ФГБОУ ВО «Петрозаводский государственный университет»

ДОКЛАД

по курсу организационное обеспечение информационной безопасности
на тему: "Аналитическое обоснование на разработку системы защиты информации сервиса по ремонту бытовой техники Технический Ремонтович"

Выполнили студенты группы 22307:
Ананьин Егор, Базаров Максим, Богатырёв Павел,
Гордеев Никита, Сергин Даниил

Версия 1

Преподаватель
Соколов Владислав Евгеньевич

Петрозаводск,
2023

Информационная характеристика и организационная структура объекта информатизации:

Объект информатизации - компания по ремонту бытовой техники, занимающаяся ремонтом и восстановлением работоспособности бытовой техники для физических и юридических лиц. В компании есть директор, два мастера и офис-менеджер, который занимается приёмом заказов. Помещение ремонтной мастерской состоит из 4 комнат.

Основные и вспомогательные технические средства, программное обеспечение, режимы работы, процесс обработки информации:

1. Компьютеры: Каждый работник компании имеет компьютер на своем рабочем месте, связанный с локальной сетью и соединенный с сервером. Все компьютеры работают под управлением операционной системы Windows 10.

2. Сервер: Офис-менеджер использует свой компьютер в качестве сервера для всех компьютеров в компании.

3. Интернет: Все компьютеры имеют возможность выхода в Интернет.

4. Антивирусная программа: Все компьютеры защищены антивирусной программой.

5. Файловая система: Архив клиентов ведется через файловую систему, где каждому клиенту соответствует отдельная папка.

6. Программное обеспечение: Дополнительное программное обеспечение может быть использовано для управления клиентскими данными, учета и других необходимых операций.

7. Режимы работы: Компьютеры используются для обработки и хранения информации о клиентах, заказах, состоянии ремонта и других операций.

8. Процесс обработки информации: Информация о клиентах и их заказах вводится и обрабатывается через компьютеры, сохраняется в файловой системе и используется для отслеживания и управления процессом ремонта бытовой техники.

Возможные каналы утечки информации и мероприятия по их устранению и ограничению:

1. Утечка информации через сеть и компьютеры:
    a. Pansomware (вымогательство с использованием шифрования): Этот тип вредоносного программного обеспечения зашифровывает данные на зараженных компьютерах и требует выкуп за их разблокировку. Это может привести к потере важной информации и нарушению бизнес-процессов.
    b. Троянские программы: Троянские программы представляют собой программы, которые маскируются под полезное или безобидное программное обеспечение, но вместе с тем выполняют вредоносные функции. Они могут проникнуть в систему через электронную почту, зараженные ссылки или другие способы, и представлять угрозу конфиденциальности данных и целостности системы.
    c. Кейлоггеры: Кейлоггеры - это программное обеспечение, которое записывает все нажатия клавиш на компьютере, включая пароли и другую конфиденциальную информацию. Они могут быть использованы для кражи учетных данных и доступа к системам компании.

   d. Ботнеты: Ботнет - это сеть зараженных компьютеров, которая управляется злоумышленниками с целью использования этих компьютеров для запуска кибератак. Ваша организация может стать частью ботнета без вашего согласия, что может привести к нарушению работоспособности и безопасности сети.
2. Утечка информации через физический доступ:
   a. Вредоносные программы через съемные носители: Зараженные USB-флешки или другие съемные носители могут быть использованы для распространения вредоносных программ в вашей организации. При подключении таких устройств к компьютерам они могут передавать вирусы или другие вредоносные программы на компьютеры и внести серьезные проблемы в систему.
3. Утечка информации через слабые пароли и нежелательные действия сотрудников:
   a. Социальная инженерия: Это метод манипулирования сотрудниками организации путем использования дезинформации или выманивания конфиденциальной информации. Злоумышленники могут использовать фишинговые электронные письма, поддельные веб-сайты или даже личное общение, чтобы получить доступ к важным данным.

1. Мероприятия по ограничению и устранению утечки информации в сети и компьютеры:
   - Установка брандмауэра и настройка правил доступа для защиты сети от несанкционированного доступа извне.
   - Регулярные обновления операционной системы и антивирусного программного обеспечения для обнаружения и предотвращения уязвимостей.
   - Использование сетевых протоколов, которые обеспечивают шифрование данных при передаче (например, HTTPS).
   - Аутентификация и авторизация пользователей для ограничения доступа к конфиденциальной информации только уполномоченным сотрудникам.
   - Шифрование данных на жестких дисках компьютеров для защиты информации от физического доступа.
   - Ограничение использования внешних носителей данных (например, USB-флешек) и контроль за их использованием.
   - Регулярно резервируйте важные данные, чтобы иметь возможность восстановления в случае атаки.

2. Мероприятия по ограничению и устранению утечки информации через физический доступ включают:
   - Ограничение доступа к помещениям рабочей мастерской только авторизованным сотрудникам.
   - Установка видеонаблюдения для контроля за доступом в помещение и помощи в идентификации потенциальных нарушителей.

3. Мероприятия по ограничению и устранению утечки информации через слабые пароли и нежелательные действия сотрудников включают:
   - Обязательное использование сильных паролей для доступа к компьютерам и другим учетным записям с доступом к конфиденциальной информации.
   - Проведение регулярных обучающих программ и напоминаний сотрудникам о правилах безопасности информации и предотвращении фишинговых атак.
   - Внедрение политики использования компьютеров компании только для рабочих целей и запрет на загрузку нежелательного программного обеспечения или посещение небезопасных веб-сайтов.

- Ограничивайте доступ к системам и данным только тем сотрудникам, которым это необходимо для выполнения их задач.

Перечень предлагаемых к использованию сертифицированных средств защиты информации:

- Брандмауэр: Рекомендуется использовать сертифицированный брандмауэр для защиты сети компании от несанкционированного доступа.
- Антивирусное программное обеспечение: Рекомендуется использовать сертифицированное антивирусное программное обеспечение для обнаружения и предотвращения вредоносных программ.
- Шифрование данных: Рекомендуется использовать сертифицированные средства шифрования данных для защиты конфиденциальной информации на компьютерах и в сети.
- Система контроля доступа: Рекомендуется использовать сертифицированную систему контроля доступа для управления правами доступа сотрудников к конфиденциальной информации.

Обоснование необходимости привлечения специализированных организаций:

Учитывая важность защиты информации в компании, рекомендуется привлечение специализированных организаций, имеющих необходимые лицензии на проведение работ по защите информации. Это обусловлено следующими причинами:

1. Экспертиза: Специализированные организации обладают опытом и экспертизой в области информационной безопасности, что позволит провести комплексный анализ системы и предложить наиболее эффективные меры по защите информации.

2. Сертификация: Специализированные организации имеют возможность сертифицировать решения и средства защиты информации, что гарантирует их соответствие стандартам безопасности.

3. Актуальность: Специализированные организации следят за последними тенденциями и угрозами в области информационной безопасности, что позволяет им обеспечить компанию современными и эффективными решениями.

4. Комплексный подход: Специализированные организации могут предложить комплексный подход к защите информации, включающий оценку уязвимостей, разработку политик безопасности, обучение сотрудников и другие необходимые мероприятия.

Оценка материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ:

Оборудование в комнатах:
- Комната директора:
    - Компьютер с ОС Windows 10: Средний бюджет на один компьютер - 90,000 рублей.
    - Принтер для печати документов: Средний бюджет на принтер - 22,500 рублей.
    - Система видеонаблюдения: Средний бюджет на камеру - 5,000 рублей.
- Комната мастеров (мастерская):

    - Каждый мастер должен иметь свой компьютер с ОС Windows 10: 2 мастера * 90,000 = 180,000 рублей.
    - Принтер для печати инструкций и технической документации, маркировки и учета техники: Средний бюджет на принтер - 22,500 рублей.
    - Система видеонаблюдения: Средний бюджет на камеру - 2 штуки * 5,000 рублей = 10,000 рублей.
- Офис-менеджера:
    - Компьютер с ОС Windows 10 для приема заказов и управления бухгалтерией: 90,000 рублей.
    - Принтер для печати счетов и документов, маркировки и учета техники: 22,500 рублей.
    - Сканер для сканирования документов: 15,000 рублей.
    - Система видеонаблюдения: Средний бюджет на камеру - 2 штуки * 5,000 рублей = 10,000 рублей.
- Склад:
    - Система видеонаблюдения: Средний бюджет на камеру 5,000 рублей

Трудовые затраты:
- Разработка и внедрение СЗИ:
    - Инженер по подключению и настройке систем безопасности: 2 месяца * 40,000 рублей/месяц = 80,000 рублей.
- Обучение персонала:
    - Обучение сотрудников по новым процедурам и использованию СЗИ: 30,000 рублей.

Итоговые материальные затраты:
    - 117,500 (директор) + 212,500 (мастера) + 137,500 (офис-менеджер) + 5,000 (склад) + 80,000 (инженер) + 30,000(обучение) = 582,500 руб.
- Общая стоимость оборудования: 582,500 рублей.

Ориентировочные сроки разработки и внедрения СЗИ:

1. Подготовительный этап (1 месяц):
    - Проведение анализа текущего состояния безопасности информации в компании.
    - Определение требований и стандартов безопасности, соответствующих особенностям деятельности компании.
    - Назначение ответственного за проект по внедрению СЗИ.
    - Определение бюджета проекта.
2. Проектирование СЗИ (2 месяца):
    - Разработка технического задания на создание системы защиты информации.
    - Проектирование архитектуры СЗИ с учетом особенностей офиса и мастерской.
    - Выбор и закупка необходимого оборудования и программного обеспечения.
3. Внедрение СЗИ (3 месяца):
    - Установка физических средств безопасности (контроль доступа, видеонаблюдение).
    - Настройка программных средств, включая антивирусное ПО и системы мониторинга.
    - Обучение сотрудников правилам безопасности и использованию новой системы.

4. Разработка политики информационной безопасности (1 месяц):
    - Формирование документа с описанием политики безопасности и правил обработки информации.
    - Согласование политики с руководством и сотрудниками.
5. Регулярное обслуживание и обновление (постоянно):
    - Регулярное обновление технических средств защиты информации.
    - Проведение аудитов безопасности и внесение корректив в систему при необходимости.
6. Обучение и поддержка (постоянно):
    - Постоянное обучение сотрудников новым методам и средствам обеспечения безопасности.
    - Поддержка сотрудников в вопросах информационной безопасности.