ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЛАБОРАТОРНА РОБОТА №1

з навчальної дисципліни «Комплексні системи захисту інформації»

Тема: Дослідження структури об’єкту захисту

Виконав:

студентка 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 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.