ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЛАБОРАТОРНА РОБОТА №1-4

з навчальної дисципліни «Комплексні системи захисту інформації»

Тема: Дослідження структури об’єкту захисту. Ідентифікація небезпечних чинників на об’єкт захисту. Модель порушника. Розробка політики інформаційної безпеки

Виконав:

студент групи – 6.04.125.010.21.2

факультету - ІТ

спеціальності 125-кібербезпека

Бойко Вадим

Перевірила:

Мерлак О.В.

Харків, 2024 р.

ЗМІСТ

РОЗДІЛ 1. ДОСЛІДЖЕННЯ СТРУКТУРИ ОБ’ЄКТУ ЗАХИСТУ

* 1. Попереднє дослідження об’єкта, визначення його складових, структурних підрозділів …………………………………………………… 4
  2. Структурна схема досліджуваного об’єкту, з ідентифікацією та аналізом інформаційних потоків та інформаційних ресурсів …………… 6
  3. Типи технологій передачі інформації на об’єкті для кожного інформаційного потоку …………………………………………………… 11
  4. Носії інформації, що використовуються для зберігання інформаційних ресурсів, та методи й засоби їх захисту ………………... 13

РОЗДІЛ 2. ІДЕНТИФІКАЦІЯ НЕБЕЗПЕЧНИХ ЧИННИКІВ НА ОБ’ЄКТ ЗАХИСТУ

2.1 Перелік загроз, ймовірність виникнення загроз та обґрунтування оцінки для інформаційних потоків ……………………………………… 18

2.2 Перелік загроз, ймовірність виникнення загроз та обґрунтування оцінки для інформаційних ресурсів ……………………………………… 26

2.3 Перелік загроз, ймовірність виникнення загроз та обґрунтування оцінки для носіїв інформації ……………………………………………... 29

2.4 Сумарна таблиця загроз для інформації ……………………………... 33

РОЗДІЛ 3. МОДЕЛЬ ПОРУШНИКА

3.1 Зовнішні і внутрішні групи порушників на підприємстві ………… 36

3.2 Модель порушника …………………………………………………... 38

РОЗДІЛ 4. РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Загальні положення ………………………………………………….. 47

4.2 Глосарій ………………………………………………………………. 48

4.3 Мета, цілі та завдання політики ……………………………………... 49

4.3.1 Мета

4.3.2 Цілі

4.3.3 Завдання

4.4 Сфера застосування політики ……………………………………….. 50

4.5 Заходи захисту від загроз з середньою ймовірністю ………………. 51

4.5.1 Захист інформаційних ресурсів від порушення режиму роботи джерел живлення

4.5.2 Захист інформаційних ресурсів від підкупу і шантажу співробітників

4.5.3 Захист інформаційних ресурсів від DoS-атака або DDoS-атаки

4.5.4 Захист інформаційних ресурсів від несанкціонованого доступу до даних

4.5.5 Захист інформаційних ресурсів від несанкціонованого доступу до БД

4.5.6 Захист інформаційних ресурсів від підключення з незареєстрованого пристрою

4.5.7 Захист інформаційних ресурсів від SQL-ін'єкції

4.5.8 Захист інформаційних ресурсів від кібератак (шкідливе ПЗ)

4.5.9 Захист інформаційних ресурсів від модифікації даних зловмисниками

4.6 Заходи захисту від загроз з низькою ймовірністю …………………. 59

4.6.1 Захист інформаційних ресурсів від виникненням технічних несправностей елементів засобів

4.6.2 Захист інформаційних ресурсів від підслуховування ІзОД сторонніми особами

4.6.3 Захист інформаційних ресурсів від читання даних з екрану або читання документів, які залишені без нагляду сторонніми особами

4.6.4 Захист інформаційних ресурсів від крадіжки документів або пристроїв з сервісного центру

4.6.5 Захист інформаційних ресурсів від атаки “людина посередині” (Man-in-the-Middle)

4.6.6 Захист інформаційних ресурсів від фішингу

4.6.7 Захист інформаційних ресурсів від розкриття конфіденційних даних клієнтів

4.6.8 Захист інформаційних ресурсів від не навмисного пошкодження пристрою

4.6.9 Захист інформаційних ресурсів від порушення приватності або неетичного поводження з пристроєм клієнта

4.6.10 Захист інформаційних ресурсів від не навмисного постачання неякісних деталей

4.6.11 Захист інформаційних ресурсів від спостереження за введенням ПІН-коду клієнта сторонніми особами

4.6.12 Захист інформаційних ресурсів від недбалого зберігання або неправильної утилізація даних

4.6.13 Захист інформаційних ресурсів від маніпуляції даними для власної вигоди

4.6.14 Захист інформаційних ресурсів від втрати даних через людську помилку

4.7 Кроки у випадку перегляду політики інформаційної безпеки внаслідок виникнення інциденту ……………………………………….. 70

**Лабораторна робота №1**

**ДОСЛІДЖЕННЯ СТРУКТУРИ ОБ’ЄКТУ ЗАХИСТУ**

**Мета роботи:** придбання теоретичних знань та практичних навичок з аналізу структури об’єкту захисту.

**Завдання**

1. Виконати попереднє дослідження об’єкта з метою визначення його складових, структурних підрозділів.
2. Представити структурну схему досліджуваного об’єкту, з ідентифікацією та аналізом інформаційних потоків та інформаційних ресурсів.
3. Визначити тип технологій передачі інформації на об’єкті (автоматизована, автоматична, за допомогою персоналу тощо) для кожного інформаційного потоку.
4. Визначити носії інформації, що використовуються для зберігання інформаційних ресурсів, та методи й засоби їх захисту.
5. Зробити загальні висновки, щодо необхідності захисту інформаційних ресурсів підприємства.

**РОЗДІЛ 1. ДОСЛІДЖЕННЯ СТРУКТУРИ ОБ’ЄКТУ ЗАХИСТУ**

**1.1 Попереднє дослідження об’єкта, визначення його складових, структурних підрозділів**

Об'єктом дослідження даної роботи є сервісний центр з ремонту комп'ютерів.  
 Сервісний центр є невеликим підприємство, що спеціалізується на наданні послуг з діагностики, ремонту та обслуговування комп'ютерної техніки. Він забезпечує клієнтів якісними та надійними рішеннями щодо відновлення роботи комп'ютерів, ноутбуків та інших пристроїв. Персонал центру складається з кваліфікованих техніків, які володіють різноманітними навичками з ремонту та обслуговування техніки.

Складові сервісного центру:

1. Персонал:

* приймальник - 1 особа;
* майстри - 2 осіб;
* керівник - 1 особа;
* бухгалтер - 1 особа;
* системний адміністратор - 1 особа;
* завідувач складом - 1 особа;
* прибиральник - 1 особа.

1. Приміщення:

* приймальня;
* майстерня;
* склад;
* приміщення керівника;
* приміщення бухгалтера;
* приміщення системного адміністратора;
* підсобка;
* бомбосховище.

1. Обладнання:

* комп'ютери - 8 шт;
* інструменти;
* запчастини.

1. Програмне забезпечення

* сайт для клієнтів;
* сайт з адміністративною панеллю.

Структурні підрозділи:

* Приймальня (прийом та видача техніки, оформлення замовлень);
* Майстерня (діагностика, ремонт, тестування);
* Склад запчастин (зберігання комплектуючих);
* Адміністрація (керівництво, бухгалтерія, системний адміністратор).

Розглянемо, які вразливості та небезпеки можуть впливати на загальний стан безпеки сервісного центру:

1. Несанкціонований доступ до інформації: слабкі паролі, несанкціонований доступ до комп'ютерів та мережі, втрата або крадіжка носіїв інформації.
2. Втрата або пошкодження даних: апаратні збої, програмні помилки, кібератаки.
3. Витік конфіденційної інформації: необережне поводження з інформацією, несанкціоноване прослуховування каналів зв'язку, соціальна інженерія.

Небезпеки, що впливають на загальний стан безпеки сервісного центру:

1. Кібератаки: віруси, хакери, DDoS-атаки.
2. Фізичні загрози: пожежа, повені, крадіжка, травматичні ситуації, неправильне використання обладнання.

**1.2 Структурна схема досліджуваного об’єкту, з ідентифікацією та аналізом інформаційних потоків та інформаційних ресурсів**

Розглянемо структурну схема сервісного центру та їх вид діяльності.

1. Приймальня:

* Приймає техніку клієнтів.
* Оформляє замовлення (додає дані про клієнта та пристрій до БД №1).
* Зберігає тимчасово особисті речі клієнтів.
* Видає техніку клієнтам та паперові квитанцією про деталі виконання ремонту і чек.

2) Майстерня:

* Здійснює діагностику, ремонт та тестування комп'ютерної техніки.
* Має зони для роботи з різними типами комп'ютерів (настільні, ноутбуки, сервери).
* Заповнює БД №2 і вносить результати ремонту даного пристрою.
* Зберігає деякі запчастини та інструменти.

3) Склад запчастин:

* Зберігає запчастини та інструменти.
* Веде облік запчастин.

4) Адміністрація:

* Здійснює керівництво сервісним центром.
* Веде бухгалтерський облік.
* Займається звітністю.
* Займається захистом інформаційних ресурсів.
* Забезпечує маркетинг та рекламу.

Таблиця 1.1 - Аналіз інформаційних потоків

|  |  |  |  |
| --- | --- | --- | --- |
| **Напрямок** | **Інформаційний потік (що робить?)** | **Характеристика (дані, які передаються)** | **Тип передачі** |
| Клієнт -> Приймальня | Замовлення на ремонт | Дані про:   * ім'я * контактні дані * опис проблеми | Усний, онлайн (заповнення форми на сайті) |
| Приймальня -> Майстерня | Дані про пристрій | Дані про:   * пристрій * тип роботи | Фізичний (передавання пристрою), електронний (адмін панель) |
| Майстерня -> Склад запчастин | Дані про пристрій та деталі | Дані про:   * пристрій * деталі | Електронний |
| Склад запчастин -> Майстерня | Дані про пристрій та деталь | Дані про:   * пристрій * деталь | Електронний та фізичний (деталі) |
| Майстерня -> Приймальня | Дані про результат роботи | Дані про:   * пристрій * результат ремонту * ціну * контактні дані центру | Електронний |
| Приймальня -> Клієнт | Оплата за послуги та квитанція для клієнта | Дані про:   * клієнта * результат роботи * ціну * чек | Фізичний, електронний |
| Майстерня -> Адміністрація | Звітність про виконання робіт | Дані про:   * пристрій * результат ремонту * ціна * кількість відпрацьованих годин | Електронний |
| Приймальня -> Адміністрація | Звітність про клієнтів | Дані про:   * клієнта * пристрій * опис проблеми * результат робіт * ціна | Електронний |
| Склад запчастин -> Адміністрація | Звітність про облік запчастин | Дані про:   * запчастини * наявність запчастин * витрачені запчастини * ціна | Електронний |

Таблиця 1.2 - Аналіз інформаційних ресурсів

|  |  |  |  |
| --- | --- | --- | --- |
| **Тип ресурсу** | **Місце зберігання** | **Характеристика (що входить)** | **Методи захисту** |
| Дані про клієнтів | База даних №1 | * ім'я * контактні дані * пристрій * опис проблеми | Знаходяться на сервері, до якого доступ є лише за VPN, та для конкретних пристроїв. Також робиться резервна копія кожного дня. |
| Дані про виконання робіт | База даних №3 | * пристрій * опис проблеми * результат | Знаходяться на сервері, до якого доступ є лише за VPN, та для конкретних пристроїв. Також робиться резервна копія кожного дня. |
| Дані про запчастини (облік) | База даних №2 | * артикул * опис запчастини * виробник * модель * серійний номер * кількість * ціна | Знаходяться на сервері, до якого доступ є лише за VPN, та для конкретних пристроїв. Також робиться резервна копія кожного дня та синхронізується зі сторонніми ресурсами. |
| Фінансова документація | Сторонній сервіс | Фінансовий звіт:   * інформація про підприємство * доходи * витрати * чистий прибуток * адміністративні витрати * зарплата   Бухгалтерська документація:   * квитанції * накладні * касові чеки | Доступ за ЕЦП. |
| Сайт | Виділений сервер | * інформація про сервісний центр * форма замовлення | Дані передаються через шифрований канал, та передають заявку до сервісного центру. |
| Технічна документація | Паперові документи, електронні файли | * інструкції з ремонту * схеми * інструкції з експлуатації | Сейф та хмарне сховище. |
| Інші документи | Електронні файли | * ліцензії * страхові поліси * сертифікати | Хмарне сховище та сейф. |

**1.3 Типи технологій передачі інформації на об’єкті для кожного інформаційного потоку**

Таблиця 1.3 – Типи технологій передачі інформації

|  |  |  |
| --- | --- | --- |
| **Сторони (які приймають участь)** | **Інформаційний потік** | **Тип технології передачі** |
| Клієнти, приймальник | Замовлення на ремонт | Автоматизована, за допомогою персоналу |
| Майстри, приймальник | Дані про виконання роботи (результат) | Автоматизована |
| Завідувач складом | Облік запчастин (БД) | Автоматизована |
| Клієнти, приймальник | Оплата за послуги | За допомогою персоналу |
| Бухгалтер, керівник | Звітність | За допомогою персоналу, автоматизована |

Тепер, згідно (табл.1.3), більш детально опишемо типи технологій передачі інформації у сервісному центрі з ремонту комп’ютерів.

1. Замовлення на ремонт:

* Автоматизована, за допомогою персоналу: Клієнт особисто спілкується з приймальником і він заповнює дані про клієнта, пристрій та проблему до БД №1. Потім приймальник передає дані та пристрій до майстерні.
* Автоматизована: Клієнт заповнює форму замовлення на веб-сайті, де обробляється заявка.

1. Дані про виконання роботи:

* Автоматизована: Майстер заносить результати роботи в БД №3 (в поле з результатом).

3) Облік запчастин:

* Автоматизована: Завідувач складом видає запчастин відповідно до заявки, облік запчастин ведеться автоматично, використовуючи БД №2.

4) Оплата за послуги:

* За допомогою персоналу: Клієнт особисто сплачує за ремонт.

5) Звітність:

* Автоматизована: Бухгалтер заповнює звіти (в електронному вигляді) на сторонньому сервісі.
* За допомогою персоналу: Облік готівкового та безготівкового розрахунків.

**1.4 Носії інформації, що використовуються для зберігання інформаційних ресурсів, та методи й засоби їх захисту**

Таблиця 1.5 - Персонал та їх обов’язки

|  |  |
| --- | --- |
| **Персонал** | **За що відповідає** |
| Приймальник | * Створює електронну заявку на виконання робіт; * Віддає техніку, закриває замовлення, створює чек на оплату. |
| Майстер | * Оброблення електронної заявки від клієнта про пристрій (без даних про клієнта); * Робить запит на деталі зі складу; * Ремонтує пристрій. |
| Завідувач складом | * Обробляє заявку на видачу деталі; * Інвентаризує склад; * Замовляє деталі у постачальника. |
| Бухгалтер | * Фінанси та облік; * Заробітна платня. |
| Керівник | * Фінанси та облік; * Набір персоналу; * Навчання персоналу. |
| Системний адміністратор | * Слідкує за тим, щоб система працювала; * Слідкує за безпекою у телекомунікаційному просторі. |

Таблиця 1.6 - Носії інформації та їх захист

|  |  |
| --- | --- |
| **Носій інформації** | **Захист** |
| База даних клієнтів | Знаходяться на сервері, до якого доступ є лише за VPN, та для конкретних пристроїв, також робиться резервна копія кожного дня. |
| База даних запчастин | Знаходяться на сервері, до якого доступ є лише за VPN, та для конкретних пристроїв, також робиться резервна копія кожного дня та синхронізується зі сторонніми ресурсами. |
| База даних про виконання робіт | Знаходяться на сервері, до якого доступ є лише за VPN, та для конкретних пристроїв, також робиться резервна копія кожного дня. |
| Електронна звітність | Доступ лише з конкретного пристрою, який знаходиться у демілітаризованій зоні, також доступ за ЕЦП. |
| Бухгалтерська звітність | Знаходиться на сторонньому сервісі, тому тільки ЕЦП. |
| Архіви | Знаходяться під замком. |
| Сервери | Знаходяться у приміщенні, до якого мають доступ лише конкретні люди. |
| Електронні заявки клієнтів | Весь трафік шифрується, також є захист від відомих на даний момент вразливостей. |
| Інформація про працівників (особові справи) | Паперові - знаходяться під замком, а електронні – на сторонньому сервісі. |
| Чеки на оплату | Копії зберігаються на касі, та раз на місяць перевіряється електронна звітність від банку. |

Методи захисту носіїв інформації:

1. Фізичний захист:

* Обмеження доступу до приміщень:
* Відеоспостереження
* Сигналізація
* Контроль доступу (замки, картки)
* Зберігання документів:
* Сейфи

1. Інформаційна безпека:

* Паролі:
* Для доступу до комп'ютерів
* Для доступу до програмного забезпечення
* Для доступу до файлів
* Шифрування даних
  + Шифрування жорстких дисків
  + Шифрування резервних копій
  + Шифрування електронної пошти
  + Шифрування каналів зв’язку
* Обмеження прав доступу
  + Налаштування прав доступу до файлів і папок
  + Налаштування прав доступу до програмного забезпечення
  + Налаштування прав доступу до мережевих ресурсів

1. Технічні засоби захисту:

* Брандмауер:
* Контроль вхідного та вихідного трафіку
* Блокування несанкціонованого доступу
* Налаштування правил для різних програм

1. Програмне забезпечення:

* Антивірусне програмне забезпечення

1. Інформаційна безпека персоналу:

* Навчання персоналу:
* Правила роботи з інформацією
* Політика інформаційної безпеки
* Конфіденційність

1. Резервне копіювання:

* Регулярне резервне копіювання даних:
* Локальні резервні копії.

**ВИСНОВОК**

Інформаційні ресурси є одним з найважливіших активів будь-якого підприємства. Вони включають в себе дані про клієнтів, фінансову інформацію, комерційну таємницю, програмне забезпечення та інші цінні відомості. Втрата або витік інформації може призвести до серйозних наслідків для підприємства, таких як: фінансові втрати, втрата репутації, зниження конкурентоспроможності, юридичні проблеми та штрафи.

Для захисту інформаційних ресурсів від ризиків витоку, втрати або несанкціонованого доступу, підприємствам рекомендується вживати таких заходів:

* Розробка та впровадження політики інформаційної безпеки;
* Вживання заходів для фізичного захисту інформації;
* Використання методів та засобів інформаційної безпеки;
* Навчання персоналу правилам роботи з інформацією;
* Регулярне оновлення програмного забезпечення;
* Здійснення резервного копіювання даних.

Захист інформаційних ресурсів є важливою задачею для будь-якого підприємства, використання комплексного підходу дозволить мінімізувати ризики та втрати.

**Лабораторна робота № 2**

**ІДЕНТИФІКАЦІЯ НЕБЕЗПЕЧНИХ ЧИННИКІВ НА ОБ’ЄКТ ЗАХИСТУ**

**Мета роботи:** придбання опанування практичних навичок з визначення та ідентифікації загроз для обраного об’єкта захисту.

**Завдання**

1. До інформаційних ресурсів та інформаційних потоків (визначених у попередній лабораторній роботі) визначити перелік загроз.

2. Визначити відповідно до інформаційної системи, що розглядається, ймовірність виникнення кожної загрози за шкалою: висока, середня, низька. Обґрунтуйте свою оцінку.

**РОЗДІЛ 2. ІДЕНТИФІКАЦІЯ НЕБЕЗПЕЧНИХ ЧИННИКІВ НА ОБ’ЄКТ ЗАХИСТУ**

**2.1 Перелік загроз, ймовірність виникнення загроз та обґрунтування оцінки для інформаційних потоків**

Загрози інформаційних потоків

1) Замовлення на ремонт (клієнт -> приймальня).

Загрози:

* порушення режиму роботи джерел живлення;
* виникненням технічних несправностей елементів засобів;
* підслуховування ІзОД (інформація з обмеженим доступом) сторонніми особами;
* читання даних з екрану або читання документів, які залишені без нагляду сторонніми особами;
* крадіжка документів або пристроїв з сервісного центру;
* підкуп і шантаж співробітників;
* підпали;
* атака “людина посередині” (Man-in-the-Middle) під час заповнення форми на сайті;
* фішинг (зловмисники можуть відправляти фішингові повідомлення або створювати фішингові веб-сайти для отримання конфіденційної інформації від клієнтів);
* DoS-атака або DDoS-атака (тимчасова недоступність системи, як результат втрата клієнтів);
* розкриття конфіденційних даних клієнтів приймальниками (використання даних клієнта без їх дозволу).

2) Передання пристрою клієнта до майстерні (приймальня -> майстерня).

Загрози:

* крадіжка пристрою сторонніми особами;
* ненавмисне пошкодження пристрою;
* порушення приватності або неетичне поводження з пристроєм клієнта;

3) Передавання деталей у майстерню (склад запчастин -> майстерня).

Загрози:

* ненавмисне постачання неякісних деталей (вони можуть мати вразливості, які можуть бути використані зловмисниками для виконання атак).

4) Оплата за послуги (приймальня -> клієнт).

Загрози:

* спостереження за введенням ПІН-коду клієнта сторонніми особами;
* недбале збереження або неправильне утилізація даних про фінансові дані клієнтів;

5) Написання звітності про виконання робіт (майстерня -> адміністрація).

Загрози:

* маніпуляція даними для власної вигоди (щоб приховати факти або створити фальшиве враження про виконану роботу);
* ненавмисне видалення, редагування даних у звіті;
* несанкціонований доступ до даних;
* поломки або аварії пристрою при написанні звітності.

6) Написання звітності про клієнтів (приймальня -> адміністрація).

Загрози:

* несанкціонований доступ до даних;
* витік конфіденційної інформації;
* маніпуляція даними для власної вигоди;
* поломки або аварії пристрою при написанні звітності.

Таблиця 2.1 – Ймовірність загроз інформаційних потоків

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Загроза** | **К** | **Ц** | **Д** | **С** | **Рівень ризиків** | **Рівень збитків** | **Сума загроз** |
| 1 | Порушення режиму роботи джерел живлення |  | + | + |  | 2 | 1 | 3 |
| 2 | Виникненням технічних несправностей елементів засобів |  | + | + |  | 1 | 1 | 2 |
| 3 | Підслуховування ІзОД сторонніми особами | + |  |  |  | 1 | 2 | 3 |
| 4 | Читання даних з екрану або читання документів, які залишені без нагляду сторонніми особами | + |  |  |  | 1 | 1 | 2 |
| 5 | Крадіжка документів або пристроїв з сервісного центру | + |  | + |  | 1 | 1 | 2 |
| 6 | Підкуп і шантаж співробітників | + | + | + |  | 2 | 2 | 4 |
| 7 | Атака “людина посередині” (Man-in-the-Middle) | + | + |  |  | 1 | 2 | 3 |
| 8 | Фішинг | + |  |  |  | 1 | 2 | 3 |
| 9 | Розкриття конфіденційних даних клієнтів | + |  |  |  | 1 | 2 | 3 |
| 10 | DoS-атака або DDoS-атака |  |  | + |  | 2 | 2 | 4 |
| 11 | Ненавмисне пошкодження пристрою |  | + | + |  | 1 | 1 | 2 |
| 12 | Порушення приватності або неетичне поводження з пристроєм клієнта | + |  |  |  | 1 | 2 | 3 |
| 13 | Ненавмисне постачання неякісних деталей |  | + | + |  | 1 | 1 | 2 |
| 14 | Спостереження за введенням ПІН-коду клієнта сторонніми особами | + |  |  |  | 1 | 2 | 3 |
| 15 | Недбале збереження або неправильне утилізація даних | + |  |  |  | 1 | 2 | 3 |
| 16 | Маніпуляція даними для власної вигоди |  | + |  |  | 1 | 2 | 3 |
| 17 | Ненавмисне видалення, редагування даних у звіті | + |  |  |  | 1 | 1 | 2 |
| 18 | Несанкціонований доступ до даних | + | + |  |  | 2 | 3 | 5 |

Пояснення до таблиці

1. Скорочення:

* К (конфіденційність)
* Ц (цілісність)
* Д (доступність)
* С (спостережність)

1. Шкала для визначення ймовірність виникнення загроз:

* Низький (Н) - 1 бал
* Середній (С) - 2 бали
* Високий (В) - 3 бали

Обґрунтування оцінки загроз інформаційних потоків

1. Порушення режиму роботи джерел живлення:

* рівень ризиків середній, оскільки відключення електропостачання, які стали доволі частими у наш час, можуть призвести до втрати даних та пошкодження обладнання через короткі замикання; рівень збитків низький, оскільки на підприємстві є додаткові джерела живлення та система резервного копіювання даних.

1. Виникненням технічних несправностей елементів засобів:

* рівень ризиків низький, оскільки проводиться регулярне технічне обслуговування, використовується якісне обладнання та є дотримання правил експлуатації; рівень збитків низький, оскільки дані можуть бути відновлені з резервних копій та обладнання може бути відремонтовано або замінене.

1. Підслуховування ІзОД сторонніми особами:

* рівень ризиків низький, оскільки наслідки підслуховування можуть бути несуттєвими, якщо дані не є конфіденційними, також проводиться шифрування даних; рівень збитків середній, оскільки це може призвести до розкриття конфіденційної інформації та втрати репутації.

1. Читання даних з екрану або читання документів, які залишені без нагляду сторонніми особами:

* рівень ризиків низький, оскільки співробітники обізнані та документи зберігаються в сейфах; рівень збитків низький, оскільки дані можуть бути не конфіденційними.

1. Крадіжка документів або пристроїв з сервісного центру:

* рівень ризиків низький, оскільки вжиті заходи з фізичної безпеки; рівень збитків низький, оскільки є резервні копії даних.

1. Підкуп і шантаж співробітників:

* рівень ризиків середній, оскільки проводиться моніторинг доступу до даних та навчання персоналу; рівень збитків середній, оскільки це залежати від типу та обсягу розкритої інформації.

1. Атака Man-in-the-Middle:

* рівень ризиків низький, оскільки є шифрування даних та з’єднання здійснюється через віртуальну приватну мережу (VPN); рівень збитків середній, оскільки може призвести до розкриття конфіденційної інформації, репутаційних втрат та фінансових збитків.

1. Фішинг:

* рівень ризиків низький, оскільки проводиться навчання персоналу, є фільтрація спаму та блокування підозрілих URL-адрес; рівень збитків середній, оскільки це може призвести до розкриття конфіденційної інформації.

1. Розкриття конфіденційних даних клієнтів:

* рівень ризиків низький, оскільки є контроль доступу та політики конфіденційності; рівень збитків середній оскільки це може призвести до розкриття конфіденційної інформації.

1. DoS-атака або DDoS-атака:

* рівень ризиків середній, оскільки проходять навчання персоналу, але існує ймовірність успішної атаки, також ця атака може призвести до відмови в обслуговуванні для клієнтів; рівень збитків середній, оскільки ця атака може призвести до фінансових витрат та втрату клієнтів.

1. Ненавмисне пошкодження пристрою:

* рівень ризиків низький, оскільки пошкодження пристрою можуть бути несуттєвими; рівень збитків низький, оскільки пристрій можна відремонтувати самостійно.

1. Порушення приватності або неетичне поводження з пристроєм клієнта:

* рівень ризиків низький, оскільки вжито заходів для захисту приватності клієнтів; рівень збитків середній, оскільки можуть призвести до втрати довіри клієнтів.

1. Ненавмисне постачання неякісних деталей:

* рівень ризиків низький, оскільки вжито заходів для контролю якості деталей; рівень збитків низький, оскільки неякісні деталі можуть бути повернені або замінені та витрати на ремонт можуть бути незначними.

1. Спостереження за введенням ПІН-коду клієнта сторонніми особами:

* рівень ризиків низький, оскільки вжито заходів для захисту ПІН-кодів клієнтів; рівень збитків середній, оскільки це може призвести до крадіжки коштів клієнта.

1. Недбале збереження або неправильне утилізація даних:

* рівень ризиків низький, оскільки присутнє навчання персоналу правилам поводження з даними; рівень збитків середній, оскільки є резервні копії.

1. Маніпуляція даними для власної вигоди:

* рівень ризиків низький, оскільки вжито заходів для захисту даних, наслідки можуть бути несуттєвими та проводиться аудит; рівень збитків середній, оскільки може призвести до фінансових витрат, втрати репутації.

1. Ненавмисне видалення, редагування даних у звіті:

* рівень ризиків низький, оскільки наслідки цієї загрози є несуттєвими; рівень збитків низький, оскільки дані можна відновити за допомогою резервних копій.

1. Несанкціонований доступ до даних:

* рівень ризиків середній, оскільки існує ймовірність успішного несанкціонованого доступу до даних, також може бути розкрита конфіденційна інформація; рівень збитків високий, оскільки може призвести до втрати довіри клієнтів, до репутаційних збитків та фінансових втрат.

**2.2 Перелік загроз, ймовірність виникнення загроз та обґрунтування оцінки для інформаційних ресурсів**

Загрози інформаційних ресурсів

1. Дані про клієнтів:

Загрози:

* Несанкціонований доступ до бази даних через несправний VPN або атаки на сервер можуть призвести до витоку особистих даних клієнтів.
* Ризик втрати даних внаслідок вірусів, атак або несправностей на сервері, якщо резервні копії не будуть доступні або пошкоджені.

1. Дані про виконання робіт:

Загрози:

* Ризик витоку конфіденційної інформації про ремонт та пристрої.
* Втрата даних через технічні проблеми або атаки на сервер.

1. Дані про запчастини:

Загрози:

* Ризик несанкціонованого доступу до даних про запчастини з метою зламування системи або здійснення крадіжок.
* Можливість зміни даних про запчастини або їх кількість зловмисниками.

1. Фінансова документація:

Загрози:

* Ризик несанкціонованого доступу до фінансових даних або зміни фінансових звітів з метою шахрайства або фінансового шкодування.

1. Технічна документація:

Загрози:

* Втрата або пошкодження паперових документів через природні чи технічні катастрофи.
* Ризик кібератак на хмарне сховище або несправностей в системі, що може призвести до втрати електронних документів.
* Крадіжка паперових документів.

1. Інші документи:

Загрози:

* Порушення конфіденційності ліцензій, страхових полісів та сертифікатів через несанкціонований доступ або втрату даних.

Таблиця 2.2 – Ймовірність загроз інформаційних ресурсів

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Загроза** | **К** | **Ц** | **Д** | **С** | **Рівень ризиків** | **Рівень збитків** | **Сума загроз** |
| 1 | Несанкціонований доступ до БД | + | + |  |  | 2 | 2 | 4 |
| 2 | Втрати даних внаслідок вірусів, атак або несправностей на сервері | + | + | + |  | 2 | 2 | 4 |
| 3 | Втрата або пошкодження паперових документів через природні чи технічні катастрофи |  | + | + | + | 1 | 2 | 3 |
| 4 | DoS-атака або DDoS-атака |  |  | + |  | 2 | 2 | 4 |
| 5 | Фішинг | + |  |  |  | 2 | 2 | 4 |
| 6 | SQL-ін'єкції |  | + | + |  | 2 | 2 | 4 |
| 7 | Кібератаки на сервери | + | + | + | + | 2 | 3 | 5 |
| 8 | Модифікація даних зловмисниками | + | + |  |  | 2 | 2 | 4 |
| 9 | Крадіжка паперових документів | + |  | + |  | 1 | 2 | 3 |

Обґрунтування оцінки загрози інформаційних ресурсів

1. Несанкціонований доступ до БД:

* Рівень ризику середній, ця загроза може мати серйозні наслідки для організації, включаючи витік конфіденційної інформації, порушення цілісності даних та обмеження доступу до систем.

1. Втрати даних внаслідок вірусів, атак або несправностей на сервері:

* Рівень ризику середній, ця загроза може призвести до втрати даних та обмеження доступу до систем, але наслідки можуть бути меншими, якщо існують ефективні заходи захисту.

1. Втрата або пошкодження паперових документів через природні або технічні катастрофи:

* Рівень ризику низький, хоча ця загроза може призвести до втрати або пошкодження документів, наслідки можуть бути менш серйозними, якщо існують засоби резервного копіювання та відновлення даних.

1. DoS-атака або DDoS-атака:

* Рівень ризику середній, ця загроза може призвести до відмови в обслуговуванні і значно обмежити доступність системи для користувачів, але впроваджені заходи захисту від відомих атак.

1. Фішинг:

* Рівень ризику середній, ця загроза може бути небезпечною, оскільки може призвести до витоку конфіденційної інформації, але наслідки можуть бути менш серйозними, якщо користувачі виявлять підозрілу активність.

1. SQL-ін'єкції:

* Рівень ризику середній, ця загроза може призвести до витоку конфіденційної інформації та порушення цілісності даних, але наслідки можуть бути менш серйозними, якщо існують ефективні заходи захисту.

1. Кібератаки на сервери:

* Рівень ризику середній, ця загроза може мати серйозні наслідки для конфіденційності, цілісності та доступності даних, і вимагає негайних заходів захисту та реагування.

1. Модифікація даних зловмисниками:

* Рівень ризику середній, бо ця загроза може призвести до втрати репутації, фінансових втрат, але впроваджено шифрування і резервне копіювання даних.

1. Крадіжка паперових документів:

* Рівень ризику низький, бо документи зберігаються у сейфах.

**2.3 Перелік загроз, ймовірність виникнення загроз та обґрунтування оцінки для носіїв інформації**

Загрози носіїв інформації

1. База даних клієнтів

Загрози:

* Несанкціонований доступ до БД,
* Підключення з незареєстрованого пристрою,
* DDoS-атака,
* SQL-ін'єкції,
* Кібератаки (шкідливе ПЗ).

1. База даних запчастин

Загрози:

* Несанкціонований доступ до БД,
* Підключення з незареєстрованого пристрою,
* DDoS,
* SQL-ін'єкції,
* Кібератаки (шкідливе ПЗ),

1. База даних про виконання робіт

Загрози:

* Несанкціонований доступ до БД,
* Підключення з незареєстрованого пристрою,
* Втрата даних через світло / DDoS,
* SQL-ін'єкції,
* Кібератаки (шкідливе ПЗ).

1. Електронна звітність

Загрози:

* Несанкціонований доступ з неавторизованого пристрою у разі викрадення ЕЦП.

1. Бухгалтерська звітність

Загрози:

* Несанкціонований доступ з неавторизованого пристрою у разі викрадення ЕЦП,
* Кібератаки на сервіс.

1. Архіви

Загрози:

* Викрасти документи,
* Стихійні лиха, пожежі.

1. Сервери

Загрози:

* Викрадення серверу,
* Знеструмлення будівлі,
* Стихійні лиха,
* Втрата даних через людську помилку,
* Dos-атака.

1. Електронні заявки клієнтів

Загрози:

* Створення непотрібних заявок,
* SQL-ін'єкції,
* Кібератаки (шкідливе ПЗ).

1. Інформація про працівників (особові справи)

Загрози:

* Можуть бути викрадені для рекрутингу.

Таблиця 2.3 – Ймовірність загроз носіїв інформації

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Загроза** | **К** | **Ц** | **Д** | **С** | **Рівень ризиків** | **Рівень збитків** | **Сума загроз** |
| 1 | Несанкціонований доступ до БД | + | + |  |  | 2 | 2 | 4 |
| 2 | Підключення з незареєстрованого пристрою | + | + |  |  | 2 | 1 | 3 |
| 3 | DDoS-атака |  |  | + |  | 1 | 1 | 1 |
| 4 | SQL-ін'єкції | + | + | + |  | 2 | 2 | 4 |
| 5 | Кібератаки (шкідливе ПЗ) |  | + |  | + | 2 | 2 | 4 |
| 6 | Несанкціонований доступ з неавторизованого пристрою у разі викрадення ЕЦП | + |  |  | + | 2 | 2 | 4 |
| 7 | Викрадення документів |  | + | + |  | 1 | 1 | 2 |
| 8 | Викрадення серверу |  | + | + |  | 1 | 2 | 3 |
| 9 | Знеструмлення будівлі |  |  | + |  | 1 | 1 | 2 |
| 10 | Стихійні лиха, пожежі |  | + | + | + | 1 | 1 | 2 |
| 11 | Втрати даних через людську помилку |  | + |  |  | 1 | 1 | 2 |
| 12 | Створення непотрібних заявок |  | + | + | + | 1 | 1 | 2 |

Обґрунтування оцінки загрози носіїв інформації

1. Несанкціонований доступ до БД:

* Рівень ризику середній, бо у разі виникнення такої ситуації зловмисник буде мати повний контроль над даними, та тоді збитки будуть досить великі, хоча вжито достатні методи для захисту БД.

1. Підключення з незареєстрованого пристрою:

* Рівень ризику середній, бо у разі виникнення такої ситуації це буде означати, що файервол не працює, та скоріше за все хтось має контроль над мережею, рівень збитків не великий, бо якщо людина лише з’явилась у мережі це не означає, що вона щось зможе зробити у мережі.

1. DDoS-атака:

* Рівень ризику досить низький, бо дані копіюються кожного дня, та у разі атаки ми не будемо мати дані лише на 1 день.

1. SQL-ін'єкції:

* Рівень ризику високий, бо у разі виникнення такої ситуації - зловмисник отримує повний контроль над БД, хоча вжито заходів для захисту баз даних.

1. Кібератаки (шкідливе ПЗ):

* Рівень ризику середній, та стосовно рівня збитків – теж може бути середнім оскільки не відомо на скільки масштабна може бути атака та на скільки вона може вдарити по репутації.

1. Несанкціонований доступ з неавторизованого пристрою у разі викрадення ЕЦП:

* Рівень ризику середній, оскільки у разі отримання ЕЦП та знаючи пароль можна зробити будь що з підприємством.

1. Викрадення документів:

* Рівень ризику низький, бо є паперова версія документів, хоча у разі виникнення такої ситуації є електронні копії та стосовно заходів безпеки - документи знаходяться у сейфі.

1. Викрадення серверу:

* Рівень ризику низький оскільки досить складно отримати доступ до серверу, хоча у разі виникнення - збитки можуть бути великі, оскільки все зберігається на сервері.

1. Знеструмлення будівлі:

* Рівень ризику низький, рівень збитків також низький, бо можна зробити автономне живлення, або якщо це одноразово - сервіс не буде працювати день.

1. Стихійні лиха, пожежі:

* Рівень ризику низький, бо будівля знаходиться у достатньо безпечному місці та всі документи та носії інформації знаходяться у безпечному місці.

1. Втрати даних через людську помилку:

* Рівень ризику маленький, оскільки все автоматизовано, та у разі помилки є бекапи.

1. Створення непотрібних заявок:

* Рівень ризику маленький, оскільки заявки валідуються менеджером вручну.

**2.4 Сумарна таблиця загроз для інформації**

Таблиця 2.4 – Сумарна таблиця загроз для інформації

|  |  |  |  |
| --- | --- | --- | --- |
| **Критерій** | **Загальна сума з табл. 2.1** | **Загальна сума з табл. 2.2** | **Загальна сума з табл. 2.3** |
| Конфіденційність | 12 | 4 | 6 |
| Цілісність | 8 | 9 | 6 |
| Доступність | 7 | 7 | 5 |
| Спостережність | 0 | 4 | 2 |

В таблиці 2.1 «Загрози інформаційних потоків» зазначено, що найбільш значущими загрозами для інформаційних потоків є загрози для конфіденційності. Загрози для цілісності та доступності також є важливими, але їх вплив зазвичай менш значний. А загрози для спостережності самі по собі не є значними, але можуть бути використані для посилення інших загроз.

В таблиці 2.2 «Загрози носіїв інформації» зазначено, що найбільш значущими загрозами для носіїв інформації є загрози для цілісності. Загрози для доступності також є важливими, але їх вплив менш значний. А загрози для конфіденційності та спостережності самі по собі не є значними.

В таблиці 2.3 «Загрози інформаційних ресурсів» зазначено, що найбільш значущими загрозами для інформаційних ресурсів є загрози для конфіденційності та цілісності. Загрози для доступності та спостережності також є важливими, але їх вплив менш значний.

ВИСНОВОК

Загроза – це подія або дія, яка може призвести до шкоди або втрати для активу. В контексті інформаційної безпеки, загрози можуть бути спрямовані на:

* конфіденційність: розкриття інформації несанкціонованим особам;
* цілісність: пошкодження або знищення даних;
* доступність: порушення доступу до інформаційних систем або даних;
* спостережність: здатність системи збирати, зберігати та аналізувати дані.

Визначення ймовірності виникнення загроз допомагає приймати обґрунтовані рішення щодо пріоритетів у сфері інформаційної безпеки, ефективно використовувати ресурси на заходи з захисту інформації, та знизити ризик виникнення інцидентів інформаційної безпеки.

В даній лабораторній роботі, було проведено аналіз інформаційних ресурсів, інформаційних потоків та носіїв інформації для сервісного центру з ремонту комп’ютерів, також визначено загрози та оцінку ймовірності.

Важливо пам'ятати, що визначення ймовірності виникнення загроз може змінюватися з часом, тому потрібно регулярно переглядати оцінку ймовірності виникнення загроз.

**Лабораторна робота № 3**

**МОДЕЛЬ ПОРУШНИКА**

**Мета роботи:** ознайомитись з основними моделями порушників та їх класифікацією.

**Завдання**

1. Визначити зовнішні і внутрішні групи порушників на підприємстві.
2. Обґрунтувати можливі мотиви порушень на підприємстві.
3. Розробити модель порушника, спираючись на прикладах, що розглянуті на лекційному занятті за темою «Модель порушника безпеки інформації в КС». Пріоритетними є приклади 1 та 2.
4. Результат виконання лабораторної роботи представити у вигляді звіту.

**РОЗДІЛ 3. МОДЕЛЬ ПОРУШНИКА**

**3.1 Зовнішні і внутрішні групи порушників на підприємстві**

Для об’єкту «Сервісний центр з ремонту комп’ютерів» розробляється КСЗІ. Було виділено зовнішні та внутрішні порушники. Потім наводиться опис порушників.

Зовнішній порушник – це порушник, що дiє iз зовнiшнього щодо боку. У цiй моделі розглядається особа, що не має доступу до приміщень, у яких розташовані засоби комп’ютерної технiки, i не є авторизованим користувачем. Зовнiшнiй порушник має можливiсть реалiзувати загрозу iнформацiї тiльки впливаючи на інформацію з боку інших автоматизованих систем (що не входять до складу).

Категорії осiб, якi можуть бути зовнiшнiми порушниками:

* Конкуренти сервісного центру
* Хакери та кіберзлочинці
* Незадоволені клієнти
* Відвідувачі
* Незадоволені колишні співробітники
* Кур’єри
* Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)
* Шахраї
* Будь-які особи за межами контрольованої зони.

Внутрішній порушник – це порушник, що діє зсередини. У цiй моделi розглядається особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної технiки . Внутрішній порушник має можливість реалізувати загрозу iнформацiї й може бути як авторизованим користувачем, так i неавторизованим.

Категорії осiб, якi можуть бути внутрішніми порушниками:

* Системний адміністратор
* Завідувач складом
* Бухгалтер
* Майстри
* Приймальник
* Керівник
* Прибиральник
* Технічний персонал, який обслуговує будови та приміщення (електрики та сантехніки)
* Постачальники деталей.

**3.2 Модель порушника**

Визначення категорії порушників, що визначені в моделi, узагальнено й подано в таблиці 3.1. У таблицях 3.2 - 3.6 узагальнено й подано специфiкацiї моделi порушника за мотивами здiйснення порушень, за рiвнем квалiфiкацiї та обізнаності щодо ІТС, за показником можливостей використання засобів та методів подолання системи захисту, за часом дiї, за мiсцем дiї. У графi «Рiвень загроз» зазначених таблиць наведено рейтингову оцiнку загроз порушника (можливих збиткiв). Рiвень загрози характеризуеться такими категоріями:

1 – незначний (низький);

2 – нижчий за середнiй;

3 – середній;

4 – вищий за середнiй;

5 – значний (високий).

В таблиці 3.7 подано модель порушника політики безпеки інформації.

Таблиця 3.1 – Категорії порушників, визначених у моделі

|  |  |  |
| --- | --- | --- |
| **Позначення** | **Визначення категорії** | **Рівень загроз** |
| *Внутрішні по відношенню до ІТС* | | |
| ПВ1 | Системний адміністратор | 5 |
| ПВ2 | Завідувач складом | 3 |
| ПВ3 | Бухгалтер | 5 |
| ПВ4 | Майстри | 4 |
| ПВ5 | Приймальник | 3 |
| ПВ6 | Керівник | 5 |
| ПВ7 | Прибиральник | 2 |
| ПВ8 | Технічний персонал, який обслуговує будови та  приміщення (електрики та сантехніки) | 1 |
| ПВ9 | Постачальники деталей | 4 |
| *Зовнішні по відношенню до ІТС* | | |
| ПЗ1 | Конкуренти сервісного центру | 4 |
| ПЗ2 | Хакери та кіберзлочинці | 5 |
| ПЗ3 | Незадоволені клієнти | 3 |
| ПЗ4 | Відвідувачі | 2 |
| ПЗ5 | Незадоволені колишні співробітники | 3 |
| ПЗ6 | Кур’єри | 2 |
| ПЗ7 | Представники організацій, що взаємодіють з  питань технічного забезпечення (енерго-, водо-,  теплопостачання і таке інше) | 3 |
| ПЗ8 | Шахраї | 3 |
| ПЗ9 | Будь-які особи за межами контрольованої зони | 2 |

Таблиця 3.2 – Специфікація моделі порушника за мотивами здійснення порушень

|  |  |  |
| --- | --- | --- |
| **Позначення** | **Мотив порушення** | **Рівень загроз** |
| М1 | Безвідповідальність | 1 |
| М2 | Самоствердження | 2 |
| М3 | Корисливий інтерес | 3 |
| М4 | Професійний обов’язок | 4 |
| М5 | Вимагання і шантаж | 3 |
| М6 | Соціальний або політичний мотив | 4 |

Таблиця 3.3 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

|  |  |  |
| --- | --- | --- |
| **Позначення** | **Основні кваліфікаційні ознаки порушник** | **Рівень загроз** |
| К1 | Немає знань та iнформацiї про порядок функцiонування , без навичок щодо користування штатними засобами системи | 1 |
| К2 | Має навички щодо користування ПК на рiвнi користувача | 2 |
| К3 | Володiє базовими знаннями функцiонування ПЗ й ОС i  практичними навичками роботи iз засобами, що  реалiзованi у | 4 |
| К4 | Має знання щодо функцiонування засобiв i механiзмiв захисту, що використовуються у , та їх недолiки | 5 |

Таблиця 3.4 − Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

|  |  |  |
| --- | --- | --- |
| **Позначення** | **Характеристика можливостей порушника** | **Рівень загроз** |
| З1 | Володіє фiзичним доступом до автоматизованого робочого мiсця , але не є авторизованим користувачем | 1 |
| З2 | Має можливість запуску фіксованого набору завдань  (програм), що реалізують заздалегідь передбачені функції обробки інформації | 3 |
| З3 | Має можливість керування функціонуванням елементів , тобто конфігурує програмне забезпечення та комплекс засобів захисту | 5 |
| З4 | Немає фізичного доступу до ресурсів | 1 |
| З5 | Застосовує дистанційні методи розвідки | 3 |

Таблиця 3.5 − Специфікація моделі порушника за часом дії

|  |  |  |
| --- | --- | --- |
| **Позначення** | **Характеристика за часом дії порушника** | **Рівень загроз** |
| Ч1 | Пiд час бездiяльностi компонентiв системи (пiд час планових перерв у роботi, у неробочий час) | 4 |
| Ч2 | Пiд час функцiонування | 5 |
| Ч3 | Пiд час перерв у роботi для обслуговування та ремонту | 3 |
| Ч4 | До впровадження систем захисту інформації | 1 |

Таблиця 3.6 − Специфікація моделі порушника за місцем дії

|  |  |  |
| --- | --- | --- |
| **Позначення** | **Характеристика місця дії порушника** | **Рівень загроз** |
| Д1 | Усерединi будiвлi та примiщень, але без доступу до  технiчних засобiв | 1 |
| Д2 | Усерединi будiвлi та примiщень, з доступу до  технiчних засобiв | 3 |
| Д3 | З робочих місць працівників | 5 |
| Д4 | З iнших об'єктiв , у тому числi каналів зв'язку | 2 |
| Д5 | З доступом у зони даних (баз даних, архівів й т.ін.) | 5 |

Таблиця 3.7 − Модель порушника політики безпеки інформації

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Категорія** | **Характеристики дій порушника** | | | | | **Рівень загроз** |
| **Мотив порушення** | **Кваліфікація** | **Можливості** | **Час дії** | **Місце дії** |
| *Внутрішні по відношенню до ІТС* | | | | | | |
| Системний адміністратор | М3 | К3 | З3 | Ч1-Ч4 | Д2 - Д4, Д5 | 5 |
| Завідувач складом | М3, М5 | К2 | З2 | Ч2 | Д1, Д4 | 3 |
| Бухгалтер | М1, М3 | К2, К3 | З2 | Ч1, Ч2 | Д3, Д4 | 5 |
| Майстри | М1, М4 | К2, К3 | З2 | Ч2 | Д1, Д3, Д4 | 4 |
| Приймальник | М1, М3 | К2, К23 | З2 | Ч2 | Д1, Д4 | 3 |
| Керівник | М1 | К2, К3 | З2 | Ч2 | Д1, Д4, Д5 | 5 |
| Прибиральник | М1, М4 | К2 | З1 | Ч1-Ч3 | Д1, Д4 | 2 |
| Технічний персонал, який обслуговує будови та  приміщення (електрики та сантехніки) | М4 | К2 | З1 | Ч1-Ч3 | Д1, Д4 | 1 |
| Постачальники деталей | М1 | К2 | З4 | Ч2 | Д1, Д4 | 4 |
| *Зовнішні по відношенню до ІТС* | | | | | | |
| Конкуренти сервісного центру | М3 | К3, К4 | З4 | Ч2 | Д1, Д4 | 4 |
| Хакери та кіберзлочинці | М3 - М5 | К4 | З4, З5 | Ч2 | Д1, Д4 | 5 |
| Незадоволені клієнти | М2, М6 | К2, К3 | З4 | Ч2 | Д1, Д4 | 3 |
| Відвідувачі | М2 | К1, К2 | З4 | Ч2 | Д1, Д4 | 2 |
| Незадоволені колишні співробітники | М2 | К1, К2 | З4 | Ч2 | Д1, Д4 | 3 |
| Кур’єри | М1 | К1, К2 | З4 | Ч2 | Д1, Д4 | 2 |
| Представники організацій, що взаємодіють з  питань технічного забезпечення (енерго-, водо-, теплопостачання) | М4 | К2 | З1 | Ч2, Ч4 | Д1, Д4 | 3 |
| Шахраї | М3 - М5 | К2-К4 | З1, З5, З4 | Ч2 | Д1, Д4 | 3 |
| Будь-які особи за межами контрольованої зони | М6 | К1-К4 | З4 | Ч2 | Д4 | 2 |

З останньої таблиці видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить системний адміністратор ІТС. Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

ВИСНОВОК

В даній лабораторній роботі, було розглянуто основні моделі порушників та їх класифікація. Було визначено зовнішні і внутрішні групи порушників на підприємстві “Сервісний центр з ремонту комп’ютерів” та обґрунтовано можливі мотиви порушень на підприємстві. Також, розробили модель порушника, і визначили хто становить найбільшу загрозу для підприємства.

Результати розробки моделі порушника дозволили нам визначити потенційно небезпечних осіб та головні ризики для підприємства. Проте, для ефективної реалізації заходів з запобігання порушенням і забезпечення безпеки підприємства необхідно постійно вдосконалювати моніторинг та аналіз діяльності персоналу, залучати зацікавлених сторін і вдосконалювати стратегії відповіді на можливі загрози.

**Лабораторна робота №4**

**РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**Мета роботи:** набуття досвіду зі створення політики інформаційної безпеки.

**Завдання**

1. Вхідними даними лабораторної роботи є критичні напрями захисту та основні небезпечні чинники, які студент має визначити відповідно до результатів виконання попередніх лабораторних робіт. Вхідні дані коротко резюмувати у звіті.

2. Написати власне розділи політики інформаційної безпеки, які стосуються критичних напрямів. Розроблені розділи політики інформаційної безпеки повинні бути достатніми стосовно загроз високої та середньої ймовірності виникнення та передбачати правила захисту від загроз низької ймовірності виникнення.

3. Зробити загальні висновки з виконаної роботи, де визначити подальші дії щодо розробки повної політики інформаційної безпеки та кроки у випадку перегляду політики інформаційної безпеки внаслідок виникнення інциденту.

**РОЗДІЛ 4. РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**4.1 Загальні положення**

Забезпечення інформаційної безпеки є необхідною умовою для здійснення діяльності Сервісного центру з ремонту комп’ютерів (далі - СЦРК). Порушення інформаційної безпеки може призвести до серйозних наслідків, включаючи втрату довіри з боку клієнтів і зниження конкурентоспроможності. Основою заходів по забезпеченню режиму інформаційної безпеки адміністративного рівня, тобто заходів, що робляться керівництвом організації, є політика безпеки.

Під політикою безпеки розуміється сукупність документованих управлінських рішень, направлених на захист інформації і асоційованих з нею ресурсів. Політика безпеки СЦРК визначає основні напрями і вимоги по забезпеченню інформаційної безпеки СЦРК. Забезпечення безпеки інформації включає будь-яку діяльність, направлену на захист інформації і/або підтримуючої інфраструктури. Справжня політика інформаційної безпеки охоплює всі автоматизовані і телекомунікаційні системи, власником і користувачем яких є СЦРК.

Положення цього документа відносяться до всього штатного персоналу, тимчасових службовців і інших співробітників СЦРК, а також клієнтів СЦРК і третіх осіб, що мають доступ до автоматизованих і телекомунікаційних систем СЦРК.

**4.2 Глосарій**

**Політика інформаційної безпеки** - набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

**ПЗ (програмне забезпечення)** - сукупність програм системи оброблення інформації та програмних документів, необхідних для їх експлуатації.

**ІзОД (інформація з обмеженим доступом)** - інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону.

**TLS (Transport Layer Security)** - криптографічний протокол, що надає можливості безпечної передачі даних в інтернеті для навігації, отримання пошти, спілкування, обміну файлами, тощо.

**VPN (virtual private network)** - узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри.

**4.3 Мета, цілі та завдання політики**

4.3.1 Мета

* Визначення принципів управління ризиків пов’язаних із шпигунством.
* Визначення вимог для захисту підприємства від кібератак та шпигунства.
* Визначення дій, які потрібно виконати у разі виникнення інцидентів.

4.3.2 Цілі

* Забезпечення захисту інформаційних активів підприємства від зовнішніх загроз та загроз пов’язаних з навмисними або не навмисними діями співробітника установи
* Забезпечення ефективності функціонування СУІБ
* Попередження та мінімізація ризиків інформаційної безпеки, впровадження відповідних заходів для запобігання виникнення інцидентів.

4.3.3 Завдання

* Засад захисту інформаційних ресурсів підприємства
* Засад забезпечення надійності бізнес процесів підприємства
* Впровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки
* Впровадження процесного підходу до забезпечення інформаційної безпеки підприємства.

**4.4 Сфера застосування політики**

Сфера застосування політики охоплює всі аспекти діяльності сервісного центру з ремонту комп'ютерів.

Політика розповсюджується на всі підрозділи сервісного центру. Вона застосовується до всіх процесів, послуг, програмно-технічних рішень та проектів, які здійснюються сервісним центром. Ця політика є обов'язковою для всіх співробітників сервісного центру та будь-яких третіх сторін, з якими вони співпрацюють у сфері ремонту комп'ютерів.

Об'єктами регулятивного впливу є:

* Інформаційні ресурси, такі як дані про клієнтів, бази даних, нормативна документація тощо.
* Програмне забезпечення, включаючи системне та сервісне програмне забезпечення.
* Фізичні ресурси, які використовуються для роботи з комп'ютерами та іншим технічним обладнанням.
* Сервісні ресурси, наприклад, доступ до Інтернету, електронної пошти, телефонного зв'язку тощо.
* Кадровий ресурс, тобто співробітники сервісного центру.
* Треті сторони, які можуть бути залучені до надання послуг з ремонту комп'ютерів.

**4.5 Заходи захисту від загроз з середньою ймовірністю**

4.5.1 Захист інформаційних ресурсів від порушення режиму роботи джерел живлення

Необхідно вживати наступні заходи:

* Резервне живлення: Використання додаткових джерел живлення, таких як резервні акумулятори або генератори, може забезпечити безперебійну подачу енергії в разі відмови основного джерела живлення.
* Системи резервного живлення для даних центрів: Для великих інформаційних систем, таких як дата-центри, використовуються спеціальні системи резервного живлення, які можуть автоматично переключати живлення на альтернативні джерела в разі відмови основного джерела.
* Моніторинг та автоматизація: Важливо мати системи моніторингу, які можуть виявити відхилення у роботі джерел живлення та автоматично вжити заходів для їх виправлення.
* Фізичний захист: Забезпечення фізичного захисту джерел живлення від несанкціонованого доступу, такого як захищені приміщення або контроль доступу, може допомогти запобігти втручанням у їх роботу.

4.5.2 Захист інформаційних ресурсів від підкупу і шантажу співробітників

Необхідно вживати наступні заходи:

* Створення культури безпеки: Важливо розробити та просунути культуру безпеки серед співробітників, зосередивши увагу на важливості захисту конфіденційної інформації. Навчання персоналу про ризики підкупу і шантажу, а також про методи їх виявлення і запобігання, може значно зменшити загрозу.
* Перевірка перед прийняттям на роботу: Здійснення ретельних перевірок кандидатів перед їх наймом може допомогти у виявленні осіб з попереднім історією шахрайства або інших недоречностей.
* Розмежування доступу: Обмеження доступу до конфіденційної інформації тільки для необхідних співробітників може зменшити ризик витоку даних через підкуп або шантаж.
* Моніторинг активності: Використання систем моніторингу, які виявляють підозрілу або несправедливу активність співробітників, може допомогти вчасно виявити випадки підкупу чи шантажу.
* Строга політика санкцій: Встановлення чіткої політики щодо відповідальності за порушення безпеки даних, включаючи підкуп і шантаж, і застосування належних санкцій для порушників може створити ефективний стримувальний ефект.
* Конфіденційність та анонімність: Забезпечення можливості співробітникам повідомляти про підозрілу або неетичну поведінку анонімно може сприяти виявленню випадків підкупу або шантажу всередині організації.

4.5.3 Захист інформаційних ресурсів від DoS-атаки або DDoS-атаки

Необхідно вживати наступні заходи:

* Мережеві фільтри та файрволи: Використання мережевих фільтрів і файрволів для виявлення і блокування трафіку, що має ознаки DoS або DDoS атак, може допомогти зменшити їх вплив на інформаційні ресурси.
* Обмеження швидкості інтенсивності запитів: Встановлення обмежень на швидкість інтенсивності запитів від одного джерела може допомогти у виявленні та обмеженні впливу DoS або DDoS атак.
* Системи виявлення і запобігання інтранет-захоплення: Встановлення систем виявлення і запобігання інтранет-захоплення (IDS/IPS) може допомогти вчасно виявити та відвернути атаки DoS та DDoS.
* Планування та відновлення: Розроблення планів реагування на DDoS атаки і відновлення після їхнього завершення може допомогти зменшити час недоступності інформаційних ресурсів.

4.5.4 Захист інформаційних ресурсів від несанкціонованого доступу до даних

Необхідно вживати наступні заходи:

* Аутентифікація і авторизація: Використання сильних методів аутентифікації (наприклад, паролів, біометричних ідентифікаторів тощо) для перевірки особистості користувачів і авторизації доступу до даних тільки для осіб з відповідними правами доступу.
* Шифрування даних: Використання шифрування для захисту даних під час їх передачі по мережі і зберігання на пристроях. Шифрування даних унеможливлює несанкціонований доступ до них без належного ключа.
* Моніторинг доступу: Встановлення систем моніторингу, які виявляють та реєструють активність користувачів і сповіщають адміністраторів про підозрілу діяльність.
* Фізичний захист: Забезпечення фізичного захисту серверних приміщень та інших місць зберігання даних, включаючи контроль доступу і відеоспостереження.
* Регулярне оновлення програмного забезпечення: Проведення регулярних оновлень і патчів для всього програмного забезпечення, що використовується для обробки та зберігання даних, для запобігання використанню вразливостей.
* Тренінг персоналу: Навчання персоналу щодо методів захисту інформації, виявлення підозрілої діяльності та процедур реагування на інциденти безпеки даних.
* Строга політика доступу і контроль прав: Встановлення строгої політики доступу до даних і обмеження прав доступу до необхідного мінімуму для виконання робочих обов'язків.

4.5.5 Захист інформаційних ресурсів від несанкціонованого доступу до БД

Необхідно вживати наступні заходи:

* Аутентифікація і авторизація: Застосування сильних методів аутентифікації, таких як паролі, двофакторна аутентифікація або біометричні ідентифікатори, для перевірки особистості користувачів перед наданням доступу до БД. Крім того, важливо обмежувати права доступу кожного користувача до БД лише необхідним мінімумом для виконання їхніх робочих обов'язків.
* Шифрування даних: Використання шифрування для захисту даних у БД під час їх зберігання та передачі. Шифрування може унеможливити несанкціонованим особам читання або зміну даних, якщо вони незаконно отримають доступ до БД.
* Моніторинг активності: Встановлення систем моніторингу, які виявляють та реєструють активність користувачів в БД. Це дозволить вчасно виявляти підозрілу діяльність і реагувати на неї.
* Фізичний захист серверних приміщень: Забезпечення фізичного захисту серверних приміщень, де знаходяться БД, включаючи контроль доступу, відеоспостереження та інші заходи безпеки.
* Оновлення та патчі: Проведення регулярних оновлень та встановлення патчів для програмного забезпечення баз даних для заповнення вразливостей та забезпеченя високого рівня безпеки.
* Резервне копіювання і відновлення: Регулярне створення резервних копій даних БД і розробка планів відновлення в разі порушення безпеки або втрати даних.
* Навчання персоналу: Навчання персоналу щодо важливості захисту даних і правил безпеки, включаючи вимоги до паролів, захисту доступу та ідентифікації підозрілої діяльності.

4.5.6 Захист інформаційних ресурсів від підключення з незареєстрованого пристрою

Необхідно вживати наступні заходи:

* Мережевий доступ контролю: Встановіть механізми контролю доступу до мережі, такі як MAC-фільтрація, яка дозволить лише зареєстрованим пристроям отримувати доступ до мережі.
* Аутентифікація користувачів: Вимагайте аутентифікації користувача на всіх рівнях мережі, відбираючи доступ до ресурсів на основі ідентифікаторів користувачів і паролів.
* Внутрішні мережеві брандмауери: Встановіть мережеві брандмауери, які контролюють рух даних всередині мережі, і блокують спроби з'єднання з незареєстрованими пристроями.
* Моніторинг мережі: Використовуйте системи моніторингу мережі для виявлення незвичайної або недозволеної активності, що може вказувати на підключення незареєстрованих пристроїв.
* Централізований управління пристроями: Використовуйте системи централізованого управління пристроями для контролю за тим, які пристрої мають доступ до мережі і які дозволи.
* Оновлення політик безпеки: Періодично переглядайте та оновлюйте політики безпеки вашої мережі, включаючи правила щодо доступу та взаємодії з незареєстрованими пристроями.
* Навчання персоналу: Навчіть персонал розпізнавати потенційно небезпечні ситуації, пов'язані з підключенням незареєстрованих пристроїв, і надавайте їм інструкції щодо того, як реагувати на них.

4.5.7 Захист інформаційних ресурсів від SQL-ін'єкції

Необхідно вживати наступні заходи:

* Використання параметризованих запитів: Використовуйте параметризовані запити або підготовлені вирази для передачі параметрів до бази даних. Це дозволяє розділити дані від коду SQL, унеможливлюючи атакуючому впровадити шкідливий код.
* Валідація введених даних: Перевіряйте та валідуйте всі дані, які вводяться користувачами або отримуються з зовнішніх джерел, перед тим як вони будуть використані в запитах до бази даних. Це допоможе виявити та блокувати спроби SQL-ін'єкцій.
* Використання обмежених привілеїв: Надавайте обмежені привілеї доступу до бази даних для веб-додатків, які виконуються від імені користувача. Не використовуйте адміністративні або суперкористувацькі облікові записи в коді програм.
* Вимкнення виведення помилок на продакшн-серверах: Виведення помилок SQL на веб-сторінках може розкрити конфіденційну інформацію, яка може бути використана атакувачами для виконання SQL-ін'єкцій. Вимкніть виведення помилок або налаштуйте їх таким чином, щоб вони не розкривали конфіденційну інформацію.
* Використання механізмів захисту БД: Використовуйте вбудовані механізми захисту баз даних, такі як фаєрволи, обмеження доступу та моніторинг активності.
* Аудит безпеки: Проводьте регулярні аудити безпеки коду та інфраструктури для виявлення потенційних вразливостей SQL-ін'єкцій та інших загроз безпеці.

4.5.8 Захист інформаційних ресурсів від кібератак (шкідливе ПЗ)

Необхідно вживати наступні заходи:

* Антивірусне програмне забезпечення: Встановіть та підтримуйте актуальне антивірусне програмне забезпечення на всіх комп'ютерах та пристроях у мережі. Регулярно оновлюйте вірусні бази даних для ефективного виявлення і блокування шкідливих програм.
* Фаєрволи: Використовуйте фаєрволи для контролю трафіку в мережі та захисту від несанкціонованого доступу. Фаєрволи можуть блокувати небажаний трафік та захищати внутрішню мережу від зовнішніх загроз.
* Антишпигунське програмне забезпечення: Встановлення антишпигунського програмного забезпечення для виявлення і видалення шпигунського ПЗ, яке може намагатися витягти конфіденційні дані з вашої системи.
* Оновлення програмного забезпечення: Регулярно оновлюйте всі програми та операційні системи на комп'ютерах та пристроях. Часті оновлення включають у себе патчі, що виправляють вразливості, які можуть бути використані зловмисниками для вторгнення.
* Фішинговий захист: Навчіть персонал розпізнавати фішингові атаки та інші соціально інженерні методи, які можуть бути використані для введення шкідливого ПЗ в систему.
* Шифрування даних: Використовуйте шифрування для захисту конфіденційних даних, особливо під час їх передачі через мережу або зберігання на пристроях.
* Регулярні резервні копії даних: Регулярно робіть резервні копії важливих даних і зберігайте їх в безпечному місці. Це допоможе відновити дані в разі успішного вторгнення або атаки шкідливим ПЗ.

4.5.9 Захист інформаційних ресурсів від модифікації даних зловмисниками

Необхідно вживати наступні заходи:

* Шифрування даних: Використовуйте шифрування для захисту конфіденційних даних під час їх зберігання і передачі. Шифрування даних зробить їх нерозбірливими для зловмисників, які намагаються модифікувати їх.
* Цифровий підпис: Використовуйте цифрові підписи для перевірки цілісності даних. Цифровий підпис дає можливість перевірити, чи були дані модифіковані після їх підписання.
* Обмеження доступу: Обмежте доступ до даних тільки для авторизованих користувачів і встановіть строгі правила контролю доступу до важливих систем і ресурсів.
* Аудит і моніторинг: Встановіть системи аудиту та моніторингу, які будуть відстежувати активність користувачів і виявляти підозрілу діяльність, включаючи спроби модифікації даних.
* Регулярні аудити безпеки: Проводьте регулярні аудити безпеки для виявлення потенційних вразливостей, які можуть бути використані для модифікації даних зловмисниками.
* Резервне копіювання даних: Регулярно робіть резервні копії важливих даних і зберігайте їх в безпечному місці. Це допоможе відновити дані в разі успішного вторгнення або модифікації даних зловмисниками.

**4.6 Заходи захисту від загроз з низькою ймовірністю**

4.6.1 Захист інформаційних ресурсів від виникненням технічних несправностей елементів засобів

Захист інформаційних потоків від виникнення технічних несправностей елементів засобів є важливим завданням для забезпечення безпеки системи.

Для досягнення цієї мети необхідно вживати наступні заходи:

* Регулярне тестування та обслуговування обладнання: Проводити регулярні перевірки та обслуговування всіх елементів інформаційної системи, включаючи апаратне та програмне забезпечення, мережеві пристрої та канали зв'язку. Це дозволить виявити та усунути потенційні несправності до їх виникнення.
* Використання резервних копій: Регулярно створювати резервні копії даних та програмного забезпечення. Це дозволить відновити інформацію у випадку виникнення технічних несправностей.
* Застосування систем резервування: Впровадити системи резервування критичних компонентів інформаційної системи, таких як сервери, мережеві пристрої та канали зв'язку. Це дозволить забезпечити безперервну роботу інформаційної системи у випадку виходу з ладу одного з компонентів.
* План відновлення після аварії: Розробити та регулярно оновлювати план відновлення після аварії, який описує дії, необхідні для відновлення роботи інформаційної системи у випадку виникнення серйозної технічної несправності.

Контроль полягає у регулярній перевірці виконання заходів, описаних у цьому розділі, а також у аналізі даних про виникнення технічних несправностей та вживанні заходів для їх усунення, а також у оновленні плану відновлення після аварії відповідно до змін в інформаційній системі.

4.6.2 Захист інформаційних ресурсів від підслуховування ІзОД сторонніми особами

Необхідно вживати наступні заходи:

* Шифрування каналів зв'язку: Використовувати криптографічні методи для шифрування даних, що передаються по каналах зв'язку. Це дозволить зробити інформацію не доступною для сторонніх осіб, які не мають ключа дешифрування.
* Використання віртуальних приватних мереж (VPN): Застосовувати VPN для створення захищених віртуальних каналів зв'язку через незахищені мережі, такі як Інтернет.
* Фізичний захист каналів зв'язку: Забезпечити фізичний захист каналів зв'язку від несанкціонованого доступу, наприклад, шляхом прокладання кабелів в захищених місцях або використання оптоволоконних кабелів.
* Контроль радіочастотного спектру: Проводити моніторинг радіочастотного спектру на предмет наявності несанкціонованих радіопередач, які можуть використовуватися для підслуховування інформації.

Контроль полягає у регулярній перевірці виконаних заходів, описаних у цьому розділі, проведені тестування на проникнення для виявлення вразливостей в системах інформаційної безпеки, аналізуванні даних про виявлені інциденти інформаційної безпеки та вживання заходів для їх усунення, та оновлені ПЗ систем IDS відповідно до вимог.

4.6.3 Захист інформаційних ресурсів від читання даних з екрану або читання документів, які залишені без нагляду сторонніми особами

Необхідно вживати наступні заходи:

* Використання фільтрів конфіденційності: Використовувати фільтри конфіденційності, які обмежують кут огляду екрану комп'ютера, роблячи його неможливим для читання сторонніми особами, які знаходяться збоку.
* Застосування програмного забезпечення для захисту екрану: Використовувати програмне забезпечення для захисту екрану, яке автоматично блокує комп'ютер, коли користувач відходить від нього.
* Підвищення рівня обізнаності користувачів: Проводити навчання користувачів з питань інформаційної безпеки, включаючи правила роботи з конфіденційною інформацією на комп'ютері.

Контроль передбачає регулярне перевіряння виконання заходів, описаних у цьому розділі, проведення тестування на проникнення для виявлення вразливостей в системах інформаційної безпеки, а також аналіз даних про виявлені інциденти інформаційної безпеки з подальшим вживанням заходів для їх усунення.

4.6.4 Захист інформаційних ресурсів від крадіжки документів або пристроїв з сервісного центру

Необхідно вживати наступні заходи:

* Фізичний захист: Забезпечити фізичний захист сервісного центру від несанкціонованого проникнення, наприклад, шляхом встановлення систем відеоспостереження, контролю доступу та охорони.
* Контроль доступу: Впровадити систему контролю доступу, яка дозволяє лише авторизованим співробітникам сервісного центру отримувати доступ до документів та пристроїв.
* Підвищення рівня обізнаності персоналу: Проводити навчання персоналу сервісного центру з питань інформаційної безпеки, включаючи правила роботи з конфіденційною інформацією.

Контроль передбачає регулярну перевірку виконання заходів, описаних у цьому розділі, проведення аудитів інформаційної безпеки сервісного центру, а також аналіз даних про виявлені інциденти інформаційної безпеки з метою вживання заходів для їх усунення.

4.6.5 Захист інформаційних ресурсів від атаки “людина посередині” (Man-in-the-Middle)

Необхідно вживати наступні заходи:

* Використання протоколів HTTPS та TLS: Використовувати протоколи HTTPS та TLS для захисту каналів зв'язку та забезпечення автентичності та цілісності інформації.
* Використання віртуальних приватних мереж (VPN): Застосовувати VPN для створення захищених віртуальних каналів зв'язку через незахищені мережі, такі як Інтернет.
* Використання брандмауерів: Впровадити брандмауери для блокування несанкціонованого доступу до інформаційних систем.
* Навчання користувачів: Проводити навчання користувачів з питань інформаційної безпеки, включаючи правила розпізнавання та запобігання атакам типу “людина посередині”.

Контроль за забезпеченням захисту інформаційних ресурсів у сервісному центрі передбачає регулярну перевірку виконання заходів, описаних у розділі 6, включаючи проведення аудитів інформаційної безпеки та аналіз даних про виявлені інциденти для усунення виявлених вразливостей.

4.6.6 Захист інформаційних ресурсів від фішингу

Необхідно вживати наступні заходи:

* Навчання користувачів: Проводити навчання користувачів з питань інформаційної безпеки, включаючи правила розпізнавання та запобігання фішинговим атакам.
* Використання систем фільтрації електронної пошти: Впровадити системи фільтрації електронної пошти для блокування фішингових листів.
* Використання антивірусного програмного забезпечення: Використовувати антивірусне програмне забезпечення для виявлення та видалення фішингового програмного забезпечення.
* Застосування брандмауерів: Впровадити брандмауери для блокування несанкціонованого доступу до інформаційних систем.

Контроль включає регулярну перевірку виконання заходів, проведення тестування на проникнення для виявлення вразливостей та аналіз даних про виявлені інциденти інформаційної безпеки з подальшим усуненням виявлених проблем.

4.6.7 Захист інформаційних ресурсів від розкриття конфіденційних даних клієнтів

Необхідно вживати наступні заходи:

* Впровадження політики конфіденційності: Розробити та впровадити політику конфіденційності, яка визначає правила збору, зберігання, використання та розкриття конфіденційних даних клієнтів.
* Обмеження доступу до даних: Обмежити доступ до конфіденційних даних клієнтів лише авторизованим співробітникам, яким ця інформація необхідна для виконання їхніх завдань.
* Застосування шифрування: Шифрувати конфіденційні дані клієнтів, що зберігаються на носіях інформації та передаються по каналах зв'язку.
* Фізичний захист даних: Забезпечити фізичний захист носіїв інформації, на яких зберігаються конфіденційні дані клієнтів.
* Підвищення рівня обізнаності персоналу: Проводити навчання персоналу з питань інформаційної безпеки, включаючи правила роботи з конфіденційними даними клієнтів.

Контроль передбачає регулярну перевірку виконання заходів, описаних у цьому розділі, проведення аудитів інформаційної безпеки для виявлення вразливостей в системах захисту конфіденційних даних, а також аналіз даних про виявлені інциденти інформаційної безпеки з подальшим усуненням виявлених проблем.

4.6.8 Захист інформаційних ресурсів від не навмисного пошкодження пристрою

Необхідно вживати наступні заходи:

* Навчання користувачів: Проводити навчання користувачів з питань інформаційної безпеки, включаючи правила роботи з комп'ютерною технікою та іншими електронними пристроями.
* Створення резервних копій даних: Регулярно створювати резервні копії даних, що зберігаються на пристроях.
* Застосування програмного забезпечення для відновлення даних: Використовувати програмне забезпечення для відновлення даних у випадку їх пошкодження.
* Фізичний захист пристроїв: Зберігати пристрої в безпечних місцях, де вони не будуть піддаватися ризику пошкодження.

Контроль включає регулярну перевірку виконання заходів, описаних у цьому розділі, проведення інспекцій пристроїв для виявлення пошкоджень, а також аналіз даних про виявлені інциденти інформаційної безпеки з подальшим усуненням виявлених проблем.

4.6.9 Захист інформаційних ресурсів від порушення приватності або неетичного поводження з пристроєм клієнта

Необхідно вживати наступні заходи:

* Впровадження політики конфіденційності: Розробити та впровадити політику конфіденційності, яка чітко визначає правила збору, зберігання, використання та розкриття інформації про пристрої клієнтів. Ця політика повинна гарантувати, що інформація про пристрої клієнтів буде використовуватися лише в законних цілях та з їхньої згоди.
* Обмеження доступу до даних: Обмежити доступ до інформації про пристрої клієнтів лише авторизованим співробітникам, яким ця інформація необхідна для виконання їхніх службових обов'язків. Слід чітко визначити, хто має доступ до якої інформації та з якою метою.
* Фізичний захист даних: Забезпечити фізичний захист носіїв інформації, на яких зберігається інформація про пристрої клієнтів. Це може включати зберігання носіїв інформації в сейфах, обмеження доступу до приміщень, де вони зберігаються, та використання систем відеоспостереження.
* Підвищення рівня обізнаності персоналу: Проводити регулярні навчання персоналу з питань інформаційної безпеки, включаючи правила роботи з інформацією про пристрої клієнтів. Персонал повинен розуміти важливість захисту конфіденційності клієнтів та знати, як правильно поводитися з їхніми пристроями.

Регулярно перевіряти виконання заходів, описаних у цьому розділі. Це може включати перевірки політики конфіденційності, аудити інформаційної безпеки та аналіз даних про інциденти, пов'язані з порушенням приватності клієнтів. Проводити розслідування будь-яких випадків підозрілої активності або порушення політики конфіденційності. У разі виявлення порушення вживати відповідних заходів, таких як дисциплінарні стягнення щодо співробітників або повідомлення про інцидент правоохоронним органам.

4.6.10 Захист інформаційних ресурсів від не навмисного постачання неякісних деталей

Необхідно вживати наступні заходи:

* Впровадження системи контролю якості: Розробити та впровадити систему контролю якості, яка регламентує процес закупівлі, зберігання та використання деталей. Ця система повинна включати в себе: чіткі критерії якості деталей (технічні характеристики, відповідність стандартам, сертифікати якості); методи перевірки деталей (вхідний контроль, лабораторні випробування, візуальний огляд); відповідальність за дотримання критеріїв якості (управління закупівлями, контроль якості, відділ виробництва).
* Використання перевірених постачальників: Співпрацювати лише з перевіреними та надійними постачальниками деталей, які мають хорошу репутацію та гарантують якість своєї продукції.
* Проведення вхідного контролю: Ретельно перевіряти всі деталі, що надходять від постачальників, на відповідність критеріям якості. Це може включати візуальний огляд, лабораторні випробування та інші методи контролю.
* Зберігання деталей в належних умовах: Зберігати деталі в належних умовах, щоб запобігти їх пошкодженню або псуванню. Це може включати зберігання в сухих, чистих та провітрюваних приміщеннях, а також захист від механічних пошкоджень.
* Використання системи відстеження деталей: Впровадити систему відстеження деталей, яка дозволить ідентифікувати походження деталей та контролювати їх використання.
* Проведення навчання персоналу: Проводити регулярні навчання персоналу з питань контролю якості та захисту від ненавмисного постачання неякісних деталей.

Контроль передбачає регулярну перевірку виконання заходів, описаних у цьому розділі, проведення аудитів системи контролю якості для виявлення недоліків та їх усунення, а також аналіз даних про виявлені неякісні деталі з метою вжиття заходів для запобігання їх повторному постачанню.

4.6.11 Захист інформаційних ресурсів від спостереження за введенням ПІН-коду клієнта сторонніми особами

Необхідно вживати наступні заходи:

* Встановлення захисних екранів: Встановити захисні екрани на банкоматах, платіжних терміналах та інших пристроях, щоб ускладнити стороннім особам спостереження за введенням ПІН-коду.
* Застосування камер відеоспостереження: Встановити камери відеоспостереження в зонах самообслуговування, де розташовані банкомати та інші подібні пристрої. Це допоможе зафіксувати дії сторонніх осіб, які можуть намагатися спостерігати за введенням ПІН-кодів.
* Навчання клієнтів: Проводити навчання клієнтів з питань інформаційної безпеки, включаючи правила введення ПІН-коду. Клієнти повинні знати, що не можна нікому повідомляти свій ПІН-код та прикривати клавіатуру рукою під час його введення.

Контроль включає регулярну перевірку стану захисних екранів та камер відеоспостереження, проведення аналізу даних з камер відеоспостереження для виявлення підозрілих дій та опитування клієнтів щодо їх досвіду користування банкоматами та іншими подібними пристроями з метою виявлення можливих проблем з безпекою.

4.6.12 Захист інформаційних ресурсів від недбалого зберігання або неправильної утилізація даних

Необхідно вживати наступні заходи:

* Впровадження політики зберігання даних: Розробити та впровадити політику зберігання даних, яка визначає правила зберігання, доступу та утилізації даних.
* Обмеження доступу до даних: Обмежити доступ до даних лише авторизованим співробітникам, яким ця інформація необхідна для виконання їхніх завдань.
* Шифрування даних: Шифрувати дані, що зберігаються на носіях інформації та передаються по каналах зв'язку.
* Фізичний захист даних: Забезпечити фізичний захист носіїв інформації, на яких зберігаються дані.
* Знищення даних: Знищувати дані, які більше не потрібні, безпечним способом.

Контроль передбачає регулярну перевірку виконання заходів, описаних у цьому розділі, проведення аудитів інформаційної безпеки для виявлення вразливостей в системах захисту даних, а також аналіз даних про виявлені інциденти інформаційної безпеки.

4.6.13 Захист інформаційних ресурсів від маніпуляції даними для власної вигоди

Необхідно вживати наступні заходи:

* Впровадження політики конфлікту інтересів: Розробити та впровадити політику конфлікту інтересів, яка забороняє співробітникам використовувати дані для власної вигоди.
* Впровадження системи контролю аудиту: Впровадити систему контролю аудиту, яка дозволяє відстежувати дії користувачів з даними.
* Підвищення рівня обізнаності персоналу: Проводити регулярні навчання персоналу з питань інформаційної безпеки, включаючи правила роботи з даними.
* Застосування програмного забезпечення для виявлення шахрайства: Використовувати програмне забезпечення для виявлення шахрайства, яке може виявляти підозрілу активність з даними.

Контроль включає регулярну перевірку виконання заходів, описаних у цьому розділі, проведення аналізу даних з системи контролю аудиту для виявлення підозрілих дій, а також розслідування випадків підозрілої активності з даними.

4.6.14 Захист інформаційних ресурсів від втрати даних через людську помилку

Необхідно вживати наступні заходи:

* Впровадження політики резервного копіювання: Розробити та впровадити політику резервного копіювання, яка визначає правила створення, зберігання та відновлення резервних копій даних.
* Навчання персоналу: Проводити регулярні навчання персоналу з питань інформаційної безпеки, включаючи правила роботи з даними та запобігання втраті даних.
* Застосування систем відновлення даних: Впровадити системи відновлення даних, які дозволяють відновити дані у випадку їх втрати.

Контроль включає регулярну перевірку виконання заходів, описаних у цьому розділі, проведення тестування систем резервного копіювання та відновлення даних, а також аналіз даних про виявлені випадки втрати даних з подальшими заходами для їх запобігання.

**4.7 Кроки у випадку перегляду політики інформаційної безпеки внаслідок виникнення інциденту**

Інцидент: Шпигунство на підприємстві

Сценарій: Людина створює такий самий бізнес або людині пропонують продати будь-яку інформацію стосовно підприємств, або завдати шкоду для підприємства.

Опис інциденту:

На підприємстві було виявлено серйозні випадки шпигунства, які мали на меті отримання конфіденційної інформації та завдання шкоди його діяльності. Інцидент включав спроби незаконного доступу до внутрішніх систем, крадіжку конфіденційних даних та спроби залучення внутрішніх співробітників до передачі конфіденційної інформації стороннім особам або конкурентам.

Кроки для мінімізації інциденту:

* Підписання договорів стосовно комерційної таємниці для того, щоб працівники не могли розповсюджувати інформацію стосовно підприємства.
* Підписання документів стосовно конкуренції, щоб працівники не могли займатись тим самим бізнесом, для усунення конкуренції
* Документ має містити пункти стосовно розв’язання конфлікту у разі його виникнення та пункти стосовно відшкодування у разі виникнення інциденту.
* Документ має містити пункти - як повинні поводити себе працівники, якщо їм пропонують шпигунство або отримання будь якої інформації стосовно підприємства та даних, які має підприємство.

ВИСНОВОК

В результаті виконання лабораторної роботи було виявлено критичні напрями захисту та основні небезпечні чинники, які мають великий вплив на інформаційну безпеку організації. Основні загрози середньої та низької ймовірності виникнення були визначені та ретельно розглянуті у відповідних розділах політики інформаційної безпеки.

У подальших діях щодо розробки повної політики інформаційної безпеки важливо включити наступні кроки:

* Політика погоджується директором підприємства, затверджується рішенням адміністратора та директором підприємства та набирає чинності з дати, визначеної адміністратором та директором.
* Політика переглядається за необхідністю, але не рідше ніж один раз на рік. Позаплановий перегляд здійснюється у разі змін в інформаційній інфраструктурі та/або впроваджені на підприємстві нових інформаційних технологій, а також змін в законодавстві України.
* Підрозділом, відповідальним за підтримання Політики в актуальному стані, за своєчасне внесення змін та доповнень до Політики є 10 діб.
* У разі невідповідності будь-якої частини Політики вимогам чинного законодавства України, в тому числі в зв’язку з прийняттям нових актів законодавства України та зміною чинних, Політика буде діяти лише в тій частині, що не суперечить чинному законодавству. До внесення відповідних змін в Політику, працівники підприємства в своїй роботі повинні керуватися чинним законодавством України.
* Проведення навчання та інструктаж персоналу з оновлених процедур та правил безпеки.