ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ БИОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ (РОСБИОТЕХ)»

Международный технологический колледж

ПЦК «Информационные системы»

Дисциплина «Сертификация информационных систем»

Отчет к лабораторной работе № 1

«Анализ законодательства РФ в области защиты информации»

Выполнил:

студент группы 22б-ИСо-1

Сахацкая В.П.

Принял:

преподаватель Кучковский В.А.

Москва

2025 год

**СОДЕРЖАНИЕ**

Задание 1. Анализ ФЗ "О персональных данных"………………………..3

Задание 2. Создание справочника…………………………………………5

Задание 3. Анализ мер защиты информации……………………………...7

**Задание 1. Анализ ФЗ "О персональных данных"**

А) Глава 1 ФЗ "О персональных данных" содержит общие положения о целях и принципах обработки персональных данных, а также определения основных терминов, используемых в законе. В этой главе также устанавливаются права субъекта персональных данных и обязанности оператора при их обработке.

Глава 2 ФЗ "О персональных данных" регламентирует порядок обработки персональных данных, включая основные принципы, виды обработки, сроки хранения, перечень разрешенных действий с данными, требования к защите персональных данных и ответственность за их нарушение.

Б) Основные понятия:

Персональные данные - любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор - государственный орган, муниципальное образование, юридическое или физическое лицо, самостоятельно или совместно с другими определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Принципы обработки персональных данных:

- Обработка персональных данных осуществляется на законной и справедливой основе;

- Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

- Не допускается объединение баз данных, содержащих персональные данные, которые обрабатываются в целях, несовместимых между собой.

Условия обработки персональных данных:

- Согласие субъекта персональных данных на обработку его персональных данных;

- Обработка персональных данных допускается без согласия субъекта персональных данных в определенных случаях, предусмотренных законом.

В)

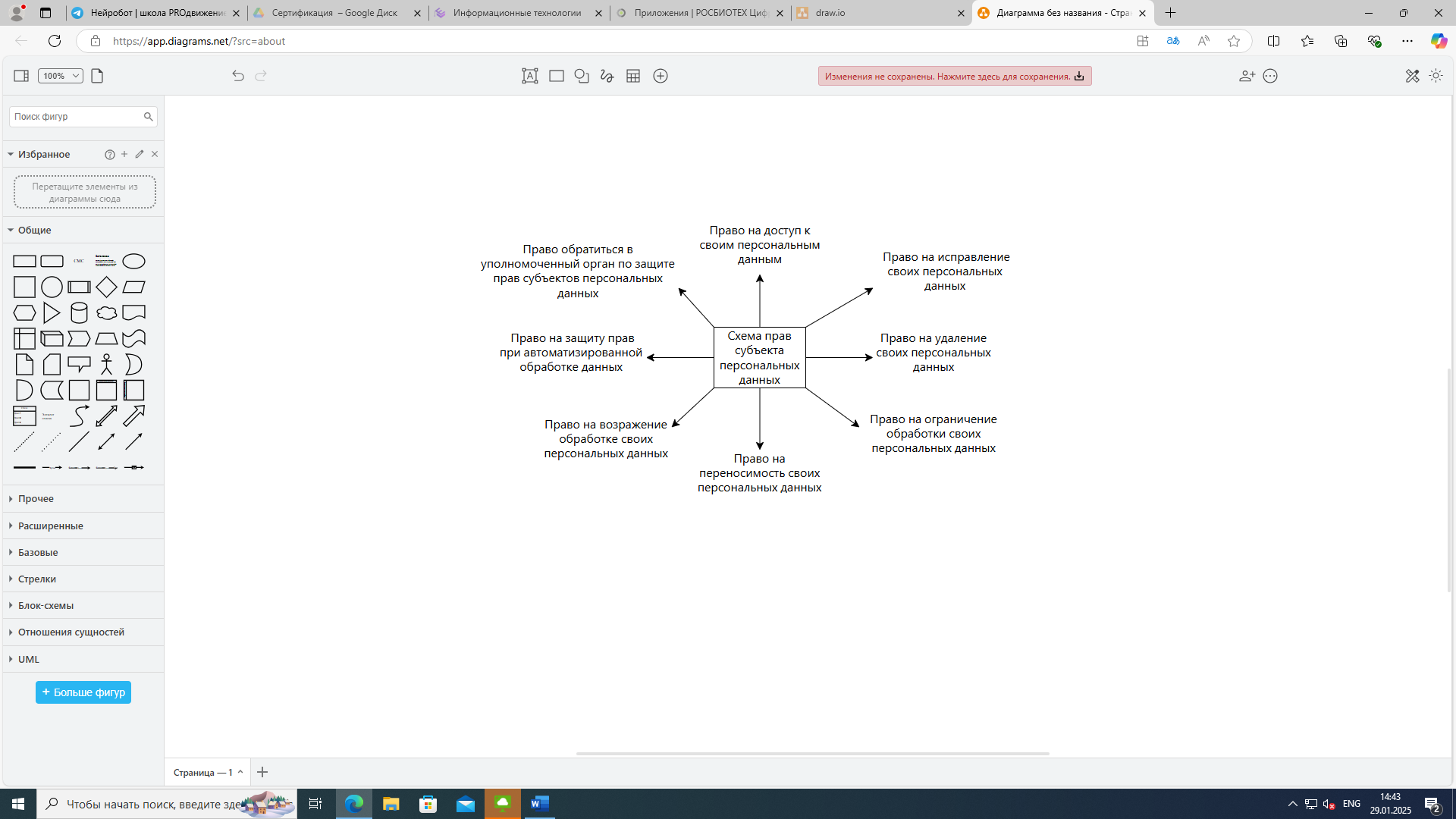


Схема 1 - Права субъекта персональных данных.

**Задание 2. Создание справочника**

А)

|  |  |
| --- | --- |
| Понятие | Определение |
| Информационная безопасность | Состояние защищенности информации от нежелательного доступа, разглашения, модификации или уничтожения. |
| Утечка персональных данных | Несанкционированное раскрытие персональной информации субъекта, которая может быть использована во вред. |
| Шифрование данных | Процесс преобразования информации в зашифрованный вид с использованием специальных алгоритмов. |
| Защита данных | Комплекс мер и действий по обеспечению конфиденциальности, целостности и доступности информации. |
| Политика информационной безопасности | Совокупность принципов, правил, процедур и мер, направленных на обеспечение информационной безопасности в организации. |

Таблица 1 – основные понятия и определения

Б) Перечень основных требований к защите персональных данных:

1. Обеспечение конфиденциальности персональных данных;

2. Обеспечение целостности и доступности персональной информации;

3. Регулярное проведение аудитов и проверок систем защиты данных;

4. Использование средств шифрования для защиты информации;

5. Установка ограничений доступа к персональным данным;

6. Обучение сотрудников правилам обработки и защиты данных.

В) Алгоритм действий при обнаружении утечки персональных данных:

1. Изолировать и остановить источник утечки данных;

2. Оценить объем и характер утекших данных;

3. Уведомить ответственных лиц о случившемся;

4. Восстановить утекшие данные и устранить причину утечки;

5. Провести анализ утечки и принять меры для предотвращения подобных инцидентов в будущем;

6. Провести обучение сотрудников по правилам обработки и защите персональных данных.

**Задание 3. Анализ мер защиты информации**

А) Статья 19 ФЗ-152 "Меры по обеспечению безопасности персональных данных" устанавливает обязанность оператора и иных лиц, имеющих доступ к персональным данным, принимать необходимые правовые, организационные и технические меры для обеспечения безопасности таких данных.

Б) Классификация мер защиты информации по категориям:

1. Правовые меры:

- Разработка и принятие внутренних документов, регулирующих порядок обработки персональных данных;

- Обеспечение соблюдения требований законодательства в области защиты персональных данных;

- Обеспечение контроля за соблюдением правил обработки персональных данных и соблюдением прав субъектов данных.

2. Организационные меры:

- Аудит безопасности информационных систем, содержащих персональные данные;

- Организация обучения персонала по правилам обработки персональных данных;

- Установление процедур управления доступом к персональным данным и их обработке.

3. Технические меры:

- Шифрование персональных данных при передаче и хранении;

- Защита информационных систем от несанкционированного доступа (пароли, антивирусное программное обеспечение, брандмауэры и др.);

- Регулярное обновление программного обеспечения и аппаратного обеспечения для предотвращения уязвимостей.

В) Примеры реализации мер защиты:

1. Правовые меры:

- Разработка Положения о защите персональных данных и внедрение его в деятельность организации;

- Составление соглашений с сотрудниками и контрагентами на обязательные меры по защите персональных данных;

- Проведение ежегодного аудита соблюдения законодательства о персональных данных и внутренних правил обработки информации.

2. Организационные меры:

- Организация обучающих семинаров для персонала по безопасной работе с персональными данными;

- Установление процедур контроля доступа к информационным системам с персональными данными;

- Создание документированных инструкций по работе с персональными данными и контролю за их обработкой.

3. Технические меры:

- Внедрение системы шифрования данных, передаваемых по открытым каналам связи;

- Установка брандмауэров и антивирусного программного обеспечения для защиты информационных систем;

- Регулярные обновления операционных систем и программного обеспечения для устранения уязвимостей и обеспечения безопасности персональных данных.