МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 «Кібербезпека»

на тему: **ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

Студент групи СЗД-42 Скребков Антон Олександрович _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Гребенніков Асаді Болдхоягович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н., доц. Г.В. Шуклін

«_____»_____ 2022р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Скребкову Антону Олександровичу

1. Тема роботи: Технології проектування систем захисту інформації

Затверджена наказом по університеті від «____»_____ 2022 р. № ___

2. Термін здачі студентом оформленої роботи «____» _____ 2022 р.

3. Об'єкт дослідження: є процеси захисту інформації в інформаційно-телекомунікаційних системах.

4. Предмет дослідження: є методи і засоби захисту інформації в інформаційно-телекомунікаційних системах.

5. Мета роботи: проектування комплексної системи захисту інформації в автоматизованих системах.

6. Перелік питань, які мають бути розроблені:

1. Аналіз загроз інформації в автоматизованих системах.

2. Аналіз методів та засобів захисту інформації в автоматизованих системах.

3. Проектування комплексної системи захисту інформації в автоматизованих системах.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____2022 р.

Науковий керівник _____ Шуклін Г.В.

Завдання прийняв до виконання _____ Скребков А.О.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз загроз інформації в автоматизованих системах	До 04.04.22	Виконано
2	Аналіз методів та засобів захисту інформації в автоматизованих системах	До 25.04.22	Виконано
3	Проектування комплексної системи захисту інформації в автоматизованих системах	До 06.05.22	Виконано
4	Реферат, вступ, висновки	До 13.05.22	Виконано
5	Перевірка роботи на антиплагіат+передзахист	До 01.06.22	
6	Захист роботи	До 21.06.22	
7	Випуск	30.06.22	

Студент _____ Скребков А.О.

(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи _____ Шуклін Г.В.

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 59 сторінок, 4 рисунки, 3 таблиці, 23 джерела.

Об'єкт дослідження – процеси захисту інформації в інформаційно-телекомунікаційних системах.

Предмет дослідження – методи та засоби захисту інформації в інформаційно-телекомунікаційній системі.

Мета роботи – проектування комплексної системи захисту інформації в автоматизованих системах.

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

В роботі проведено дослідження вимог чинного законодавства України щодо захисту інформації в інформаційно-телекомунікаційній системі. В рамках роботи проведено обстеження середовищ функціонування інформаційно-телекомунікаційної системи, розроблені моделі загроз інформаційній безпеки та моделі порушника, політика інформаційної безпеки і технічне завдання. Крім того, обрано методи та засоби захисту інформації в АС класу 2.

Галузь використання – інформаційна безпека.

ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, КОМПЛЕКС ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ,

ГЕНЕРАТОР ШУМУ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АКТИВНІ МЕТОДИ ЗАХИСТУ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ……..….....6
ВСТУП…….……..….....7
1 ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ 8
1.1.Підґрунтя щодо створення КСЗІ 8
1.2. Шляхи втрати інформації в автоматизованих системах 12
1.3. Класифікація основних засобів протидії загрозам безпеки 17
1.4. Нормативно-правова база робіт по створенню КСЗІ 26
2 КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ 28
2.1. Обґрунтування необхідності створення КСЗІ 28
2.2. Категоріювання ОІД 29
2.3. Обстеження середовищ функціонування ІТС 31
2.4. Акт обстеження об’єкту інформаційної діяльності 32
2.5. Політика інформаційної безпеки 34
2.6. Модель загроз інформаційній безпеці 35
2.7. Модель порушника інформаційної безпеки 37
2.8. Технічне завдання на створення КСЗІ 40
3 ОБҐРУНТУВАННЯ ТА ВИБІР ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В АС-2 53
3.1. Захист від витоку технічними каналами 53
3.2. Захист від несанкціонованих дій з інформацією 53
ВИСНОВКИ 57
ПЕРЕЛІК ПОСИЛАНЬ 58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОІД – об'єкт інформаційної діяльності

ОС – обчислювальна система

ПК – персональний комп'ютер

АС – автоматизована система

КС – комп’ютерна система

МНСІ – матеріальний носій секретної інформації

САЗ – система активного захисту

КТ – контрольована територія

КЗЗ – комплекс засобів захисту

НСД – несанкціонований доступ

КВА – контрольно-вимірювальна апаратура

ІзОД – інформація з обмеженим доступом

СЗІ – система захисту інформації

КСЗІ – комплексна система захисту інформації

ІТС – інформаційно-телекомунікаційна система

ТЗІ – технічний захист інформації

ОТЗС – основні технічні засоби і системи

ДТЗС – допоміжні технічні засоби системи

ПЕМВ – побічні електромагнітні випромінювання

ПЕОМ – персональні електронно-обчислювальні машини

ПЕМВН – побічні електромагнітні випромінювання і наведення

DDoS – Distributed Denial-of-service

DoS – Denial-of-service

ВСТУП

На даний час в провідних країнах світу склалася досить чітко окреслена система концептуальних поглядів на проблеми забезпечення інформаційної безпеки. Проте, як свідчить сьогодення, злочинні дії пов’язані з інформацією як у приватному так і не тільки не зменшуються, але і мають досить стійку тенденцію до зростання.

Комплексні системи захисту інформації створюються задля забезпечення інформаційної безпеки. Інформаційна безпека – це стан захищеності інформаційного середовища підприємства. Сукупність заходів, які забезпечують досягнення та підтримку стану захищеності називають управлінням інформаційною безпекою. Проблема створення системи захисту інформації містить у собі завдання розробки системи захисту інформації та її оцінка. Для розуміння того, чи задовольняє СЗІ комплекс вимог до даних систем, проводиться аналіз технічних характеристик системи захисту інформації, що і є вирішенням завдання її оцінки. З використанням сертифікації засобів захисту інформації та атестації СЗІ у процесі її впровадження, вирішується завдання оцінки у теперішній час.

Мета роботи – створення комплексної системи захисту інформації в автоматизованій системі другого класу.

Об’єкт дослідження – захист інформації в інформаційно-телекомунікаційних системах.

Предмет дослідження – Комплексний захист інформації в інформаційно-телекомунікаційній системі.

У даній роботі розглядається методика створення комплексної системи захисту інформації в автоматизованій системі другого класу.

1 ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1. Підґрунтя щодо створення КСЗІ

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» свідчить про те, що комплексною системою захисту інформації називають взаємопов'язану сукупність організаційних та інженерно–технічних заходів, засобів і методів захисту інформації [1].

Восьма стаття цього закону, а саме «Умови обробки інформації в системі» свідчить про те, що інформація з обмеженим доступом або та, що є власністю держави, має оброблятись у системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю, яка здійснюється за результатами державної експертизи. Для створення комплексної системи захисту інформації, що є власністю держави, використовують засоби захисту інформації, що мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи [1].

У 2006 році 29 березня були затверджені «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно–телекомунікаційних системах», в них визначено, що задля забезпечення захисту інформації в системі створюється КСЗІ. Призначення КСЗІ – захистити інформацію від подій таких як:

- витік технічними каналами, в тому числі каналами ПЕМВН, що були утворені під впливом фізичних процесів;
- несанкціоновані дії з інформацією;
- вплив на засоби обробки інформації, що може призвести до порушення її цілісності та був здійснений шляхом формування фізичних полів і сигналів [2].

У разі обробки у системі інформації, що є державною таємницею або з рішення власника інформації, здійснюється захист інформації від витоку технічними каналами.

Закон України «Про інформацію» свідчить про те, що публічна або задокументована інформація в різних галузях, таких як політика, економіка тощо, є об'єктом інформаційних відносин [3].

Отримання, використання, поширення та зберігання інформації – це основні види інформаційної діяльності, далі розглянемо детальніше кожен термін:

- отриманням інформації є набуття суб’єктами інформації;
- використанням інформації є задоволення інформаційних потреб суб’єктів;
- поширенням інформації є розповсюдження публічно оголошуваної чи документованої інформації;
- зберіганням інформації є забезпечення належного стану інформації;

Об'єднання обчислювальної системи, фізичного середовища, персоналу та оброблювальної інформації, що складається у організаційно-технічну систему з реалізацією інформаційної технології, називається автоматизованою системою.

На даний час використовують наступну класифікацію АС:

АС-1 – це обробка інформації однієї або декількох категорій конфіденційності, що здійснюється одномашинним однокористувацьким комплексом. Прикладом може слугувати автономна автономний ПК з доступністю через організаційні засоби безпеки.

АС-2 – це обробка інформації різних категорій конфіденційності, що здійснюється локалізованим багатомашинним багатокористувацьким комплексом. Прикладом може слугувати локальна обчислювальна мережа. Відмінністю від АС-1 є наявність категорій користувачів з різними правами доступу та можливість одночасної обробки інформації різних категорій конфіденційності.

АС-3 – це обробка інформації різних категорій конфіденційності, що здійснюється розподіленим багатомашинним багатокористувацьким комплексом. Прикладом є глобальна мережа. Відмінністю від АС-2 є необхідність у передачі інформації через незахищене середовище.

Класифікація кожного класу автоматизованих систем здійснюється на основі вимог до забезпечення властивостей інформації. Існують три властивості безпеки інформації, а саме конфіденційність, цілісність та доступність, згідно цього, кожен клас автоматизованих систем має наступні підкласи з підвищеними вимогами щоб забезпечити:

- конфіденційність інформації, що оброблюється;
- цілісність інформації, що оброблюється;
- доступність інформації, що оброблюється;
- конфіденційність і цілісність інформації, що оброблюється;
- конфіденційність і доступність інформації, що оброблюється;
- цілісність і доступність інформації, що оброблюється;
- конфіденційність, цілісність і доступність інформації, що оброблюється [4].

Приведена вище класифікація є корисною для того, щоб забезпечити полегшений вибір переліку функцій, які повинен забезпечити комплекс засобів захисту обчислювальної системи АС. Мінімізація витрат на старті створення КСЗІ АС – це одна з функцій цього підходу. Проте потрібно провести повний аналіз загроз та оцінити ризики для того, щоб створити КЗЗ, який найкраще буде відповідати характеристикам АС.

Порядок отримання, використання, поширення та зберігання інформації, що передбачається правовими нормами, називається режимом доступу до інформації.

В даному контексті, інформацію можна поділити на наступні категорії: відкрита та з обмеженим доступом (ІзОД).

Згідно закону України "Про інформацію", вся інформація класифікується за режимом доступу, з урахуванням правових норм (рис. 1.1) [5].

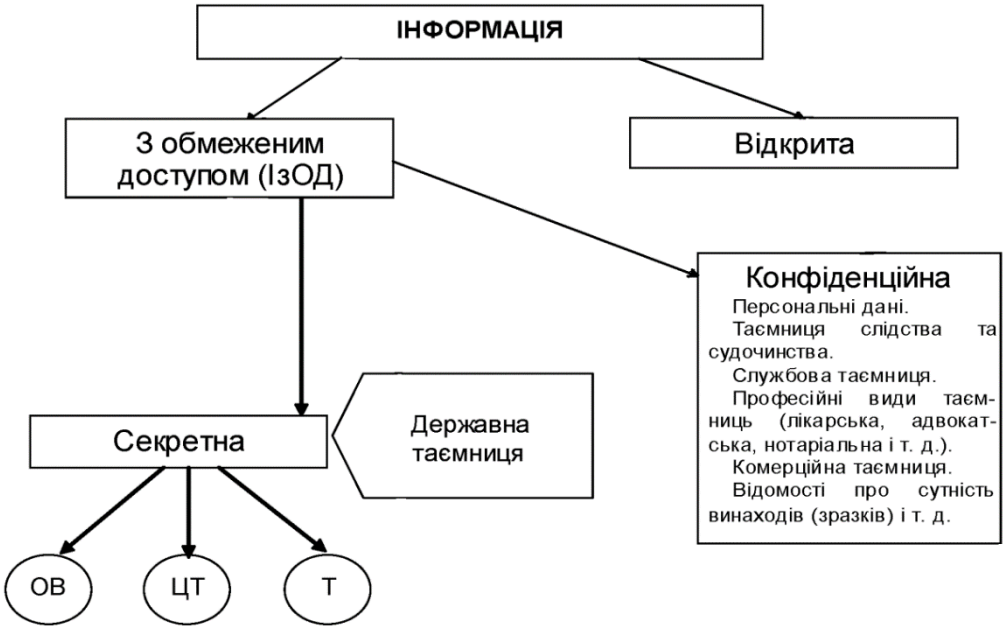

Рис. 1.1. Законодавча класифікація видів інформації в Україні

ІзОД не є відкритою інформацією та має поділ – конфіденційна та таємна.

Конфіденційною інформацією називають відомість, що знаходиться у окремих осіб і може поширюватися за їх бажанням.

Таємною або секретною інформацією називають інформацію, яка може охоплювати сфери оборони, науки, державної безпеки тощо, та розголошення якої може завдати шкоди національній безпеці України. Така інформація визначається як державна таємниця і підлягає охороні державою. Секретна інформація має поділ на особливо важливу, цілком таємну та таємну [6].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» свідчить про те, що забезпечення цілісності під час обробки відкритої інформації у системі здійснюється за допомогою захисту від несанкціонованих дій, ці дії можуть привести до пошкодження або знищення інформації. При обробці ІзОД необхідно забезпечити захист цієї інформації від неконтрольованого

та несанкціонованого ознайомлення, модифікації, знищення, копіювання, поширення [2].

1.2. Шляхи втрати інформації в автоматизованих системах

Щоб забезпечити конфіденційність, цілісність і доступність інформації, необхідно захистити інформацію від витоку та забезпечити захист від втручання системи або об’єкта, де перебуває інформація.

Найчастіше виникають помилки від користувачів або від обслуговуючого персоналу системи, ці помилки є ненавмисними та найнебезпечнішими. Інколи ці помилки можна розглядати як загрозу, результатом якої є колапс системи. В деяких випадках, через помилку виникає ситуація, яка є безпосередньою загрозою для безпеки об’єкта, навіть без урахування дій зловмисників. За приклад візьмемо випадок, коли швейцарський оператор, увівши невірну інформацію у комп’ютері, викликав зіткнення двох літаків у небі.

Результати досліджень, які проводили фахівці з інформаційної безпеки, свідчать про те, що шкода, яка завдається інформаційним ресурсам, у більшій степені є наслідком ненавмисних помилок, а саме 65% шкоди. Загрози природного характеру, такі як пожежа або землетрус, виникають значно рідше.

В загальному випадку загрози можна розподілити наступним чином (рис. 1.2):

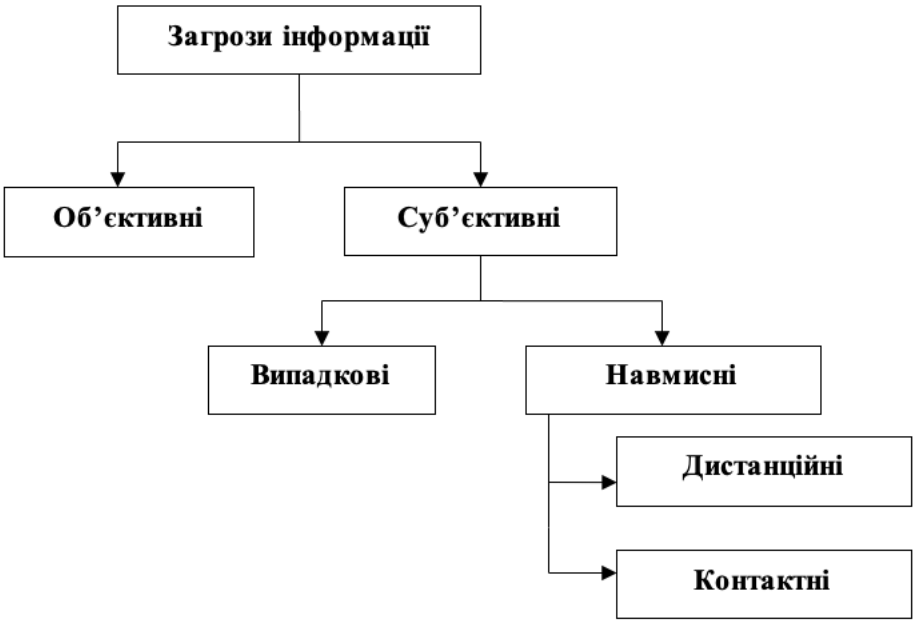

Рис. 1.2. Загальна класифікація загроз інформації

За походженням суб'єктивні загрози мають поділ на випадкові загрози і навмисні. До випадкових загроз відносяться ті загрози, що були викликані помилками проектування АС і СЗІ, тобто через помилки у програмному забезпечені, через збій та відмову системи забезпечення та апаратури або помилками, що були допущені персоналом, який обслуговує систему. Навмисними загрозами називають загрози, що виникли через цілеспрямовані дії людей.

За місцем розміщення навмисні загрози бувають дистанційними та контактними. Дистанційні загрози – це загрози, які виникають за межею території, що контролюється. Контактні загрози – це загрози, що були здійснені в межі зони, що контролюється, наприклад при НСД до приміщення, в якому зберігається інформація.

За типом основного засобу, який використовується для реалізації загрози, всі джерела загроз поділяються на групи, де такими є: людина, апаратура, програма, фізичне середовище.

Існують чотири класи, що поділяють загрози за результатами впливу на інформацію або на систему, що її обробляє. Ця класифікація застосовується при ситуаціях, коли було:

- порушено конфіденційність інформації, тобто інформація була отримана користувачами без дотримування встановлених правил доступу;
- порушено цілісність, тобто в ситуації, в якій інформація була частково або повністю знищена або модифікована;
- порушено доступність інформації, а саме, при непрацездатності системи або при блокуванні доступу;
- втрачено спостережливість або керованість системи обробки, тобто неможливість ідентифікувати користувача і надати йому відповідні повноваження.

Канали витоку інформації можуть утворюватися при експлуатації ПЕОМ або ПК, якщо розглядати ці пристрої як ТЗІ, можна зробити висновок, що вони є вдалим прикладом для ознайомлення за багатьма каналами витоку інформації – від радіоканалу до матеріально-речового. Персональні електронно-обчислювальні машини мають тенденцію повсюдно використовуватися задля оброблення ІзОД, тож буде доречним розгляд принципів, як утворюються канали витоку інформації при використанні персональних обчислювальних машин.

Сучасні персональні обчислювальні машини працюють автономно від інших або у тандемі через комп'ютерні мережі, які поділяються на локальні і глобальні.

Список ділянок, що підлягатимуть захисту даних, виглядає наступним чином:

- оперативна або постійна пам'ять ПЕОМ;
- магнітні, магнітооптичні, лазерні та інші носії;
- зовнішні пристрої зберігання інформації колективного доступу;
- екрани пристроїв відображення;

- пам'ять пристроїв введення та виведення;
- пам'ять керуючих пристроїв і лініях зв'язку, що утворюють канали сполучення комп'ютерних мереж.

Канали витоку інформації утворюються за допомогою:

- електромагнітних полів;
- наведення струмів і напруг в провідних системах;
- випромінювання інформації, що оброблюється на частотах паразитної генерації елементів і пристроїв ТЗ ЕОМ;
- випромінювання інформації, що оброблюється на частотах КВА.

Для освіти додаткових каналів витоку інформації, що навмисно створюються, можна використати наступні пропозиції:

- розмістити в персональних електронно-обчислювальних машинах закладки на мову або оброблювану інформацію;
- інсталювати радіомаячки у персональну електронно-обчислювальну машину;
- умисно застосовувати конструктивно-схемні рішення, що можуть призводити до збільшення електромагнітних випромінювань в певній частині спектра;
- інсталювати закладки, що можуть забезпечити знищення персональної електронно-обчислювальної машини ззовні;
- інсталювати елементну базу, яка виходить з ладу.

Класифікація можливих каналів витоку інформації проводиться на принципах, що забезпечують обробку інформації, джерело якої – можливий канал витоку.

Три типи суб’єктів можуть оброблювати інформацію, а саме:

- людина;
- апаратура;
- програма.

Також канали витоку поділяються на три групи, в залежності від вищеназваних типів обробки. Якщо обробка інформації забезпечується людиною, можуть виникнути наступні можливі канали витоку:

- розкрадання матеріального носія інформації;
- читання або зберігання інформації з екрану сторонньою особою;
- читання або зберігання інформації з залишених без нагляду паперових роздруківок.

Якщо обробка інформації забезпечується апаратурою, можуть виникнути наступні можливі канали витоку:

- підключення апаратних засобів з метою забезпечити доступ до інформації у персональній електронно-обчислювальній машині;
- використання технічних засобів для перехоплення електромагнітних випромінювань технічних засобів персональних електронно-обчислювальних машин.

Якщо обробка інформації забезпечується програмою, можуть виникнути наступні можливі канали витоку:

- НСД до інформації;
- розшифровка зашифрованої інформації;
- копіювання інформації з носіїв;
- відключення або блокування програмних засобів захисту.

Якщо здійснюється перехоплення інформації з персональної електронно-обчислювальної машини, повинен бути здійснений технічний контроль таких каналів витоку інформації:

- побічних електромагнітних випромінювань у діапазоні частот від 10 Гц до 100 МГц;
- наведення сигналів в ланцюгах електроживлення, заземлення і в лініях зв'язку;

- небезпечних сигналів, які можуть утворюватися через електроакустичні перетворення, що відбуваються у спеціальній апаратурі контролю інформації, вони контролюються в діапазоні частот 300 Гц – 3,4 кГц;
- що можуть утворюватися через вплив високочастотних електромагнітних полів на різні дроти у приміщенні, внаслідок чого, перетворитися у прийомну антену, вони контролюються в діапазоні частот 20 кГц – 100 МГц.

Відомо, що дисплей через його склад зі схем, що забезпечують зображення через генерацію сигналів обладнання, є найнебезпечнішим каналом витоку інформації. Відеосистеми містять відеобуфер, який можна уявити як оперативну пам’ять, призначення якої – зберігати текст та графічну інформацію, що виведена на екран. Перетворення даних з відеобуфера у сигнали дисплею, які намагаються перехопити, є основною функцією відеосистеми.

1.3. Класифікація основних засобів протидії загрозам безпеки

Взаємопов’язану сукупність заходів (інженерних, технічних тощо) та засобів захисту інформації для підтримки її захищеності, називають комплексною системою захисту інформації. Захищеність інформації пояснюється такими властивостями:

- доступністю – при наявності повноважень у користувача, є можливість використання певного ресурсу згідно з правилами користування та політикою безпеки;
- конфіденційністю – інформація є приватною, секретною та не має бути розголошена;
- цілісністю – заборона модифікації інформації користувачем, в якого не має відповідних повноважень.

Розглянемо таку властивість системи як спостережливість. Фіксація діяльності користувача та інсталяція ідентифікаторів, що причетні до його процесів, називають спостережливістю. Мета цієї властивості – запобігти порушенню політики безпеки та забезпечити відповідальність у разі порушення.

Комплексом заходів, що спрямовані на швидке рішення завдань для забезпечення захищеності через регламентацію дій персоналу, засобів забезпечення технічного захисту інформації та забезпечення інформаційної діяльності, називають організаційний захист інформації. Він включає в себе наступні заходи:

- розробка довідки для персоналу та юзерів;
- розробка адміністраційних правил інформаційної системи (облік, зберігання, ідентифікація юзерів);
- створення плану дій при виявленні спроби НСД до інформаційної системи або інших надзвичайних ситуацій.

Захист інформації, ціль якого – підтвердити цілісність або справжність, приховати або відновити зміст, попередити несанкціоноване розголошення, та який був реалізований через перетворення інформації за допомогою спеціальних ключів, називається криптографічним захистом інформації.

Забезпечення попередження, шляхом інженерно-технічних засобів, від руйнації або знищення носія інформації через навмисні дії або природний вплив, називається інженерним захистом інформації. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” №80/94-ВР від 05.07.1994 визначає інженерний ЗІ як складову технічного захисту інформації [2].

Призначення технічного захисту інформації – це захистити інформацію від НСД та від витоку техканалами. Для того, щоб забезпечити ТЗІ, створюють комплекс ТЗІ, який є складовою КСЗІ.

НСД до інформації є доступом, який може порушувати політику розмежування доступу у системі. Здійснення НСД можливе як штатними засобами, тобто за допомогою ПЗ, що вже включене до складу системи

адміністратором або розробником, так і за допомогою ПЗ, що були впроваджені у систему зловмисником.

Перелічимо основні способи НСД:

- прямий контакт з об’єктом для отримання доступу;
- використання ПЗ, які звертаються до об’єкту через оминання захисту системи;
- модифікація засобів захисту системи;
- порушення структури або функцій системи за допомогою впровадження в систему апаратних або програмних механізмів.

Програмним, апаратним, або програмно-апаратним засобом, що створений в якості окремого продукту, наділений необхідною документацією та може забезпечити захист системи або контролювати ефективність захисту системи від загроз несанкціонованого доступу, називають засіб технічного захисту інформації від несанкціонованого доступу.

Здійснення захисту від несанкціонованого доступу можливе у наступних складових системи:

- у прикладному та системному програмного забезпеченні;
- в апаратній частині серверу та робочої станції;
- у комунікаційному обладнанні та каналах зв’язку.

Для здійснення захисту від несанкціонованого доступу на прикладному і системному рівнях програмного забезпечення, використовуються системи, які:

- розмежовують доступ до інформації;
- ідентифікують та автентифікують;
- проводять аудит та моніторинг;
- здійснюють антивірусний захист.

Для здійснення захисту від несанкціонованого доступу на апаратному рівні забезпечення використовують системи сигналізації, апаратні ключі та засоби, що блокують пристрої та інтерфейси.

Для здійснення захисту від несанкціонованого доступу в комунікаційних системах, використовують наступні засоби:

- міжмережеві екрани, тобто Firewall – вони використовуються для того, щоб заблокувати зовнішні атаки та забезпечити проходження мережевого трафіка, згідно з правилами захисту. Мають поділ на приватну мережу та мережу із загальним доступом;
- системи, що виявляють втручання, використовуються щоб виявити спроби НСД ззовні та всередині мережі, а також забезпечити захист від DoS та DDoS атак. Через попередження шкідливих дій, ці системи здатні знижувати час простою після атаки і забезпечити зменшення витрат для підтримки працездатного стану мережі;
- засоби, які створюють віртуальні приватні мережі, використовують щоб організувати захищені канали та через них передати дані через незахищене середовище. Вони займаються забезпеченням прозорості сполучення мереж та збереженням конфіденційності та цілісності інформації через динамічне шифрування;
- засоби, які аналізують захищеність, використовуються щоб проаналізувати корпоративну мережу і виявити можливі канали реалізації загроз. Застосовуються для попередження можливих атак на корпоративну мережу, оптимізації витрат на захист та контролю поточного стану захищеності мережі.

Для того, щоб не допустити витік інформації техканалами зв’язку, запроваджується наступний захист:

- використовуються екранований кабель та екрановані конструкції;
- встановлюються високочастотні фільтри на лініях зв’язку;
- будуються екрановані приміщення «капсули»;
- використовується екранованe обладнання;
- встановлюються активні системи зашумлення;
- створюється контрольована зона.

Щоб забезпечити інформаційну безпеку в мережах, необхідно проведення різних заходів, які можна назвати системою захисту інформації. Низку заходів та норм, що спрямовані протидіяти загрозі та мета яких – мінімізувати можливі збитки користувачів і власників систем, називають системою захисту інформації.

Технічними заходами від витоку інформації є наступні заходи:

- захист від НСД;
- важливі комп'ютерні підсистеми мають бути резервованими;
- якщо у окремих ланок порушена працездатність, необхідно організувати обчислювальні мережі з можливістю перерозподілити ресурси;
- інсталяція пожежного устаткування;
- інсталяція сигналізації.

Організаційними заходами від витоку інформації є наступні заходи:

- серверна охорона;
- проведення важливих робіт та заходів двома та більше людьми;
- необхідно мати у наявності план, щодо відновлення сервера у випадку його непрацездатності.

При профілактиці або при ремонті комп'ютера може відбутися НСД до залишків інформації, яка міститься на носіях, шляхом її читання, навіть не зважаючи на те, що вона була видалена користувачем звичайним методом. Така ж ситуація може виникнути при транспортуванні носія без охорони.

При роботі сучасних комп'ютерних засобів, на інтегральних схемах, на яких вони побудовані, змінюються рівні напруги і струму, внаслідок чого, у ланцюгах живлення або у близько розташованій апаратурі, виникають електромагнітні поля та наведення, які з використанням спецзасобів можливо трансформувати в оброблювальну інформацію.

НСД до інформації також можливий при безпосередньому підключенню порушником засобів до мережевих апаратних засобів і каналів зв’язку.

Для захисту від НСД використовують ідентифікацію, аутентифікацію та паролі.

Для забезпечення безпеки інформаційних ресурсів, право на які є у певних осіб або груп осіб, що діють за власною ініціативою або посадовими обов'язками, необхідно виключити можливість НСД та здійснити посилення контролю санкціонованого доступу до ІзОД, а також впровадити системи розпізнавання і розмежувати доступ. Для побудови таких систем використовується принцип допуску та виконання звернення до інформації, яке має певну ознаку повноважень.

В таких системах, ідентифікація та аутентифікація є ключовими чинниками. Ідентифікацією називають об'єкт, якому присвоєно унікальне ім'я або образ. Аутентифікацією називають перевірку того, чи об'єкт відповідає тому, за кого він себе видає.

У випадку позитивного результату перевірки ідентифікації і аутентифікації об'єкта, об'єкт буде допущено до користування інформацією з певними обмеженнями, або без них. Якщо результат перевірки буде негативним, то у допуску буде відмовлено.

Існують наступні об'єкти ідентифікації та аутентифікації:

- людина;
- технічний засіб;
- документ;
- магнітний носій інформації.

Встановити дійсність об'єкту може людина, апаратний пристрій, програма тощо.

Паролем називають певні символи, що в сукупності визначають об'єкт. Необхідно обрати пароль згідно з вимогами щодо розміру, стійкості до добору та наявність певних символів. Зрозуміло, що більша довжина паролю забезпечує вищу надійність, бо для його підбору потрібно більше зусиль та часу. Варто зазначити, що довжина залежить від розвитку технічних засобів та швидкодії.

Гарним досвідом є періодична зміна паролю, для зниження ймовірності перехоплення.

Пароль можна використовувати для ідентифікації та аутентичності терміналу, через який здійснюється вхід у систему користувача, і навпаки, для аутентичності комп'ютера до користувача.

Існують більш складні технічні системи ідентифікації користувача, за їх допомогою ідентифікація здійснюється згідно індивідуальних параметрів людини, а саме:

- відбиток пальця;
- відбиток руки;
- райдужна оболонка очей;
- тембр голосу.

Фізичними методами ідентифікації, які містять у собі носії кодів паролів, є спецперепустки у відповідних системах, картки з магнітною смугою, пластикові картки з особистими даними власника, картки з мікросхемою тощо.

Методи реалізації засобів захисту інформації можуть бути програмними, програмно-апаратними та апаратними.

Розглянемо детальніше програмні засоби захисту інформації, вони можуть бути впроваджені у більшості операційних систем, забезпечують безпеку обчислювальної системи, обмежують доступ згідно паролів, ключів тощо. Перевагою цього типу є помірна ціна та висока ступінь захисту. Однак, якщо підключити цю систему до глобальної мережі, збільшується шанс злому захисту. Отже, для локальних мереж, цей захист цілком прийнятний.

Далі розглянемо програмно-апаратні засоби захисту інформації, це пристрої, в основі яких лежать мікропроцесори. Ці мікропроцесори, в умовах зміни алгоритму функціонування не будуть мати потреби у модифікації в схемотехніці. Також цим пристроям властиво адаптуватися у будь-якій ОС та мати високий рівень захисту. Пристрої цього типу є більш дорожчими, ніж попередній тип, але в той же час є найгнучкішими, можуть змінювати конфігурацію за вимогою замовника та можуть забезпечити високий рівень захисту для локальної мережі яка підключена до глобальної.

Третій тип – апаратний засіб захисту інформації, в пристроях такого типу реалізація функціональних вузлів виконується на надвеликих інтегральних системах з незмінним алгоритмом функціонування. Також цим пристроям властиво адаптуватися у будь-якій ОС, бути найдорожчими у розробці та мати найвищий рівень захисту, через неможливість потрапляння та внесення змін. Отже, висока вартість і статичність алгоритму ускладнює використання таких засобів.

Програмно-апаратні засоби, забезпечуючи легку модифікацію алгоритму функціонування, не маючи недоліків програмних методів, поступаються за швидкістю апаратним засобам.

Також існує окрема група заходів, яка зберігає інформацію, виявляє несанкціоновані запити та порушення у режимі реального часу.

Четвертий тип – криптографічний засіб захисту інформації. За допомогою криптографічних засобів захисту інформації можна:

- створити та проаналізувати надійність криптографічного алгоритму та протоколу;
- адаптувати алгоритми до різної апаратної і програмної платформи;
- в нових прикладних системах використовувати існуючі технології криптографії;
- використовувати технології криптографії для того, щоб захистити інтелектуальну власність.

Сьогодні створюються кросплатформні телекомунікаційні системи на базі єдиних алгоритмічних стандартів, внаслідок чого виникає цікавість відносно досліджень, ціллю яких є адаптувати алгоритми до різних платформ, програмних та апаратних. Один алгоритм має працювати на різноманітних програмних та апаратних платформах: смартфон, смарт-карта, настільний комп’ютер, маршрутизатор тощо.

Ті засоби, що існують у телекомунікаційних мережах для захисту даних, поділяються на асиметричні криптоалгоритми та симетричні криптоалгоритми.

На початку передавання інформації, її стан є відкритим та незахищеним, в процесі передачі здійснюється шифрування та, відповідно, перетворення на шифрограму. Маючи вигляд шифрограми, інформація може передаватися по захищеному або незахищеному каналу зв’язку. Адресат інформації, після її отримання, здійснює процедуру дешифрування через зворотне перетворення криптограми. Як результат, маємо відкриту інформацію, яка доступна для санкціонованого користувача.

У криптографічному перетворенні використовується спеціальний алгоритм, його запуск здійснюється за допомогою унікального числа, так званий шифрувальний ключ. Для успішного обміну зашифрованою інформацією, правильна ключова установка повинна бути у відправника та одержувача та зберігатися у таємниці.

Ступінь секретності для ключа, що використовується у системі зі закритим зв'язком визначає стійкість. Поширюваність ключа має не обмежуватися іншими користувачами мережі, тому що вони також повинні мати можливість вільного обміну зашифрованою інформацією. Таким чином, проблема автентифікації прийнятих даних вирішується криптографічними системами. При перехопленні відправлених даних, зловмисник, матиме лише зашифрований текст, а одержувач, при прийнятті зашифрованих даних, зможе виконати розшифрування та не бути дезінформованим.

Також має місце простіший спосіб шифрування даних – це спосіб, в основі якого лежить використання генерації псевдовипадкових чисел. Він полягає у тому, щоб згенерувати гаму шифру маючи певний ключ і накласти отриману гаму на відкриту інформацію через оборотний спосіб. Реалізація такого методу легко здійснюється та може забезпечити швидке шифрування, але є недолік – недостатня стійкість методу до дешифрування.

Класична криптографія використовує одну секретну одиницю – ключ, який забезпечує шифрування інформації від відправника, а отримувач її розшифровує. Якщо дані знаходяться на магнітних або інших носіях, то ключ може забезпечити

шифрування інформації під час запису на носій, а також здійснити розшифрування у разі читання з нього.

Можна зробити висновок, що надійна криптографічна система повинна забезпечувати:

- прозорість шифрування і розшифрування для користувача;
- максимальне ускладнення процедури дешифрування закритих даних;
- відсутність позначення змісту переданих даних на ефективності криптографічного алгоритму.

Асиметричні системи або системи з відкритим ключем мають сьогодні високу перспективу та полягають у ключі, який використовується для шифрування, який є відмінним відносно розшифрувального ключа, а також може бути відомим для всіх користувачів системи. Розшифровуваний ключ є секретним та шифрувального не дозволить визначити секретний розшифровуваний. Такі системи більше використовуються для шифрування інформації, що передається, ніж для захисту інформації, яка зберігається на носіях інформації.

Криптографія забезпечує безпеку даних в інтернеті та наразі активно впроваджуються необхідні криптографічні механізми в цю мережу. Широке використання криптографії і глобальних інформаційних мереж є досягненням сучасного світу.

1.4. Нормативно-правова база робіт по створенню КСЗІ

Нормативний документ про «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» НД ТЗІ 3.7-003-05, свідчить про те, що процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і

впровадження інформаційної технології, яка забезпечує обробку інформації в інформаційно-телекомунікаційній системі (ІТС) згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами (НД) у сфері захисту інформації. Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС. Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо. Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження господарської діяльності у сфері захисту інформації [16].

Отже, завдяки аналізу Законів України визначаємо вимоги до захисту та види ІЗоД, окреслюємо види загроз на об’єктах інформаційної діяльності, та досліджуємо способи та засоби захисту інформації такі як: захист від НСД та захист витоку технічними каналами шляхом реалізації КТЗІ.

2 КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Обґрунтування необхідності створення КСЗІ

Необхідність створення комплексної системи захисту інформації підпорядковується власнику цієї інформації, при умові надання відповідного права нормативно-правовими актами, або ж законодавчим нормам і вимогам, котрі обов’язково обмежують доступ до деяких видів даних або забезпечують її цілісність та доступність.

Для того, щоб обґрунтувати необхідність створення комплексної системи захисту інформації, потрібно використовувати результати проведених оцінювань та аналізів, а саме:

- обмежити доступ до деяких видів даних, заборонити таке обмеження або визначити необхідність захисту відповідно інших критеріїв, підставою для цих дій слугує аналіз нормативно-правових актів;
- визначити наявність видів у складі автоматизовано оброблювальної інформації, доступ до яких може бути обмежений або забезпечена цілісність чи доступність, згідно вимогам нормативно-правових актів;
- оцінити можливі переваги використання інформаційно-телекомунікаційних систем при створенні комплексної системи захисту інформації.

Згідно з результатами аналізу і оцінювання робиться висновок про доцільність розробки КСЗІ.

Категоріювання здійснюється в об'єктах, в яких циркулює ІзОД, а саме:

- в автоматизованих системах та засобах обчислювальною техніки, під час дії та проектування;

- у технічних засобах, призначення яких – це робота з ІзОД та які не відносяться до автоматизованих систем, як виняток, засоби засновані на криптографічних методах захисту;
- у приміщеннях з розміщеними автоматизованими системами, пристроями, іншими технічними засобами, призначеними для роботи з ІзОД, включаючи засоби засновані на криптографічних методах захисту.

Категоріювання проводиться з метою вживання обґрунтованих заходів щодо технічного захисту ІзОД, яка циркулює на об`єктах, вид витоку каналами побічних електромагнітних випромінювань й наводок, а також акустичних (віброакустичних) полів [7].

2.2. Категоріювання ОІД

АКТ № 11

«категоріювання кімнати №101 для роботи з інформацією з грифом «цілком таємно»

3.09.16 м. Київ

Комісія в складі:

голова Махно Д. М. – начальник

члени: Пирогов С. С. – нач. РСО

Іванов А. С. – зам. нач. РСО

Призначена наказом №1 від 14.04.2016 провела категоріювання кімнати для нарад № 101.

Через те, що система технічного захисту інформації для конкретного об'єкту інформаційної діяльності була вперше розроблена і впроваджена, проводиться

категоріювання. Комісією було розглянуто та проаналізовано ситуаційний та генеральний плани, схеми електроживлення та схеми комунікацій, які виходять за межі контрольованої зони.

Комісією було встановлено:

1. Кімната для роботи з інформацією №101, циркулює наступна інформація:

1.1 Мовна, тобто та, яка лунає у випадку розмови співробітників підприємства. Гриф обмеження доступу – таємно.

1.2 Інформація, яка міститься у персональній електронно-обчислювальній машині. Гриф обмеження доступу – цілком таємно

2. Приміщення з циркуляцією інформації з обмеженим доступом в момент розмови співробітників підприємства, має бути присвоєно другу категорію.

3. У наявності всі нормативні документи технічного захисту інформації

Додатки:

1. Ситуаційний план
2. Генеральний план
3. Схеми комунікацій, які виходять за межі комплексу захисту
4. План розташування основних технічних засобів та допоміжних технічних засобів системи на об’єкті інформаційної діяльності

Кількість примірників - 1

Комісія в складі:

голова	Махно Д. М. – начальник РСО	_____
члени:	Пирогов С. С.	_____
	Іванов А. С. – зам. нач. РСО	_____

2.3. Обстеження середовищ функціонування ІТС

Щодо характеристики обчислювальної системи, обчислювальна система АС-2 складається з наступних компонентів:

- дві персональні електронно-обчислювальні машини, до комплекту яких входять: клавіатура, комп’ютерна миша, монітор та кабелі живлення;
- один ПК Office AMD Plus Блок системний "FORWARD-office" AMD Sempron X4 3850 (1.3 ГГц) / ОЗУ 4 Gb / НЖМД 320 Gb / Radeon R3 int / LAN / 400W / ОС XP.

Щодо характеристики фізичного середовища, план контрольованої зони будівлі 22 по вул. Лобановського. Інв. № 45 від 3.11.2016 визначає контрольовану зону АС-2.

Адреса АС-2: м. Київ, вул. Лобановського, 22.

Акт обстеження детальніше визначає фізичне середовище і буде розглянутий в наступному пункті.

Щодо характеристики середовища користувачів, поділ суб’єктів доступу до АС-2 здійснюється за двома категоріями: присутність доступу до даних та відсутність доступу до даних. Цей поділ здійснюється згідно рівню повноважень відповідно роботам, які виконуються на АС-2.

Технічний персонал, а саме системний адміністратор, який забезпечує працездатний стан системи, відноситься до категорії суб’єктів, які обслуговують кімнату №101 та не мають доступ до ресурсів АС-2.

Для системних адміністраторів існує інструкція, згідно якої виконуються його обов’язки, а саме «Інструкція системного адміністратора автоматизованої системи», також його дії обмежуються згідно рамок організаційних обмежень, які встановлені роллю, що йому призначена. Контролем виконання цих обов’язків займається адміністратор безпеки.

Доступ суб’єктів до ресурсу АС-2 здійснюється за певними умовами:

персонал отримує доступ виключно при адміністраторі безпеки або іншої відповідальної особи;

користувач отримує доступ до інформації з обмеженим доступом виключно при необхідності, та тільки якщо користувач виконує покладені на нього обов’язки.

Функціонування АС-2 можливе у таких режимах:

1) Основний режим – є дозвіл на доступ користувача та обробку інформації з обмеженим доступом;
2) Службовий режим – при ньому може виконуватися технічне обслуговування, а доступом наділений лише адміністратор безпеки.
3) Аварійний режим – доступ є виключно у персоналу автоматизованої системи.

До характеристики персоналу та користувачів автоматизованої системи входять: кількість користувачів і категорії користувачів, форми допуску тощо.

Повноваження та права доступу до інформації, що зберігається та циркулює, визначають такі ролі:

- адміністратор баз даних;
- адміністратор безпеки ІТС;
- оператори;
- обслуговуючий персонал.

2.4. Акт обстеження об’єкту інформаційної діяльності

Для службового користування

Прим. № 1

ЗАТВЕРДЖЕНО

Ген. Дир.

Сергєєв А.С.

01.11.2016

АКТ

обстеження на об’єкті інформаційної діяльності

ТОВ «Рубін» вул. Лобановського 22

(назва, належність об'єкта інформаційної діяльності)

1. Обстеження на ОІД проведено 29.09.2016 р. комісією у складі: голова комісії Махно А.С , члени: Пирогов В.Д., Іванов С.С.

2. Характеристика ОІД.

ОІД – приміщення, що розташоване на 1 поверсі адміністративного будинку за адресою: м. Київ вул. Лобановського 22. Межі контрольованої зони об’єкта (див. рис 1) співпадають із контрольованою зоною, у якому розташований ОІД.

3. Характеристика складових ОІД

У приміщенні ТОВ «Рубін» виконується обробка інформації, яка є державною або іншою таємницею, що передбачена законом, а також конфіденційної інформації, якою володіє держава, або захист якої передбачено законом (інформації з обмеженим доступом). Обробка інформації відбувається у режимі реального часу.

Архітектурно-будівельними особливостями приміщення є:

- товщина стін 400 мм;
- в приміщені розташовано дерев’яні двері.

У суміжних приміщеннях ІзОД не циркулює. В суміжних приміщеннях, та в будинку без належного контролю не працюють іноземні громадяни, неконтрольоване перебування сторонніх осіб унеможливлено.

Складові об’єкта інформаційної діяльності, які впливають на ефективність захисту інформації з обмеженим доступом, а також які є середовищем поширення носіїв цієї інформації за межі контрольованої зони:

- система заземлення підключення до місцевої мережі і знаходяться у мережі контрольованої зони;
- система опалення автономне і знаходиться у межах контрольованої зони.

4. Електроживлення – знижувальна трансформаторна підстанція, від якої живляться ОТЗ і ДТЗС, знаходиться за межами контрольованої зони.

5. За результатами аналізу, в установі наявні:

- затверджена схема контрольованої зони в межах якої розташований об’єкт інформаційної діяльності;
- дані про можливі місця розміщення зовні контрольованої зони засобів технічної розвідки тривалого перехоплення зазначені в окремій моделі загроз для об’єкта інформаційної діяльності.

6. Дані щодо терміну проведення категоріювання об'єктів та подання на затвердження актів із категоріювання.

Акт категоріювання ОІД ТОВ кімната №201 «Рубін» вул. Лобановського 22.

голова комісії	Махно А.С.	_____
члени:	Пирогов В.Д.	_____
	Іванов С.С.	_____

2.5. Політика інформаційної безпеки

Визначення норм, правил та обмежень використовування елементів ІС здійснюється політикою безпеки, яка є механізмом управління ІС.

Відповідальність за безпеку інформації завжди несе керівник організації.

У керівника є можливість призначити конкретного працівника відповідальним за безпеку окремого елементу ІС.

Кожен працівник повинен бути ознайомлений з даним документом та дотримуватися усіх правил, вимог і обов’язків.

Політика безпеки покриває виключно обов’язкові та загальні положення безпеки. Згідно обов’язків, посадових інструкцій та практичних навичок і досвіду,

вирішуються всі деталі персоналом організації, наприклад, використання шифрування або ПЗ, наділення правами доступу працівників тощо.

2.6. Модель загроз інформаційній безпеці

Таємно

МП

«___» _____2016 р.

ТОВ ”Рубін”

(ПРИМІЩЕННЯ № 101)

МОДЕЛЬ ЗАГРОЗ

для інформації з обмеженим доступом, яка циркулює на об’єкті інформаційної діяльності

2016

Таблиця 2.1

Зведена таблиця моделі загроз інформації АС класу 2

№ п/п	Перелік суттєвих загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз	Наслідки (порушення властивостей)			
				К	Ц	Д	С
1	Вихід з ладу технічних засобів	Персонал, користувачі ТЗ, сторонні особи, які отримали несанкціонований доступ	Фізичний НСД до обладнання, що захищається		+	+	
2	Порушення фізичної цілісності АС 2	Персонал, користувачі, сторонні особи, ТЗ	Фізичний НСД до обладнання, що захищається		+		
3	Порушення режимів функціонування АС 2	Персонал, користувачі, сторонні особи, ТЗ	Фізичний НСД до обладнання, що захищається, застосування ЗП, програм, комп'ютерних вірусів		+		
4	Читання "сміття" (залишкової інформації з запам'ятовуючих пристроїв, магнітних аудіо касет)	Персонал, користувачі, сторонні особи, ТЗ, ПЗ	НСД до МНСІ або оперативної пам'яті сторонніх осіб, застосування ЗП, програм	+			
5	Читання даних, які виведені на екрані або роздруковані, встановлення мікро аудіо-відео записуючих пристроїв, читання друкованих документів, які залишені без догляду	Користувач відвідувач, персонал, стороння особа	Стороння особа, яка знаходиться у службовому приміщенні	+	+	+	+
6	Використання технічних пристроїв без санкціонованого узгодження	Користувач відвідувач, персонал, стороння особа	Фізичний НСД до обладнання, що захищається	+	+	+	+
7	Копіювання документів, магнітних та інших носіїв інформації без санкціонованого узгодження	Користувач відвідувач, персонал, стороння особа	НСД до МНСІ , подолання заходів захисту, застосування ЗП, комп'ютерних вірусів	+			

Продовження таблиці 2.1

8	Використання персоналу АС з корисливою метою	Користувач відвідувач, персонал, стороння особа	Шантаж, підкуп	+	+	+	+
9	Отримання атрибутів доступу та їх подальшим використанням для маскування під зареєстрованого користувача (“маскарад”)	Персонал, користувачі, відвідувачі, сторонні особи	Застосування ЗП, підглядування процесу реєстрації, використання вад систем захисту	+	+	+	+
10	Впровадження і використання забороненого ПЗ або несанкціоноване використання ПЗ, за допомогою якого отримується доступ до критичної інформації	Персонал, користувачі, відвідувачі, сторонні особи, ПЗ	Фізичний НСД до обладнання та ПЗ, подолання заходів захисту	+	+	+	+
11	Впровадження і використання комп’ютерних вірусів	Персонал, користувачі, відвідувачі, сторонні особи, ПЗ	Фізичний НСД до обладнання та ПЗ, подолання заходів захисту	+	+	+	+

2.7. Модель порушника інформаційної безпеки

Порушник є особою, яка використовує певні інструменти (методи) для здійснення спроби виконання дій, що призводять до порушення певних властивостей інформації, які визначає політика безпеки. Можливості, знання, час та місце дії відображає модель порушника.

У випадку автоматизованої системи, порушники поділяються на наступні типи:

- внутрішні (персонал, користувачі);
- зовнішні (сторонні особи).

Збитки, які можуть бути нанесені порушниками можуть бути:

- незначними;

- значимими, але, здебільшого, припустимими;
- середніми;
- дуже значними.

За рівнем володіння інформацією про АС класу 2, порушники:

- І – знають функціональні особливості засобів обчислювальної техніки, основи формування запитів до масивів даних та масивів у цілому, можуть використовувати штатні засоби;
- ІІ – мають поглиблені знання та досвід у сфері технічних засобів АС та їх обслуговування;
- ІІІ – мають поглиблені знання у сфері програмування, обчислювальної техніки і використання АС.
- IV – знають механізм дії та функції засобів захисту в АС.

Порушники за показниками використання методів і способів отримання ІзОД та інформації про АС класу 2:

- І рівень – використання тільки агентурних методів отримання відомостей;
- ІІ рівень – використання пасивних технічних засобів перехоплення інформаційних сигналів;
- ІІІ рівень – використання тільки штатних засобів АС або недоліків проектування системи захисту для реалізації НСД до інформації з обмеженим доступом;
- IV рівень – використання способів і засобів активного впливу на автоматизовану систему другого класу, зі зміною конфігурації системи (підключення, модифікація засобів, спеціальне ПЗ).

Місця здійснення порушення:

- І рівень – без доступу до території;
- ІІ рівень – з доступом до території;
- ІІІ рівень – з доступом до робочого місця автоматизованої системи другого класу;

- IV рівень – з доступом до масивів (носіїв) накопичення та зберігання ІзОД;
- V рівень – з доступом до засобів адміністрування і захисту інформації автоматизованої системи другого класу.

Розглянемо опис методів та способів здійснення несанкціонованого доступу до інформації з обмеженим доступом. НСД до ІзОД може здійснюватися:

1) сторонніми особами (відвідувачами), які знаходяться на території учбового корпусу та здійснюють злочинні дії. При цьому вірогідна можливість їхнього оснащення найсучаснішими переносними засобами для несанкціонованого одержання інформації:
2) співробітниками ОІД при здійсненні ними ненавмисних дій при виконанні робіт, які мають зв’язок з виконавчою діяльністю.

Для кожної з загроз визначено:

- на які властивості інформації (конфіденційність, цілісність, доступність) або автоматизованої системи (спостережливість, керованість), спрямована загроза;
- джерела виникнення загрози;
- способи здійснення загрози.

Існують наступні критерії для аналізу порушників:

- мотив;
- рівень кваліфікації стосовно автоматизованої системи;
- можливість використовувати засоби та методи подолання системи захисту;
- специфікація моделі порушника за часом дії;
- специфікація моделі порушника за місцем дії;
- сумарний рівень загрози.

Кожен критерій оцінюється за 4-бальною шкалою та підсумовується в кінці.

2.8. Технічне завдання на створення КСЗІ

УЗГОДЖЕНО

…….

М.П.

«____»_____20__р.

ЗАТВЕРДЖУЮ

…….

М.П.

«____»_____20__р.

АВТОМАТИЗОВАНА СИСТЕМА

ТОВ РУБІН

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

АС - 2

Технічне завдання

Київ – 2016

ЗМІСТ

1. Терміни та визначення
2. Загальні відомості
3. Мета і призначення КСЗІ
4. Загальна характеристика автоматизованої системи
5. Вимоги до КСЗІ
5.1. Загальні вимоги
5.2. Вимоги до функціональних послуг
5.3. Вимоги до гарантій
5.4. Вимоги до комплексу технічного захисту інформації від витоку технічними каналами
6. Етапи виконання робіт

1. Терміни та визначення

Технічне завдання передбачає використання термінів та визначень згідно з ДСТУ 3396.2-97, ДСТУ, НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [19].

У технічному завданні визначаються вимоги та технічні заходи до забезпечення захисту інформації в АС ТОВ Рубін. Умовне позначення – АС2, замовником є ТОВ Рубін, виконавцем є ТОВ КРИПТОН, джерелом фінансування роботи є рахунок ТОВ Рубін

2. Загальні відомості

Повною назвою роботи є «Розробка комплексної системи захисту інформації в автоматизованій інформаційній системі ТОВ Рубін».

Шифром роботи є КСЗІ ТОВ Рубін.

Підприємство–розробник підсистеми та реквізити: ТОВ Криптон, Рахунок: ЄГРПОУ: 44275534, IBAN: UA213223130000026007233566001.

Спеціальний дозвіл на впровадження діяльності з державною таємницею, від 2016 року, №35, є дійсним до 2024 року.

Ліцензія серія ВА № 54563 Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України або Державної Служби спеціального зв’язку та захисту інформації України.

Підприємство–замовник підсистеми та реквізити: ТОВ Рубін, Рахунок: ЄГРПОУ: 44364987, IBAN: UA213223130457767253804827634.

Терміни початку і закінчення роботи зі створення КСЗІ:

Початок – 10.10.2016 року.

Закінчення – 15.10.2016 року.

3. Мета і призначення КСЗІ

Мета: забезпечити безпеку для інформації в момент її обробки засобами автоматизованої системи, забезпечення захисту повинно здійснюватися на кожному технологічному етапі обробки і в кожному режимі функціонування.

Обробка інформації здійснюється за допомогою наступних кроків:

- отримання інформації від ТОВ Рубін та її збереження у локальних БД;
- використання накопиченої інформації ТОВ Криптон;
- обмін даними між локальними автоматизованими системами через канали кабельної системи.

Для того, щоб забезпечити безпеку даних на кожній із стадій життєвого циклу автоматизованої системи, КСЗІ використовує наступні заходи та засоби захисту:

- реалізація за межами обчислювальної системи АС-2 організаційних заходів;
- захист від НСД шляхом програмно-апаратних засобів;
- забезпечення відсутності витоку даних технічними каналами;
- захист інформації під час операцій у каналах зв'язку.

Комплексна система захисту інформації в автоматизованій системі призначена для того, щоб:

- забезпечити відсутність витоку ІзОД технічними каналами;
- керувати доступом користувачів АС-2;
- розмежовувати доступ користувачів АС-2 в залежності від категорії конфіденційності;
- блокувати несанкціоновані дії з критичною інформацією;
- створити багаторівневий захист від атак даних АС-2.

Нормативно-правовою базою щодо захисту інформації та створення КТЗІ АС-2 є Закони України "Про інформацію", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах" [2].

Державними стандартами є:

- ДСТУ 3396.0-96. Технічний захист інформації. Основні положення [17].
- ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт [18].

4. Загальна характеристика автоматизованої системи

Автоматизувати обробку інформації оброблення матеріалів у галузі військового текстилю є призначенням автоматизованої системи.

Найвищим грифом інформації, який буде оброблений засобами автоматизованої системи і буде передаватися через канали зв'язку, – цілком таємно. При грифі «цілком таємно», інформація обробляється постійно.

База даних є інформаційним ресурсом автоматизованої системи. У складі автоматизованої системи функції збору, обробки, передачі і накопичення інформації вирішують завдання для того, щоб забезпечити базу даних.

Організація інформаційних зв'язків автоматизованої системи виконується наступним чином, автоматизована система бере на себе і під контроль усі потоки даних, які виходять від бази даних та мають залежність від даного рівня управління.

База даних – це джерело інформації для автоматизованої системи.

До базових елементів автоматизованої системи відносяться автоматизовані робочі місця, які повинні забезпечити постачання упорядкованої первинної інформації для бази даних.

Технічні засоби автоматизованого робочого місця функціональних вузлів можуть цілодобово працювати без вимкнення живлення, а саме вісім годин на добу. Стандартне ПЗ автоматизованого робочого місця містить у собі мережеву операційну систему Windows 10 та СКБД Microsoft Excel.

5. Вимоги до КСЗІ

5.1. Загальні вимоги

Архітектура автоматизованої системи дозволяє розв'язати функціональні завдання в замкненому середовищі. Мінімальний час передавання критичних даних між локальними сегментами мережі має забезпечуватися структурою мережі та розподілом потоків інформації.

Виключно функціонування СЗІ забезпечує можливість роботи автоматизованої системи у штатних режимах.

При розташуванні, монтажі та прокладенні інженерно-технічних комунікацій автоматизованої системи, потрібно дотримуватися вимог, які

розписані у відповідних стандартах та нормативних документах системи технічного захисту інформації.

Виявлення потенційних загроз інформаційній безпеці – є першим етапом робіт, який відноситься до організаційних і підготовчих заходів стосовно створення комплексу технічного захисту інформації.

Технічні засоби, приміщення та системи забезпечення діяльності автоматизованої системи мають бути обстежені. При обстеженні обов’язково має бути:

- виконання робіт щодо знаходження можливих джерел витоку даних через роботу засобів перетворення, а саме обробка, відображення, зберігання даних і допоміжних систем і засобів;
- розгляд ланок передачі даних, ланок електроживлення, сигналізації та керування тощо, як джерел витоку інформації з обмеженим доступом;
- досліджені засоби обчислювальної техніки в яких циркулює інформація з обмеженим доступом, на наявність в них технічних каналів витоку даних за допомогою ПЕМВН.

До неформалізованої моделі загроз для даних, при розробці якої враховувалися результати обстеження, повинна включати в себе:

- план із розташуванням структурних елементів автоматизованої системи, в якому зазначені місця, де розташовані технічні засоби, системи обробки даних та інженерні комунікації, які знаходяться за межами зони безпеки;
- опис можливих технічних каналів витоку даних та опис впливу на них;
- опис можливого способу реалізації НСД до даних;
- оцінювання можливих збитків при реалізації загрози.

Для того, щоб реалізувати частину політики безпеки даних, які покладаються на технічні заходи та відповідають моделі загроз, у комплексі засобів захисту необхідно:

- забезпечити вхід до системи та завантажити операційну систему виключно після того, як користувач пред’явив електронний ідентифікатор або ввів особистий пароль;
- контролювати введення даних в автоматизовану систему та встановлення ПЗ;
- контролювати виведення інформації на носії які вилучаються;
- підтримувати функції адміністратора захисту даних в автоматизованій системі;
- реєструвати дії користувачів відносно ресурсів системи;
- забезпечити цілісність даних;
- перевіряти цілісність та працездатність комплексу технічного захисту інформації;
- автоматично блокувати екран робочої станції, якщо користувач відійшов;
- розмежувати на багато рівнів повноваження персоналу автоматизованої системи відносно ресурсів автоматизованої системи;
- контролювати запуск процесів та їх виконання;
- у невідведений час заборонити роботу зареєстрованих користувачів;
- шифрувати інформацію, аутентифікувати повідомлення та підтверджувати проходження повідомлень у випадку передачі каналами зв’язку.

Виконувати завдання повинні зареєстровані користувачі, знаходячись у функціонально замкненому середовищі де має бути доступ до ресурсів, які обмежуються рамками завдань.

На автоматизованому робочому місці ПЗ користувача не може обійтись без програмних модулів захисту, які взаємодіють із сервером захисту для того, щоб реалізувати функціональні послуги безпеки.

Для того, щоб керувати комплексом технічного захисту інформації у складі автоматизованої системи, у адміністратора безпеки має бути передбачено

автоматизоване робоче місце. До складу віддалених сегментів автоматизованої системи, мають включатися такі ж самі автоматизовані робочі місця. Розташування автоматизованих робочих місць має бути із дотриманням організаційних заходів у спеціальних приміщеннях.

Комплексна система захисту інформації має здійснювати забезпечення підтримкою не менше 3 категорій таємності інформації, не менше 5 рівнів повноважень користувачів та роботи не менше 3 користувачів.

Реалізація КСЗІ має бути сукупністю узгоджених організаційних та технічних заходів. Організаційні заходи повинні:

- визначати та встановлювати обов’язки захисту даних осіб і підрозділів, які займаються обробкою інформації;
- визначати технологічні процеси обробки даних, враховуючи вимоги захисту інформації;
- встановити порядок модернізації та впровадження засобів обробки даних, а також засобів захисту цих даних;
- організувати фізичний та протипожежний захист автоматизованої системи;
- розробити правила та порядок контролю функціонування комплексу технічного захисту інформації.

5.2. Вимоги до функціональних послуг

Комплекс засобів захисту комплексу технічного захисту інформації установи ТОВ Рубін згідно вимогам НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" повинен реалізовувати наступний профіль захищеності інформації:

2.КЦД.4 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2} [22].

5.3. Вимоги до гарантій

Відповідно рекомендаціям документу "Технічне завдання на створення типової комплексної системи захисту інформації" рівень гарантій реалізації

визначеного функціонального профілю захищеності АІС установи ТОВ Рубін має бути не нижчим за Г4 (згідно з вимогами НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу») [21].

Вимогами до гарантій архітектури комплексу засобів захисту є:

- добре визначені і максимально незалежні компоненти мають бути складовими комплексу захисту інформації;
- принцип мінімуму повноважень має бути в основі проектування кожного з компонентів;
- принцип відкритих систем має бути в основі побудови архітектури комплексу захисту інформації, яка повинна передбачити можливість реалізації додаткових послуг безпеки даних у частині НСД.

Вимогами до гарантій середовища опрацювання є:

- розробка та впровадження розробником документованих методик, згідно яких буде здійснюватися управління конфігурацією КЗЗ автоматизованої системи;
- забезпечення внесення змін в ПЗ і документацію – мета системи управління конфігурацією;
- розробка додаткових програмних засобів захисту повинна здійснюватися з використанням сучасних засобів розробки та сучасних і документованих мов програмування під ОС Windows;
- здійснення керування конфігурацією має відбуватися базовими версіями – це версія комплексу засобів захисту, зміна якої можлива виключно через формальні процедури зміни;
- керуванню підлягають програмні засоби, налаштування та документація комплексу засобів захисту;
- внесення змін до елементів конфігурації повинно відбуватися в результаті приймання етапів робіт зі створення комплексу технічного

захисту інформації, відповідно організаційним документам, які були узгоджені.

Вимогами до гарантій середовища функціонування є:

- надання розробником засобів інсталяції, генерації та запуску комплексу засобів захисту, які можуть гарантувати початок експлуатації із безпечного стану;
- опис необхідних налаштувань та параметрів конфігурації, під час розробки комплексу засобів захисту, що дозволять почати з безпечного стану.

Вимогою до гарантій експлуатаційної документації на комплекс засобів захисту є необхідність включення загального опису комплексу засобів захисту, настанови користувача та адміністратора, а також експлуатаційної документації виробників на покупні продукти, які є у складі комплексу засобів захисту.

Вимогою до гарантій випробувань комплексу засобів захисту є необхідність утримання у собі процедур перевірки усіх послуг безпеки, що заявлені.

5.4 Вимоги до комплексу технічного захисту інформації від витоку технічними каналами

Витік даних технічними каналами витоку можливий через побічні електромагнітні випромінювання та наведення, а також каналів: акустичного і візуально-оптичного.

Вимогами до системи електроживлення автоматизованої системи є:

- трансформаторна підстанція низької напруги, яка розміщена у межах КТ, повинна здійснювати електроживлення установи ТОВ Рубін. Розділовий трансформатор здійснює електроживлення, якщо трансформаторна підстанція знаходиться за межами КТ;
- віддаленість побутової та освітлювальної мереж від мережі електроживлення установи ТОВ Рубін, яка повинна забезпечити безперебійність та працездатність ТОВ Рубін;
- здійснення електроживлення через протизавадні мережеві фільтри.

Вимогами до кіл заземлення автоматизованої системи є:

- заземлення всіх металевих конструкцій;
- відсутність у системи заземлення виходу за межі КТ;
- не перевищування 2 Ом опором кіл заземлення від засобів ТОВ Рубін до вузлів системи заземлення.

Проведення спеціальних досліджень ОІД забезпечує конкретизацію засобів та заходів захисту інформації від витоку інформації технічними каналами (табл. 2.2).

6. Етапи виконання робіт

Таблиця 2.2

Етапи виконання робіт

№ п/п	Назва етапу та роботи проведені згідно етапу	Термін	Чим закінчується робота
1	Попередній етап	Відповідно умовам договору	
1.1	Проводиться обстеження об’єкта інформаційної діяльності		Актом обстеження об’єкта інформаційної діяльності
1.2	Визначаються перелік загроз і можливі канали витоку даних		Моделлю загроз
1.3	Визначаються вимоги до комплексу технічних засобів захисту для захисту від несанкціонованого доступу та витоку технічними каналами		Розділами ТЗ на створення комплексної системи захисту інформації
2	Етап проектування і розробки комплексу технічних засобів захисту	Відповідно умовам договору	
2.1	Проектується комплекс технічних засобів захисту		Вибором проектних рішень
2.2	Розробляється техніко-робоча та експлуатаційна документація		Проектною та експлуатаційною документацією на комплекс технічних засобів захисту

Продовження таблиці 2.2

2.3	Виконуються роботи із захисту інформації від витоку каналами ПЕМВН		Протоколами спеціальних досліджень та приписами на експлуатацію
2.4	Налаштовуються сервіси безпеки операційної системи Windows		Виконанням налаштувань відповідно експлуатаційним документам. Протоколом приймання робіт
2.5	Розроблюється організаційна документація і впроваджуються організаційні заходи захисту		Розробленими та впровадженими організаційними документами та заходами захисту
2.6	Розроблюються програми та методики випробувань комплексної системи захисту інформації		Програмою та методиками випробувань
3	Етап випробувань і передачі комплексу технічних засобів захисту в експлуатацію	Відповідно умовам договору	
3.1	Організовуються і проводяться попередні випробування комплексної системи захисту інформації		Протоколами попередніх випробувань, актом про приймання комплексної системи захисту інформації в дослідну експлуатацію
3.2	Навчання користувачів		Програмою навчання користувачів Актом про завершення навчання
3.3	Організовується та проводиться дослідна експлуатація комплексної системи захисту інформації		Журналами дослідної експлуатації, актом завершення дослідної експлуатації
3.4	Подається заявка на проведення державної експертизи		Заявкою на проведення державної експертизи
4	Державна експертиза комплексної системи захисту інформації	Відповідно окремого договору	Атестатом відповідності

Висновок по розділу: при обстеженні ОІД визначено, що інформація яка буде оброблятись становить державну таємницю. Розроблено згідно вихідних даних, модель можливих загроз та модель вірогідних порушників. На підставі

отриманих документів формуємо технічне завдання на побудову КСЗІ. За результатом створення подаємо заявка на експертизу, після схвалення та проведення експертизи отримуємо атестат відповідності.

3 ОБҐРУНТУВАННЯ ТА ВИБІР ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В АС-2

3.1. Захист від витоку технічними каналами

Для захисту інформації від витоку колами живлення однофазної мережі застосовано фільтр мережевий М-13 ТУ У 30267382.003-99. Кількість каналів фільтрації - 2. Номінальний струм не більше 5 А

1. Призначення виробу.

1.1. Мережевий фільтр (МФ) типу “М-13” призначений для захисту інформації від витоку колами живлення постійного та змінного струму основних і допоміжних технічних засобів обробки інформації.

2. Технічні характеристики.

2.1. Номінальна робоча напруга, не більше 250В.

2.2. Номінальний струм навантаження, не більше 5А.

2.3. Затухання в смузі частот:

- затухання лінійно зростає від 3 дБ до 65 дБ на частотах від 5 кГц до 150 кГц;
- затухання лінійно зростає від 65 дБ до 135 дБ на частотах від 150 кГц до 630 кГц;
- затухання не менше 110 дБ на частотах від 630 кГц до 1000 МГц;

2.4. Втрата напруги 220В, 50Гц при робочому струмі, не більше 3В.

2.5. Кількість проводів – 2.

2.6. Маса, не більше 4,9 кг.

2.7. Габаритні розміри – 320*140*55

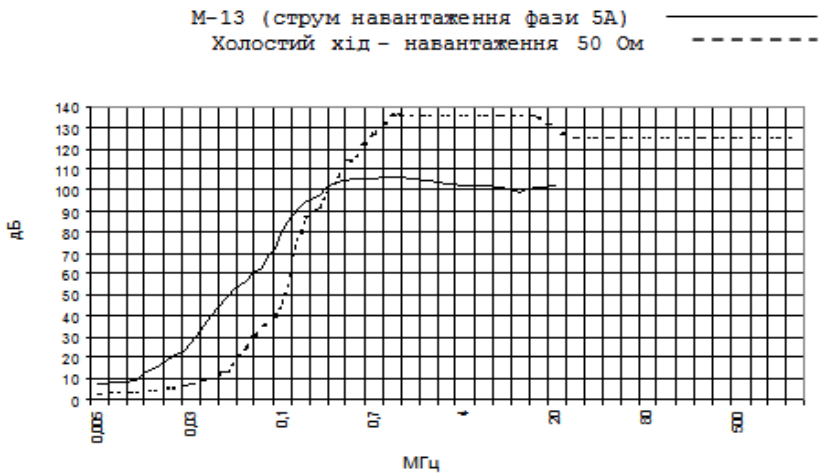

Рис. 3.1. АЧХ фільтру М-13 ТУ У 30267382.003-99

Для забезпечення захисту інформації від витоку через ПЕМВ застосовано генератор радіозавад "ЛГШ-501".

Рис. 3.2. Генератор ЛГШ 501

Цей генератор радіозавад призначений для того, щоб працювати у складі САЗ, що обробляється на об'єктах ЕВТ до 1 категорії включно. САЗ може забезпечити захист інформації від витоків по каналах ПЕМВН за допомогою створення широкополосного шумового електромагнітного перепаду в діапазоні частот від 0,01 до 1800 МГц.

Принцип роботи системи активного захисту базованої на генераторі ЛГШ-501:

Створюється на межі КЗ шумова перешкода, яка зашумляє побічні випромінювання захищеного об'єкта.

Живлення ЛГШ-501 відбувається мережею змінного струму напругою 220В і частотою 50Гц. Прилад може використовуватися цілодобово.

Увімкнення / вимкнення режиму генерації перешкод здійснюється кнопкою "Сеть" на задній панелі пристрою.

Таблиця 3.1.

Технічні характеристики.

Уровень сигнала на выходных разъемах генератора в диапазоне частот	
• 10–150 кГц с полосой пропускания 200 Гц	не менее 65 дБ
• 0,15–30 МГц с полосой пропускания 9 кГц	не менее 85 дБ
• 30–1000 МГц с полосой пропускания 120 кГц	не менее 70 дБ
• 1–1,8 ГГц с полосой пропускания 120 кГц	не менее 60 дБ
Количество телескопических антенн	2 шт
Длина телескопической антенны	не менее 55 см
Электропитание	сеть 220 В, 50 Гц
Режим работы	круглосуточно
Средняя наработка на отказ	не менее 10000 ч
Средний срок службы	10 лет
Габаритные размеры генераторного блока	230x100x45 мм
Масса	не более 2 кг

3.2. Захист від несанкціонованих дій з інформацією.

Несанкціоновані дії в АС це такі, що порушують встановлений порядок розмежування доступу до інформації в АС. Гриф третьої версії є програмним комплексом засобів захисту даних від НСД, його призначення – забезпечити захист ІзОД, яка оброблюється в АС першого та другого класів. Даний КЗЗ реалізує стандартний функціональний профіль захисту інформації від НСД 2.КЦД.2 = { КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }.

***Позначення послуг безпеки згідно з НД ТЗІ 2.5-004*:**

- КЦД – конфіденційність, цілісність, доступність;
- ДВ-1– ручне відновлення;
- ДР-1 – квоти;

- КА-2 – базова адміністративна конфіденційність;
- КД-2 – базова довірча конфіденційність;
- КО-1 – повторне використання об'єктів;
- НИ-2 – одиночна ідентифікація та автентифікація;
- НК-1 – однонаправлений достовірний канал;
- НО-2 – розподіл обов'язків адміністраторів;
- НТ-2 – самотестування при старті;
- НР-2 – захищений журнал;
- НЦ-2 – комплекс засобів захисту з гарантованою цілісністю;
- ЦА-2 – базова адміністративна цілісність;
- ЦД-1 – мінімальна довірча цілісність;
- ЦО-1 – обмежений відкат [21].

ВИСНОВКИ

Питання захисту інформації в інформаційно-телекомунікаційних мережах дуже актуальне на даний час.

В роботі проведено дослідження вимог чинного законодавства України щодо захисту інформації в інформаційно-телекомунікаційній системі.

Встановлені вимоги до захисту конфіденційної та таємної інформації.

Встановлено, що існують два типу загроз інформації в інформаційно-телекомунікаційних системах: загрози витоку технічними каналами та загрози несанкціонованих дій з інформацією.

Для побудови комплексної системи захисту інформації в АС класу 2 застосовано положення існуючих нормативних документів технічного захисту інформації.

В рамках роботи проведено обстеження середовищ функціонування інформаційно-телекомунікаційної системи, розроблені моделі загроз інформаційній безпеки та порушника, політика інформаційної безпеки, технічне завдання. Обрано засоби захисту інформації в АС класу 2.

Для захисту інформації в АС класу 2 від витоку технічними каналами застосовано:

- активний метод, а саме просторове зашумлення радіосигналом виду білий шум;
- пасивний метод із застосуванням фільтру низьких частот по мережі живлення основних та додаткових технічних засобів.

Для захисту інформації в АС класу 2 від несанкціонованого доступу застосовано програмний КЗЗ Гриф 3.

Таким чином мета роботи досягнута.

ПЕРЕЛІК ПОСИЛАНЬ

Законодавчі та нормативні документи

1. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»

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

3. Закон України «Про Національну систему конфіденційного зв'язку»

4. Закон України «Про інформацію»

5. Закон України «Про телекомунікації»

6. Закон України «Про радіочастотний ресурс України»

7. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»

8. Закон України «Про державну таємницю»

9. Закон України «Про ліцензування певних видів господарської діяльності»

10. Закон України «Про електронні документи та електронний документообіг»

11. Закон України «Про наукову і науково-технічну експертизу»

12. Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання»

13. Закон України «Про ратифікацію Статуту і Конвенції міжнародного союзу електрозв’язку»

14. Закон України «Про електронний цифровий підпис», від 22.05.2003 № 852-IV»

15. Закон України «Про електроні документи та електронний документообіг», від 22.05.2003 № 851-IV»

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

17. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

18. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

19. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

20. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

22. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999.

23. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.