МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

# КОМЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

**МЕТОДИЧНІ ВКАЗІВКИ**
до виконання курсового проєкту
для студентів спеціальності
125 «Кібербезпека»

Обговорено і рекомендовано
на засіданні кафедри

кібербезпеки та математичного моделювання
*Протокол №5*
*від «23» листопада 2021р.*

Чернігів 2021

Комплексні системи захисту інформації. Методичні вказівки до виконання курсового проєкту / Укладачі: Ткач Ю.М., Семендяй С.М. – Чернігів: Національний університет «Чернігівська політехніка», 2021. –-132 с.

Укладачі: Ткач Юлія Миколаївна, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор.

Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання.

Відповідальний за випуск: Петренко Тарас Анатолійович, кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання.

Рецензент: Мехед Дмитро Борисович, кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання.

**ЗМІСТ**

# ВСТУП

Навчальним планом з курсу "Комплексні системи захисту інформації" передбачається виконання курсового проєкту, що сприяє більш глибокому вивченню основних розділів курсу.

Загальне завдання полягає у побудові комплексної системи захисту інформації (КСЗІ), відповідно до обраних тем.

Виконання, оформлення та захист курсового проєкту здійснюються студентом в індивідуальному порядку, відповідно до даних методичних вказівок.

# 1. МЕТА ТА ЗАВДАННЯ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт – важливий етап навчального процесу та науково-дослідної роботи студента, її виконання сприяє поглибленому ознайомленнюз додатковою науково-технічною літературою, документами, форумами, науковими працями вітчизняних та закордонних вчених. Також студенти набувають практичних навичок самостійно вирішувати задачі, критично мислити, шукати необхідну літературу, чітко і лаконічно формулювати запитання та формувати запити.

Метою курсового проєкту є закріплення та поглиблення теоретичних знань та практичних умінь, набутих у процесі засвоєння навчального матеріалу дисципліни.

Завдання курсового проєкту :

1. Оберіть певну тему згідно списку .
2. Опишіть перший етап в створенні КСЗІ. (Обґрунтування необхідності створення КСЗІ).
3. Опишіть другий етап в створенні КСЗІ. (Обстеження середовищ функціонування АС).
4. Опишіть третій етап в створенні КСЗІ. (Визначення потенційних загроз для інформації, яка буде циркулювати в АС).
5. Опишіть четвертий етап в створенні КСЗІ. (Розробка політики безпеки інформації в АС).
6. Опишіть п’ятий етап в створенні КСЗІ. (Розробка плану захисту інформації в АС).
7. Опишіть шостий етап в створенні КСЗІ. (Розробка технічного завдання на створення КСЗІ в АС).
8. Опишіть сьомий етап в створенні КСЗІ. (Складання техноробочого проекту створення КСЗІ).
9. Опишіть восьмий етап в створенні КСЗІ. (Підготовка КСЗІ до введення в дію).

10. Опишіть дев’ятий етап в створенні КСЗІ. (Попередні випробування КСЗІ в АС).

11. Опишіть десятий етап в створенні КСЗІ. (Дослідна експлуатація КСЗІ).

12. Опишіть одинадцятий етап в створенні КСЗІ. (Експертиза КСЗІ).

13. Опишіть дев’ятий етап в створенні КСЗІ. (Супроводження КСЗІ).

14. Розробивши всі етапи КСЗІ, зробіть висновки згідно теми вашого підприємства.

15. Підготовка організаційно-розпорядчої документації:

a) НАКАЗ __.__.20__ №___

Про затвердження Переліку відомостей, що відноситься до конфіденційної інформації.

b) АКТ обстеження об’єкта інформаційної діяльності.

c) Модель загроз.

d) Політика безпеки інформації.

e) Автоматизована система відділу безпеки. План захисту на КСЗІ.

f) Технічне завдання.

g) КСЗІ. Техноробочий проект.

h) Паспорт-формуляр.

i) Положення про службу захисту інформації.

j) Інструкція користувачу щодо порядку обробки інформації з обмеженим доступом.

k) Інструкція з режимних заходів щодо захисту інформації під час її обробки в автоматизованій системі.

l) Інструкція з адміністрування системи автоматизованої системи.

m) Інструкція з правил видачі вилучення та зберігання персональних ідентифікаторів користувачів.

n) Інструкція по правилам управління паролями.

o) НАКАЗ __.__.20__ №___ Про призначення комісії з проведення попередніх випробувань

p) Програма та методики випробувань.

q) Протокол попередніх випробувань комплексної системи захисту інформації.

r) АКТ повноти виконаних заходів із захисту інформації при створенні комплексної системи захисту інформації.

s) АКТ приймання комплексної системи захисту інформації автоматизованої системи.

t) АКТ завершення дослідної експлуатації комплексної системи захисту інформації в автоматизованій системі.

u) Атестат відповідності.

## 2. ТЕМАТИКА КУРСОВИХ ПРОЄКТІВ

Тема роботи являє собою предметну область, відповідно до якоюстудент буде розробляти КСЗІ.

Тема курсового проєкту вибирається студентом самостійно із рекомендованого викладачем списку.

Можливий індивідуальний вибір студентом теми курсового проєкту, за узгодженням з викладачем.

Дві однакові теми в межах однієї академічної групи допускаються лише за узгодження з викладачем. В такому випадку результати виконання курсового проєкту не можуть збігатись більше, ніж на 20%.

# 3. СТРУКТУРА КУРСОВОГО ПРОЄКТУ, ОСНОВНІ ЕТАПИ ЇЇ ВИКОНАННЯ

Процес виконання курсового проєкту включає наступні етапи:

- вибір теми;
- підбір та опрацювання літератури;
- аналіз предметної області;
- підготовка і захист курсового проєкту.

Курсовий проєкт повинна мати певну логіку побудови, послідовність, завершеність. Загальний обсяг курсового проєкту має бути в межах 20 сторінок друкованого тексту. До загального обсягу курсового проєкту не входять додатки, список використаних джерел.

Рекомендована структура курсового проєкту:

1. Титульний лист (додаток А).
2. Зміст (додаток Д).
3. Вступ.
4. Етапи створення КСЗІ (12 етапів).
5. Висновки.
6. Список використаних джерел (додаток Б)
7. Додатки.

Список використаних скорочень

КСЗІ – комплексна система захисту інформації.

ОІД – об'єкт інформаційної діяльності.

ЗЗІ – засоби захисту інформації.

ТЗІ – технічний захист інформації.

АС – автоматизована система.

АСВБ – автоматизована система класу 1 відділу безпеки.

ІзОД – інформація з обмеженим доступом.

НСД – несанкціонований доступ.

ПЕМВН – побічні електромагнітні випромінювання і наводки.

ОІД – об’єкт інформаційної діяльності.

ОТЗ – основні технічні засоби.

ДТЗ – допоміжні технічні засоби.

ПМА – програма і методика випробувань.

ЖМД – жорсткий магнітний диск.

ГМД – гнучкий магнітний диск.

НСД – несанкціонований доступ.

НД ТЗІ – нормативний документ системи технічного захисту інформації.

КЗЗ – комплекс засобів захисту.

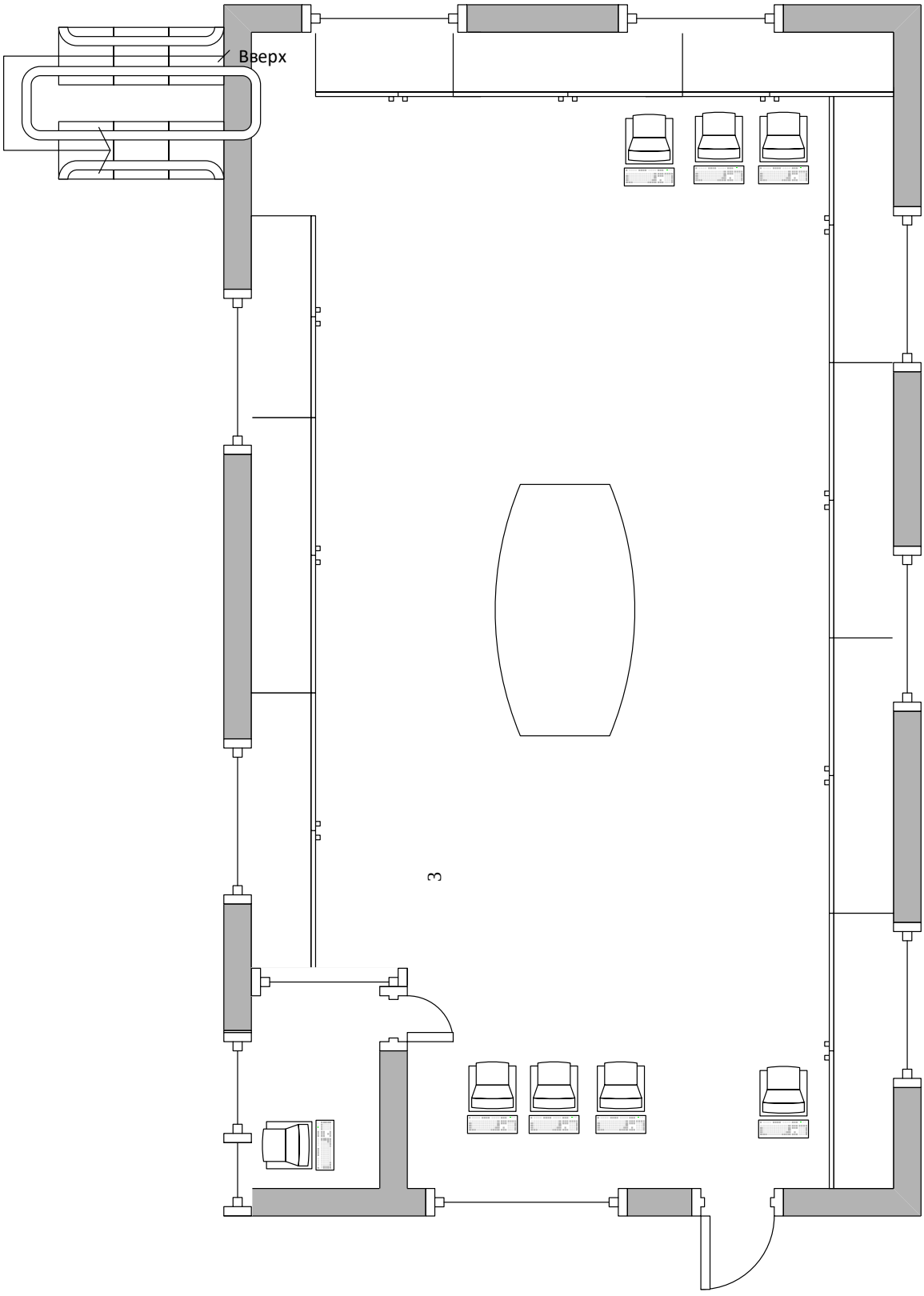


Рис.1. Ситуаційний план (1 поверх)

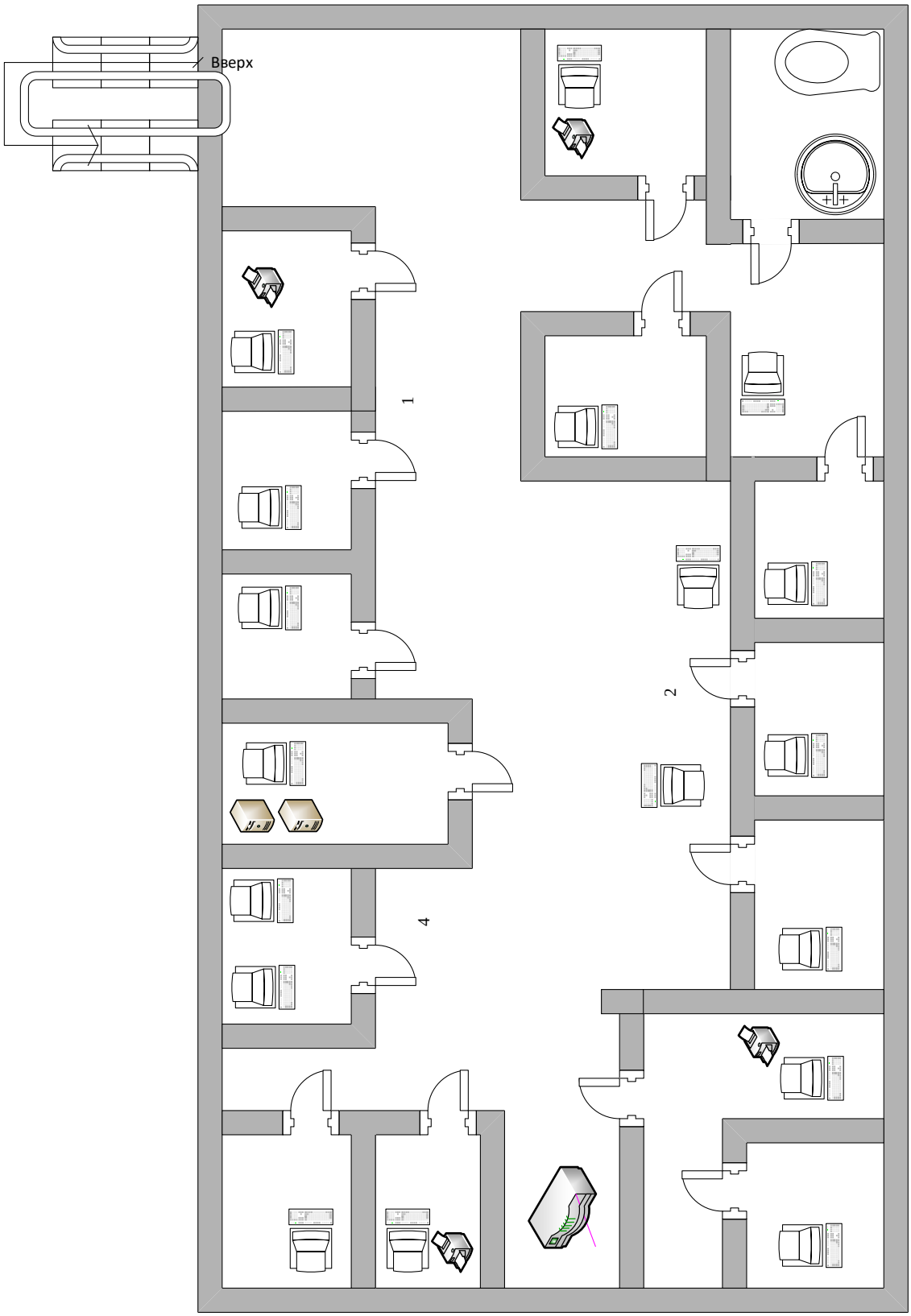


Рис.2. Ситуаційний план (2 поверх)

## Етап 1. Обґрунтування необхідності створення КСЗІ

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.

Вихідні дані для обґрунтування необхідності створення КСЗІ в загальному випадку отримуються по результатам:

1. Аналізу нормативно-правових актів (державних, відомчих і таких, які діють в межах установи, організації, підприємства), 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;

2. 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;

3. Оцінки можливості переваг (фінансово-економічних, соціальних і т.д.) експлуатація ІТС у випадку створення КСЗІ.

На основі проведеного аналізу приймається рішення про необхідність створення КСЗІ на підприємстві.

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

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

В Додатку А знаходяться такі документи:

1. Наказ «Про затвердження Переліку відомостей, що відносяться до конфіденційної інформації».

2. Перелік відомостей, що відносяться до конфіденційної інформації.

3. Акт визначення вищого ступеню обмеження доступу інформації.

## Етап 2. Обстеження середовищ функціонування АС

Автоматизована система представляю собою сукупність інформації, персоналу та комплексу засобів автоматизації діяльності, які реалізуються 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 базі даних.

Тому, для більш точного визначення інформаційної системи туристичної фірми як сукупності інформації, персоналу, матеріальних носіїв, засобів автоматизації, технічних та технологічних рішень обробки інформації.

В туристичній фірмі застосовують 1 тип автоматизованої системи – 2 класу (у вигляді мережі окремих робочих станцій, які не мають вихід до мережі Інтернет).

Інформація загальнодоступної інформації:

1. Інформація щодо статуту організації, правил внутрішнього трудового розпорядку дня та правил техніки безпеки при роботі з технікою.

2. Інформація щодо посад працівників, прізвище, ім’я та по батькові та їх робочі телефони.

3. Інформація про графіки роботи організації.

4. Клієнтські бази даних;

5. Інформація про списки підприємств по регіону та їх керівників.

Перелік інформації обмеженого доступу:

1. Особиста інформація про працівників та їх посадові інструкції.

2. Інформація про поставки техніки та обладнання для підприємства.

3. Інформація щодо фінансової діяльності організації (бухгалтерський облік та заробітна плата працівників та обслуговуючого персоналу).

4. Інформація про мережеві налаштування комп'ютерів та серверів.

5. Інформація щодо документації організації.

В Додатку Б знаходяться такі документи: Акт обстеження.

## Етап 3. Визначення потенційних загроз для інформації, яка буде циркулювати в АС

В процесі проведення обстеження туристичної фірми, визначаються потенційні загрози для інформації, таким чином обов'язково створюється модель загроз та модель порушника, дані вимоги створюються відповідно нормативно-правових документів, такі як:

1. 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);

2. 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);

3. 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 (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

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 (шкоди) по кожному з видів порушень.

В Додатку В знаходяться такі документи: Модель загроз.

## Етап 4. Розробка політики безпеки інформації в АС

Даний етап комплексної системи захисту інформації передбачає вивчення об’єкта, на якому створюється КСЗІ, при цьому уточнює модуль загроз, модель потенційного порушника та аналіз ризиків, що виконуються на основі попередніх етапів.

Розробляючи політику безпеки, треба враховувати специфіку порівняно з іншими інформаційними системами. Особливості інформаційної системи туристичної фірми зумовлені специфікою тих завдань, які виконують за її допомогою, а саме:

1. Уся інформація, яка обробляється, накопичується і зберігається в системі, є конфіденційною, тому значну увагу доводиться приділяти криптографічному захисту за допомогою шифрування, розподілу доступу й автентифікації в мережі, захисту місць підключення до мереж зв’язку тощо;

2. Інформація, яка циркулює в такій системі, не може бути втрачена, дубльована або модифікована. У зв’язку з цим посилюються вимоги до надійності апаратного і програмного забезпечення, оперативного і повного (за можливостями) відновлення інформації після аварій та збоїв у роботі;

Основними принципами створення системи захисту:

1. Конфіденційність, тобто гарантія, що інформація дається тільки авторизованим користувачам;

2. Цілісність, тобто гарантія, що інформація не може бути несанкціонованого змінена;

3. Доступність і безперервність роботи системи, тобто гарантія, що достовірна інформація буде доступна, коли це потрібно.

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.

В Додатку Г знаходяться такі документи: Політика безпеки.

## Етап 5. Розробка плану захисту інформації в АС

Для забезпечення ефективного захисту автоматизованої системи розробляють план захисту інформації для підприємства. План захисту представляє собою набір документів, згідно до яких здійснюється організація захисту інформації на всіх етапах життєвого циклу автоматизованої системи, а саме:

1. Класифікація інформації автоматизованої системи;
2. Загальний опис компонентів автоматизованої системи;
3. Технології розробки інформації в автоматизованої системи;
4. Модель загроз автоматизованої системи.

В Додатку Д знаходяться такі документи: План захисту інформації.

## Етап 6. Розробка технічного завдання на створення КСЗІ в АС

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є основним організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі.

Технічне завдання на КСЗІ розробляється відповідно до вимог функціонального складу і порядку розробки і впровадження технічних засобів,

що забезпечують безпеку інформації в процесі її оброки в автоматизованій системі. Додатково необхідно також викласти вимоги до організаційних, фізичних та інших заходів захисту (комплекс програмно-технічних заходів захисту інформації).

Дане технічне завдання є обов'язковим документом під час проведення експертизи автоматизованої системи на відповідність вимог.

Роботу з погодження проекту проводить технічного завдання на КСЗІ в АС здійснюють спільно Розробник ТЗ та Замовник.

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

В Додатку Е знаходяться такі документи:

2 Технічне завдання.

## Етап 7. Складання технороботочого проекту створення КСЗІ

Технороботочий проект комплексної системи захисту інформації в АС розробляється на підставі та у відповідності до технічного завдання на створення КСЗІ в АС. На цьому етапі розробляється перелік документів, в якому описується, як саме створюється система, її експлуатація, а також модернізація КСЗІ в АС.

Технороботочий проект включає такі етапи:

### Розробка технічного проєкту

На етапі розробки технічного проєкту. Необхідно розробити загальні проєкті 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 (інструкція) щодо забезпечення цього порядку обслуговуючим персонал і користувачами, порядку супроводження КСЗІ впродовж життєвого АС.

В Додатку Є знаходяться такі документи: Технороботчий проект.

## Етап 8. 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 (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах. В основному має бути завершені робота і затверджені документи, що входять до Плану захисту (за виключенням тих, для розробки яких необхідні результати етапів робіт).

Проект КСЗІ розробляється на підставі та у відповідності до ТЗ на створення ІТС (доповнення до нього, окремого ТЗ на створення КСЗІ). 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.

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.

В Додатку Ж знаходяться такі документи: Паспорт-формуляр.

## Етап 9. 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.

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.

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.

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.

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

В Додатку З знаходяться такі документи:

1. Протокол попередніх випробувань комплексної системи захисту інформації.

2. Акт приймання комплексної системи захисту інформації.

## Етап 10. Дослідна експлуатація КСЗІ

Дослідну експлуатацію організовує та проводить Замовник.

Під час дослідної експлуатації КСЗІ:

1. Відпрацьовування технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

2. Співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

3. Здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагодження та конфігурування КЗЗ;

4. Здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державно експертизу.

В Додатку И знаходяться такі документи: Акт завершення дослідної експлуатації.

## Етап 11. Експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань АС. Для проведення експертизи КСЗІ або засобу безпеки (далі – засіб ТЗІ) Замовник надсилає заяву встановленої форми на ім’я Голови (заступника голови) Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку) за адресою: 03680, м. Чернігів, вул. Солом’янська, 13.

За результатами розгляду заяви у місячний термін приймається рішення

про можливість й доцільність проведення експертизи та визначення підрозділу Держспецзв'язку підприємства, установи або в організації, які проводитимуть експертизу (далі – Організатор експертизи).

Відносини між Замовником і Організатором експертизи регламентується укладеним між ними договором про проведення експертизи. Термін проведення експертизи визначається договором і не повинен перевищувати 6 місяців. У разі значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації Держспецзв'язку та Замовника.

Замовник надає Організатору експертизи комплект організаційно-технічної документації на КСЗІ в АС або засіб ТЗІ, необхідний для проведення експертних випробувань.

Організатор експертизи, за результатами аналізу наданих Замовником документів і з урахуванням загальних методик оцінювання задекларованих характеристик об'єкта експертизи, формує програму і окремі методики проведення експертизи та розробляє , у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань відповідне програмно-технічне забезпечення.

Програма проведення експертизи узгоджується із замовником та Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації Держспецзв'язку, а окремі методики – з зазначеним департаментом.

Терміни розробки окремих методик та необхідного програмно-технічного забезпечення залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи.

Результати експертних робіт за окремими методиками оформлюються у вигляді протоколу виконання робіт, затвердженого Організатором експертизи.

У разі виявлення невідповідності об'єкта експертизи вимогам нормативних документів з ТЗІ, Організатор експертизи може запропонувати Замовнику виконати доробку КСЗІ в ІТС або засобу ТЗІ. Терміни доробки визначається спільним протоколом або додатковою угодою до договору між

Замовником та Організатором експертизи.

Відомості щодо всіх доробок, а також додаткових експертних робіт оформлюються окремими протоколами.

За результатами проведених робіт Організатор експертизи складає експертний висновок щодо відповідності КСЗІ в ІТС або засобу ТЗІ вимоги нормативних документів з ТЗІ і разом з протоколом виконаних робіт подається до Адміністрації Держспецзв'язку.

У разі наявності у Замовника обґрунтованих претензій щодо порядку проведення або результатів експертизи, він може звернутися до Адміністрації Держспецзв'язку з пропозицією щодо здійснення контролю за проведенням Організатором експертизи експертних робіт. Мета проведення Експертизи КСЗІ в АС полягає у дослідженні, перевірці, аналізі та оцінці КСЗІ в АС щодо можливості її використання для забезпечення безпеки в АС.

Суб'єктами, що приймають участь в Державній експертизі КСЗІ в АС є:

1. Замовник (організація – власник КСЗІ та АС);

2. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку – контролюючий орган);

3. Організатор (організація-виконавець Державної експертизи);

4. Експерти.

Відповідно до 1.4 «Положення про Державну експертизу в сфері технічного захисту інформації» (Затвердженого наказом Адміністрації Держспецзв'язку України №93 від 16.05.07), КСЗІ підлягає обов'язковій перевірці на відповідність вимогам нормативних документів з безпеки (НД ТЗІ). НД ТЗІ та технічного завдання на КСЗІ в АС і містить наступні етапи:

1. Аналіз документації на КСЗІ в АС;

2. Розробка програми та методики проведення Експертизи КСЗІ в АС;

3. Узгодження програми і методики з Державною службою спеціального зв'язку та захисту інформації України (Програма також погоджується із замовником);

4. Обстеження об'єкта і проведення випробувань;

5. Оформлення протоколів проведення випробувань;

6. Оформлення Експертного висновку.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причини усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування. В першу чергу такий порядок рекомендується застосувати для складних з точки зору архітектури, складу та обсягів робіт КСЗІ. При цьому експертами послідовно здійснюється оцінка технічних та організаційних рішень на всіх етапах робіт. Це дає змогу оперативно усувати недоліки проектування та скоротити час проведення державної експертизи, яка може бути в основаному завершена до етапу приймальний випробувань АС.

Необхідно звернути увагу, що державну експертизу КСЗІ не може проводити організація, яка розробляє КСЗІ. Організація, що проводить Державну експертизу визначається ДССЗЗІ України.

## Етап 12. Супроводження КСЗІ

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації.

Підготовка організаційно-розпорядчої документації

**Посадова інструкція генерального директора**

І. Загальні положення

Директор підприємства належить до професійної групи «Керівники».

Призначення на посаду керівника підприємства та звільнення з неї здійснюється з дотриманням вимог Кодексу законів про працю України та чинного законодавства про працю.

Директор підприємства є підзвітним засновникам підприємства в особі Коломієць Марини В'ячеславівни.

ІІ. Завдання та обов'язки

Директор підприємства:

1. Визначає, формулює, планує, здійснює і координує всі види діяльності підприємства.

2. Визначає напрями розвитку підприємства у формуванні цінової, кредитно-банківської, податкової та страхової політики, соціальної та зовнішньоекономічної діяльності.

3. Організує роботу і ефективну взаємодію виробничих одиниць, цехів та інших структурних підрозділів підприємства, направляє їх діяльність на досягнення високих темпів розвитку і удосконалення виробництва та продукції.

4. Забезпечує відповідність продукції кращим світовим зразкам з метою задоволення потреб замовників і споживачів у відповідних видах продукції, підвищення продуктивності праці, ефективності виробництва і якості продукції на основі широкого запровадження нової техніки і прогресивної технології, організації праці, виробництва і управління, удосконалення господарського механізму.

5. Направляє діяльність персоналу на досягнення високих економічних та фінансових результатів.

6. Забезпечує виконання підприємством програми оновлення продукції, планів капітального будівництва, обов'язків перед державним бюджетом, постачальниками, замовниками і банками.

7. Організує виробничо-господарську діяльність підприємства на основі застосування методів обґрунтованого планування, нормативних матеріалів, фінансових і трудових витрат, широкого розповсюдження передового досвіду, а також максимальної мобілізації резервів виробництва шляхом досягнення

високих техніко-економічних показників, підвищення технічного рівня і якості продукції, раціонального і економного витрачання всіх видів ресурсів.

8. Вживає заходів щодо забезпечення підприємства кваліфікованими кадрами, найкращого використання безпечних і сприятливих умов праці, додержання вимог законодавства про охорону навколишнього середовища.

9. Здійснює заходи з соціального розвитку колективу підприємства, забезпечує розроблення, укладання і виконання колективного договору, проводить роботу щодо зміцнення трудової і виробничої дисципліни, сприяє розвитку творчої ініціативи і трудової активності працівників.

10. Забезпечує сполучення економічних і адміністративних методів керівництва, матеріальних і моральних стимулів підвищення ефективності виробництва, а також підсилення відповідальності кожного працівника за доручену йому справу.

11. Вирішує всі питання в межах наданих йому прав, доручає виконання окремих організаційно-господарських функцій іншим посадовим особам: заступникам керівника, керівникам виробничих підрозділів підприємства.

12. Забезпечує додержання законності, активне використання правових засобів удосконалення управління, зміцнення договірної дисципліни і обліку, господарського розрахунку.

13. Здійснює заходи щодо соціального захисту колективу підприємства, забезпечення і збереження зайнятості працівників.

14. Представляє підприємство в органах державної влади і у взаємовідносинах з партнерами.

15. Готує проекти нормативних документів, що вимагають затвердження загальними зборами акціонерів.

III. Права

Директор підприємства має право:

1. Без доручення діяти від імені підприємства.

2. Представляти інтереси підприємства у взаємовідносинах з громадянами, юридичними особами та органами державної влади.

3. Розпоряджатися майном підприємства з дотриманням вимог, визначених законодавством, Статутом підприємства, іншими нормативними правовими актами.

4. Відкривати в банківських установах розрахунковий та інші рахунки.

5. Укладати трудові договори з працівниками.

6. Приймати рішення за поданням:

1. про притягнення працівників, що порушили виробничу та трудову дисципліну, винних в завданні матеріальної шкоди підприємству, до матеріальної та дисциплінарної відповідальності;

2. про моральне та матеріальне заохочення працівників, що відзначилися.

IV. Відповідальність

Директор підприємства несе відповідальність:

1. За неналежне виконання або невиконання своїх посадових обов'язків, що передбачені цією посадовою інструкцією, - в межах, визначених чинним законодавством України про працю.

2. За правопорушення, скоєні в процесі здійснення своєї діяльності, - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

3. За завдання матеріальної шкоди - в межах, визначених чинним цивільним законодавством та законодавством про працю України.

4. Директор підприємства несе персональну відповідальність за наслідки прийнятих ним рішень, що виходять за межі його повноважень, які визначені чинним законодавством, Статутом підприємства, іншими нормативними правовими актами. Керівник підприємства не звільняється від відповідальності, якщо дії, що тягнуть відповідальність, були здійснені особами, яким він делегував свої права.

5. Директор підприємства, який недобросовісно використовує майно та кошти підприємства у власних інтересах, або в інтересах, протилежних інтересам засновників, несе відповідальність в межах, визначених цивільним,

кримінальним та адміністративним правом.

V. Директор підприємства повинен знати:

1. Закони, постанови, укази, розпорядження, рішення та інші нормативно-правові акти органів державної влади і місцевого самоврядування, які регулюють порядок діяльності підприємства.

2. Профіль, спеціалізацію і особливості структури підприємства.

3. Перспективи, вітчизняні і світові тенденції технологічного, технічного, економічного і соціального розвитку галузі і підприємства.

4. Можливості ефективного використання виробничих потужностей, наявних технологічних процесів, їх реструктуризації або заміни.

5. Порядок розроблення і затвердження планів та програм виробничо-господарської діяльності.

6. Сучасні методи господарювання і управління.

7. Порядок укладання і виконання господарських договорів.

8. Вітчизняні і зарубіжні досягнення науки і технології відповідно до галузі виробництва і досвід завоювання позицій на світових і регіональних ринках продукції.

9. Економіку, організацію виробництва, праці і управління.

10. Напрями та принципи розвитку менеджменту, маркетингу, комерційної діяльності, податкової справи.

11. Етику ділового спілкування та ведення переговорів.

VI. Кваліфікаційні вимоги

Повна вища освіта відповідного напряму підготовки (магістр, спеціаліст). Післядипломна освіта в галузі управління. Стаж роботи за професіями керівників нижчого рівня не менше 5 років.

VII. Взаємовідносини (зв’язки) за посадою

За відсутності директора підприємства його посадові обов’язки виконують заступники, які призначаються у встановленому порядку. Заступники несуть відповідальність за якісне, своєчасне та ефективне виконання посадових обов’язків директора підприємства на час його відсутності.

## Посадова інструкція бухгалтера

І. Загальні положення

Бухгалтер належить до професійної групи «Професіонали».

Призначення на посаду бухгалтера та звільнення з неї здійснюється наказом директора підприємства за поданням головного бухгалтера з дотриманням вимог Кодексу законів про працю України.

Бухгалтер підпорядковується безпосередньо головному бухгалтеру підприємства або керівнику відповідного структурного підрозділу головної бухгалтерії.

За відсутності бухгалтера його обов'язки виконує особа, призначена у встановленому порядку), яка набуває відповідних прав та несе відповідальність за належне виконання покладених на неї обов'язків.

ІІ. Завдання та обов'язки

Бухгалтер:

1. Самостійно і в повному обсязі веде облік необоротних активів, запасів, коштів, розрахунків та інших активів, власного капіталу та зобов'язань, доходів та витрат за прийнятою на підприємстві формою бухгалтерського обліку з додержанням єдиних методологічних засад бухгалтерського обліку та з урахуванням особливостей діяльності підприємства й технології оброблення даних.

2. Забезпечує повне та достовірне відображення інформації, що міститься у прийнятих до обліку первинних документах, на рахунках бухгалтерського обліку.

3. За погодженням з власником (керівником) підприємства та керівником підрозділу бухгалтерського обліку, подає в банківські установи документи для перерахування коштів згідно з визначеними податками й платежами, а також для розрахунків з іншими кредиторами відповідно до договірних зобов'язань.

4. Бере участь у проведенні інвентаризації активів і зобов'язань, оформленні матеріалів, пов'язаних з нестачею та відшкодуванням втрат під нестачі, крадіжки й псування активів підприємства, у перевірках стану

бухгалтерського обліку у філіях, представництвах, відділеннях та інших відокремлених підрозділах підприємства.

5. Готує дані для включення їх до фінансової звітності, здійснює складання окремих її форм, а також форм іншої періодичної звітності, яка ґрунтується на даних бухгалтерського обліку.

6. Забезпечує підготовку оброблених документів, реєстрів і звітності для зберігання їх протягом установленого терміну.

Бере участь у підготовці пропозицій щодо:

1. внесення змін до обраної облікової політики, удосконалення внутрішньогосподарського (управлінського) обліку та правил документообігу;

2. розроблення додаткової системи рахунків і регістрів аналітичного обліку, звітності й контролю господарських операцій;

3. забезпечення збереження майна, раціонального та ефективного використання матеріальних, трудових та фінансових ресурсів, залучення кредитів та їх погашення, регулювання діяльності підприємства та інших питань, пов’язаних з інформацією про фінансове становище підприємства та результати його діяльності.

Постійно знайомиться та вивчає нові нормативно-методичні ти довідкові документи з питань організації та ведення бухгалтерського обліку та вносить пропозиції щодо їх впровадження на підприємстві.

Виконує окремі службові доручення свого безпосереднього керівника.

III. Права

Бухгалтер має право:

1. Ознайомлюватися з проектами рішень керівництва підприємства, що стосуються його діяльності.

2. Вносити на розгляд головного бухгалтера пропозиції по вдосконалення роботи, пов’язаної з обов’язками, що передбачені цією інструкцією.

3. В межах своєї компетенції повідомляти безпосередньому керівнику про всі виявлені недоліки в діяльності підприємства та вносити пропозиції щодо їх усунення.

4. Вимагати та отримувати особисто або за дорученням головного бухгалтера у керівників структурних підрозділів та фахівців інформацію та документи, необхідні для виконання його посадових обов’язків.

5. Залучати фахівців усіх структурних підрозділів до виконання покладених на нього завдань.

6. Вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов’язків.

IV. Відповідальність

Бухгалтер несе відповідальність:

1. За неналежне виконання або невиконання своїх посадових обов’язків, що передбачені цією посадовою інструкцією, — в межах, визначених чинним законодавством України про працю.

2. За правопорушення, скоєні в процесі здійснення своєї діяльності, — в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

3. За завдання матеріальної шкоди – в межах, визначених чинним цивільним законодавством та законодавством про працю України

V. Бухгалтер повинен знати:

4. Нормативні, методичні та інші керівні матеріали з організації та ведення бухгалтерського обліку та складання фінансової звітності.

5. Облікову політику, систему регістрів обліку, правила документообігу й технологію оброблення облікової інформації на підприємстві.

6. План рахунків бухгалтерського обліку активів, капіталу, зобов’язань і господарських операцій.

7. Систему і форми внутрішньогосподарського (управлінського) обліку, звітності й контролю.

8. Основи трудового законодавства.

9. Правила та норми охорони праці.

VI. Кваліфікаційні вимоги

Провідний бухгалтер (з дипломом спеціаліста): повна вища освіта відповідного напряму підготовки (магістр, спеціаліст) та підвищення кваліфікації. Стаж роботи за професіє ю бухгалтера I категорії по менше 2 років.

Бухгалтер I категорії (з дипломом спеціаліста): повна або базова вища освіта відповідного напряму підготовки (магістр, спеціаліст або бакалавр) та підвищення кваліфікації; для магістра — без вимог до стажу роботи, спеціаліста — стаж роботи за професією бухгалтера II категорії не менше 2 років, бакалавра — не менше 3 років.

Бухгалтер II категорії (з дипломом спеціаліста): повна або базова вища освіта відповідного напряму підготовки (спеціаліст або бакалавр) ти підвищення кваліфікації; для спеціаліста — без вимог до стажу роботи, стаж роботи за професією бухгалтера не менше 2 років.

Бухгалтер (з дипломом спеціаліста): повна або базова вища освіта відповідного напряму підготовки (спеціаліст або бакалавр) без вимог до стажу роботи.

**Посадова інструкція юриста**

I. Загальні положення

Юрист належить до категорії спеціалістів.

На посаду юриста призначається особа, яка має вищу юридичну освіту та досвід роботи від 1 року на аналогічній посаді.

Юрист повинен мати презентабельний зовнішній вигляд, вміння правильно і грамотно формулювати свої висловлювання, стійкість у стресових ситуаціях.

Юрист повинен знати:

1. Нормативно – правову базу, яка регламентує господарську діяльність підприємств;

2. Структуру та компетенцію державних органів, органів місцевого самоврядування, судів;

3. Повинен вільно орієнтуватися в основних галузях права (цивільному, підприємницькому, адміністративному, трудовому, податковому, банківському,

кримінальному тощо);

4. Порядок укладання та оформлення договорів;

5. Правила складання позовних заяв, апеляцій, касаційних скарг, договорів, протоколів розбіжностей до них, юридичних довідок;

6. Надання усних і письмових юридичних консультацій;

7. Порядок ведення переговорів з клієнтами;

8. Етику ділового спілкування;

9. Правила роботи з документами, основи діловодства, порядок систематизації та ведення правової документації з використанням сучасних інформаційних технологій.

Призначення на посаду юриста та звільнення з цієї посади оформляється наказом керівника юридичної фірми.

Юрист підпорядковується безпосередньо керівнику юридичної фірми.

II. Посадові обов'язки

Юрист:

1. Здійснює роботу для забезпечення додержання законності в діяльності юридичної фірми та захист його правових інтересів;

2. Здійснює правову експертизу наказів, інструкцій, положень та інших документів юридичної фірми, за необхідності візує їх, а також бере участь у їх підготовці;

3. Здійснює підготовку юридичних довідок і висновків з питань діяльності юридичної фірми;

4. Представляє інтереси юридичної фірми в усіх органах державної влади, місцевого самоврядування, судах усіх інстанцій;

5. Надає юридичні послуги клієнтам юридичної фірми та представляє їхні інтереси на підставі укладеного Договору про надання юридичних послуг та Довіреності, оформленої належним чином;

6. Надає весь комплекс юридичних послуг клієнтам від імені юридичної фірми, а саме здійснює підготовку і аналіз договорів, протоколів розбіжностей, юридичних довідок, наказів, протоколів та всіх інших документів, надає усні та

письмові консультації з правових питань, представляє інтереси клієнтів в органах державної влади, місцевого самоврядування та в судах всіх інстанцій, в органах державної виконавчої служби, здійснює отримання ліцензій, дозволів для здійснення господарської діяльності клієнтів.

7. Веде ділове спілкування з клієнтами юридичної фірми, відповідає на телефонні дзвінки;

8. Організує та проводить переговори в інтересах фірми або її клієнтів з третіми особами;

9. Визначає перелік необхідних документів для надання юридичних послуг клієнту, у разі потреби допомагає в отриманні таких документів;

10. Здійснює надання юридичних послуг як на своєму робочому місті, так і з виїздом до клієнта або інших установ та організацій;

11. Здійснює моніторинг законодавства та повідомляє керівника та клієнтів юридичної фірми про всі зміни в законодавстві, які стосуються їхньої діяльності;

12. Ознайомлюється з правовими системами та базами даних, періодичними виданнями з юридичної тематики, готує аналітичні статті, доповіді, бере участь у презентаціях юридичної фірми, конференціях тощо;

13. Здійснює інші обов’язки в межах своєї компетенції за дорученням керівництва.

III. Права юриста

Запитувати та отримувати документи, інформацію та матеріали, необхідні для виконання обов’язків, що передбачені цією посадовою інструкцією.

Вести листування, в тому числі в електронному вигляді, з державними органами, установами, організаціями від імені та в інтересах як юридичної фірми, так і від її клієнтів.

Представляти інтереси юридичної фірми і її клієнтів перед іншими органами, установами та особами за дорученням.

Вносити на розгляд керівництва пропозиції щодо покращення та вдосконалення своєї роботи та роботи інших працівників фірми.

Вимагати від керівництва забезпечення організаційно – технічних умов для належного виконання своїх посадових обов'язків.

IV. Відповідальність юриста

За неналежне виконання або невиконання своїх посадових обов'язків, які передбачені цією інструкцією, - відповідно до трудового договору та законодавства України про працю.

За інші порушення в процесі своєї діяльності – в межах, становлених цивільним, кримінальним, адміністративним законодавством України.

Конфіденційність. Збереження комерційної таємниці

До конфіденційної інформації належать відомості, що знаходяться у володінні, користуванні або розпорядженні юридичної фірми і поширюються за його згодою відповідно до передбачених ним умов.

До конфіденційної інформації юридичної фірми належать відомості про структуру юридичної фірми та її клієнтів, стан їхніх банківських рахунків, рівень доходів та боргових зобов'язань, методи вивчення ринку послуг, інформація щодо клієнтів юридичної фірми (відомості про співробітників та керівників, їх номера телефонів, адреси тощо), її компаньонах та конкурентах.

Комерційною таємницею юридичної фірми є такі відомості про саму юридичну фірму та її клієнтів: умови договорів (контрактів), дані про контрагентів, інформація про переговори, калькуляція витрат та прибутків, бази даних та інші комп'ютерні програми, креслення, схеми тощо. Комерційна таємниця є конфіденційною інформацією.

Не становлять конфіденційної інформації відомості, розкриття яких передбачене чинним законодавством.

Юрист зобов'язаний не розголошувати усі відомості, що становлять конфіденційну інформацію, які були отримані ним за період роботи, і використовувати ці відомості лише за згодою та в інтересах юридичної фірми та її клієнтів. Юрист зобов'язаний вживати заходів щодо збереження конфіденційної інформації від посягань з боку третіх осіб.

Всі документи у будь-якому вигляді (а також будь-які робочі записи,

чернетки, креслення, схеми) які створені юристом на виконання службових завдань є власністю юридичної фірми.

Юрист зобов'язується не розголошувати умови свого трудового договору або окремих його частин, посадової інструкції. Ця умова не поширюється на вимоги, встановлені чинним законодавством України.

Юристу не дозволяється ні прямо, ні посередньо привласнювати або використовувати на свою користь майно, документи, а також будь-які робочі записи, чернетки, креслення, схеми, які належать юридичній фірмі.

За неправомірне розголошення комерційної таємниці юрист несе цивільно-правову, адміністративну та кримінальну відповідальності відповідно до чинного законодавства.

За неправомірне розголошення комерційної таємниці юрист несе дисциплінарну відповідальність (догана, звільнення), а також може бути позбавлений премії, відсотків та інших видів заохочення.

Юрист повинен додержуватися нерозголошення конфіденційної інформації і комерційної таємниці також і після припинення своїх трудових обов'язків з юридичною фірмою.

V. Інші умови

Ця посадова інструкція складена в двох екземплярах, один з яких зберігається у керівника юридичної фірми, а інший – у юриста.

Ця посадова інструкція може бути уточнена та змінена відповідно до зміни структури юридичної фірми та її задач.

Зміни та доповнення до цієї посадової інструкції вносяться наказом керівника юридичної фірми.

**Посадова інструкція начальника відділу продаж**

I. Загальні положення

Відповідальний за відділ продажів відноситься до категорії керівників, приймається на роботу і звільняється Президентом компанії.

Основним завданням начальника відділу продажів є здійснювати організацію збуту продукції.

Відповідальний за відділ продажів у своїй діяльності підпорядковується безпосередньо Комерційному директору.

Відповідальний за відділ продажів повинен знати:

1. законодавчі та нормативні акти, що регламентують підприємницьку та комерційну діяльність;
2. ринкову економіку, підприємництво та ведення бізнесу;
3. порядок ціноутворення, оподаткування, основи маркетингу;
4. порядок розробки комерційних умов, бізнес-планів, угод, договорів, контрактів;
5. етику ділового спілкування;
6. структуру управління організацією;
7. основи діловодства;
8. методи обробки інформації з використанням сучасних технічних засобів, комунікацій зв'язку, обчислювальної техніки.

У своїй діяльності Відповідальний за відділ продажів керується:

1. законодавчими і нормативними актами, що стосуються виконуваної ним роботи;
2. статутом організації;
3. правилами внутрішнього трудового розпорядку;
4. наказами та розпорядженнями керівництва організації;
5. цією посадовою інструкцією.

На час відсутності Начальника відділу продажів його права та обов'язки переходять до іншого посадовій особі, про що оголошується в наказі.

II. Посадові обов'язки

1. Відповідальний за відділ продажів зобов'язаний:
2. Виконувати план продажів;
3. Аналізувати і систематизувати клієнтську базу;
4. Контролювати стан дебіторської та кредиторської заборгованостей клієнтів;
5. Вирішувати конфліктні ситуації «клієнт-менеджер»;

6. Своєчасне надавати у відділ розвитку замовлення на постачання товару по клієнтській базі;

7. Розробляти критерії оплати менеджерів відділу продажів;

8. Організовувати навчання, тренінги для менеджерського складу (спільно з відділом розвитку);

9. Брати участь в організації та проведенні виставок;

10. Контролювати зовнішній вигляд, стан робочих місць і дисципліну;

11. Вирішувати Рекламаційні питання по товару з клієнтами, складати необхідну документацію;

12. Встановлювати і контролювати відпускні ціни, розробляти цінову політику.

13. Здійснювати підбір співробітників відділу

III. Права

Відповідальний за відділ продажів має право:

1. Вносити пропозиції щодо додаткового преміювання за умови виконання плану продажів;

2. Вносити пропозиції щодо прийому і звільнення співробітників відділу продажів;

3. Депремірувати співробітників відділу продажів;

4. Вносити пропозиції щодо депреміювання працівників інших підрозділів у разі невиконання ними посадових обов'язків;

5. Вносити пропозиції щодо зміни асортиментної політики електропобутового напряму.

IV. Відповідальність

Відповідальний за відділ продажів несе відповідальність за:

1. Недбале, халатне ставлення до своїх обов'язків.

2. Нетактовну ставлення до співробітників організації.

3. Неправомірні дії з документами та інформацією про діяльність організації (зобов'язаний зберігати комерційні таємниці організації).

4. Порушення внутрішнього розпорядку підприємства.

5. Якість і своєчасність виконання покладених на нього цією посадовою інструкцією обов’язків.

Дисциплінарна, матеріальна і інша відповідальність Начальника відділу продажів визначається відповідно до чинного законодавства України.

**Посадова інструкція системного адміністратора**

І. Загальні положення:

1. Адміністратор системи безпосередньо підпорядковується директору організації.

2. Посадова інструкція визначає посадові обов’язки, повноваження й відповідальність, а також умови роботи адміністратора системи.

3. Адміністратор системи призначається на посаду й звільняється з посади відповідно до чинного трудового законодавства розпорядженням директора організації.

4. У період тимчасової відсутності адміністратора системи його обов’язки виконує особа, призначена у встановленому порядку. Дана особа отримує відповідні права й відповідає за виконання зазначених обов’язків.

ІІ. У своїй роботі керується й повинен знати:

1. Основи інформатики, вищої математики.

2. Основи теорії алгоритмів, методи побудови формальних мов, основні структури даних, основи машинної графіки, архітектурні особливості й фізичні основи побудови сучасних ПК.

3. Основні моделі даних і їх організацію.

4. Мови системного програмування.

5. Принципи побудови мов запитів і маніпулювання даними.

6. Синтаксис, семантику й формальні способи опису мов програмування, конструкції розподіленого й паралельного програмування, методи й основні етапи трансляції.

7. Принципи побудови експертних систем.

8. Способи й механізми керування даними.

9. Принципи організації, склад і схеми роботи операційних систем.

10. Принципи керування ресурсами, методи організації файлових систем.

11. Принципи побудови мережевої взаємодії.

12. Основні методи розробки програмного забезпечення.

13. Апаратне забезпечення.

14. Інформаційне законодавство.

15. Законодавство про авторські й суміжні права.

16. Правила й норми охорони праці, техніки безпеки й протипожежного захисту.

17. Правила користування оргтехнікою й ПК.

18. Правила внутрішнього трудового розпорядку.

III. Посадові обов'язки:

1. Консультувати працівників організації з питань використання обчислювальної техніки й комп'ютерних інформаційних технологій.

2. Здійснювати інсталяцію, настроювання й оптимізацію системного програмного забезпечення, і освоєння прикладних програмних засобів.

3. Розробляти й впроваджувати прикладні програми.

4. Здійснювати підключення й заміну зовнішніх обладнань, проводити тестування засобів обчислювальної техніки.

5. Забезпечувати ведення комп'ютерних баз даних.

6. Проводити комп'ютерні антивірусні заходи.

7. Брати участь в адмініструванні локальної обчислювальної мережі організації.

8. Організовувати супроводження договорів із сторонніми організаціями, що надають послуги по комунікаційнім, програмному й апаратному оснащенню організації.

9. Забезпечувати обмін інформацією локальної мережі із зовнішніми організаціями по телекомунікаційних каналах.

10. Здійснювати тестування й ремонт окремих обладнань, засобів обчислювальної техніки, кабельних ліній локальної мережі.

11. Усувати аварійні ситуації, пов’язані з ушкодженням програмного забезпечення й баз даних.

12. Організовувати тестування й навчання співробітників організації основам комп’ютерної грамотності й роботі із прикладними програмними засобами.

13. Забезпечувати технічний супровід застосовуваних локальних мереж і програмного забезпечення.

14. Виконувати профілактичні роботи з підтримки працездатності засобів обчислювальної техніки.

15. Організовувати ремонт засобів обчислювальної техніки із залученням спеціалізованих установ.

16. Здійснювати систематичний аналіз ринку апаратних засобів і програмного забезпечення.

17. Підготовляти пропозиції про придбання, розробку або обмін апаратного забезпечення.

18. Здійснювати своєчасне повідомлення про плани модернізації апаратного й програмного забезпечення.

19. Підтримувати позитивний та моральний клімат в відділі. Проявляти взаємовиручку, відповідальність, довіру, підтримку, оптимізм.

20. Виконувати окремі службові доручення безпосереднього керівника.

21. Виконувати правила трудового розпорядку, прийняті в організації.

22. Підтримувати WEB сторінку організації в належному стані.

IV. Посадові повноваження:

1. Запитувати від співробітників і керівників організації інформацію й документи, необхідні для виконання своїх посадових обов’язків.

2. Знайомитися з документами, що визначають права й обов’язки по займаній посаді, критеріями оцінки якості виконання посадових обов’язків.

3. Вносити на розгляд керівництва пропозиції з удосконалювання роботи, пов’язаної з підприємством передбаченими даною інструкцією обов’язками.

V. Посадова відповідальність:

За невиконання або неналежне виконання своїх посадових обов’язків, передбачених даною інструкцією, – у межах, установлених чинним трудовим законодавством України.

1. За невиконання посадових обов’язків.

2. За порушення правил внутрішнього розпорядку організації.

3. За порушення ділової етики.

4. За нераціональне використання комп’ютерної техніки.

5. За правопорушення, здійснені в процесі своєї діяльності, установлені чинним законодавством України.

6. За надання недостовірної інформації керівництву та на WEB сторінку.

7. За недбале поводження у веденні документації.

8. За розголошення інформації, що є службовою.

VI. Умови роботи:

1. Режим роботи адміністратора системи визначається відповідно до Правил внутрішнього трудового розпорядку.

2. Адміністратор системи у зв’язку з виробничою необхідністю може виїжджати в службові (місцеві й регіональні) відрядження.

3. супровідні документи.

4. Наводити в належний порядок обладнання після проведення робіт; при необхідності мити і чистити обладнання з дотриманням відповідних інструкцій щодо його експлуатації.

5. Підтримувати позитивний моральний клімат в офісі. Виявляти взаємовиручку, відповідальність, довіру, підтримку, оптимізм.

6. Виконувати окремі службові доручення безпосереднього керівника.

7. Виконувати правила трудового розпорядку, прийняті в компанії.

Посадові повноваження:

1. Запитувати від співробітників і керівників Підрозділу інформацію і документи, необхідні для виконання своїх посадових обов'язків.

2. Знайомитися з документами, що визначають права і обов'язки за займаною посадою, критеріями оцінки якості виконання посадових обов'язків.

3. Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з передбаченими даною інструкцією обов'язками.

V. Посадова: відповідальність:

1. За невиконання або неналежне виконання своїх посадових обов'язків, передбачених цією посадовою інструкцією, - в межах, визначених чинним цивільним законодавством України.

2. За невиконання посадових обов'язків.

3. За порушення правил внутрішнього розпорядку компанії.

4. За порушення ділової етики.

5. За нераціональне використання комп'ютерної техніки.

6. За правопорушення, скоєні в процесі своєї діяльності, встановлені чинним законодавством України.

7. За надання недостовірної інформації керівництву.

8. За недбале ставлення до ведення документації.

VI. Умови роботи:

1. Режим роботи користувача ПК визначається відповідно до Правил внутрішнього трудового розпорядку, встановленими в компанії.

2. Користувач ПК в зв'язку з виробничою необхідністю може виїжджати в службові (місцеві і регіональні) відрядження.

## Посадова інструкція заступника директора

I. Загальні положення

Заступник директора відноситься до категорії керівників, приймається на роботу і звільняється з неї наказом директора фірми.

На посаду заступника директора підприємства призначається особа, яка має вищу професійну (технічну або інженерно-економічну) освіту і стаж роботи на керівних посадах у відповідній профілю підприємства галузі не менше 5 років.

Заступник директора підпорядковується безпосередньо директору.

У своїй діяльності заступник директора керується:

1. нормативними документами з питань виконуваної роботи;

2. статутом підприємства;

3. правилами внутрішнього трудового розпорядку;

4. наказами та розпорядженнями Директора;

5. даною посадовою інструкцією.

Заступник директора повинен знати:

1. законодавчі та нормативні правові акти, що регламентують виробничо-господарську і фінансово-економічну діяльність фірми, постанови державних, регіональних та місцевих органів державної влади та управління, що визначають пріоритетні напрями розвитку економіки і відповідної галузі;

2. методичні та нормативні матеріали інших органів, що стосуються діяльності фірми;

3. профіль, спеціалізацію та особливості структури фірми;

4. перспективи технічного, економічного і соціального розвитку галузі і фірми;

5. виробничі потужності і кадрові ресурси фірми;

6. технологію виробництва продукції фірми;

**Посадова інструкція начальника служби безпеки**

I. Загальні положення

Начальник служби безпеки відноситься до категорії керівників.

На посаду начальника служби безпеки призначається особа, що має вищу професійну освіту і стаж роботи не менше 5 років.

Призначення на посаду начальника безпеки і звільняється з посади наказом директора підприємства.

Начальник служби безпеки в своїй діяльності керується:

1. Положенням про службу безпеки.

2. Справжньою посадовою інструкцією.

Начальник служби безпеки підпорядковується безпосередньо директору підприємства.

Начальник служби безпеки здійснює керівництво службою.

На час відсутності начальника служби безпеки (хвороба, відпустка, відрядження, пр.) Його обов'язки виконує заступник (за відсутності такого -

особа, призначена наказом директора підприємства), який набуває відповідних прав та несе відповідальність за належне виконання покладених на нього обов'язків.

II. Завдання та обов'язки Начальник служби безпеки:

1. Забезпечує надійний захист об'єктів організації від крадіжок, розкрадань і інших злочинних посягань, пожеж, аварій, актів вандалізму, стихійних лих, громадських заворушень і т.п.

2. Розробляє і здійснює керівництво заходами з безпеки об'єктів.

3. Виробляє адекватні загрозі засоби захисту і види режимів охорони.

4. Присікає спроби несанкціонованого проникнення на об'єкт, що охороняється.

5. Відображає загрозу і сприяє ліквідації шкідливих наслідків безпосереднього нападу на об'єкт, що охороняється.

6. Здійснює перевірку та оцінку лояльності службовців об'єкту, що охороняється.

7. Забезпечує недоторканність перевозяться матеріальних цінностей, відображаючи спроби несанкціонованого доступу до них.

8. Здійснює на об'єкті, що охороняється зв'язок з базовим органом служби охорони об'єкта, а під час перевезення - з транспортними та територіальними органами внутрішніх справ.

9. Досконало володіє прийомами рукопашного бою і самозахисту.

10. Володіє засобами індивідуального захисту, холодною та вогнепальною зброєю.

11. Користується різними видами зв'язку на охоронюваному об'єкті.

12. Виявляє і усуває нескладні технічні несправності в системах сигналізації і зв'язку, що охороняється.

13. Забезпечує дотримання суворого контрольно-пропускного режиму при здійсненні профілактичних, ремонтних і інших робіт.

14. Здійснює всебічну допомогу правоохоронним та іншим державним органам у розслідуванні випадків злочинних посягань на об'єкти, що

охороняються.

15. Надає невідкладну медичну допомогу при пораненнях, травмах і т.д.

III. Начальник служби безпеки має право

1. Знайомитися з проектами рішень керівництва підприємства, що стосуються діяльності служби безпеки.

2. Вносити на розгляд керівництва підприємства пропозиції щодо поліпшення діяльності служби безпеки.

3. Знайомитися з проектами рішень керівниками всіх (окремих) структурних підрозділів підприємства.

4. Запитувати у керівників структурних підрозділів та фахівців інформацію та документи, необхідні для виконання своїх посадових обов'язків.

5. Підписувати і візувати документи в межах своєї компетенції.

6. Вносити на розгляд керівництва підприємства подання про призначення, переміщення і звільнення співробітників служби безпеки; пропозиції про їх заохочення або про накладення на них стягнень.

7. Вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов'язків і прав.

Начальник служби безпеки несе відповідальність:

1. За неналежне виконання або невиконання своїх посадових обов'язків, передбачених цією посадовою інструкцією, - в межах, визначених чинним законодавством України.

2. За правопорушення, скоєні в процесі здійснення своєї діяльності - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

3. За завдання матеріальної шкоди - в межах, визначених чинним трудовим і цивільним законодавством України.

V. Начальник служби безпеки повинен знати

Закони та інші нормативно-правові акти України, що регламентують охоронну діяльність.

Специфіку і структуру організації.

Принципи організації охорони об'єктів організації.

Характеристики технічних засобів захисту об'єктів від несанкціонованого доступу до них.

Тактику захисту охоронюваних об'єктів від злочинних посягань.

Стратегію і тактику ведення переговорів зі злочинцями.

Сучасну вітчизняну і зарубіжну техніку (системи сигналізації, зв'язку і т.п.), підтримання її в експлуатаційному стані.

Характеристику технічних засобів захисту інформації від несанкціонованого доступу.

Призначення і види зв'язку.

Правила входження в зв'язок і правила поведінки в ефірі.

Загальні принципи надання першої медичної допомоги; правила і норми охорони праці, техніки безпеки і протипожежного захисту.

Правила прийому, супроводу і здачі товарно-матеріальних цінностей.

Правила супроводу окремих співробітників організації.

**Посадова інструкція ПК користувача**

I. Загальні положення

Посадова інструкція визначає посадові обов'язки, повноваження і відповідальність, а також умови роботи користувача ПК структурного підрозділу (далі Підрозділи).

користувача ПК призначається на посаду і звільняється з посади відповідно до чинного трудового законодавства наказом генерального директора компанії.

користувача ПК підпорядковується менеджеру відділу прямих продажів Підрозділу.

В період тимчасової відсутності користувача ПК його обов'язки виконує особа, призначена у встановленому порядку. Дана особа набуває відповідних прав і несе відповідальність за виконання зазначених обов'язків.

II. У своїй роботі керується і повинен знати:

1. Основи інформатики.

2. Програми MS Office, службові програми Підрозділу.

3. Зразки, форми, шаблони і стандарти документів, прийняті в компанії. Різновиди і структуру документів, методи, правила і особливості їх складання, оформлення.

4. Порядок систематизації інформації і складання бази даних.

5. Організацію і стандарти діловодства.

6. Основи ділового етикету, навички ведення ділових (в т.ч. телефонних) переговорів.

7. Правила користування оргтехнікою і ПК.

8. Правила внутрішнього трудового розпорядку.

9. Правила і норми охорони праці, техніки безпеки і протипожежного захисту.

10. Правила користування оргтехнікою і ПК.

11. Правила внутрішнього трудового розпорядку.

III. Посадові обов'язки:

1. Виконувати різні обчислювальні і графічні роботи, пов'язані з виробничою діяльністю, проводити набір тексту.

2. Реєструвати операції і зміни в базі Підрозділу.

3. Виписувати і відправляти факсом рахунку замовникам.

4. Передавати рахунки в бухгалтерію.

5. Редагувати агентську базу клієнтів в базі і роздруковувати необхідну інформацію менеджеру.

6. Перевіряти номери телефонів замовників по базі.

7. Відправляти і приймати гарантійні листи, прайси факсом.

8. Оформляти бланки і гарантійні листи, зміни.

9. Приймати дзвінки, що надходять в команду в разі відсутності менеджера.

10. Перевіряти інформацію, надану по базі менеджерами.

11. Роздруковувати документи необхідні в роботі менеджера (прайси, гарантійні листи, тексти оголошень).

Своєчасно виписувати накладні і рахунок-фактуру, а також відповідні податкове та екологічне законодавство;

1. порядок складання і узгодження бізнес-планів виробничо-господарської та фінансово-економічної діяльності фірми;

2. ринкові методи господарювання та управління фірми;

3. систему економічних індикаторів, що дозволяють підприємству визначати своє положення на ринку і розробляти програми виходу на нові ринки збуту;

4. порядок укладення та виконання господарських і фінансових договорів;

5. кон'юнктуру ринку;

6. науково-технічні досягнення і передовий досвід у відповідній галузі виробництв;

7. управління економікою і фінансами фірми;

8. організацію виробництва і праці;

9. порядок розробки та укладення галузевих тарифних угод, колективних договорів та регулювання соціально-трудових відносин;

10. трудове законодавство;

11. правила і норми охорони праці;

12. правила ділового спілкування;

13. правила і підходи роботи з клієнтами;

14. правила внутрішнього трудового розпорядку;

15. правила і норми пожежної безпеки.

На час відсутності заступника директора його обов'язки виконує призначений у встановленому порядку інший заступник директора, що несе повну відповідальність за належне виконання покладених на нього обов'язків.

II. Завдання та обов'язки

Право підпису ряду документів.

Організовує роботу і ефективну взаємодію всіх структурних підрозділів, цехів та виробничих одиниць, підвищує рентабельність фірми.

Розробляє і погоджує з директором фірми плани:

1. Розвитку виробництва на рік;

2. Бюджетування фірми (на квартал, рік).

Вирішує питання, що стосуються фінансово-економічної та виробничо-господарської діяльності фірми.

Доручає окреме ведення іншим посадовим особам - керівникам виробничих одиниць підприємств, функціональних і виробничих підрозділів.

Контролює роботу всіх структурних підрозділів фірми.

Організовує поточну організаційно-виконавчу роботу всієї фірми.

Забезпечує виконання фірмою всіх зобов'язань перед постачальниками, замовниками і кредиторами, включаючи установи банку, а також господарських і трудових договорів.

Затверджує штатний розклад фірми, встановлює посадові оклади та надбавки щокварталу або в міру необхідності.

Очолює організацію роботи у фірмі по стимулюванню персоналу.

Забезпечує дотримання економії матеріальних і трудових ресурсів.

Проводить роботи з удосконалення планування економічних і фінансових показників діяльності підприємства, по створенню й поліпшенню нормативів трудових витрат, витрачання товарно-матеріальних цінностей і використання виробничих потужностей.

Здійснює контроль за порядком обліку надходження і витрачання коштів, використанням матеріальних цінностей.

Забезпечує контроль за ходом дотримання фінансової дисципліни.

Контролює своєчасність подання звітності про результати економічної звітності про результат економічної діяльності в установленому порядку та терміни на розгляд директору.

III. Права

Заступник директора має право:

1. Діяти від імені підприємства за дорученням.

2. Представляти інтереси фірми у взаємовідносинах з громадянами, юридичними особами, органами державної влади та управління за дорученням

та розпорядженням директора.

3. Здійснювати перевірку діяльності всіх підрозділів підприємства в області економіки та організації виробництва, давати їм відповідні вказівки, спрямовані на підвищення його ефективності.

4. Вимагати від підрозділів підприємства представлення матеріалів, необхідних для виконання обов'язків, передбачених цим Положенням.

5. Представляти директору підприємства пропозиції про заохочення працівників усіх підрозділів за високі економічні показники роботи та притягнення до відповідальності за порушення встановлених вимог в області економіки та організації виробництва.

IV. Відповідальність

Заступник директора несе відповідальність за:

1. Невиконання (неналежне виконання) своїх посадових обов'язків, передбачених даною посадовою інструкцією, в межах, визначених чинним законодавством України.

2. Вчинені в процесі своєї діяльності правопорушення, - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

3. Завдання матеріальної шкоди - в межах, визначених чинним трудовим, кримінальним та цивільним законодавством України.

4. Розголошення комерційної таємної інформації.

5. Проведення без дозволу директора інтерв'ю, зустрічей, переговорів, що стосуються діяльності фірми.

6. Порушення вимог дисципліни відповідно до норм чинного трудового законодавства, за порушення внутрішнього трудового розпорядку в компанії.

## Висновки

В результаті виконання курсового проєкту було проведено розробку комплексної системи захисту інформації для туристичної фірми «… (назва фірми)». Відповідно було розроблено усю супровідну документацію по впровадженню КСЗІ.

Комплексна система захисту інформації (КСЗІ) – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації (ЗІ).

Організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) 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 Держспецзв’язку України.

В побудові КСЗІ можна виділити наступні етапи:

1. Обґрунтування необхідності створення КСЗІ.
2. Обстеження середовищ функціонування АС.
3. Визначення потенційних загроз інформації, що циркулюватиме в АС.
4. Розробка політики безпеки інформації в АС.
5. Розробка плану захисту інформації в АС.
6. Розробка технічного завдання на створення КСЗІ в АС.
7. Складання технороботочого проекту створення КСЗІ.
8. Підготовка КСЗІ до введення в дію.
9. Попередні випробування КСЗІ в АС.
10. Дослідна експлуатація КСЗІ.
11. Експертиза КСЗІ.
12. Супроводження КСЗІ.

## Список використаних джерел

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. 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;

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

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

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

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

23. 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.

**Додаток А**

**ТУРИСТИЧНА ФІРМА «… (НАЗВА ФІРМИ)»**
**НАКАЗ**
**03.03.2021 №03/03-1**
**Про затвердження Переліку відомостей, що відноситься до конфіденційної інформації ТФ «… (назва фірми)» 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 туристичній фірмі «… (назва фірми)» 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 (...(ПІБ)).
4. Контроль за нерозголошення інформації з грифом обмеженого доступу «Для службового користування» покласти на відповідального відділ безпеки (...(ПІБ)).
5. Контроль за виконанням цього наказу залишаю за собою.

Генеральний директор
туристичної фірми
«… (назва фірми)»
...(ПІБ)

**Перелік відомостей, що відноситься до конфіденційної інформації ТФ «… (назва фірми)» та якій надається грифи обмеження доступу «Конфіденційна інформація»**

Таблиця 1

| № | Інформація | Гриф обм.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 підприємства, політика безпеки підприємства | 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 «… (назва фірми)»» | конфіденційно |
| 9) | Відомості про співробітників компанії «… (назва фірми)» | конфіденційно |
| 10) | Відомості щодо обліку та видачі печаток, штампів та бланків | конфіденційно |
| 11) | Відомості про стан та ефективність роботи підприємства (фінансово-економічні положення компанії, бухгалтерські звіти) | конфіденційно |
| 12) | Відомості про процес, характер та умови укладення угод, договорів, контрактів з клієнтами | конфіденційно |
| 13) | Стратегічні плани маркетингового розвитку туристичної фірми | конфіденційно |
| 14) | Відомості про ділові переговори | конфіденційно |
| 15) | Відомості про кредити та банківські операції туристичної фірми | конфіденційно |
| 16) | Посадові інструкції для працівників ТФ «… (назва фірми)» | для службового користування |

**«ЗАТВЕРДЖУЮ»**
Генеральний директор
туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«03» березня 2021 року

**Акт**

**Визначення вищого ступень обмеження доступу інформації, яка циркулюватиме на об'єкті інформаційної діяльності – приміщення № 1 відділу безпеки туристичної фірми «… (назва фірми)»**

**Комісія в складі:**

**голови:** Генеральний директор туристичної фірми «… (назва фірми)» ...(ПІБ);

**члена:** відповідального за відділ безпеки туристичної фірми «… (назва фірми)» ...(ПІБ), заступник відповідального за відділ безпеки туристичної фірми «… (назва фірми)» ...(ПІБ).

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 об'єкті інформаційної діяльності (далі – ОІД) – приміщення № 1 відділу безпеки туристичної фірми «… (назва фірми)».

**Комісією встановлено**:

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

1. Інформація на паперових носіях інформації – «конфіденційно»;
2. Мовна інформація – без обмеження доступу.

**Висновок:**

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

**Голова комісії:**
Генеральний директор туристичної
фірми «… (назва фірми)»
...(ПІБ)

**Члени комісії:**
Відповідального за відділ безпеки
туристичної фірми «… (назва фірми)»
...(ПІБ)
Заступник відповідального за відділ безпеки
туристичної фірми «… (назва фірми)»
...(ПІБ)

**Додаток Б**

**«ЗАТВЕРДЖУЮ»**
Генеральний директор
туристичної фірми
«… (назва фірми)»
_____...(ПІБ)
«03» березня 2021 року

**АКТ**
**обстеження об'єкта інформаційної діяльності**

Обстеження на ОІД проведено комісією у складі:

**голови:** Генеральний директор туристичної фірми «… (назва фірми)» ...(ПІБ);

**члена:** відповідальний за відділ безпеки туристичної фірми «… (назва фірми)» ...(ПІБ), заступник відповідального за відділ безпеки туристичної фірми «… (назва фірми)» ...(ПІБ).

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 програмного забезпечення.

Комісія постановила:

1.1. В робочому приміщенні, де циркулює така інформація:

1.1.1. Мовна інформація (під час робочого часу) вголос та під час розмов між співробітниками цього підприємства. Гриф обмеження доступу – конфіденційно.

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

1.2. Відстань до меж контрольованої зони.

1.3. Підстанція електроживлення виходить за межи контрольованої зони.

1.4. Система заземлення - виходить за межі контрольованої зони.

1.5. Системи зв'язку виходять за межи контрольованої зони.

1.6. У наявності всі НД ТЗІ.

1.7. Програмне забезпечення потребує оновлення.

**Висновки:**

Стан захищеності інформація на ОІД не відповідає нормативним документам.

**Рекомендації:**

1) Розробити модель загроз для інформації з обмеженим доступом;
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 туристичної
фірми «… (назва фірми)» ...(ПІБ)

**Члени комісії:**

Відповідальний за відділ безпеки
туристичної фірми «… (назва фірми)» ...(ПІБ)

Заступник відповідального за відділ безпеки
туристичної фірми «… (назва фірми)» ...(ПІБ).

**Додаток В**

**«ЗАТВЕРДЖУЮ»**
Генеральний директор
туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«03» березня 2021 року

**МОДЕЛЬ ЗАГРОЗ**
**для інформації з обмеженим доступом, яка планується до циркуляції в автоматизованій системі класу 2 на об'єкті інформаційної діяльності – приміщення № 1 туристичної фірми«… (назва фірми)»**

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 автоматизованої системи (АС) класу 2 туристичної фірми «… (назва фірми)», 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 (ТЗІ), 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 автоматизованої

системи

Зовнішній контроль стану безпеки.

Схема ситуаційного плану наведена у додатку А. Туристична фірма «… (назва фірми)». Туристична фірма «… (назва фірми)» орендує 2 поверхи в торгівельно-розважальному центрі «Аркадія», по вулиці Борщагівська 154. Загальна площа магазину 200 кв.м. (по 100 кв.м. відповідно на кожному поверсі).

Контроль доступу на контрольовану зону торгівельно-розважального центру «Аркадія» здійснюється з використанням організаційних (контрольно-перепусний режим) для співробітників, що працюють на території центру та технічними (засобами фізичного захисту, системи відеоспостереження) заходами захисту для запобігання надзвичайних ситуацій.

Контроль доступу до туристичної фірми «… (назва фірми)» здійснюється з використанням технічних засобів (засоби фізичного захисту, системи відеоспостережння, система пожежної безпеки, система сигналізації, металеві решітки на вікнах та система електроно-механічного замка для доступу у технічне приміщення).

Централізована система зберігання і обробки даних.

Основними технічними засобами централізованої системи зберігання та обробки даних є:

– сервери (основні та резервні);
– зовнішня система зберігання даних;
– поштовий сервер.

Спеціалізоване програмне забезпечення.

Спеціалізоване програмне забезпечення, 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 баз даних, обліку і так далі знаходяться в головному сервері баз даних, 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 базами даних. На відміну від комп’ютерів, сервери завжди знаходяться у включенному стані. На випадок збоїв з електропостачанням в серверній встановлені джерела безперебійного живлення (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 (збереження, передавання, модифікація, приймання, відображення, друкування, накопичення) ІзОД в АС класу 2 з грифом обмеження «конфіденційно» та «для службового користування»;

– робота з паперовими документами, що мають гриф обмедення 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 об'єкті інформаційної діяльності – приміщення № 1 відділу безпеки туристичної фірми «… (назва фірми)» від 03 березня 2021 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 торгового підприємтсва складається з:

– приміщення яке складається з 5 кімнат (відділ по роботі з постачальниками та реклами, відділ безпеки, відділ планово-фінансовий, торговий зал на території якого ще знаходиться кабінет відповідального за торгову залу, відділ роботи з персоналом) та туалет (додаток А);
– 100 розеток під пристрої;
– 12 розеток під стаціонарний телефон;
– 6 принтер-сканер-ксерокс;
– 12 телефонів;
– 26 ПК;
– сервер з базами даних і сервер системи управління мережним обладнанням захисту – 4;
– 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 (арфівації), 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. 2.

Таблиця 2.

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. |

В приміщенні знаходяться таки типи технічних засобів (табл. 3)

Таблиця 3

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 |

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:

3. Акустичні – за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті двері, вікна, вентиляційні канали).

4. 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).

5. Оптико-електронні (лазерні канали) канали – за рахунок приймання та демодуляції відбитого від вібруючих під дією акустичного сигналу поверхонь приміщень (шибок, дзеркал тощо) випромінювання.

6. Акустоелектричні – за рахунок впливу звукових коливань на допоміжних технічних засобах і системах (ДТЗС) за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу та виникнення електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам, за рахунок «мікрофонного ефекту», за рахунок використання «високочастотного електромагнітного нав'язування»).

7. 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.

8. 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 (повені, землетруси, стихійні лиха тощо) 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 туристичної фірми. Потенційні загрози наведені в таблиці 4. Значення параметрів К, Ц, Д означають конфіденційність, цілісність, доступність.

Таблиця 4

Потенційні загрози

| Загрози | Порушення властивостей | | |
|---|---|---|---|
| | К | Ц | Д |
| Природні загрози | | | |
| Стихійні природні лиха (пожежа, землетрус, ожеледиця, снігопад, повінь, буревій, гроза), 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 порушення роботи системи, видалення даних, проблема у роботі програмного/апаратного забезпечення та їх компонентів) | | ▲ | ▲ |
| Випадкове пошкодження каналів зв’язку | | ▲ | ▲ |
| Ненавмисне виключення обладнання або зміна режимів роботи програм (випадкове виключення ПК, виключення електроживлення) | | ▲ | ▲ |
| Випадкова пошкодження носіїв інформації (зламати чи частково пошкодити флеш-накопичувачі, диски) | | ▲ | ▲ |
| Випадковий запуск програм, які при некомпетентній роботі завдадуть шкоду роботі системі (Випадкове форматування носіїв інформації, оновлення драйверів та операційної системи за допомогою завантажувальних дисків) | | ▲ | ▲ |
| Випадкове зараження вірусами при передачі даних | ▲ | ▲ | ▲ |
| Випадкове розголошення конфіденційної інформації 3-м лицям | ▲ | ▲ | ▲ |
| Розголошення, передача, втрата атрибутів доступу до системи (паролів, електронних карточок, ключів) | ▲ | ▲ | ▲ |
| Використання ПЗ, яке може нанести шкоду роботі системі (використання у роботі програм, яким потрібний великий обсяг операційної пам’яті) | ▲ | ▲ | ▲ |
| Халатне ставлення співробітниками до правил при роботі з системою (некомпетентність співробітників у роботі з системою) | ▲ | ▲ | ▲ |
| Навмисні загрози | | | |
| Фізичне спотворення системи (знищення приладів, носіїв інформації) | | ▲ | ▲ |
| Виключення чи припинення роботи систем функціонування (припинення роботи електроживлення, система охолодження, вентиляції , лінії зв’язку) | | ▲ | ▲ |
| Вербування співробітників (шантаж, підкуп) | ▲ | ▲ | ▲ |

| | | | |
|---|---|---|---|
| Викрадення носіїв інформації (флеш-накопичувачей, дисків, ПК) | ▲ | ▲ | ▲ |
| 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 (шкоди) 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 (такий, що очікується) рівень шкоди. Приклад цієї оцінки наведено також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока). Наявність таких оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної з властивостей захищеності інформації;

– Джерела загроз (зовнішні або внутрішні).

Потенційні загрози інформації об'єкта інформаційної діяльності наведені в табл. 5.

Таблиця 5

Модель загроз

| **Види загрози** | **Імовірність** | **Рівень шкоди** | **Джерела** |
|---|---|---|---|
| Природні загрози | | | |
| Стихійні природні лиха (пожежа, землетрус, ожеледиця, снігопад, повінь, буревій, гроза), 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 (випадкове порушення роботи системи, видалення даних, проблема у роботі програмного/апаратного забезпечення та їх компонентів) | Низька | Неприпустимо високий | Внутрішні |
| Ненавмисне виключення обладнання або зміна режимів роботи програм (випадкове виключення ПК, виключення електроживлення) | Висока | Середня | Внутрішні |
| Випадкова пошкодження носіїв інформації (зламати чи частково пошкодити флеш-накопичувачі, диски) | Низька | Низький | Внутрішні |
| Випадковий запуск програм, які при некомпетентній роботі завдадуть шкоду роботі системі (Випадкове форматування носіїв інформації, оновлення драйверів та операційної системи за допомогою завантажувальних дисків) | 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 (паролів, електронних карточок, ключів) | Низька | Середня | Внутрішні |
| Використання ПЗ, яке може нанести шкоду роботі системі (використання у роботі програм, яким потрібний великий обсяг операційної пам'яті) | Середня | Високий | Внутрішні |
| Халатне ставлення співробітниками до правил при роботі з системою (некомпетентність співробітників у роботі з системою) | Низька | Неприпустимо високий | Внутрішні |
| Випадкове пошкодження каналів зв'язку | Середня | Високий | Внутрішні |
| Навмисні загрози | | | |
| Фізичне спотворення системи (знищення приладів, носіїв інформації) | Середня | Неприпустимо високий | Внутрішні |
| Виключення чи припинення роботи систем функціонування (припинення роботи електроживлення, система охолодження, вентиляції , лінії зв'язку) | Середня | Високий | Зовнішні |
| Вербування співробітників (шантаж, підкуп) | Висока | Високий | Внутрішні , зовнішні |
| Викрадення носіїв інформації (флеш-накопичувачем, дисків, ПК) | Середня | Високий | Зовнішні |
| Несанкціоноване копіювання | Висока | Високий | Внутрішні |
| Розкрадання виробничих відходів (роздруківок, записів, записаних носіїв інформації) | 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 об'єктах інформаційної діяльності розглядаються суб'єкти, внаслідок навмисних або випадкових дій котрих, і (або) 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 (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

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 (інтересами, планами);

– 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. 6).

Таблиця. 6

Класифікація порушників за рівнем можливостей

| Рівні | Внутрішні загрози | Зовнішні загрози |
|---|---|---|
| I рівень – можливість ведення діалогу з АС, а саме можливість запуску прикладних програм операційної системи, що унеможливлює обробку інформації | - технічний персонал, який обслуговує будинки й приміщення (електрики, сантехніки, прибиральники тощо)<br>- особи, які входять до штату туристичної фірми «… (назва фірми)» але не мають допуску та доступу до обробки ІзОД на АС | - будь-які особи, які перебувають за межами АС |
| II рівень – можливість установки і запуску програм з новими функціями обробки інформації | - внутрішні: персонал, який обслуговує засоби обчислювальної техніки (інженери і техніки, які відповідають за технічний стан АС)<br>- користувачі АС | - відвідувачі (особи, які мають разові перепустки на територію) |
| III рівень – можливість управління функціонуванням АС, впливу на доступні масиви програмного забезпечення та інформації | - користувачі АС, які мають доступ до ІзОД в АС<br>- користувачі АС з адміністративними ролями | - представники організацій, які взаємодіють з питань технічного забезпечення, обслуговування, супровід техніки, яка входить до складу АС<br>- представники організацій, які взаємодіють з питань життєзабезпечення АС і ОІД в цілому |
| IV рівень – можливість повного доступу до ресурсів, проектування, реалізації, впровадження, супроводу програмно-апаратного забезпечення АС | 1. особи, які відповідають за захист ІзОД в АС | співробітники іноземних спецслужб, шпигуни від конкурентів |

Порушники за рівнем володіння інформацією про АС:

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

II рівень – мають високий рівень знань і досвідом роботи з технічними засобами автоматизованих системи і їх обслуговування.

III 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 автоматизованих системах.

Порушники за показниками можливості використання методів і способів отримання ІзОД і інформації про АС:

I рівень – використовують виключно агентурні методи отримання відомостей.

ІІ рівень – використовують пасивні технічні засоби перехоплення інформаційних сигналів.

ІІІ рівень – використовують виключно штатні засоби автоматизованих систем або недоліки проектування системи захисту інформації для реалізації несанкціонованого доступу до ІзОД.

IV рівень –застосовують методи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових чи внесення змін до штатних технічних засобів АС, впровадження і використання спеціального програмного забезпечення і т.п.).

Порушники за місцем вчинення дії:

І рівень – без отримання доступу на територію;

ІІ рівень – з отриманням доступу на територію;

ІІІ рівень – з отриманням доступу до АС;

IV рівень – з отриманням доступу до масивів (носіїв) накопичення і зберігання ІзОД;

V рівень – отримання доступу до КСЗІ АС.

Порушники за часом дії:

І рівень – до впровадження АС або її окремих компонентів;

ІІ рівень – під час бездіяльності компонентів АС (в неробочий час, планових та не планових перерв);

ІІІ рівень – під час функціонування АС;

IV рівень – як під час функціонування, так і під час зупинки в роботі АС.

Порушники за мотивами вчинення порушення:

І рівень – безвідповідальність;

ІІ рівень – самозатвердження;

ІІІ рівень – корисливі інтереси;

IV рівень – професійний обов’язок.

Генеральний директор
ТФ «… (назва фірми)» ...(ПІБ)

Відповідальний за відділ
безпеки ТФ «… (назва фірми)» ...(ПІБ)

**Додаток Г**

**«ЗАТВЕРДЖУЮ»**
Генеральний директор
туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«03» березня 2021 року

**Політика безпеки інформації, яка циркулює в АС класу 2 туристичної фірми «… (назва фірми)»**

**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 (дані щодо персональних ідентифікаторів та паролів користувачів, їхніх повноважень та прав доступу до об'єктів, встановлених робочих параметрів окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);
- 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 (наприклад, дисковий простір, тривалість сеансу користувача із засобами АС, час використання центрального процесора і т. ін.), 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 – служба захисту інформації, якому надаються повноваження щодо організації та впровадження прийнятої політики безпеки в АС.

Всі працівники туристичної фірми «… (назва фірми)», 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 комплексною системою захисту інформації**

Реалізація політики безпеки здійснюється за допомогою комплексної системи захисту інформації 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-правоових та організаційних заходів і інженерно-технічних засобів щодо захисту інформації від НСД.

Нормативно-правові заходи захисту інформації

Комплекс нормативно-правових заходів захисту інформації АС:

– створення системи документів нормативно-правового забезпечення робіт з захисту інформації в АС;

– 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;

– доведення до персоналу і користувачів АС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;

– 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:

– застосування режимних заходів на ОІД;

– забезпечення фізичного захисту обладнання АС, носіїв інформації, інших ресурсів;

– організацію проведення обстеження середовищ функціонування АС;

– виконання робіт з захисту інформації та взаємодії з цих питань з іншими суб’єктами системи ТЗІ в Україні;

– регламентацію доступу користувачів і персоналу до ресурсів АС;

– 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:

– розмежування доступу користувачів до інформації та інших ресурсів АС;

– блокування несанкціонованих дій з інформацією та іншими ресурсами АС, локалізації цих дій по відношенню до ресурсів та ліквідації їх наслідків;

– забезпечення контролю та захисту потоків інформації, яка обробляється в АС;

– 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;

– підтримання цілісності критичних ресурсів системи захисту, середовища виконання прикладних програм та інформації в ПТК;

– забезпечення контролю за цілісністю об'єктів, що підлягають захисту;

– організації обліку, зберігання та обігу матеріальних носіїв інформації;

– 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 машинних носіїв інформації (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 операційних систем і функціональних програм;

– облік, видачу, використання і зберігання МНІ, що містять еталонні і резервні копії операційних систем і функціональних програм;

– контроль цілісності системного програмного забезпечення;

– контроль цілісності КЗЗ АС туристичної фірми «… (назва фірми)».

– Організаційні заходи антивірусного захисту інформації в АС туристичної фірми «… (назва фірми)» повинні передбачати:

– використання ліцензійного антивірусного програмного забезпечення 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 (встановлення заборони) користувачеві прав читати або модифікувати об'єкт.

КЗЗ повинен надавати можливість адміністратору системи та адміністратору безпеки (відповідно до своїх повноважень) для кожного захищеного об'єкта визначити конкретних користувачів (групи користувачів), які мають право читати або модифікувати об'єкт.

КЗЗ повинен здійснювати розмежування доступу до слабозв’язаних об’єктів на підставі імені користувача (групи користувачів) 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 базами даних повинно здійснюватися за допомогою надання адміністратором БД користувачеві певної ролі.

Запити на зміну прав доступу (надання прав доступу, внесення користувача до певної групи або надання певної ролі) повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора системи, адміністратора безпеки, адміністратора баз даних (СКБД).

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 (право на запуск певного ПК надається відповідно до його функціональних обов'язків).

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

Адміністратори мають право працювати (створювати, модифікувати, вилучати, друкувати та копіювати на МНІ) 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 програмного забезпечення (право на запуск певного ПК надається відповідно до його функціональних обов'язків).

Вимоги до правил адміністрування КЗЗ і реєстрації дій користувачів

Щодо реєстрації дій користувачів КЗЗ повинен забезпечити реалізацію наступних функцій (реєстрацію наступних подій, що мають відношення до безпеки):

- реєстрація користувача в системі (вхід/вихід до/з системи);
- зміна паролю користувачем ;
- зміна прав та повноважень доступу до файлів та ресурсів;
- створення, доступ та знищення файлів;
- 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 (електроживлення, заземлення, пожежної та охоронної сигналізації), комунікацій і зв'язку (телефон, факс);
– проектна та експлуатаційна документація на компоненти фізичного середовища.

Територія фізичного середовища

Територія, яка знаходиться під цілодобовою охороною.

Будівля, де розгорнута АС

Доступ працівників туристичної фірми «… (назва фірми)» в будівлю здійснюється за перепустками. Доступ сторонніх осіб в будівлю контролюється черговим відповідного підрозділу і здійснюється за узгодженням керівника туристичної фірми»… (назва фірми)». 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 (у відповідності до вимог «Тимчасового положення про категоріювання об'єктів» ДСТСЗІ від 10.07.95 за № 35).

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 туристичної фірми «… (назва фірми)».

Відповідальний за відділ
безпеки туристичної фірми ...(ПІБ)
«… (назва фірми)»

**Додаток Д**

**«ЗАТВЕРДЖУЮ»**
Генеральний директор
туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«03» березня 2021 року

АВТОМАТИЗОВАНА СИСТЕМА ВІДДІЛУ БЕЗПЕКИ
Туристичної фірми «… (назва фірми)»

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

**ПЛАН ЗАХИСТУ НА КСЗІ**

Чернігів-2021

1. ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСВБ

1.1 Загальні положення

План захисту інформації в АСВБ (далі - План захисту), визначає політику туристичної фірми «… (назва фірми)» 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 політики безпеки інформації, 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 (цілісності, доступності, конфіденційності) 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 інформації з обмеженим доступом, обробка яких здійснюється в АСВБ і які можуть знаходитись на паперових, магнітних та інших носіях;

– інформаційні масиви та бази даних, програмне забезпечення, 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 (персонал) АСВБ та власники інформації.

– 1.4 Шляхи забезпечення безпеки інформації

– Забезпечення безпеки інформації в АСВБ досягається:

– організацією та впровадженням системи допуску посадових осіб (користувачів) 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 комплексної системи захисту інформації.

2. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В АСВБ

2.1 Склад інформації в АСВБ

АСВБ призначена для роботи з інформацією з обмеженим доступом, яка представлена у вигляді текстових документів, електронних таблиць.

До інформації АСВБ відносяться також загальне, функціональне та спеціальне програмне забезпечення 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 інформацію з обмеженим доступом. ІзОД, яка обробляється в АСВБ, є власністю туристичної фірми»… (назва фірми)», і поділяється на такі категорії:

– конфіденційна інформація;
– ДСК.

В АСВБ до інформації з обмеженим доступом відноситься інформація, яка включена до «Переліку відомостей, що відноситься до конфіденційної інформації ТФ «… (назва фірми)» та якій надається грифи обмеження доступу «Для службового користування» та «Конфіденційна інформація».

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

2.3 Класифікація інформації за типом представлення в АСВБ

У таблиці 7 для кожної з визначених категорій інформації вказано тип її логічного та фізичного представлення.

Таблиця 7

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) |

3. ОПИС КОМПОНЕНТІВ АСВБ ТА ТЕХНОЛОГІЇ ОБРОКИ ІНФОРМАЦІЇ

3.1 Компоненти АСВБ

До компонентів АСВБ відносяться такі:

- технічне забезпечення (ПЕОМ та технічні засоби захисту);
- програмне забезпечення;
- дані;
- користувачі АСВБ;
- технічний персонал.

3.1.1 Технічне забезпечення

АСВБ побудовано на базі одного автономного комп'ютера.

Склад технічних засобів АСВБ наведено в Паспорті формулярі АСВБ.

3.1.2 Програмне забезпечення

Програмне забезпечення АСВБ поділяється на загальне, функціональне та спеціальне.

Перелік програмного забезпечення 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:
- Технічне завдання;
- Інструкція користувача АС 2;
- Інструкція з адміністрування системи;
- Технічна документація на систему захисту інформації;
- Паспорт-формуляр на АСВБ;
- Облікові картки користувачів АСВБ;
- Положення про службу захисту інформації;
- 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 (адміністратор документів);
- системний адміністратор.

Облікова картка користувача містить такі реквізити:

- ім'я користувача в АСВБ;
- прізвище та ініціали, підрозділ;
- посада користувача;
- рівень допуску (найвищий гриф секретності інформації, з якою дозволено працювати користувачеві);
- роль користувача в системі (або декілька ролей у випадку суміщення адміністративних ролей);

Для кожного користувача, що буде працювати в АСВБ, заповнюється одна або декілька

облікових карток – у залежності від ролей, які він виконує в системі. Кожна облікова картка відповідає обліковому запису користувача в базі даних 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(ів) та звичайного користувача, заповнюються щонайменше дві облікові картки (одна картка для ролі «звичайний користувач» та хоча б одна картка для адміністративних ролей) 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 таблиці 8. Оскільки програмні засоби, як активні об’єкти, не мають своїх атрибутів доступу, у цій таблиці вони розглядаються тільки як пасивні об’єкти.

Таблиця 8

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;<br>2. Програмні засоби: загальне, функціональне та спеціальне ПЗ;<br>3. Дані: дані захисту, резервні копії, облікові картки користувачів, проектні та експлуатаційні документи на АСВБ. |
| 2 | Системний адміністратор | 1. Технічні засоби: комп’ютер;<br>2. Програмні засоби: загальне та функціональне ПЗ, програмні засоби захисту;<br>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;<br>2. Програмні засоби: загальне, функціональне та спеціальне ПЗ;<br>3. Дані: текстові документи та електронні таблиці, експлуатаційні документи на АСВБ. |
| 4 | Звичайний користувач | 1. Технічні засоби: комп’ютер;<br>2. Програмні засоби: загальне, функціональне та спеціальне ПЗ;<br>3. Дані: текстові документи та електронні таблиці, експлуатаційні документи на АСВБ |
| 5 | Персонал (продаці-консультанти) | 1. Технічні засоби: комп’ютер;<br>2. Програмні засоби: загальне та функціональне ПЗ;<br>3. Дані: експлуатаційна документація на технічні засоби. |

3.2 Технологія обробки інформації

3.2.1 Організація роботи з інформацією обмеженого доступу

Звичайні користувачі працюють у системі з документами, які містять інформацію з обмеженим доступом.

Інформація з обмеженим доступом зберігається на жорсткому магнітному диску АСВБ та на змінних носіях інформації (дискети, флеш накопичувачі).

Змінні носії інформації з ІзОД зберігаються в спеціальному відділі у металевому сейфі

та доступ до них регламентується розпорядчими документами ТФ «… (назва фірми)».

Друк та експорт інформації з обмеженим доступом відбувається відповідно розпорядчих документів ТФ «… (назва фірми)».

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 інформації з обмеженим доступом в АСВБ та належного функціонування комплексної системи захисту інформації створюється служба захисту інформації.

Склад та функції служби захисту інформації в АСВБ визначаються відповідно до документа «Положення про службу захисту інформації».

Повноваження користувачів встановлюються керівництвом ТФ «… (назва фірми)» 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 ТФ «… (назва фірми)».

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 ТФ «… (назва фірми)»., 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 (дискет, флеш накопичувачів);
- 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 службу захисту інформації в АСВБ відповідно адміністративних ролей в АСВБ покладаються наступні основні функції:

Заступник відповідального за безпеку:

- ведення облікових карток користувачів;

– ведення бази даних захисту;
– настройка 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 програмного забезпечення, у тому числі програмного забезпечення КЗЗ;
– супроводження апаратного забезпечення (разом із технічним персоналом).

Усі дії, які прямо чи опосередковано можуть вплинути на захищеність інформації (зміни дозволів на доступ до файлів та папок, очищення журналів операційної системи, зміни настройок BIOS Setup тощо), 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 (видалення) користувачів в(з) АСВБ та змін їхніх повноважень.

На підставі облікової картки заступника відповідального за безпеку вводить у базу даних 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 бази даних захисту та ознайомлює з ними користувача.

При необхідності видалення користувача з АСВБ (при звільненні з роботи, при зміні посадових обов'язків та ін.) 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 (у тому числі атрибути доступу), має можливість змінювати стан системи та значення параметрів конфігурації системи та ін. Адміністратор безпеки встановлює пароль на доступ до апаратних налаштувань комп'ютерів (Bios Setup Supervisor Password).

Системний адміністратор здійснює супроводження програмного та апаратного забезпечення. 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 ТФ «… (назва фірми)».

Охорону контрольованої зони та перепускний режим до будівлі, точніше до торгово-розважального центру «Аркадія», де розташовано ТФ «… (назва фірми)» з АСВБ здійснює відомча охорона «…(ОХОРОННА ФІРМА)».

В неробочий час приміщення з АСВБ опечатується та здається під охорону службі охорони «…(ОХОРОННА ФІРМА)».

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 інформації з обмеженим

доступом, 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 технічного захисту інформації, який забезпечує блокування наступних технічних каналів витоку інформації:

– каналів побічних електромагнітних випромінювань і наводок (ПЕМВН);
– радіотехнічний канал;
– візуально-оптичний.

Роботи по створенню комплексу безпеки проведені власними силами туристичної фірми»… (назва фірми)».

Відповідальний за захист інформації в АСВБ організовує та координує роботи із ТЗІ, як планові (відповідно до вимог Акту атестації КТЗІ), 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 служби захисту інформації в АСВБ. Після проведення необхідних заходів з ТЗІ представниками служби захисту інформації в АСВБ вносяться відповідні записи про зміні у складі АСВБ в Паспорті-формулярі на АСВБ.

7.2 Модернізація програмного забезпечення

Модернізація програмного забезпечення проводиться в разі необхідності (наприклад, у випадку надання розробниками сервісних пакетів, появи нових версій тощо). Поновлення всього програмного забезпечення 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 технічним завданням або додатком до основного технічного завдання.

8. ПОРЯДОК ПРОВЕДЕННЯ ВІДНОВЛЮВАЛЬНИХ РОБІТ І ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОГО ФУНКЦІОНУВАННЯ АСВБ

У разі виникнення проблем у роботі технічного та програмного забезпечення 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 програмного забезпечення АСВБ проводиться під час перебування системи в стані поновлення програмного забезпечення, відновлення КЗЗ – під час перебування системи в стані відновлення.

При проведенні відновлення програмного забезпечення за необхідності використовуються відповідні дистрибутиви. Відновлення операційної системи 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 інформації з обмеженим доступом дозволяється тільки після отримання атестата відповідності КСЗІ вимогам нормативних документів із питань захисту інформації.

Дозвіл на обробку інформації з обмеженим доступом за допомогою АСВБ дається наказом генерального диектора туристичної фірми «… (назва фірми)».

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 (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).

Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 квітня 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;

ТФКО-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 систему захисту інформації ЛОЗА-1;

Технічне завдання 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

| № п/п | Назва заходу | Термін | Примітка |
|---|---|---|---|
| Організаційні заходи | | | |
| 1 | Розробка документів (інструкцій, правил, розпоряджень тощо) 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 | |
| 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 туристичної фірми ...(ПІБ)
«… (назва фірми)»

**Додаток Е**

**«ЗАТВЕРДЖЕНО»**
Відповідальний за відділ
безпеки туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«17» березня 2021 року

**АВТОМАТИЗОВАНА СИСТЕМА ВІДДІЛУ БЕЗПЕКИ**
**туристичної фірми «… (назва фірми)»**
**(шифр – «АСВБ»)**

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

**ТЕХНІЧНЕ ЗАВДАННЯ**

Чернігів-2021

1. ЗАГАЛЬНІ ВІДОМОСТІ

1.1. Повна назва системи та її умовне позначення

Повна назва: Комплексна система захисту інформації автоматизованої системи відділу безпеки туристичної фірми «… (назва фірми)».

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 «… (назва фірми)» та «…(ОХОРОНННА ФІРМА)» відповідно вимог Договору від 17.12.15 № 1АС/245 (далі - Договір).

1.3. Замовник

Відкрите акціонерне товариство ТФ «… (назва фірми)»

Чернігів, вул. Борщагівська 154.

1.4. Виконавець

Підприємство «…(охороннна фірма)»

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 ТФ «… (назва фірми)».

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. Автоматизированные системы. 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;

9. реєстрацію даних про події, що відбуваються в системі і мають відношення до безпеки інформації;

10. підтримку цілісності середовища виконання прикладних програм та ІзОД, що повинна оброблятися в АСВБ;

11. виявлення уразливостей в ОС;

12. захист від атак порушників безпеки;

13. захист від проникнення і поширення комп’ютерних вірусів;

14. захист інформації під час передачі телекомунікаційним середовищем;

15. контроль за функціонуванням КСЗІ.

16. виявлення загроз безпеці інформації, що передається, обробляється та зберігається в АСВБ;

17. унеможливлення реалізації загроз для інформації, порушення її конфіденційності, цілісності та доступності в АСВБ.

КСЗІ АСВБ повинна передбачати:

18. організаційні, правові заходи діяльності користувачів АСВБ;

19. адміністративні заходи обмеження фізичного доступу до обробки інформації;

20. технічні заходи і програмно-апаратні засоби захисту від НСД;

21. захист інформації, що обробляється в АСВБ від витоку технічними каналами.

2.2. Функціональне призначення і особливості застосування КСЗІ АСВБ

КСЗІ АСВБ призначена для:

22. забезпечення виконання визначеної для АСВБ ПБ інформації;

23. реєстрації спроб реалізації загроз інформації та сповіщення адміністраторів безпеки про факти несанкціонованих дій з ІзОД;

24. контролю за діями користувачів АСВБ та реєстрації подій, які мають відношення до безпеки інформації;

25. підтримання цілісності , конфіденційності, доступності ІзОД АСВБ;

26. блокування несанкціонованих дій з ІзОД;

27. організації обліку, зберігання та обігу матеріальних носіїв інформації, які використовуються в АСВБ;

28. контролю за функціонуванням КСЗІ;

29. захисту ІзОД від її витоку технічними каналами на НСД доступу.

30. Під час проектування КСЗІ АСВБ необхідно забезпечити:

31. ефективний рівень захисту ІзОД, яка циркулюватиме в АСВБ;

32. економічну доцільність прийнятих рішень;

33. 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 (конфігурація апаратних засобів операційної системи і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) 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:

1. 21 системних блоків;
2. 21 моніторів;
3. 21 графічні маніпулятори типу «миша»;
4. 21 клавіатур;
5. 21 принтерів.

3.1.3. Програмне забезпечення АСВБ

До складу АСВБ входить наступне програмне забезпечення:

6. операційна система Windows 7;
7. пакет прикладних програм Microsoft Office 2010;
8. АС баз даних;

9. драйвери системних пристроїв;

10. антивірусна програма ESET Smart Security.

Інше програмне забезпечення:

11. система захисту інформації від НСД «Захист».

12. 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 ТФ «… (назва фірми)», що знаходиться в межах КЗ ТФ «… (назва фірми)». Охорона ТФ «… (назва фірми)», здійснюється цілодобово відомчою охороною підприємства «Urban». 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 роботоздатності АСВБ;

– режим технічного обслуговування АСВБ.

3.7. Можливі загрози інформації

3.7.1. Класифікація загроз

Наведена у Політики безпеки, додаток Е.

3.7.2. Модель порушника

Представлена в Моделі загроз для ІзОД, яка планується до циркуляції в автоматизованій системі класу 2 на ОІД - приміщення ТФ «… (назва фірми)», додаток Д.

3.7.3. Модель загроз

Наведена в Моделі загроз для ІзОД, яка планується до циркуляції в автоматизованій системі класу 2 на ОІД – приміщення ТФ «… (назва фірми)» додаток Д.

4. ВИМОГИ ДО КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1. Вимоги щодо організаційного забезпечення захисту

4.1.1. З метою забезпечення захисту ІзОД під час її обробки в АСВБ наказом генерального директора ТФ «… (назва фірми)» створюється служба захисту інформації в АСВБ, якій надаються повноваження щодо організації і впровадження КСЗІ, контролю за станом захищеності інформації тощо. У своїй діяльності служба захисту інформації керується документом «Положення про службу захисту інформації».

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 операційною системою Windows 7, 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 базах.

Системний адміністратор АСВБ повинен забезпечувати:

– безперебійну роботу операційної системи АСВБ;
– справну роботу системних драйверів;
– встановлення необхідного програмного забезпечення та своєчасне його оновлення;
– своєчасне оновлення баз антивірусного програмного забезпечення.

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

Усі дії, які прямо чи опосередковано можуть вплинути на захищеність інформації (зміни дозволів на доступ до файлів та папок, очищення журналів ОС, зміни настройок BIOS Setup тощо), 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 ТФ «… (назва фірми)»

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, комплекс засобів захисту (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 (відповідні вимоги наведені в документі НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу).

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 (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об’єкта (ініціювати процес). 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 або 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 (тимчасових файлів, файлів, в яких зберігаються бази документів, документи, резервні копії журналу захисту, та, можливо, інші об’єкти доступу) програмні засоби системи повинні використовувати процедуру безповоротного видалення.

В АСВБ необхідно використовувати Windows 7, 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 (на рівні розподілу потоків інформації між групами користувачів). 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 (процесів).

КЗЗ повинен здійснювати керування доступом до баз документів та документів на підставі атрибутів доступу користувача і документа згідно з правилами розмежування доступу, наведеними у пп. 4.3.7.1 та 4.3.7.2.

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 (процесів).

КЗЗ повинен реалізовувати правила розмежування доступу до даних захисту, наведені в п. 4.3.7.3.

4.2.5.3. Доступ до програмних засобів

КЗЗ повинен надавати доступ до процесів (файлів, що виконуються), за допомогою яких здійснюється обробка ІзОД, тільки користувачам АСВБ.

КЗЗ повинен надавати доступ до процесів (файлів, що виконуються), за допомогою яких здійснюється ведення бази даних захисту та перегляд журналу захисту, тільки адміністратору безпеки та системному адміністратору (можливість запуску процесу не означає можливості доступу до даних, для обробки яких призначений процес).

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 (збійних ситуацій), 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 (після усунення причин помилки);
- 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, 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 (друк та копіювання на знімні носії).

Усі записи про події мають містити інформацію про дату, час і тип (у тому числі успішність чи неуспішність) події, а для подій аудита (відстеження дій користувачів) - 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, викладеними в п. 4.3.7.3.

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.

Функції для кожної з визначених в АСВБ ролей наведені в пп. 4.1.3

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 аутентифікований 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 (тобто файли, що виконуються);
– 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 (в залежності від конфігурації КЗЗ, яку визначає адміністратор): завершити роботу операційної системи 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 операційної системи 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 (exe-, com-, bat-файлів тощо), 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 (у залежності від конфігурації КЗЗ, яку визначає адміністратор): завершити роботу операційної системи 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 (перелік користувачів із наданими їм правами доступу до бази);

– список аудита.

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

Документи (текстові документи, електронні таблиці).

Кожний документ має такі атрибути:

– назва;

– ключові слова та вирази;

– час створення;

– час останнього коригування;

– власник;

– рівень доступу;

– список доступу (перелік користувачів із наданими їм правами доступу до документа);

– список аудита.

Дані захисту:

– база даних захисту (перелік користувачів із їхніми атрибутами доступу та даними, необхідними для автентифікації);

– журнал захисту;

– параметри конфігурації системи;

– оперативні дані про роботу системи.

Програмні засоби КЗЗ.

Інші програмні засоби (загальне, функціональне і спеціальне ПЗ та службові дані, необхідні для його роботи).

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 (жорсткий диск, дисководи для змінних дисків, принтери), у тому числі засоби захисту.

У таблиці 9 перелічені об’єкти доступу та вказані носії, на яких вони зберігаються.

Таблиця 9

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 (у тому числі програмні засоби КЗЗ);
– 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 (наприклад, за допомогою стандартних файлових менеджерів) до файлів, в яких зберігаються бази документів, документи, база даних захисту та журнал захисту.

Користувачі повинні мати можливість працювати з базами документів, документами, базою даних захисту та журналом захисту тільки за допомогою призначеного для цього процесу (процесів).

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 (файлів), 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 (див. п. 4.2.9) з наданими їм видами доступу.

4.3.5. Атрибути доступу користувачів

До атрибутів доступу користувачів належать такі дані:
– роль;
– рівень допуску.

Ролі користувачів та правила їх суміщення описані в п.4.2.9.

Рівень допуску користувача визначає найвищий ступінь секретності інформації, із якою йому дозволено працювати, і обирається з переліку, наведеного в п. 4.3.4.

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 (тобто користувач або група не вказані в переліку заборон з відповідним видом доступу);
– в списку доступу бази йому або групі, до якої він належить, надано цей доступ (тобто користувач або група вказані в переліку дозволів з відповідним видом доступу).

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 (тобто користувач або група не вказані в переліку заборон з відповідним видом доступу);
– в списку доступу документа йому або групі, до якої він належить, надано цей
– доступ (тобто користувач або група вказані в переліку дозволів з відповідним видом доступу).

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 базу даних 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 (поза машинні документи), 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 (у тому числі ті, що стосуються програмних засобів КЗЗ), проводяться за узгодженням з адміністратором безпеки. Порядок узгодження повинен визначатись документом «Планом захисту інформації».

Повсякденні обов'язки щодо адміністрування (відстеження потенційно небезпечних подій, усунення збійних ситуацій тощо) 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 (див. перелік подій у п. 4.2.6).

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 об'єкті інформаційної діяльності (приміщенні № 3), де встановлена вказана автоматизована система, комплексу технічного захисту інформації, який є невід'ємною складовою КСЗІ АСВБ.

КТЗІ на ОІД необхідно створювати відповідно вимог нормативних документів, перелік яких наведено в п. 2.3 цього Технічного завдання.

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.

Роботи повинні проводитись відповідно до нормативно-правових актів та нормативних документів з питань ТЗІ, перелік яких наведено в п. 2.3.

Для захисту ІзОД від витоку технічними каналами повинні використовуватися пасивні засоби ТЗІ згідно із Переліком засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України.

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. Вказані пристрої встановлюються відповідно вимог своєї технічної документації на максимально можливі відстані від АСВБ. Технічні характеристики стосовно їх потужності повинні відповідати потужності споживання технічних засобів підключених до них;

– 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. У разі неможливості видалення вказаних ліній та комунікацій, провести їх екранування. Екрани повинні буди підключені до контуру заземлення;

– 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:

1. унеможливлення організаційними та інженерно-технічними заходами несанкціонованого проникнення на ОІД сторонніх осіб з метою встановлення пристроїв технічної розвідки (відеопередавачів);

2. встановлення на ОІД лише технічних засобів, які пройшли спеціальну перевірку на предмет наявності в них приховано встановлених пристроїв технічної розвідки;

3. унеможливлення встановлення на лінійно-кабельні комунікації, комунікації життєзабезпечення, які виходять за межі ОІД пристроїв технічної розвідки;

4. перевірки приміщення ОІД, лінійно-кабельних комунікацій, комунікацій життєзабезпечення, які виходять за межі ОІД, на наявність приховано встановлених пристроїв технічної розвідки (відеопередавачів);

5. 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 розділі 3 цього 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:

1. функціонування в автоматичному режимі;
2. блокування проникнення комп'ютерних вірусів зі змінних носіїв;
3. несанкціонованого розповсюджуваних виконавчих файлів;
4. лікування (або видалення) комп'ютерних вірусів з занесенням інформації про це у відповідні протоколи КЗЗ;
5. автоматичне оновлення антивірусного ПЗ;
6. 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:

– Автоматизована система відділу безпеки ТФ «… (назва фірми)».
– Комплексна система захисту інформації. План захисту інформації;
– Комплексна система захисту інформації. 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 таблиці 10.

Таблиця 10

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 | … |
| 2. | Проведення заходів щодо захисту інформації від витоку технічними каналами | … |
| 3. | Проведення заходів щодо захисту інформації від НСД | … |
| 4. | Розробка експлуатаційної документації на КСЗІ | … |
| 5. | Розробка «Програми та методики випробувань» | … |
| 6. | Розробка експлуатаційних документів КСЗІ | … |
| 7 | Проведення попередніх випробувань і передача КСЗІ в дослідну експлуатацію | … |
| 8. | Навчання користувачів | … |

| | | |
|---|---|---|
| 9. | Дослідна експлуатація | … |
| 10. | Підготовка комплекту документів для проведення експертизи КСЗІ | … |

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 технічного завдання 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
ТФ «… (назва фірми)» ...(ПІБ)

**Додаток Є**

**«ЗАТВЕРДЖЕНО»**
Відповідальний за відділ
безпеки туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«17» березня 2021 року

**АВТОМАТИЗОВАНА СИСТЕМА ВІДДІЛУ БЕЗПЕКИ ТФ «… (назва фірми)»**
**(шифр - «АСВБ»)**

**КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ (шифр - КСЗІ «АСВБ»)**

**ТЕХНОРОБОЧИЙ ПРОЕКТ**

Чернігів-2021

1. ВІДОМІСТЬ ПРОЕКТНОЇ ДОКУМЕНТАЦІЇ ДО ТЕХНОРОБОЧОГО ПРОЕКТУ КСЗІ В АСВБ

Таблиця 11

Відомість проектної документації до Техноробочого проекту

| № п/п | Найменування | Кіл-ть арк. |
|---|---|---|
| 1. | Перелік відомостей, що відносяться до конфіденційної інформації ТФ «… (назва фірми)» та якій надається гриф обмеження доступу | 2 |
| 2. | Акт визначення вищого ступеню обмеження доступу інформації, яка циркулюватиме на об'єкті інформаційної діяльності відділу безпеки ТФ «… (назва фірми)» | 1 |
| 3. | Акт обстеження середовищ функціонування автоматизованої системи на об'єкті інформаційної діяльності відділу безпеки ТФ «… (назва фірми)». | 1 |
| 4. | Модель загроз для інформації, яка планується до циркуляції в автоматизованій системі класу 2 на об'єкті інформаційної діяльності ТФ «… (назва фірми)» | 15 |
| 5. | Політика безпеки інформації, яка циркулює в автоматизованій системі класу 2 ТФ «… (назва фірми)» | 6 |
| 6. | План захисту інформації | 14 |
| 7. | Автоматизована система відділу безпеки ТФ «… (назва фірми)». Комплексна система захисту інформації. Технічне завдання | 17 |

2. ВІДОМІСТЬ ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ ДО ТЕХНОРОБОЧОГО ПРОЕКТУ КСЗІ ЗІ

Таблиця 14 «Відомість експлуатаційної документації»

| № п\п | Найменування | Кіл-ть арк. |
|---|---|---|
| 1. | Паспорт-формуляр на автоматизовану систему класу 2 відділу безпеки ТФ «… (назва фірми)» | 4 |

3. ПОЯСНЮВАЛЬНА ЗАПИСКА ДО ТЕХНОРОБОЧОГО ПРОЕКТУ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЛАСУ 2 ВІДДІЛУ БЕЗПЕКИ ТФ «… (назва фірми)»

3.2. Загальні відомості

Повна назва: Комплексна система захисту в автоматизованій системі класу 2 об'єкту інформаційної діяльності - приміщення відділу безпеки ТФ «… (назва фірми)».

Розробка КСЗІ в АСВБ є складовою частиною робіт з впровадження АСВБ в діяльність, що виконуються між ТФ «… (назва фірми)» та «…(ОХОРОННА ФІРМА)»

Замовник: ТФ «… (назва фірми)».

Виконавець: «…(ОХОРОННА ФІРМА)»

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

Організаційні та організаційно-технічні заходи щодо захисту інформації в АСВБ що зазначені в цьому Техпроекті здійснюються у період з 20.02.2015 року по 20.09.2021 року.

Фінансування робіт здійснюється за рахунок коштів передбачених для безпеки в ТФ «… (назва фірми)».

Порядок оформлення та пред'явлення Замовнику результатів виконання робіт зі створення КСЗІ в АСВБ визначається вимогами що представлені у п.1.7 Технічного завдання.

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.

Під час розробки КСЗІ враховується інформація яка наведена в документах перелік яких наведено в п. 1 цього Техноробочого проекту.

Відомості які зазначають структуру та склад АСВБ, а саме: структура та обладнання, що використовується в АСВБ; програмне забезпечення, що використовується в основних складових АСВБ; характеристика інформації та технологія її обробки в АСВБ (характеристика інформаційного середовища); характеристики обслуговуючого персоналу АСВБ; користувачі, об'єкти, процеси та їх атрибути в АСВБ, наведені в Технічному завданні.

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 роботоздатності в АСВБ наступного програмного забезпечення:

- операційної системи Windows 7; драйвери системних пристроїв АСВБ; пакет прикладних програм Microsoft Office 2010; антивірусна програма ESET Smart Security 2021.

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

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

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

Проведення адміністрування системи захисту інформації «Захист», щодо впровадження функціональних послуг захисту інформації наведених в технічному завданні, 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: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

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

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

Встановлення на лінію охоронної сигналізації протизавадного фільтра «...». Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

Підключення всіх компонентів АСВБ до контуру заземлення.

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

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

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

3.3.2. Будівельно-монтажні роботи із захисту інформації в АС

Обладнання віконного отвору металевими гратами відповідно вимог п.п 4.1.2 Технічного завдання на створення КСЗІ

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

3.3.3. Організаційні заходи із захисту інформації в АС

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

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

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: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

Визначення обмежень співробітників підприємства.

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

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

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

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

– порядок присвоєння реєстраційних (системних) імен користувачів; порядок видачі паролів користувачам;

– порядок зміни паролів та реєстраційних (системних) імен користувачів; порядок вилучення паролів; склад імен та паролів;

– обов'язки користувача під час поводження користувачів з паролями.

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

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: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

Складання Інструкції про порядок оперативного відновлення функціонування АС класу 2 відділу безпеки ТФ «… (назва фірми)» в який повинно бути зазначено:

– порядок дій адміністраторів при виявленні НСД;

– порядок дій представників служби захисту інформації та охорони при виникненні надзвичайних ситуацій;

Відповідальний: ...(ПІБ)

Відмітка про виконання: ...(ПІБ)

Підпис виконавця:_____

3.4. Показники захищеності АСВБ від НСД

Відповідно відомостей наведених в Технічному завданні 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 (технічних завдань) на їх розробку

Організація постачання та впровадження в АСВБ технічних засобів захисту здійснюється відділом безпеки ТФ «… (назва фірми)».

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 Техноробочогопроекту.

Попередні випробування проводяться після виконання в повному обсязі пусконалагоджувальних робіт.

Спеціалістами відділу безпеки ТФ «… (назва фірми)» 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 (монтаж) біля АСВБ будь яких технічних пристроїв (засобів) 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
ТФ «… (назва фірми)» ...(ПІБ)

**Додаток Ж**

**«ЗАТВЕРДЖЕНО»**
Відповідальний за відділ
безпеки туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«25» березня 2021 року

**ПАСПОРТ-ФОРМУЛЯР**

**НА АВТОМАТИЗОВАНУ СИСТЕМУ 2 КЛАСУ ВІДДІЛУ БЕЗПЕКИ**

**ТУРИСТИЧНОЇ ФІРМИ«… (назва фірми)»**

Чернігів-2021

*1. Загальні положення*

1.1. Паспорт - формуляр (далі - Паспорт) на автоматизовану систему класу 2 відділу безпеки туристичної фірми «… (назва фірми)».

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 туристичної фірми «… (назва фірми)» орендує 2 поверхи в торгівельно-розважальному центрі «Аркадія», по вулиці Борщагівська 154. Загальна площа магазину 200 кв.м. (по 200 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 об'єкті інформаційної діяльності – приміщення № 2 відділу безпеки здійснює такі види інформаційної діяльності:

2.3.1. Обробка (перетворення, відображення, накопичення, друк) інформації з обмеженим доступом 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 туристична фірма «… (назва фірми)» 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 «…(ОХОРОННА ФІРМА)».

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

Труби системи опалення встановлено під підвіконням та підводяться до внутрішньої котельні ВАТ «…(ОХОРОННА ФІРМА)».

Кабель системи заземлення підключено до електричних розеток та виведено до контуру заземлення, який знаходиться в межах контрольованої зони ВАТ «…(ОХОРОННА ФІРМА)».

Лінії електроживлення прокладено в стінах неекранованими мідними проводами та виводяться до електричного розподільчого щита, який знаходиться в межах контрольованої зони туристична фірма «… (назва фірми)». Від розподільчого щита кабель електроживлення прокладено до трансформаторної підстанції, яка знаходиться в межах контрольованої зони

ВАТ «…(ОХОРОНННА ФІРМА)».

2.5. Схема розміщення ОІД в приміщенні № 2 ВАТ «…(ОХОРОНННА ФІРМА)». та відносно межі контрольованої зони туристична фірма «… (назва фірми)».

2.6 Охорона туристичної фірми «… (назва фірми)» в цілому здійснює відомча охорона відповідно розпоряджень та інструкцій ВАТ «…(ОХОРОНННА ФІРМА)».

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.

*4. Відомості про закріплення АСВБ під час експлуатації*

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

*5. Технічні засоби, засоби технічного захисту*

*5.1. 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** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

*5.2. 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** | |
| | | | | |
| | | | | |
| | | | | |

*5.3. Допоміжні технічні засоби*

| **№ з/п** | **Найменування допоміжних** | **Тип** | **Заводський (інвентарний) №** | **Примітки** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | **технічних засобів** | | | |
| | | | | |
| | | | | |
| | | | | |

*5.4. 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** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

*6. Відповідальні за ОІД*

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

*7. Реєстрація проведених робіт (технічне обслуговування, модернізація, ремонт тощо основних, допоміжних технічних засобів та засобів захисту)*

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

*8. Відмітки про проведення перевірки складу програмного забезпечення АСВБ*

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

*9. Періодичні, контрольні, інспекційні та інші перевірки стану комплексної системи захисту інформації*

| **Дата** | **Вид перевірки** | **Результати перевірки** | **Дата, № Акту перевірки** | **Відмітки про усунення недоліків** |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

*10. Картка-замісник пакета документів на КСЗІ в АСВБ*

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

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

*11. Особливі примітки*

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

**Додаток З**

**«ЗАТВЕРДЖУЮ»**
Генеральний директор
туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«25» квітня 2021 року

**АКТ**
**приймання комплексної системи захисту інформації автоматизованої системи класу 2 відділу безпеки ТФ «… (назва фірми)»**

**Комісія у складі:**
голова: Відповідальний за відділ безпеки ТФ «… (назва фірми)» ...(ПІБ);
члени: Заступник відповідального за відділ безпеки …, начальник спеціального відділу ...(ПІБ)

Було проведено приймання у дослідну експлуатацію комплексну систему захисту інформації (далі – КСЗІ) яка створена в автоматизованій системі класу 2 відділу безпеки (далі – АСВБ) ТФ «… (назва фірми)» .

Під час роботи комісії встановлено:

1. КСЗІ в АСВБ створена відповідно вимог документу «Автоматизована система відділу безпеки ТОВ ТФ «… (назва фірми)» . Комплексна система захисту інформації. Технічне завдання», а саме:
   - вимог до захисту інформації від витоку технічними каналами;
   - вимог до захисту інформації від несанкціонованого доступу 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 комплексної системи захисту інформації в автоматизованій системі класу 2 відділу безпеки ТФ «… (назва фірми)» 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 ТФ «… (назва фірми)» ...(ПІБ)

**Члени комісії:**

Заступник відповідального
за відділ безпеки ТФ «… (назва фірми)» …

Начальник спеціального відділу
ТФ «… (назва фірми)» ...(ПІБ)

**Додаток И**

**«ЗАТВЕРДЖУЮ»**
Генеральний директор
туристичної фірми
«… (назва фірми)»
_____ ...(ПІБ)
«25» квітня 2021 року

**АКТ**
**завершення дослідної експлуатації комплексної системи захисту інформації в автоматизованій системі класу 2 відділу безпеки ТФ «… (назва фірми)»**

**Комісія у складі:**
голова: Відповідальний за відділ безпеки ТФ «… (назва фірми)» ...(ПІБ);
члени: Заступник відповідального за відділ безпеки …, начальник спеціального відділу ...(ПІБ)

Було проведено дослідну експлуатацію комплексної системи захисту інформації (далі – КСЗІ) яка створена в автоматизованій системі класу 2 відділу безпеки (далі – АСВБ) об'єкту інформаційної діяльності – приміщення № 1 ТФ «… (назва фірми)» (далі – ОІД).

Підставою для проведення дослідної експлуатації КСЗІ в АСВБ є:

«Автоматизована система відділу безпеки ТФ «… (назва фірми)» . Комплексна система захисту інформації. Технічне завдання» (далі – Технічне завдання);

Протокол попередніх випробувань комплексної системи захисту інформації в автоматизованій системі класу 2 відділу безпеки ТФ «… (назва фірми)» (далі – Протокол попередніх випробувань).

Під час проведення дослідної експлуатації комісією встановлено:

1. Всі компоненти АСВБ працюють справно та без збоїв відповідно задекларованих параметрів наведених в експлуатаційних документах.

2. Система заземлення, до якої підключено всі компоненти, в справному стані.

3. Система захисту інформації від несанкціонованого доступу роботоздатна та адміністрування її програмного забезпечення відповідає задекларованої в Технічному завданні технології обробки інформації за допомогою АСВБ, а саме:

- здійснює ідентифікацію та аутентифікацію користувачів АСВБ;
- блокує завантаження операційної системи АСВБ з гнучкого диска та 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 (пристроїв) 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 (завантаження) програм, які не входять до баз даних операційної системи АСВБ.
- дає можливість управління потоками інформації.

4. При проведенні тестового оброблення інформації в АСВБ відповідно технології обробки інформації наведеної в Технічному завданні, а саме:

- створенні файлу з тестовою інформацією за допомогою програми «Захищені документи» та зберіганні його на жорсткий магнітний диск, флеш накопичувач в створених для цього базах документів;
- друкуванні файлу за допомогою принтеру АСВБ;

– знищенні користувачем документів з тестовою інформацією ;
– здійсненні зчитування інформації з CD-ROM, флеш накопичувача;
– недоліків та збоїв не виникало.
– Впроваджені в КСЗІ організаційні заходи захисту інформації в АСВБ, а саме:
– порядок доступу користувачів до АСВБ та інформації, яка в ній зберігається;
– порядок та зміст інструктажів користувачів АСВБ;
– порядок обробки інформації користувачами за допомогою АСВБ;
– порядок дій начальника спеціального відділу, користувачів АСВБ та представників служби захисту інформації в АСВБ при виникненні загроз інформації, яка обробляється в АСВБ;
– порядок оперативного відновлення функціонування АСВБ;
– порядок обліку та використання магнітних носіїв інформації;
– порядок видачі вилучення та зберігання персональних ідентифікаторів користувачів АСВБ та адміністраторів АСВБ;
– правила управління паролями в АСВБ;
– правила з забезпечення режиму конфіденційності під час обробки інформації в АСВБ;
– порядок організації фізичного та протипожежного захисту АСВБ;
– порядок дій начальника спеціального відділу по підтримці внутрішньо об’єктового режиму на ОІД;
– порядок блокування технічних каналів витоку інформації та шляхів несанкціонованого доступу, не мають між своїх вимог розбіжностей, завдань, які б неможливо було виконати та забезпечують вимоги Технічного завдання щодо захисту інформації в АСВБ.

6. Впроваджені в КСЗІ організаційно-технічні заходи стосовно захисту інформації від її витоку технічними каналами відповідають умовам інформаційного середовища АСВБ та вимогам Технічного завдання.

7. Всі користувачі, які плануються до обробки інформації за допомогою АСВБ, здали заліки зі знань:

порядку обробки інформації за допомогою АСВБ;

підтримання режиму конфіденційності під час обробки інформації за допомогою АСВБ;

порядку дій при виникненні загроз інформації.

8. За АСВБ закріплено адміністратори які входять до складу створеної в ТФ «… (назва фірми)» служби захисту інформації в АСВБ.

9. Комплект експлуатаційних документів КСЗІ в АСВБ, перелік яких наведено в Протоколі попередніх випробувань КСЗІ, є достатнім щодо організації захисту інформації в АСВБ та обробки ІзОД за допомогою АСВБ.

10. АСВБ повністю укомплектована та знаходиться в робочому стані.

**Висновок**

КСЗІ в АСВБ:

– забезпечує визначену для АСВБ системи політику безпеки інформації;
– здійснює розмежування доступу користувачів в АСВБ до інформації різних категорій конфіденційності;
– блокує несанкціоновані дії з ІзОД;
– реєструє спроби реалізації загроз інформації та сповіщає адміністраторів безпеки інформаційно-телекомунікаційної системи про факти несанкціонованих дій з ІзОД;
– забезпечує спостереженість інформації шляхом контролю за діями користувачів АСВБ та реєстрації 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;

– забезпечує дотримання вимог режиму конфіденційності під час роботи користувачів в АСВБ з ІзОД.

Під час проведення дослідної експлуатації КСЗІ в АСВБ збоїв в роботі будь яких компонентів АСВБ, пристроїв захисту інформації, систем охоронної та протипожежної сигналізації не виявлено.

Створена КСЗІ в АСВБ може бути представлена на експертизу щодо отримання атестату відповідності на КСЗІ в АСВБ.

**Голова комісії:**

Відповідальний за відділ
безпеки ТФ «… (назва фірми)» ...(ПІБ)

**Члени комісії:**

Заступник відповідального
за відділ безпеки ТФ «… (назва фірми)» ...(ПІБ)

Начальник спеціального відділу
ТФ «… (назва фірми)» ...(ПІБ)

# 4. ВИМОГИ ДО ОФОРМЛЕННЯ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт виконують за допомогою комп'ютера на одній стороні аркуша білого паперу формату А4 (297х210 мм), 14-го розміру шрифту з інтервалом 1,5 і з кількістю абзаців на сторінці не більше 5. Перед текстом курсового проєкту розміщують титульний лист та відгук, підписані науковим керівником.

Необхідно дотримуватись таких розмірів полів: зліва - 30 мм для підшивки і зауважень, справа - 10 мм, знизу і зверху - 20 мм. Абзацний відступ повинен бути однаковим впродовж усього тексту роботи і дорівнювати 1,25 см.

Під час виконання курсового проєкту необхідно дотримуватись рівномірної щільності тексту, контрастності й чіткості зображення впродовж усієї роботи. Лінії, літери, цифри та інші знаки мають бути чіткі, не розпливчасті, однаково чорними впродовж усієї курсового проєкту.

Помилки, описки та графічні неточності допускається виправляти підчищенням або зафарбовуванням білою фарбою і нанесенням на тому ж місці, або між рядками, виправленого зображення машинописним способом або від руки. Виправлене повинно бути чорного кольору.

Скорочення слів і словосполучень у курсовому проєкті має здійснюватись відповідно до чинних стандартів з бібліотечної та видавничої справи.

Заголовки розділів друкують великими літерами по центру. Заголовки підрозділів друкують маленькими буквами (крім першої великої) з абзацного відступу. Крапку наприкінці заголовка не ставлять.

Перенесення слів у заголовку розділу не допускається. Кожний розділ починається з нової сторінки. Текст підрозділів пишеться в межах одного розділу без розриву.

Відстань між заголовком розділу і підрозділу - 1 рядок, між заголовком підрозділу і текстом курсового проєкту - 1 рядок.

Не допускається розміщення назви розділу, параграфу в нижній частині сторінки, якщо після неї розміщено тільки один рядок тексту.

Сторінки нумеруються арабськими цифрами. На титульному листі номер не ставиться, на наступних сторінках - у правому верхньому кутку без крапки (наскрізна нумерація з додатками).

Протягом всього тексту повинна бути одноманітність термінів, позначень, умовних скорочень та символів. Терміни повинні відповідати діючим стандартам.

У змісті (додаток Д) вказують номери сторінок, з яких починаються розділи, підрозділи.

Всі наведені цитати, цифрові дані та іншу інформацію, запозичену з літературних джерел, необхідно чітко виділяти із посиланням на джерело (порядковий номер за списком використаних джерел), із зазначенням сторінки у квадратних дужках. Наприклад: [25, с.77]; [15, с.183].

При наявності у тексті переліку, складових частин, фактів і таке інше, їх слід нумерувати порядковою нумерацією арабськими цифрами із дужкою, наприклад: 1), 2) і друкувати малими літерами із абзацного відступу.

### 4.1 Оформлення таблиць

Таблицю слід розміщувати одразу після тексту, в якому вона згадується вперше, або на наступній сторінці. На всі таблиці повинні бути посилання в тексті: "див. табл. 2.1". Кожна таблиця повинна мати назву, яку потрібно писати малими літерами (крім першої прописної). Назва розміщується над таблицею, є стислою і відображає зміст таблиці.

Таблиці нумеруються послідовно арабськими цифрами в межах кожного розділу (номер таблиці включає номер розділу і порядковий номер таблиці). При переносі частини таблиці на наступний аркуш зазначають: "Продовження табл. 2.1" .

Заголовки граф починають з великих літер, а підзаголовки – з малих,якщо вони складають одне речення із заголовком. Для скорочення тексту заголовків і підрозділів граф окремі поняття допускається заміняти літернимипозначеннями,

якщо вони пояснені в тексті, або приведені на малюнках.

Якщо цифрові дані в графах таблиці виражені в різних одиницях виміру, то їх указують в заголовках кожної графи. Якщо всі показники розміщені в таблиці, виражені в одній і тій же одиниці виміру, скорочене визначення одиниці виміру розміщають над таблицею в заголовку.

Графу "Номер з/п" у таблицю включати не слід, за винятком випадків, коли на ці номери є посилання.

Якщо текст, що повторюється в графі таблиці, складає одне слово, то замість нього ставлять лапки, якщо із двох і більше слів, то при першому повторі пишуть –те ж, а потім ставлять лапки. Ставити лапки замість цифр, знаків, математичних символів, які повторюються, не допускається. Якщоцифрові, або інші дані в таблиці не приводяться, замість них ставлять прочерк.

Цифри в графах таблиці потрібно розміщувати так, щоб числа були точно одне над другим. Числові значення величин в одній графі повинні мати однакову кількість десяткових знаків. Дрібні числа приводяться у вигляді десяткових дробів.

## 4.2 Оформлення формул

Формули та рівняння розміщуються безпосередньо за текстом, в якому вони згадуються, по середині рядка. До і після кожної формули чи рівняння залишається один вільний рядок. Наведені в курсовому проєкті формули нумерують (при наявності на них посилань (наприклад: див. формулу 1.1)) подвійною нумерацією арабськими цифрами в межах кожного розділу. Номери вказують з правої сторони аркуша на рівні формули в круглих дужках, наприклад (1.1) - першийрозділ, перша формула. Пояснення значень символів і числових коефіцієнтів слід наводити під формулою у тій самій послідовності, в якій вони дані у формулі. Значення кожного символу і числового коефіцієнта треба подавати знового рядка. Перед поясненням першого символу пишуть з абзацу слово "де" без двокрапки.

Наприклад:

$$E=m*c^2 \quad (1.1)$$

,де E – Енергія; m – маса; c – швидкість світла.

### 4.3 Оформлення рисунків

Ілюстрації (малюнки, графіки, схеми, діаграми) позначають словом "Рисунок". Ілюстрації необхідно розміщувати в роботі безпосередньо після тексту, де вони відзначаються вперше або на наступній сторінці.

При необхідності під ілюстрацією розміщають пояснювальні дані. Ілюстрації повинні мати назву, яку розташовують під ілюстрацією після пояснювальних даних разом з номером ілюстрації (див. додаток Г). Нумерація ілюстрацій проводиться арабськими цифрами в межах розділу, наприклад: Рисунок 1.2 (другий рисунок першого розділу).

### 4.4 Оформлення додатків

Кожний додаток починається з нового аркуша і повинен мати заголовок, який відображає зміст додатку. З абзацу пишуть слово "Додаток". Додатки мають наскрізну одинарну нумерацію великими літерами української абетки, наприклад: "Додаток А". На додатки у тексті обов'язково слід робити посилання.

### 4.5. Оформлення посилань у тексті

Посилання в роботі на літературні джерела слід позначати в кінці речення порядковим номером за переліком посилань, виділеними двома квадратними дужками, наприклад, «… у роботах [1-7] …». При посиланні на рисунки, таблиці, формули, вказують їх порядковий номер, наприклад: на рисунку 2.1; дивись рисунок 2.1; у таблиці 2.1; за формулою (2.1); у формулі (2.1).

# 5. КРИТЕРІЇ ОЦІНКИ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт подається на кафедру для перевірки науковим керівником не пізніше, ніж за тиждень до екзаменаційної сесії. Курсовий проєкт, яка відповідає викладеним у методичних рекомендаціях вимогам, оцінюється для студентів за стобальною шкалою з врахуванням наступних критеріїв:

Таблиця 5.1 – Критерії оцінки курсового проєкту

| Критерії | Бали |
|---|---|
| Оцінка структури роботи (повнота розкриття теми у змісті) | 60 балів |
| Оцінка теоретичного рівня роботи | |
| Повнота аналізу предметної області | |
| Правильність вибору та аналізу об’єктів | |
| Характеристика аналітичного рівня роботи | |
| Ілюстративність роботи: наявність таблиць, рисунків | |
| Відповідність вступу та висновків вимогам, які викладено в методичних вказівках по написанню курсового проєкту | |
| Оцінка повноти та правильність складання переліку посилань | |
| Відповідність оформлення роботи вимогам стандартів та правил | |
| Виконання календарного плану написання роботи | |
| Оцінка доповіді студента при захисті роботи | 40 балів |
| Оцінка відповіді студента на додаткові запитання | |
| Всього | 100 |

Співвідношення 100-бальної шкали оцінювання написання та захисту курсового проєкту зі шкалою ECST та 5-бальною шкалою оцінки наведено нижче.

Таблиця 5.2 – Шкала оцінювання успішності студентів

| Оцінка за національною шкалою | Оцінка за шкалою навчального закладу, балів | Оцінка за шкалоюECTS |
|---|---|---|
| 5 – «відмінно» | 100-90 | A |
| 4 – «добре» | 89-82 | B |
| 4 – «добре» | 81-75 | C |
| 3 – «задовільно» | 74-67 | D |
| 3 – «задовільно» | 66-60 | E |
| 2 – «незадовільно» | 59-35 | FX |
| 2 – «незадовільно» | до 34 | F |

Робота може бути оцінена на **"відмінно"** в тому разі, якщо в ній розкрита сутність проблеми дослідження, її актуальність, приведений огляд монографічної і періодичної літератури, статистичні матеріали. Роботамістить аналіз проблеми, розрахунки та обґрунтування рішень щодо вдосконалення методів вирішення проблеми, заявленої в рамках обраної теми. Виконані вимоги щодо оформлення роботи.

Оцінка **"добре"** виставляється у разі, якщо в роботі недостатньо обґрунтовані пропозиції автора щодо вдосконалення ефективності діяльності об'єкту дослідження, інші вимоги, які були перелічені в попередньому пункті виконані.

Оцінка **"задовільно"** виставляється у разі, якщо робота поверхово висвітлює зміст теми дослідження, не містить обґрунтованих рекомендацій по вирішенню проблем дослідження. Мають місце помилки в оформленні роботи.

Робота оцінюється на **"незадовільно"** та повертається на доопрацювання, якщо автор не розкрив зміст теми, не залучив практичний матеріал до аналізу проблеми дослідження та допустив помилки привикладенні змісту питань та оформленні роботи.

# 6. ОРГАНІЗАЦІЯ ЗАХИСТУ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт подається на кафедру для перевірки науковим керівником не пізніше ніж за тиждень до екзаменаційної сесії. Якщо робота виконана і оформлена правильно, то науковий керівник пише відгук і допускає курсовий проєкт до захисту.

Курсовий проєкт до захисту не допускається, якщо вона:

– подана науковому керівникові на перевірку з порушенням строків, установлених календарним планом;

– написана на тему, яка своєчасно не була затверджена по кафедрі;

– виконана не самостійно;

– не реалізовані запити, інструменти керування або інший елемент структури курсового проєкту;

– побудова структури не відповідає вимогам.

Заключним етапом є захист курсового проєкту. Він проводиться у строки, визначені деканатом. Курсові роботи захищають перед комісією, призначеною кафедрою. Студент по результатам дослідження готує роздатковий матеріал для членів комісії та презентацію в програмі PowerPoint. Студенту надається слово для викладання змісту дослідження (до 7 хвилин).

Під час захисту курсового проєкту студент має виявити глибокі знання з вивчених розділів курсу, вміти розкрити зміст розглянутих у курсовому проєкті положень і відповісти на поставлені членами комісії запитання. За результатами захисту комісія може уточнити попередню оцінку курсового проєкту, що її запропонував рецензент.

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

6. Горбань О. Основи теорії систем і системного аналізу [Текст]: Навчальнийпосібник / Олександр Миколайович Горбань, Володимир Євгенович Бахрушин. — Запоріжжя: ГУ «ЗІДМУ», 2004. — 204 с. — ISBN 966-8227- 23-9.

7. Сурмін Ю. Теорія систем та системний аналіз [Текст]: Навч. посібник / Юрій Петрович Сурмін; Міжрегіональна Академія управління персоналом. - К.: МАУП, 2003. - 368 с. - ISBN 966-608-290-X.

8. Колпаков В. Теорія та практика прийняття управлінських рішень [Текст]: Навч. посібник / Віктор Михайлович Колпаков; Міжрегіональна Академія управління персоналом. - 2-ге вид., перероб. та дод. - К.: МАУП, 2004. - 504 с. - ISBN 966-608-357-4.

9. Анфілатів В. Системний аналіз в управлінні [Текст]: Навч. посібник / В.С. Анфілатов, А.А. Ємельянов, А.А. Зозулин; За ред. А.А. Ємельянова. - М.: Фінанси та статистика, 2002. - 368 с. - ISBN 5-279-02435-X.

5. Плотинський Ю. Моделі соціальних процесів [Текст]: Навчальний посібник для вищих навчальних закладів/Юрій Менделійович Плотинський. - Вид. 2-ге, перероб. та дод. - М.: Логос, 2001.-296 с. - ISBN 5-94010-045-7.

## Додаткові рекомендовані джерела

1. Сорока К. Основи теорії систем і системного аналізу [Текст]: Навч. посібник / Костянтин Олексійович Сорока. — Харків: ХНАМГ, 2004. — 291 с. — ISBN 966-695-056-1.

2. Yeates D. Systems Analysis and Design [Text]: Textbook / Donald Yeates, TonyWakefield. — 2nd Edition. — Harlow, England: Pearson Education Limited, 2004. — 517 p. — ISBN 0273-65536-1.

3. Bowman K. Systems Analysis [Text]: A Beginner's Guide / Kevin Bowman. — New York: Palgrave Macmillan, 2004. — 186 p. — ISBN 0–333–98630–X.

4. Ye N. Secure Computer and Network Systems [Text]: Modeling, Analysis and Design / Nong Ye. — Chichester, West Sussex, England: John Wiley & Sons Ltd., 2008. — 354 p. — ISBN 978-0-470-02324-2.

5. Томашевський В. Моделювання систем [Текст]: Підручник / Валентин Миколайович Томашевський; за загальною ред. академіка НАН УкраїниМ. З. Згуровського. — К.: Видавнича группа BHV, 2005. — 352 с. — (Інформатика). — ISBN 966-552-120-9.

**ДОДАТКИ**

Додаток А- Зразок титульного листа курсового проєкту

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»**
**ІНСТИТУТ ЕЛЕКТРОННИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**
**Кафедра кібербезпеки та математичного моделювання**

Прізвище, ім'я та по-батькові студента

# КУРСОВИЙ ПРОЄКТ

**з дисципліни: "Комплексні системи захисту інформації"**
**на тему : "_____"**
Курс_____Група

**Науковий керівник:**
**_____**
**_____**

**Робота подана на кафедру** **Робота допущена до захисту** **Робота захищена з**

**____Науковий керівник** **оцінкою_**
**____**

**"___"_____20__р.** **"___"_____20__р.** **"___"_____20__р.**

**_____Голова комісії**
**_____Член комісії**

Чернігів 20___р.

Додаток Б - Приклади оформлення бібліографічного опису у списку літературних джерел

| Характеристика джерела | Приклад оформлення |
|---|---|
| 1 | 2 |
| Книги: Один автор | 1. Василій Великий. Гомілії / Василій Великий ; [пер. з давньогрец. Л. Звонська]. — Львів : Свічадо, 2006. — 307 с. — (Джерела християнського Сходу. Золотий вік патристики IV—V ст. ; № 14).<br>2. Коренівський Д. Г. Дестабілізуючий ефект параметричного білого шуму<br>в неперервних та дискретних динамічних системах / Коренівський Д. Г. — К.<br>: Ін-т математики, 2006. — 111 с. — (Математика та її застосування) (Праці /Ін-т математики НАН України ; т. 59). |
| Два автори | 1. Ромовська З. В. Сімейне законодавство України / З. В. Ромовська, Ю. В. Черняк. — К. : Прецедент, 2006. — 93 с. — (Юридична бібліотека. Бібліотека адвоката) (Матеріали до складання кваліфікаційних іспитів для отримання Свідоцтва про право на заняття адвокатською діяльністю ; вип.<br>11). |
| Три автори | 1. Акофф Р. Л. Ідеалізоване проектування: як запобігти завтрашній кризі сьогодні. Створення майбутнього організації / Акофф Р. Л., Магідсон Д., Еддісон Г. Д.; пров. з англ. Ф. П. Тарасенко. - Дніпропетровськ<br>: Баланс Бізнес Букс, 2007. - XLIII, 265 с. |
| Чоти и автори | 1. Методика нормування ресурсів для виробництва продукції рослинництва<br>/ [ Вітвіцький В. В., Кисляченко М. Ф., Лобастов І. В., Нечипорук А. А.]. —<br>К. : НДІ "Украгропромпродуктивність", 2006. — 106 с. — (Бібліотекаспеціаліста АПК. Економічні нормативи).. |
| П'ять і більше авторів | 1. Психологія менеджменту / [ Власов П. К., Липницький А. В., Лючихіна<br>І. М. та ін] ; за ред. Г. С. Нікіфорова. - [3-тє вид.]. -Х. : Гуманітар. центр, 2007. - 510 с. |
| Без автора | 1. Історія Свято-Михайлівського Золотоверхого монастиря / [авт. тексту В.Клос]. — К. : Грані-Т, 2007. — 119 с. — (Грані світу). |

| | |
|---|---|
| Багатотомний документ | 1. Міждержавні стандарти: каталог в 6 т. / [уклад. Ковальова І. Ст, Рубцова Є. Ю.; ред. Іванов Ст Л]. - Львів: НТЦ "Леонорм-Стандарт", 2005<br>- .- (Серія "Нормативна база підприємства"). Т. 1.-2005. -277 с.<br>2. Бондаренко В. Г. Теорія ймовірностей та математична статистика. Ч.1/<br>В. Г. Бондаренко, І. Ю. Канівська, С. М. Парамонова. - К.: НТУУ "КПІ", 2006. - 125 с. |
| Матеріали конференцій, з'їздів | 1. Економіка, менеджмент, освіта в системі реформування агропромислового комплексу : матеріали Всеукр. конф. молодих учених- аграрників ["Молодь України і аграрна реформа"], (Харків, 11—13 жовт. 2000р.) / М-во аграр. політики, Харк. держ. аграр. ун-т ім. В. В. Докучаева. — Х. :<br>Харк. держ. аграр. ун-т ім. В. В. Докучаева, 2000. — 167 с. |
| Препринти | 1. Шиляєв Б. А. Розрахунки параметрів радіаційного пошкодження матеріалів нейтронами джерела ННЦ ХФТІ/ANL USA з підкритичним, збиранням, що керується скорювачем електронів / Шиляєв Б. А., Воєводін В. М.<br>- Х.: ННЦ ХФТІ, 2006. - 19 с. - (Препринт / НАН України, Нац. нав. центр "Харк. фіз.-техн. ін-т"; ХФТІ 2006-4). |
| Депоновані науков іпраці | 4. 1. Соціологічне дослідження малих груп населення / В. І. Іванов [та ін.]; М-во освіти Ріс. Федерації, Фінансова академія. - М., 2002.<br>5. – 110 с. - Деп. у ВІНІТІ 13.06.02, № 145432.<br>6. 2. Розумовський В. А. Управління маркетинговими дослідженнями в регіоні/В. А. Разумовський, Д. А. Андрєєв. – М., 2002. – 210 с. - Деп. в<br>7. ІНІОН Ріс. акад. наук 1 5.02.02, № 139876. |
| Словники | 1. Тимошенко З. І. Болонський процес в дії : словник-довідник основ,термінів і понять з орг. навч. процесу у вищ. навч. закл. / З. І. Тимошенко, О.<br>І. Тимошенко. — К. : Європ. ун-т, 2007. — 57 с. |
| Атласи | 1. Україна : екол.-геогр. атлас : присвяч. всесвіт, дню,науки в ім'я миру та розвитку згідно з рішенням 31 сесії ген. конф. ЮНЕСКО / [наук, редкол.: С.С. Куруленко та ін.] ; Рада по вивч. продукт, сил України НАН України [та ін.]. — 7 [наук, редкол.: С. С. Куруленко та ін.]. — К. : Варта, 2006. — 217,<br>[1] с. |

| | |
|---|---|
| Законодавчі та нормативні документи | 1. Кримінально-процесуальний кодекс України : за станом на 1 груд. 2005 р. / Верховна Рада України. — Офіц. вид. — К. : Парлам. вид-во, 2006. — 207 с. — (Бібліотека офіційних видань). |
| Стандарти | 1. Вимоги щодо безпечності контрольно-вимірювального та лабораторного електричного устаткування. Частина 2-020. Додаткові вимоги до лабораторних центрифуг (EN 61010-2-020:1994, IDT) : ДСТУ EN 61010-2- 020:2005. — [Чинний від 2007-01-01]. — К. : Держспоживстандарт України,<br>2007. — IV, 18 с. — (Національний стандарт України). |
| Каталоги | 1. Міждержавні стандарти: каталог: в 6 т. / [уклад. Ковальова І. В., Павлюкова В. А.; ред. Іванов Ст Л.]. - Львів: НТЦ "Леонорм-стандарт", 2006 -. - (Серія "Нормативна база підприємства").<br>Т. 5.— 2007.— 264 с.<br>Т. 6. — 2007. — 277 с. |
| Бібліогра ф-фічні показчики | 1. Систематизований покажчик матеріалів з кримінального права, опублікованих у Віснику Конституційного Суду України за 1997—2005 роки<br>/ [уклад. Кирись Б. О., Потлань О. С]. — Львів : Львів, держ. ун-т внутр.<br>справ, 2006. — 11 с. — (Серія: Бібліографічні довідники ; вип. 2). |
| Дисертації | 1. Петров П. П. Активність молодих зірок сонячної маси: дис .....доктора фіз.-мат. наук : 01.03.02 / Петров Петро Петрович. - К., 2005. - 276 с |
| Автореферати дисертацій | 1. Новосад І. Я. Технологічне забезпечення виготовлення секцій робочих органів гнучких гвинтових конвеєрів : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.02.08 „Технологія машинобудування‖ /І. Я.<br>Новосад. — Тернопіль, 2007.—20, [1] с. |
| Авторські свідоцтва | 1. А. с. 1007970, МКИ[3] В 25 J 15/00. Пристрій для захоплення неорієнтованих деталей типу валів/В. С. Ваулін, В. Г. Кемайкін. - №3360585/25-08; заяв. 23.11.81; опубл. 30.03.83, Бюл. №12. |
| Патенти | 1. Пат. 2187888, МПК[7] Н 04 В 1/38, Н 04 J 13/00. Приймальний пристрій / Чугаєва В. І.; заявник та патентовласник, Чернігів, наук.-дослід. ін-т зв'язку. - № 2000131736/09;<br>заяв. 18.12.00; опубл. 20.08.02, Бюл. №23 (II год.). |

| | |
|---|---|
| Частина книги, періодичного, продовжуваного видання | 1. Регіональні особливості смертності населення України / Л. А. Чепелевська, Р. О. Моісеєнко, Г. І. Баторшина [та ін.] // Вісник соціальної гігієни та організації охорони здоров'я України. — 2007. — № 1.<br>— С 25—29.<br>2. Чорний Д. М. Міське самоврядування: тягарі проблем, принади цивілізації /Д. М. Чорний // По лівий бік Дніпра: проблеми модернізації міст України : (кінець XIX—початок XX ст. /Д. М. Чорний. — Х., 2007. — Розд. 3.<br>— С 137—202. |
| Електронні ресурси | 1. Богомольний Б. Р. Медицина екстремальних ситуацій [Електронний ресурс] : навч. посіб. для студ. мед. вузів III—IV рівнів акредитації / Б. Р. Богомольний, В. В. Кононенко, П. М. Чуєв. — 80 Min / 700 MB. — Одеса : Одес. мед. ун-т, 2003. — (Бібліотека студента-медика) — 1 електрон, опт. диск (CD-ROM) ; 12 см. — Систем, вимоги: Pentium ; 32 Mb RAM ; Windows 95, 98, 2000, XP ; MS Word 97-2000.— Назва з контейнера.<br>2. Розподіл населення найбільш численних національностей за статтю та віком, шлюбним станом, мовними ознаками та рівнем освіти [Електронний ресурс] : за даними Всеукр. перепису населення 2001 р. / Держ. ком. статистики України ; ред. О. Г. Осауленко. — К. : CD-вид-во "Інфодиск", 2004. — 1 електрон, опт. диск (CD-ROM) : кольор. ; 12 см. — (Всеукр. перепис населення, 2001). — Систем, вимоги: Pentium-266 ; 32 Mb RAM ; CD- ROM Windows 98/2000/NT/XP. — Назва з титул, екрану.<br>Бібліотека і доступність інформації у сучасному світі: електронні ресурси в науці, культурі та освіті : (підсумки 10-ї Міжнар. конф. „Крим- 2003‖) [Електронний ресурс] / Л. Й. Костенко, А. О. Чекмарьов, А. Г. Бровкін, І. А. Павлуша // Бібліотечний вісник — 2003. — № 4. — С 43. —<br>Режим доступу до журн. : http://www.nbuv.ciov.ua/articles/2003/03klinko.htm. |

Додаток В – Зразок оформлення таблиці

Таблиця 1.1

Аналіз виконання кошторису доходів та видатків за звітний період

| Найменування видатків | КЕКВ | 2015 | | 2016 | | Відхилення 2016 до 2015 | |
|---|---|---|---|---|---|---|---|
| | | сума, грн. | питома вага, % | сума, грн. | питома вага,% | сума, грн. | питома вага, % |
| Оплата праці | 2110 | 789360 | 43,1 | 787456 | 43,4 | 1904 | + 0,3 |
| Нарахування на оплату Праці | 2120 | 286538 | 15,7 | 285847 | 15,7 | 691 | - |
| Предмети, матеріали, обладнання та Інвентар | 2210 | 146258 | 8,0 | 136128 | 7,5 | 10130 | - 0,5 |
| Продукти Харчування | 2230 | 348960 | 19,1 | 347912 | 19,2 | 1048 | + 0,1 |
| Оплата комунальних послуг та Енергоносіїв | 2270 | 258963 | 14,1 | 257256 | 14,2 | 1707 | + 0,1 |
| Разом | - | 1830079 | 100,0 | 1814599 | 100,0 | 15480 | - |

Джерело: складено автором за даними кошторису установи

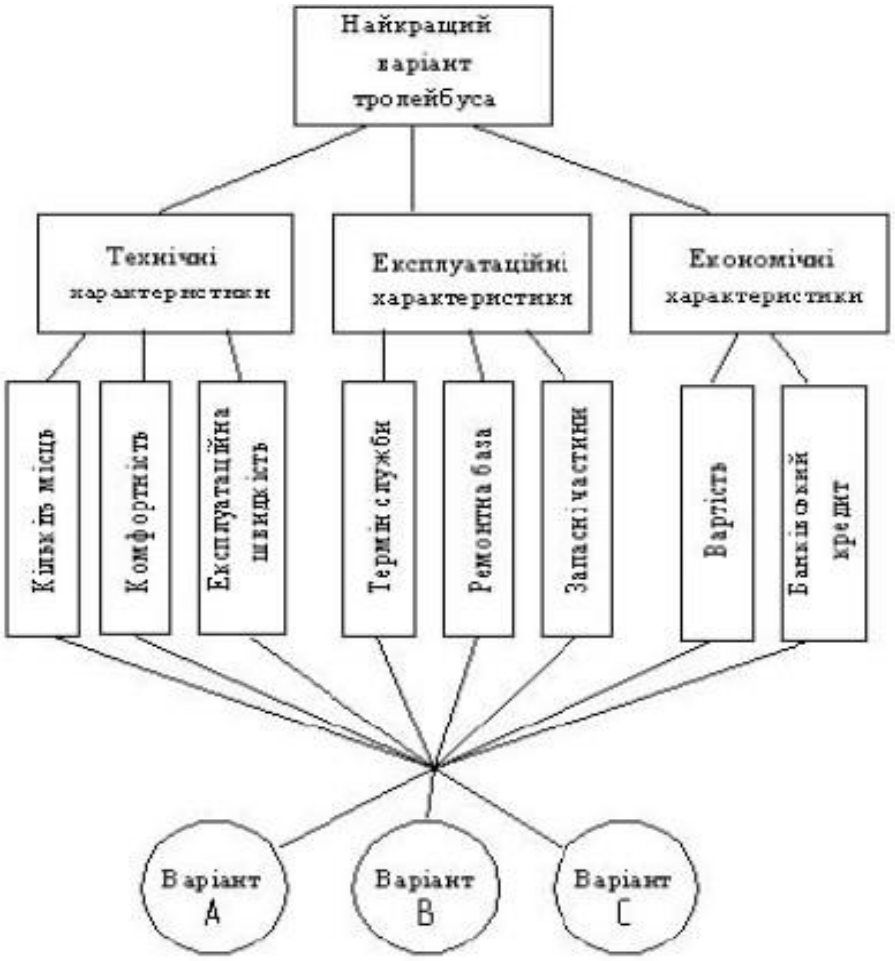


Рис. 1.1. Ієрархічна модель проблеми вибору

Джерело: складено автором

Додаток Д - Зразок відгуку на курсовий проєкт

**ВІДГУК**
**НА КУРСОВИЙ ПРОЄКТ**
**з теми „ .....”**

студента.....
_____курсу, групи_____, спеціальності _____
Курсовий проєкт з дисципліни _____
Реєстраційний №_____дата отримання „___‖____20 р.
Науковий керівник _____

**Основна характеристика курсового проєкту:**

**Мета дослідження** : досягнута повністю (частково, не досягнута )

**Завдання дослідження** :виконані повністю (частково, не виконані)

**Структура роботи:** витримується згідно вимогам (частково відповідаєвимогам, не відповідає вимогам)

**Характер зовнішнього оформлення роботи:** охайний (задовільний,неохайний)

**Зауваження:**

**Недоліки роботи:**

**Загалом робота заслуговує позитивної оцінки та може бутидопущена до захисту**

**Науковий керівник_____ (підпис)**

**За результатами захисту робота оцінена _____**
**Члени комісії _____**