інформації, а саме, ситуації, в яких інформацію частково або повністю модифікують чи знищують, що може призвести до втрати достовірності та вірогідності даних;
- порушення доступності – непрацездатність системи, наприклад, ситуації, коли система стає непрацездатною або доступ до неї блокується, може бути наслідком атак, вірусів або інших форм впливів;
- втрата спостережливості або керованості системи – неможливість ідентифікації користувача та його дій, коли система втрачає здатність ідентифікувати користувача та надавати йому відповідні повноваження, що може призвести до використання неправомірного доступу та потенційно шкідливих дій.

Ці класи загроз визначають різні аспекти, які слід враховувати при розробці та впровадженні заходів безпеки для забезпечення стійкості та функціональності інформаційних систем.

Перелік областей персональних електронно-обчислювальних машин, захист даних яких необхідно забезпечити, включають в себе постійну та оперативну пам’ять, захист носів інформації різного виду (лазерний, магнітний та магнітооптичний), зовнішній пристрій для збереження інформації з колективним доступом, захист екранів та моніторів, захист пам'яті пристроїв виведення та введення, захист пам'яті керуючих пристроїв і ліній зв'язку, які формують канали сполучення комп'ютерних мереж.

Формування каналів витоку інформації відбувається через електромагнітні поля, а також за допомогою наведення напружень і струмів в провідних системах, випромінювань оброблюваної інформації на частотах паразитної генерації

елементів і пристроїв технічного захисту електронно-обчислювальних машин, а також випромінювання інформації при обробці на контрольно-вимірювальній апаратурі.

Окрім вищенаведених каналів, які обумовлені процесами, що відбуваються в персональній електронно-обчислювальні машині та її технічними характеристиками, в області персональних електронно-обчислювальних машин також можуть бути навмисно введені додаткові канали витоку інформації.

Додаткові канали витоку інформації можуть бути свідомо виготовлені шляхом вбудовування мікрофонів чи інших прихованих засобів у персональні електронно-обчислювальні машини. Наприклад, можуть бути використані спеціальні закладні пристрої, які приховано вбудовані в систему та маскуються як електронні блоки. Ці пристрої призначені для перехоплення оброблюваної інформації, такої як мовлення користувача.

Ще одним способом навмисного витоку інформації є встановлення радіомаячок в ПЕОМ для передачі конфіденційних даних на зовнішні приймачі. Цей метод може бути використаний для віддаленого збору інформації.

Застосування спеціальних конструктивних рішень, спрямованих на збільшення електромагнітних випромінювань в певному частотному діапазоні, може стати причиною ненавмисного розголошення інформації. Заходи безпеки повинні бути узгоджені з архітектурними та технічними рішеннями, щоб ефективно мінімізувати цей ризик.

Зловмисники можуть встановлювати закладні пристрої, призначені для знищення персональних електронно-обчислювальних машин ззовні. Це може включати в себе вплив на роботу системи, перевантаження або знищення важливих компонентів.

Здатність елементної бази виходити з ладу може бути використана як метод витоку інформації. Це може включати в себе зміну напруги, перегрів або дефект елементів системи, що може призвести до виходу з ладу ПЕОМ або її окремих компонентів. Заходи безпеки, такі як резервне копіювання даних та постійний моніторинг елементів, можуть бути важливими для попередження таких атак.

Крім цього, для першого наближення до класифікації можливих каналів витоку інформації можна використовувати принципи обробки отриманої інформації, зокрема три типи обробки: людиною, апаратурою та програмою. Кожен тип обробки передбачає три групи каналів витоку.

У відношенні до персональних електронно-обчислювальних машин, канали витоку інформації, які піддаються основній обробці людиною, включають наступні можливості:

- розкрадання матеріальних носіїв інформації – цей метод витоку інформації охоплює викрадення фізичних носіїв, на яких зберігається конфіденційна інформація, таких як магнітні диски, стрічки або картки пам'яті. Зловмисники можуть отримати фізичний доступ до цих пристроїв і використовувати їх для незаконного копіювання, переміщення або видалення конфіденційних даних. Запобіжні заходи можуть включати в себе фізичні заходи безпеки, такі як обмежений доступ до приміщень, де зберігається обладнання, і шифрування даних на носіях;
- читання інформації з екрану (монітору) сторонніми особами – цей вид атаки може виникнути, коли стороння особа намагається визначити або зафіксувати інформацію, яка відображається на екрані монітора. Запобіжним заходом також може бути фізичний захід безпеки;
- читання інформації з паперових документів, які залишаються без нагляду – цей сценарій витоку інформації може виникнути, коли конфіденційні документи залишаються без нагляду і стають доступними стороннім особам. Для захисту від цього ризику, необхідно встановити правила безпеки щодо залишення обладнання і документів без нагляду, а також використовувати засоби фізичного захисту для обмеження доступу до цих зон.

У відношенні до персональних електронно-обчислювальних машин, канали витоку інформації, які піддаються основній обробці апаратурою, включають наступні можливості:

- підключення до персональних електронно-обчислювальних машин спеціально розроблених апаратних засобів, які надають доступ до інформації – цей метод витоку інформації може включати в себе використання спеціально адаптованих апаратних пристроїв, які намагаються отримати несанкціонований доступ до персональних електронно-обчислювальних машин. Зловмисники можуть використовувати ці пристрої для обходу стандартних заходів безпеки, щоб отримати доступ до конфіденційної інформації на комп'ютері. Це вимагає ретельної перевірки та моніторингу зовнішніх підключень, а також застосування заходів контролю доступу;
- зловмисник використав спеціальні технічні засоби, щоб перехопити електромагнітні випромінювання технічних засобів ПЕОМ – цей вид атаки передбачає використання спеціальних технічних засобів для перехоплення електромагнітних сигналів, які виникають під час функціонування технічних засобів ПЕОМ. Наприклад, зловмисники можуть використовувати засоби для аналізу електромагнітних випромінювань індикаторів, клавіш, або навіть внутрішніх компонентів електронних пристроїв. Заходи безпеки можуть включати в себе екранування електроніки та використання криптографічних методів для захисту інформації від можливого перехоплення.

У відношенні до персональних електронно-обчислювальних машин, канали витоку інформації, які піддаються основній обробці програмою, включають наступні можливості:

- реалізація несанкціонованого доступу програми до інформації – цей канал витоку може виникнути, коли програма отримує доступ до інформації без належних авторизацій або використовує недоліки в системі безпеки для отримання конфіденційних даних. Захист від цього витоку може включати в себе вдосконалення системи автентифікації та авторизації, а також ретельний моніторинг дій програм;

- здійснення програмою розшифровки зашифрованої інформації. Якщо програма отримує доступ до зашифрованих даних і може їх розшифрувати, це може призвести до розкриття конфіденційної інформації. Для захисту від цього виду витоку слід використовувати надійні алгоритми шифрування та контроль доступу до ключів шифрування;
- копіювання програмою інформації з носіїв – цей канал витоку стосується ситуацій, коли програма несанкціоновано копіює інформацію з різних носіїв даних. Для уникнення цього важливо встановлювати обмеження на доступ до зовнішніх пристроїв, а також регулярно перевіряти та моніторити дії програм;
- блокування або відключення програмних засобів захисту. Якщо програмні засоби захисту можуть бути блоковані або відключені, це може послужити шляхом для несанкціонованого доступу та зловживань. Ефективний захист включає в себе вдосконалення системи виявлення і запобігання вторгнень, а також забезпечення недоступності цих засобів для несанкціонованих користувачів.

Канали витоку інформації можуть виникнути під час використання особистих комп’ютерів або персональних електронно-обчислювальних машин, і розглядаючи ці пристрої можна прийти до висновку, що вони можуть слугувати ідеальним об’єктом для вивчення різноманітних каналів витоку інформації - від бездротових радіоканалів до матеріально-речових аспектів.

Розглядаючи їхню важливість в інформаційному захисті, загалом у суспільстві, а також широке використання для обробки обмежено доступної інформації, стає зрозумілим, що розгляд принципів формування каналів витоку інформації при експлуатації ПК та ПЕОМ є особливо важливим та актуальним. Варто зазначити, що сучасні ПЕОМ можуть функціонувати як самостійно, так і взаємодіючі з іншими машинами через комп’ютерні мережі, які можуть бути як локальними, так і глобальними.

Описуючи можливий витік інформації каналами ПЕМВН, зазначимо, що під час операцій в обчислювальній техніці, в її конструктивних елементах та кабельних з'єднаннях відбувається потік електричних струмів інформаційних сигналів. Цей процес породжує електромагнітні поля, чиї рівні можуть бути достатніми для перехоплення сигналів і витягування інформації, використовуючи спеціалізоване обладнання.

Канали витоку інформації можуть виникати через випромінювання інформативних сигналів під час функціонування обладнання та внаслідок наведення цих сигналів у лініях зв'язку, електромережах і заземленні, а також інших комунікаційних шляхах, які виходять за межі контрольованої зони. Інформаційні сигнали можуть подолати великі відстані і бути зафіксовані технічними засобами розвідки за межами контрольованої зони.

Діапазон частот, на яких можуть виникати (наводитися) інформаційні сигнали, визначається типами та характеристиками обладнання і може охоплювати значення від сотень герц до кількох десятків гігагерц.

Ступінь впливу наводок визначається віддаленістю між джерелами випромінювання та обладнанням, яке відчуває ці випромінювання. Цей вплив враховує довжину паралельного пробігу, міру перехідного затухання ліній, напругу інформаційного сигналу в лінії, а також рівень шумів або завад.

Можливість виникнення витоку інформації через систему заземлення існує, якщо наявні рознесені точки заземлення інформаційних кіл та якщо утворюється різниця потенціалів у різних точках, що призводить до виникнення струмів у заземленні. Така ж сама ситуація може виникнути при великому опорі в системі заземлення або через недосконалість екранів, що спричинює асиметрію ліній відносно екрана і призводить до виникнення інформативних струмів між корпусом екрана та землею.

При проведенні технічного контролю ПЕОМ, важливо узгоджувати вплив на потенційні канали витоку інформації. Далі наведемо приклади найважливіших аспектів, які потребують спеціальної уваги.

Технічний контроль має охоплювати вимірювання побічних електромагнітних випромінювань в діапазоні частот від 10 герц до 100 мегагерц. Це може включати аналіз випромінювань від різних компонентів ПЕОМ, таких як процесори, пам'ять та інші елементи, що можуть стати джерелами непередбачених витоків інформації.

Важливим етапом технічного контролю є вивчення можливостей наведення сигналів в ланцюгах електроживлення, заземлення та лініях зв'язку. Дослідження інтерференцій та наведень може розкрити можливі канали витоку інформації через систему електроживлення.

Технічний контроль повинен включати перевірку наявності небезпечних сигналів, що виникають через електроакустичні перетворення. Додаткова увага повинна бути приділена контролю цих сигналів у діапазоні частот від 300 герц до 3,4 кілогерц.

Проведення перевірки на канали витоку інформації, що виникають внаслідок впливу високочастотних електромагнітних полів на дроти в приміщенні, є критичним. Особливу увагу слід зосереджувати на перевірці в діапазоні частот від 20 кілогерц до 100 мегагерц.

Загальна мета технічного контролю полягає в ідентифікації та ліквідації всіх потенційних каналів витоку інформації, забезпечуючи тим самим найвищий рівень безпеки оброблюваної інформації в персональних електронно-обчислювальних машинах.

Важливо розуміти, що дисплей є найнебезпечнішим каналом витоку інформації, оскільки його схеми визначають сигнали, які представляють інформацію, що відображається на екрані комп'ютера. Цей процес здійснюється за допомогою відеобуфера, який є своєрідною областю оперативної пам'яті, призначеною для зберігання текстової або графічної інформації, що виводиться на екран. Основна функція відеосистеми полягає в перетворенні даних з відеобуфера в сигнали, які керують роботою екрану, формуючи зображення для користувача.

1.3. Засоби протидії загрозам

Автоматизована система представляє собою комплексну організаційно-технічну структуру, що об'єднує в собі обчислювальну систему, фізичне середовище, персонал та оброблювану інформацію. У сфері технічного захисту інформації в автоматизованій системі зазвичай виокремлюють два основних напрями: захист самої системи та оброблюваної інформації від несанкціонованого доступу, а також захист інформації від витоку через технічні канали, такі як оптичні, акустичні, захист від витоку каналами побічних електромагнітних випромінювань та наведень. [1]

Комплексна система захисту інформації охоплює взаємодію різноманітних заходів, наприклад, інженерних, а також технічних засобів, спрямованих на забезпечення найвищого рівня захищеності інформації. Захищеність інформації визначається наступними ключовими властивостями:

1. Доступність:
    - доступність інформації забезпечується наявністю відповідних повноважень у користувача;
    - користувач може використовувати конкретний ресурс відповідно до правил користування та політики безпеки;
    - забезпечення доступності передбачає належну реалізацію усіх авторизаційних процедур та контроль доступу.
2. Конфіденційність:
    - конфіденційність інформації означає, що вона є приватною та секретною, а отже, не повинна розголошуватися без належних повноважень;
    - заходи з шифрування, обмеження прав доступу та інші технічні засоби сприяють збереженню конфіденційності.
3. Цілісність:
    - цілісність інформації гарантує, що користувач без належних повноважень не може внести зміни у дані;

- заборона модифікації інформації здійснюється за допомогою механізмів контролю цілісності та відстеження будь-яких спроб неправомірної модифікації.

4. Спостережність:
   - спостережність дозволяє системі відстежувати та фіксувати всі дії, які здійснюються користувачами та процесами в рамках системи, це важливо для створення докладного журналу подій, який може бути використаний для аналізу та виявлення потенційних загроз безпеці;
   - система спостережності визначає ідентифікатори осіб, які мають доступ до конкретних подій та ресурсів, та ідентифікує процеси, що взаємодіють з системою, це сприяє точному визначенню, хто і що виконує, що є важливим для контролю і управління системою безпеки.

Ці властивості визначають надійний фундамент для створення комплексної системи захисту інформації, спрямованої на забезпечення високого рівня безпеки, дотримання стандартів конфіденційності та запобігання неправомірним змінам у дані.

Організаційний захист інформації є важливим комплексом заходів, спрямованих на оперативне вирішення завдань щодо забезпечення безпеки інформації. Цей комплекс включає в себе ряд адміністративних та обмежувальних заходів, які націлені на регламентацію діяльності персоналу та встановлення порядку функціонування засобів забезпечення інформаційної діяльності та засобів забезпечення технічного захисту інформації (ТЗІ). Організаційні заходи охоплюють створення концепції інформаційної безпеки, розробку посадових інструкцій для персоналу, встановлення правил адміністрування компонентів інформаційної системи, а також розробку планів дій у разі надзвичайних ситуацій та навчання користувачів правилам інформаційної безпеки.

Криптографічний захист інформації представляє собою ефективний метод захисту, який використовує перетворення інформації за допомогою спеціальних даних, таких як ключі. Ці перетворення призначені для шифрування або

дешифрування інформації, підтвердження її справжності, забезпечення цілісності, авторства та запобігання несанкціонованій модифікації чи розголошенню.

Інженерний захист інформації, визначений як запобігання пошкодженню носіїв інформації внаслідок навмисних або природних впливів за допомогою інженерно-технічних засобів, включає в себе заходи, такі як використання обмежуючих конструкцій та систем охоронно-пожежної сигналізації.

Технічний захист інформації, який має на меті захист від несанкціонованого доступу та витоку інформації технічними каналами, включає створення комплексу технічного захисту, який входить до складу Комплексної Системи Захисту Інформації (КСЗІ).

Несанкціонований доступ (НСД) визначається як можливість отримання доступу до інформації з використанням ресурсів, які входять до складу комплексної системи (КС) і порушують встановлені правила розмежування доступу. Несанкціонований доступ може здійснюватися якщо зловмисник використовує штатні засоби, які включають в себе програмно-апаратне забезпечення, розроблене тоді, коли створювалася комплексна система або коли системний адміністратор впровадив таке програмно-апаратне забезпечення вже під час використання КС та входить у схвалену конфігурацію комплексної системи, а також у випадку коли зловмисник використовує програмно-апаратні засоби, які були включені до складу комплексної системи ним самим.

Основні методи НСД включають:

- звертання до складових для отримання конкретного виду доступу;
- розробка засобів, що обходять існуючі ТЗЗ і забезпечують доступ до об'єктів;
- внесення змін до існуючих засобів захисту для здійснення несанкціонованого доступу;
- зловмисник додає програмні або апаратні механізми, які можуть порушити функції та структуру комплексної системи і забезпечити отримання несанкціонованого доступу.

Під захистом від несанкціонованого доступу розуміється комплекс заходів, спрямованих на дотримання правил захисту даних. Це включає в себе розробку та підтримку системи захисту інформації, що забезпечує виконання встановлених ПРД.

З методологічного погляду, у контексті захисту від НСД, важливо розглядати наступні основні напрямки:

1. Забезпечення та оцінювання захищеності даних у діючих АС:
   - оцінити та забезпечити інформаційну захищеність в реально діючих автоматизованих системах;
   - необхідно реалізувати та оцінити ефективність захисту, який розглядається як склад компонентів, що реалізує обчислювальну систему за рамками експлуатаційного середовища, прикладом можуть слугувати програми та техніка.
2. Заходи для захисту даних мають наступну загальну мету:
   - забезпечити безпеку даних, коли вони оброблюються в автоматизованій системі;
   - забезпечити безпеку даних на кожному з етапів життєвого циклу автоматизованої системи, а також на усіх етапах обробки інформації.

Життєвий цикл автоматизованої системи містить у собі етапи розробки, впровадження, використання та затвердження використання.

Коли в автоматизованій системі передбачається оброблення даних, правила захисту та обробки якої регламентуються певними документами чи актами, обов’язковим є наявність дозволу, який надав відповідний державний орган. Цей дозвіл надається на підставі висновку експертів, які перевіряють чи відповідають встановленим нормам реалізовані засоби захисту.

Автоматизована система включає в себе обчислювальну систему, яка є основною частиною автоматизованої системи, об'єднує апаратні та програмні засоби, що призначені для обробки інформації. Кожен з компонентів операційної системи може розглядатися як самостійний продукт, який може розроблятися та виводитися на ринок незалежно. Кожен компонент має імплементувати свої

функції захисту даних, та його ефективність оцінюється окремо від процесу експертизи автоматизованої системи, що є частиною сертифікації. Сертифікація засобів захисту видається на підставі відповідності критеріям та вимогам функцій захисту, які були імплементовані. Значне полегшення процесу експертизи може забезпечити сертифікат на саму автоматизовану систему чи на її компоненти.

Технічний захист даних від НСД представляє собою програмні, апаратні або програмно-апаратні компоненти. Він здатний забезпечувати самостійний захист або реалізувати навіть більш найдійний захист за допомогою засобів захисту інших типів, зменшуючи загрози для даних в комп'ютерних системах, а також включає в себе усю документацію.

Технічні канали, які потребують уваги в процесі захисту, включають побічні електромагнітні випромінювання, акустичні сигнали, оптичні засоби передачі та інші. Вони є потенційними шляхами для несанкціонованого збору інформації та потребують ефективних методів захисту.

Процес захисту від несанкціонованого доступу включає в себе різні аспекти інформаційної системи, такі як:

- Прикладні та системні програмні забезпечення, які розмежовують доступ, ідентифікують та автентифікують, проводять аудит та моніторинг, а також антивірусний захист.
- Апаратні частини робочих станцій і серверів , які використовують апаратні ключі, сигналізацію та блокують пристрої та інтерфейси вводу та виводу.
- Комунікаційне обладнання та канали зв'язку, де використовують предмети мережевого захисту даних, а саме мережеві екрани (такі засоби як firewall та брандмауер розташовуються на вході мережі з метою ефективного утримання атак, що можуть виникнути з зовнішнього середовища. Вони координують та контролюють потік мережевого трафіку відповідно до установлених правил захисту, а також забезпечують чітке розмежування внутрішніх (приватних) та зовнішніх (загальнодоступних) мереж з метою підвищення рівня безпеки системи),

системи виявлення утручань (за допомогою спеціальних механізмів, попереджують про шкідливі дії і, таким чином, після атаки сильно зменшують час простою. Загалом, використовуються для того, щоб виявити можливі спроби несанкціонованого доступу як у середині так і за межами мережі), засоби створення віртуальних приватних мереж (організовують захищені канали для того, щоб передавати дані через незахищене середовище. Прикладом є VPN, який зберігає інформацію при її передачі, динамічно шифруючи її) та засоби аналізу захищеності (забезпечують контроль поточного стану захисту мережі та, тим самим, упереджують атаки корпоративної мережі, які можуть статися у майбутньому).

Застосування цих заходів дозволяє створити комплексний технічний захист інформації, що є необхідним для забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів в сучасних інформаційних системах.

З метою уникнення витоку інформації технічними каналами зв'язку, впроваджується комплекс заходів захисту, який включає:

- використання екранованих кабелів та конструкцій для мінімізації електромагнітних випромінювань;
- встановлення високочастотних фільтрів на лініях зв'язку для контролю та обмеження передачі інформації за межі призначених меж;
- будівництво екранованих приміщень у формі "капсул" для ізоляції та захисту від зовнішніх електромагнітних впливів;
- використання екранованого обладнання для зменшення ризику несанкціонованого витоку інформації;
- встановлення активних систем зашумлення для контролю і нейтралізації небажаних електромагнітних сигналів;
- створення контрольованих зон з обмеженим доступом, де забезпечується найвищий рівень захисту.

Для забезпечення інформаційної безпеки в мережах важливо впровадження різноманітних заходів, що складають систему захисту інформації. Ці заходи та норми спрямовані на запобігання потенційним загрозам та мінімізацію можливих збитків для користувачів та власників системи.

Технічні заходи для запобігання витоку інформації включають такі заходи:

- захист від несанкціонованого доступу (НСД), включаючи використання технічних засобів;
- резервування важливих комп'ютерних підсистем для забезпечення неперервної працездатності;
- організація обчислювальних мереж з можливістю перерозподілу ресурсів у випадку відмови окремих ланок;
- встановлення пожежного устаткування для попередження та ліквідації пожежних загроз;
- встановлення систем сигналізації для вчасного виявлення та реагування на потенційні загрози.

Організаційні заходи для запобігання витоку інформації включають такі заходи:

- здійснення серверної охорони для забезпечення фізичного захисту обладнання;
- проведення важливих робіт та заходів за участю двох чи більше осіб для забезпечення контролю та уникнення недозволених дій;
- розробка плану відновлення сервера в разі його непрацездатності для швидкого відновлення роботи.

Під час профілактики або ремонту комп'ютера існує можливість несанкціонованого доступу (НСД) до залишкової інформації, яка може бути вилучена користувачем звичайним способом. Також ця ситуація може виникнути при транспортуванні носія без відповідного захисту. Використання сучасних комп'ютерних засобів може спричиняти зміни в рівнях напруги і струму на

інтегральних схемах, що в свою чергу породжує електромагнітні поля та наведення, які можуть бути перетворені в оброблювальну інформацію.

Несанкціонований доступ до інформації також може відбутися при прямому підключенні порушником засобів до мережевих апаратних засобів та каналів зв'язку. Для уникнення таких ситуацій використовуються методи ідентифікації, аутентифікації та використання паролів.

Для забезпечення безпеки інформаційних ресурсів, право на які належить певним особам або групам осіб, необхідно виключити можливість несанкціонованого доступу та посилити контроль за санкціонованим доступом до інформаційно-звітних об'єктів держави. Для цього застосовуються системи розпізнавання та розмежування доступу, базованих на принципі допуску та виконання звернення до інформації.

У таких системах, ідентифікація та аутентифікація виступають важливими елементами, де ідентифікація визначає унікальний ідентифікатор об'єкта, а аутентифікація перевіряє відповідність об'єкта тим, за кого він себе видає. У разі успішної перевірки об'єкт має доступ до інформації з певними обмеженнями або без них, в іншому випадку допуск буде відхилений.

Різноманітні об'єкти в сфері ідентифікації та аутентифікації включають:

- людина: один з найбільш основних об'єктів ідентифікації. Біометричні параметри, такі як відбиток пальця, відбиток руки, райдужна оболонка очей та тембр голосу, використовуються для перевірки особистості.
- технічний засіб: це може включати різноманітні технологічні пристрої, такі як смарт-карти, ключі, RFID-мітки, які служать для ідентифікації та аутентифікації користувачів у системі.
- документ: офіційні документи, такі як паспорти, ID-карти, водійські посвідчення, можуть використовуватися як засіб ідентифікації особи.
- магнітні носій інформації: карти з магнітною смугою, USB-накопичувачі та інші магнітні носії можуть використовуватися для зберігання та передавання інформації, що потребує аутентифікації.

Перевірку дійсності цих об'єктів можуть здійснювати різні суб'єкти, такі як людина, технічні пристрої та програмне забезпечення.

Поняття паролю визначається як унікальний набір символів, який використовується для ідентифікації об'єкта. Важливо дотримуватися вимог до його розміру, стійкості та включення різноманітних символів. Довжина паролю та його складові пропорційно визначаються рівнем технічного розвитку та швидкістю його злому, оскільки чим довший пароль – тим більше часу необхідно для того, щоб його підібрати, тому рекомендується періодично змінювати паролі з дотримуванням усіх правил щодо створення паролю (велика довжина, використання не тільки маленьких літер, а також і великих, а також використання цифр та спецсимволів) для забезпечення високого рівня безпеки.

Технічні системи ідентифікації також можуть використовувати біометричні параметри людини, які є індивідуальними для кожного (палець, долоні, очі, голос) для перевірки особистості користувача, забезпечуючи додатковий рівень безпеки, тим самим створюючи двохфакторну аутентифікацію, яка є досить популярним способом забезпечення безпеки даних користувача майже у кожному сервісі, але у цих випадках двохфакторна аутентифікація утворюється за допомогою більш простої комбінації, наприклад, паролю та коду, який повинен прийти на номер телефону або електрону пошту, що були вказані при реєстрації, після подолання першого етапу аутентифікації, а саме правильного введення пароля. Також, в якості захисту від зламу пароля методом перебору можна запровадити бан на повторне введення, якщо пароль було введено невірно, наприклад, 5 разів, і з кожним подальшим неправильним введенням, робити час бану все більше та більше, однак, при цьому необхідно запровадити більш захищений спосіб доступу, не зважаючи на бан від неправильно введеного паролю, для того, щоб забезпечити доступ для справжнього власника до даних або комп’ютера не зважаючи на втрату пароля.

В якості більш простих фізичних засобів ідентифікації можуть виступати перепустки, пластикові картки з фото та особистими даними власника, картки з магнітною смужкою та інші.

Засоби захисту інформації поділяються на програмні, програмно-апаратні та апаратні.

Програмні засоби, що впроваджуються у операційні системи, забезпечують безпеку обчислювальних систем та захист від НСД за допомогою паролів, але можуть мати обмежену ефективність у глобальних мережах через збільшений шанс злому, хоча для локальної мережі захист такого типу підходить, зважаючи на його переваги, до яких відносяться відносно високий ступінь захисту і середня ціна.

Програмно-апаратні засоби, засновані на мікропроцесорах, володіють гнучкістю та можливістю зміни конфігурації, але вартість їх розробки та впровадження можуть бути вищою. Серед переваг варто відмітити властивість адаптації у більшості операційних систем і рівень захисту локальних мереж що підключені до глобальних, який є високим, а також завдяки мікропроцесорній архітектурі, при необхідності у зміні алгоритму функціонування, модифікація схемотехніки не є потребою.

Апаратні засоби, що використовують великі інтегральні схеми, мають статичний алгоритм функціонування та високий рівень захисту, але можуть бути менш гнучкими у зміні конфігурації. Як і у попереднього типу засобів, зберігається властивість адаптації у більшості операційних систем. Зрозуміло, що вартість розробки та впровадження є найбільш високою, відповідно до рівня захисту, який також є найбільш високим завдяки відсутності можливості внесення змін.

Криптографічні засоби захисту інформації, використовуючи алгоритми шифрування та унікальні шифровальні ключі, гарантують конфіденційність та автентичність даних. Застосування криптографії забезпечує безпеку обміну зашифрованою інформацією через захищені або незахищені канали зв'язку. Такі засоби важливі для забезпечення захисту інформації в сучасному технологічному середовищі.

У сучасному світі активно розробляються універсальні телекомунікаційні системи, базою яких є єдині алгоритмічні стандарти. Це призводить до загального

інтересу щодо досліджень, метою яких є адаптація алгоритмів до різноманітних програмних та апаратних платформ. Одним і тим же алгоритмом повинно бути можливо користуватися на різних програмних та апаратних платформах, таких як смартфони, смарт-карти, настільні комп'ютери та маршрутизатори.

Засоби захисту даних в телекомунікаційних мережах класифікуються на асиметричні та симетричні криптоалгоритми. У початковий момент передачі даних, їх стан можна описати як відкритий і незахищений. Протягом передачі даних, вони шифруються, тим самим перетворючи їх у шифрограму. В цьому вигляді інформацію можна передавати через як захищені, так і незахищені канали зв'язку. Після того, як сталося отримання інформації адресатом, проводиться процедура дешифрування за допомогою зворотнього перетворення криптограми. В результаті отримуємо, доступну для санкціонованого користувача, відкриту інформацію.

В області криптографічного перетворення використовуються унікальні алгоритми, і їх активація виконується за допомогою спеціального числа, відомого як шифрувальний ключ. Для того, щоб здійснити успішний обмін зашифрованими даними, важлива наявність правильної установки ключа відправником та одержувачем, при цьому ключ повинен зберігатися у таємниці.

Стійкість визначається рівнем секретності ключа, який використовується системою із закритим зв’язком. Поширюваність ключа не повинна бути обмеженою кількістю інших користувачів мережі, оскільки ці користувачі мають володіти можливістю вільно обмінюватися інформацією, яка є зашифрованою. Отже, використання криптографічних систем дозволяє вирішувати проблему автентифікації прийнятих даних. У випадку перехоплення даних, які вже відправлені, зловмисник зможе заволодіти тільки зашифрованим текстом, і лише справжній адресат, використовуючи правильний ключ, зможе виконати розшифрування та отримати доступ до відкритої інформації, уникнувши дезінформації.

Також існує більш простий метод шифрування даних, який використовує генерацію псевдовипадкових чисел. Цей метод полягає в створенні шифрованого

потоку (гами) за допомогою конкретного ключа, а потім застосування цього шифрованого потоку до відкритої інформації в оберненому порядку. Цей метод має перевагу легкої реалізації та швидкого шифрування, але йому притаманний недолік - обмежена стійкість до дешифрування.

Класична криптографія оперує одиничною секретною одиницею, відомою як ключ, яка використовується для зашифрування інформації перед відправкою, і отримувач використовує цей ключ для розшифрування отриманої інформації. У випадку, коли дані зберігаються на магнітних або інших носіях, ключ може використовуватися для шифрування інформації під час запису на носій і розшифрування при подальшому читанні.

Можна зробити висновок, що надійна криптографічна система повинна враховувати наступні аспекти:

- користувачам повинно бути легко використовувати систему шифрування і розшифрування, забезпечуючи зручність і зрозумілість процесу.
- криптографічна система повинна надійно захищати ключі та процес дешифрування від несанкціонованого доступу, забезпечуючи високий рівень безпеки.
- криптографічний алгоритм повинен забезпечувати конфіденційність, не дозволяючи визначити зміст переданих даних навіть при вивченні ефективності самого алгоритму.

Асиметричні системи, також відомі як системи з відкритим ключем, сьогодні є перспективним напрямком розвитку в галузі криптографії. Основним принципом цих систем є використання ключів, які відрізняються для шифрування та розшифрування інформації. Відкритий ключ може бути відомий для всіх користувачів системи, в той час як секретний ключ залишається конфіденційним. У таких системах важливою особливістю є те, що розшифрування виконується секретним ключем, який не може бути визначений на підставі відомого відкритого ключа. Це забезпечує високий рівень безпеки для передаваної інформації. Асиметричні системи широко використовуються для шифрування передаваної інформації, забезпечуючи захист від несанкціонованого доступу.

Однак їх ефективність у захисті інформації, яка зберігається на носіях, може бути меншою порівняно із застосуванням інших методів криптографії.

Криптографія відіграє важливу роль в забезпеченні безпеки даних в Інтернеті, і на сьогоднішній день необхідні криптографічні механізми активно впроваджуються в цю глобальну мережу. Широке використання криптографії і глобальних інформаційних мереж є досягненням сучасного світу, оскільки воно забезпечує конфіденційність, цілісність та доступність даних в онлайн-середовищі. За допомогою криптографічних методів, таких як шифрування та підписи, забезпечується захист інформації від несанкціонованого доступу та змін. Активне впровадження криптографічних засобів в Інтернет дозволяє користувачам здійснювати безпечні та конфіденційні транзакції, обмін даними та комунікації в цифровому середовищі. Це важливий елемент для забезпечення довіри між користувачами та сервісами в Інтернеті, а також сприяє збереженню конфіденційності особистої інформації та захисту від різноманітних кіберзагроз. Такий підхід дозволяє ефективно використовувати потужності глобальної мережі, не втрачаючи при цьому безпеку та приватність користувачів.

До інженерного захисту інформації відноситься забезпечення стійкості будівлі до впливу різних небезпечних чинників, таких як землетруси, пожежі, затоплення та інші чинники, що можуть пошкодити або знищити інформацію з обмеженим доступом.

Від землетрусів зможе захистити лише правильна будівельна конструкція приміщення, яка може бути спроектована таким чином, щоб витримувати землетруси. Незважаючи на нещодавні випадки землетрусів на території України та біля неї, все ж таки, у рамках нашої держави не прийнято виконувати захист такого типу, через, як правило, дуже рідкі та поодинокі випадки, на відміну, наприклад, Японії, де землетруси це норма, тож переважна більшість новітніх будівель оснащують захистом такого типу. Незважаючи на це, розглянемо існуючі інженерні рішення для захисту від такого типу загрози.

Загалом, забезпечення захисту приміщення від землетрусів вимагає комплексного підходу та застосування різноманітних інженерних рішень. Ось деякі із можливих заходів та технологій:

- використання амортизаторів та демпферів може допомогти поглибити ефекти землетрусу. Ці системи абсорбують та розподіляють енергію, зменшуючи вплив на будівлі;
- удосконалення стійкості ґрунту під будівлею за допомогою ґрунтових підкріплень або геотекстилю може зменшити вібрації та ризик ушкоджень;
- застосування жорстких конструкцій із високоміцних матеріалів може покращити відповідь будівлі на землетрус;
- використання активних систем контролю вібрацій, таких як контролюючі гідроциліндри або маси, які можуть зміщатися, дозволяє активно реагувати на коливання будівлі;
- встановлення сейсмічних ізоляторів між фундаментом та будівлею дозволяє будівлі рухатися незалежно від ґрунту, зменшуючи трансмісію землетрусних хвиль;
- використання гнучких матеріалів або технологій може дозволити будівлі гнутися та деформуватися під час землетрусу, зменшуючи ризик ушкоджень;
- встановлення гідравлічних амортизаторів може допомогти поглибити ефекти землетрусу та захистити будівлі.

Це лише деякі із можливих інженерних рішень. Ефективність заходів залежить від конкретних умов будівництва, геологічних особливостей регіону та інших факторів. Рекомендується провести комплексний аналіз та консультації з інженерами, спеціалізованими на питаннях сейсмобезпеки, для визначення найбільш ефективних рішень для конкретного випадку.

Як вже раніше описувалося в роботі, для захисту від пожеж, окрім використання вогнеупорних матеріалів при будуванні захищеного приміщення,

таких як гіпсокартон, вогнестійка цегла, вогнестійкий бетон та вогнестійкі фарби, також використовують системи пожежогасіння з різними видами пожежогасної речовини, таких як рідка, пінна, аерозольна, газова і порошкова, розглянемо детальніше склад та принцип дії таких систем.

Спринклерні і дренчерні системи пожежогасіння відрізняються в першу чергу в пристроях кінцевих зрошувачів та обидві системи є ефективними засобами захисту від пожежі та використовуються для автоматичного виявлення та локалізації пожежі, а також для нейтралізації її на ранніх стадіях. Розглянемо основні риси кожної системи.

Спринклерне пожежогасіння:

1. Принцип дії: спринклерна система має ряд спринклерів, розташованих по всій площі захищеного приміщення. Кожен спринклер працює автономно та реагує на підвищення температури, що виникає при пожежі.
2. Активація: спринклер активується ізольовано, лише той, який опинився в області високої температури.
3. Види спринклерів: існують різні типи спринклерів для різних умов і застосувань, такі як швидкодіючі, повільнодіючі, спеціально призначені для високих приміщень тощо.
4. Водопостачання: зазвичай спринклери працюють від централізованої системи водопостачання або спеціального резервуара.

Дренчерне пожежогасіння:

1. Принцип дії: дренчерна система відрізняється тим, що вона призначена для локального обливання зони, яка виявляється при виникненні пожежі. Вода подається із мережі насосів чи іншого джерела водопостачання.
2. Активація: дренчерні головки можуть активуватися автоматично за допомогою термодатчиків або вручну, в залежності від типу системи.
3. Види дренчерів: є різні види дренчерів для різних умов, такі як звичайні, керовані, високотискані тощо.

4. Застосування: дренчерні системи часто використовуються в місцях з підвищеною небезпекою пожежі, таких як склади легкозаймистих матеріалів або виробництва, де може бути важко контролювати пожежу.

Обидві системи мають свої переваги і недоліки, і вибір між ними залежить від конкретних умов та вимог конкретного об'єкта.

Спринклерні і дренчерні системи є дуже ефективними засобами гасіння пожежі, і вони використовують воду або піна. Вода є одним з найбільш ефективних вогнегасників, а піна може використовуватися для пожеж різного класу, таких як горючі рідини. Вибір вогнегасного середовища визначається конкретними потребами та характеристиками об'єкта.

При встановленні необхідно розробити детальний проект системи, визначивши розташування спринклерів, трубопроводів, тиск води або іншої речовини. Важливо визначити які зони приміщення потребують покриття. Зазвичай один спринклер покриває певну площу, і це важливо врахувати при їхньому розташуванні. Розташування спринклерів може бути на стелях, але можуть також бути встановлені на стінах, в залежності від ефективності у кожній індивідуальній ситуації.

Газ для газового пожежогасіння подається через спеціальний пристрій, який називається газовим генератором. Газовий генератор є ключовим елементом в системі газового пожежогасіння і забезпечує подачу вогнегасного газу в пожежну зону. Зазвичай це робиться через трубопровід, який сполучає генератор із зонами, які підлягають захисту.

Також схожа ситуація з аерозольним типом, вони використовують дрібні частки твердої або рідкої речовини, розпилені в повітрі. Аерозольні системи також мають генератор аерозолю, який генерує та випускає аерозоль в зону пожежі.

Аналогічно і у випадку з порошковим типом, за винятком того, що порошок може бути вбудований безпосередньо в вогнегасник, утримуватися в ньому під тиском і вивільнятися при активації. Також, порошок може бути подаваний в вогнегасник із зовнішнього контейнера чи цистерни.

Для захисту від потопів інженерним шляхом, існують підходи піднятих підлог для створення додаткового простору, де можна розмістити дренажні труби або системи відведення води, включно з нахилом підлоги у бік дренажного отвору, також використання автоматичних систем відкачування води і ущільнення герметизуючими матеріалами стелі, підлоги та стін. Також використання систем раннього виявлення затоплень, систем автоматичного відключення електропостачання та водопостачання, особливо у парі з рідкими системами пожежогасіння.

Створення екранованих приміщень та встановлення екранованих шаф є засобами електромагнітного екранування, яке використовується для захисту від електромагнітних полів іншого обладнання чи для утримання та захисту конфіденційної інформації. Такі системи використовують спеціальні матеріали та конструкції для зниження або блокування електромагнітних сигналів. Перелічимо кілька способів, які використовуються для реалізації екранованих приміщень та шаф:

- екрановані матеріали:
    1. Феромагнітні матеріали, які здатні відводити електромагнітні поля, що допомагає у блокуванні електромагнітних хвиль.
    2. Провідники: використовуються металеві поверхні або металеві мережі для відбивання або поглиблення електромагнітних хвиль.
    3. Фольга: тонкі шари фольги вкладаються в матеріали для забезпечення екранування від електромагнітних перешкод.
- електромагнітна конструкція:
    1. Фарадейська клітка - це металева клітка або оболонка навколо приміщення чи шафи, яка може допомагати відбивати електромагнітні сигнали.
    2. Спеціальні екрановані матеріали та ущільнювачі, що вбудовані в двері та вікна для забезпечення екранування від електромагнітних полів.
- електромагнітні фільтри:

1. Фільтри використовуються для фільтрації електромагнітних сигналів (фільтри для живлення, комунікацій, аудіо і відео пристроїв тощо).

Ці методи можуть використовуватися окремо чи в комбінації для забезпечення максимального ефекту екранування.

2. ЕТАПИ СТВОРЕННЯ ЗАХИЩЕНОГО ПРИМІЩЕННЯ

2.1. Формування загальних вимог

Стандартний документ "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" (НД ТЗІ 3.7-003-2005) вказує на те, що процес розробки комплексної системи захисту інформації включає координацію різноманітних заходів, спрямованих на створення та впровадження інформаційної технології. Ця технологія призначена для обробки інформації в інформаційно-телекомунікаційній системі відповідно до вимог, встановлених законодавчими та нормативними актами у сфері захисту інформації. Для кожної конкретної інформаційно-телекомунікаційної системи властивості оброблюваної інформації, клас автоматизованої системи та умови експлуатації визначають склад, структуру та вимоги до захисту інформації [7].

Вимоги та норми визначені законом можуть слугувати причиною для того, щоб визначити чи є необхідність створити КСЗІ, також вони дають чітке визначення чи необхідно обмежувати доступ до конкретної інформації, а також чи необхідно забезпечувати її цілісність. Також ця необхідність може виникати на підставі прийнятого рішення, коли таке рішення було прийнято людиною, котрій належить інформація але тільки у випадках, коли нормативно-правова база надає їй таку можливість.

Обґрунтування потреби у створенні КСЗІ у вигляді вихідних даних в загальному випадку отримуються якщо:

- аналізувати нормативно-правову базу, яка регулює можливість обмежити доступ певних даних чи навпаки, встановити заборону на таке обмеження, або визначати чи необхідно забезпечувати захист даних, відповідно до інших критеріїв;
- визначити чи наявні у даних, які повинні оброблятися, такі види, для яких необхідно обмежити доступ або забезпечити доступність та цілісність відповідно до нормативно-правової бази;

- виконати оцінювання наявних переваг, при використанні ІТС, якщо було створено КСЗІ.

На основі результатів аналізу та оцінок можна зробити висновок щодо доцільності розробки комплексної системи захисту інформації.

Категорізація проводиться для об'єктів, де циркулює інформація з обмеженим доступом, таких як автоматизовані системи, технічні засоби, а також приміщення з розміщеними автоматизованими системами та іншими технічними засобами для обробки інформації. Категорізація проводиться з метою застосування обґрунтованих заходів з технічного захисту інформації, яка циркулює на об'єктах, враховуючи можливі канали витоку та заходи забезпечення безпеки.

Коли виконуються роботи по рішенню зазначених вище завдань, ІТС прийнято розглядати у вигляді комплексної організаційно-технічної системи, що складається з обчислювальної системи, фізичного середовища, середовища користувачів, даних які підлягають обробці та з самої технології обробки цих даних.

Проведення обстеження має свою мету – збір загальних даних для розробки вимог щодо КСЗІ. Наприклад, створити опис кожного середовища діяльності ІТС та виявити елементи, що можуть мати вплив на безпеку даних, безпосереднім або опосередкованим видом. Також важливо виявити який взаємний вплив мають елементи різноманітних середовищ та задокументувати результати обстеження для того, щоб у подальшому, а саме на наступних етапах робіт, використовувати їх.

Коли обстежується обчислювальна система ІТС важливо проаналізувати та детально описати:

- загальну структурну схему та з чого вона складається, наприклад технічні та програмні засоби, зв’язок між ними, їх особливості;
- канали зв’язку які використовуються у системі, у тому числі характеристика та вид кожного з них;

- окремі компоненти та яка наявна особливість їхньої взаємної дії та впливу, який вони мають між собою;
- обмеження які можуть виникнути при використанні засобів.

Коли обстежується інформаційне середовище, важливо проаналізувати та детально описати оброблювальну та збережену в ІТС інформацію, а коли проводиться аналіз, дані повинні бути класифіковані згідно режимів доступу та правових режимів.

Коли обстежується фізичне середовище в ІТС розглядається взаємне розміщення засобів обробки інформації, систем зв'язку та інфраструктури. Обстеження відповідає вимогам ДСТУ 3396.1 та НД ТЗІ 3.1-001 з питань захисту інформації. Аналізу підлягають такі характеристики фізичного середовища, як розташування компонентів, наявність охорони, режим доступу, вплив навколишнього середовища, елементи комунікацій та інфраструктури, системи заземлення, умови зберігання носіїв інформації та документація.

Коли обстежується середовище користувачів вивчається їхній функціональний склад, обов'язки, кваліфікація, повноваження стосовно доступу та управління КСЗІ, а також рівень доступу до ІТС та інших компонентів, і наявність систем захисту інформації.

На етапі формування завдання на створення КСЗІ визначаються мета створення, завдання захисту інформації в ІТС, варіанти рішення задач захисту, основні напрями захисту, проводиться аналіз ризиків та визначається перелік суттєвих загроз. Також визначаються загальна структура та склад КСЗІ, вимоги до заходів, методів та засобів захисту, обмеження щодо їх застосування, умови функціонування, введення в дію та витрати на створення КСЗІ.

2.2. Розробка політики безпеки

На етапі вивчення об’єкта для створення КСЗІ розробники проводять ретельне дослідження об’єкта, визначають модель загроз, потенційні порушення та результати аналізу можливостей управління ризиками. Також вони здійснюють додаткові дослідження, спрямовані на пошук шляхів реалізації завдання на

створення КСЗІ, і розробляють проект та звітність з науково-дослідницької роботи.

Оформлення політики безпеки на поточному етапі включає в себе визначення стратегічних рішень для протидії основним загрозам. Здійснюється формулювання загальних вимог, правил, обмежень та рекомендацій для того, щоб використовувати захищені технології оброблення даних в рамках ІТС. Документи політики інформаційної безпеки створюються на цьому етапі, а також можуть бути розроблені для всієї ІТС або для окремих компонентів КСЗІ, відповідаючи вимогам нормативних документів. У план захисту рекомендується включити стратегію безпеки як окремий документ.

Політика безпеки та її положення пов'язані з подальшими проектними рішеннями, організаційними аспектами, визначенням відповідальності, процедурами експлуатації та впровадження КСЗІ. Це взаємодія, яка включається в документ для подальшого прийняття рішень на відповідному етапі робіт. У виняткових випадках ця робота може бути включена до технічного завдання на створення КСЗІ, з виконанням відповідно до визначених етапів у ТЗ.

2.3. Розробка технічного завдання

Технічне завдання на створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі – це є ключовий організаційно-технічний документ, що встановлює вимоги до захисту даних, які оброблюються, до процедури розробки КСЗІ, випробувань та введення системи в експлуатацію.

Для створення комплексної системи захисту інформації використовується технічне завдання, яке має бути розроблено на відповідному етапі створення інформаційно-телекомунікаційної системи. Це завдання враховує комплексний підхід до побудови комплексної системи захисту інформації, охоплюючи всі необхідні заходи та засоби для того, щоб запобігти різного роду загрозам безпеці даних на кожному з етапів життєвого циклу інформаційно-телекомунікаційної системи. Технічне завдання для того щоб створити комплексну систему захисту

інформації може використовуватися як для вперше створених інформаційно-телекомунікаційних систем, так і під час покращення існуючих систем.

Для складання технічного завдання до комплексної системи захисту інформації можна використовувати різні підходи:

- включити його як окремий розділ до тех. завдання на створення інформаційно-телекомунікаційної системи;
- створити його як окремий (частковий) документ тех. завдання;
- включити його як додаток до тех. завдання на створення інформаційно-телекомунікаційної системи.

Не існує обмежень щодо вибору конкретного варіанту.

У разі, якщо інформаційно-телекомунікаційна система створюється вперше, рекомендується обрати перший варіант. Для випадків модернізації комплексної системи захисту інформації, а також модернізації існуючих ІТС або тих, які вже мають затверджене технічне завдання на створення, рекомендується використовувати другий або третій варіант, які не включають окремий блок із заходами з захисту інформації.

Для інтегрованих інформаційно-телекомунікаційних систем, що базуються на принципах модульності, рекомендується визначити вимоги до комплексної системи захисту інформації для кожного окремого компонента ІТС у відповідному документі. Можливо використовувати один документ для кількох аналогічних компонентів КСЗІ, зазначаючи відмінності або особливості, за умови, що цей документ не є частиною технічного завдання, що використовується для створення ІТС.

Однотипними компонентами можна вважати комплексні системи захисту інформації інформаційно-телекомунікаційних систем, якщо вони забезпечують операції комутації в мережах обміну даними або мають однакові функціональні завдання в локальних мережах інтегрованої ІТС. Умови їх роботи повинні бути ідентичними або подібними. При цьому технічне завдання включає вимоги до окремих компонентів ІТС і ІТС в цілому, а також вимоги до забезпечення безпечної взаємодії цих компонентів.

Єдиним критерієм обмеження для розробки окремого технічного завдання на створення комплексної системи захисту інформації є збереження єдиної системи концепцій, імен, ідентифікаційних об'єктів і т.д., які використовуються в ТЗ на створення інформаційно-телекомунікаційних систем.

Для будь-якого з узгоджених варіантів розробки та проектування технічного завдання на комплексну систему захисту інформації його зміст, процедура погодження та затвердження повинні відповідати вимогам НД ТЗІ 3.7-001.

2.4. Розробка проєкту

Проєкт комплексної системи захисту інформації ґрунтується на технічному завданні на створення інформаційно-телекомунікаційної системи. В той час, коли розробляється проєкт комплексної системи захисту інформації повинні бути сформульовані та узгоджені проєктні рішення щодо виконання вимог тех. завдання, а також для забезпечення взаємодії і сумісності різноманітних компонентів комплексної системи захисту інформації, так само як і різноманітних методів та заходів захисту інформації. Проєкт КСЗІ повинен бути реалізований на наступних етапах створення інформаційно-телекомунікаційної системи: технічний проєкт, робочий проєкт та ескізний проєкт.

Можливо вилучити етап ескізного проєкту КСЗІ та виконати об'єднання технічного проєкту КСЗІ з робочим проєктом КСЗІ в єдиний етап у вигляді техно-робочого проєкту КСЗІ. Структура документації для кожного з етапів розробки проєкту КСЗІ визначається згідно з технічним завданням, а зміст і види – згідно з вимогами НД ТЗІ 2.5-004. Документація для програмних засобів розробляється відповідно до набору стандартів ЄСПД, а для обладнання, а саме технічних засобів – відповідно до набору стандартів ЄСКД.

Етап створення ескізного проєкту КСЗІ передбачає розробку попередніх проєктних рішень комплексної системи захисту інформації, включаючи окремі складові частини, а також розробку і затвердження документації. Визначаються наступні елементи:

- функції як комплексної системи захисту інформації, так і її компонентів;

- з чого складаються комплекси захисту від запобігання витоків тех. каналами та спеціальних впливів;
- з чого складаються заходи недопущення та протидії технічній розвідці, організаційним, правовим та іншим захисним заходам;
- склад комплексу засобів захисту;
- узагальнена структура комплексної системи захисту інформації, а також схема взаємодії її компонентів.

Здійснюється пропозиція щодо попередніх технічних рішень, які сприяють реалізації завдань та функцій КСЗІ.

Технічний проєкт передбачає в першу чергу розробку проєктних рішень для КСЗІ, що в свою чергу включає в себе створення загальних проєктних рішень, які необхідні для того, щоб втілити вимоги, які регулює технічне завдання, на комплексній системі захисту інформації. Цей етап має містити у собі структуру КСЗІ, яка б охоплювала як організаційну структуру, так і структуру засобів: програмних та технічних, повинні бути розроблені алгоритми функціонування і умови використання засобів захисту, а також архітектура та засоби і процеси реалізації архітектури комплексу засобів захисту, яка визначається за допомогою функціонального профіля послуг безпеки інформації.

Застосовуються організаційні та технічні заходи згідно з вимогами НД ТЗІ 2.5-004, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 для того щоб забезпечити послідовність розроблення КЗЗ, включно з архітектурою, середовищем розроблення, тестуванням, експлуатаційним середовищем та експлуатаційною документацією КЗЗ.

Щодо розробки документації в комплексній системі захисту інформації: створюється, оформлюється, узгоджується та затверджується необхідна кількість документів, визначених технічним завданням на КСЗІ. Зміст та стилізація цих документів мають забезпечити повний опис проєктних рішень на рівні технічного проєктування.

Розробляється та видається документація на постачання засобів захисту інформації та/або технічних вимог (технічних завдань) для їхньої розробки. Для

того щоб комплектувати КСЗІ здійснюються роботи щодо підготовки і оформлення документів для того щоб постачати захисне обладнання чи продукти, які входять до її складу. У випадку відсутності потрібного товару на ринку захисних засобів, мають бути визначені технічні вимоги або завдання для того щоб відповідні заходи були розроблені.

Задля розробки завдань на проєктування в суміжних частинах, здійснюється формулювання, оформлення та узгодження завдань на проектування, які стосуються суміжних аспектів та впливають на ефективність функціонування КСЗІ. Ці завдання обумовлені будівельними, електротехнічними, санітарно-технічними та іншими підготовчими аспектами.

На етапі розроблення робочого проєкту, проводиться формування, документування та узгодження робочих та експлуатаційних документів комплексної системи захисту інформації . У випадку потреби, також визначаються та затверджуються окремі складові частини КСЗІ.

Робоча документація складається з детальних рішень стосовно того, як реалізувати технічний проєкт КСЗІ Вона охоплює аспекти забезпечення управління комплексною системою захисту інформації, а також взаємодії її складових. Також у документації враховані вимоги для тестування, вимоги щодо того як будуть проведені пусконалагоджувальні роботи та випробування КСЗІ.

Здійснюється розроблення КЗЗ, який відповідає вищенаведеним вимогам. Також передбачається можливість адаптації готової продукції до вимог та умов функціонування комплексної системи захисту інформації. Процес розробки засобів захисту від несанкціонованого доступу проводиться відповідно до вимог НД ТЗІ 3.6-001 [16].

Склад робочої документації на КТЗІ від витоку тех. каналами включаються наступні складові, які мають бути виконані згідно вимогам НД (наприклад НД ТЗІ 3.3-001):

- схеми розміщення основних технічних засобів ІТС;
- схеми розміщення кабельного обладнання;
- схеми розміщення мереж живлення та систем заземлення [17].

Врахування умов розміщення обладнання та мінімально допустимих відстаней між цими засобами та допоміжними технічними засобами (зв'язок, кондиціонування, сигналізація, освітлення) у приміщенні з обладнанням ІТС та суміжних приміщеннях є також важливим. При розробці враховуються вищенаведені вимоги, які міститься у експлуатаційній документації.

Якщо відсутні сертифікати, які регулюють відповідність вимогам з ТЗІ для ОТЗ, які використовуються в якості компонентів КСЗІ, а також відсутності мінімально допустимих відстаней та інших умов розміщення цих засобів, необхідно провести спеціальні дослідження для визначення цих параметрів. Зазначені дослідження повинні враховувати експлуатаційні характеристики, ефективність та безпеку використання цих засобів в контексті конкретної системи КСЗІ. Результати спеціальних досліджень мають бути задокументовані та включені до робочої документації КСЗІ, забезпечуючи повну інформацію щодо умов їх розміщення, мінімально допустимих відстаней та інших факторів, що впливають на їх ефективність та безпеку в експлуатації.

У робочу документацію комплексу засобів захисту мають бути включені описи процедур для встановлення та ініціалізації комплексу, налагодження усіх механізмів обмеження доступу користувачів до інформації та апаратних ресурсів ІТС, а також контролю за їхніми діями. Документація також повинна включати процес формування та оновлення баз даних захисту та забезпечення контролю цілісності програмного забезпечення та баз даних захисту. У робочому проекті мають міститися початкові дані для їхнього внесення в базу даних захисту.

Документація з експлуатації містить у собі опис того, як функціонує комплексна система захисту інформації та надає інструкції для обслуговуючого персоналу та користувачів, а також визначає порядок супроводження комплексної системи захисту інформації протягом кожного з етапів життєвого циклу ІТС.

2.5. Введення приміщення в дію та оцінка захищеності інформації

Процес підготовки комплексної системи захисту інформації до введення в дію містить у собі виконання завдань щодо організаційної структури та створення

розпорядчих документів, які регламентують діяльність з забезпечення безпеки інформації в інформаційно-телекомунікаційній системі. Також проводиться утворення системи захисту інформації, в тому числі призначення відповідальних осіб за інформаційний захист, якщо це не було зроблено на попередніх етапах. Зазвичай завершується розробка та затвердження документів, які входять до Плану захисту, за винятком тих, для яких необхідні результати подальших етапів робіт. Ці процеси виконуються відповідно до вимог нормативного документа технічного захисту інформації 1.4-001.

Здійснюється навчання представників всіх категорій користувачів інформаційно-телекомунікаційної системи (технічного персоналу, звичайних користувачів і осіб, які мають повноваження управління засобами комплексної системи захисту інформації щодо основних положень, визначених в документах Плану захисту. Це навчання спрямоване на забезпечення їхнього відповідного розуміння правил політики безпеки інформації, експлуатації захисних засобів і т.д. Під час навчання проводиться перевірка їхньої здатності використовувати впроваджені технології захисту інформації, а також реєстрація результатів навчання.

Комплектування комплексної системи захисту інформації здійснюється шляхом забезпечення отримання продукції, такої як засоби захисту даних, обладнання, матеріали від постачальників та співвиконавців робіт. Має бути прийняте рішення відносно підготування до проведення оцінювання відповідності засобів захисту вимогам нормативних документів щодо технічного захисту інформації, які на момент проєктування комплексної системи захисту інформації не володіли відповідними сертифікатами або експертними висновками. Також вирішується питання про порядок проведення такого оцінювання під час державної експертизи комплексної системи захисту інформації.

На етапі виконання будівельно-монтажних робіт виконуються роботи у процесі переобладнання вже існуючих або під час будівництва нових приміщень, які призначені щоб розмістити в них технічні засоби та персонал, а також для зберігання матеріальних носіїв інформації.

Коли безпосередньо виконуються будівельно-монтажні роботи, необхідно дотримуватися вимог ТЗ.

Організація-власник ІТС або будівельно-монтажні фірми є виконавцями будівельних робіт відповідно до проектної документації на будівництво, яка має бути розроблена проектною організацією відповідно до нормативних документів ДБН А.2.2-2, ДБН 2.2-3.

Коли будівельні роботи завершуються, тоді повинна бути створена комісія з прийняття робіт, в яку входять представники організації-замовника будівельних робіт, проектної та будівельно-монтажної організацій. Комісія складає акт прийому робіт, який містить задовільну оцінку, якщо виконані роботи відповідають вимогам технічного захисту інформації.

На етапі пусконалагоджувальних робіт передбачено виконання кількох завдань з метою забезпечення ефективного функціонування комплексної системи захисту інформації. Перш за все, проводиться монтаж обладнання та атестація КСЗІ для запобігання витоку інформації технічними каналами. Також виконується встановлення та налагодження засобів захисту і випробування їх працездатності в автономному режимі та при комплексній взаємодії.

Монтаж обладнання, кабельного обладнання, мереж живлення та заземлення виконується згідно з конструкторською документацією робочого проєкту. У випадку, коли до складу КСЗІ включені основні технічні засоби, що не мають сертифікатів відповідності вимогам технічного захисту інформації, проводяться спеціальні дослідження для визначення мінімально допустимих відстаней між цими засобами та допоміжними технічними засобами.

Зазначені роботи виконуються відповідно до нормативних документів і вимог, визначених національними та галузевими стандартами в галузі технічного захисту інформації, такими як НД ТЗІ 2.7-007, НД ТЗІ 2.1-002 та інші. Ефективність застосованих заходів забезпечення безпеки підтверджується результатами інструментальної перевірки в ході випробувань комплексу технічного захисту інформації.

Додаткові заходи захисту, визначені під час монтажних робіт, впроваджуються згідно з вимогами проєктної, робочої та експлуатаційної документації. Атестація впровадженого комплексу технічного захисту інформації здійснюється для оцінки повноти та якості виконаних робіт.

Попередні випробування мають на меті перевірити функціональність КСЗІ і визначити можливість її введення в дослідну експлуатацію. Під час цих випробувань здійснюється оцінка рівня працездатності КСЗІ та її відповідність вимогам технічного завдання.

Передвипробування здійснюються відповідно до плану та методик, які складає розробник КСЗІ, а погоджує їх замовник інформаційно-телекомунікаційної системи. Програма і методики випробувань, а також протоколи випробувань розробляються та документуються відповідно до вимог РД 50-34.698.

Замовник інформаційно-телекомунікаційної системи відповідає за організацію передвипробувань, а їх проведення відбувається спільно розробником КСЗІ та замовником. Для цього замовник формує спеціальну комісію, призначаючи представника, який є її головою.

Результати передвипробувань оформляються у "Протоколі випробувань", в якому висловлюється висновок стосовно придатності КСЗІ до дослідної експлуатації. Також у протоколі наводиться перелік виявлених недоліків, необхідних заходів для їх усунення, і вказуються рекомендовані терміни виконання цих робіт.

Після виправлення можливих недоліків та виправлень у проектній, робочій та експлуатаційній документації, акт приймання комплексної системи захисту інформації оформляється для переходу до етапу дослідної експлуатації.

Наступним етапом є проведення дослідної експлуатації КСЗІ, під час цього виконуються такі завдання:

- тестуються процеси оброблення інформації, обіг машинних носіїв інформації, управління захисними засобами, розподіл доступу користувачів до ресурсів ІТС та моніторинг дій користувачів;

- працівники служби захисту інформації та користувачі ІТС отримують практичні навички використання технічних та програмно-апаратних засобів захисту інформації, дотримуються вимог організаційних та управлінських документів, що регулюють доступ до технічних засобів та інформаційних ресурсів;
- проводиться (при необхідності) вдосконалення програмного забезпечення, додаткове налаштування та конфігурування комплексу захисту інформації;
- здійснюється (за необхідності) виправлення робочої та експлуатаційної документації.

По завершенні робіт формується акт про завершення дослідної експлуатації, який включає в себе висновок щодо можливості (або неможливості) представлення КСЗІ на державну експертизу.

Етап державної експертизи КСЗІ є важливим етапом перевірки ІТС. Основною метою цього етапу – це визначити чи технічні вимоги та критерії захисту даних, які були визначені до КСЗІ, відповідають розробленій КСЗІ, а також визначити чи можливо ввести її в роботу в якості компонента ІТС. Положення про державну експертизу в галузі технічного захисту інформації регулює проведення державної експертизи КСЗІ в ІТС.

У випадку виявлення дефектів під час перевірки, їх усунення здійснюється до завершення етапу, і процедура усунення аналогічна тій, яка застосовується для передвипробувань. Якщо, з якої-небудь причини, недоліки не можуть бути виправлені під час перегляду, складається акт, в якому визначається перелік необхідних вдосконалень та рекомендації для їх виконання. Коли передбачені актом роботи завершені, має знову провестися ще одна експертиза.

У випадку інтегрованих ІТС, перевірка кожного компонента (модуля) КСЗІ може виконуватися окремо. Перевірка інтегрованої КСЗІ в ІТС включає в себе оцінку взаємодії вже протестованих модулів, таких як адміністрування, обмін даними, безпека, тощо. Документи з результатами робіт на різних етапах для КСЗІ в ІТС оформлюються, враховуючи відповідні документи для модулів КСЗІ. У

випадку, коли інтегрована КСЗІ має стандартні компоненти, створені для одного ТЗ, експертиза цих модулів КСЗІ включає два етапи: перший - це багатостороння перевірка обраного стандартного модуля, а другий - необхідність перевірити чи відповідають умови роботи кожного окремого об’єкта усіх компонентів КСЗІ цього типу.

Впровадження нових (оцінених) модулів в існуючу КСЗІ не вимагає повторної перевірки всієї системи. Оцінка здійснюється взаємодією нового модуля з компонентом КСЗІ, який вже перебуває в експлуатації. Це дозволяє почати перевірку КСЗІ паралельно з етапами проектування. Першочергово рекомендують застосування цієї процедури для складних архітектурних рішень та обсягів робіт КСЗІ. Експерти послідовно оцінюють технічні та організаційні рішення на всіх етапах роботи. Це дозволяє здійснити швидке усунення недоліків та забезпечити скорочення часу проведення експертизи, що може завершитися до етапу приймальних випробувань ІТС. Приймальні випробування ІТС виконуються при функціонуванні КСЗІ, використовуючи тестові дані, які не містять конфіденційної інформації.

2.6. Супроводження

Під час експлуатації комплексної системи захисту інформації, виконується організаційне забезпечення роботи всіх функцій та її роботи у цілому, а також управління захисними засобами відповідно до визначених у Плані захисту та експлуатаційних документах на модулі КСЗІ. Роботи включають в себе проведення гарантійного та післягарантійного технічного обслуговування засобів захисту даних.

3. ПОБУДОВА ЗАХИЩЕНОГО ПРИМІЩЕННЯ БАНКУ

3.1. Необхідність створення захищеного приміщення банку

Згідно з Постановою Національного банку «Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи», з метою встановлення вимог з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, Правління Національного банку України постановляє затвердити правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи [8].

Вимоги, визначені в цих Правилах, застосовуються до приміщень центрального апарату, структурних підрозділів і одиниць, територіальних управлінь, навчальних закладів Національного банку України, а також до банків України та їх відокремлених підрозділів. Ці вимоги стосуються приміщень, де проводиться обробка електронних банківських документів із відомостями, що містяться під грифом "Банківська таємниця", а також іншої електронної інформації, доступ до якої обмежений банком. Крім того, вони розповсюджуються на приміщення банків, які будуються, реконструюються або щодо яких проектна документація не була затверджена на момент набрання чинності цим Положенням [8].

Ми будемо розглядати розробку захищеного приміщення на прикладі серверного приміщення банку. Згідно з правилами, термін "серверне приміщення" вживається для опису приміщення, де знаходяться сервери прикладних програм, баз даних, файлові сервери та інші аналогічні системи. Це приміщення призначене для обробки та зберігання електронних банківських документів та баз даних.

3.2. Аудит інформаційної безпеки серверного приміщення банку

У рамках сучасної банківської діяльності серверне приміщення визначається як стратегічно важливий компонент, що забезпечує надійність,

швидкість та безпеку обробки фінансових операцій та зберігання інформації під грифом "Банківська таємниця".

Банківська таємниця є правовим інститутом, який регулюється Законом України "Про банки і банківську діяльність". Згідно з цим законом, банківська таємниця - це інформація, яка є конфіденційною та не підлягає розголошенню або використанню без згоди клієнта, включаючи відомості щодо:

фінансовий стан клієнта;

операції клієнта з банком;

дані клієнтів банку;

дані персоналу банку [9].

Банківська таємниця поширюється на всю інформацію, що є відомою працівникам банку при виконанні ними своїх службових обов'язків. Розглянемо інформацію, яка повинна підлягати захисту при обробці та зберіганні на серверах у серверному приміщені банку (Таблиця 3.1).

Таблиця 3.1

Інформація, яка повинна підлягати захисту при обробці та зберіганні на серверах у серверному приміщені банку

№	Назва інформації	Деталі	Конфіденційність
1	Дані клієнтів	До даних клієнтів відносяться: • особисті та фінансові дані клієнтів, включаючи інформацію про банківські операції та транзакції; • конфіденційна особиста інформація, така як адреса, телефонні номери та інші особисті дані.	Банківська таємниця
2	Програмні компоненти корпоративного банківського застосунку	Такий застосунок має широкий спектр функцій для забезпечення ефективного управління операціями реєстрації нових клієнтів, регулювання процесу видачі карток, оформлення кредитів та інших типів обслуговування клієнтів.	Банківська таємниця
3	Програмні компоненти клієнтських застосунків	Цей застосунок генерує запит до серверів банку для отримання інформації або виконання фінансових операцій. Його основні функції, які взаємодіють з сервером: виконання реєстрації та	Банківська таємниця

		авторизації, переказ коштів, оформлення кредитів, замовлення готівки у касах банку, зміна особистої інформації після документального підтвердження.	
4	Фінансові операції	На серверах обробляються такі фінансові операції, як переказ коштів між фізичними особами, надходження коштів із закордону (Swift або SEPA), оформлення кредиту, накопичення на вивід кешбеку, а також блокування будь-яких фінансових операцій, у випадку коли вони позначаються як підозрілі, наприклад, завеликий переказ коштів (може потребувати довідку про доходи), вивід коштів з крипто або фріланс платформ на особисту картку фізичної особи, а не, наприклад, на рахунок ФОП за допомогою якого банк та податкова контролюють факт сплати податків.	Банківська таємниця
5	Банківські документи	До банківських документів відносяться письмові розпорядження клієнта, організації чи відповідального працівника банку, які повинні містити інформацію, яка є достатньою для підтвердження законності здійснення банківської операції.	Банківська таємниця
6	Резервне копіювання (бекапи)	Це процес створення та зберігання дублікатів даних, які зберігаються на серверах. Головна мета – захист банку від втрати даних внаслідок непередбачуваних ситуацій, таких як технічні збої, атаки, природні катастрофи чи людські помилки.	Банківська таємниця

Існування виникнення ситуації, коли на дані може здійснюватися вплив, який може порушити фізичну цілісність, логічну структуру, здійснити несанкціоновані модифікацію, отримування, копіювання та поширення даних називається загрозою безпеці інформації. Тому розглянемо загрози та вразливості інформації для серверного приміщення банку (Таблиця 3.2).

Таблиця 3.2

Загрози та вразливості інформації у серверному приміщені

№	**Категорії загроз**	**Вразливості**	**Джерела виникнення загроз**
1	Вихід з ладу	Помилки в ОС та ПЗ	Персонал

	апаратури	Слабка надійність окремих вузлів апаратури	
		Нестабільне електропостачання	
		Відсутність своєчасної заміни компонентів сервера	
2	Порушення фізичної цілісності серверів	Пожежа та відмова або відсутність системи пожаротушення	Персонал, інженерний захист, технічний захист
		Відсутність інженерно-технічного захисту	
3	Порушення умов функціонування серверів	Ступінь температури чи вологості, яка не відповідає нормам внаслідок несправності системи вентиляції	Персонал
4	Помилки або навмисні дії обслуговуючого персоналу	Випадкові дії, що призводять до витоку інформації або послаблення захисту від витоку інформації через недостатню кваліфікацію системного адміністратора або обслуговуючого персоналу систем функціонування серверного приміщення (спеціалісти з електрики, пожежотушіння, вентиляції), або ж навмисні дії з власних спонукань чи внаслідок шантажу, підкупу сторонніми особами	Персонал
5	Витік інформації технічними каналами	Порушення правил проведення екранування	Персонал, сторонні особи, технічний захист, інженерний захист
		Витік каналами побічних електромагнітних випромінювань	
		Витік каналами побічних електромагнітних наведень	
6	НСД до даних внаслідок проникнення сторонніх осіб	Викрадання або знищення компонентів серверного приміщення, у тому числі носіїв інформації через недостатній захист приміщення	Сторонні особи, технічний захист, інженерний захист
7	НСД до даних внаслідок кібератак	Нестійкість алгоритмів перед впливом шкідливого ПЗ	Сторонні особи, технічний захист
		Помилки системного адміністратора	
		Вразливості у ОС або ПЗ	

Після розгляду категорій загроз та вразливостей, розглянемо рішення за допомогою яких можна запобігти та нейтралізувати вищеописані загрози.

Для запобігання появи помилок в операційній системі та програмному забезпеченні, відповідальній особі, а саме системному адміністратору, необхідно вчасно встановлювати оновлення операційної системи та програмного забезпечення, в яких розробники цих систем та програм виправляють помилки, які можуть призводити до збоїв та створювати прогалини у безпеці, а також використання перевіреного програмного забезпечення.

При слабкій надійності окремих вузлів апаратури, варто вводити постійний моніторинг цих вузлів, а також завжди мати у наявності запасні частини для швидкої заміни.

Нестабільне електропостачання може призвести до серйозних проблем, таких як втрата даних та перерви у роботі системи. Загалом банк повинен бути підключений до міської електромережі та мати два незалежних введення з різних підстанцій. Кожна лінія повинна забезпечувати передачу необхідної потужності. Інстальоване електрообладнання повинно бути оснащеним як автоматичним, так і ручним переключенням між лініями. Нестабільне електропостачання варто розподілити на два типи: тимчасове відключення на лінії (або на обох лініях) що при відсутності резервних джерел живлення повністю зупиняє роботи серверів та нестабільне електропостачання, яке супроводжується коливанням напруги.

Для того, щоб забезпечити надійність та якість електроживлення серверів, систем пожежотушіння, охорони, відеонагляду та інших систем, використовується система гарантованого електропостачання, яка містить у собі агрегат безперервного живлення зі стандартним набором акумуляторних батарей, дизельної електростанції з автоматичним пуском та пристроєм автоматичного переключення на дизельну електростанцію. Заземлення засобів комп'ютерної та іншої техніки для обробки інформації в банківській діяльності повинно мати електричний опір який не перевищує 4 Ом, це допомагає уникнути виникнення електростатичних полів, які можуть впливати на стійкість електронних пристроїв та систем, крім того заземлення грає важливу роль у відведенні перенапруг, які

можуть виникати внаслідок блискавки чи інших електричних розрядів, що загалом сприяє стабільному електричному потенціалу та забезпечує надійну роботу обладнання і запобігає непередбаченим проблемам.

Відсутність своєчасної заміни компонентів сервера може поставити під загрозу безперервне функціонування сервера та, як наслідок, стати причиною втрати працездатності банку або певних його сервісів на час заміни компоненту. Варто зазначити, що сама модульна концепція серверу має на увазі його безперервне функціонування, тобто компоненти сервера влаштовані таким чином, щоб часто їх можна було швидко замінити, не ставлячи на паузу сам сервер, така особливість забезпечується за допомогою того, що багато компонентів у сервері ставляться парами, наприклад, блоки живлення, щоб вихід з ладу одного з них не знеструмив весь сервер, або ж використання дисків із гарячою заміною для запобігання втрати інформації або зупинки серверу.

Пожежа у серверному приміщенні банку є серйозною загрозою, яка може призвести до великих втрат даних, перерв у роботі фінансових операцій та порушення конфіденційності клієнтської інформації. В умовах сучасних технологічних вирішень та великого обсягу цифрових даних, які обробляються банками, захист від пожежі є важливою складовою систем безпеки.

Пожежна загроза у банківському серверному приміщенні може виникнути з різних причин, включаючи електричні неполадки, перегрів обладнання, коротке замикання, технічні несправності у системах кондиціонування повітря та інші фактори. В разі виникнення пожежі, банк стикається з ризиком втрати важливих даних, знищення обладнання та порушенням нормального функціонування систем, що може призвести до фінансових втрат і втрати довіри клієнтів.

Автоматична система газового пожежогасіння і система оповіщення під час пожежі є необхідними для приміщення де розташовуються сервера. Внутрішні поверхні цих приміщень повинні бути облицьовані матеріалами, які відповідають вимогам пожежної безпеки та відповідають санітарно-гігієнічним стандартам.

Для того щоб недопустити проникнення сторонніх речовин через повітропроводи системи вентиляції та канали для введення кабелів і комунікацій

до серверних приміщень, рекомендується встановлювати вогнетривкі пробки або вогнетривкі аварійні заслінки.

Несправності системи вентиляції в серверному приміщенні можуть призвести до серйозних порушень умов функціонування серверів, створюючи потенційно небезпечні умови для обладнання та даних, які вони обробляють. Підтримка оптимальних температур і вологості у серверних кімнатах є критично важливою для забезпечення стабільності та ефективності обчислювальних систем. Умови функціонування серверів, такі як температура та вологість, мають безпосереднє вплив на їх продуктивність та надійність. Висока температура може призвести до перегріву обладнання, що збільшує ризик відмов та може впливати на тривалість його служби. З іншого боку, низька температура може викликати конденсацію та інші проблеми, особливо при стрімких змінах температури.

Несправна система вентиляції може викликати ряд проблем, таких як нерівномірний розподіл тепла, недостатня циркуляція повітря та збільшення температурного градієнту в приміщенні. Це може призвести до "гарячих точок" або зон, де температура вища, ніж інде в кімнаті, що може бути небезпечним для обладнання, розташованого в цих областях.

Важливою також є відповідна вологість повітря, оскільки занадто сухе або, навпаки, занадто вологе середовище може викликати електростатичні розряди, корозію та інші проблеми з обладнанням.

Саме тому централізована чи окрема система припливно-витяжної вентиляції з функцією очищення від пилу, а також окрема система автоматичного кондиціонування повітря, що також забезпечує очищення від пилу є необхідною складовою серверних приміщень.

Проблеми безпеки в серверних приміщеннях не завжди виникають внаслідок технічних вразливостей чи кібератак. Спільно з помилками обслуговуючого персоналу та можливими навмисними діями, низка нових викликів стає важливим аспектом безпеки інформаційних систем. Недостатня кваліфікація членів обслуговуючого персоналу, таких як системні адміністратори, спеціалісти з електрики, пожежогасіння та вентиляції, може призвести до

серйозних наслідків, таких як витік конфіденційної інформації або послаблення систем захисту.

Помилки або недостатні знання з експлуатації обладнання та систем ведуть до можливості виникнення вразливостей, що може бути використано для несанкціонованого доступу чи зміни в параметрах безпеки. Зірвання термінів експлуатації та обслуговування, неправильна обробка обладнання, а також несправні вентиляційні системи або системи пожежогасіння можуть стати факторами, що сприяють виникненню аварій та порушенню цілісності серверних приміщень.

Серйозною загрозою також є навмисні дії обслуговуючого персоналу. Від зловживання прав доступу до власних спонукань, шантажу та підкупу сторонніми особами до видалення журналів подій чи інших заходів для приховання слідів – ці аспекти можуть призвести до серйозних наслідків для безпеки інформації та надійності систем.

Для запобігання появи таких загроз необхідною умовою є наявність у серверному приміщені облікового журналу на паперових носіях, в якому зафіксовані дані щодо дати та часу, коли приміщення було відкрито та закрито, дані працівника, який знаходився у кімнаті, а також опис робіт, які були проведені цим працівником. Також правилами регулюється заборона розміщення робочих місць співробітників банку у серверному приміщені, що також зменшує час перебування у такому приміщення персоналу і таким чином, зменшує і появу загрози.

Технічний канал витоку інформації - це сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки (рис. 3.1).

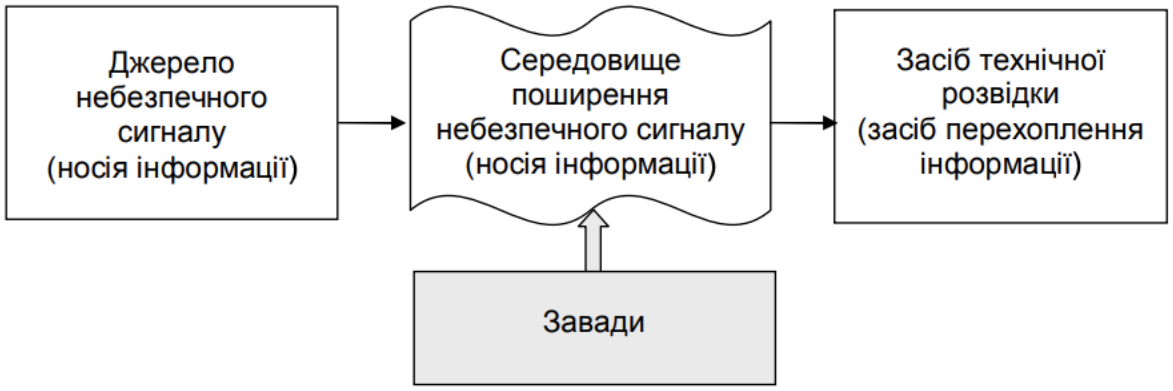

Рисунок 3.1 – Технічний канал витоку інформації

Тобто, технічним каналом витоку інформації є фізичний шлях небезпечного сигналу (носія інформації) від джерела небезпечного сигналу до зловмисника.

Небезпечний сигнал - сигнал (поле), у тому числі побічний, який містить інформацію з обмеженим доступом і який може бути перехоплений засобами технічної розвідки

Носій інформації - небезпечний сигнал, який містить інформацію з обмеженим доступом, прикладом може слугувати електричний струм, або електромагнітне поле.

Середовищем поширення небезпечного сигналу може бути повітряне середовище, лінії електроживлення, заземлення, сигналізації, управління, інженерні комунікації і

спорудження, огороджувальні будівельні конструкції, якими може поширюватися небезпечний сигнал.

Засоби технічної розвідки - це технічні засоби, які призначені для несанкціонованого перехоплення інформації.

Інформаційна діяльність на ОІД, а саме у серверному приміщені, передбачає лише один вид роботи з інформацією, а саме її обробка технічними засобами та системами, а також зберігання її на носіях інформації.

Відповідно, на ОІД можна виділити первинне джерело небезпечного сигналу (який може розповсюджуватись в просторі на досить великі відстані і може бути перехопленим засобами технічної розвідки противника поза межами

контрольованої зони), а саме технічні засоби та системи, що обробляють інформацію, а до середовища поширення небезпечного сигналу варто віднести комунікації технічних засобів та систем і інженерні комунікації, які виходять за межі контрольованої зони.

До технічних каналів, які обробляються у технічних засобах та системах, відносять канали побічних електромагнітних випромінювань та наведень.

Для неможливості перехоплення небезпечного сигналу у вигляді електромагнітних полів необхідно навколо ОІД організаційно створити і забезпечити контрольовану зону, тобто територію навколо об’єкта інформаційної діяльності, на якій виключено несанкціоноване розташування технічних і транспортних засобів та неконтрольоване перебування сторонніх осіб.

Канал побічних електромагнітних випромінювань ОТЗС утворюється шляхом перехоплення приймачами засобів технічної розвідки побічних електромагнітних полів, які формуються навколо електронних елементів та провідників ОТЗС при проходженні ними інформаційних сигналів та поширення цих полів за межі контрольованої зони. Інформаційними сигналами у даному випадку є електричні струми, що несуть інформацію. Навколо ОТЗС завжди присутні поля випромінювання, оскільки ці випромінювання небажані та носять побічний характер, їх називають побічними електромагнітними випромінюваннями.

Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС, як різновид каналів побічних електромагнітних наведень, утворюється шляхом безпосереднього зняття з ліній електроживлення (заземлення) ОТЗС засобами технічної розвідки за межами КЗ небезпечних електричних сигналів, що наводяться в цих лініях побічними електромагнітними полями ОТЗС та/або просочуються в ці лінії (або виникають в лінії електроживлення через нерівномірність споживання електроенергії) при функціонуванні ОТЗС.

Запобігання витоку інформації каналами ПЕМВН досягається шляхом створення контрольованої зони та організації режиму доступу до неї, екранування

приміщення та використання екранованих шаф, просторового електромагнітного зашумлення, лінійного зашумлення ліній електроживлення та заземлення ОТЗС, електроживлення від автономних електричних джерел, що розташовані у межах КЗ, використання в лінії електроживлення ТЗЗ, які затримують сигнали низького рівня та мережевих фільтрів, а також використання автономного від ДТЗС заземлення ОТЗС.

Несанкціонований доступ сторонніх осіб до приміщення може призвести до надзвичайно серйозних наслідків, таких як отримання доступу зловмисником до конфіденційної інформації, викрадення або знищення компонентів серверного приміщення та інших носіїв інформації. Використовується автоматизована система доступу чи кодовий замок для того, щоб запобігти НСД до серверного приміщення. Необхідно встановлювати два чи більше рубежі охоронної сигналізації, при цьому кожний рубіж повинен бути підключений за допомогою окремих кодів до приймально-контрольних приладів. Ці прилади розташовані на посту охорони банку чи іншого суб’єкта охорони.

Кібератаки є однією з основних загроз для конфіденційності та цілісності інформаційних систем. В цьому контексті, кілька чинників впливу стають ключовими причинами, що спричиняють НСД та можуть вибудовувати вразливості в інфраструктуру:

- розвиток кіберзлочинності включає в себе постійне удосконалення та розширення арсеналу шкідливого програмного забезпечення. Нестійкість алгоритмів, використовуваних для захисту даних, може стати слабким місцем у системі, яке кіберзлочинці використовують для отримання несанкціонованого доступу;
- людський фактор залишається однією з найбільш вразливих частин в інформаційній безпеці, оскільки помилки адміністратора, такі як недостатня конфігурація безпеки чи недостатнє виявлення та реагування на потенційні загрози, можуть відкривати доступ до даних для несанкціонованого використання;

- застосування застарілих або піратських версій операційних систем та програмного забезпечення може призвести до виникнення вразливостей, які використовуються кіберзлочинцями для здійснення атак, саме тому актуалізація та вчасне оновлення ліцензійних систем стають критичними для мінімізації ризиків.

До основних заходів протидії таким загрозам є встановлення надійних захисних систем для відсіювання несанкціонованих вторгнень, використання брандмауерів та системи виявлення та запобігання (IDS/IPS) для моніторингу та блокування атак на мережевому рівні, застосування шифрування даних, навчання персоналу щодо найновіших загроз та технік кібератак є необхідним, оскільки свідомість персоналу та його дій при соціально інженерних атаках та кібератаках є ключовою складовою безпеки.

3.3. Вимоги до створення захищеного приміщення

3.3.1. Інженерно-технічні вимоги

Серверне приміщення повинно розташовуватися у віддалених кінцях будівлі, подалі від вентиляційних шахт, ліфтів, підвалів та труб з водою. Якщо можливо, приміщення слід розташовувати у внутрішній частині будівлі або в напрямку внутрішнього двору. Згідно з правилами заборонено розміщувати робочі місця співробітників банку в серверних приміщеннях, тож головний розподільчий пункт буде знаходитись у сусідній кімнаті.

Рекомендується облаштування серверних у приміщеннях, де немає вікон задля захисту обладнання від сонячних промінів та простішої підтримки необхідного мікроклімату.

Загалом, висуваються наступні вимоги щодо розмірів приміщення: висота серверної повинна бути не менш ніж 244 см, а мінімальною рекомендованою площею серверного приміщення є 14 м^2.

Оскільки серверна шафа висотою 42U, а саме Estap EVL70142U6080, яку ми беремо за основу, при повній комплектації серверним обладнанням може важити 600 кг, її ширина складає 60 см, а глибина – 80 см, то площа, яку шафа займає на

підлозі дорівнює 60*80/10000 = 0,48 м^2, тож підлога повинна витримувати від 600/0,48 = 1250 кг/м^2 (рис 3.2).

Рис 3.2 – Шафа серверна підлогова Estap EVL70142U6080

Для того щоб вмістити серверну шафу заввишки 42U необхідні високі стелі, щоб окрім шаф вмістити ще й фальш підлогу. Фальш підлога потрібна для структурованої кабельної мережі, тобто більшість кабелів має знаходитись під антистатичною фальш підлогою, оскільки звичайна підлога може накопичувати статичний заряд, а якщо станеться розряд, це може пошкодити обладнання. Таким чином, фальш підлога забезпечує легкий доступ до всіх комунікацій через люки, можливість встановити додаткове охолодження у випадку необхідності, а також додатковий захист від затоплення. Фальш підлогу візьмемо 50 см + 200 см шафу + 25 см для припливно-витяжної вентиляції та запас у 25 см, тож згідно з цим, стеля

заввишки 3 метри буде достатньою. До того ж стелю необхідно гідроізолювати, оптимальним варіантом для гідроізоляції стелі є проникаюча гідроізоляція «Мегатрон». Технологія гідроізоляції зводиться до нанесення на стелю проникаючого складу на основі цементу, полімерів та поліуретанові мастики, який гідроізолює всю товщу бетонного перекриття.

Так як серверна – це досить шумне технічне приміщення, яке не розраховане на довге перебування людей усередині, тож в якості шумоізоляції необхідно використовувати товсті стіни, а саме товщиною 40 см, а також двері з ущільнювачами.

Необхідна централізована чи окрема система припливно-витяжної вентиляції з функцією очищення від пилу, а також окрема система автоматичного кондиціонування повітря, що також забезпечує очищення від пилу є необхідною складовою серверних приміщень. Ці системи повинні забезпечувати у приміщенні температуру повітря в межах 18-24 градусів Цельсія та відносну вологість не більше 60% у будь-яку пору року.

Відповідно до пожежної безпеки, рекомендовано інсталювати мультиканальну аспіраційну систему пожежних сповіщувачів із високою чутливістю класу А. Ця система постійно аналізує повітря у приміщенні, що дозволяє миттєво реагувати на дим. Ця система може бути проведена як під фальш підлогу, так і в кожну стійку або шафу окремо (рис. 3.3).

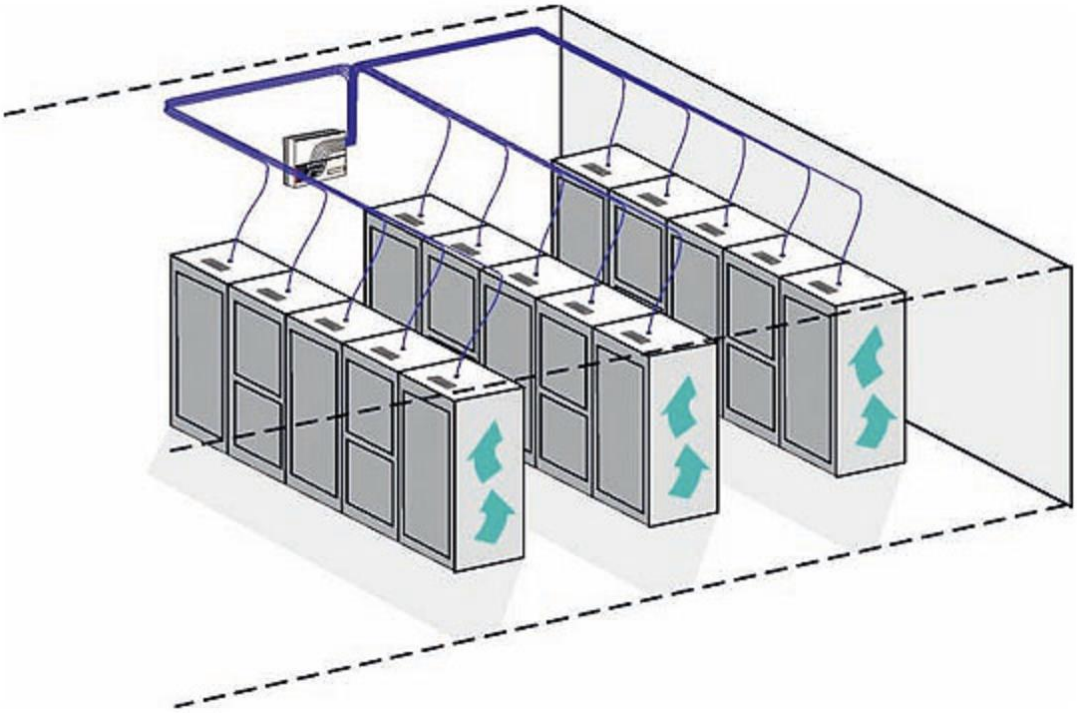

Рисунок 3.3 – Застосування мультиканальної аспіраційної системи пожежних сповіщувачів для захисту серверних шаф

Також додамо чотириканальні комбіновані датчики диму, тепла, полум'я та газу, вони будуть адресними, щоб системний адміністратор або інша відповідальна особа змогла зрозуміти, в якому конкретно місці почалися проблеми чи потрібне обслуговування обладнання. Такі датчики фіксують кілька станів: "нормальна робота", "пожежа", "несправність", "забруднення датчика" та інші. Ці датчики, виявивши нестандартну ситуацію, надсилатимуть на смартфони відповідальних осіб сигнали тривоги. Двері, стельові перекриття, стіни та перегородки повинні бути зроблені з вогнетривких матеріалів (вогнетривкі бетон та цегла) або бути облицьованими такими матеріалами (гіпсовінілові оздоблювальні панелі) для забезпечення вогнестійкості не менше 45 хвилин.

Щодо автоматичної системи пожежогасіння, звичайні спринклерні системи не підходять, оскільки волога миттєво знищить або пошкодить усе обладнання, тож використовувати необхідно автоматичну систему газового пожежогасіння. В якості головного компоненту цієї системи використовується інертний газ, який ще називають інергеном. Цей компонент є безпечним для людей та не заважає роботі обладнання, так як при розпиленні не відбувається конденсація.

Також для того щоб недопустити проникнення стороннiх речовин через повiтропроводи системи вентиляцiї та канали для введення кабелiв i комунiкацiй до серверних примiщень, рекомендується встановлювати вогнетривкi пробки або вогнетривкi аварiйнi заслiнки.

Використовується автоматизована система доступу чи кодовий замок для того, щоб запобiгти НСД до серверного примiщення. Необхiдно встановлювати два чи бiльше рубежi охоронної сигналiзацiї, при цьому кожний рубiж повинен бути пiдключений за допомогою окремих кодiв до приймально-контрольних приладiв. Ці прилади розташованi на посту охорони банку чи iншого суб'єкта охорони.

Одною з найбiльш захищених систем контролю та управлiння доступом є аутентифiкацiя по вiдбитку пальця за допомогою ультразвукових бiометричних сканерiв, окрiм того, наявна система повинна забезпечувати наступнi параметри:

- доступ до примiщення є лише у осiб, якi були внесенi до бази даних системи контролю та управлiння доступом, або у випадку обслуговування обладнання спецiалiзованими службами доступ до примiщення повинен надаватися лише пiд наглядом вiдповiдальних осiб;
- обмежений час проходу, щоб запобiгти проходу кiлькох людей по одному пропуску;
- контроль стану дверей з оповiщенням про злом чи незакриття;
- журнал подiй у примiщенні з полями: хто вiдкрив, коли, що робив усередині;
- заборона на повторний вхiд, якщо не було виконано вихiд.

План контрольованої зони банку визначає контрольовану зону серверного примiщення.

Реалiзацiя заходiв ТЗI вiд можливого впливу зовнiшнiх електромагнiтних полiв та вiд витоку технiчними каналами, а саме каналами ПЕМВН у серверному примiщенні повинна виконуватися методом екранування примiщення чи використання екранованих шаф з класом опору до злому не менше II.

Для реалізації екрана рекомендується використовувати наступні матеріали: листова сталь, листи міді, латуні, алюмінієві та їх сплави, металева сітка з розміром вічка не менше 6х6 мм.

Висуваються наступні вимоги при виготовленні екрана:

- металеві листи мають зварюватися суцільним швом або бути з’єднані фальцем з подальшим пропаянням місць з’єднання суцільним швом;
- сітки повинні бути з’єднані між собою пайкою або бути зварені суцільним швом;
- коли відбувається зварювання може використовуватися переривчастий шов з проміжками між точками зварювання не більше 25 мм;
- деталі кріплення слід зварювати з екраном по всьому периметру в місцях їх проходження через екран.

Екран необхідно відокремлювати від металевих деталей інженерних конструкцій, уникати гальванічного контакту з ними.

Для створення екрану у дверних прорізах застосовуються металеві двері.

Щоб забезпечити електричний контакт між дверима та коробкою (яка з’єднується з екраном шляхом зварювання) по периметру використовується контактний пристрій з корозієстійкого пружного матеріалу (прикладом може слугувати берилієва бронза), який має гребінчасті контакти із кроком гребінки не більше 25 мм і далі здійснюється укладання цих контактів на планку з корозієстійкого матеріалу. З'єднання гребінчастих контактів та планок із зачищеною поверхнею двері (коробки) забезпечують за допомогою гвинтів, розташованих з кроком не більше 50 мм. Також можливо встановити контактний пристрій на дверній коробці, а контактну планку на дверях відповідно. Також щоб забезпечити електричний контакт між дверима та коробкою використовують замковий пристрій по периметру, який гарантує притискання до дверей коробки.

Неметалеві труби, які є діелектриками, вводяться в екрановане приміщення за допомогою металевих патрубків, які зварюються по периметру з екраном, поперечний розмір яких дорівнює 50 мм або менше, а довжина їх не є меншою за два попередніх розміри.

Щодо металевих труб, то вони поділяються на природні заземлювачі та не природні заземлювачі, перші можна вводити в приміщення за допомогою сталевих труб (які потрібно приварити до екрану по периметру введення, а також ізолювати від введених металевих труб) поперечний розмір яких дорівнює 50 мм або менше і довжина складає три метри та більше, другі ж просто зварюють до екрану по периметру.

До інформаційних кабелів, які розповсюджуються за межі контрольованої зони встановлюється вимога мати п’яту категорію екранування або вище, бути оптоволоконними або будь-якими іншими, які мають захист від електромагнітного випромінювання.

До кабелів електроживлення встановлюється вимога введення їх через фільтри електроживлення.

До всіх інших кабелів встановлюється вимога введення їх за допомогою сталевих труб поперечний розмір яких дорівнює 50 мм або менше і довжина яких складає три метра або більше. Якщо цього виявиться замало, введення варто здійснювати через фільтри, але тільки не інформаційних кабелів, бо для них використовують феромагнітний порошок, який засипається в труби.

Рекомендоване розміщення фільтрів електроживлення зовні приміщення у близькості до місця, де введені електричні проводи.

Вимоги щодо заземлювача (що не є природнім заземлювачем) приміщення встановлюються наступні, він повинен бути розташований за 10 метрів та більше до межі контрольованої зони та інженерних комунікацій, що виходять за неї.

Заземлення засобів комп'ютерної та іншої техніки для обробки інформації в банківській діяльності повинно мати електричний опір який не перевищує 4 Ом.

Екранування вважається ефективним, якщо воно не нижче 20 дБ в діапазоні частот від 0,15 до 1000 МГц, а його вимірювання здійснюється юридичними особами, які володіють ліцензією Державної служби спеціального зв’язку та захисту інформації України для здійснення відповідної діяльності.

Як серверне приміщення, так і банк в цілому, повинен бути підключений до міської електромережі та мати два незалежних введення з різних підстанцій.

Кожна лінія повинна забезпечувати передачу необхідної потужності. Інстальоване електрообладнання повинно бути оснащеним як автоматичним, так і ручним переключенням між лініями. Для того щоб забезпечити необхідну надійність та якість електроживлення серверів та інших компонентів захищеної кімнати, використовується система гарантованого електропостачання, вона включає в себе дизельний генератор з автоматичним пуском та акумуляторні батареї.

Для живлення серверів рекомендується використовувати джерела безперебійного живлення з функцією повного перетворення вхідної. При монтажі агрегату безперервного живлення необхідно розміщувати вхідні та вихідні проводи в окремих пакетах, і відстань між ними повинна бути 40 см або більше.

Для створення локальних мереж у банку необхідно використовувати екрановані виті пари п’ятої категорії та вище, наприклад FTP, STP та SFTP за допомогою оптоволоконного кабелю.

3.3.2. Програмно-апаратні вимоги

За основну одиницю сервера візьмемо сервер DELL R740, детальна конфігурація якого наведена у таблиці 3.3.

Таблиця 3.3

Рекомендована конфігурація сервера DELL R740

№	Компонент	Деталі	Кількість
1	Процесор	Intel Xeon Silver 4210 (24 ядра, 48 потоків, 2,1 ГГц, 16 Мб кеша)	2
2	Оперативна пам’ять	256 Гб DDR4-2666 ECC	16 x 16 Гб
3	Постійна пам’ять	12 Тб HDD (SAS 12 Гб/с, 7200 об/хв) 2 Тб SSD (NVMe PCIe Gen3 x4)	2 x HDD 2 x SSD
4	Блок живлення	1100 Вт (80 Plus Platinum)	2
5	Мережевий адаптер	10GbE (SFP+, Mellanox ConnectX-3 EN)	2
6	RAID-контроллер	Dell PERC H730P – захист даних від втрати при відмові дисків	1

На серверах встановлюється програмне забезпечення, яке потрібне для роботи сервісів банку та інших служб домену, для обслуговування та моніторингу, а також для захисту від злому та стійкості до навантажень. Рекомендоване програмне забезпечення наведене у таблиці 3.4.

Таблиця 3.4

Рекомендоване програмне забезпечення сервера

№	ПЗ	Деталі
1	Red Hat Enterprise Linux	Red Hat Enterprise Linux – це корпоративна операційна система Linux, яка призначена для використання у великих організаціях, включаючи банки. Вона відрізняється високою надійністю, безпекою та масштабованістю. Вона має репутацію однієї з найнадійніших операційних систем Linux та пройшла сертифікацію за стандартами безпеки FIPS 140-2 та Common Criteria. Red Hat Enterprise Linux включає безліч функцій безпеки, які допомагають захистити дані та інфраструктуру банку. Red Hat Enterprise Linux може масштабуватись від невеликих до великих дата-центрів.
2	Oracle Database 21c	Oracle Database 21c – це найновіша версія системи управління базами даних Oracle. Вона пропонує високу продуктивність, масштабованість та безпеку, необхідні для роботи дата-центру банку. Oracle Database 21c також підтримує сучасні технології, такі як штучний інтелект та машинне навчання.
3	Firewall	Виконує фільтрацію мережевого трафіку, запобігаючи несанкціонованому доступу до серверів банку, поширення шкідливого ПО, DDos/Dos атаки. Firewall зазвичай використовується у поєднанні з іншими системами безпеки, такими як IDS та IPS.
4	Nginx і Apache	Встановлення Nginx і Apache здійснюється для збільшення продуктивності встановлюється два веб-сервери: швидкий Nginx, який віддає користувачам «статику» (фізично існуючі на сервері документи, що не потребують обробки перед відправкою), а решта запитів переадресовує серверу застосунків Apache, який займається генерацією динамічних документів.
5	FTP-сервер	Дозволяє отримувати доступ до файлів на сервері за протоколом FTP. Як правило, використовується для адміністрування сайту (як для оновлення програмного коду, так і для завантаження об'ємних файлів). Більш безпечною альтернативою FTP є SFTP, протокол базується на SSH і дозволяє шифрувати передані та отримані дані.
6	Memcached	Система, яка «запам'ятовує» результат обробки запитів та використовує ці дані при повторних зверненнях для прискорення генерації сторінок.
7	IBM Spectrum Protect	Рішення для резервного копіювання та відновлення даних, яке підтримує різні типи даних, обсяги даних та частоти резервного

		копіювання. IBM Spectrum Protect також дозволяє зберігати резервні копії даних на локальних носіях, у хмарі або гібридному середовищі.
8	SolarWinds Orion	Комплексне рішення для моніторингу системи та інфраструктури, яке підтримує різні типи систем та додатків. Воно може використовуватися для відстеження продуктивності, використання ресурсів та безпеки.

Окрім самого «заліза» та програмного забезпечення, яке на нього встановлюється, дуже важливим елементом є інтернет провайдер, а також їх кількість. Для надійності треба мінімум 3 магістральні провайдери, так як на практиці бувають випадки одночасного відключення відразу кількох.

3.3.3. Організаційні вимоги

Коли настає час вводити приміщення до режиму експлуатації, необхідно провести наступні заходи:

- перевірити чи достатньо ефективне екранування приміщення, а також кабелів і комунікацій;
- дооснастити приміщення у випадку необхідності, а саме інсталювати додаткові фільтри, перерозвести провідники та інші вдосконалення.

Після того, як роботи були завершені, складається акт відповідності вимогам та протоколи вимірювання достатності екранування, один раз на кожні 5 років виконується таке вимірювання.

Також до організаційних вимог відноситься організація контролю доступу та охорони, ретельний підбір персоналу (зазвичай за серверну кімнату відповідальна одна людна – системний адміністратор) та проведення тренінгів для цього персоналу щодо дій у надзвичайних ситуаціях, навчання правилам безпеки та роботи з конфіденційною інформацією, а також застереження від соціального інжинірингу зі сторони зловмисників, крім того організація оновлення програмного забезпечення до актуальних стабільних версій та постійний моніторинг відповідності середовища приміщення до вимог, які визначені нормативними документами.

ВИСНОВКИ

У світлі наростаючої важливості забезпечення безпеки інформації, побудова захищених приміщень стає важливим елементом системи захисту конфіденційної інформації. Особливо це стосується серверних приміщень банків, де обробляється величезний обсяг конфіденційної інформації.

В роботі було розглянуто поняття захищеного приміщення, його складові, потенційні загрози, засоби та методи захисту від цих загроз, роботи які необхідно проводити задля того, щоб захистити приміщення від фізичних загроз, несанкціонованого доступу та витоку технічними каналами інформації, яка обробляється та зберігається у цьому приміщенні, згідно з нормативними документами у галузі інформаційної безпеки.

У ході дослідження загроз інформації та засобів протидії у захищеному приміщенні визначено, що забезпечення безпеки інформації вимагає комплексного підходу, що охоплює як технічні та інженерні, так і організаційні аспекти.

Було проведено аудит інформаційної безпеки серверного приміщення, який включає визначення інформації, яка повинна підлягати захисту при обробці та зберіганні на серверах у серверному приміщені банку, визначення загроз та вразливостей, які сприяють реалізації цих загроз, а також джерела виникнення цих загроз.

Особлива увага була приділена побудові захищеного приміщення серверної банку, обґрунтовуючи необхідність його створення, були визначені інженерно-технічні, програмно-апаратні та організаційні вимоги та рекомендації, дотримання яких забезпечить створення та довгострокову підтримку захищеного приміщення від різних типів загроз.

Отже, робота над проєктом захищеного приміщення є важливим етапом у забезпеченні інформаційної безпеки та вимагає врахування комплексу факторів. Етапи, що були розглянуті, та визначені вимоги є основою для успішного впровадження та функціонування захищеного приміщення з сучасним

обладнанням та сучасними засобами захисту, що відповідають вимогам стандартів і нормативам.

ПЕРЕЛІК ПОСИЛАНЬ

Законодавчі та нормативні документи

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України».
4. Закон України «Про Національну систему конфіденційного зв'язку».
5. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
6. Закон України «Про інформацію».
7. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».
8. Постанова Національного Банку України «Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи».
9. Закон України «Про банки і банківську діяльність».
10. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України».
11. Закон України «Про телекомунікації».
12. Закон України «Про державну таємницю».
13. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»
14. Закон України «Про наукову і науково-технічну експертизу»
15. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

16. НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу».
17. НД ТЗІ 3.3-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації».