ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЛАБОРАТОРНА РОБОТА №1-2

з навчальної дисципліни «Комплексні системи захисту інформації»

Тема: Дослідження структури об’єкту захисту. Ідентифікація небезпечних чинників на об’єкт захисту

Виконав:

студент групи – 6.04.125.010.21.2

факультету - ІТ

спеціальності 125-кібербезпека

Бойко Вадим

Перевірила:

Мерлак О.В.

Харків, 2024 р.

**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.

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 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.