Проведённое обследование и анализ структуры Научно-исследовательская компания «Демо Лаб» на основании представленных материалов была составлена структура организации, визуализированная в виде схемы 1.

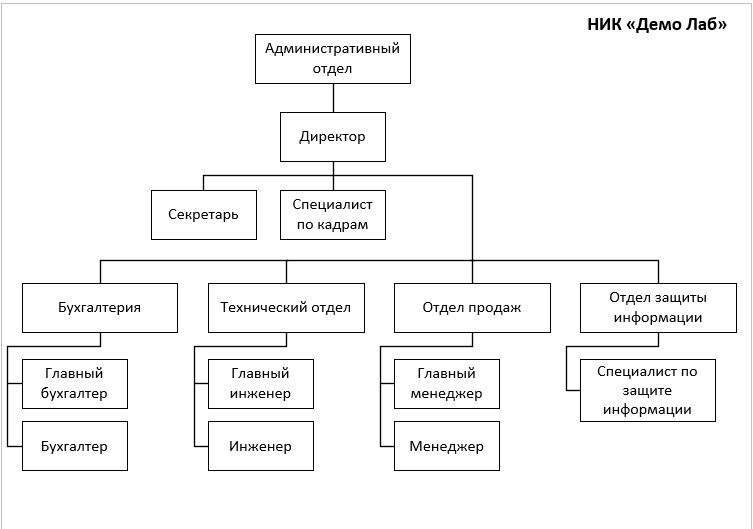


Схема 1 – Структура организации

В административный отдел входят – директор, секретарь и специалист по кадрам, директору подчиняются все следующие отделы.

* Бухгалтерия – этот отдел включает в себя главного бухгалтера и бухгалтера. Бухгалтер подчиняется главному бухгалтеру.
* Технический отдел – этот отдел включает в себя главного инженера и инженера. Инженер подчиняется главному инженеру.
* Отдел продаж – этот отдел включает в себя главного менеджера и менеджера. Менеджер подчиняется главному менеджеру.
* Отдел защиты информации – этот отдел включает в себя специалиста по защите информации.

После была составлена диаграмма DFD потоков информации представленная в схеме 2, где указано какие потоки существуют между всеми отделами. Все потоки пронумерованы. Данные потоки описаны в таблице.



Схема 2 – Диаграмма DFD

Далее составлена таблица потоков информации, где имеются номера потоков, их наименование и описание.

Таблица 1

|  |  |  |
| --- | --- | --- |
| **1** | **2** | **3** |
| **Номер информационного потока** | **Наименование** | **Описание** |
| 1 | Запросы на покупку электронных компонентов | **Клиенты** передают запросы на покупку электронных компонентов в **Отдел продаж** |
| 2 | Обновление информации о клиентах | **Отдел продаж** обновляет информацию в **Базе данных клиентов** |
| 3 | Передача заказов на разработку систем | **Отдел продаж** передает заказы на разработку в **Технический отдел** |
| 4 | Сохранение данных о разработке | **Технический отдел** сохраняет данные о разработке в **Базе данных проектов** |

Таблица 1 - продолжение

|  |  |  |
| --- | --- | --- |
| **1** | **2** | **3** |
| 5 | Обновление кадровой информации | **Административный отдел** обновляет кадровую информацию в **Базе данных сотрудников** |
| 6 | Ведение финансового учета | **Бухгалтерия** ведет финансовый учет в **Финансовой базе данных** |
| 7 | Контроль и обеспечение безопасности данных | **Отдел защиты информации** контролирует и обеспечивает безопасность данных во всех отделах. |

# ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласно Постановлению Правительства РФ № 1119 от 1 ноября 2012 года, уровень защищенности персональных данных в организации определяется по категориям обрабатываемых данных, количеству субъектов и актуальным угрозам. Если уровень защищенности соответствует 3-му, это подразумевает наличие угроз 3-го типа, которые не касаются недокументированных возможностей программного обеспечения. Например, если система обрабатывает специальные категории персональных данных сотрудников или меньше 100 000 клиентов, либо биометрические данные, то устанавливается 3-й уровень защиты.

Для компании «Демо Лаб», если угрозы относятся к 3-му типу, а система работает с особыми категориями ПДн сотрудников или менее 100 000 клиентов, то уровень защищенности будет 3. Это требует реализации организационных и технических мер, определенных Приказом ФСТЭК России № 21, включая назначение ответственного за безопасность данных, использование сертифицированных средств защиты, контроль доступа и регулярный аудит.

# ОПРЕДЕЛЕНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласно Приказу ФСТЭК России № 21, для достижения целостности ИСПДн на уровне 2 необходимо реализовать следующие меры:

Организационные меры:

* Разработка локальных нормативных актов (положение о защите ПДн, инструкции, соглашения о конфиденциальности).
* Ограничение доступа к данным только для уполномоченных лиц.
* Обучение сотрудников по вопросам защиты информации.
* Проведение регулярного резервного копирования и хранение копий в защищенном месте.
* Ведение журнала событий и проведение аудита безопасности.
* Технические меры:
* Установка средств аутентификации и контроля доступа.
* Обеспечение защиты от вредоносного ПО и использование лицензионного программного обеспечения.
* Шифрование данных и установка файерволлов.
* Защита физических носителей и организация резервного питания оборудования.

Также важно контролировать изменения данных, защищать от внутренних угроз, тестировать процедуры восстановления и использовать системы обнаружения вторжений. Это обеспечит целостность ИСПДн и соответствие требованиям законодательства.

# ФОРМИРОВАНИЕ КОНЦЕПЦИИ ПОЛИТИКИ ЗАЩИТЫ ДАННЫХ

## Используемые технологии анализа

Для обеспечения безопасности персональных данных (ПДн) и предотвращения утечек информации применяются следующие технологии анализа:

1. Анализ сетевого трафика: Мониторинг передачи данных через локальную сеть и внешние каналы (интернет, почта, мессенджеры) для выявления несанкционированных попыток передачи ПДн.

2. Контроль съемных носителей: Препятствование записи ПДн на неучтенные USB-накопители и внешние жесткие диски.

3. Мониторинг печати: Регистрация и выявление попыток печати документов с содержанием ПДн.

4. Контроль буфера обмена: Блокировка копирования ПДн в буфер обмена и их передачи в программное обеспечение.

5. Аудит хранилищ данных: Контроль сохранения ПДн на серверах и автоматизированных рабочих местах (АРМ).

6. Анализ общих сетевых ресурсов: Выявление фактов хранения ПДн в общих папках, базах данных, почтовых архивах и других сетевых ресурсах.

2. Объекты защиты

|  |  |  |
| --- | --- | --- |
| № п/п | Название Объекта защиты | Состав объекта защиты |
| 1 | База данных сотрудников | Биографические данные, национальность, религиозная принадлежность, образование, должность, судимости, адрес, телефон, состав семьи, зарплата, трудовой договор |
| 2 | База данных клиентов | ФИО, контактные данные, история заказов, платежные данные. |
| 3 | Локальная сеть | Трафик между АРМ, серверами и внешними сетями |
| 4 | Съемные носители | USB-накопители, внешние жесткие диски. |
| 5 | Принтеры и МФУ | Документы, содержащие ПДн. |

## Списки отправителей и получателей

|  |  |  |
| --- | --- | --- |
| № п/п | Название периметра | Список |
| 1 | |  |  | | --- | --- | |  | Внутренняя сеть | | АРМ сотрудников, серверы, базы данных. |
| 2 | |  |  | | --- | --- | |  | Внешняя сеть | | Почтовые серверы, мессенджеры, облачные хранилища. |

## Политики защиты данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Название Политики | Тип политики (Политика защиты данных, Политика защиты данных на агентах) | Объекты защиты | Правила срабатывания |
| 1 | Защита от утечек через сеть | Политика защиты данных | Локальная сеть, внешняя сеть | Блокировка передачи ПДн на внешние ресурсы. |
| 2 | Контроль съемных носителей | Политика защиты данныхПДн | Съемные носители | Запрет записи ПДн на неучтенные устройства. |
| 3 | Мониторинг печати | Политика защиты данных | Принтеры и МФУ | Уведомление о попытке печати документов с ПДн. |
| 4 | Контроль буфера обмена | Политика защиты данных | АРМ сотрудников | Блокировка копирования ПДн в буфер обмена |

## Правила агентского мониторинга

|  |  |  |
| --- | --- | --- |
| № п/п | Правила | Описание правила |
| 1 | Блокировка передачи ПДн | Автоматическая блокировка попыток передачи ПДн через почту, мессенджеры или облачные хранилища. |
| 2 | |  |  | | --- | --- | |  | Уведомление о записи на съемные носители | | Уведомление администратора о попытке записи ПДн на USB-накопители. |
| 3 | Аудит печати | Регистрация всех попыток печати документов с ПДн. |
| 4 | Контроль буфера обмена | Блокировка копирования ПДн в буфер обмена и уведомление администратора. |

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ \_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_)

Дата Подпись Расшифровка