|  |  |
| --- | --- |
| **К Г Э У** | МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  **Федеральное государственное бюджетное образовательное учреждение высшего образования**  «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ» |

Отчет по лабораторной работе №1

по дисциплине «Информационная безопасность»

по теме «Изучение видов информации ограниченного доступа»

**Выполнил:**

студент Тазеев Рустам Рамилевич

Группа: ТРП-1-23

**Проверил:**

Доцент ИТИС

Хуснутдинов Рамиль Миннегаязович

Казань 2024

**Вариант 3**

**Цель работы**: изучение видов информации, для которых соблюдение конфиденциальности является обязательным согласно законодательным требованиям РФ в области информационной безопасности, а также ознакомление с ответственностью за их разглашение.

1. В своей работе в качестве вида информации я выбрал «персональные данные»

2. Перечень законодательных, нормативных правовых актов, регулирующих взаимоотношения в обществе, связанных с [выбранным видом информации с ограниченным доступом], представлен в таблице 1:

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Вид нормативного правового акта | Наименование нормативного правового акта | Статья, пункт, в котором упоминается вид информации с ограниченным  доступом |
| *1* | *Федеральный закон* | *Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»* | *Пункты 1-3* |
| 2 | *Распорядительный документ* | *Приказ Роскомнадзора от 30.05.2017 № 94* | *Пункты 1-3, Приложение 1* |
| 3 | *Федеральный закон* | *Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ* | *Статьи 1-25, сам федеральный закон имеет 670 упоминаний данного вида информации* |
| 4 | *Трудовое законодательство* | *Глава 14 Трудового кодекса Российской Федерации* | *Статья 86* |
| 5 | *Федеральный закон* | *Федеральный закон от 31.07.2020 № 248-ФЗ (ред. От 06.12.2021) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»* | *Статья 2, пункт 5, подпункт 22* |

Термины и определения, касающиеся [выбранного вида информации с ограниченным доступом], представлены в таблице 2.

Таблица 2

|  |  |
| --- | --- |
| Термин | Определение |
| Персональные данные | любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) |
| Оператор | государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие 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 |
| Автоматизированная обработка персональных данных | обработка персональных данных с помощью средств вычислительной техники |
| Распространение персональных данных | действия, направленные на раскрытие персональных данных неопределенному кругу лиц |
| Предоставление персональных данных | действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц; |
| Блокирование персональных данных | временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных); |
| Уничтожение персональных данных | действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных; |
| Обезличивание персональных данных | действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных; |
| Информационная система персональных данных | совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств; |
| Трансграничная передача персональных данных | передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. |

К персональным данным относятся следующие сведения:

* **Общие**: ФИО, дата рождения, адрес регистрации, СНИЛС, ИНН, информация об образовании, сведения о месте работы, номер телефона, e-mail, паспортные данные.
* **Специальные**: Расовая принадлежность, национальность, политические и религиозные взгляды, особенности здоровья, подробности интимной жизни, информация о судимостях.
* **Биометрические**: Отпечатки пальцев, группа крови, рост, вес, цвет глаз и волос, фотографии.
* **Иные**: В эту группу входит информация, которую нельзя отнести к другим видам персональных данных. Например, принадлежность к определенной социальной группе, трудовой стаж работника.

К персональным данным НЕ могут относиться следующие сведения:

* Госномер транспортного средства
* Лицевой счет ЖКХ
* Любая другая информация, связанная с имуществом человека, но не с ним самим

Описание порядка предоставления доступа (оформление допуска) к персональным данным представлено ниже.

1.Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

3. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

7. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

1) непосредственно;

2) с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

8. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий, предусмотренных настоящей статьей, не допускается.

Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

9. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

10. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений настоящей статьи или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

Требования, перечисленные в пунктах 6- 10 не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления функций, полномочий и обязанностей.

За правонарушения, связанные с разглашением сведений, относящихся к персональным данным предусмотрены виды юридической ответственности, представленные в таблице 3.

Таблица 3

|  |  |  |
| --- | --- | --- |
| Вид юридической ответственности | Основание (ссылка на статью, пункт НПА) | Правонарушение /  преступление |
| *Уголовная* | *Ст. 137 УК РФ* | *Распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации* |
|  |  |
|  |  |
| *Административная* | *Ст. 13.11 КоАП РФ* | *Нарушение законодательства Российской Федерации в области персональных данных* |
| *Ст. 13.14 КоАП РФ* | *Разглашение персональных данных (за исключением случаев, если это влечет уголовную ответственность) лицом, получившим к ним доступ в связи с исполнением служебных или профессиональных обязанностей,* |
|  |  |
| *Гражданско- правовая* | *Ст. 15, 151, 1082, 1099 - 1101 ГК РФ, ч. 2 ст. 24 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»* | *Разглашение персональных данных* |
|  |  |
|  |  |
| *Дисциплинарная* | *подп. «в» п. 6 ч. 1 ст. 81, ст. ст. 90, 192 ТК РФ* | *Разглашение персональных данных связанных с работой организации* |
| *Ст. 90, 238, п. 7 ч. 1 ст. 243 ТК РФ* | *Нанесение ущерба, причиненного работодателю в результате разглашения сведений, относящихся к персональным данным* |
|  |  |

Пример из судебной практики, относящийся к делу, связанному с нарушением норм, регулирующих взаимоотношения в обществе, связанных с персональными данными представлен в таблице 4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид юридической ответственности | Решение суда | Основание | Краткое описание правонарушения/ преступления | Ссылка на источник |
| Уголовная | Суд признал женщину виновной и штрафовал на 101 000 ₽. Трое потерпевших предъявили требования о компенсации морального вреда. Каждый получил по 10 000 ₽. | Государство гарантирует и охраняет тайну переписки и телефонных разговоров. Операторы сотовой связи должны ее обеспечить путем предупреждения сотрудников об уголовной ответственности за разглашение данных. | Управляющая салоном сотовой связи из Санкт-Петербурга решила подзаработать. Вопреки запретам о неразглашении конфиденциальной информации в трудовом договоре, она продала посторонним людям детализацию звонков семи абонентов.  В приговоре не сказано, как стало известно о преступлении. Скорее всего, незаконную покупку детализаций пресекли правоохранительные органы. | https://journal.tinkoff.ru/media/delo-no-1-154\_2021.k2uympntdzgh..pdf |

Примеры известных случаев несанкционированных воздействий на персональные данные представлены в таблице 5

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Краткое описание инцидента (добавить ссылку) | Негативные последствия | Возможные причины  инцидента |
| 1 | В связи с увеличением работы на удалёнке из-за пандемии, возросло количество утечек информации. Одной из крупнейших стала утечка данных 5 млн учащихся школы английского языка SkyEng, которая включает информацию о клиентах, учителях и сотрудниках, а также их контактные данные. Злоумышленники оценили стоимость этих данных в 40 тыс. рублей. Журналисты подтвердили подлинность утечки, которая произошла из-за доступа к серверу MongoDB весной текущего года. Такие инциденты, когда базы данных становятся доступными для продажи или бесплатного распространения, происходят всё чаще.  Источник: https://www.anti-malware.ru/analytics/Threats\_Analysis/Top-10-data-leakage-in-Russia | Варианты использования «слитых» данных варьируются от безобидно-надоедливых, таких как контекстная или таргетированная реклама, до серьёзных, когда пострадавшим пользователям от имени сервиса SkyEng могут предложить оплатить фейковые услуги. | Одним из сценариев утечки является атака извне на сервер, который хранит данные пользователей. Возможен и сбор сведений средствами социальной инженерии. Также используются различного рода фишинговые сайты, копирующие сервис-жертву. |
| 2 | В июле 2019 года с помощью DeviceLock были обнаружены крупные утечки данных клиентов «Альфа-банка». Первая база данных содержала информацию о 55 тыс. клиентов, включая Ф. И. О., контактные номера и адреса, датированные 2014 и 2015 годами. Вторая база, относящаяся к 2018–2019 годам, включала 504 записи с полными паспортными данными, балансами карт и информацией об отделениях обслуживания. С середины 2019 года эта база стала доступна в открытом доступе.  Кроме того, в одном архиве с ней находились базы других банков: ХКФ (24,4 тыс. клиентов с паспортными данными и контактами) и ОТП (800 тыс. клиентов с номерами телефонов, почтовыми адресами, лимитами и заметками о взаимодействии).  Источник: https://www.anti-malware.ru/analytics/Threats\_Analysis/Top-10-data-leakage-in-Russia | Основатель DeviceLock предположил, что появление базы «Альфа-банка» объёмом в 55 тыс. записей связано с массовым сокращением в конце 2014 года крупного ИТ-отдела. После инцидента с увольнением база долгое время находилась на различных форумах, и недавно её выложили в полностью открытый доступ. Исходя из размеров второй базы, а также из того, что клиенты, чьи данные в ней указаны, подходят под одну и ту же выборку по сумме счёта, можно сделать вывод, что виновником её утечки мог стать менеджер по клиентам. | Люди, записанные в базах, могут стать жертвами большого количества мошенников: информация оттуда открывает злоумышленникам широкие возможности по использованию социальной инженерии. |
| 3 | В 2021 году в одном кредитном союзе произошел инцидент, не связанный с утечкой информации, но также принесший огромный ущерб компании. | Бывшая сотрудница союза спустя два дня после увольнения зашла под своей учетной записью на сетевой диск и удалила 21 Гб данных, включая папку с названием «Не удалять», которая содержала лицензии и ПО для кибербезопасности организации. | Злоумышленницу удалось вычислить, но архив за последний год работы кредитного союза был уничтожен. Штраф составил $10 тысяч, нарушительнице грозит 10 лет тюрьмы. |

Основные организационные и технические меры, направленные на обеспечение безопасности, учитывающие специфику обработки [выбранного вида информации с ограниченным доступом] представлены ниже.

Организационные меры:

1. Основные организационные и технические меры, направленные на обеспечение безопасности, учитывающие специфику обработки персональных данных представлены ниже.
2. Организационные меры:
3. Разработка и принятие локальных нормативных актов и организационно-распорядительных документов по работе с персональными данными и их защите. Организации требуется принять такие ЛНА, как: политика защиты персданных, обработка пользователей ПДн сайтов; положения о порядке уничтожения персданных, о внутреннем аудите работы с персональными данными и т.д. Недостаточно скачать бланки необходимой документации из интернета, поставив название своей организации. Требуется адаптировать шаблоны документов под специфику осуществляемой хозяйственной деятельности.
4. Назначение ответственного лица (или лиц) за работу с ПНд. Указанные обязанности возлагаются в небольших организациях на одного сотрудника (как правило, юриста или кадровика) или нескольких. Обязанности по защите возлагаются приказом. В крупных компаниях создаются структурные подразделения, занимающиеся вопросами защиты персданных. Обязанности возлагаются приказом или закрепляются трудовым договором, должностными обязанностями. Рекомендуется разрабатывать документацию отдельно для каждой категории ПДн (например, для сотрудников компании и ее контрагентов).
5. Ознакомление сотрудников оператора с законодательными актами, ЛНА и внутренними приказами (распоряжениями), регламентирующими порядок работы с ПДн.
6. Обучение сотрудников в области работы и защиты персональных данных. Необходимо ответственно подходить к исполнению назначенным сотрудником возложенных на него обязанностей, понимать, что назначение не является формальностью. Назначенный работник должен обладать необходимыми знаниями и навыками. Это достигается путем прохождение специального обучения по работе и защите пресданных или самообразования.
7. Организация работы с субъектами персональных данных, контрагентами, что включает в себя заключение соглашений о конфиденциальной информации, выдачу поручения обрабатывать ПНд, получение согласия субъектов персданных.
8. Своевременное выявление и устранение нарушений требований к порядку работы с ПДн.
9. Организация рабочих помещений, в которых хранится и обрабатывается носитель ПДн: введение пропускного режима или контроля допуска третьих лиц в помещения, где хранятся носители ПДн, их нахождение только в сопровождении и под контролем работников организации (ИП), оборудование сейфов и специально отведенных мест для хранения носителей персданных.
10. Проведение анализа процессов работы с персданными для определения перечня необходимых технических мер защиты.
11. Регулярное изменение паролей на компьютерах и в информационных системах, которые используются для обработки персданных.

Технические меры:

1. Прохождение аттестации безопасности информационной системы, используемой для обработки персданных, с получением аттестата.
2. Управление доступом к персональным данным (протоколирование действий с персданными, оповещение о несанкционированном доступе в систему посредством применения соответствующих утилитов).
3. Обеспечение целостности персданных, которое осуществляется средствами самих операционных систем и систем управления базами данных. Необходимо использовать операционные системы, сертифицированные ФСТЭК и ФСБ.
4. Использование антивирусов, имеющих сертификаты ФСБ (например, Лаборатории Касперского), с целью предотвращения вирусных атак и сохранности ПДн.
5. Создание межсетевого экрана. Рекомендуется использовать межсетевые экраны третьего или четвертого уровня в зависимости от категории защищенности, к которой относится оператор персданных.
6. Анализирование защищенности на рабочих терминалах и серверах, принятие мер по устранению выявленных недостатков, усиление защитных мер. Для анализа используются сетевые сканеры, сертифицированные ФСТЭК и ФСБ.

**Выводы:** Выводы: согласно отчетам аналитиков (https://www.rbc.ru/society/11/03/2024/65ec41e89a7947dc41bd43f9), количество инцидентов информационной безопасности, связанных с несанкционированным воздействием на персональные данные в период с 2018 по 2023 годы возрастает, несмотря на принимаемые меры безопасности, из-за проблем в адаптации законодательства современным вызовам в информационном пространстве. Причинами данных инцидентов являются недостаточная защита систем, человеческий фактор и уязвимости программного обеспечения. Несанкционированные воздействия на персональные данные могут повлечь за собой финансовые убытки, утрату доверия со стороны клиентов и юридические последствия.

Считаю, что внедрение современных систем шифрования и регулярное обучение сотрудников может снизить количество правонарушений, связанных с персональными данными, так как это поможет предотвратить несанкционированный доступ и повысит общую осведомлённость о рисках информационной безопасности.

Такие меры, как многоуровневая аутентификация и мониторинг сетевого трафика, являются наиболее эффективными для защиты информации, составляющих персональные данные, так как они создают дополнительные барьеры для злоумышленников и позволяют своевременно выявлять подозрительные активности.

**Библиографические ссылки**

1. https://journal.tinkoff.ru/media/delo-no-1-154\_2021.k2uympntdzgh..pdf
2. <https://vc.ru/legal/621922-sud-v-moskve-oshtrafoval-skyeng-na-60-tysyach-rublei-za-utechku-dannyh-polzovatelei>
3. https://www.rbc.ru/finances/05/11/2019/5dbc07929a7947c6597cf70f
4. https://www.securitylab.ru/news/523953.php
5. https://www.rbc.ru/society/11/03/2024/65ec41e89a7947dc41bd43f9