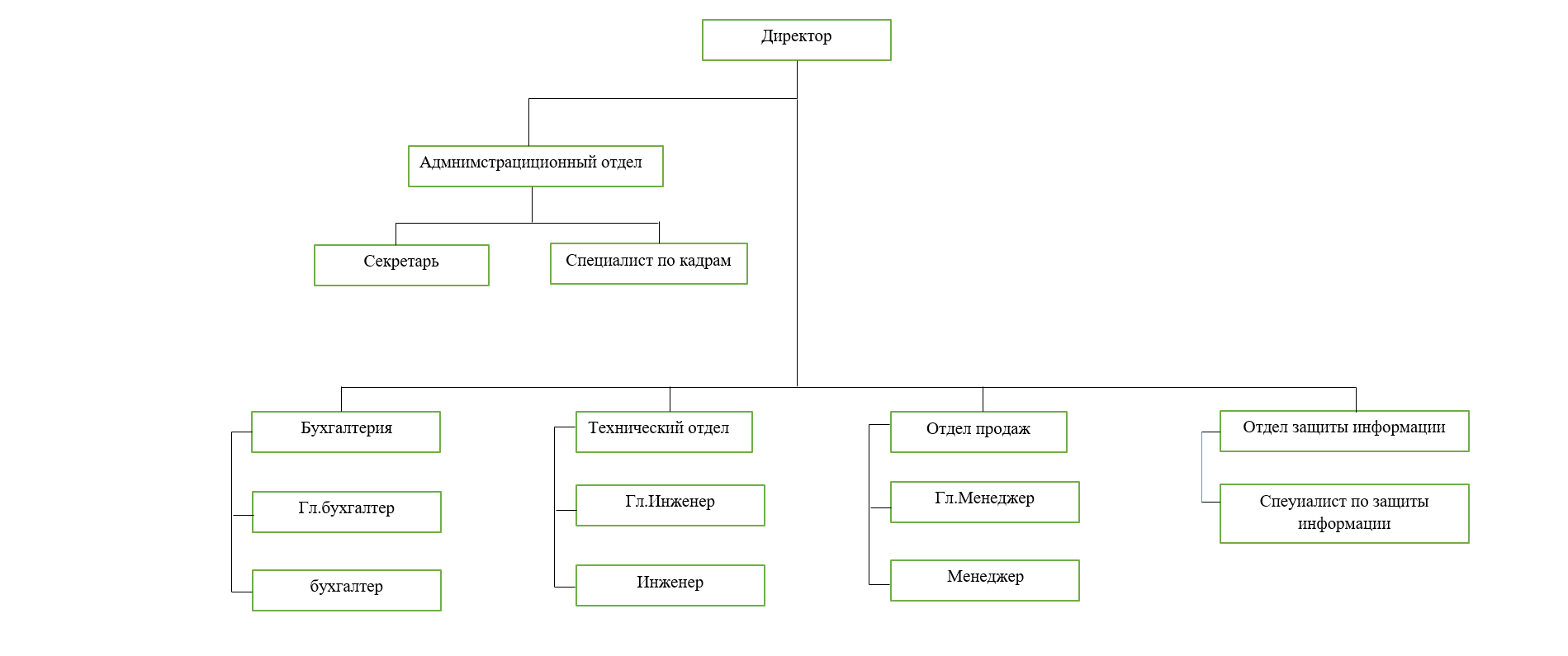
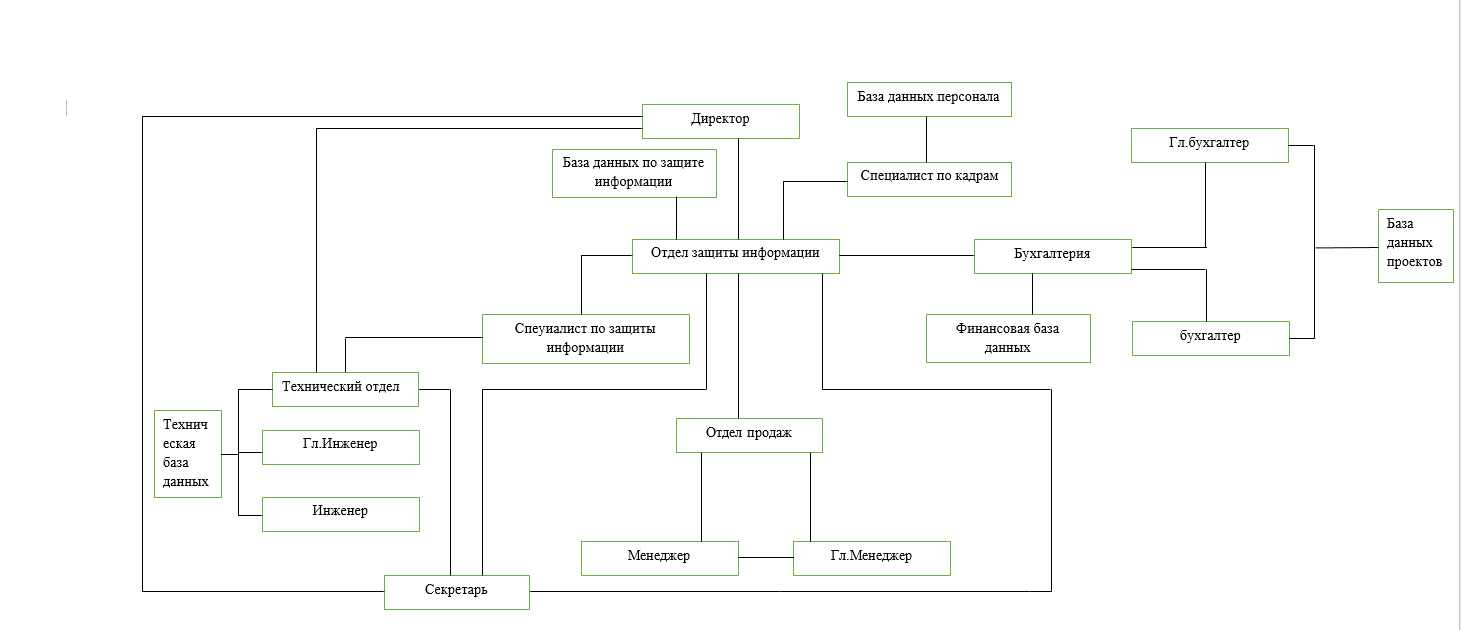
Проведённое обследование и анализ структуры Научно-исследовательская компания «Демо Лаб» на основании представленных материалов была составленна структура организации (показать и объяснить):



Составленна диаграмма DFD потоков информации, где (показать и объяснить):



|  |  |  |
| --- | --- | --- |
| **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** |
| 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. |

В соответствии с **Постановлением Правительства Российской Федерации № 1119 от 1 ноября 2012 года**, уровень защищенности персональных данных в информационной системе организации определяется на основе категорий обрабатываемых данных, количества субъектов персональных данных и типа актуальных угроз. Если рассматривать ситуацию, при которой уровень защищенности персональных данных соответствует **3-му уровню**, это означает, что для информационной системы актуальны угрозы **3-го типа**, то есть угрозы, не связанные с наличием недокументированных возможностей в системном и прикладном программном обеспечении. В таком случае, если информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100 000 субъектов, не являющихся сотрудниками оператора, либо биометрические персональные данные, либо иные категории персональных данных более чем 100 000 субъектов, не являющихся сотрудниками оператора, то устанавливается **3-й уровень защищенности**.

Для компании «Демо Лаб», если бы актуальными были угрозы 3-го типа, а информационная система обрабатывала, например, специальные категории персональных данных сотрудников или менее чем 100 000 клиентов, либо биометрические данные, либо иные категории персональных данных более чем 100 000 субъектов, то уровень защищенности персональных данных был бы определен как **3-й уровень**. Этот уровень требует реализации организационных и технических мер, предусмотренных **Приказом Федеральной службы по техническому и экспортному контролю России № 21**, включая назначение ответственного за безопасность персональных данных, использование сертифицированных средств защиты информации, обеспечение контроля доступа и регулярный аудит системы.

определить содержание мер по обеспечению безопасности персональных данных

В соответствии с Приказом ФСТЭК России № 21 для обеспечения целостности ИСПДн на уровне 2 необходимо реализовать следующие меры:

Организационные меры:

- Разработать локальные нормативные акты (положение о защите ПДн, инструкции, договоры о конфиденциальности).

- Ограничить доступ к данным только уполномоченных лиц.

- Провести обучение сотрудников по вопросам защиты информации.

- Организовать регулярное резервное копирование и хранить копии в защищенном месте.

- Вести журнал событий и проводить аудит безопасности.

Технические меры:

- Установить средства аутентификации и контроля доступа.

- Обеспечить защиту от вредоносного ПО и использование лицензионного софта.

- Применить шифрование данных и использовать файерволлы.

- Защитить физические носители и организовать резервное питание оборудования.

Дополнительно следует контролировать изменения данных, защищать от внутренних угроз, тестировать процедуры восстановления и использовать системы обнаружения вторжений. Это позволит обеспечить целостность ИСПДн и соответствовать требованиям законодательства.

сформировать концепцию политики защиты данных (в соответствии с шаблоном

1. Используемые технологии анализа

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

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

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

3. Мониторинг печати: Выявление и регистрация попыток печати документов, содержащих ПДн.

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

5. Аудит хранилищ данных: Контроль хранения 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. |

3.Списки отправителей/получателей

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

4. 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 |

5.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