**Задание 1.**

В соответствии с Постановлением Правительства РФ №1119 от 01.11.2012 г. меры по защите персональных данных в ИСПДн зависят от требуемого уровня защищенности ИСПДн. ИСПДн Оператора состоит из следующих компонентов:

ИСПДн «СУБД Microsoft SQL Server 2016» - системы управления реляционными базами данных Microsoft, которая обрабатывает данные с помощью SQL. Характеристика ИСПДн «СУБД Microsoft SQL Server 2016»:

|  |  |
| --- | --- |
| Тип актуальных угроз | 3 |
| Категория ПДн | иные |
| Объем обрабатываемых персональных данных | < 100 000 |
| Персональные данные сотрудника | Не обрабатываются |
| Структура информационной системы | Локальная информационная система |
| Наличие подключений информационной системы к  сетям связи общего пользования и (или) сетям  международного информационного обмена | нет |
| Режим обработки персональных данных | Многопользовательский |
| Режим разграничения прав доступа пользователей  информационной системы | Разграничение доступа |

ИСПДн «1С Предприятие: Бухгалтерия» - это профессиональный инструмент бухгалтера, с помощью которого можно вести бухгалтерский и налоговый учет, готовить и сдавать обязательную отчетность. Характеристика ИСПДн «1С Предприятие: Бухгалтерия»:

|  |  |
| --- | --- |
| Тип актуальных угроз | 3 |
| Категория ПДн | иные |
| Объем обрабатываемых персональных данных | < 100 000 |
| Персональные данные сотрудника | Не обрабатываются |
| Структура информационной системы | Локальная информационная система |
| Наличие подключений информационной системы к  сетям связи общего пользования и (или) сетям  международного информационного обмена | нет |
| Режим обработки персональных данных | Многопользовательский |
| Режим разграничения прав доступа пользователей  информационной системы | Разграничение доступа |

ИСПДн «1С:Зарплата и управление персоналом 8» — программа массового назначения, позволяющая в комплексе автоматизировать задачи, связанные с расчетом заработной платы персонала и реализацией кадровой политики, с учетом требований законодательства и реальной практики работы предприятий. Характеристика ИСПДн «1С:Зарплата и управление персоналом 8»:

|  |  |
| --- | --- |
| Тип актуальных угроз | 3 |
| Категория ПДн | иные |
| Объем обрабатываемых персональных данных | < 100 000 |
| Персональные данные сотрудника | Не обрабатываются |
| Структура информационной системы | Локальная информационная система |
| Наличие подключений информационной системы к  сетям связи общего пользования и (или) сетям  международного информационного обмена | нет |
| Режим обработки персональных данных | Многопользовательский |
| Режим разграничения прав доступа пользователей  информационной системы | Разграничение доступа |

ИСПДн «СБиС» - сеть деловых коммуникаций и обмена электронными документами между компаниями, госорганами и обыкновенными людьми. Характеристика ИСПДн «СБиС»:

|  |  |
| --- | --- |
| Тип актуальных угроз | 3 |
| Категория ПДн | иные |
| Объем обрабатываемых персональных данных | < 100 000 |
| Персональные данные сотрудника | Не обрабатываются |
| Структура информационной системы | Распределенная информационная система |
| Наличие подключений информационной системы к  сетям связи общего пользования и (или) сетям  международного информационного обмена | нет |
| Режим обработки персональных данных | Многопользовательский |
| Режим разграничения прав доступа пользователей  информационной системы | Разграничение доступа |

Требуемый уровень исходной защищенности определяется исходя из нескольких факторов:

1. Категории ПДн;
2. Чьи данные обрабатываются: сотрудников или нет;
3. Количества субъектов ПДн;
4. Типа актуальных угроз.

В зависимости от совокупности этих факторов и определяется уровень защищенности. Для упрощения можно воспользоваться готовой таблицей, показанной на рисунке ниже.



Для ИСПДн «СУБД Microsoft SQL Server 2016», ИСПДн «1С Предприятие: Бухгалтерия», ИСПДн «1С:Зарплата и управление персоналом 8», ИСПДн «СБиС» согласно с Постановлением Правительства РФ №1119 от 01.11.2012 г для данных ИСПДн требуется 4-й уровень защищенности.

**Задание 2.**

Для обеспечения безопасности персональных данных в информационной системе персональных данных Оператора, адаптируя базовый набор мер по обеспечению безопасности под требования ОЦЛ, можно предложить следующие организационные и технические меры:

Организационные меры включают в себя:

* идентификация пользователей ИС по паролю (реализация средствами ПО самой ИСПДн);
* регистрация входа \ выхода пользователей в ИС;
* физическая охрана ИСПДн, контроль доступа в помещение;
* очистка освобождаемых областей оперативной памяти компьютера и внешних накопителей;
* наличие администратора (службы) безопасности, ответственных за ведение, нормальное функционирование и контроль работы средств защиты информации.

Технические меры включают в себя:

* Антивирусную защиту;
* Систему обнаружения и предотвращения вторжений;
* Защиту технических средств;
* Защиту ИС, ее средств, систем связи и каналов передачи данных;
* Систему защиты от несанкционированного доступа;
* Физическую защиту

**Задание 3.**

1. Используемые технологии анализа:

* Анализ направлений движения информационных потоков ИС
* Текстовые объекты, содержащие ПДн
* Изменение, доступ к журналу доступа к ПДн

## Объекты защиты

| № п/п | Название Объекта защиты | Состав объекта защиты |
| --- | --- | --- |
| 1 | Клиентская база | Информация о клиентах, партнерах, заказчиках |
| 2 | ИСПДн Оператора | Система управления базами данных (СУБД Microsoft SQL Server 2016), программное обеспечение 1С: Бухгалтерия (версия 8), 1С: Зарплата и управление персоналом (версия 8),СБиС |
| 3 | Среда передачи данных | Локальная сеть |
| 4 | Персональные данные | Любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) |
| 5 | Почта/Email, мессенджеры/WhatsApp | Обмен информацией между сотрудниками |
| 6 | Журнал доступа к ПДн | Журнал, содержащий полномочия сотрудника оператора по доступу к ПДн |

1. Списки отправителей/получателей

| № п/п | Название периметра | Список |
| --- | --- | --- |
| 1 | Локальная вычислительная сеть Оператора | Сеть, используемая для передачи данных внутри компании |
| 2 | Пользователи ИСПДн | Лица, являющиеся клиентами компании |
| 3 | Партнеры, заказчики | Детальная информация о партнерах и заказчиках за 10 лет |
| 4 | Электронная почта | Сотрудники компании "Демо Лаб" и их рабочие адреса электронной почты. Указание внешних контрагентов, партнеров и клиентов компании. |
| 5 | Мессенджеры/WhatsApp | Сотрудники компании "Демо Лаб" с указанием их номеров или идентификаторов в мессенджерах |
| 6 | ИСПДн Оператора | Пользователи и администраторы информационных систем с указанием их учетных записей |
| 7 | Электронный журнал обмена сообщениями ИСПДн | Информационные системы, задействованные в работе журнала доступа к ПДн |

1. Политики защиты данных

| № п/п | Название Политики | Тип политики (Политика защиты данных, Политика защиты данных на агентах) | Объекты защиты | Правила срабатывания |
| --- | --- | --- | --- | --- |
| 1 | Контроль передачи данных | Политики защиты данных | ИСПДн Оператора, Почта/Email, мессенджеры/WhatsApp | Срабатывание при совпадении по регулярному выражению |
| 2 | Контроль доступа к журналу ПДн | Политики защиты данных | Журнал доступа ПДн | Срабатывание при каждом обращении к журналу доступа к ПД |
| 3 | Контроль изменений в журнале доступа к журналу ПДн | Политики защиты данных | Журнал доступа ПДн | Срабатывание при каждом изменении журнала доступа к ПД |
| 4 | Контроль записи данных на съемные устройства | Политики защиты данных | ИСПДн Оператора, Локальная вычислительная сеть Оператора, Персональные данные, Клиентская база | Использование устройств не из списка доверительных устройств |
| 5 | Контроль принтеров | Политики защиты данных | ИСПДн Оператора, Локальная вычислительная сеть Оператора, Персональные данные, Клиентская база | Печать документов, содержащих защищаемую инфомацию |
| 6 | Контроль буфера обмена | Политики защиты данных | ИСПДн Оператора, Локальная вычислительная сеть Оператора, Персональные данные, Клиентская база  Почта/Email, мессенджеры/WhatsApp | Запись в журнал при совпадении данных по регулярному выражению |

## Правила агентского мониторинга

| № п/п | Правило | Описание правила |
| --- | --- | --- |
| 1 | Мониторинг электронной почты | Проведение постоянного мониторинга и анализа электронной почты сотрудников с целью выявления и предотвращения утечки конфиденциальной информации или нарушений внутренних правил компании |
| 2 | Мониторинг мессенджеров | Проведение регулярного мониторинга переписки сотрудников через мессенджеры, такие как WhatsApp, с целью выявления потенциальных угроз безопасности и предотвращения утечки конфиденциальной информации |
| 3 | Мониторинг корпоративных телефонов | Мониторинг использования корпоративных сотовых телефонов для контроля обмена информацией и предотвращения недобросовестного использования устройств с целью сохранения конфиденциальности информации компании |
| 4 | Мониторинг доступа к ИСПДн | Регулярное отслеживание и контроль за доступом к системам обработки персональных данных для предотвращения несанкционированного доступа или использования информации о сотрудниках и клиентах. |