МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри ЗЗІ
_____ В.В. Козловський

«____»_____ 2020 р.

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Комплексна система захисту інформації для комерційної організації

Автор: В.С. Тимощук

Науковий керівник: к.т.н., доцент Т.Л. Щербак

Нормоконтролер: д.т.н., професор М.О. Шутко

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Засобів захисту інформації

Освітнього ступеня: «Магістр»

Спеціальність: 125 Кібербезпека

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗЗІ

_____ В.В. Козловський

«____»_____ 2020 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
студента Тимощука Василя Сергійовича

1. Тема: Комплексна система захисту інформації для комерційної організації
затверджена наказом ректора від 13.10.2020 р. № 1994/ст.
2. Термін виконання: з 05 жовтня 2020р. по 27 грудня 2020р.
3. Вихідні дані: Обстеження об'єкту як підготовки до розробки КСЗІ; Розробка політики, плану та ТЗ для АС класу; Підготовка до введення в дію КСЗІ.
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
1. Обстеження об'єкту як підготовки до розробки КСЗІ
2. Розробка політики, плану та ТЗ для АС класу
3. Підготовка до введення в дію КСЗІ

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи

№ п/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі		Виконано
2.	Аналіз літературних джерел		Виконано
3.	Обґрунтування рішення		Виконано
4.	Збір інформації		Виконано
5.	Обстеження об’єкту як підготовки до розробки КСЗІ		Виконано
6.	Розробка політики, плану та ТЗ для АС класу		Виконано
7.	Підготовка до введення в дію КСЗІ		Виконано
8.	Оформлення і друк пояснювальної записки		Виконано
9.	Оформлення презентації		Виконано
10.	Отримання рецензій від опонентів		Виконано
11.	Захист в ЕК		

Дипломник В.С. Тимощук

(підпис, дата)

Дипломний керівник Т.Л. Щербак

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 117 сторінок, має 4 рисунка, 23 таблиці. Список використаних джерел містить 39 найменувань і займає 5 сторінок.

Метою кваліфікаційної роботи є розробка комплексної системи захисту інформації для комерційної організації.

В кваліфікаційній роботі здійснено розробку комплексної системи захисту інформації для комерційної організації

Ключові слова: КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗОВАНА СИСТЕМА, ТЕХНІЧНЕ ЗАВДАННЯ.

ЗМІСТ

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ

АС	–	Автоматизована система
АСВБ	–	Автоматизована система класу 2 відділу безпеки
БД	–	Бази даних
ГМД	–	Гнучкий магнітний диск
ДТЗ	–	Допоміжні технічні засоби
ЖМД	–	Жорсткий магнітний диск
ЗЗІ	–	Засоби захисту інформації
ІзОД	–	Інформація з обмеженим доступом
ІС	–	Інформаційна система
КЗЗ	–	Комплекс засобів захисту
КСЗІ	–	Комплексна система захисту інформації
НД ТЗІ	–	Нормативний документ системи технічного захисту інформації
НСД	–	Несанкціонований доступ
ОІД	–	Об’єкт інформаційної діяльності
ОТЗ	–	Основні технічні засоби
ПЕМВН	–	Побічні електромагнітні випромінювання і наводки
ПІБ	–	Політика інформаційної безпеки
ПЗ	–	Програмне забезпечення
ПМА	–	Програма і методика випробувань
ТЗІ	–	Технічний захист інформації

ВСТУП

Основою для визначення необхідності створення КСЗІ являються норми та вимоги діючого законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації чи забезпечення її цілісності, доступності, чи прийнято власником інформації рішення тому, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Аналіз нормативно-правових актів, на основі яких можуть встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, чи визначення необхідності забезпечення захисту інформації у відповідності з іншими критеріями.

Визначення наявності у складі інформації, що належить автоматизованій обробці, таких її видів, які вимагають обмеження доступу до неї чи забезпечення цілісності і доступності у відповідності з вимогами нормативно-правових актів. Оцінки можливості переваг експлуатація ІТС у випадку створення КСЗІ. На основі проведеного аналізу приймається рішення про необхідність створення КСЗІ на підприємстві.

Головною метою комплексної системи захисту інформації являється забезпечити безпеку та безперервність продажу, але 100-відсотковий захист забезпечити не можливо, але забезпечити від деяких ризиків та втрат для комерційної організації дані заходи можуть зберегти компанію, тому дана тема є **актуальною**.

КСЗІ направлена на забезпечення захисту інформації та нерозголошення, витоку, несанкціонованого доступу та модифікації даних в системі, охорону продукції та персонал.

Інформація, що циркулює на підприємстві: інформація щодо постачальників, клієнтів (клієнтська база), договорі/контракти, банківські рахунки, накази, та описана в таких нормативних документах:

- Закон України «Про інформацію»;
- Закон України «Про захист персональних даних»;

- Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закон України «Про електронні документи в електронному документообігу»;
- Закон України «Про торгові марки»;
- Закон України «Про захист прав споживачів»;
- Постанова Кабінету Міністрів України «Порядок впровадження торгової діяльності та правил комерційної обслуговування населення».

За порушення Законів України передбачається відповідальність, описана в Кримінальному Кодексі України, позбавлення ліцензії комерційної організації чи/і конфіскація майна.

Для забезпечення інформаційної безпеки на торговому організації приймається так названа – КСЗІ – сукупність організаційних та інженерно-технічних заходів, які направлені на забезпечення захисту інформації від нерозголошення, витоку та несанкціонованого доступу. КСЗІ являється глобальною концепцією безпеки та основа для безпеки інфраструктури в цілому.

Метою є розробка комплексної системи захисту інформації для комерційної організації.

У процесі підготовки кваліфікаційної роботи були поставлені наступні **задачі**:

- Обстеження об’єкту як підготовки до розробки КСЗІ;
- Розробка політики, плану та ТЗ для АС класу;
- Підготовка до введення в дію КСЗІ.

Об’єкт дослідження. Комерційна організація.

Предмет дослідження. Комплексна система захисту інформації.

Новизна роботи. Розробка комплексної системи захисту інформації для комерційної організації.

Практична цінність. Результати досліджень можна використовувати для комерційної організації.

РОЗДІЛ 1 ОБСТЕЖЕННЯ ОБ'ЄКТУ ЯК ПІДГОТОВКИ ДО РОЗРОБКИ КСЗІ

1.1 Обґрунтування необхідності створення КСЗІ

Комерційна організація «ТИМ-ТИМ» було створено відповідно до законодавства України «Про торгові марки» та «Про захист прав споживачів», також Постанова Кабінету Міністрів України «Порядок впровадження торгової діяльності і правил комерційної обслуговування населення» [9].

Основна задача комерційної організації – забезпечити можливість покупки будь-якого товару при високоякісному обслуговуванні. Реалізувавши товар та отримавши прибуток за планом, комерційна організація досягає своє цілі [9].

Основними функціями комерційної організації являються [9]*:*

- Представили якісний товар для покупців;
- Обов'язково товар повинен бути сертифікований в Україні;
- Пошук направлений по вдосконаленню існуючих форм обслуговування та впровадження нових;
- Побудова різних схем формування цін та знижок;
- Контроль виконання персоналом організації встановленої цінової політики;
- Зберігати всі бізнес-плани та бізнес проекти від конкурентів;
- Представники/продавці-консультанти пропонують консультацію про асортимент для покупців.

Основна направлення захисту інформаційних ресурсів В комерційній організації [9]*:*

Правові заходи [9]:

- Виконання норм а положень державної політики в області захисту;
- Контроль по захищенню інформації, яка являється власністю держави;

Організаційні заходи [9]:

- Політика безпеки;
- Режимні заходи;
- Створення структури, відповідальність за безпеку інформації;
- Контроль за виконання та ефективністю заходів по захисту інформації;

Програмно-апаратні заходи [9]:

Технічний захист інформації:

- Захист від витоку технічними каналами;
- Захист від несанкціонованого доступ;
- Антивірусний захист;
- Автентифікація та авторизація користувачів;
- Розмежування доступу до інформаційних ресурсів;
- Аудит.
- КЗІ.

Інженерні засоби захисту [9]:

- Створення системи гарантованого електропостачання;
- Встановлення камер відеоспостереження;
- Встановлення на кожному продукті чіпу, який після покупки розмагнічується продавцем/касиром.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ [9].

Необхідно розробити наступні документи [26]:

1. Наказ про затвердження Переліку відомостей, що відноситься до конфіденційної інформації КО «ТИМ-ТИМ» та якій надається грифи обмеження доступу та «Конфіденційна інформація», Додаток А.
2. Перелік відомостей, що відноситься до конфіденційної інформації комерційної організації «ТИМ-ТИМ» та якій надається грифи обмеження доступу «Конфіденційна інформація», табл.1.1.

3. Акт визначення вищого ступень обмеження доступу інформації, яка циркулюватиме на об’єкті інформаційної діяльності – приміщення № 1 відділу безпеки комерційної організації «ТИМ-ТИМ», Додаток Б.

Таблиця 1.1 – Перелік відомостей, що відноситься до конфіденційної інформації комерційної організації «ТИМ-ТИМ» та якій надається грифи обмеження доступу «Конфіденційна інформація»

№	Інформація	Гриф обмеження доступу
1.	Відомості про ідентифікатори та паролі системного адміністратора та інших осіб, що мають доступ до управління автоматизованою системою	для службового користування
2.	Відомості про ідентифікатори та паролі співробітників	для службового користування
3.	Технічні заходи щодо захисту конфіденційної інформації та для службового користування	для службового користування
4.	Нормативна та експлуатаційна документація щодо технічних рішень, прийнятих у спеціальних проектах та проектах захисту організації, політика безпеки організації	для службового користування
5.	Програми професійної підготовки співробітників для обслуговування клієнтів	для службового користування
6.	Відомості про організацію, реагування та дій у разі виникнення надзвичайної ситуації	для службового користування
7.	Відомості, про систему охорони, перепускного режиму	для службового користування
8.	Відомості про клієнтську базу компанії «ТИМ-ТИМ»	конфіденційно
9.	Відомості про співробітників компанії «ТИМ-ТИМ»	конфіденційно
10.	Відомості щодо обліку та видачі печаток, штампів та бланків	конфіденційно
11.	Відомості про стан та ефективність роботи організації (фінансово-економічні положення компанії, бухгалтерські звіти, рівень платоспроможності фірми)	конфіденційно
12.	Відомості про процес, характер та умови укладення угод, договорів, контрактів з клієнтами	конфіденційно
13.	Стратегічні плани маркетингового розвитку комерційної організації	конфіденційно
14.	Відомості про ділові переговори	конфіденційно
15.	Відомості про кредити та банківські операції комерційної організації	конфіденційно
16.	Посадові інструкції для працівників КО «ТИМ-ТИМ»	для службового користування

1.2 Обстеження середовищ функціонування АС

Мета організації. Для того, щоб розробити перелік відомостей обмеженого доступу, перелік об’єктів захисту на підприємстві, в даному випадку – комерційному, слід описати насамперед інформаційну систему. Конкретний опис місця для впровадження КЗІ – це є важливим аспектом для отримання великого прибутку та поновлення клієнтської бази [26].

Задачами [26]:

- Оперативно оцінювати ситуацію з апаратним та ПЗ;
- Ефективно керувати ресурсами на підприємстві;
- Контроль вразливостей інформаційних ресурсів;
- Надавати звітність постійну, або за необхідності;
- Оцінка ефективності міри захисту.

Опис. АС представляю собою сукупність інформації, персоналу та комплексу засобів автоматизації діяльності, які реалізуються комерційні технологічні процеси, або його частин. Таке розуміння добре гармонізує з сучасним підходом до обробки інформації в документованій формі, де документом вважається зафіксованим на матеріальному носії інформації з реквізитами, які дозволяють ідентифікувати її. Таким чином, документом являється не тільки текст, але й зображення на листах, і файл на матеріальному носії, та стрічка запису в БД [26].

Тому, для більш точного визначення ІС комерційної організації як сукупності інформації, персоналу, матеріальних носіїв, засобів автоматизації, технічних та технологічних рішень обробки інформації [26].

В комерційній організації застосовують 1 тип автоматизованої системи – 2 класу [12].

Інформація загальнодоступної інформації [12]:

- Інформація щодо статуту організації, правил внутрішнього трудового розпорядку дня та правил техніки безпеки при роботі з технікою.
- Інформація щодо посад працівників, прізвище, ім’я та по батькові та їх робочі телефони.
- Інформація про графіки роботи організації.
- Клієнтські БД.
- Інформація про списки підприємств по регіону та їх керівників.

Перелік інформації обмеженого доступу [12]:

- Особиста інформація про працівників та їх посадові інструкції.

- Інформація про поставки техніки та обладнання для організації.
- Інформація щодо фінансової діяльності організації.
- Інформація про мережеві налаштування комп’ютерів та серверів.
- Інформація щодо документації організації.

Необхідно розробити наступні документи [12]:

1. Акт обстеження, Додаток В.
2. Ситуаційний план (1 поверх), Рис.1.1.
3. Ситуаційний план (2 поверх), Рис.1.2.
4. План мережі (1 поверх), Рис.1.3.
5. План мережі (2 поверх), Рис.1.4.

1.3. Визначення потенційних загроз для інформації, яка буде циркулювати в АС

В процесі проведення обстеження комерційної організації, визначаються потенційні загрози для інформації, таким чином обов’язково створюється модель загроз та модель порушника, дані вимоги створюються відповідно нормативно-правових документів, такі як [12]:

✓ НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу» (Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22);

✓ НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» (Затверджений наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53);

✓ НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 р. №125).

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути внутрішніми або зовнішніми [12].

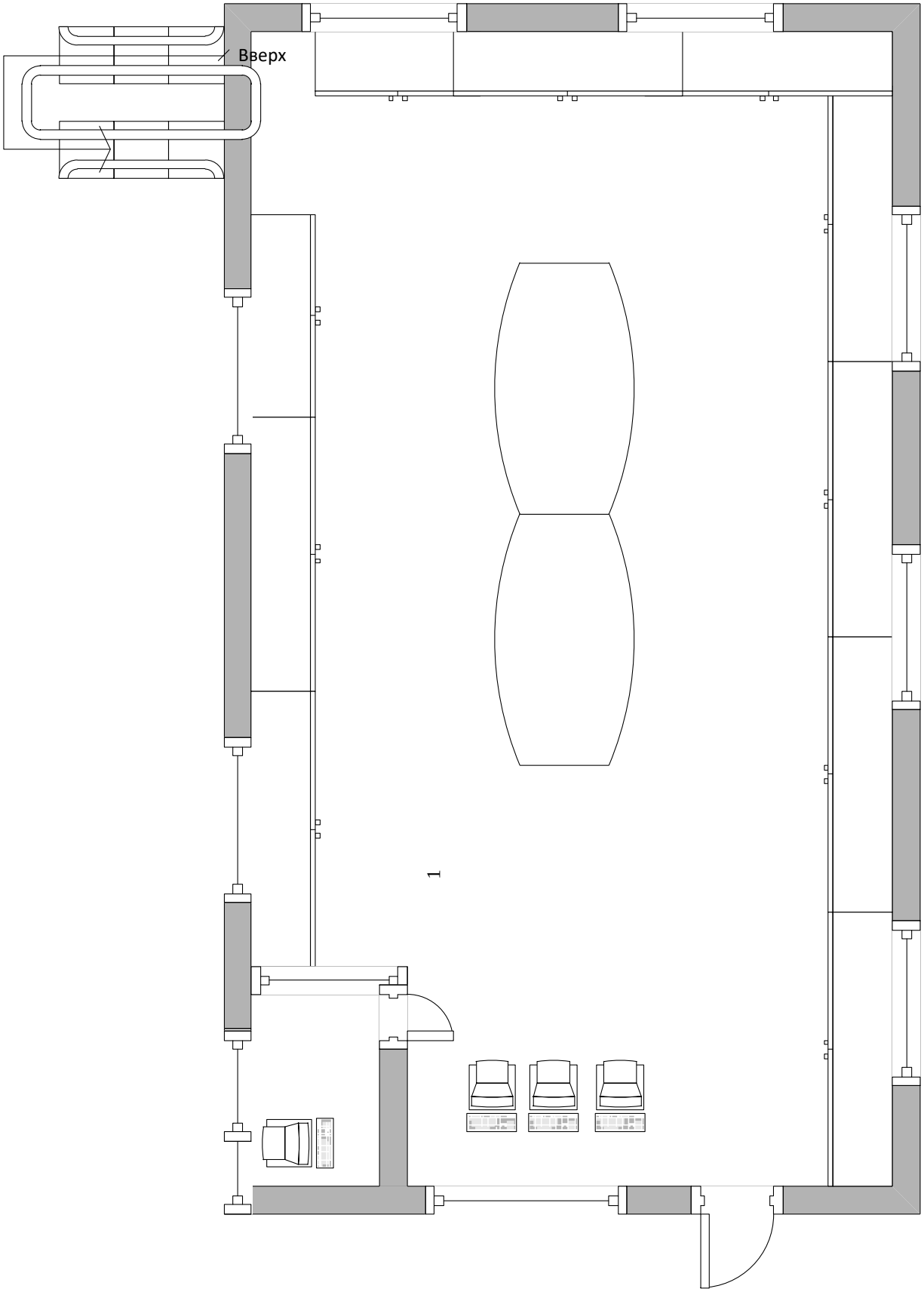


Рисунок 1.1 – Ситуаційний план (1 поверх)

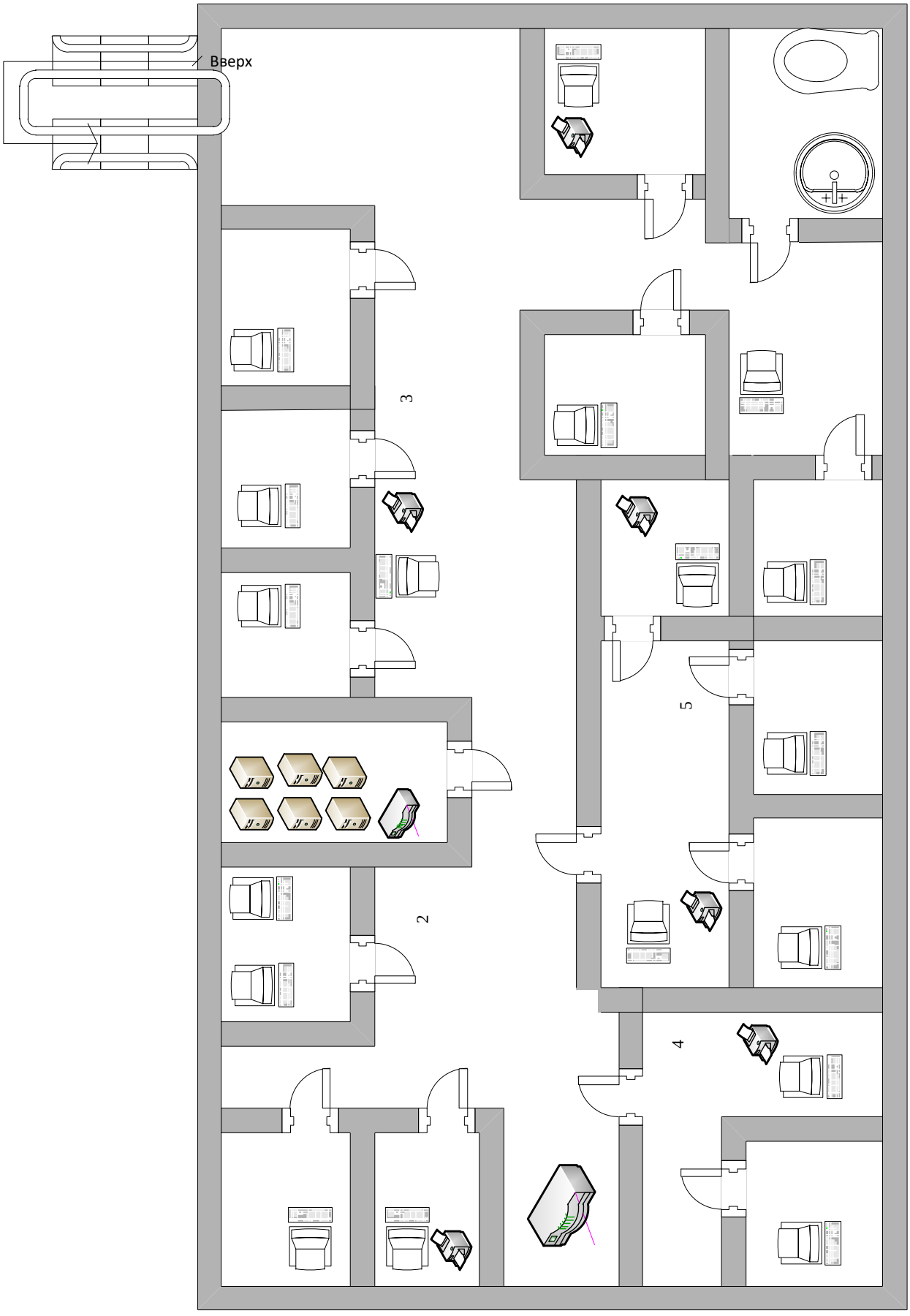


Рисунок 1.2 – Ситуаційний план (2 поверх)

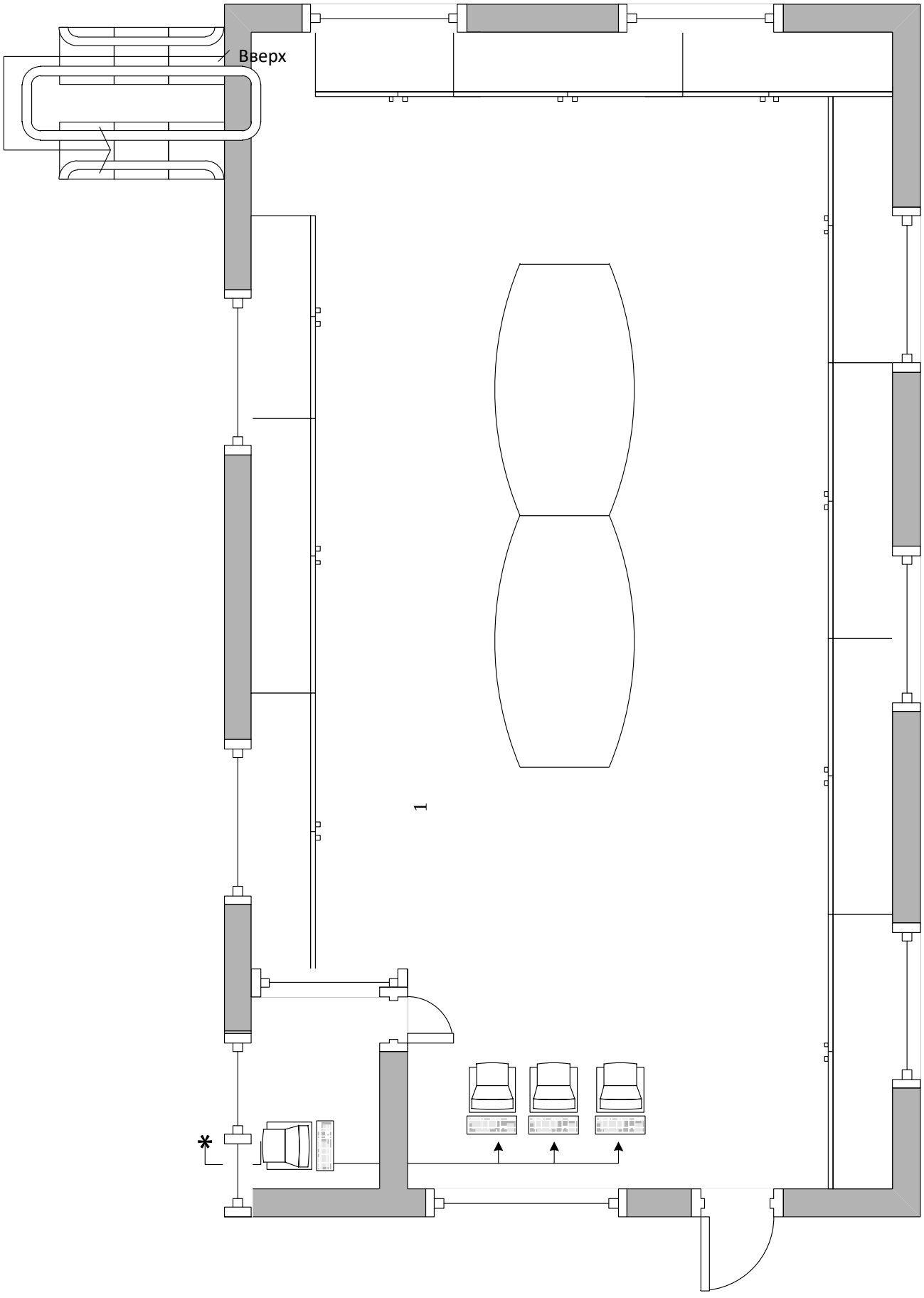


Рисунок 1.3 – План мережі (1 поверх)

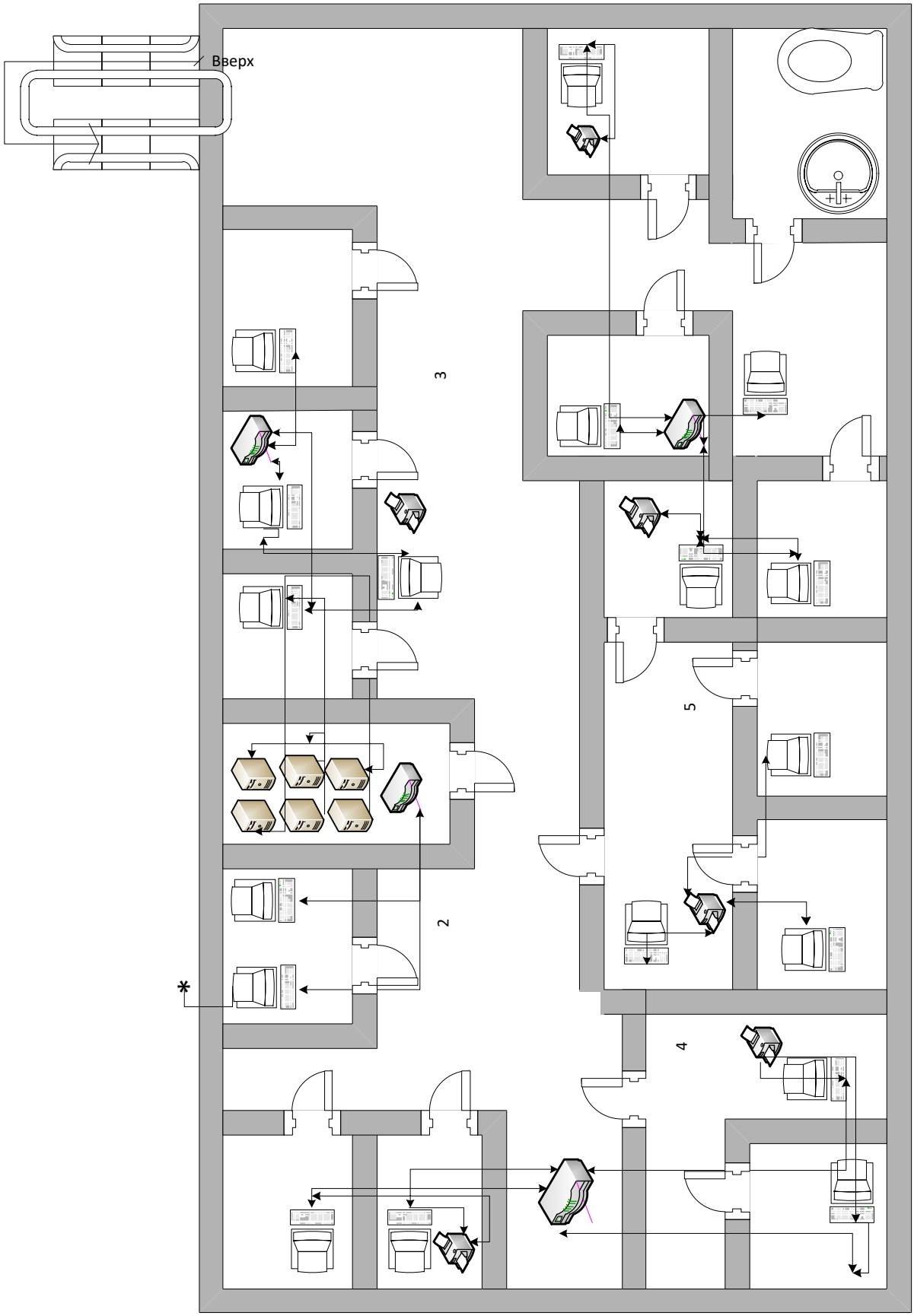


Рисунок 1.4 – План мережі (2 поверх)

Модель порушника повинна визначати [28]:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути [28]:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- можливість модифікації та зміни інформації;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
- можливість отримання доступ до матеріальних носіїв інформації;
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Варіантами моделі загроз визначені властивості захищеності інформаційних об’єктів, які можуть бути порушеними – конфіденційність (К), цілісність (Ц), доступність (Д) та якісна оцінка ймовірності здійснення загроз та рівнів збитків по кожному з видів порушень [28].

- Методика розроблення такої моделі полягає в тому, що в один із стовпчиків таблиці заноситься перелік видів загроз. Надалі для кожної із можливих загроз шляхом їх аналізу необхідно визначити [28]:
    - Ймовірність виникнення таких загроз.
    - Можливий рівень шкоди.
    - Джерела загроз.

Необхідно розробити наступні документи:

1. Модель загроз, Додаток Г.

РОЗДІЛ 2 РОЗРОБКА ПОЛІТИКИ, ПЛАНУ ТА ТЗ ДЛЯ АС КЛАСУ 2

2.1 Розробка політики безпеки інформації в АС

Даний етап КСЗІ передбачає вивчення об’єкта, на якому створюється КСЗІ, при цьому уточнює модуль загроз, модель потенційного порушника та аналіз ризиків, що виконуються на основі попередніх етапах [18].

Розробляючи політику безпеки банківських електронних систем, треба враховувати їхню специфіку порівняно з іншими ІС. Особливості ІС комерційної організації зумовлені специфікою тих завдань, які виконують за її допомогою, а саме [18]:

- вся інформація, яка обробляється, накопичується і зберігається в системі, є конфіденційною, тому значну увагу доводиться приділяти КЗІ за допомогою шифрування, розподілу доступу й автентифікації в мережі, захисту місць підключення до мереж зв’язку тощо;
- інформація, яка циркулює в такій системі, не може бути втрачена, дубльована чи модифікована. У зв’язку з цим посилюються вимоги до надійності апаратного і ПЗ, оперативного і повного відновлення інформації після аварій та збоїв у роботі;

Основними принципами створення системи захисту [18]:

- конфіденційність;
- цілісність;
- доступність та безперервність.

Загроза неавторизованого проникнення до системи охоплює всі типи несанкціонованого доступу, у тому числі такі: фальсифікація санкції на доступ, неправомірне використання паролів, спроби працювати від імені іншої особи, несанкціоноване використання носіїв даних, перехоплення повідомлень у каналах зв’язку, вірусні атаки тощо. Загроза ненавмисної модифікації виникає унаслідок помилок у програмному забезпеченні, апаратних збоїв, помилок персоналу та користувачів і т. ін. Затримка або погіршення обслуговування можуть призвести до втрати коштів унаслідок штрафних санкцій і, що найважливіше, до втрати довіри до банківської системи [18].

Необхідно розробити наступні документи:

1. Політика безпеки, Додаток Д.

2.2 Розробка плану захисту інформації в АС

Для забезпечення ефективного захисту АС розробляють план захисту інформації для організації – набір документів, згідно до яких здійснюється організація захисту інформації на всіх етапах життєвого циклу автоматизованої системи, а саме [18]:

- ✓ Класифікація інформації автоматизованої системи;
- ✓ Загальний опис компонентів автоматизованої системи;
- ✓ Технології розробки інформації в автоматизованої системи;
- ✓ Модель загроз автоматизованої системи.

Необхідно розробити наступні документи:

1. План захисту інформації.

2.3 Розробка технічного завдання на створення КСЗІ в АС

ТЗ на КСЗІ є основним організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі [35].

Технічне завдання на КСЗІ розробляється згідно вимог функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброки в АС. Додатково необхідно також викласти вимоги до організаційних, фізичних та інших заходів захисту [35].

Дане ТЗ є обов’язковим документом під час проведення експертизи АС на відповідність вимог. Роботу з погодження проекту проводить технічного завдання на КСЗІ в АС здійснюють спільно Розробник ТЗ та Замовник [35].

В свою чергу Розробник за домовленістю із Замовником відправляє ТЗ на КСЗІ в АС на затвердження в Адміністрацію Держспецзв’язку України [35].

Необхідно розробити наступні документи:

1. Технічне завдання.

«ЗАТВЕРДЖУЮ»
Генеральний директор
комерційної організації
«ТИМ-ТИМ»
_____ Тимощук В.С.
«03» листопада 2020 року

АВТОМАТИЗОВАНА СИСТЕМА ВІДДІЛУ БЕЗПЕКИ
Торгового організації «ТИМ-ТИМ»

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ
(шифр – КСЗІ «АСВБ»)

ПЛАН ЗАХИСТУ НА КСЗІ

Київ-2020

1. ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСВБ

1.1 Загальні положення

План захисту інформації в АСВБ (далі – План захисту), визначає політику комерційної організації «ТИМ-ТИМ» в сфері захисту інформації в АСВБ та організацію захисту інформації на всіх етапах її життєвого циклу. Він розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованої ПІБ, визначає і документально закріплює об’єкти захисту інформації в АСВБ, основні завдання захисту, загальні правила обробки інформації в АСВБ, мету побудови та функціонування КСЗІ, заходи із захисту інформації. План захисту фіксує на певний момент часу склад АСВБ, перелік оброблюваних відомостей, технологію обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації відповідно вимог НД ТЗІ 1.4-001-2000. План захисту повинен регулярно переглядатися та при необхідності змінюватися.

АСВБ призначено для автоматизації процесів обробки інформації з обмеженим доступом.

1.2 Основні завдання захисту інформації

Основними завданнями захисту інформації в АСВБ є:

- забезпечення визначених політикою безпеки властивостей інформації під час експлуатації АСВБ та його керованості;
- своєчасне виявлення та знешкодження загроз для ресурсів АСВБ з врахуванням її архітектури, причин та умов, які спричиняють або можуть привести до порушення її функціонування та розвитку;
- створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні АСВБ;
- керування засобами захисту інформації, керування доступом користувачів до ресурсів АСВБ, контроль за їхньою роботою з боку СЗІ, оперативне сповіщення про спроби НСД;

- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;
- створення умов для максимально можливої локалізації джерел загроз, що виникають внаслідок неправомірних дій фізичних та юридичних осіб, впливу зовнішнього середовища та інших чинників негативного впливу на безпеку функціонування АСВБ.

1.3 Об’єкти захисту

Виходячи з рекомендацій НД ТЗІ 1.4-001-2000, об’єктами захисту АСВБ є:

- відомості, віднесені до ІзОД, обробка яких здійснюється в АСВБ і які можуть знаходитись на паперових, магнітних та інших носіях;
- інформаційні масиви та БД, ПЗ, інші інформаційні ресурси;
- обладнання АСВБ та інші матеріальні ресурси, включаючи технічні засоби та системи, що не задіяні в обробці інформації, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки;
- засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;
- користувачі АСВБ та власники інформації.

1.4 Шляхи забезпечення безпеки інформації

Забезпечення безпеки інформації в АСВБ досягається:

- організацією та впровадженням системи допуску посадових осіб до роботи з інформацією;
- організацією обліку, зберігання, обігу інформації та її носіїв;
- здійсненням контролю за забезпеченням захисту інформації, яка обробляється в АСВБ та за збереженням носіїв інформації;
- використанням програмно-технічних засобів КСЗІ.

2. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В АСВБ

2.1 Склад інформації в АСВБ

АСВБ призначена для роботи з ІзОД, яка представлена у вигляді текстових документів, електронних таблиць.

До інформації АСВБ відносяться також загальне, функціональне та спеціальне ПЗ АСВБ та дані захисту.

2.2 Класифікація інформації за режимом доступу та правовим режимом

За режимом доступу інформація, що обробляється в АСВБ, поділяється на відкриту інформацію та ІзОД. Остання, яка обробляється в АСВБ, є власністю комерційної організації «ТИМ-ТИМ», і поділяється на такі категорії:

- конфіденційна інформація;
- ДСК.

В АСВБ до ІзОД відноситься інформація, яка включена до «Переліку відомостей, що відноситься до конфіденційної інформації КО «ТИМ-ТИМ» та якій надається грифи обмеження доступу «Для службового користування» та «Конфіденційна інформація».

В АСВБ до відкритої інформації відносяться всі види ПЗ та інформація, яка не визначена відповідними документами як конфіденційна.

2.3 Класифікація інформації за типом представлення в АСВБ

У табл. 2.1 для кожної з визначених категорій інформації вказано тип її логічного та фізичного представлення.

3. ОПИС КОМПОНЕНТІВ АСВБ ТА ТЕХНОЛОГІЇ ОБРОКИ ІНФОРМАЦІЇ

3.1 Компоненти АСВБ

До компонентів АСВБ відносяться такі:

- технічне забезпечення;
- ПЗ;
- дані;
- користувачі АСВБ;
- технічний персонал.

3.1.1 Технічне забезпечення

АСВБ побудовано на базі одного автономного комп’ютера.

Таблиця 2.1 – Класифікація інформації за типом представлення в АСВБ

№ п/п	Інформація	Логічне представлення	Фізичне представлення	Місце зберігання
Відкрита інформація				
1	Загальне, функціональне та спеціальне програмне забезпечення	Програмний засіб	Файл	Жорсткий диск комп'ютера
2	Програмні засоби захисту	Програмний засіб	Файл	Жорсткий диск комп'ютера
3	Дистрибутиви ПЗ, у тому числі ПЗ захисту	Дистрибутив	Файл	CD-ROM, Жорсткий диск комп'ютера
4	Документи, які містять відкриту інформацію	Текстовий документ, електронна таблиця	Файл	Жорсткий диск комп'ютера або змінні диски
Конфіденційна інформація				
5	Документи, яким встановлений гриф «конфіденційно», «для службового користування»	Текстовий документ, електронна таблиця	Файл	Жорсткий диск комп'ютера, гнучкі магнітні диски (дискети)
6	Дані захисту	Таблиця БД захисту, журнал захисту, параметр конфігурації системи	Файл, параметр системного реєстру	Жорсткий диск комп'ютера
7	Резервні копії даних захисту	Таблиця БД захисту, текстовий документ, журнал захисту	Файл	гнучкі магнітні диски (дискети)

Склад технічних засобів АСВБ наведено в Паспорті формулярі АСВБ.

3.1.2 ПЗ

ПЗ АСВБ поділяється на загальне, функціональне та спеціальне.

Перелік ПЗ наведено в Паспорті формулярі АСВБ

3.1.3 Дані

За місцем зберігання дані АСВБ поділяються на два види: дані на магнітних та інших носіях та дані на паперових носіях.

3.1.3.1 Дані на магнітних та інших носіях

Серед даних, що зберігаються на магнітних та інших носіях, розрізняють дані постійного та тимчасового зберігання.

3.1.3.2 Дані на паперових носіях

До даних, що зберігаються на паперових носіях, відносяться:

- Друковані документи;
- Документація на АСВБ:

- ТЗ;
- Інструкція користувача АС 2;
- Інструкція з адміністрування системи;
- Технічна документація на СЗІ;
- Паспорт-формуляр на АСВБ;
- Облікові картки користувачів АСВБ;
- Положення про СЗІ;
- План захисту інформації;
- Інструкція щодо забезпечення режимних заходів під час обробки конфіденційної інформації в АСВБ.

3.1.4. Користувачі АСВБ та технічний персонал

Відповідно до рівня повноважень щодо доступу до секретної інформації, характеру робіт, які виконуються в процесі функціонування АСВБ, для користувачів АСВБ визначаються такі ролі:

- звичайний користувач;
- відповідальний за безпеку;
- заступник відповідального за безпеку;
- системний адміністратор.

Облікова картка користувача містить такі реквізити:

- ім’я користувача в АСВБ;
- прізвище та ініціали, підрозділ;
- посада користувача;
- рівень допуску;
- роль користувача в системі;

Для кожного користувача, що буде працювати в АСВБ, заповнюється одна чи декілька облікових карток – у залежності від ролей, які він виконує в системі. Кожна облікова картка відповідає обліковому запису користувача в БД захисту. Роль звичайного користувача не суміщається в одному обліковому

записі з жодною з адміністративних ролей, адміністративні ролі можна суміщати між собою.

Тому в разі виконання однією особою функцій адміністратора та звичайного користувача, заповнюються щонайменше дві облікові картки з різними іменами для реєстрації в системі.

Технічний персонал АСВБ забезпечує роботоздатність технічних засобів АСВБ та обслуговування приміщень, де встановлені ці засоби.

3.1.5. Активні та пасивні об’єкти АСВБ та їхня взаємодія

Активними об’єктами в технологічному процесі обробки інформації в АСВБ є користувачі АСВБ, персонал, а також програмні засоби.

До пасивних об’єктів АСВБ, які беруть участь у технологічному процесі обробки інформації, відносяться: дані, програмні засоби та технічні засоби.

Таким чином, програмні засоби можуть бути як активними, так і пасивними об’єктами. Активними вони є, коли представляють користувача, пасивними, коли користувач звертається до них.

Активні та пасивні об’єкти, з якими взаємодіє активний об’єкт, представлені в табл. 2.2. Оскільки програмні засоби, як активні об’єкти, не мають своїх атрибутів доступу, у цій таблиці вони розглядаються тільки як пасивні об’єкти.

3.2 Технологія обробки інформації

3.2.1 Організація роботи з ІзОД

Звичайні користувачі працюють у системі з документами, які містять ІзОД. ІзОД зберігається на жорсткому магнітному диску АСВБ та на змінних носіях інформації.

Змінні носії інформації з ІзОД зберігаються в спеціальному відділі у металевому сейфі та доступ до них регламентується розпорядчими документами КО «ТИМ-ТИМ».

Друк та експорт ІзОД відбувається відповідно розпорядчих документів КО «ТИМ-ТИМ».

Таблиця 2.2 – Активні та пасивні об’єкти, з якими взаємодіє активний об’єкт

№ пп	Активний об’єкт (суб’єкт)	Пасивні об’єкти
1	Відповідальний за безпеку	1. Технічні засоби: комп’ютер; 2. Програмні засоби: загальне, функціональне та спеціальне ПЗ; 3. Дані: дані захисту, резервні копії, облікові картки користувачів, проектні та експлуатаційні документи на АСВБ.
2	Системний адміністратор	1. Технічні засоби: комп’ютер; 2. Програмні засоби: загальне та функціональне ПЗ, програмні засоби захисту; 3. Дані: дані захисту, резервні копії системних даних, дистрибутиви ПЗ, експлуатаційні документи на АСВБ
3	Заступник відповідального за безпеку (адміністратор документів)	1. Технічні засоби: комп’ютер; 2. Програмні засоби: загальне, функціональне та спеціальне ПЗ; 3. Дані: текстові документи та електронні таблиці, експлуатаційні документи на АСВБ.
4	Звичайний користувач	1. Технічні засоби: комп’ютер; 2. Програмні засоби: загальне, функціональне та спеціальне ПЗ; 3. Дані: текстові документи та електронні таблиці, експлуатаційні документи на АСВБ
5	Персонал (продаці-консультанти)	1. Технічні засоби: комп’ютер; 2. Програмні засоби: загальне та функціональне ПЗ; 3. Дані: експлуатаційна документація на технічні засоби.

3.2.2 Технологія роботи з документами

Документи зберігаються в базах документів, для яких встановлюється адміністративне керування доступом. Керування доступом до документів здійснюють адміністратори документів.

Безпосередньо з усіма документами працюють звичайні користувачі. Для забезпечення можливості керування доступом адміністраторам документів надається можливість читання документів, а також може надаватись можливість роботи з документами.

Нові документи створюються користувачами вручну або імпортуються з іншого носія. Документи також можуть бути експортовані на інший носій.

4. ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАХИСТУ

4.1 Загальні підходи до забезпечення політики безпеки

Для забезпечення захисту ІзОД в АСВБ та належного функціонування комплексної СЗІ створюється СЗІ.

Склад та функції СЗІ в АСВБ визначаються відповідно до документа «Положення про СЗІ».

Повноваження користувачів встановлюються керівництвом КО «ТИМ-ТИМ» та узгоджуються з спеціальним відділом. Облік користувачів АСВБ здійснюється за допомогою облікових карток, на підставі яких адміністратор безпеки вводить, змінює або видаляє інформацію про користувача АСВБ. Облікові картки заповнюються та зберігаються в спеціальному відділі.

Питання організації навчання користувачів, які допускаються до роботи на АСВБ, з питань захисту інформації під час її обробки за допомогою АСВБ, включаються до Календарного плану основних заходів з безпеки в КО «ТИМ-ТИМ».

Навчання повинно бути направлено на засвоєння всіма категоріями користувачів вимог нормативних актів з питань захисту інформації та охорони державної таємниці.

Усі користувачі повинні знати вимоги основних документів щодо захисту інформації, вимоги розпорядчих документів КО «ТИМ-ТИМ», які регламентують порядок проведення робіт з ІзОД за допомогою АСВБ.

Доведення до користувачів вимог діючих нормативних та організаційно-розпорядчих документів щодо захисту інформації в АСВБ здійснюється начальником спеціального відділу.

До обробки інформації на АСВБ допускаються лише особи, яки успішно здали відповідні заліки та включені до затвердженого списку осіб, які допущені до обробки інформації за допомогою АСВБ.

Виконання робіт в АСВБ дозволяється працівникам, які включені до списку користувачів АСВБ.

Начальник спеціального відділу забезпечує виконання вимог нормативних документів щодо забезпечення режимних заходів під час роботи з ІзОД, а саме:

- облік друкованих документів;
- облік змінних носіїв інформації;
- облік технічних засобів, що пройшли спецдослідження;

- ведення облікових карток користувачів у частині, що його стосується.

Основні функції щодо забезпечення захисту інформації в АСВБ покладаються на службу захисту інформації в АСВБ до складу якої входить відповідальний за безпеку, заступник відповідального за безпеку та системний адміністратор. На СЗІ в АСВБ відповідно адміністративних ролей в АСВБ покладаються наступні основні функції:

Заступник відповідального за безпеку:

- ведення облікових карток користувачів;
- ведення БД захисту;
- налаштування системи;
- зміна, у разі необхідності, власника баз документів;
- спостереження за роботою системи;
- архівація баз документів;
- архівація даних захисту;
- настройка апаратного забезпечення;
- створення баз документів;
- керування доступом до документів.

Системний адміністратор:

- супроводження ПЗ, у тому числі ПЗ КЗЗ;
- супроводження апаратного забезпечення.

Усі дії, які прямо чи опосередковано можуть вплинути на захищеність інформації, адміністратори АСВБ виконують з дозволу відповідального за безпеку в АСВБ.

Контроль за дотриманням персоналом та користувачами АСВБ положень політики безпеки покладається на відповідального за безпеку та інчих членів даного відділу в АСВБ.

4.2 Порядок введення користувачів в(з) АСВБ та змін їхніх повноважень.

На підставі облікової картки заступника відповідального за безпеку вводить у БД захисту інформацію про користувача АСВБ, після чого ознайомлює під розпис користувача з його повноваженнями.

У випадку зміни повноважень користувача до облікової картки користувача вносяться необхідні зміни. На цій підставі заступник відповідального за безпеку вносить зміни до БД захисту та ознайомлює з ними користувача.

При необхідності видалення користувача з АСВБ вноситься відповідний запис до облікової картки користувача і на цій підставі заступник відповідального за безпеку видаляє користувача з АСВБ.

4.3 Керування системою та її компонентами

Керування системою здійснюють відповідальний за безпеку та системний адміністратор.

Відповідальний за безпеку вводить до системи нових користувачів та коригує відомості про них, має можливість змінювати стан системи та значення параметрів конфігурації системи та ін. Адміністратор безпеки встановлює пароль на доступ до апаратних налаштувань комп’ютерів.

Системний адміністратор здійснює супроводження апаратного та ПЗ. За необхідності він має можливість за узгодженням із відповідальним за безпеку змінювати стан системи та значення параметрів конфігурації, які безпосередньо не пов’язані з керуванням доступом.

5. ФІЗИЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Технічні засоби АСВБ розташовано в приміщенні, яке знаходяться в межах контрольованої зони КО «ТИМ-ТИМ».

Охорону контрольованої зони та перепускний режим до будівлі, точніше до торгово-розважального центру «IQ», де розташовано КО «ТИМ-ТИМ» з АСВБ здійснює відомча охорона «ЛУН».

В неробочий час приміщення з АСВБ опечатується та здається під охорону службі охорони «ЛУН».

Вхідні двері до приміщення № 1 з встановленою в ньому АСВБ – скляні та обладнані датчиком руху, після закриття магазину, двері блокуються відділом безпеки, замками різних систем. Крім того приміщення обладнано системою охоронної сигналізації.

Доступ до приміщення, у якому здійснюється обробка ІзОД, здійснюється обмежений колом осіб, які допущені до роботи в цьому приміщенні.

6. ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

У приміщенні, де розташовано АСВБ, створено комплекс ТЗІ, який забезпечує блокування наступних ТКВІ:

- ПЕМВН;
- радіотехнічний канал;
- візуально-оптичний.

Роботи по створенню комплексу безпеки проведені власними силами комерційної організації «ТИМ-ТИМ».

Відповідальний за захист інформації в АСВБ організовує та координує роботи із ТЗІ, як планові, так і одноразові – при проведенні заходів щодо змін та модернізації обладнання АСВБ.

7. ПОРЯДОК МОДЕРНІЗАЦІЇ КОМПОНЕНТІВ СИСТЕМИ

7.1 Модернізація обладнання

При змінах конфігурації технічних засобів АСВБ чи їх модернізації роботи з ТЗІ організовує та координує відповідальний за ТЗІ спільно з представниками СЗІ в АСВБ. Після проведення необхідних заходів з ТЗІ представниками СЗІ в АСВБ вносяться відповідні записи про зміні у складі АСВБ в Паспорті-формулярі на АСВБ.

7.2 Модернізація ПЗ

Модернізація ПЗ проводиться в разі необхідності. Поновлення всього ПЗ здійснює системний адміністратор за узгодженням з начальником служби захисту інформації в АСВБ та з відповідними відмітками в «Паспорті-формулярі на АСВБ».

7.3 Модернізація КЗЗ

Модернізація КЗЗ здійснюється відповідно до документа НД ТЗІ 3.6-001-2000 згідно з окремим ТЗ або додатком до основного ТЗ.

8. ПОРЯДОК ПРОВЕДЕННЯ ВІДНОВЛЮВАЛЬНИХ РОБІТ І ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОГО ФУНКЦІОНУВАННЯ АСВБ

У разі виникнення проблем у роботі технічного та ПЗ АСВБ системний адміністратор має вжити заходів для відновлення працездатності системи.

Відновлювальні роботи потребують зміни стану системи. Правила проведення відновлення працездатності технічних засобів АСВБ наведені в документі «Політика безпеки інформації в АСВБ».

Відновлення ПЗ АСВБ проводиться під час перебування системи в стані поновлення ПЗ, відновлення КЗЗ – під час перебування системи в стані відновлення.

При проведенні відновлення ПЗ за необхідності використовуються відповідні дистрибутиви. Відновлення ОС Windows проводиться за допомогою стандартної процедури відновлення Windows.

9. КОНТРОЛЬ ЗА ФУНКЦІОНУВАННЯМ КСЗІ

Організація контролю за функціонуванням КСЗІ в АСВБ покладається на відповідального за відділ безпеки в АСВБ.

10. ПОРЯДОК ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ КСЗІ

Обробка в АСВБ ІзОД дозволяється тільки після отримання атестата відповідності КСЗІ вимогам нормативних документів із питань захисту інформації.

Дозвіл на обробку ІзОД за допомогою АСВБ дається наказом генерального директора КО «ТИМ-ТИМ».

11. СИСТЕМА ДОКУМЕНТІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСВБ

Захист інформації в АСВБ регламентується такими документами:

- Закон України «Про інформацію» від 02.10.1992 № 2657-XII;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР;

- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI;
- Постанова Кабінету Міністрів України «Про затвердження Правил захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.06 р.;
- Постанова Кабінету Міністрів України «Про затвердження інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27.11.98 р. № 1893;
- ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»;
- ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення»;
- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»;
- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;
- НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
- Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 листопада 2007 року № 93;
- Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах, затверджене постановою Кабінету Міністрів України від 16 лютого 1997 року № 180;
- НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробовування комплексу технічного захисту інформації. Основні положення;

- КОКО-95 Тимчасове положення про категоріювання об’єктів;
- ТР ЕОТ-95 Тимчасові рекомендації з безпеки у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок;
- Інструкція щодо забезпечення режимних заходів щодо захисту інформації з обмеженим доступом під час її обробки в АСВБ;
- Положення про службу захисту інформації в АСВБ;
- Технічна документація на СЗІ ЛОЗА-1;
- ТЗ на створення КСЗІ в АСВБ;
- Інструкція з адміністрування системи АСВБ;
- Інструкція користувача АСВБ;
- Інструкція по оперативному відновленню функціонування АС.

12. КАЛЕНДАРНИЙ ПЛАН ІЗ ЗАХИСТУ ІНФОРМАЦІЇ В АСВБ

Таблиця 2.3 – Календарний план із захисту інформації

№ п/п	Назва заходу	Термін	Примітка
Організаційні заходи			
1	Розробка документів з різних напрямів захисту інформації в АСВБ	У разі необхідності	
2	Внесення змін та доповнень до чинних в АСВБ документів з урахуванням умов, що склалися	У разі необхідності	
3	Координація робіт із ремонту технічних засобів АСВБ	У разі збоїв або відмов	
4	Координація робіт із ремонту технічних засобів захисту	У разі збоїв або відмов	
5	Координація робіт із відновлення загального та функціонального програмного забезпечення АСВБ	У разі збоїв або відмов	
6	Координація робіт із поновлення програмного забезпечення комплексу засобів захисту	Модернізація або розробка нового ПЗ	
7	Розгляд результатів виконання затверджених заходів і робіт із захисту інформації	1 раз на місяць	
8	Оновлення Плану захисту інформації в АСВБ	У разі змін у складі АСВБ або умов її функціонування	
Контрольно-правові заходи			
9	Контроль за виконанням користувачами та технічним персоналом вимог відповідних інструкцій, розпоряджень, наказів	1 раз в квартал	
10	Відстеження небезпечних подій у журналі захисту	1 раз на тиждень	
11	Участь у контролі за наявністю на жорстких дисках комп’ютерів незахищеної секретної інформації	Відповідно до термінів перевірок відповідальним за ТЗІ	

Продовження таблиці 2.3

12	Контроль за станом зберігання та використання носіїв інформації на робочих місцях	1 раз на місяць	
Профілактичні заходи			
13	Поновлення вірусних баз	2 рази на місяць	
Інженерно-технічні заходи			
14	Організація та координація робіт з ТЗІ щодо блокування технічних каналів витоку інформації	Термін визначається в Акті атестації КТЗІ	

Відповідальний за відділ безпеки
комерційної організації «ТИМ-ТИМ» Верес В.В.

«ЗАТВЕРДЖЕНО»
Відповідальний за відділ
безпеки комерційної організації
«ТИМ-ТИМ»
_____ В.В. Верес
«17» листопада 2020 року

АВТОМАТИЗОВАНА СИСТЕМА ВІДДІЛУ БЕЗПЕКИ
комерційної організації «ТИМ-ТИМ»
(шифр – «АСВБ»)

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ
(шифр – КСЗІ «АСВБ»)

ТЕХНІЧНЕ ЗАВДАННЯ

Київ-2020

1. ЗАГАЛЬНІ ВІДОМОСТІ

1.1. Повна назва системи та її умовне позначення

Повна назва: КСЗІ АС відділу безпеки комерційної організації «ТИМ-ТИМ».

Умовне позначення: КСЗІ АСВБ.

1.2. Шифр теми і реквізити договору

Розробка КСЗІ АСВБ є складовою частиною робіт з впровадження АСВБ в діяльність, що виконуються між «ТИМ-ТИМ» та «ЛУН» відповідно вимог Договору від 17.12.15 № 1АС/245 (далі – Договір).

1.3. Замовник

Відкрите акціонерне товариство КО «ТИМ-ТИМ»

03061, Київ, вул. Гришко 3а.

1.4. Виконавець

Підприємство «ЛУН»

1.5. Планові терміни початку і закінчення роботи із створення КСЗІ

Терміни початку і закінчення робіт щодо створення КСЗІ АСВБ визначаються Договором.

1.6. Відомості про джерела та порядок фінансування робіт

Фінансування робіт із створення КСЗІ АСВБ здійснюється КО «ТИМ-ТИМ».

1.7. Порядок оформлення та пред’явлення Замовнику результатів робіт

- Технічне завдання оформлено згідно з вимогами НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
- Порядок оформлення та пред’явлення Замовнику результатів виконання робіт зі створення КСЗІ АСВБ визначається вимогами:
- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу;
- НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;

- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
- РД 50-34.698-90. АС. Требования к созданию документов.

Результатом роботи має бути КСЗІ АСВБ. Замовник отримує дистрибутиви програмних засобів, а також комплект документації відповідно до п. 5 цього ТЗ.

2. МЕТА СТВОРЕННЯ І ПРИЗНАЧЕННЯ КСЗІ

2.1. Мета створення КСЗІ АСВБ

Комплексна система захисту інформації АСВБ створюється для забезпечення захисту від несанкціонованого доступу до інформації, а саме для:

- розмежування та контроль доступу користувачів АСВБ згідно їх повноважень до ІзОД;
- реєстрацію даних про події, що відбуваються в системі і мають відношення до безпеки інформації;
- підтримку цілісності середовища виконання прикладних програм та ІзОД, що повинна оброблятися в АСВБ;
- виявлення вразливостей в ОС;
- захист від атак порушників безпеки;
- захист від проникнення і поширення комп’ютерних вірусів;
- захист інформації під час передачі телекомунікаційним середовищем;
- контроль за функціонуванням КСЗІ.
- виявлення загроз безпеці інформації, що передається, обробляється та зберігається в АСВБ;
- унеможливлення реалізації загроз для інформації, порушення її конфіденційності, цілісності та доступності в АСВБ.

КСЗІ АСВБ повинна передбачати:

- організаційні, правові заходи діяльності користувачів АСВБ;
- адміністративні заходи обмеження фізичного доступу до обробки інформації;
- технічні заходи і програмно-апаратні засоби захисту від НСД;
- захист інформації, що обробляється в АСВБ від витоку технічними каналами.

2.2. Функціональне призначення і особливості застосування КСЗІ АСВБ

КСЗІ АСВБ призначена для:

- забезпечення виконання визначеної для АСВБ ПБ інформації;
- реєстрації спроб реалізації загроз інформації та сповіщення адміністраторів безпеки про факти несанкціонованих дій з ІзОД;
- контролю за діями користувачів АСВБ та реєстрації подій, які мають відношення до безпеки інформації;
- підтримання цілісності , конфіденційності, доступності ІзОД АСВБ;
- блокування несанкціонованих дій з ІзОД;
- організації обліку, зберігання та обігу матеріальних носіїв інформації, які використовуються в АСВБ;
- контролю за функціонуванням КСЗІ;
- захисту ІзОД від її витоку технічними каналами на НСД доступу.

Під час проектування КСЗІ АСВБ необхідно забезпечити:

- ефективний рівень захисту ІзОД, яка циркулюватиме в АСВБ;
- економічну доцільність прийнятих рішень;
- забезпечення дотримання вимог режиму секретності під час проведення робіт зі створення КСЗІ АСВБ.

3. ЗАГАЛЬНА ХАРАКТЕРИСТИКА АСВБ ТА УМОВ ЇЇ ФУНКЦІОНУВАННЯ

Характеристика АСВБ

АСВБ розроблено на базі 21 комп’ютерів та принтерами.

Відповідно НД ТЗІ 2.5-005-99 за сукупністю характеристик АСВБ відносяться до автоматизованої системи класу «2».

3.1.1. Структура АСВБ

АСВБ призначено для автоматизації процесів обробки ІзОД. Основним режимом роботи АСВБ є робота в службовий час. Схема функціональної структури АСВБ наведена у додатку А.

3.1.2. Обладнання АСВБ

До складу АСВБ входить наступне обладнання:

- 21 системних блоків;
- 21 моніторів;
- 21 графічні маніпулятори типу «миша»;
- 21 клавіатур;
- 21 принтерів.

3.1.3. ПЗ АСВБ

До складу АСВБ входить наступне ПЗ:

- операційна система Windows 10;
- пакет прикладних програм Microsoft Office 2010;
- АС БД;
- драйвери системних пристроїв;
- антивірусна програма ESET Smart Security.

Інше ПЗ:

- СЗІ від НСД «Захист».

Детальний перелік ПЗ, що використовується в АСВБ буде визначено в паспорті-формулярі на АСВБ.

3.2. Характеристика фізичного середовища

Компоненти АСВБ розміщуються в приміщенні № 3 відділу безпеки КО «ТИМ-ТИМ», що знаходиться в межах КЗ КО «ТИМ-ТИМ». Охорона КО «ТИМ-ТИМ», здійснюється цілодобово відомчою охороною організації «ЛУН». Приміщення обладнано охоронною сигналізацією. Вхідні двері до приміщення № 1 з встановленою в ньому АСВБ – скляні та обладнані датчиком руху, після

закриття магазину, двері блокуються відділом безпеки, замками різних систем. Режим допуску до приміщення, де розміщується АСВБ, забезпечує неможливість проникнення сторонніх осіб у приміщення та їх доступу до обладнання АСВБ.

3.3. Характеристика персоналу

Представлена у додатку Д документа «План ЗІ»

3.4. Характеристика інформації, що обробляється в АСВБ

Розглянено у Переліку відомостей, додаток Б

3.5. Характеристика технології обробки інформації

Викладена у додатку Д документа «План ЗІ»

3.6. Особливості функціонування АСВБ

АСВБ використовується для обробки ІзОД в час, визначений службовою необхідністю. Надання машинного часу або устаткування в оренду стороннім організаціям не передбачається.

Функціонування АСВБ передбачає такі режими роботи:

- основний робочий режим роботи – функціонування АСВБ в робочий час для
- виконання визначених регламентом функціональних задач;
- режим адміністрування АСВБ – підтримка ІР в актуальному стані;
- режим тестування системи та окремих її компонентів – забезпечення рішення контрольних задач для перевірки працездатності АСВБ;
- режим технічного обслуговування АСВБ.

3.7. Можливі загрози інформації

3.7.1. Класифікація загроз

3.7.2. Модель порушника

Представлена в Моделі загроз для ІзОД, яка планується до циркуляції в автоматизованій системі класу 2 на ОІД – приміщення КО «ТИМ-ТИМ».

3.7.3. Модель загроз

4. ВИМОГИ ДО КСЗІ

4.1. Вимоги щодо організаційного забезпечення захисту

4.1.1. З метою забезпечення захисту ІзОД під час її обробки в АСВБ наказом генерального директора КО «ТИМ-ТИМ» створюється служба захисту інформації в АСВБ, якій надаються повноваження щодо організації і впровадження КСЗІ, контролю за станом захищеності інформації тощо. У своїй діяльності СЗІ керується документом «Положення про СЗІ».

4.1.2. Приміщення, в якому розташована АСВБ, повинно відповідати наступним вимогам:

- двері повинні бути обладнані 3 замковими пристроями різної конфігурації;
- вікна повинні бути обладнані металевими гратами;
- вікна та двері повинні бути обладнані датчиками системи охоронної сигналізації.

4.1.3. Відповідно до рівня повноважень щодо доступу до ІзОД, характеру робіт, які виконуються у процесі функціонування АСВБ, організовується доступ осіб до АСВБ з наступними ролями:

- Звичайні користувачі;
- Відповідальний за відділ безпеки;
- Заступник відповідального за відділ безпеки;
- Системний адміністратор.

Звичайний користувач АСВБ повинен безпосередньо здійснювати обробку ІзОД в АСВБ відповідно вимог Інструкції користувача АСВБ. Звичайний користувач АСВБ повинен мати базові навики роботи з обчислювальною технікою, з ОС Windows 10, текстовим редактором Microsoft Office Word та редактором електронних таблиць Microsoft Office Excel.

Відповідальний за відділ безпеки АСВБ повинен безпосередньо здійснювати:

- ведення баз даних захисту;
- встановлення значень параметрів конфігурації системи, безпосередньо пов’язаних із доступом до інформації;

- спостереження за роботою системи;
- заміну, у разі необхідності, власника баз документів та документів.

Також повинен створювати бази та керувати доступом до документів, які містяться в БД.

Системний адміністратор АСВБ повинен забезпечувати:

- безперебійну роботу операційної системи АСВБ;
- справну роботу системних драйверів;
- встановлення необхідного ПЗ та його оновлення;
- своєчасне оновлення баз антивірусного ПЗ.

До того ж, надійну роботу компонентів АСВБ забезпечує технічний персонал.

Усі дії, які прямо чи опосередковано можуть вплинути на захищеність інформації, системний адміністратор має узгоджувати з адміністратором безпеки. Порядок узгодження повинен визначатись «Планом захисту інформації».

4.1.4. Контроль за друком та експортом інформації повинен здійснювати секретаріат КО «ТИМ-ТИМ»

4.1.5. Усі носії, які містять ІзОД, повинні зберігатись в спеціальному відділу в окремому металевому сейфі або шафі.

4.2. Вимоги щодо захисту інформації від НСД

Згідно із специфікаціями, наведеними в документі НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу, КЗЗ від НСД має такий профіль захисту – КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2

Процес розробки КЗЗ має відповідати рівню гарантій Г-2.

4.2.1. Базова довірча конфіденційність (КД-2).

Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що

дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об’єкт може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об’єкта. Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об’єктів і процесів. Прикладом реалізації даного рівня послуги є реалізоване в ЦМХ керування доступом на підставі тріад власник/група/всі інші.

4.2.2. КА-2. Базова адміністративна конфіденційність

Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об’єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об’єкта шляхом керування належністю користувачів, процесів і об’єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об’єкта. КЗЗ повинен надавати можливість адміністратору чи користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об’єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту та імпорту.

4.2.3. Повторне використання об’єктів (К0-1)

Послуга застосовується до оперативної та дискової пам’яті.

Під час видалення файлів програмні засоби системи повинні використовувати процедуру безповоротного видалення.

В АСВБ необхідно використовувати Windows 10, оскільки ця ОС забезпечує очищення звільненої оперативної пам’яті під час її перерозподілу.

Перевірку доступу слід виконувати окремо для кожного користувача, щоб права доступу, надані одному користувачу, не вплинули на права, які надаються іншому.

4.2.4. Мінімальна довірча цілісність (ЦД-1).

На даному рівні користувач, домену якого належить об’єкт, може накладати обмеження на доступ до об’єктів з боку інших користувачів. Керування правами має грубу вибірковість. Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об’єктів. Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об’єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта. Запити на зміну прав доступу до об’єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об’єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об’єкт. Права доступу до кожного захищеного об’єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об’єктів під час їх експорту і імпорту.

4.2.5. Мінімальна адміністративна цілісність (ЦА-1)

Послуга застосовується до таких об’єктів доступу:

- бази документів;
- документи;
- дані захисту;
- програмні засоби КЗЗ.

4.2.5.1. Доступ до баз документів та документів

КЗЗ повинен надавати користувачам можливість працювати з базами документів та документами тільки за допомогою призначеного для цього процесу.

КЗЗ повинен здійснювати керування доступом до баз документів та документів на підставі атрибутів доступу користувача і документа згідно з правилами розмежування доступу.

КЗЗ повинен надавати можливість змінювати атрибути доступу баз документів та документів лише користувачу з роллю відповідальний за відділ безпеки. Це дозволить йому визначати користувачів і/або їх групи, які мають право модифікувати документ. Атрибути доступу бази документів та документа повинні встановлюватись в момент їх створення.

4.2.5.2. Доступ до даних захисту

КЗЗ повинен надавати можливість працювати з даними захисту тільки за допомогою призначеного для цього процесу.

КЗЗ повинен реалізовувати правила розмежування доступу до даних захисту.

4.2.5.3. Доступ до програмних засобів

КЗЗ повинен надавати доступ до процесів, за допомогою яких здійснюється обробка ІзОД, тільки користувачам АСВБ.

КЗЗ повинен надавати доступ до процесів, за допомогою яких здійснюється ведення БД захисту та перегляд журналу захисту, тільки адміністратору безпеки та системному адміністратору.

КЗЗ повинен надавати можливість змінювати атрибути доступу файлів лише адміністратору безпеки та системному адміністратору.

4.2.6. Ручне відновлення (ДВ-1)

У системі слід передбачити певний порядок обробки помилок, які виникають під час роботи системи.

Програмні засоби повинні надавати адміністратору можливість вказати системі, яким чином вона має реагувати на помилку. Серед можливих реакцій мають бути такі:

- повторити дію, що викликала помилку;
- перевести КЗЗ у стан, призначений для відновлення.

Усі можливі помилки та способи їх виправлення мають бути документовані.

Дистрибутив КЗЗ повинен надавати можливість повної або часткової повторної інсталяції КЗЗ.

4.2.7. Захищений журнал (НР-2)

Для реєстрації подій у КЗЗ повинен вестись журнал захисту, який має бути захищеним від несанкціонованого ознайомлення, модифікації та знищення.

Засоби реєстрації КЗЗ повинні забезпечувати реєстрацію таких подій:

- вхід/вихід користувача в АСВБ;
- створення/видалення облікових записів користувачів;
- зміни облікових записів користувачів;
- створення/видалення об’єктів доступу;
- зміни атрибутів доступу об’єктів доступу;
- спроби доступу до об’єктів доступу;
- зміни конфігурації КЗЗ;
- виявлення порушень цілісності програмного середовища;
- початок та закінчення роботи прикладних програм, призначених для роботи з
- інформацією, що захищається;
- виведення інформації на зовнішні носії.

Усі записи про події мають містити інформацію про дату, час і тип події, а для подій аудита – також про користувача, процес і об’єкт, пов’язані з подією.

Адміністратору безпеки необхідно надати можливість встановлювати політику аудита, яка б визначала, які саме події аудита реєструються засобами КЗЗ.

Доступ до журналу захисту повинен надаватись тільки адміністратору безпеки, згідно з правилами розмежування доступу.

Адміністратору безпеки необхідно надати засоби для зручної роботи з журналом, які також дозволяли б створювати копії журналу та працювати із раніше створеними копіями.

Слід передбачити автоматичну реакцію системи на критичні події, такі як, наприклад, виявлення порушень цілісності програмного середовища.

4.2.8. Множинна ідентифікація і автентифікація (НИ-3)

Кожний користувач повинен однозначно ідентифікуватись КЗЗ на підставі введеного імені.

Перш ніж дозволити будь-якому користувачу виконувати будь-які контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача на підставі введеного ним пароля та наданого фізичного ідентифікатора.

Як фізичні ідентифікатори можуть використовуватись диски та накопичувачі USB Flash.

Введення імені та пароля повинно проводитись з клавіатури. Кількість символів у паролі повинні бути не менше ніж 6.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого ознайомлення, модифікації або руйнування.

4.2.9. Однонаправлений достовірний канал (НК-1)

Достовірний канал установлюється з ініціативи користувача після натискання їм комбінації клавіш Ctrl-Alt-Del.

Достовірний канал використовується для початкової ідентифікації і автентифікації користувача.

4.2.10. Розподіл обов’язків адміністраторів (НО-2)

В АСВБ слід визначити 3 ролі користувачів:

- звичайний користувач;
- відповідальний за відділ безпеки;
- заступник відповідального за відділ безпеки;
- системний адміністратор;

- обслуговуючий персонал.

Відповідальний за відділ безпеки, заступник відповідального за відділ безпеки та системний адміністратор повинні бути членами групи адміністраторів операційної системи.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він був автентифікований як користувач АСВБ, якому надана ця роль.

4.2.11. КЗЗ з гарантованою цілісністю (НЦ-2)

КЗЗ повинен перевіряти цілісність таких об’єктів:

- програмні компоненти КЗЗ;
- параметри та розділи системного реєстру, в яких зберігаються важливі для захисту дані;
- завантажувальні сектори жорстких дисків.
- облікові записи користувачів та груп користувачів Windows.

Цілісність об’єктів слід перевіряти за допомогою підрахунку контрольних сум.

У разі виявлення порушень цілісності КЗЗ повинен зареєструвати у журналі відповідну подію та відреагувати на порушення одним із двох способів: завершити роботу ОС або перевести КЗЗ у стан відновлення. Можливість повернути КЗЗ до робочого стану повинні мати лише системний адміністратор.

Усі помилки, які виникають під час перевірки цілісності, слід вважати порушеннями цілісності.

За допомогою засобів ОС необхідно забезпечити виконання засобів захисту у власному домені – в ізольованій області пам’яті, недоступній іншим процесам.

Слід сформулювати вимоги до налагодження операційної системи, які гарантують, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити користувачів на доступ до об’єктів захисту контролюються КЗЗ.

Поновлення та відновлення програмних засобів КЗЗ повинно проводитись системним адміністратором за узгодженням з адміністратором безпеки. Порядок узгодження повинен визначатись «Планом захисту інформації».

4.2.12. Самотестування при старті (НТ-2)

КЗЗ повинен перевіряти правильність функціонування програмних засобів, які входять до складу КЗЗ. Для цього слід перевіряти цілісність файлів, що виконуються, які належать до КЗЗ. Перевірка цілісності виконується за допомогою підрахунку контрольних сум файлів.

Перевірку цілісності необхідно виконувати при ініціалізації КЗЗ, під час роботи КЗЗ та за запитом адміністратора безпеки чи системного адміністратора.

У разі виявлення під час ініціалізації порушень цілісності програмних засобів КЗЗ повинен перейти у стан відновлення.

У разі виявлення порушень цілісності програмних засобів КЗЗ під час роботи КЗЗ повинен відреагувати на порушення одним із двох способів: завершити роботу ОС або перевести КЗЗ у стан відновлення.

4.3. Політика безпеки інформації

4.3.1. Об’єкти доступу

В АСВБ виділяють такі об’єкти доступу:

- бази документів.
- бази документів призначені для зберігання документів. Всередині бази документи можуть бути розподілені по папках.

Кожна база має такі атрибути:

- назва;
- власник;
- максимальний рівень доступу документів;
- список доступу;
- список аудита.

Створити базу документів може лише Відповідальний за відділ безпеки. Відповідальний за відділ безпеки, який створив базу документів, стає її власником.

Документи.

Кожний документ має такі атрибути:

- назва;
- ключові слова та вирази;
- час створення;
- час останнього коригування;
- власник;
- рівень доступу;
- список доступу;
- список аудита.

Дані захисту:

- БД захисту;
- журнал захисту;
- параметри конфігурації системи;
- оперативні дані про роботу системи.

Програмні засоби КЗЗ.

Інші програмні засоби: Тимчасові файли, які створюються під час роботи прикладними програмами. Інформація в оперативній пам’яті комп’ютера. Дані, які знаходяться на екрані монітора під час роботи програмних засобів АСВБ. Дані у друкованому вигляді. Змінні носії. Інформація у вигляді полів та сигналів, які утворюються в результаті функціонування технічних засобів обробки, зберігання та відображення інформації. Технічні засоби АСВБ, у тому числі засоби захисту.

У табл. 2.4 перелічені об’єкти доступу та вказані носії, на яких вони зберігаються.

Таблиця 2.4 – Перелік об’єктів та носіїв зберігання

Об’єкт доступу	Місце зберігання
Бази документів та документи	Жорсткий диск та змінні носії (флеш накопичувачі, ком пакт диски)
Дані захисту	Жорсткий диск
Програмні засоби КЗЗ	Жорсткий диск
Інші програмні засоби	Жорсткий диск
Тимчасові файли	Жорсткий диск

4.3.2. Принципи керування доступом

КЗЗ повинен реалізовувати адміністративне керування доступом до таких об’єктів:

- бази документів;
- документи;
- дані захисту;
- програмні засоби;
- тимчасові файли.

4.3.3. Правила розмежування інформаційних потоків

Програмні засоби системи повинні здійснювати розмежування інформаційних потоків від об’єкта до користувача і від користувача до об’єкта. Розмежування інформаційних потоків слід здійснювати на підставі атрибутів доступу об’єкта та користувача.

Необхідно організувати роботу таким чином, щоб користувачі не мали безпосереднього доступу до файлів, в яких зберігаються бази документів, документи, БД захисту та журнал захисту.

Користувачі повинні мати можливість працювати з базами документів, документами, БД захисту та журналом захисту тільки за допомогою призначеного для цього процесу.

Відповідальний за відділ безпеки повинний мати можливість для кожного процесу, який використовується для доступу до баз документів, документів, бази даних захисту та журналу захисту, визначити користувачів та групи користувачів, які мають, а також не мають права ініціювати цей процес – для

цього слід відповідним чином встановити права на доступ до файлу, які відповідають процесу.

4.3.4. Атрибути доступу об’єктів доступу

До атрибутів доступу баз документів належать такі дані:

- власник;
- список доступу.

До атрибутів доступу документів належать такі дані:

- рівень доступу, який відповідає грифу обмеження доступу, що зберігається в документі, і обирається з такого переліку:
- конфіденційно;
- відкрита інформація;
- список доступу.

Для даних системи захисту атрибутом доступу є список доступу, який містить перелік адміністративних ролей з наданими їм видами доступу.

4.3.5. Атрибути доступу користувачів

До атрибутів доступу користувачів належать такі дані:

- роль;
- рівень допуску.

Рівень допуску користувача визначає найвищий ступінь секретності інформації, із якою йому дозволено працювати.

4.3.6. Види доступу

КЗЗ повинен підтримувати такі види доступу до баз документів: читання; створення папок; видалення папок; перейменування папок; створення документів; запис атрибутів; запис атрибутів доступу; перейменування; видалення.

КЗЗ повинен підтримувати такі види доступу до документів: читання; запис; видалення; друк; збереження у файлі; читання атрибутів доступу; запис власника; запис рівня доступу; запис списку доступу; запис списку аудита.

Для даних захисту слід передбачити такі види доступу: читання; запис.

4.3.7. Правила розмежування доступу

4.3.7.1. Правила розмежування доступу до баз документів

Можливість працювати з базами документів повинні мати лише оператори та відповідальний за відділ безпеки.

Оператор отримує доступ до бази документів, якщо виконуються такі умови:

- користувач виконує роль «Звичайний користувач» або «Відповідальний за відділ безпеки»;
- в списку доступу бази йому або групі, до якої він належить, не заборонено цей доступ;
- в списку доступу бази йому або групі, до якої він належить, надано цей доступ.

Власник бази має особливі повноваження щодо доступу до «своєї» бази.

Якщо користувач є власником бази і виконує роль «Відповідальний за відділ безпеки», він отримує до бази такі види доступу: читання списку документів; читання атрибутів; запис власника; запис списку доступу; запис списку аудита.

Крім цього, встановлюються обмеження, які не дозволяють звичайним користувачам керувати доступом до баз.

Звичайні користувачі не можуть отримати такі види доступу до бази документів: запис атрибутів; перейменування; видалення; запис власника; запис списку доступу; запис списку аудита.

4.3.7.2. Правила розмежування доступу до документів

Можливість працювати з документами повинні мати лише секретаріат, відповідальний/заступник за відділ безпеки.

Користувач отримує доступ до документа, якщо виконуються такі умови:

- рівень допуску користувача не нижчий за рівень доступу документа;
- йому встановлена роль «Звичайний користувач» або йому встановлена роль «Відповідальний за відділ безпеки»;

- в списку доступу документа йому або групі, до якої він належить, не заборонено цей доступ;
- в списку доступу документа йому або групі, до якої він належить, надано цей
- доступ.

Власник бази має особливі повноваження щодо доступу до документів, які містяться в «його» базі. Ці повноваження не залежать від списку доступу бази.

Якщо користувач є власником бази, в якій міститься документ, і виконує роль «Відповідальний за відділ безпеки», він отримує до документа такі види доступу: читання атрибутів доступу; запис власника; запис рівня доступу; запис списку доступу; запис списку аудита.

Крім цього, встановлюються обмеження, які не дозволяють звичайним користувачам керувати доступом до документів.

Звичайні користувачі не можуть отримати такі види доступу до документів: читання атрибутів доступу; запис власника; запис рівня доступу; запис списку доступу; запис списку аудита.

Для виконання вимог до друку експорту та документів в системі діє ще одне правило.

Якщо документ має рівень доступу конфіденційно, користувач отримує доступ на друк або збереження документа у файлі лише за умови введення паролю.

4.3.7.3. Правила розмежування доступу до даних захисту

Доступ до даних захисту слід надавати відповідно до ролі користувача.

Права на читання та запис даних у БД захисту та право на перегляд журналу захисту повинен мати лише користувач із роллю «Відповідальний за відділ безпеки».

Право на читання та зміни значень параметрів конфігурації КЗЗ, безпосередньо пов’язаних із керуванням доступом, повинен мати лише користувач із роллю «Відповідальний за відділ безпеки». Права на читання та

зміну значень інших параметрів конфігурації КЗЗ, права на читання даних про поточну поведінку КЗЗ та права на оперативне керування КЗЗ повинні мати користувачі з ролями «Відповідальний за відділ безпеки» та «Системний адміністратор» відповідно до розподілу обов'язків, який визначається «Планом захисту інформації».

4.3.8. Правила адміністрування КЗЗ

Коригування переліку користувачів із їхніми атрибутами доступу здійснює Відповідальний за відділ безпеки.

Коригування атрибутів доступу баз документів та документів здійснює Відповідальний за відділ безпеки.

Коригування атрибутів доступу файлів та папок здійснює Відповідальний за відділ безпеки.

В окремих випадках атрибути доступу файлів та папок може встановлювати системний адміністратор за узгодженням з адміністратором безпеки. Порядок узгодження повинен визначатись «Планом захисту інформації».

Для всіх користувачів АСВБ заповнюються облікові картки, на підставі яких відповідальний за відділ безпеки вводить, змінює або видаляє інформацію про користувача.

Інсталяцію та поновлення всіх програмних засобів здійснює системний адміністратор.

Усі роботи, які прямо чи опосередковано можуть вплинути на захищеність інформації, проводяться за узгодженням з адміністратором безпеки. Порядок узгодження повинен визначатись документом «Планом захисту інформації».

Повсякденні обов'язки щодо адміністрування виконують відповідальний за відділ безпеки та системний адміністратор. Розподіл обов'язків між ними визначається «Планом захисту інформації».

4.3.9. Реєстрація дій користувачів

КЗЗ повинен вести журнал захисту та надавати адміністратору безпеки зручні засоби його перегляду та настроювання.

Засоби реєстрації повинні забезпечувати можливість реєстрації всіх важливих із точки зору безпеки інформації подій.

У випадку виникнення небезпечної події КЗЗ повинен повідомити про це адміністратора безпеки. Для цього можуть використовуватись такі засоби:

- створення на жорсткому диску файлу із відповідною інформацією;
- друк повідомлення на принтері;
- звуковий сигнал.

4.4. Вимоги до КСЗІ у частині захисту інформації від витоку технічними каналами

Захист ІзОД, яка циркулюватиме в АСВБ, від витоку технічними каналами повинен досягатись шляхом створення на ОІД, де встановлена вказана АС, комплексу технічного захисту інформації, який є невід'ємною складовою КСЗІ АСВБ.

Захист інформації від витоку технічними каналами передбачає:

- аналіз умов функціонування АСВБ, її розташування на ОІД та відносно межі контрольованої зони;
- виявлення каналів можливого витоку інформації;
- розробку заходів із технічного захисту інформації, обґрунтування та вибір технічних рішень із ТЗІ, впровадження КТЗІ на ОІД, розробку необхідної документації;
- проведення атестаційних випробувань КТЗІ.

4.4.1. Загальні вимоги до об'єктів, що захищаються

До об'єктів що захищаються повинні висуватися наступні вимоги:

- реалізація захищеності ІзОД повинна досягатись без застосування екранування приміщення та активних засобів захисту інформації;
- використання пасивних засобів захисту ІзОД у разі виявлення наведених інформативних сигналів у мережі електроживлення, лініях зв'язку і сигналізації та на інших лініях, які мають вихід за межі контрольованої зони;

- забезпечення АСВБ автономним контуром заземлення.

Всі технічні системи та засоби можуть встановлюватись на ОІД за умови сумісності із існуючими засобами захисту та попереднього проведення спеціальних досліджень.

4.4.2. Вимоги до КТЗІ щодо захисту ІзОД від витоку каналами ПЕМВН

Для захисту ІзОД від її витоку каналами ПЕМВН необхідно передбачити наступні технічні заходи захисту:

- на лінію електроживлення, від якої здійснюється електроживлення всіх компонентів, встановлюється мережевий завадозаглушувальний фільтр та розподільчий трансформатор.
- обладнати всі компоненти АСВБ та технічні засоби захисту окремим контуром заземлення опір якого відповідно вимог ТР ЕОТ-95 повинен бути не більше 4 Ом;
- на ОІД видалити всі незадіяні лінійні комунікації;
- унеможливити проходження біля компонентів АСВБ будь яких ліній та комунікацій, які мають вихід за межі контрольованої зони, на відстані, яка не забезпечує захищеність інформації від її витоку за рахунок наведень на них інформативних сигналів.
- унеможливити встановлення біля компонентів АСВБ будь яких технічних засобів, лінії яких мають вихід за межі контрольованої зони, або могли б здійснювати перевипромінення інформативних сигналів від АСВБ.

4.4.3. Вимоги до КТЗІ щодо захисту ІзОД від витоку радіотехнічним каналом Захист ІзОД від витоку радіотехнічним каналом повинен передбачати:

- унеможливлення організаційними та інженерно-технічними заходами несанкціонованого проникнення на ОІД сторонніх осіб з метою встановлення пристроїв технічної розвідки;
- встановлення на ОІД лише технічних засобів, які пройшли спеціальну перевірку на предмет наявності в них приховано встановлених пристроїв технічної розвідки;

- унеможливлення встановлення на лінійно-кабельні комунікації, комунікації життєзабезпечення, які виходять за межі ОІД пристроїв технічної розвідки;
- перевірки приміщення ОІД, лінійно-кабельних комунікацій, комунікацій життєзабезпечення, які виходять за межі ОІД, на наявність приховано встановлених пристроїв технічної розвідки (відеопередавачів);
- унеможливлення після створення КСЗІ та введення в дію АСВБ встановлення на ОІД будь яких технічних засобів, меблів та предметів інтер'єру, які попередньої не пройшли спеціальної перевірки на наявність приховано встановлених пристроїв технічної розвідки (відеопередавачів).

4.3.4. Вимоги до КТЗІ щодо захисту ІОД від її витоку за рахунок візуально-оптичного каналу

Блокування візуально-оптичного каналу повинно передбачати обладнання вікон ОІД непрозорими шторами або жалюзі, які повинні унеможливити огляд ОІД ззовні незалежно від поверху та наявності розташованих навпроти будинків.

4.4. Середовище функціонування

Вимоги до середовища функціонування викладено в ТЗ.

4.5. Вимоги до виявлення та блокування розповсюдження вірусів

Виявлення та блокування розповсюдження вірусів в АСВБ необхідно реалізовувати адміністративно-організаційними, апаратними, програмними та програмно-апаратними способами.

До адміністративно-організаційних слід віднести заборону можливості встановлення та виконання програм, що не відносяться до складу АСВБ.

Підсистема антивірусного захисту повинна забезпечувати:

- функціонування в автоматичному режимі;
- блокування проникнення комп'ютерних вірусів зі змінних носіїв;
- несанкціонованого розповсюджуваних виконавчих файлів;
- лікування комп'ютерних вірусів з занесенням інформації про це у відповідні протоколи КЗЗ;

- автоматичне оновлення антивірусного ПЗ;
- блокування доступу користувачів до зараженої інформації.

5. ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ ТА ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ

За результатами виконання робіт зі створення КСЗІ має бути розроблено наступні документи:

- АС відділу безпеки КО «ТИМ-ТИМ».
- КСЗІ. План захисту інформації;
- КСЗІ. Програма та методики випробувань.

Деякі експлуатаційні документи на КСЗІ можуть бути замінені відповідними документами, що входять до експлуатаційної документації на засоби захисту, що застосовуються в КСЗІ.

6. ВИМОГИ ДО ЗАБЕЗПЕЧЕННЯ РЕЖИМНИХ ЗАХОДІВ У ПРОЦЕСІ РОЗРОБКИ КСЗІ

Під час виконання робіт зі створення та випробувань КСЗІ повинні забезпечуватись заходи щодо унеможливлення ознайомлення зі змістом всіх робіт сторонніми особами, які не будуть приймати участь в обробці ІзОД за допомогою АСВБ.

7. ЕТАПИ ВИКОНАННЯ РОБІТ

Етапи виконання робіт при створенні КСЗІ наведено в табл. 2.5.

Таблиця 2.5 – Етапи виконання робіт при створенні КСЗІ

№	Найменування робіт	Виконавець
1.	Розробка технічного завдання та його узгодження з Державною службою спеціального зв’язку та захисту інформації України	Калуга П.Р.
2.	Проведення заходів щодо захисту інформації від витоку технічними каналами	Калуга П.Р.
3.	Проведення заходів щодо захисту інформації від НСД	Калуга П.Р.
4.	Розробка експлуатаційної документації на КСЗІ	Калуга П.Р.
5.	Розробка «Програми та методики випробувань»	Калуга П.Р.
6.	Розробка експлуатаційних документів КСЗІ	Калуга П.Р.
7	Проведення попередніх випробувань і передача КСЗІ в дослідну експлуатацію	Калуга П.Р.
8.	Навчання користувачів	Калуга П.Р.
9.	Дослідна експлуатація	Калуга П.Р.
10.	Підготовка комплекту документів для проведення експертизи КСЗІ	Калуга П.Р.

8. ПОРЯДОК ВНЕСЕННЯ ЗМІН І ДОПОВНЕНЬ ДО ТЕХНІЧНОГО ЗАВДАННЯ

Зміни до затвердженого технічного завдання на створення КСЗІ в АСВБ, необхідність внесення яких виявлена в процесі виконання робіт, оформлюються окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до ТЗ на створення КСЗІ складається із вступної частини і змінених розділів. У вступній частині зазначається причина складання доповнення. У змінених розділах наводяться номери та зміст змінених розділів та/або пунктів, що скасовуються.

9. ПОРЯДОК КОНТРОЛЮ ТА ПРИЙМАННЯ КСЗІ

Приймання робіт повинно здійснюватись комісією, призначеною Замовником, відповідно до узгодженої програми згідно з вимогами ГОСТ 34.201-89, РД-50-34.698-90.

9.1. Порядок проведення попередніх випробувань

Метою випробувань є встановлення відповідності досягнутого в АСВБ рівня захищеності інформації вимогам ТЗ та визначення готовності до експлуатації.

Оцінку результатам випробувань дає комісія, яку призначає Замовник, за участю Виконавця.

Після завершення випробувань затверджуються акт приймання до дослідної експлуатації.

9.2. Експертиза КСЗІ

Експертиза КСЗІ може проводиться одночасно з попередніми випробуваннями.

Експертиза КСЗІ АСВБ проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації.

Відповідальний за відділ безпеки
КО «ТИМ-ТИМ» Верес В.В.

Розділ 3 ПІДГОТОВКА ДО ВВЕДЕННЯ В ДІЮ КСЗІ

3.1 Складання техноробочого проекту створення КСЗІ

Техноробочий проект КСЗІ в АС розробляється на підставі та у відповідності до ТЗ на створення КСЗІ в АС. На цьому етапі розробляється перелік документів, в я кому описується як саме створюється система, її експлуатація, а також модернізація КСЗІ в АС [34].

Техноробочий проект включає такі етапи [34]:

- *Розробка технічного проекту*

На етапі розробки технічного проекту. Необхідно розробити загальні проекті рішення, для реалізації вимог ТЗ на КСЗІ, рішення щодо структури КСЗІ, її алгоритмів функціонування та умов використання засобів захисту, рішень щодо архітектури КЗЗ та механізмів реалізації, визначення профілем послуг безпеки інформації.

Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до рівня гарантій реалізації послуг безпеки згідно зі специфікаціями НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000, НД ТЗІ 3.7-003-05.

Виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ.

- *Розробка робочого проекту*

На етапі створення робочого проекту виконується опис порядку функціонування АС та настанови щодо забезпечення цього порядку обслуговуючим персонал і користувачами, порядку супроводження КСЗІ впродовж життєвого АС.

Необхідно розробити наступні документи:

1. Техноробочий проект.

«ЗАТВЕРДЖЕНО»
Відповідальний за відділ
безпеки комерційної організації
«ТИМ-ТИМ»
_____ В.В. Верес
«17» листопада 2020 року

АВТОМАТИЗОВАНА СИСТЕМА ВІДДІЛУ БЕЗПЕКИ КО «ТИМ-ТИМ» (шифр – «АСВБ»)

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ (шифр – КСЗІ «АСВБ»)

ТЕХНОРОБОЧИЙ ПРОЕКТ

Київ-2020

1. ВІДОМІСТЬ ПРОЕКТНОЇ ДОКУМЕНТАЦІЇ ДО ТЕХНОРОБОЧОГО ПРОЕКТУ КСЗІ В АСВБ

Таблиця 3.1 – Відомість проектної документації до Техноробочого проекту

№ п/п	Найменування	Кіл-ть арк.
1.	Перелік відомостей, що відносяться до конфіденційної інформації КО «ТИМ-ТИМ» та якій надається гриф обмеження доступу	2
2.	Акт визначення вищого ступеню обмеження доступу інформації, яка циркулюватиме на ОІД відділу безпеки КО «ТИМ-ТИМ»	1
3.	Акт обстеження середовищ функціонування АС на ОІД відділу безпеки КО «ТИМ-ТИМ».	1
4.	Модель загроз для інформації, яка планується до циркуляції в АС класу 2 на ОІД КО «ТИМ-ТИМ»	15
5.	Політика безпеки інформації, яка циркулює в АС класу 2 КО «ТИМ-ТИМ»	6
6.	План захисту інформації	14
7.	АС відділу безпеки КО «ТИМ-ТИМ». Комплексна СЗІ. ТЗ	17

2. ВІДОМІСТЬ ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ ДО ТЕХНОРОБОЧОГО ПРОЕКТУ КСЗІ ЗІ

Таблиця 3.2 – Відомість експлуатаційної документації

№ п\п	Найменування	Кіл-ть арк.
1.	Паспорт-формуляр на АС класу 2 відділу безпеки КО «ТИМ-ТИМ»	4

3. ПОЯСНЮВАЛЬНА ЗАПИСКА ДО ТЕХНОРОБОЧОГО ПРОЕКТУ КСЗІ АС КЛАСУ 2 ВІДДІЛУ БЕЗПЕКИ КО «ТИМ-ТИМ»

3.2. Загальні відомості

Повна назва: Комплексна система захисту в автоматизованій системі класу 2 ОІД – приміщення відділу безпеки КО «ТИМ-ТИМ».

Розробка КСЗІ в АСВБ є складовою частиною робіт з впровадження АСВБ в діяльність, що виконуються між КО «ТИМ-ТИМ» та «ЛУН»

Замовник: КО «ТИМ-ТИМ».

Виконавець: «ЛУН»

Підставою для виконання робіт по створенню КСЗІ в АСВБ є ТЗ на створення КСЗІ в АСВБ.

Організаційні та організаційно-технічні заходи щодо захисту інформації в АСВБ що зазначені в цьому Техпроекті здійснюються у період з 20.06.2020 року по 20.11.2020 року.

Фінансування робіт здійснюється за рахунок коштів передбачених для безпеки в КО «ТИМ-ТИМ».

КСЗІ в АСВБ призначена для:

- забезпечення визначеної для АСВБ політики безпеки інформації; розмежування доступу користувачів АСВБ до інформації різних категорій конфіденційності;
- блокування несанкціонованих дій з ІзОД;
- реєстрації спроб реалізації загроз інформації та сповіщення адміністраторів безпеки про факти несанкціонованих дій з ІзОД;
- забезпечення спостереженості інформації шляхом контролю за діями користувачів АС 2 та реєстрації подій, які мають відношення до безпеки інформації; підтримання цілісності критичних ресурсів АСВБ;
- організації обліку, зберігання та обігу матеріальних носіїв інформації, які використовуються в АСВБ;
- забезпечення управління засобами захисту КСЗІ та контролю за її функціонуванням. захисту ІзОД від витоку її технічними каналами.

Під час проектування КСЗІ в АС 2 необхідно забезпечити: заданий рівень захисту ІзОД, яка циркулюватиме в АСВБ; економічну доцільність прийнятих рішень.

Відомості які зазначають структуру та склад АСВБ, а саме: структура та обладнання, що використовується в АСВБ; ПЗ, що використовується в основних складових АСВБ; характеристика інформації та технологія її обробки в АСВБ; характеристики обслуговуючого персоналу АСВБ; користувачі, об’єкти, процеси та їх атрибути в АСВБ, наведені в ТЗ.

3.3. Основні технічні рішення та заходи при створенні КСЗІ в АСВБ

3.3.1. Технічні заходи із захисту інформації в АСВБ

Проведення інсталяції та перевірки працездатності в АСВБ наступного ПЗ:

- ОС Windows 10;
- драйвери системних пристроїв АСВБ;
- пакет прикладних програм Microsoft Office 2010;
- антивірусна програма ESET Smart Security 2020.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Проведення інсталяції та модернізації СЗІ «Захист» відповідно документації з інсталяції вказаної системи.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Проведення адміністрування СЗІ «Захист», щодо впровадження функціональних послуг захисту інформації наведених в ТЗ, а саме вона повинна забезпечувати наступний функціональний профіль захищеності: КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Встановлення на лінію електроживлення від якої здійснюється електроживлення всіх компонентів АСВБ мережевого протизавадного фільтра «Альтер».

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Встановлення на лінію охоронної сигналізації протизавадного фільтра «КЦД». Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Підключення всіх компонентів АСВБ до контуру заземлення.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Проведення робіт щодо пошуку в приміщенні можливо потай встановлених пристроїв технічної розвідки.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

3.3.2. Будівельно-монтажні роботи із захисту інформації в АС

Обладнання віконного отвору металевими гратами.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

3.3.3. Організаційні заходи із захисту інформації в АС

Складання Інструкції користувачу АСВБ в якій повинно бути відображено наступні заходи:

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Складання Інструкції з адміністрування системи АСВБ в якій обов’язково повинно бути зазначено: порядок дій адміністратора безпеки; порядок дій системного адміністратора; порядок дій адміністратора документів

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Визначення обмежень співробітників організації.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Складання правил адміністрування компонент інформаційної системи: порядок видалення інформації в мережі; порядок зберігання інформації на підприємстві.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Складання Інструкції по правилам управління паролями в АСВБ в який повинно бути зазначено:

- порядок присвоєння реєстраційних імен користувачів;
- порядок видачі паролів користувачам;
- порядок зміни паролів та реєстраційних імен користувачів;
- порядок вилучення паролів;
- склад імен та паролів;
- обов’язки користувача під час поводження користувачів з паролями.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Складання Інструкції з режимних заходів захисту інформації під час її циркуляції в АСВБ в який повинно бути зазначено:

- загальні вимоги до організації обробки конфіденційної інформації в АСВБ;
- порядок дій користувачів щодо забезпечення режимних заходів захисту конфіденційної інформації;
- порядок друку і обліку користувачами документів, які містять ІзОД;
- порядок знищення або збереження ІзОД, яка міститься на машинних носіях;

- порядок обліку файлів які містять ІзОД, на машинному носії інформації;
- порядок обліку машинного носія інформації;
- відповідальність користувача.

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

Складання Інструкції про порядок оперативного відновлення функціонування АС класу 2 відділу безпеки КО «ТИМ-ТИМ» в який повинно бути зазначено:

- порядок дій адміністраторів при виявленні НСД;
- порядок дій представників служби захисту інформації та охорони при виникненні надзвичайних ситуацій;

Відповідальний: Верес В.В.

Відмітка про виконання: Акапулькова Л.І.

Підпис виконавця:_____

3.4. Показники захищеності АСВБ від НСД

Відповідно відомостей наведених в ТЗ для АС необхідно реалізувати наступний функціональний профіль захищеності: КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2. Реалізацію вказаного функціонального профілю буде здійснювати застосована система захисту інформації – КЗЗ від НСД «Захист».

3.5. Порядок постачання засобів захисту інформації та/або розробки технічних вимог на їх розробку. Організація постачання та впровадження в АСВБ технічних засобів захисту здійснюється відділом безпеки КО «ТИМ-ТИМ».

3.6. Порядок проведення тестування, пусконалагоджувальних робіт та проведення попередніх випробувань КСЗІ в АСВБ

Пусконалагоджувальні роботи включають в себе виконання технічних та організаційних заходів захисту інформації що передбачені в п.3 цієї

Пояснювальної записки до Техноробочого проекту. Попередні випробування проводяться після виконання в повному обсязі пусконалагоджувальних робіт.

Спеціалістами відділу безпеки КО «ТИМ-ТИМ» за результатами попередніх випробувань оформляється «Протокол випробувань», в якому міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт. Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

3.7. Порядок адаптації засобів захисту до умов функціонування КСЗІ

Режим роботи всіх компонентів АСВБ, пристроїв захисту повинен забезпечувати надійну їх роботу та забезпечувати захист інформації з урахуванням фізичного та кліматичного середовища розташування.

3.8. Схеми розміщення АСВБ, кабельного обладнання, мереж живлення та систем заземлення

Монтаж компонентів АСВБ на ОІД повинен відповідати вимогам нормативних документів з ТЗІ.

Встановлення біля АСВБ будь яких технічних пристроїв на відстані менш ніж 1,5 метрів або прокладання будь-яких ліній та кабелів на відстані менш ніж 1 метр – заборонено.

3.9. Заходи щодо підготовки КСЗІ до введення у дію

Для введення КСЗІ в дію необхідно виконати наступні заходи:

- провести налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів АСВБ на ту кількість, яка визначена відповідними списками;
- визначити порядок контролю за діями користувачів;
- визначити порядок контролю цілісності програмного забезпечення та баз даних захисту в АСВБ;

- визначити порядок навчання і підвищення кваліфікації персоналу, який має доступ до АСВБ;
- визначити заходи із перевірки кваліфікації користувачів та адміністраторів безпеки АСВБ.

3.10. Порядок проведення експертизи КСЗІ в АС 2

Експертиза КСЗІ в АСВБ проводиться фірмою-ліцензіатом яка має відповідну ліцензію на виконання вказаних робіт від Адміністрації Державної служби спеціального зв'язку та безпеки України.

Після проведеної експертизи на КСЗІ в АСВБ відповідним чином видається «Атестат відповідності КСЗІ».

Відповідальний за відділ безпеки
КО «ТИМ-ТИМ» Верес В.В.

3.2 Підготовка КСЗІ до введення в дію

Проводиться робота з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в АС. Здійснюється створення СЗІ, якщо цього не було зроблено на попередніх етапах. В основному має бути завершені робота і затверджені документи, що входять до Плану захисту [21].

Проект КСЗІ розробляється на підставі та у відповідності до ТЗ на створення ІТС. Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. Проект КСЗІ виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робочий проект [21].

Для всіх стадій розробки проекту КСЗІ склад документації визначається ТЗ на КСЗІ, види та зміст – ГОСТ 34.201, НД ТЗІ 2.5 – 004. Документація на програмні засоби виконується згідно з комплексом стандартів ЄСПД, на технічні засоби – згідно з комплексом стандартів ЕСКД [21].

Необхідно розробити наступні документи:

1. Паспорт-формуляр.

«ЗАТВЕРДЖЕНО»
Відповідальний за відділ
безпеки комерційної організації
«ТИМ-ТИМ»
_____ В.В. Верес
«25» листопада 2020 року

ПАСПОРТ-ФОРМУЛЯР

НА АВТОМАТИЗОВАНУ СИСТЕМУ 2 КЛАСУ ВІДДІЛУ БЕЗПЕКИ

КОМЕРЦІЙНОЇ ОРГАНІЗАЦІЇ «ТИМ-ТИМ»

Київ-2020

1. Загальні положення

1.1. Паспорт–формуляр на АС класу 2 відділу безпеки КО «ТИМ-ТИМ».

1.2. Безпосередня відповідальність за ведення Паспорту покладається на керівника СЗІ в АСВБ.

Заповнювати та вносити зміни до Паспорта мають право тільки представники СЗІ на підставі звітних документів.

2. Загальні відомості про ОІД, на якому знаходиться АСВБ

2.1. ОІД – приміщення № 2 КО «ТИМ-ТИМ» орендує 2 поверхи в торгівельно-розважальному центрі «IQ», біля станції метро «Позняки», по вулиці Гришко 3а. Загальна площа магазину 550 кв.м. (по 225 кв.м. відповідно на кожному поверсі).

2.2. Характеристика приміщення, у якому розташовано ОІД:

- зовнішні стіни – цегельні, товщина яких становить 500 мм;
- внутрішні стіни – цегельні, товщина яких становить 450 мм;
- підлога – залізобетонні плити, вкрита лінолеумом;
- стеля – залізобетонні плити, вкрита лінолеумом;
- кількість вікон – 9;
- кількість вхідних дверей – одні;
- двері – дерев’яні, оббиті залізними листами, обладнані замковими пристроями та датчиками охоронної сигналізації

2.3. Згідно з «Актом визначення вищого ступеню обмеження доступу інформації, яка циркулюватиме на ОІД – приміщення № 2 відділу безпеки здійснює такі види інформаційної діяльності:

2.3.1. Обробка ІзОД за допомогою АСВБ з вищим грифом обмеження доступу «цілком конфіденційно».

2.3.2. Робота з паперовими документами, що містять інформацію з вищим грифом обмеження доступу «цілком конфіденційно»

2.4. ОІД обладнано такими системами життєзабезпечення:

- система міського телефонного зв’язку;
- система охоронної сигналізації; система пожежної сигналізації;

- система електроживлення;
- система опалення;
- система заземлення.

Лінія міського телефонного зв’язку прокладена по стінах неекранованими проводами і має вихід за межі контрольованої зони КО «ТИМ-ТИМ» до приміщення АТЗІ.

Лінія пожежної сигналізації прокладена постелі та стінах неекранованими проводами до пульта пожежної сигналізації, який встановлено в службовому приміщенні охорони на контрольно-пропускному пункті ВАТ «ЛУН».

Лінія охоронної сигналізації прокладена по стінах неекранованими проводами до пульта охоронної сигналізації, який встановлено в службовому приміщенні охорони на контрольно-пропускному пункті ВАТ «ЛУН».

Труби системи опалення встановлено під підвіконням та підводяться до внутрішньої котельні ВАТ «ЛУН».

Кабель системи заземлення підключено до електричних розеток та виведено до контуру заземлення, який знаходиться в межах контрольованої зони ВАТ «ЛУН».

Лінії електроживлення прокладено в стінах неекранованими мідними проводами та виводяться до електричного розподільчого щита, який знаходиться в межах контрольованої зони КО «ТИМ-ТИМ». Від розподільчого щита кабель електроживлення прокладено до трансформаторної підстанції, яка знаходиться в межах контрольованої зони ВАТ «ЛУН».

2.5. Схема розміщення ОІД в приміщенні № 2 ВАТ «ЛУН». та відносно межі контрольованої зони КО «ТИМ-ТИМ».

2.6 Охорона комерційної організації «ТИМ-ТИМ» в цілому здійснює відомча охорона відповідно розпоряджень та інструкцій ВАТ «ЛУН».

2.7. Схема розміщення меблів інтер’єру, засобів технічного захисту, основних та допоміжних технічних засобів, на ОІД.

3. Призначення комплексної системи захисту інформації в АСВБ:

КСЗІ в АСВБ призначена для:

- забезпечення визначеної для АСВБ політики безпеки інформації;
- розмежування доступу користувачів АСВБ до інформації різних категорій конфіденційності;
- блокування несанкціонованих дій з ІзОД;
- реєстрації спроб реалізації загроз інформації та сповіщення адміністраторів безпеки про факти несанкціонованих дій з ІзОД;
- забезпечення спостереженості інформації шляхом контролю за діями користувачів АСВБ та реєстрації подій, які мають відношення до безпеки інформації;
- підтримання цілісності критичних ресурсів АСВБ;
- організації обліку, зберігання та обігу матеріальних носіїв інформації, які використовуються в АСВБ;
- забезпечення управління засобами захисту КСЗІ та контролю за її функціонуванням.
- захисту ІзОД від витоку її технічними каналами.

Таблиця 3.3 – Відомості про закріплення АСВБ під час експлуатації

Посада	**Прізвище особи, відповідальної за експлуатацію**	**Номер і дата наказу**		**Підпис відповідальної особи**
		про закріплення	про відкріплення	

3.2. Технічні засоби, засоби технічного захисту

Таблиця 3.4 – Основні технічні засоби

№ з/п	**Найменування та склад технічних засобів**	**Тип**	**Заводський №, інвентарний №**	**Дата і № документа, на підставі якого встановлено пристрій**	**Дата і № документа, на підставі якого вилучено пристрій**

Таблиця 3.5 – Склад програмного забезпечення АСВБ

№ з/п	**Найменування і версія програмного продукту**	**Дата і підпис посадової особи служби захисту інформації в АС**		**Відмітки про проведення перевірки програмного забезпечення**
		про встановлення	**про вилучення**	

Таблиця 3.6 – Допоміжні технічні засоби

№ з/п	Найменування допоміжних технічних засобів	Тип	Заводський (інвентарний) №	Примітки

Таблиця 3.7 – Засоби технічного захисту інформації

№ з/п	Найменування та склад технічних засобів	Тип	Заводський (інвентарний) №	Дата і № документа, на підставі якого встановлено пристрій	Дата і № документа, на підставі якого вилучено пристрій

Таблиця 3.8 – Відповідальні за ОІД

Посада	Прізвище, ім'я, по батькові	№ наказу, дата	
		про призначення	про звільнення

Таблиця 3.9 – Реєстрація проведених робіт

Дата проведення робіт	Найменування технічного засобу та вид проведених робіт	Підстава для проведення робіт	Прізвище та ініціали особи, яка виконувала роботи	Підпис

Таблиця 3.10 – Відмітки про проведення перевірки складу програмного забезпечення АСВБ

Дата перевірки	Результат перевірки	Посада, прізвище та ініціали особи, яка здійснювала перевірку	Підпис

Таблиця 3.11 – Періодичні, контрольні, інспекційні та інші перевірки стану комплексної системи захисту інформації

Дата	Вид перевірки	Результати перевірки	Дата, № Акту перевірки	Відмітки про усунення недоліків

Таблиця 3.12 – Картка-замісник пакета документів на КСЗІ в АСВБ

№ з/п	Найменування документа	Номер та дата документа	Номер справи, у якій зберігається документ	Примітка

Особливі примітки

_____

_____

3.3 Попередні випробування КСЗІ в АС

Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію. Під час випробувань перевіряються працездатності КСЗІ та відповідність її вимогам ТЗ [24].

Попередні випробування проводяться згідно з програмою та методиками випробувань. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІТС. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50 – 34.698 [24].

Попередні випробування організовує замовник ІТС, а проводять розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІТС створюється комісія. Головою комісії призначається представником замовника [24].

Результати попередніх випробувань оформлюються «Протоколом випробувань», де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт [24].

Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію [24].

Необхідно розробити наступні документи:

1. Протокол попередніх випробувань комплексної системи захисту інформації, Додаток Е.
2. Акт приймання комплексної системи захисту інформації, Додаток Є.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні **задачі**:

- Обстеження об’єкту як підготовки до розробки КСЗІ;
- Розробка політики, плану та ТЗ для АС класу;
- Підготовка до введення в дію КСЗІ.

В результаті виконання кваліфікаційної роботи було проведено розробку КСЗІ для КО «ТИМ-ТИМ». Відповідно було розроблено усю супровідну документацію по впровадженню КСЗІ. КСЗІ – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів ЗІ.

Організаційні заходи ЗІ – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів забезпечення ТЗІ. Вони являються обов’язковою складовою побудови КСЗІ. Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом. Діяльність з побудови КСЗІ відноситься до ліцензованих видів діяльності і ліцензується службою Державною службою спеціального зв’язку України.

При побудові КСЗІ можна виділяються наступні етапи:

- Обґрунтування необхідності створення КСЗІ.
- Обстеження середовищ функціонування АС.
- Визначення потенційних загроз для інформації.
- Розробка політики безпеки інформації, плану захисту інформації в АС та ТЗ на створення КСЗІ в АС.
- Складання технороботочого проекту створення КСЗІ.
- Підготовка КСЗІ до введення в дію.
- Попередні випробування КСЗІ в АС.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації;

2. ДБН А.2.2-3-97 Проектування. Склад, порядок розробки, узгодження і затвердження проектної документації для будівництва;

3. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: постанова Кабінету Міністрів України № 821 від 16.11.2016; // Офіційний вісник України від 02.12.2016. – 2016. – № 93, стор. 39, стаття 3033.

4. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення;

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

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

7. Етапи побудови КСЗІ. URL: http://altersign.com.ua/korysnainformacija/pobudova-kszi/etapy-pobudovykszi. [15] Положення про державну експертизу в сфері технічного захисту інформації: наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України № 93 від 16.05.2007 року // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/z0820-07 (дата звернення: 12.07.2017).

8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР;

9. Закон України «Про інформацію» від 2 жовтня 1992 року №2658-XII;

10. Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України № 1126 від 8.10.1997. // База даних «Законодавство

України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/1126-97- %D0%BF (дата звернення: 12.07.2017).

11. Манжай О. В. Правові засади захисту інформації: навчальний-посібник. Харків : Ніка Нова, 2014. 104 с.

12. НД 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106341 (дата звернення: 12.07.2017).

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

14. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

15. НД ТЗІ 1.1-004-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

16. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення;

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

18. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

19. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

20. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 (дата звернення: 12.07.2017).

21. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи;

22. 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;

23. НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів безпеки від несанкціонованого доступу;

24. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

25. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106349 (дата звернення: 12.07.2017).

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

27. НД ТЗІ 3.7-003-05. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://dstszi.kmu.gov.ua/dstszi/doccatalog/doc ument?id=106350 (дата звернення: 12.07.2017).

28. Носов В. В., Манжай О. В. Організація та забезпечення інформаційної безпеки: навчальний посібник. Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. 216 с.

29. Перелік суб’єктів господарювання, що мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається

Кабінетом Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=277736&cat_id=266373 (дата звернення: 12.07.2017).

30. Побудова Комплексних Систем Захисту Інформації (КСЗІ). URL: http://www.iqusion.com/ua/produkti-iservisi/zakhist-informatsiji/120-kszi.html.

31. Положення про державний контроль за станом технічного захисту інформації: наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України №87 від 16.05.07. // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon5.rada.gov.ua/laws/show/z0785-07 (дата звернення: 12.07.2017).

32. Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом Держспецзв'язку України від 16.05.07 № 93, зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087.

33. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Затверджено постановою КМУ від 16.02.98 № 180;

34. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. № 1229/99;

35. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних, та інформаційно-телекомунікаційних системах: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № Порядок створення комплексних систем захисту інформації, проведення експертизи та видачі Експертних висновків і Атестатів відповідності. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=39479&cat_id=38689&ctime=1127824089206 (дата звернення: 11.09.2017).

36. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06 // Офіційний вісник України. - 2006. - № 13 (12.04.2006), стор. 164, стаття 878.

37. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994; [із змінами і доповненнями на 19.04.2014] // Відомості Верховної Ради України. – 1994. – № 31 (02.08.1994). – ст. 286.

38. Про інформацію: закон України від 02.10.1992; [із змінами і доповненнями на 01.01.2017] // Відомості Верховної Ради України. – 1992. – № 48 (01.12.1992). – ст. 650.

39. Тимчасове положення про категоріювання об’єктів (КОКО-95). Затверджено наказом Державної служби України з питань ТЗІ від 9 червня 1995р. № 25.

ДОДАТОК А

КОМЕРЦІЙНА ОРГАНІЗАЦІЯ «ТИМ-ТИМ»
НАКАЗ
03.11.2020 №03-003
Про затвердження Переліку відомостей, що відноситься до конфіденційної інформації КО «ТИМ-ТИМ» та якій надається грифи обмеження доступу та «Конфіденційна інформація»

На виконання вимог Закону України «Про інформацію» та п. 2 постанови Кабінету Міністрів України від 27.11.98 р. N 1893 (зі змінами від 01.10.2014) «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави»

НАКАЗУЮ:

1. Затвердити Перелік конфіденційної інформації, яка належіть комерційній організації «ТИМ-ТИМ» і якій надається грифи обмеження доступу та «Конфіденційна інформація» (надалі – Перелік), що додається.

2. Керівникам структурних підрозділів та самостійних відділів:

2.1. Довести цей Перелік до відома працівників в частині, що їх стосується.

2.2. Забезпечити контроль за використанням та збереженням інформації з грифом обмеженого доступу «Для службового користування» та «Конфіденційна інформація»

3. Контроль за роботою з документами, які містять конфіденційну інформацію покласти на відповідального за відділ безпеки (Верес В.В.).

4. Контроль за нерозголошення інформації з грифом обмеженого доступу «Для службового користування» покласти на відповідального відділ безпеки (Верес В.В.).

5. Контроль за виконанням цього наказу залишаю за собою.

Генеральний директор
комерційної організації «ТИМ-ТИМ» Тимощук В.С.

ДОДАТОК Б

«ЗАТВЕРДЖУЮ»
Генеральний директор
комерційної організації
«ТИМ-ТИМ»
_____ Тимощук В.С.
«03» листопада 2020 року

АКТ
Визначення вищого ступень обмеження доступу інформації, яка циркулюватиме на ОІД – приміщення № 1 відділу безпеки комерційної організації «ТИМ-ТИМ»

Комісія в складі:
голови: Генеральний директор КО «ТИМ-ТИМ» Тимощук В.С.;
члена: відповідального за відділ безпеки КО «ТИМ-ТИМ» Верес В.В., заступник відповідального за відділ безпеки КО «ТИМ-ТИМ» Кум С.А.

Відповідно до вимог НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», провела визначення вищого ступеню обмеження доступу інформації, яка циркулюватиме на ОІД – приміщення № 1 відділу безпеки КО «ТИМ-ТИМ».

Комісією встановлено:

Вищий гриф обмеження доступу інформації, яка планується до циркуляції на об’єкт інформаційної діяльності:

- інформація на паперових носіях інформації – «конфіденційно»;
- мовна інформація – без обмеження доступу.

Висновок:

Вищий гриф обмеження доступу інформації, яка циркулюватиме на ОІД – «конфіденційно».

Голова комісії:
Генеральний директор комерційної
організації «ТИМ-ТИМ» Тимощук В.С.

Члени комісії:
Відповідального за відділ безпеки
комерційної організації «ТИМ-ТИМ» Верес В.В.

Заступник відповідального за відділ безпеки
комерційної організації «ТИМ-ТИМ» Кум С.А.

ДОДАТОК В

«ЗАТВЕРДЖУЮ»
Генеральний директор
комерційної організації
«ТИМ-ТИМ»
_____ Тимощук В.С.
«03» листопада 2020 року

АКТ
обстеження ОІД

Обстеження на ОІД проведено комісією у складі:

голови: Генеральний директор КО «ТИМ-ТИМ» Тимощук В.С.;

члена: відповідальний за відділ безпеки КО «ТИМ-ТИМ» Верес В.В., заступник відповідального за відділ безпеки КО «ТИМ-ТИМ» Кум С.А.

Комісія розглянула та проаналізувала:

1. ситуаційний план компанії;
2. схеми електроживлення та контрольованих зон;
3. схеми комунікацій, що мають вихід за межі контрольованих зон;
4. наявність НД ТЗІ;
5. встановленого ПЗ.

Комісія постановила:

1. В робочому приміщенні, де циркулює така інформація:

1.1. Мовна інформація вголос та під час розмов між співробітниками цього організації. Гриф обмеження доступу – конфіденційно.

1.2. Інформація в ПЕОМ. Гриф обмеження доступу – конфіденційно.

2. Відстань до меж контрольованої зони.
3. Підстанція електроживлення виходить за межи контрольованої зони.
4. Система заземлення – виходить за межі контрольованої зони.
5. Системи зв’язку виходять за межи контрольованої зони.
6. У наявності всі НД ТЗІ.
7. ПЗ потребує оновлення.

Висновки:

Стан захищеності інформація на ОІД не відповідає нормативним документам.

Рекомендації:

1) Розробити модель загроз для ІзОД;

2) Розробити технічні вимоги та завдання з питань ТЗІ;

3) Згідно моделі загроз виявити можливі канали витоку інформацій та перекрити їх.

Голова комісії:
Генеральний директор комерційної
організації «ТИМ-ТИМ» Тимощук В.С.

Члени комісії:
Відповідальний за відділ безпеки
комерційної організації «ТИМ-ТИМ» Верес В.В.
Заступник відповідального за відділ безпеки
комерційної організації «ТИМ-ТИМ» Кум С.А.

ДОДАТОК Г

«ЗАТВЕРДЖУЮ»
Генеральний директор
комерційної організації
«ТИМ-ТИМ»
_____ Тимощук В.С.
«03» листопада 2020 року

МОДЕЛЬ ЗАГРОЗ
для ІзОД, яка планується до циркуляції в АС класу 2 на ОІД – приміщення № 1 КО «ТИМ-ТИМ»

1. НОРМАТИВНІ ПОСИЛАННЯ

Закон України «Про інформацію» від 02.10.1992 № 2657-XII (Редакція станом на 21.05.2015);

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР (Редакція станом на 19.04.2014);

Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (Редакція станом на 30.09.2015);

Постанова Кабінету Міністрів України «Про затвердження Правил захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.06 р. № 373 (Редакція станом на 13.10.2011);

Постанова Кабінету Міністрів України «Про затвердження інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27.11.98 р. № 1893 (Редакція станом на 17.10.2014);

ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт» (Чинний від 01.07.1997 р.);

ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» (Чинний від 01.01.1998 р.);

НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» (Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22);

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» (Затверджений наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53);

НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 р. №125).

2. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Модель загроз для інформації АС класу 2 КО «ТИМ-ТИМ», призначеної для обробки інформації з грифом «для службового користування» та «конфіденційно» містить відомості про можливі загрози для ІзОД, а також опис дій можливого порушника правил роботи в АС.

Модель загроз визначає склад і джерела загроз, оцінку можливості їх прояву, шляхи їх здійснення, оцінку очікуваного збитку від реалізації загроз.

Модель загроз призначена для аналізу ризиків, визначення політики інформації

безпеки та вимог до КСЗІ, формування планів безпеки, реалізації організаційних, первинних і основних технічних заходів захисту інформації, що підлягає захисту, і контролю функціонування КСЗІ.

3. МОДЕЛЬ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ, ЩО ПЛАНУЄТЬСЯ ДО ЦИРКУЛЯЦІЇ В АС КЛАСУ 2

3.1 Загальна структурна схема та склад обчислювальної системи АС

Зовнішній контроль стану безпеки.

Схема ситуаційного плану. Комерційна організація «ТИМ-ТИМ» Торгова компанія «ТИМ-ТИМ» орендує 2 поверхи в торгівельно-розважальному центрі «IQ», біля станції метро «Позняки», по вулиці Гришко 3а. Загальна площа магазину 550 кв.м. (по 225 кв.м. відповідно на кожному поверсі).

Контроль доступу на контрольовану зону торгівельно-розважального центру «IQ» здійснюється з використанням організаційних для співробітників, що працюють на території центру та технічними заходами захисту для запобігання надзвичайних ситуацій.

Контроль доступу до комерційної підриємства «ТИМ-ТИМ» здійснюється з використанням технічних.

Централізована система зберігання і обробки даних.

Основними технічними засобами централізованої системи зберігання та обробки даних є:

- сервери;
- зовнішня система зберігання даних;
- поштовий сервер.

Спеціалізоване ПЗ.

Спеціалізоване ПЗ, призначене для ведення обліку та експлуатації інформаційно-телекомунікаційної системи.

Ядро комутації та маршрутизації мережі.

Основними технічними засобами ядра комутації та маршрутизації мережі є:

- міжмережевий екран;
- маршрутизатор;
- система запобігання мережним вторгненням.

Локальна мережа користувачів центрального рівня.

Основними технічними засобами локальної мережі користувачів є: користувачі та адміністратори.

Загальна схема роботи компанії полягає у тому що комп’ютери об’єднані в єдину локальну мережу по схемі клієнт-сервер. Головним носієм і центром БД, обліку і так далі знаходяться в головному сервері БД, доступ до якого, в цілях безпеки, мають лише оператори. Для зв’язку використовуються кабелі на основі витих пар, які забеспечубть необхідну швидкість передачі інформації. Комп’ютери, які використовують працівники закладу, мають стандартну технічну характеристику, необхідну для швидкої і якісної робот з БД. На відміну від комп’ютерів, сервери завжди знаходяться у включенному стані. На випадок збоїв з електропостачанням в серверній встановлені ДБЖ.

3.2 Технічні характеристики каналів зв’язку

Основна частина циркулюючої у АС інформації, передається через комп’ютерну мережу, що базується на кабелях на основі витої пар. Також використовується система міського телефоного зв’язку.

3.3 Характеристики інформації, що обробляється

Відповідно до функціонального призначення на ОІД плануються такі види інформаційної діяльності:

- передача мовної інформації, що містить інформацію з вищим грифом обмеження доступу – «конфіденційно»;
- обробка ІзОД в АС класу 2 з грифом обмеження «конфіденційно» та «для службового користування»;
- робота з паперовими документами, що мають гриф обмеження доступу «конфіденційно» та «для службового користування»;
- ІзОД, що надходить та обробляється в АС зберігається у вигляді структурованих або неструктурованих файлів за технологією «1 файл – 1 документ».

Інформація, що обробляється в системі, підлягає захисту відповідно до статей 18 та 23 Закону України «Про інформацію».

Згідно Акт визначення вищого ступень обмеження доступу інформації, яка циркулюватиме на ОІД – приміщення № 1 відділу безпеки комерційної організації «ТИМ-ТИМ» від 03 листопада 2020 року. Плануються такі види інформаційної діяльності на ОІД:

- інформація на паперових носіях інформації – «конфіденційно»;
- інформація АС класу 2 – «конфіденційно»;
- мовна інформація – «конфіденційно».

3.4 Характеристики фізичного середовища

Фізичне середовищє комерційної підприємтсва складається з:

- приміщення яке складається з 5 кімнат та туалет;
- 100 розеток під пристрої;
- 12 розеток під стаціонарний телефон;
- 6 принтер-сканер-ксерокс;
- 12 телефонів;
- 21 ПК;
- сервер з БД і сервер системи управління мережним обладнанням захисту – 6;
- 9 вікон;
- 10 датчиків пожарної сигналізації;
- 9 датчиків розбитого скла;
- 6 камер спостереження;
- 10 датчиків руху;
- 1 ПК для відео спостереження, який не під’єднаний до локальної мережі;
- 1 вихід;
- Сходи, що ведуть на другий поверх, де знаходяться всі відділи та керівництво.

ОІД обладнено наступними системами життєзабезпечення:

- дротова локальна мережева система;
- система міського телефоного зв’язку;
- система охоронної сигналізації;
- система пожежної сигналізації;
- система безперервного електроживлення;
- система кондиціювання;
- система опалення.

3.5 Характеристики персоналу та користувачів АС

Суб'єкти, що мають доступ до технічних засобів АС, поділяються на такі категорії користувачів:

Системний адміністратор (СА). Має повноваження щодо конфігурування операційних систем, програмного, апаратного забезпечення користувачів, активного мережного обладнання, системи зберігання даних, здійснює адміністрування поштового серверу, мережного обладнання та мережних засобів захисту, засобів що використовуються для управління зазначеним обладнанням. Системний адміністратор має адміністративні права в операційних системах зазначених технічних засобів та, відповідно, повний доступ до технологічної інформації, що на них зберігається та обробляється. СА здійснює віддалене адміністрування мережного обладнання. Має повноваження на адміністрування баз даних.

Відповідальний за відділ безпеки (ВБ). Має повноваження щодо конфігурування засобів захисту обладнання, баз даних, додавати до відома та забезпечувати виконання вимог діючих нормативних та організаційно-розпорядчих документів щодо захисту інформації. Відповідальний за безпеку здійснює адміністрування засобів захисту та загальний контроль за станом безпек, контролює відповідність настроювань програмних та технічних засобів встановленій політиці безпеки. Для забезпечення можливості контролю ВБ може мати обмежені облікові записи на всіх компонентах системи, що дозволяють йому виключно перегляд певної конфігураційної і звітної інформації на серверах та активному мережному обладнанні системи. ВБ має адміністративні права в операційних системах зазначених технічних засобів та, відповідно, повний доступ до технологічної інформації, що на них обробляється.

Користувач (К). Має повноваження, відповідно до своїх повноважень, щодо перегляду конфіденційної інформації, створення, перегляд та модифікації даних внутрішнього документообігу та необхідних для ведення бази даних довідників, які не містять персональних даних, а саме для оформлення картики постійного покупця.

Обслуговуючий персонал. Має фізичний доступ до обладнання у супроводі уповноваженого персоналу.

Правила розмежування доступу касирів-консультантів та адміністраторів стосовно інформаційних об'єктів та технічних засобів системи наведено в табл. 1.

В приміщенні знаходяться таки типи технічних засобів (табл. 2).

3.6. Описи технічних каналів витоку та загроз ІзОД

Під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого добувають інформацію про цей об'єкт, і фізичного середовища, в якій розповсюджується інформаційний сигнал. По суті, під ТКВІ розуміють спосіб отримання за допомогою ТЗР розвідувальної інформації про об'єкт. Можливі канали витоку інформації:

- Акустичні – за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті двері, вікна, вентиляційні канали).
- Вібраційні – за рахунок впливу звукових коливань на елементи і конструкції будівель, викликаючи вібрації (огороджувальні конструкції: стіни, стелі, підлоги, вікна, двері, короба вентиляційних систем тощо; інженерні комунікації: труби водопостачання, опалення, кондиціонування тощо).

Таблиця 1 – Правила розмежування доступу операторів та адміністраторів

Найменування технічних засобів, системного і прикладного ПЗ, засобів захисту та інформаційних ресурсів	Уповноважений персонал		
	СА	ВБ	К
Технічні засоби			
Мережне обладнання	Адмін права	-	-
Засоби управління мережним обладнанням (сервери системи управління мережним обладнанням захисту, засоби управління, що встановлені, адміністрування активного мережного обладнання)	Адмін права	-	-
Сервери доменів	-	Адмін права	-
Системне і прикладне програмне забезпечення			
ОС серверів домену	-	Адмін права	-
ОС серверів системи управління мережним обладнанням захисту, засобів управління, що встановлені, адміністрування активного мережного обладнання	Адмін права	-	-
Засоби захисту			
Програмні засоби захисту	Адмін права	Адмін права	-
Мережні засоби захисту	Адмін права	Адмін права	-
Інформаційні ресурси			
Технологічна інформація мережного обладнання	Читання \ модиф.	Читання	-
Технологічна інформація поштового серверу, серверів системи управління мережним обладнанням захисту, засобів управління, що встановлені на АРМ адміністрування активного мережного обладнання	Читання \ модиф.	Читання	-
Технологічна інформація серверів застосувань	Читання \ модиф.	Читання	-
Технологічна інформація серверів домену	Читання \ модиф.	Читання \ модиф.	-
Пошта	Читання \ модиф.	Читання \ модиф.	Читання \ модиф.
Дані БД	-	-	Читання \ модиф.

Таблиця 2 – Типи технічних засобів

№	Тип технічних засобів	Призначення	Примітки
1.	Сервер	Для зберігання ІзОД	Зберігає всю інформацію
2.	ПК	Для обробки, модифікації ІзОД	Локальна мережа не має виходу за мережі приміщення та доступу до мережі Інтернет
3.	Телефонний апарат	Для зв’язку з іншими відділами	Підключення до внутрішніх та зовнішніх ліній зв’язку
4.	Принтер-сканер-ксерокс	Для друку, сканування та копіювання документів	Підключення до локальної мережі

- Оптико-електронні канали – за рахунок приймання та демодуляції відбитого від вібруючих під дією акустичного сигналу поверхонь приміщень випромінювання.
- Акустоелектричні – за рахунок впливу звукових коливань на допоміжних технічних засобах і системах (ДТЗС) за рахунок зміни параметрів під дією акустичного поля, створюваного джерелом мовного сигналу та виникнення електрорушійної сили (ЕРС).
- Параметричні – за рахунок впливу звукових коливань на основні технічні засоби (ОТЗ) і ДТЗС за рахунок паразитної модуляції інформаційним сигналом випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, які перебувають у приміщеннях, де ведуться конфіденційні переговори, за рахунок утворення вторинних радіохвиль, при «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких змінюються під дією мовного сигналу.
- Через закладні пристрої – канали витоку витоку видової інформації.

4. ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ АС

Основним припущенням в ході аналізу загроз, що існують для ІТС, є те, що співробітники, які мають повний адміністративний доступ до компонентів системи і фізичний доступ до комутаційного та серверного обладнання, не розглядаються як потенційні порушники. Визначені в цьому технічні заходи, спрямовані на захист від зловмисних дій співробітників з адміністративними правами, розглядаються як додаткові. Основними заходами захисту від таких загроз є: кадрова політика та взаємний контроль адміністраторів при виконанні важливих технологічних операцій.

Захист від форс-мажорних обставин в рамках створення ІТС та КСЗІ не розглядаються.

Особливості реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту

До особливостей реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту входять режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежна охорона і інші чинники, що впливають на безпеку оброблюваної інформації;

5. ПОТЕНЦІЙНІ ЗАГРОЗИ ІНФОРМАЦІЇ

Опис загоз, що вважається найбільш вірогідним для комерційної організації . Потенційні загрози наведені в таблиці 3. Значення параметрів К, Ц, Д означають конфіденційність, цілісність, доступність.

Таблиця 3 – Потенційні загрози

Загрози	Порушення властивостей		
	К	Ц	Д
Природні загрози			
Стихійні природні лиха, у результаті яких буде порушена робота систем електроживлення, цілісність приміщення		▲	▲
Ненавмисні (випадкові) загрози			
Ненавмисні дії, у результаті яких відбувається часткова чи повна відмова системи		▲	▲
Випадкове пошкодження каналів зв’язку		▲	▲
Ненавмисне виключення обладнання або зміна режимів роботи програм		▲	▲

Продовження таблиці 3 – Потенційні загрози

Випадкова пошкодження носіїв інформації		▲	▲
Випадковий запуск програм, які при некомпетентній роботі завдадуть шкоду роботі системі		▲	▲
Випадкове зараження вірусами при передачі даних	▲	▲	▲
Випадкове розголошення конфіденційної інформації 3-м лицям	▲	▲	▲
Розголошення, передача, втрата атрибутів доступу до системи	▲	▲	▲
Використання ПЗ, яке може нанести шкоду роботі системі	▲	▲	▲
Халатне ставлення співробітниками до правил при роботі з системою	▲	▲	▲
Навмисні загрози			
Фізичне спотворення системи		▲	▲
Виключення чи припинення роботи систем функціонування		▲	▲
Вербування співробітників	▲	▲	▲
Викрадення носіїв інформації	▲	▲	▲
Несанкціоноване копіювання	▲	▲	
Несанкціоноване використання ПК співробітників	▲	▲	▲
Незаконне отримання паролів, ключів або інших реквізитів доступу, для отримання доступу під іменем співробітника	▲	▲	▲
Навмисне встановлення програмних закладок, вірусів, жучків	▲	▲	▲
Незаконне підключення до ліній передачі даних	▲	▲	▲

6. МОДЕЛЬ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ, ЯКА ПЛАНУЄТЬСЯ ЦИРКУЛЮВАТИ В АС КЛАСУ 2

Нижче запропоновано варіанти моделі загроз. В цій моделі визначені властивості захищеності інформаційних об’єктів, які можуть бути порушеними – конфіденційність (К), цілісність (Ц), доступність (Д) та якісна оцінка ймовірності здійснення загроз та рівнів збитків по кожному з видів порушень.

- Методика розроблення такої моделі полягає в тому, що в один із стовпчиків таблиці заноситься перелік видів загроз. Надалі для кожної із можливих загроз шляхом їх аналізу необхідно визначити:
- Ймовірність виникнення таких загроз. Визначення ймовірності можна використати її якісні оцінки. В таблиці можуть бути наведені якісні оцінки їх ймовірності неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька;
- Можливий рівень шкоди. Приклад цієї оцінки наведено також за якісною шкалою. Наявність таких оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної з властивостей захищеності інформації;
- Джерела загроз.

Потенційні загрози інформації об’єкта інформаційної діяльності наведені в табл. 4.

Таблиця 4 – Модель загроз

Види загрози	**Імовірність**	**Рівень шкоди**	**Джерела**
Природні загрози			
Стихійні природні лиха, у результаті яких буде порушена робота систем електроживлення, цілісність приміщення	Низька	Неприпустимо високий	Зовнішні
Ненавмисні (випадкові) загрози			
Ненавмисні дії, у результаті яких відбувається часткова чи повна відмова системи	Низька	Неприпустимо високий	Внутрішні
Ненавмисне виключення обладнання або зміна режимів роботи програм	Висока	Середня	Внутрішні
Випадкова пошкодження носіїв інформації	Низька	Низький	Внутрішні
Випадковий запуск програм, які при некомпетентній роботі завдадуть шкоду роботі системі	Низька	Високий	Внутрішні
Випадкове зараження вірусами при передачі даних	Висока	Неприпустимо високий	Внутрішні
Випадкове розголошення конфіденційної інформації 3-м лицям	Середня	Неприпустимо високий	Внутрішні
Розголошення, передача, втрата атрибутів доступу до системи	Низька	Середня	Внутрішні
Використання ПЗ, яке може нанести шкоду роботі системі	Середня	Високий	Внутрішні
Халатне ставлення співробітниками до правил при роботі з системою	Низька	Неприпустимо високий	Внутрішні
Випадкове пошкодження каналів зв’язку	Середня	Високий	Внутрішні
Навмисні загрози			
Фізичне спотворення системи	Середня	Неприпустимо високий	Внутрішні
Виключення чи припинення роботи систем функціонування	Середня	Високий	Зовнішні
Вербування співробітників	Висока	Високий	Внутрішні, зовнішні
Викрадення носіїв інформації	Середня	Високий	Зовнішні
Несанкціоноване копіювання	Висока	Високий	Внутрішні
Розкрадання виробничих відходів	Середня	Неприпустимо високий	Внутрішні, зовнішні
Несанкціоноване використання ПК співробітників	Середня	Високий	Внутрішні
Незаконне отримання паролів, ключів або інших реквізитів доступу, для отримання доступу під іменем співробітника	Низька	Неприпустимо високий	Внутрішні, зовнішні
Навмисне встановлення програмних закладок, вірусів, жучків	Висока	Неприпустимо високий	Внутрішні, зовнішні
Незаконне підключення до ліній передачі даних	Середня	Середня	Внутрішні

Наявність такої інформації дозволяє побудувати більш предметну загальну модель системи захисту; оцінити значення залишкового ризику, як функцію захищеності по кожній із функціональних властивостей захищеності; визначити структуру системи захисту та її

основні компоненти. З даної моделі загроз можна зробити висновок, що для реалізації загроз порушник може діяти через засоби зв'язку, технічні канали або безпосередньо на елементи локальних мереж. В останньому випадку порушнику необхідно отримати фізичний доступ до загальних елементів локальних мереж.

7. МОДЕЛЬ ПОРУШНИКА

За порушників на ОІД розглядаються суб'єкти, внаслідок навмисних або випадкових дій котрих, і випадкові події, внаслідок настання яких можливі реалізації загроз для інформації.

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т. ін. По відношенню до АС порушники можуть бути внутрішніми або зовнішніми.

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- можливість модифікації та зміни інформації;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
- можливість отримання доступ до матеріальних носіїв інформації;
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Порушники класифікуються за рівнем можливостей, що надаються їм всіма доступними засобами (табл. 5).

Порушники за рівнем володіння інформацією про АС:

І рівень – володіють інформацією про функціональні особливості засобів обчислювальної техніки, основні закономірності формування в них масивів даних і запитів до них, вміють користуватися штатними засобами.

ІІ рівень – мають високий рівень знань і досвідом роботи з технічними засобами АС і їх обслуговування.

ІІІ рівень – мають високий рівень знань в області обчислювальної техніки і програмування та експлуатації автоматизованих систем.

IV рівень – володіють інформацією про функції та механізм дії засобів захисту в АС.

Порушники за показниками:

І рівень – використовують виключно агентурні методи отримання відомостей.

ІІ рівень – використовують пасивні технічні засоби перехоплення інформаційних сигналів.

ІІІ рівень – використовують виключно штатні засоби АС або недоліки проектування системи ЗІ для реалізації НСД до ІзОД.

IV рівень –застосовують методи і засоби активного впливу на АС, що змінюють конфігурацію системи.

Таблиця 5 – Класифікація порушників за рівнем можливостей

Рівні	Внутрішні загрози	Зовнішні загрози
I рівень	- технічний персонал, який обслуговує будинки й приміщення - особи, які входять до штату комерційної організації «ТИМ-ТИМ» але не мають допуску та доступу до обробки ІзОД на АС	- будь-які особи, які перебувають за межами КЗ
II рівень	- внутрішні: персонал, який обслуговує засоби обчислювальної техніки - користувачі АС	- відвідувачі
III рівень	- користувачі АС, які мають доступ до ІзОД в АС - користувачі АС з адміністративними ролями	- представники організацій, які взаємодіють з питань технічного забезпечення, обслуговування, супровід техніки, яка входить до складу АС - представники організацій, які взаємодіють з питань життєзабезпечення АС і ОІД в цілому
IV рівень	- особи, які відповідають за захист ІзОД в АС	співробітники іноземних спецслужб, шпигуни від конкурентів

I рівень – без отримання доступу на територію;
II рівень – з отриманням доступу на територію;
III рівень – з отриманням доступу до АС;
IV рівень – з отриманням доступу до масивів накопичення і зберігання ІзОД;
V рівень – отримання доступу до КСЗІ АС.

Порушники за часом дії:

I рівень – до впровадження АС або її окремих компонентів;
II рівень – під час бездіяльності компонентів АС;
III рівень – під час функціонування АС;
IV рівень – як під час функціонування, так і під час зупинки в роботі АС.

Порушники за мотивами вчинення порушення:

I рівень – безвідповідальність;
II рівень – самозатвердження;
III рівень – корисливі інтереси;
IV рівень – професійний обов’язок.

Генеральний директор
КО «ТИМ-ТИМ» Тимощук В.С.

Відповідальний за відділ
безпеки КО «ТИМ-ТИМ» Верес В.В.

ДОДАТОК Д

«ЗАТВЕРДЖУЮ»
Генеральний директор
комерційної організації
«ТИМ-ТИМ»
_____ Тимощук В.С.
«03» листопада 2020 року

Політика безпеки інформації, яка циркулює в АС класу 2 комерційної організації «ТИМ-ТИМ»

Загальні положення

Політика безпеки інформації в АС повинна поширюватися на об'єкти комп'ютерної системи, які безпосередньо чи опосередковано впливають на безпеку службової інформації.

До таких об'єктів належать:

- адміністратор безпеки та співробітники СЗІ;
- користувачі, яким надано повноваження інших адміністраторів;
- користувачі, яким надано право доступу до службової інформації або до інших видів інформації;
- слабо- та сильнозв'язані об'єкти, які містять службову інформацію або інші види інформації, що підлягають захисту;
- системне та функціональне програмне забезпечення, яке використовується в АС для оброблення інформації або для забезпечення КЗЗ;
- технологічна інформація КСЗІ;
- засоби адміністрування та управління обчислювальною системою АС та технологічна інформація, яка при цьому використовується;
- окремі периферійні пристрої, які задіяні у технологічному процесі обробки службової інформації;
- обчислювальні ресурси АС, безконтрольне використання яких або захоплення окремим користувачем може призвести до блокування роботи інших користувачів, компонентів АС або АС в цілому.

Загальні вимоги політики безпеки

Інформація, яка обробляється в АС, не підлягає неконтрольованому та несанкціонованому ознайомленню, розмноженню, розповсюдженню, копіюванню, відновленню, а також неконтрольованій та несанкціонованій модифікації.

В основу політики безпеки АС покладений адміністративний принцип розмежування доступу, який реалізується відповідно до принципу мінімуму повноважень, згідно з яким право доступу може бути надане користувачеві лише за фактом службової необхідності. Наявність службової необхідності визначається посадовими обов'язками користувачів.

З метою забезпечення необхідного режиму доступу до інформації повинен бути визначений відповідальний підрозділ – СЗІ, якому надаються повноваження щодо організації та впровадження прийнятої політики безпеки в АС.

Всі працівники комерційної організації «ТИМ-ТИМ», які беруть участь в обробці інформації в АС, повинні бути зареєстровані як користувачі в системних журналах АС.

Керування правами доступу користувачів до захищених об’єктів та параметрами КЗЗ у складі АС повинен здійснювати спеціально уповноважений працівник – адміністратор безпеки АС.

Надання доступу до інформації АС повинно здійснюватися тільки за умови достовірного розпізнавання ідентифікаційних параметрів користувачів АС. Процедура розпізнавання та надання повноважень здійснюється як організаційними заходами, так і з використанням програмно-апаратних засобів розмежування доступу.

Машинні носії інформації повинні мати відповідні ідентифікаційні реквізити.

Спроби порушення встановленого порядку доступу до інформації повинні блокуватись.

Реалізація політики безпеки КСЗІ

Реалізація політики безпеки здійснюється за допомогою КСЗІ АС – взаємопов'язаній сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

КСЗІ АС забезпечує реалізацію вимог із захисту інформації, які визначені у Технічному завданні на створення КСЗІ в АС а саме щодо:

- цілісності та доступності функціональної та технологічної інформації АС;
- конфіденційності, цілісності та доступності технологічної інформації КСЗІ.

КСЗІ АС розглядається як сукупність взаємопов'язаних нормативно-правовових та організаційних заходів і інженерно-технічних засобів щодо захисту інформації від НСД.

Нормативно-правові заходи захисту інформації

Комплекс нормативно-правових заходів захисту інформації АС:

1. створення системи документів нормативно-правового забезпечення робіт з захисту інформації в АС;
2. впровадження заходів з забезпечення безпеки інформації в АС, виконання правових та договірних вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників служби захисту інформації в АС;
3. доведення до персоналу і користувачів АС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;
4. запровадження системи контролю за своєчасністю, ефективністю і повнотою реалізації в АС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

Організаційні заходи захисту інформації

Комплекс організаційних заходів захисту інформації в АС включає:

1. застосування режимних заходів на ОІД;
2. забезпечення фізичного захисту обладнання АС, носіїв інформації, інших ресурсів;
3. організацію проведення обстеження середовищ функціонування АС;
4. виконання робіт з захисту інформації та взаємодії з цих питань з іншими суб’єктами системи ТЗІ в Україні;
5. регламентацію доступу користувачів і персоналу до ресурсів АС;
6. здійснення профілактичних заходів щодо попередження ненавмисного порушення політики безпеки, зокрема попередження появи вірусів та ін.

Інженерно-технічні засоби захисту інформації

Комплекс інженерно-технічних засобів захисту інформації – сукупність програмно-апаратних засобів захисту призначено для:

1. розмежування доступу користувачів до інформації та інших ресурсів АС;
2. блокування несанкціонованих дій з інформацією та іншими ресурсами АС, локалізації цих дій по відношенню до ресурсів та ліквідації їх наслідків;
3. забезпечення контролю та захисту потоків інформації, яка обробляється в АС;
4. забезпечення спостереженості за діями користувачів та персоналу АС, реєстрації, збору, зберігання, обробки даних про події, які мають відношення до безпеки інформації, сповіщення адміністратора безпеки про такі події;
5. підтримання цілісності критичних ресурсів системи захисту, середовища виконання прикладних програм та інформації в ПТК;
6. забезпечення контролю за цілісністю об'єктів, що підлягають захисту;
7. організації обліку, зберігання та обігу матеріальних носіїв інформації;
8. забезпечення управління засобами КСЗІ та контролю за її функціонуванням.

Основні організаційні заходи

Організаційні заходи щодо керування доступом повинні передбачати:

- визначення порядку доступу користувачів у захищене приміщення, до технічних засобів, носіїв інформації, програмного та інформаційного забезпечення;
- визначення порядку внесення/вилучення даних щодо атрибутів доступу користувача до АС установи банку.

Організаційні заходи щодо реєстрації та обліку повинні передбачати визначення порядку:

- обліку, використання і зберігання МНІ;
- організації зберігання, використання і знищення документів і носіїв, що містять інформацію з обмеженим доступом, відповідно до вимог нормативних документів.

Організаційні заходи щодо забезпечення цілісності інформації повинні передбачати:

- резервне копіювання на МНІ еталонних копій ОС і функціональних програм;
- облік, видачу, використання і зберігання МНІ, що містять еталонні і резервні копії операційних систем і функціональних програм;
- контроль цілісності системного ПЗ;
- контроль цілісності КЗЗ АС комерційної організації «ТИМ-ТИМ».

Організаційні заходи антивірусного захисту інформації в АС комерційної організації «ТИМ-ТИМ» повинні передбачати:

- використання ліцензійного антивірусного ПЗ на всіх ПК, що входять до складу АС філіалу;
- організацію постійного та своєчасного оновлення антивірусних баз.

Резервне копіювання, архівування та відновлення інформації

Для забезпечення відновлюваності інформації у випадку збоїв системи або помилок користувачів в АС повинно здійснюватися періодичне резервне копіювання.

Резервному копіюванню підлягає:

- ІзОД, яка зберігається у файлах користувачів;
- ІзОД, яка зберігається у БД;
- настройки ОС, БД та КЗЗ;
- журнали реєстрації.

Експлуатаційні та організаційно – розпорядчі документи повинні визначати порядок та періодичність резервного копіювання, архівування та відновлення інформації, місце збереження резервних копій та відповідальних посадових осіб.

Розмежування інформаційних потоків

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувачів і захищених об'єктів. Розмежування доступу здійснюється на рівні надання користувачеві прав читати або модифікувати об'єкт.

КЗЗ повинен надавати можливість адміністратору системи та адміністратору безпеки для кожного захищеного об'єкта визначити конкретних користувачів, які мають право читати або модифікувати об'єкт.

КЗЗ повинен здійснювати розмежування доступу до слабозв’язаних об’єктів на підставі імені користувача і захищеного об'єкта та прав доступу.

КЗЗ повинен здійснювати розмежування доступу до сильнозв’язаних об’єктів на підставі імені користувача та його ролі.

Розмежування доступу до ресурсів серверу управління БД повинно здійснюватися за допомогою надання адміністратором БД користувачеві певної ролі.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора системи, адміністратора безпеки, адміністратора БД.

Обслуговуючий персонал має право створювати, модифікувати, вилучати, друкувати та копіювати на МНІ файли з текстовими документи, за які вони відповідають, а також працювати із файлами з документами, що створюються спільно з іншими користувачами, відповідно до наданих прав.

Обслуговуючий персонал має право читати та модифікувати інформацію, що міститься у БД в залежності від програмного комплексу, із яким він працює та прикладної ролі, яку він виконує у цьому комплексі.

Обслуговуючий персонал має право на перегляд та запуск загальносистемного та спеціального програмного забезпечення.

Обслуговуючий персонал не повинен виконувати налаштування конфігурації КЗЗ, загальносистемного та ПЗ, СКБД, змінювати їх склад та структуру, коригувати права доступу, тобто виконувати функції будь-кого з Адміністраторів.

Адміністратори мають право працювати з електронними документами, за які вони відповідають, а також працювати із файлами з документами, що створюються спільно з іншими користувачами, відповідно до наданих прав.

Також адміністратор БД має право працювати з програмними комплексами, що входять до складу спеціального ПЗ.

Вимоги до правил адміністрування КЗЗ і реєстрації дій користувачів

Щодо реєстрації дій користувачів КЗЗ повинен забезпечити реалізацію наступних функцій:

1. реєстрація користувача в системі;
2. зміна паролю користувачем;
3. зміна прав та повноважень доступу до файлів та ресурсів;
4. створення, доступ та знищення файлів;
5. запуск програм, які мають доступ до ІзОД.

Обов’язковими параметрами реєстрації мають бути:

- дата, час, та назва події;

- ідентифікатор суб’єкта, що ініціював подію.

Реєстрація дій користувача, пов’язаних з виводом інформації на друк за допомогою принтера, введення інформації за допомогою сканера та копіювання інформації на з’ємні машинні носії повинна фіксуватися в паперовому «Журналі обліку роботи користувачів банку».

Середовище АС

Вимоги до заземлення:

- Усі металеві конструкції в приміщенні повинні бути заземлені;
- Система заземлення не повинна мати вихід за межі контрольованої території;
- Опір кіл заземлення від засобів філії до вузлів системи заземлення не повинен перевищувати 4 Ом.

Вимоги до електроживлення

Електроживлення АС філії повинне здійснюватися від трансформаторної підстанції низької напруги, розміщеної у межах контрольованої території. У випадку знаходження трансформаторної підстанції за межами контрольованої території електроживлення повинно здійснюватися через розділовий трансформатор.

Мережа електроживлення АС філії повинна бути відділена від мережі освітлення та побутової мережі і забезпечувати безперебійну експлуатацію та працездатність АС.

Електроживлення повинно здійснюватися через протизавадні мережеві фільтри.

Вимоги до захисту інформації від витоку візуально-оптичним каналом

Для захисту інформації від витоку візуально-оптичним каналом вікна приміщень, де розташована АС філії, повинні бути обладнані жалюзями або шторами.

Фізичне середовище АС

До компонентів фізичного середовища АС відносяться:

- територія, будівля та приміщення, де знаходяться компоненти АС;
- місця зберігання змінних, паперових та інших носіїв інформації;
- охорона території, будівлі, приміщень та режими доступу до цих компонентів;
- системи життєзабезпечення, комунікацій і зв’язку;
- проектна та експлуатаційна документація на компоненти фізичного середовища.

Територія фізичного середовища

Територія, яка знаходиться під цілодобовою охороною.

Будівля, де розгорнута АС

Доступ працівників КО «ТИМ-ТИМ» в будівлю здійснюється за перепустками. Доступ сторонніх осіб в будівлю контролюється черговим відповідного підрозділу і здійснюється за узгодженням керівника комерційної організації»ТИМ-ТИМ». Співробітники, які приймають в будинку сторонніх осіб, зустрічають їх при вході і супроводжують на вихід після завершення візиту.

Приміщення де знаходяться компоненти АС

Приміщенню, в якому розміщуються компоненти АС, категорія об’єкта інформаційної діяльності не надана, у зв’язку з тим, що в ньому не передбачається обробка інформації, яка становить державну таємницю.

Приміщення контролюються охороною. Доступ до приміщення, де знаходиться АС, здійснюється посадовими особами, які мають на це право за характером своєї діяльності. Всі співробітники отримують доступ лише в ті приміщення, які дозволені їм політикою безпеки.

Приміщення у позаслужбовий час опечатуються металевими печатками посадових осіб, що в них працюють.

Місця зберігання носіїв інформації

Місця та порядок зберігання змінних носіїв інформації здійснюється згідно відповідних інструкцій.

Системи життєзабезпечення, комунікацій та зв'язку

Системи життєзабезпечення: система електроживлення, система заземлення, система пожежної та охоронної сигналізації повинна відповідати вимогам із захисту інформації.

Документація на компоненти фізичного середовища

Проектна та експлуатаційна документація на компоненти фізичного середовища зберігається у спеціально відведеному місці. Відповідальність за її збереження несе призначена для цього посадова особа структурного підрозділу комерційної організації»ТИМ-ТИМ».

Відповідальний за відділ безпеки
комерційної організації «ТИМ-ТИМ» Верес В.В.

ДОДАТОК Е

«ЗАТВЕРДЖУЮ»
Генеральний директор
комерційної організації
«ТИМ-ТИМ»
_____ Тимощук В.С.
«25» листопада 2020 року

Протокол
попередніх випробувань комплексної системи захисту інформації в автоматизованій системі класу 2 відділу безпеки КО «ТИМ-ТИМ»

1. Представниками служби захисту інформації, спеціального відділу КО «ТИМ-ТИМ» та представником ПАТ «ІЛОН». було проведено попередні випробування створеної КСЗІ в АС класу 2 відділу безпеки, яка розміщена в приміщенні КО «ТИМ-ТИМ».

Підставою для проведення випробувань є ТЗ.

2. Вихідні дані

Вихідними даними для проведення випробувань КСЗІ є:

- Перелік відомостей, що відносяться до конфіденційної інформації КО «ТИМ-ТИМ» та якій надається гриф обмеження доступу.
- Акт визначення вищого ступеню обмеження доступу інформації, яка циркулюватиме на ОІД – приміщення № 1 відділу безпеки КО «ТИМ-ТИМ» .
- Акт обстеження середовищ функціонування АС на ОІД – приміщення № 1 відділу безпеки КО «ТИМ-ТИМ» .
- Модель загроз для інформації, яка планується до циркуляції в АС класу 2 на ОІД – приміщення КО «ТИМ-ТИМ» .
- Політика безпеки інформації, яка циркулює в АС класу 2 КО «ТИМ-ТИМ» .
- АС відділу безпеки КО «ТИМ-ТИМ». КСЗІ. План захисту інформації.
- АС відділу безпеки КО «ТИМ-ТИМ». КСЗІ. ТЗ.
- АС відділу безпеки КО «ТИМ-ТИМ». КСЗІ. Технороботчий проект.
- Паспорт-формуляр на АС класу 2 відділу безпеки КО «ТИМ-ТИМ».
- Положення про СЗІ в АС класу 2 відділу безпеки КО «ТИМ-ТИМ».
- Інструкція користувачу АС класу 2 відділу безпеки КО «ТИМ-ТИМ».
- Інструкція з адміністрування системи АСеми класу 2 відділу безпеки КО «ТИМ-ТИМ».
- Інструкція з режимних заходів щодо захисту інформації під час її обробки в АС класу 2 відділу безпеки КО «ТИМ-ТИМ».
- Інструкція з правил видачі вилучення та зберігання персональних ідентифікаторів користувачів АС класу 2 відділу безпеки КО «ТИМ-ТИМ».
- Інструкція по правилам управління паролями в АС класу 2 відділу безпеки КО «ТИМ-ТИМ».
- Інструкція про порядок оперативного відновлення функціонування АС класу 2 відділу безпеки КО «ТИМ-ТИМ».

3. Методика проведення випробувань

Попередні випробування проводились відповідно документу «АС відділу безпеки КО «ТИМ-ТИМ». КСЗІ. Програма та методики випробувань».

4. Виклад результатів попередніх випробувань КСЗІ

4.1. Перевірка середовища функціонування АСВБ

Середовища функціонування АСВБ на ОІД відповідають вимогам та описам наведеним в Технічному завданні, а саме:

- охорону будівлі в якому знаходиться ОІД здійснює відомча охорона ТОВ «ЛУН»;
- охорона ОІД здійснюється за допомогою системи охоронної сигналізації, пульт якої встановлено в приміщенні охорони «ЛУН» ;
- ОІД обладнано системою пожежної сигналізації;
- доступ осіб на ОІД та до АСВБ організовано відповідно списку, затвердженому директором КО «ТИМ-ТИМ» та відповідно вимог Інструкції з режимних заходів;
- склад та розміщення АСВБ, допоміжних технічних засобів та систем, систем життєзабезпечення ОІД відповідають перелікам наведеним в Паспорті-формулярі АСВБ;
- особи, які будуть мати доступ до інформації в АСВБ, визначені відповідним списком користувачів АСВБ;
- операційна система та склад ПЗ АСВБ відповідає переліку наведеному в Паспорті-формулярі АСВБ;
- організація порядку обробки конфіденційної інформації в АСВБ та форма представлення ІзОД в АСВБ відповідає задекларованої в ТЗ технології обробки інформації;
- зареєстровані в АСВБ користувачі відповідають списку осіб, які допущені до роботи з конфіденційною інформацією в АСВБ.

4.2. Перевірка експлуатаційної документації КСЗІ

Проектна та експлуатаційна документація КСЗІ в АСВБ відповідає вимогам Технічного завдання, а саме:

- перелік проектних та експлуатаційних документів на КСЗІ в АСВБ відповідає переліку експлуатаційної документації наведеному в Технічному завданні;
- зміст та об’єм інформації, що наведено в проектній та експлуатаційній документації, щодо створення КСЗІ в АСВБ, відповідає вимогам Техпроекту.

4.3. Перевірка заходів із захисту ІзОД від її витоку технічними каналами

4.3.1. Блокування каналу побічних електромагнітних випромінювань та наведень.

КСЗІ здійснює блокування витоку ІзОД, яка циркулюватиме в АСВБ, за рахунок ПЕМВН наступними заходами:

- електроживлення всіх компонентів АСВБ здійснюється через мережевий завадозаглушувальний фільтр М-17, що унеможливлює просочення ІзОД через лінію електроживлення за рахунок наведень від компонентів АСВБ інформативних сигналів на вказану лінію;
- монтаж завадозаглушувального фільтру М-17 відповідає вимогам, що наведено в пасорті на вказаний мережевий фільтр;
- на лінію охоронної та пожежної сигналізації встановлено завадозаглушувальний фільтр М-9, що унеможливлює просочення ІзОД через ці лінії за рахунок наведень на них від компонентів АСВБ інформативних сигналів;
- всі компоненти ІТС підключено до контуру системи заземлення яка відповідає вимогам п. 5.3 ТР ЕОТ 95, а саме:

- контур системи заземлення знаходиться в межах контрольованої зони КО «ТИМ-ТИМ» ;
- в якості контуру заземлення використовується глибинний заземлювач;
- опір системи заземлення становить 1,4 Ом.

4.3.2. Блокування радіотехнічного каналу

На ОІД проведено пошук можливо встановлених пристроїв технічної розвідки б могли передавати видову інформації по радіоканалу або лінійними комунікаціями.

За результатами проведених робіт зроблено наступні висновки:

- при проведенні моніторингу радіоефіру за допомогою пошукового комплексу DigiScan EX 2.1 у діапазоні частот 10 кГц – 3 ГГц радіовипромінювань, які б свідчили про факт встановлених на ОІД пристроїв технічної розвідки не виявлено.
- при проведенні обстеження будівельних конструкцій, технічних засобів, меблів та предметів інтер'єру приміщення за допомогою індикатора поля RD-14 та частотоміра ACECO SC-1 радіовипромінювань, які б свідчили про наявність закладних пристроїв не виявлено.
- при обстеженні будівельних конструкцій, меблів, предметів інтер'єру, технічних засобів за допомогою приладу пошуку оптичних систем RAY – оптичних систем не виявлено.
- при обстеженні будівельних конструкцій, меблів та предметів інтер'єру за допомогою портативного нелінійного локатора «Обь-1» – закладних пристроїв не виявлено.
- КСЗІ здійснює захист інформації від її витоку за рахунок радіотехнічного каналу витоку наступними заходами:
- організованими перепускним режимом контрольовану зону КО «ТИМ-ТИМ» та порядком відвідування сторонніх осіб приміщень КО «ТИМ-ТИМ» унеможливлюється встановлення пристроїв технічної розвідки на лінії, які виходять за межі ОІД;
- виконання вимог що наведено в експлуатаційній документації на КСЗІ стосовно порядку доступу осіб на ОІД, є достатніми щодо унеможливлення встановлення на ОІД пристроїв технічної розвідки.

4.3.3. Блокування візуально-оптичного каналу

КСЗІ блокує візуально-оптичний канал витоку інформації наступними заходами:

- вікно ОІД обладнано непрозорими жалюзями;
- виконання вимог Інструкції користувача, є достатніми щодо блокування витоку інформації за рахунок візуально-оптичного каналу.

4.4. Перевірка блокування шляхів НСД до компонентів АСВБ

КСЗІ унеможливлює НСД сторонніх осіб до компонентів АСВБ та на ОІД в цілому наступними заходами:

- ОІД обладнано системою охоронної сигналізації, яка знаходиться в робочому стані;
- в Інструкції з режимних заходів впроваджено дії начальника спеціального відділу щодо організації охорони ОІД в неробочий час та організацію режимних заходів на ОІД, виконання яких є достатніми щодо унеможливлення шляхів НСД до компонентів АСВБ та на ОІД в цілому.

4.5. Перевірка блокування шляхів НСД до ІзОД, яка циркулюватиме в АСВБ

КСЗІ унеможливлює НСД до ІзОД в АСВБ наступними заходами:

- в АСВБ впроваджено СЗІ від НСД «Лоза-2»;

- в Інструкції користувачу, Інструкції з адміністрування системи, Інструкції з режимних заходів, Інструкції по оперативному відновленню впроваджено організаційні заходи щодо унеможливлення НСД до ІзОД, яка обробляється та зберігається в АСВБ;
- виконання користувачами АСВБ вимог Інструкції по правилам управління паролями та Інструкції з ПІ забезпечують унікальність персональних даних користувача для доступу до ІзОД в АСВБ та унеможливлюють їх несанкціоноване заволодіння, ознайомлення та підбір.

СЗІ від НСД «СОН-2 (далі – КЗЗ) здійснює:

- ідентифікацію та автентифікацію користувачів АСВБ;
- блокує завантаження ОС АСВБ CD-ROM;
- здійснює розмежування доступу між користувачами АСВБ до їх захищених документів;
- здійснює контроль та цілісність програмного забезпечення в АСВБ;
- реєструє дії користувачів в АСВБ;
- блокує вікна інтерфейсу користувачів, а саме здійснення гасіння екрану монітору та блокування клавіатури з графічним маніпулятором за вибраною комбінацією клавіш або заданого періоду часу бездіяльності користувачів;
- здійснює реєстрацію в спеціальних журнальних файлах спроби несанкціонованого доступу до інформації, фактів запуску програм, які не входять до баз даних операційної системи АСВБ.

Встановлений та налагоджений в АСВБ КЗЗ реалізує наступні послуги:

1) *Базова адміністративна конфіденційність* (КА-2):

- в АСВБ надається можливість користувачам працювати з базами документів та документами, які містять ІзОД, за допомогою програми «Захищені документи», яка входить до складу КЗЗ;
- адміністратором документів в АСВБ здійснюється керування доступом користувачів АСВБ до баз документів та документів з ІзОД на підставі атрибутів доступу користувача та об’єкта згідно з правилами розмежування доступу, наведеними в ТЗ;
- КЗЗ надає можливість змінювати атрибути доступу баз документів та документів з ІзОД лише користувачу з роллю *«Адміністратор документів»;*
- атрибути доступу бази документів та документа з ІзОД встановлюються в момент їх створення;
- забезпечується можливість автоматичного внесення рівня доступу документа до тексту документа під час друку та збереження документа у файлі;
- захищає дані, які під час роботи знаходяться на екрані монітора;
- КЗЗ надає можливість працювати з даними захисту тільки адміністратору безпеки в АСВБ;.
- КЗЗ реалізує правила розмежування доступу до даних захисту, наведених в Технічному завданні;
- КЗЗ надає доступ до процесів, за допомогою яких здійснюється обробка ІзОД, тільки користувачам АСВБ.
- КЗЗ надає доступ до процесів, за допомогою яких здійснюється ведення бази даних захисту та перегляд журналу захисту, тільки адміністратору безпеки та системному адміністратору;

- КЗЗ надає можливість змінювати атрибути доступу файлів лише адміністратору безпеки та СА.
- КЗЗ здійснює захист ІзОД, що міститься в тимчасових файлах, які створюються під час роботи прикладних програм.

2) *Повторне використання об'єктів (КО-0):*

встановлена в АСВБ ОС Windows 10 забезпечує при взаємодії з КЗЗ очищення звільненої оперативної пам'яті під час її перерозподілу за рахунок чого здійснюється безповоротне видалення тимчасових файлів, файлів, в яких зберігаються бази документів, документи, резервні копії журналу захисту, та, можливо, інші об'єкти доступу.

3) *Мінімальна адміністративна цілісність* (ЦА-1):

КЗЗ надає користувачам АСВБ можливість працювати з базами документів та документами тільки за допомогою призначеного для цього процесу;

КЗЗ здійснює керування доступом до баз документів та документів на підставі атрибутів доступу користувача і документа згідно з правилами розмежування доступу наведеними в Технічному завданні;

КЗЗ надає можливість змінювати атрибути доступу баз документів та документів лише користувачу з роллю «Адміністратор документів» та дозволяє йому визначати користувачів і/або їх групи, які мають право модифікувати документ з ІзОД;

КЗЗ надає можливість працювати з даними захисту тільки за допомогою призначеного для цього процесу;

КЗЗ надає доступ до даних захисту відповідно до ролі користувача;

КЗЗ забезпечує права на читання та запис даних у базу даних захисту та право на перегляд журналу захисту має лише адміністратор безпеки;

КЗЗ надає право на читання та зміни значень параметрів своєї конфігурації, безпосередньо пов'язаних із керуванням доступом, тільки адміністратору безпеки;

КЗЗ надає доступ до процесів, за допомогою яких здійснюється обробка ІзОД, тільки користувачам АСВБ.

КЗЗ надає доступ до процесів, за допомогою яких здійснюється ведення бази даних захисту та перегляд журналу захисту, тільки адміністратору безпеки та системному адміністратору.

КЗЗ надає можливість змінювати атрибути доступу файлів лише адміністратору безпеки та системному адміністратору.

4) *Гаряча заміна* (ДЗ-1):

у операційній системі АСВБ забезпечується можливість поновлення всіх або окремих її компонентів.

5) *Ручне відновлення* (ДВ-1)

- КЗЗ забезпечує порядок обробки помилок, які виникають під час роботи системи;
- програмні засоби КЗЗ надають можливість адміністратору вказати системі КЗЗ, яким чином вона має реагувати на помилку, а саме:
- повторити дію, що викликала помилку;
- перевести КЗЗ у стан, призначений для відновлення.

6) *Захищений журнал* (НР-2):

- КЗЗ здійснює ведення журнал захисту та його захист від несанкціонованого ознайомлення, модифікації та знищення;

- КЗЗ забезпечує реєстрацію таких подій:
- вхід/вихід користувача в АСВБ;
- створення/видалення облікових записів користувачів;
- зміни облікових записів користувачів, у тому числі зміни атрибутів доступу;
- створення/видалення об’єктів доступу;
- зміни атрибутів доступу об’єктів доступу;
- спроби доступу до об’єктів доступу;
- зміни конфігурації КЗЗ;
- виявлення порушень цілісності програмного середовища;
- початок та закінчення роботи прикладних програм, призначених для роботи з інформацією, що захищається;
- виведення інформації на зовнішні носії.
- дата, час і тип події, а для подій аудита – також про користувача, процес і об’єкт, пов’язані з подією;
- адміністратор безпеки має можливість встановлювати політику аудита, яка визначає події аудита які повинні реєструватись;
- доступ до журналу захисту надається тільки адміністратору безпеки;
- КЗЗ забезпечує автоматичну реєстрацію критичних події.

7) *Множинна ідентифікація і автентифікація* (НИ-3):

- КЗЗ здійснює ідентифікацію користувачів на підставі введеного імені та автентифікацію на підставі введеного користувачем пароля при використанні персонального ідентифікатора користувача;

8) *Однонаправлений достовірний канал* (НК-1):

КЗЗ забезпечує початкової ідентифікації і автентифікації користувача з ініціативи користувача після натискання їм комбінації клавіш *Ctrl-Alt-Del*.

9) *Розподіл обов’язків адміністраторів* (НО-2):

В АСВБ реалізуються наступні ролі користувачів:

- звичайний користувач;
- адміністратор безпеки;
- адміністратор документів;
- системний адміністратор.
- адміністративними заходами заборонено реалізовувати ролі «Звичайний користувач» з адміністративними ролями та дозволено суміщення будь-яких адміністративних ролей;

10) *КЗЗ з гарантованою цілісністю* (НЦ-2)

КЗЗ перевіряє цілісність таких об’єктів:

- програмні компоненти КЗЗ;
- параметри та розділи системного реєстру, в яких зберігаються важливі для захисту дані;
- завантажувальні сектори жорстких дисків.
- облікові записи користувачів та груп користувачів Windows.
- КЗЗ забезпечує реєстрацію порушень цілісності у журналі відповідну подію та переводить КЗЗ у стан відновлення;
- КЗЗ дозволяє поновлення та відновлення програмних засобів КЗЗ тільки системному адміністратору за узгодженням з адміністратором безпеки.

11) *Самотестування при старті* (НТ-2)

КЗЗ перевіряє правильність функціонування програмних засобів, які входять до складу КЗЗ та у разі виявлення під час ініціалізації порушень.

При використанні КЗЗ в АСВБ та обов'язковому виконанні користувачами АСВБ, користувачів з адміністративними ролями організаційних заходів стосовно унеможливлення НСД до ІзОД, яка циркулюватиме в АСВБ, які викладені в Інструкції з режимних заходів, Інструкції користувачі, Інструкції з адміністрування блокуються шляхи НСД сторонніх осіб до ІзОД в АСВБ та реалізується наступний функціональний профіль захищеності: КА-2, КО-0, ЦА-1, ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

Впроваджена в АСВБ система захисту інформації «Лоза-2» має експертний висновок ДСТСЗІ СБ України 21.03.06 № 73.

4.6. Перевірка реалізації організаційних заходів щодо унеможливлення загроз ІзОД в АСВБ

Виконання начальником спеціального відділу, користувачами АСВБ, представниками служби захисту інформації в АСВБ організаційних заходів стосовно унеможливлення загроз ІзОД, яка циркулюватиме в АСВБ, які викладені в Інструкції з режимних заходів та Інструкції користувача є достатніми щодо унеможливлення загроз ІзОД, які можуть виникати під час її циркуляції в АСВБ.

5. Висновок:

КСЗІ в АСВБ:

- забезпечує визначену для АСВБ Політику безпеки інформації;
- здійснює розмежування доступу користувачів в АСВБ до інформації різних категорій конфіденційності;
- реєструє спроби реалізації загроз інформації та сповіщає адміністраторів безпеки АСВБ про факти несанкціонованих дій з ІзОД;
- забезпечує спостережність інформації шляхом контролю за діями користувачів АСВБ та реєстрацію подій, які мають відношення до безпеки інформації;
- підтримує цілісність критичних ресурсів АСВБ;
- забезпечує організацію обліку, зберігання та обігу матеріальних носіїв інформації, які використовуються в АСВБ;
- забезпечує управління засобами захисту КСЗІ та контроль за її функціонуванням;
- забезпечує захист ІзОД від її витоку технічними каналами;
- блокує НСД до ІзОД та несанкціоновані дії з ІзОД;
- блокує НСД до компонентів АСВБ та на ОІД в цілому;
- унеможливлює загрози ІзОД, яка циркулюватиме в АСВБ;
- забезпечує дотримання вимог режиму конфіденційності під час роботи користувачів АСВБ з ІзОД;

Створена КСЗІ в АСВБ може бути передана для проведення дослідної експлуатації.

Відповідальний за відділ безпеки – керівник
служби захисту інформації в АСВБ Верес В.В.

Начальник спеціального відділу
представник КО «ТИМ-ТИМ» Кудимець І.Л.

ДОДАТОК Є

«ЗАТВЕРДЖУЮ»
Генеральний директор
комерційної організації
«ТИМ-ТИМ»
_____ Тимощук В.С.
«25» листопада 2020 року

АКТ
приймання КСЗІ АС класу 2 відділу безпеки КО «ТИМ-ТИМ»

Комісія у складі:

голова: Відповідальний за відділ безпеки КО «ТИМ-ТИМ» Верес В.В.;

члени: Заступник відповідального за відділ безпеки Кум С.А., начальник спеціального відділу Кудимець І.Л.

Було проведено приймання у дослідну експлуатацію КСЗІ яка створена в АСВБ класу 2 КО «ТИМ-ТИМ» .

Під час роботи комісії встановлено:

1. КСЗІ в АСВБ створена відповідно вимог документу «АС відділу безпеки ТОВ КО «ТИМ-ТИМ». КСЗІ. Технічне завдання», а саме:

вимог до захисту інформації від витоку технічними каналами;

вимог до захисту інформації від НСД до інформації в АСВБ, компонентів АСВБ та на об’єкт інформаційної діяльності в цілому;

вимог щодо унеможливлення загроз інформації, які можуть виникати під час циркуляції в АСВБ.

2. КСЗІ в АСВБ пройшла попередні випробування та здійснює захист інформації в АСВБ про що свідчать позитивні висновки Протоколу попередніх випробувань КСЗІ в АС класу 2 відділу безпеки КО «ТИМ-ТИМ» стосовно впроваджених в КСЗІ організаційних, організаційно-технічних та технічних заходів захисту.

3. Комплект експлуатаційних документів КСЗІ в АС 2 є достатнім щодо можливості прийняття КСЗІ у дослідну експлуатацію.

Висновок:

Враховуючи вище зазначену інформацію доцільно провести дослідну експлуатацію КСЗІ в АСВБ.

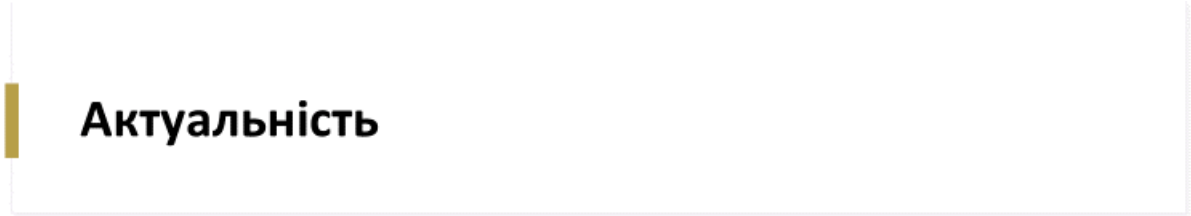
Голова комісії:
Відповідальний за відділ
безпеки КО «ТИМ-ТИМ» Верес В.В.

Члени комісії:
Заступник відповідального
за відділ безпеки КО «ТИМ-ТИМ» Кум С.А

Начальник спеціального відділу
КО «ТИМ-ТИМ» Кудимець І.Л.

ДОДАТОК Ж

Оформлення слайдів та роздаткового матеріалу



Головною метою комплексної системи захисту інформації являється забезпечити безпеку та безперервність продажу, але 100-відсотковий захист забезпечити не можливо, але забезпечити від деяких ризиків та втрат для комерційної організації дані заходи можуть зберегти компанію, тому дана тема є актуальною.

Мета та задачі роботи

Метою є розробка комплексної системи захисту інформації для комерційної організації.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

- Обстеження об’єкту як підготовки до розробки КСЗІ;
- Розробка політики, плану та ТЗ для АС класу;
- Підготовка до введення в дію КСЗІ.

Об’єкт та предмет дослідження

- Об’єкт дослідження. Комерційна організація.
- Предмет дослідження. Комплексна система захисту інформації.

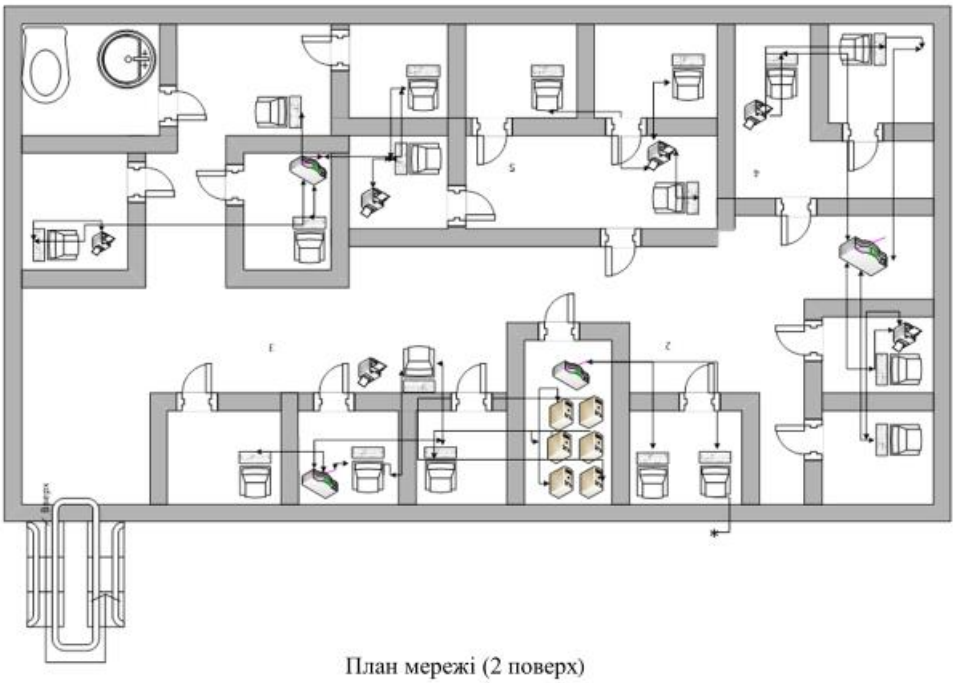
Новизна та практична цінність

- Новизна роботи. Розробка комплексної системи захисту інформації для комерційної організації.
- Практична цінність. Результати досліджень можна використовувати для комерційної організації.

РОЗДІЛ 1 ОБСТЕЖЕННЯ ОБ'ЄКТУ ЯК ПІДГОТОВКИ ДО РОЗРОБКИ КСЗІ

Мета організації. Для того, щоб розробити перелік відомостей обмеженого доступу, перелік об'єктів захисту на підприємстві, в даному випадку – комерційному, слід описати насамперед інформаційну систему. Конкретний опис місця для впровадження КЗІ – це є важливим аспектом для отримання великого прибутку та поновлення клієнтської бази.

В комерційній організації застосовують 1 тип автоматизованої системи – 2 класу.



План мережі (2 поверх)

РОЗДІЛ 2 РОЗРОБКА ПОЛІТИКИ, ПЛАНУ ТА ТЗ ДЛЯ АС КЛАСУ 2

- Розробка політики безпеки інформації в АС

КСЗІ передбачає вивчення об'єкта, на якому створюється КСЗІ, при цьому уточнює модуль загроз, модель потенційного порушника та аналіз ризиків, що виконуються на основі попередніх етапах.

- Розробка плану захисту інформації в АС

Забезпечення ефективного захисту АС розробляють план захисту інформації для організації – набір документів, згідно до яких здійснюється організація захисту інформації на всіх етапах життєвого циклу автоматизованої системи.

- Розробка технічного завдання на створення КСЗІ в АС

Технічне завдання на КСЗІ розробляється згідно вимог функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброки в АС.

Розділ 3 ПІДГОТОВКА ДО ВВЕДЕННЯ В ДІЮ КСЗІ

- Складання технроробочого проекту створення КСЗІ

Технроробочий проект КСЗІ в АС розробляється на підставі та у відповідності до ТЗ на створення КСЗІ в АС. На цьому етапі розробляється перелік документів, в я кому описується як саме створюється система, її експлуатація, а також модернізація КСЗІ в АС.

- Підготовка КСЗІ до введення в дію

Проводиться робота з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в АС. Здійснюється створення СЗІ, якщо цього не було зроблено на попередніх етапах. В основному має бути завершені робота і затверджені документи, що входять до Плану захисту.

- Попередні випробування КСЗІ в АС

Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію. Під час випробувань перевіряються працездатності КСЗІ та відповідність її вимогам ТЗ

Висновки

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

- Обстеження об'єкту як підготовки до розробки КСЗІ;
- Розробка політики, плану та ТЗ для АС класу;
- Підготовка до введення в дію КСЗІ.

В результаті виконання кваліфікаційної роботи було проведено розробку КСЗІ для КО «ТИМ-ТИМ». Відповідно було розроблено усю супровідну документацію по впровадженню КСЗІ. КСЗІ – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів ЗІ.