ФГБОУ ВО «Петрозаводский государственный университет»

# ДОКЛАД

**по курсу организационное обеспечение информационной безопасности**
**на тему: «Руководство по защите 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

Цель этого руководства — обеспечение безопасности и защиты информации в компании, занимающейся ремонтом бытовой техники. Руководство содержит подробное описание порядка определения защищаемой информации, описание технологического процесса обработки информации, а также меры, методы и средства обеспечения защиты информации в различных аспектах: законодательные, морально-этические, организационные, физические, технические и аппаратно-программные.

**Порядок определения защищаемой информации:**

1. Идентификация категорий информации:
    a. Клиентская информация, включая контактные данные и данные о ремонте бытовой техники.
    b. Финансовые данные, включая информацию о платежах и транзакциях.
    c. Коммерческие секреты, включая информацию о бизнес-процессах и партнерских отношениях.
    d. Внутренние документы, включая планы развития, политики и процедуры компании.
2. Оценка уровня конфиденциальности:
    a. Клиентская информация: конфиденциальная.
    b. Финансовые данные: строго конфиденциальная.
    c. Коммерческие тайны: строго конфиденциальная.
    d. Внутренние документы: внутренняя.
3. Установление правил доступа:
    a. Клиентская информация:
        i. Мастера имеют право доступа к информации о ремонте бытовой техники.
        ii. Офис-менеджер имеет доступ к клиентской информации для обработки заказов.
        iii. Директор имеет ограниченный доступ к клиентской информации для управленческих задач.
    b. Финансовые данные:
        i. Офис-менеджер имеет доступ к финансовым данным для учета платежей и транзакций.
        ii. Директор имеет ограниченный доступ к финансовым данным для управленческих задач.
    c. Коммерческие секреты:
        i. Директор имеет доступ к коммерческим тайнам.
    d. Внутренние документы:
        i. Директор и офис-менеджер имеют доступ к внутренним документам компании.

Все права на редактирование, удаление и передачу информации должны быть строго ограничены и осуществляться только после соответствующей авторизации и аутентификации пользователей. Доступ в Интернет с рабочих компьютеров должен быть контролируемым и ограниченным, чтобы предотвратить утечку конфиденциальной информации. Информация о внутренних операционных процессах, методах ремонта, идентификации поставщиков и другие коммерческие сведения также должны рассматриваться как конфиденциальная информация.

**Описание технологического процесса обработки информации:**

1. Прием заказов:
   Офис-менеджер принимает заказы клиентов и записывает информацию в компьютерную систему на сервер.

2. Оперативный ремонт:
   Мастера производят ремонт бытовой техники на своих рабочих местах, используя необходимые инструменты и документируют данные о проделанной работе.
3. Сохранение информации:
   Информация о ремонте и клиентах сохраняется в папках на сервере. Рекомендуется регулярное создание резервных копий данных для предотвращения потери информации.
4. Передача отремонтированной техники клиентам:
   После завершения ремонта, клиенту возвращается отремонтированная техника вместе с документацией о проделанной работе и гарантийными обязательствами.

**Меры, методы и средства обеспечения защиты информации:**

1. Законодательные меры:
   Ознакомьтесь с действующим законодательством о защите персональных данных и коммерческой информации и обязательствами, накладываемыми на вашу компанию. Соблюдайте соответствующие требования и нормы.
2. Морально-этические меры:
   Проведите обучение сотрудников по вопросам конфиденциальности, обязательствам по защите информации, осведомите их о последствиях нарушения политики безопасности информации и обратите их внимание на этические аспекты работы с конфиденциальными данными клиентов.
3. Организационные меры:
   Разработайте внутренние политики и процедуры для обработки и хранения информации. Включите процедуры доступа к информации, управления паролями, классификации и маркировки документов и управления доступом.
4. Физические меры:
   Обеспечьте безопасность помещения, в котором находятся компьютеры и сервер, с помощью контроля доступа, видеонаблюдения и ограничений на проникновение в него.
5. Технические меры:
   Обеспечьте компьютеры и сервер надежной антивирусной защитой и брандмауэром для предотвращения несанкционированного доступа и вредоносных программ. Регулярно обновляйте программное обеспечение и операционные системы.
6. Аппаратно-программные меры:
   Используйте шифрование при передаче конфиденциальной информации через сеть. Используйте средства аутентификации, такие как пароли или биометрические методы, для защиты доступа к информации на компьютерах и сервере.