Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Поволжский государственный технологический университет»

УДК 044.056

на правах рукописи

Насибуллин Константин Андреевич

Выпускная квалификационная работа

на тему

Методика и инструментальные средства создания документов по защите персональных данных в информационных системах.

Направление подготовки

10.04.01

(шифр)

Информационная безопасность

Научный руководитель д.т.н. Сидоркина И.Г.

г. Йошкар-Ола,

2023 г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....3

ГЛАВА 1 ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....6

1.1. Обзор понятий и терминов, связанных с защитой персональных данных 6

1.2. Законодательные и нормативные акты, регулирующие обработку и защиту персональных данных.....11

ГЛАВА 2 МЕТОДЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....21

2.1. Конфиденциальность.....21

2.2. Целостность и доступность.....23

2.3. Аудит и мониторинг.....28

2.4. Риски и угрозы.....36

ГЛАВА 3 СОЗДАНИЕ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.....46

ГЛАВА 4 РЕАЛИЗАЦИЯ БАЗЫ ДАННЫХ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....57

ЗАКЛЮЧЕНИЕ.....63

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.....65

ВВЕДЕНИЕ

С развитием информационных технологий, таких как Интернет, облачные вычисления, большие данные, искусственный интеллект, формируются новые риски и угрозы. Одной из таких угроз является возможность несанкционированного доступа к личной информации и ее использования, что негативно сказывается на конфиденциальности и безопасности личности. Широкое внедрение этих технологий может поставить под угрозу конфиденциальность. Поэтому создание соответствующего правового регулирования персональных данных становится важным для обеспечения защиты личных прав и контроля за использованием информации о себе. Институт персональных данных играет значительную роль в правовом статусе физического лица, направленном на обеспечение информационной безопасности. Проблема конфиденциальности и безопасного хранения таких данных особенно актуальна в цифровой среде.

В различных программных документах и исследованиях неоднократно обсуждались вопросы, связанные с защитой персональных данных и поиском баланса между интересами личности, государства и общества. Например, в государственной программе "Информационное общество на 2011-2020 годы" отмечается растущая угроза неконтролируемого роста информации о гражданах и отсутствие эффективного контроля за ее использованием в государственных информационных системах. Также наблюдается рост преступлений, связанных с нарушением конфиденциальности персональных данных при использовании информационных технологий.

Действующая Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы подчеркивает необходимость поддержания баланса между внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну.

В работе А.А. Гадельшина и М.М. Степанова рассматривается проблема классификации данных о людях, таких как файлы cookie, которые не считаются

персональными данными в Российской Федерации. Исследователи также обсуждают возможность получения таких данных злоумышленниками и вероятность их свободного обмена между третьими лицами. Был проведен сравнительно-правовой анализ законодательства Российской Федерации и Европейского союза, касающегося персональных данных. (Гаделышин, 2021)

Д.Р. Салихов отмечает, что распространение новой коронавирусной инфекции привело к возникновению множества вопросов, связанных с защитой персональных данных граждан. Эти вопросы включают обработку традиционных персональных данных в чрезвычайных ситуациях, использование биометрической идентификации для определенных категорий лиц и возможность использования генетической информации. (Салиханов, 2021)

Таким образом, различные исследования и документы подтверждают актуальность проблемы защиты персональных данных и необходимость разработки соответствующих мер и правовых норм для обеспечения конфиденциальности и защиты персональных данных граждан. Они призывают к соблюдению баланса между использованием современных технологий и защитой прав и интересов личности. Это включает в себя не только управление доступом к данным, шифрование и мониторинг, но и разработку политик безопасности, определяющих требования и правила обработки и использования персональных данных.

Для решения этих проблем и обеспечения безопасности персональных данных важно обращать внимание на законодательство, в том числе на законы о защите персональных данных в Российской Федерации. Эти законы устанавливают основные принципы и требования к обработке персональных данных, включая согласие субъекта данных, прозрачность, ограничение целей использования данных, а также обязательство обеспечивать безопасность и конфиденциальность данных.

Реализация мер по защите персональных данных требует комплексного подхода, который включает в себя не только технические и организационные

меры, но и правовые и социальные аспекты. Это означает разработку и внедрение соответствующих политик, процедур и планов реагирования на инциденты, а также обучение и осведомленность сотрудников об их ролях и обязанностях в области защиты персональных данных.

Наконец, важно постоянно отслеживать изменения в законодательстве и стандартах в области защиты персональных данных, а также отслеживать новые технологии и угрозы с целью адаптации и совершенствования мер безопасности в базе данных и обеспечения надежной защиты персональных данных.

В связи с указанным, целью работы является оценка методов и инструментальных средств создания документов по защите персональных данных в информационных системах. Для достижения указанной цели, были поставлены следующие задачи:

1. Рассмотрение основ защиты персональных данных.
2. Изучить методы защиты персональных данных.
3. Рассмотреть процесс создания документации по защите персональных данных.
4. Рассмотреть реализацию базы данных для защиты персональных данных.

Объект работы –защита персональных данных в информационных системах. Предмет - методы и инструментальные средства создания документов по защите персональных данных в информационных системах.

ГЛАВА 1 ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. Обзор понятий и терминов, связанных с защитой персональных данных

Защита персональных данных является одним из наиболее актуальных вопросов для компаний и организаций в России, включая коммерческий и государственный секторы. Законодательное регулирование защиты персональных данных в Российской Федерации осуществляется посредством нескольких федеральных законов и подзаконных актов. Примером такого законодательного акта является Федеральный закон № 152-ФЗ "О персональных данных", принятый в 2006 году, который направлен на защиту персональных данных, обрабатываемых государственными и коммерческими организациями. Несмотря на то, что с момента принятия этого закона прошло более десяти лет, обеспечение защиты персональных данных, обрабатываемых и хранящихся в информационных системах, остается одной из главных задач, как с точки зрения разработки нормативной базы, так и организации ее реализации. (152-ФЗ, 2006)

На данный момент существует множество работ и исследований, проведенных как отечественными, так и зарубежными учеными, которые посвящены вопросу обеспечения безопасности персональных данных. Эти работы доступны в различных источниках, включая онлайн-ресурсы, научные журналы и печатные издания. В этой статье мы сосредоточимся на тех, которые наиболее полно рассматривают проблемы в контексте государственного предприятия.

Например, в статье И.С. Козина предложен метод определения опасности угрозы, позволяющий составить список опасных угроз с учетом важности охраняемого объекта.(Козин, 2017) В работе В.В. Соловьева представлен способ организации схемы защиты информационной системы персональных данных. Существуют также концептуальные работы, посвященные разработке методов маскировки персональных данных в базе данных. (Соловьёв 2017)

Таким образом, доступны различные исследования и материалы, которые в значительной степени охватывают вопросы обеспечения безопасности персональных данных, в том числе в контексте государственных предприятий.

Также необходимо учитывать исследования других авторов, таких как А.В. Минбалеев из Южно-Уральского государственного университета (Челябинск), в которых также рассматриваются вопросы защиты персональных данных. (Минбалеев, 2012)

В Российской Федерации все персональные данные делятся на следующие категории в соответствии с научной классификацией:

- Общие персональные данные, такие как полное имя человека, место регистрации и проживания, номер мобильного телефона, адрес электронной почты. Обычно эти данные известны не только их владельцу, но и другим гражданам.
- Специальные персональные данные, включая политические взгляды, религиозную принадлежность, информацию о состоянии здоровья, судимости. Этот тип данных обычно защищен и доступен только по собственному желанию владельца.
- Биометрические персональные данные, такие как отпечатки пальцев, группа крови, физиологические параметры человека. Они считаются личными, если используются для идентификации личности. Например, если юридическое лицо использует сканер отпечатков пальцев для идентификации сотрудников, то оно работает с персональными данными, поскольку по ним можно определить личность человека.
- Другие типы персональных данных, включая информацию о заработной плате, датах отпуска, опыте работы и т.д. Эти данные не включены в предыдущие категории и могут варьироваться в зависимости от конкретной информации. (Кутенков, 2015)

Таким образом, для того, чтобы полностью разобраться в вопросах защиты персональных данных, важно рассмотреть исследования различных авторов, в том числе работы А.В. Минбалеева, и принять во внимание

различные типы персональных данных, которые существуют в Российской Федерации.

В России законодательство защищает все упомянутые данные от незаконного использования и распространения. Однако, несмотря на существующую законодательную защиту и обширную судебную практику, данные граждан Российской Федерации по-прежнему подвержены утечкам и часто становятся объектом купли-продажи. Согласно исследованию международной IT-организации "Лаборатория Касперского", цифровой профиль человека в Интернете, включающий полное имя, данные социальной сети, удаленный доступ к компьютеру и банковские реквизиты, может стоить от 50 до 75 долларов. Наличие таких данных позволяет злоумышленникам совершать противоправные действия, например, выдавать кредиты в банке на основании чужого паспорта.

В настоящее время число пользователей Интернета значительно увеличилось. Люди стали практически зависимы от общения и онлайн-ресурсов. Информация стала не только основным ресурсом, но и мощным инструментом в руках общества. Почти у каждого есть одна или несколько учетных записей электронной почты, но не все знают о возможных последствиях взлома. Угроза потери самых конфиденциальных данных, в том числе паспортных, становится реальностью. Кроме того, существует риск, когда мы привязываем наши банковские карты к онлайн-покупкам на веб-сайтах. В результате увеличилось количество ресурсов, доступных хакерам, которые получают несанкционированный доступ к базам данных с информацией о сообществе. Оперативная обработка персональных данных представляет реальную угрозу законным интересам и правам физических лиц. Проблема защиты личности от несанкционированного сбора, злоупотребления и незаконного распространения персональных данных остается актуальной для нашего государства и сегодня

Концепция "персональных данных" и ее регулирование являются важными аспектами в каждом государстве. В России особое внимание

уделяется обеспечению надежной защиты персональных данных. Согласно части первой статьи 24 Конституции России, сбор, хранение, использование и распространение информации о частной жизни человека без его согласия запрещено и представляет собой важное право личности. Однако осуществление этого права гражданами не было в достаточной степени учтено. Понятие "частная жизнь" не имеет четкого определения в законодательстве. Согласно Федеральному закону № 152-ФЗ от 27.07.2006 (с изменениями от 30.12.2020) "О персональных данных", персональные данные определяются как любая информация, относящаяся прямо или косвенно к конкретному или идентифицируемому физическому лицу. Очевидно, что действия, приводящие к несанкционированной потере информации о частной жизни человека, нарушают основной закон страны - Конституцию Российской Федерации. (152-ФЗ, 2006))

"Федеральный закон № 152-ФЗ "О персональных данных", принятый в 2006 году, регулирует защиту персональных данных, обрабатываемых в государственных и коммерческих организациях. Несмотря на то, что с момента принятия этого закона прошло более десяти лет, защита персональных данных, обрабатываемых или содержащихся в информационной системе, остается одной из актуальных задач, требующих совершенствования нормативно-правовой базы и эффективной организации ее реализации". Закон о персональных данных устанавливает минимальные требования к обработке биометрических персональных данных с целью проверки личности субъекта данных. Однако вопрос раскрытия таких утечек данных остается нерешенным и представляет серьезную угрозу безопасности граждан.

Поэтому в России одной из главных задач в области информационной безопасности является обращение к законодательной базе, регулирующей защиту конфиденциальных данных физических лиц, и ее совершенствование. В последнее время в стране наблюдается значительный рост числа массовых утечек персональных данных.

Очевидно, что утечка персональных данных может иметь различные причины, включая как объективные технические, так и субъективные, такие как халатность сотрудников или финансовая жадность. Персональными данными, попавшими в руки злоумышленников, можно злоупотреблять для совершения преступных действий, таких как получение кредитов, незаконные сделки с недвижимостью, денежные переводы и тому подобное.

Для организации защиты конфиденциальных данных требуется лицензия ФСТЭК на обработку персональных данных. Однако количество специалистов, обладающих необходимой квалификацией, опытом и знаниями в этой области, крайне недостаточно. Кроме того, требуются специальные помещения и соответствующее оборудование, доступ к которым может быть финансово недоступен для небольших организаций.

Некоторые работодатели не располагают достаточными ресурсами для переподготовки персонала, приобретения дополнительного оборудования и получения необходимых лицензий, необходимых для обеспечения безопасности персональных данных. Это связано с тем, что стоимость приобретения технических средств защиты персональных данных и обслуживания системы значительно превышает сумму уплаченных штрафов. (Шумкеева, 2018)

К сожалению, мы можем признать, что новые технологии противоречат существующим принципам законодательства, что свидетельствует о сомнительной эффективности действующего законодательства о защите персональных данных. В своем нынешнем виде законодательство о защите персональных данных отстает от современных технологий и требует кардинальных изменений.

1.2. Законодательные и нормативные акты, регулирующие обработку и защиту персональных данных

Существует значительная и фундаментальная нормативно-правовая база для решения этой актуальной и прикладной проблемы. Ниже приведены основные документы, включающие как федеральную законодательную базу, так и ведомственные акты:

- Федеральный закон № 152-ФЗ от 27 июля 2006 г. "О персональных данных";
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [35];
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации";
- Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. № 17 "Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";
- Приказ ФСТЭК от 18 февраля 2013 г. № 21 "Об утверждении состава и содержания организационно-технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Методика определения текущих угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (от 15 февраля 2008 г.);
- Банк данных об угрозах информационной безопасности (FSEC);
- ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения". М.: Стандартинформ, 2008;

- ГОСТ RISO/IEC 27002-2012 "Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил управления информационной безопасностью".

В настоящее время обработкой персональных данных занимаются специалисты по безопасности в каждой организации. Почти каждая организация управляет персональными данными своих сотрудников или партнеров. Каждый гражданин также взаимодействует с различными физическими и юридическими лицами, что приводит к созданию реестров или баз персональных данных. Однако применение существующих правил в этой области связей с общественностью сопряжено с трудностями для служб безопасности.

Когда персональные данные обрабатываются в базе данных, соблюдение, применение и правоприменение правил становится существенным условием. Одна из основных реформ, повлиявших на регулирование, связана с Федеральным законом 152-ФЗ, который ввел требование хранить персональные данные на серверах с 1 января 2021 года. Согласно закону, оператор, осуществляющий сбор данных, в том числе информации, полученной посредством информационно-телекоммуникационных систем, обязан регистрировать, систематизировать, компилировать, хранить, исправлять (обновлять, изменять) данные о гражданах Российской Федерации с использованием баз данных, расположенных на территории Российской Федерации.

Иногда возникают ситуации, когда по разным причинам персональные данные граждан становятся общедоступными, происходит так называемая утечка персональных данных. В настоящее время мы все чаще сталкиваемся с этим явлением. Например, в ноябре 2019 года произошла утечка клиентских данных Альфа-банка. Информация о лицах, подписавших кредитные и страховые договоры, была выставлена на продажу в Интернете. Эти договоры содержали полное имя, номер мобильного телефона, паспортные данные, адрес регистрации, сумму кредитного лимита или страховки, предмет страхования, а

также дату заключения договора. Граждане, передавая свои персональные данные юридическим лицам, индивидуальным предпринимателям или публично-правовым образованиям, надеются, что эти данные будут защищены и не будут переданы третьим лицам.

Для начала нам следует обсудить, что такое персональные данные и как они защищены в современной Российской Федерации. В соответствии с пунктом 1 части 1 статьи 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ (с изменениями от 24.04.2020) "О персональных данных" под персональными данными понимается любая информация, относящаяся к конкретному или идентифицируемому физическому лицу (субъекту персональных данных)..

Для обеспечения защиты персональных данных лица используются положения следующих нормативных правовых актов:

- Конституция Российской Федерации, принятая всенародным голосованием 12.12.1993 г. с поправками, одобренными в ходе всероссийского голосования 01.07.2020 г. Статья 24 этого правового акта гласит, что сбор, хранение, использование и распространение информации о частной жизни человека без его согласия запрещено. Это положение Конституции развито в двух перечисленных ниже правовых актах, посвященных защите информации о частной жизни человека.
- Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ. Данный правовой акт направлен на защиту прав и свобод человека и гражданина при обработке его персональных данных, включая право на неприкосновенность частной жизни и личную и семейную тайну.
- Кодифицированные правовые акты, такие как Уголовный кодекс Российской Федерации (статьи 137 и 272 Уголовного кодекса Российской Федерации), Кодекс Российской Федерации об административных правонарушениях (статья 13.11 Административного кодекса Российской Федерации) и Гражданский кодекс Российской Федерации (статья 152.2 Гражданского кодекса Российской Федерации), предусматривают различные виды ответственности за нарушение законодательства о персональных данных.

- Указ Президента Российской Федерации от 06.03.1997 № 188 (ред. от 13.07.2015) "Об утверждении перечня конфиденциальной информации". Этот правовой акт содержит точный перечень информации, которая считается конфиденциальной (коммерческая тайна, служебная тайна и т.д.).
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Настоящий правовой акт устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и определенные уровни безопасности таких данных. Эти нормативные правовые акты являются основой для обеспечения надлежащей защиты персональных данных, обеспечивая законодательную базу и правила, которые необходимо соблюдать при обработке и использовании таких данных. Они определяют права и обязанности субъектов персональных данных, требования к информационным системам, а также меры ответственности за нарушение правил обработки персональных данных. В совокупности эти нормативные акты создают основу для эффективной защиты персональных данных и обеспечения неприкосновенности личной жизни и конфиденциальности информации о частной жизни граждан.

Необходимо рассмотреть причины ситуаций утечки персональных данных в Интернете и проблемы, связанные с их защитой в сети. Существует первая проблема, связанная с прямой утечкой персональных данных в Интернет. Эта проблема возникает по целому ряду различных причин. (Трофимова, 2015)

В Российской Федерации существуют различные толкования положений Федерального закона № 152-ФЗ от 27 июля 2006 года "О персональных данных", которые могут вызвать двусмысленность. Позиции Роскомнадзора и судов по одному и тому же вопросу могут отличаться, и судебная практика может привести к различным решениям в спорных ситуациях. Например, возникает вопрос, является ли номер мобильного телефона персональными

данными. Согласно закону, номер мобильного телефона может рассматриваться как персональные данные, но Роскомнадзор считает, что это не так, поскольку речь идет о техническом устройстве, а не о личной характеристике человека. Судебная практика также неоднозначна в этом вопросе.

Несколько примеров могут проиллюстрировать эту ситуацию. В одном случае житель Белгорода подал в суд на ООО "Яндекс Директория" из-за публикации его номера телефона в Интернете. Роскомнадзор не обнаружил нарушений, так как номер был опубликован без указания владельца. Суд присоединился к мнению Роскомнадзора, решив, что номер телефона не является персональными данными, поскольку его невозможно однозначно идентифицировать, и отклонил иск жителя Белгорода. В другом случае Московский суд вынес иное решение. Коллекторское агентство позвонило гражданину без его согласия, имея только его номер телефона. Суд признал, что такая обработка персональных данных, включая номер телефона, нарушала Закон о персональных данных.

Существуют также различные интерпретации относительно использования фотографий в системе ACS в качестве биометрических персональных данных или нет. Непонимание законодательных положений приводит к ситуации, когда многие юридические лица должным образом не защищают номера телефонов или фотографии, не считая их персональными данными, что в конечном итоге приводит к утечке и распространению этих данных в Интернете. Из-за отсутствия четкого понимания законодательства многие организации не принимают достаточных мер для защиты телефонных номеров и фотографий людей, не рассматривая их как персональные данные. (Терещенко, 2018)

Такая ситуация представляет опасность для неприкосновенности частной жизни людей, поскольку их персональные данные могут стать доступными для неправомерного использования или распространения. Недостаточная защита персональных данных может привести к негативным последствиям, таким как

мошенничество, кража личной информации или нарушение неприкосновенности частной жизни.

Для обеспечения надлежащей защиты персональных данных необходимо более четкое и недвусмысленное толкование законодательства соответствующими государственными органами, такими как Роскомнадзор, а также скоординированная судебная практика по спорным вопросам. Это поможет устранить неопределенность и обеспечить последовательный подход к определению и защите персональных данных с целью предотвращения их неправильного использования и распространения в Интернете.

В Российской Федерации действуют низкие административные штрафы для юридических лиц, нарушающих законодательство о защите персональных данных. Такие штрафы варьируются от 15 000 до 75 000 рублей. Для небольших юридических лиц эта сумма может быть значительной и трудновыполнимой. В то же время крупные юридические лица, занимающиеся продажей персональных данных, могут легко справиться с таким штрафом, рассматривая его как стандартные "производственные издержки".

Причиной утечки персональных данных у некоторых юридических лиц является человеческий фактор, проявляющийся в различных аспектах. Некоторые сотрудники недостаточно осведомлены о требованиях российского законодательства о персональных данных. Другие сотрудники несерьезно относятся к своим обязанностям или выполняют закон лишь формально, не обеспечивая его фактического соблюдения. Известны также случаи, когда сотрудники организаций сами продают персональные данные своих сотрудников или клиентов третьим лицам.(Павлова, 2021)

Вторая проблема, связанная с защитой персональных данных в Интернете, заключается в том, что российским гражданам, пострадавшим от утечки персональных данных, практически невозможно получить компенсацию через суд от частных юридических лиц или государственных структур, ответственных за такие утечки. Это связано с тем, что успешные судебные иски в таких случаях могут вызвать цепную реакцию, когда каждый пользователь,

столкнувшийся с утечкой данных, подаст иски в суд с требованием компенсации. Учитывая низкий уровень защиты персональных данных в России, это может привести к серьезным финансовым потерям для юридических лиц.

Также возможно подавать иски против государственных органов, которые, несмотря на требования закона, относятся к защите персональных данных российских граждан с большой небрежностью.

Такие судебные иски могут негативно сказаться на бюджете страны. В результате дела этой категории рассматриваются в российских судах в течение длительного времени и часто приводят к присуждению минимальной компенсации пострадавшему лицу, чьи персональные данные были незаконно использованы. Однако эта компенсация не всегда позволяет вам полностью возместить убытки, понесенные в результате утечки персональных данных.

Чтобы решить первую проблему, автор данной работы предлагает разобраться со всеми причинами, приводящими к утечке персональных данных в Интернет. Во-первых, необходимо усовершенствовать законодательство о персональных данных. Федеральный закон № 152-ФЗ от 27.07.2006 (с изменениями от 24.04.2020) "О персональных данных" должен определять точный перечень персональных данных. Для этого вы можете воспользоваться классификацией персональных данных, разработанной учеными-юристами, и закрепить ее в статье 3 указанного правового акта. Например, статья 3 Федерального закона № 152-ФЗ от 27.07.2006 (с изменениями от 24.04.2020) "О персональных данных" можно сформулировать следующим образом: "Персональные данные - это информация, которая прямо или косвенно относится к определенному или идентифицируемому физическому лицу. Персональные данные включают в себя следующую информацию: полное имя человека, место регистрации и жительства, номер мобильного телефона, адрес электронной почты. Такие данные, в большинстве случаев, известны не только их владельцу, но и другим гражданам, политическим убеждениям, религиозной принадлежности, данным о состоянии здоровья, сведениям о судимости лица, а

также другой информации, признанной судом таковой в рамках рассмотрения и разрешения дела".

Чтобы решить проблему низких административных штрафов, необходимо стремиться к увеличению их размера таким образом, чтобы нарушение закона было невыгодным. Кодекс Российской Федерации об административных правонарушениях должен установить дифференцированный подход к административным штрафам, при котором размер наказания будет зависеть от оборота юридического лица - чем выше оборот, тем выше штраф. (Минбалеев, 2012)

Устранение третьей причины может быть осуществлено только самой организацией, поскольку она несет ответственность за наем сотрудников, а не государство. Поэтому решение этой проблемы должно быть возложено на юридические лица, а не на государство.

Чтобы решить вторую проблему в области защиты персональных данных в Интернете, необходимо убедить суды Российской Федерации в том, что права и свободы человека являются приоритетом для судебной системы. Суды не должны обращать внимания на экономическое положение юридических лиц или государственных органов, которые нарушили законодательство о персональных данных, что привело к нанесению ущерба гражданам. Суды обязаны справедливо рассматривать и разрешать дело, не задумываясь о возможных последствиях для "виновника" утечки персональных данных в случае вынесения неблагоприятного решения. Для достижения этой цели возможно издание специального постановления Пленума Верховного Суда Российской Федерации, в котором будут разъяснены правила применения положений российского законодательства о защите персональных данных.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является органом, ответственным за мониторинг и надзор за обработкой персональных данных, защиту прав субъектов персональных данных и средств массовой информации в России.

Кроме того, в этой области существуют и другие организационные и технические проблемы. Таким образом, персональные данные можно определить как любую информацию, относящуюся к определенному или идентифицируемому физическому лицу, которая передается другим лицам. Законодательное регулирование защиты таких данных осуществляется Конституцией Российской Федерации, Федеральным законом "О персональных данных" от 27.07.2006 № 152-ФЗ и соответствующими подзаконными актами. Однако, несмотря на обширные правовые меры, в настоящее время в области защиты персональных данных в Интернете существуют две проблемы. Первая проблема заключается в утечке таких данных в сеть, а вторая заключается в том, что получить компенсацию за ущерб, причиненный такой утечкой, крайне сложно. Решение этих двух проблем должно заключаться в устранении их причин. Если они будут успешно устранены, процент утечки персональных данных в Интернете в Российской Федерации должен значительно снизиться.

В заключение, стоит отметить, что понятие персональных данных и системы защиты информации играют важную роль в современном информационном обществе. Персональные данные представляют собой информацию, относящуюся к конкретному лицу, которая может быть использована для его идентификации. Защита персональных данных имеет особое значение, поскольку неправомерное их использование может привести к нарушению приватности и угрозам для личной жизни. (Минбалеев, 2012)

Правовое регулирование защиты персональных данных осуществляется на государственном уровне и направлено на обеспечение конфиденциальности и безопасности таких данных. Многие страны принимают законодательные акты, которые определяют права и обязанности операторов и субъектов персональных данных, а также устанавливают меры и процедуры для обеспечения их защиты.

В современных условиях, с увеличением объема и сложности обработки персональных данных, становится все более важным обеспечение надежной системы защиты информации. Это включает в себя применение технических и

организационных мер, направленных на предотвращение несанкционированного доступа, утечки и повреждения персональных данных.

Операторы имеют ответственность за обработку персональных данных в соответствии с принципами прозрачности, справедливости и законности. Субъекты персональных данных также обладают определенными правами, включая право на доступ к своим данным, их исправление, удаление и ограничение обработки. (Павлова, 2021)

В целом, правовое регулирование защиты персональных данных и развитие систем защиты информации являются важными аспектами в современном информационном обществе. Это позволяет обеспечить конфиденциальность, приватность и безопасность персональных данных, способствуя доверию и эффективному функционированию цифровой экономики и общества.

ГЛАВА 2 МЕТОДЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Конфиденциальность

В соответствии со статьей 7. Конфиденциальность персональных данных в соответствии с Федеральным законом № 261-ФЗ от 25.07.2011. Операторы и иные лица, получившие доступ к персональным данным, обязаны не разглашать и не распространять персональные данные третьим лицам без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Конфиденциальность персональных данных является обязательным требованием, которое должны соблюдать операторы и другие лица, имеющие доступ к таким данным. Однако конфиденциальность не применяется в случаях, когда личная информация обезличена или является общедоступной. Персональные данные перестают считаться конфиденциальными, если они обезличены или с момента их хранения прошло 75 лет, если иное не предусмотрено законодательством Российской Федерации.

Согласно Федеральному закону № 152-ФЗ, операторы персональных данных обязаны обеспечивать безопасную обработку таких данных путем принятия организационных и технических мер, направленных на конфиденциальность и защиту персональных данных от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, распространения и других противоправных действий. Операторы также обязаны уведомлять уполномоченный орган по защите прав носителей персональных данных (Роскомнадзор) о своем намерении обрабатывать персональные данные. Роскомнадзор включает данные об операторе в реестр операторов, которые находятся в открытом доступе. Исключением является информация о средствах обеспечения безопасности персональных данных при их обработке.

Оператор обязан получить письменное разрешение от носителей персональных данных перед их обработкой, в том числе данных, полученных

от третьих лиц. Обработка может начаться только после получения такого разрешения, за исключением случаев, предусмотренных федеральным законом, или когда эта информация является общедоступной. Важно отметить, что носитель данных имеет право запретить обработку своей личной информации.

Оператор обязан предоставить носителю персональных данных всю имеющуюся о нем информацию по запросу, а также о методах защиты данных, целях и условиях обработки. В обязанности оператора также входит уничтожение, блокирование или модификация соответствующих персональных данных по запросу носителя персональных данных или его законного представителя, если информация является неполной, неточной, устаревшей, полученной незаконным путем или не соответствует цели обработки. (Катунцева, 2016)

Оператор также должен подтвердить, что субъект согласен на обработку его персональных данных. В случае обработки общедоступных персональных данных оператор обязан предоставить доказательства того, что информация доступна каждому. Оператор обязан предоставлять уполномоченному органу по защите прав субъектов персональных данных необходимую информацию по запросу для осуществления своей деятельности. В России деятельность операторов персональных данных контролируется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности. Закон также определяет случаи, когда согласие субъекта персональных данных не требуется. Это может быть в случаях, когда: данные обрабатываются в соответствии с другими федеральными законами; между оператором и субъектом персональных данных заключено соглашение, предусматривающее обработку информации о субъекте; обработка персональных данных необходима для защиты жизни, здоровья и других жизненно важных интересов субъекта, но получение его согласия невозможно, например, если физическое лицо находится в больнице; персональные данные необходимы для доставки почты почтовыми

предприятиями; данные должны обрабатываться журналистом в профессиональных целях. целях или в научных, литературных или иных творческих целях, если это соответствует интересам и правам субъекта персональных данных; персональные данные должны обрабатываться для последующей публикации на основании федерального закона. Во всех остальных случаях оператор обязан действовать в соответствии с законодательством Российской Федерации об обработке информации и соблюдать конфиденциальность персональных данных. В случае нарушения закона оператор может понести уголовную, административную, гражданско-правовую, дисциплинарную или иную ответственность. (Каунцева, 2016)

2.2. Целостность и доступность

Целостность персональных данных означает, что данные не подвергались каким-либо изменениям или изменения были внесены только с согласия соответствующих субъектов, которым принадлежат эти данные (в соответствии с пунктом 3.1.6 Р 50.1.056-2005 "Техническая защита информации. Основные термины и определения"). Нарушение целостности персональных данных может нанести наименьший ущерб субъекту, поскольку субъект имеет право потребовать восстановления целостности своих персональных данных. Если субъекту сложно воспользоваться этим правом, считается, что есть основания для судебного иска, следовательно, нарушение целостности персональных данных влечет за собой моральный ущерб.

В случае нарушения целостности персональных данных в информационных системах персональных данных могут произойти следующие деструктивные действия:

1. Нанесение вреда программному обеспечению и пользовательским данным.

2. Повреждение встроенного ПО, данных и драйверов устройств в системе персональных данных.

3. Нанесение вреда программам, данным и драйверам устройств, ответственным за загрузку операционной системы и функционирование средств информационной безопасности.

4. Нанесение вреда программам и данным специализированного программного обеспечения.

5. Внедрение вредоносных программ, аппаратных и программных закладок и тому подобное.

6. Влияние на инструменты управления конфигурацией сети.

7. Нанесение ущерба средствам защиты информации. (Козин, 2017)

Угрозы целостности персональных данных включают потерю, уничтожение, дезинформацию и модификацию персональных данных.

Таким образом, принимая во внимание вышеизложенное, нарушение целостности персональных данных означает осуществление деструктивных действий, таких как уничтожение или модификация данных. Законодательство Российской Федерации предусматривает ответственность за нарушение целостности персональных данных, в том числе в следующих случаях:

- Незаконное уничтожение или изменение персональных данных (часть 6 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях, статья 272 Уголовного кодекса Российской Федерации);
- Хищение чужого имущества или получение права на чужое имущество путем удаления или изменения персональных данных (статья 159.6 Уголовного кодекса Российской Федерации);
- Незаконное изменение персональных данных (статья 272 Уголовного кодекса Российской Федерации).

Обеспечение целостности данных достигается за счет защиты базы данных от несанкционированного доступа. Для этого используются различные технические, программные и организационные меры, которые доступны системным администраторам. Если основной задачей является предотвращение нарушений целостности данных, то это достигается путем установления правил работы с базой данных. Выбранная версия СУБД должна предоставлять

инструменты для обнаружения информационных инцидентов, которые могут привести к повреждению системы, а также механизмы восстановления базы данных в исходное состояние, например, посредством резервного копирования данных. (Бурдов, 2015)

Системные операторы должны изначально установить набор логических правил, известных как ограничения целостности, которые предотвратят изменение данных в базе данных. Эти ограничения выполняют две функции одновременно:

1. Установите параметры, которые нельзя изменять для каждой единицы информации, например, определенное количество или значение символов.

2. Установите связи между определенными объектами, например, ссылками.

При настройке параметров работы базы данных и установлении этих правил обеспечивается определенная степень целостности данных в базе данных.

Для программиста, ответственного за обеспечение целостности данных в базе данных, первым шагом является создание табличного формата. На этом этапе вы должны:

- Создайте список допустимых значений для каждого столбца таблицы.
- Обеспечьте целостность данных в каждом конкретном столбце.

На практике концепция целостности данных имеет следующие аспекты:

- Необходимая целостность данных, где символьные строки определяются как уникальные элементы, специфичные для конкретной таблицы или базы данных.
- Целостность данных домена, когда записи в определенном столбце таблицы должны соответствовать указанным правилам. Для этого определяется тип данных в базе данных, например, только цифры, а формат записи устанавливается с помощью команды CHECK, диапазон возможных значений

ограничивается с помощью ВНЕШНЕГО ключа, CHECK, DEFAULT, NOT NULL и других правил, указанных при создании формата таблицы.

- Ссылочная целостность, при которой связи между таблицами, установленные с помощью гиперссылок, сохраняются независимо от добавления или удаления строк. Этот аспект особенно важен в базах данных SQL.(Гадельшин, 2012)

Параметры целостности данных определяются при создании архитектуры базы данных с использованием программного кодирования, требующего определенной квалификации персонала. Важно понимать природу данных, чтобы обнаруживать ошибки или вредоносные модификации.

Не существует абсолютных критериев достоверности информации; есть только критерии постоянства информации и отсутствия признаков преднамеренного изменения. При создании правил, обеспечивающих сохранность и неприкосновенность информации, применяется несколько общих типов ограничений:

- Обязательные данные, которые должны присутствовать в базе данных в любой ситуации. Если такие данные отсутствуют, это может свидетельствовать о нарушении целостности. Конкретное поле не может содержать пустое значение.
- Ограничения для данных, вводимых в определенные поля. Для каждого поля устанавливаются правила, определяющие допустимый набор данных.
- Ограничения, определяемые корпоративными правилами, установленными системными администраторами в соответствии с политикой компании по защите конфиденциальных данных.
- Целостность сущностей. Системный администратор вводит один или несколько ключей, которые совместно подтверждают целостность данных в поле таблицы. Важно понимать, что даже при наличии набора правил невозможно гарантировать абсолютную достоверность данных.

- Ссылочная целостность. Логические связи создаются между различными полями одной и той же таблицы или нескольких таблиц в базе данных. Целостность данных обеспечивается наличием неизмененных и не удаленных ссылок, подтверждающих, что информация не была подделана. Таблицы могут иметь иерархическую структуру, находиться на одном уровне или иметь отношения "родитель-потомок". В случае отношения "один ко многим" одна запись в родительской таблице соответствует нескольким записям в дочерней таблице. (Бачило, 2016)

Любые изменения в информации, будь то авторизованный пользователь или результат несанкционированного доступа, могут нарушить целостность данных. Установка правил для изменений может помочь решить эту проблему. Особое значение имеет сохранение ссылочной целостности, что достигается введением следующих правил:

- При вставке новых строк в таблицу имейте в виду, что не создаются новые ссылки, не связанные с иерархической структурой таблицы. Они должны оставаться пустыми или соответствовать изначально заданным параметрам.
- Удаление строки из дочерней таблицы не влияет на ссылочную целостность.
- Вставка строки в родительскую таблицу не создает новых ссылок.
- Удаление строки из родительской таблицы нарушает ссылочную целостность. Для решения этой ситуации может быть применено несколько подходов: полный запрет на удаление, установление правила, при котором исправление родительской таблицы автоматически приводит к удалению всех связанных ссылок в дочерних таблицах, замена ссылок в дочерней таблице пустыми значениями или использование изначально установленных значений по умолчанию. В некоторых случаях может быть установлено правило, запрещающее какие-либо изменения. Администратор базы данных определяет стратегию выбора при разработке архитектуры базы данных. Чтобы обеспечить семантическую целостность при изменении значений, необходимо установить

правила, соответствующие бизнес-процессам компании, максимально подробно прописывающие семантическую целостность. (Дроменко, 2016)

Если в организации используется модель взаимодействия клиент-сервер, то основные правила поддержания целостности данных в базе данных должны храниться на сервере. Это позволяет решать следующие задачи:

- Предоставление гарантий целостности данных, которые являются общими или аналогичными для всех приложений.
- Создание единой системы доступа к данным.
- Обеспечение быстрой реализации правил целостности за счет повышения производительности сервера. Однако есть и недостатки:
- Клиентское приложение не может отслеживать неправильно установленные правила целостности на сервере.
- Ограниченные возможности языка SQL, который не всегда может решить все проблемы, связанные с обеспечением целостности базы данных в приложениях. В большинстве случаев технические решения реализуются на сервере, что создает более высокий уровень защиты информации.

2.3. Аудит и мониторинг

Государство возлагает на операторов персональных данных (ПДН) ряд обязанностей, направленных на защиту конфиденциальности личной жизни граждан. Для выполнения этих обязанностей необходимо принять организационные меры, которые ограничат несанкционированный доступ (НРД) к конфиденциальной информации. Для обеспечения безопасности информации используется сертифицированное программное и аппаратное обеспечение. Контроль за соответствием обработки персональных данных требованиям законодательства осуществляют государственные органы, такие как Роскомнадзор и ФСТЭК России. Внутренний контроль на уровне организации поможет подготовиться к проверкам и избежать наложения штрафов.

С момента, когда компания начинает обработку персональных данных и уведомляет об этом Роскомнадзор, она попадает под надзор государственных органов, ответственных за контроль за соблюдением законодательства. Защита персональных данных стала важным компонентом национального законодательства, направленного на защиту прав на неприкосновенность частной жизни и сохранность информации о личной жизни. В рамках этой концепции оператор персональных данных - это юридическое лицо или индивидуальный предприниматель, который начинает обрабатывать личную информацию лиц, не являющихся его сотрудниками, например, клиентов банка, абонентов мобильной связи или покупателей в интернет-магазинах..

Оператор несет ответственность за следующие аспекты:

- Обеспечение сохранности данных и предотвращение их утечки или разглашения.
- Соблюдение правил обработки персональных данных в соответствии с заявленными целями настоящей процедуры. Оператор также несет ответственность за действия своих сотрудников и третьих лиц, которым данные передаются для обработки. Законодательство в целом описывает нормы ответственности, которые можно разделить на следующие категории:
- Дисциплинарная ответственность. За утечку персональных данных или иное неосторожное обращение с ними, например, их уничтожение, сотрудник может быть подвергнут дисциплинарному взысканию, замечанию или выговору. В некоторых случаях разглашение персональных данных может стать основанием для увольнения.
- Гражданская ответственность. Если организация или ее сотрудник причинили ущерб правообладателю, компенсация за этот ущерб ложится на виновника.
- Административная ответственность. Наказание в рамках административного правонарушения в соответствии с законом может включать штрафы и приостановление деятельности, связанной с использованием персональных данных.

- Уголовная ответственность. Уголовный кодекс Российской Федерации предусматривает ответственность за умышленное разглашение персональных данных, причиняющее значительный ущерб. Административная ответственность регулируется статьей 13.11 Кодекса Российской Федерации об административных правонарушениях. Оператор персональных данных может быть оштрафован за нарушения при работе с данными, такие как:
- Обработка персональных данных в целях, не предусмотренных законом, или в противоречии с ранее заявленными целями.
- Обработка данных без получения согласия правообладателя.
- Отказ в разработке или публикации политики по работе с данными, находящимися в открытом доступе.
- Непредоставление правообладателю информации о судьбе его данных.
- Отказ в уточнении, блокировании или удалении данных по запросу субъектов.
- Несоблюдение требований Федеральной службы по техническому и экспортному контролю Российской Федерации в части использования сертифицированного программного обеспечения для защиты информации.
- Отказ от хранения персональных данных на серверах, расположенных на территории Российской Федерации.(Головина, 2015)

Таким образом, оператор персональных данных несет ответственность за эти аспекты, и нарушение этих требований может привести к различным видам ответственности, включая дисциплинарную, гражданско-правовую, административную и уголовную. Административные штрафы, связанные с нарушением законодательства о персональных данных, определены в статье 13.11 Кодекса Российской Федерации об административных правонарушениях.

Уровень ответственности варьируется в зависимости от нарушения. Например, физические лица могут быть оштрафованы на 1000 рублей за незначительные нарушения, в то время как организации, которые неоднократно нарушают закон и отказываются хранить персональные данные граждан за

пределами России, могут быть оштрафованы на сумму до 18 миллионов рублей.

Стоит также отметить, что статья 13.14 Кодекса Российской Федерации об административных правонарушениях регулирует случаи разглашения информации с ограниченным доступом, в том числе персональных данных. В этом случае штрафы могут быть невелики, но ответственность распространяется даже на специальных субъектов права, таких как юристы, которые в своей служебной деятельности несут ответственность за разглашение конфиденциальной информации.

Кроме того, статья 5.39 Кодекса Российской Федерации об административных правонарушениях вводит дополнительную ответственность за отказ в раскрытии гражданину информации о том, какие документы о нем были собраны и какая информация имеется в организации. Это защищает права граждан понимать, какая информация о них находится в распоряжении третьих лиц. Кадровые агентства или службы безопасности работодателей, не получая согласия соискателей, иногда совершают подобные действия, и законодательство защищает права граждан в этом отношении.

Незаконные действия, связанные со сбором и распространением информации, могут быть квалифицированы как преступления и подпадать под действие уголовно-правового регулирования. Согласно статьям 137 и 212 Уголовного кодекса Российской Федерации предусмотрена ответственность за получение информации о гражданах без их согласия и передачу такой информации третьим лицам. Интересно отметить, что сбор и распространение информации и персональных данных граждан может быть наказуемо, даже если речь идет о данных умерших лиц, и информация была распространена без согласия их наследников. Например, в 2012 году гражданин был привлечен к уголовной ответственности по статье 137 Уголовного кодекса Российской Федерации за сбор информации о репрессированных этнических немцах Поволжья и распространение ее через архивы.

Проверки, проводимые государственными органами, такими как Роскомнадзор, ФСТЭК Российской Федерации и ФСБ Российской Федерации, являются формой контроля за соблюдением требований законодательства, касающихся обработки персональных данных. Роскомнадзор проверяет соблюдение общих требований законодательства в области защиты персональных данных. Это включает в себя проверку соответствия целей обработки персональных данных целям, указанным в уведомлении о начале деятельности, наличие публичной политики в отношении использования персональных данных на веб-сайте организации, получение согласия на обработку данных, наличие назначенных ответственных лиц и другие организационные и административные процедуры. документация.

ФСТЭК проверяет наличие технических средств защиты информации, и важно, чтобы использовались программные средства, рекомендованные и сертифицированные этим ведомством. Проверки могут быть плановыми или внеплановыми. Плановые проверки проводятся не чаще одного раза в три года, и первая из них происходит не ранее чем через три года после уведомления Роскомнадзора о начале деятельности, связанной с обработкой персональных данных. Внеплановая проверка может быть проведена в любое время в случаях, когда возникает экстренная ситуация, например, если умышленное разглашение персональных данных причинило значительный вред гражданам.

Для проведения внеплановой проверки должны быть выполнены два условия:

- Наличие информации о существенном нарушении закона, жалобах или истечении срока, предусмотренного для исправления ранее допущенных нарушений.
- Получение согласия областной прокуратуры на проведение контрольных мероприятий.

Внеплановая проверка может быть проведена только в серьезных случаях:

- Компания не выполнила предписания, изданные в результате плановой проверки, или не предоставила отчет о выполнении этих предписаний.
- Получен сигнал от граждан, компаний, правоохранительных органов, средств массовой информации или муниципальных властей о критической ситуации, которая представляет угрозу жизни или здоровью граждан или нарушает другие их права. Также может быть проведена внеплановая проверка, если деятельность организации не соответствует заявленным позициям, указанным в уведомлении. Заявление, на основании которого проводится внеплановая проверка, должно позволять установить личность заявителя.

Информация о планируемой проверке доступна компании в течение всего года в соответствии с графиком, размещенным на сайтах Генеральной прокуратуры и Роскомнадзора. Однако в случае проведения внеплановой проверки компания предупреждается за сутки по контактным каналам, указанным в уведомлении о начале действий, связанных с обработкой персональных данных. (Павлова, 2021)

Порядок проведения проверок Роскомнадзором определен в регламенте, с которым можно ознакомиться на официальном сайте ведомства. Правила описывают два типа проверок:

- Документальная проверка, осуществляемая путем запроса необходимых документов, которые затем изучаются в территориальном управлении Роскомнадзора.
- Выездная проверка, в ходе которой сотрудники Роскомнадзора посещают офис организации и на месте изучают документы и процедуры обработки персональных данных.

Инспекционная группа всегда состоит как минимум из двух сотрудников территориального подразделения, и при необходимости они могут пригласить эксперта или другого уполномоченного представителя. Продолжительность каждого вида проверки ограничена 20 днями, но по мотивированному решению

территориального подразделения Роскомнадзора срок может быть продлен еще на 20 дней. Это дополнительное время может потребоваться в случаях, когда проверяемые организации не предоставляют требуемые документы или когда в представленных документах имеются неясности.

Результатами аудита являются:

- Подготовка отчета о проверке и его направление в организацию.
- Выдача предписания об устранении выявленных нарушений закона.
- Привлечение оператора к административной ответственности.
- Выдача приказа о приостановлении деятельности.
- Направление мотивированного заключения в правоохранительные органы с просьбой привлечь сотрудников оператора к уголовной ответственности.

Акт проверки может быть обжалован в вышестоящее подразделение федеральной службы в случае несогласия с ее результатами, а протокол о привлечении к административной ответственности может быть обжалован в суде.

Роскомнадзор выступает гарантом соблюдения оператором требований законодательства об обработке персональных данных. Если гражданин обнаруживает нарушение своих прав, у него есть возможность обратиться в это ведомство. Роскомнадзор обязан оперативно реагировать на следующие виды обращений:

- Обработка персональных данных без получения согласия гражданина.
- Незаконный запрос информации о судимости, который разрешен только государственными и муниципальными органами.
- Несоответствие целей использования персональных данных ранее заявленным.
- Передача персональных данных третьим лицам для обработки или в иных целях без получения согласия гражданина.

- Раскрытие персональных данных, например, через средства массовой информации.
- Неразрушение персональных данных в случаях, предусмотренных законом. Например, банк обязан уничтожить все данные о лицах, которым было отказано в выдаче кредита, в течение трех дней после отказа.
- Отказ в блокировании, уточнении или уничтожении персональных данных.

Отказ оператора персональных данных предоставить информацию о наличии в его распоряжении документов и данных о гражданине.

Один из примеров, когда вмешательство Роскомнадзора помогло пресечь незаконный сбор и распространение персональных данных, произошел в 2019 году в подмосковных школах, где представители бизнес-школы Synergy собирали биометрические данные - отпечатки пальцев - с целью определения навыков и умений школьников без получения согласия родителей. Благодаря вмешательству агентства и выполнению им функций по контролю за соблюдением законодательства об обработке персональных данных незаконная практика была пресечена.

В случае нарушения прав вы можете обратиться в агентство не только по поводу российских резидентов, но и по поводу иностранных компаний, работающих в России. На официальном сайте этого ведомства вам необходимо перейти в раздел "Обращения граждан" и выбрать подраздел "Обработка персональных данных". В рамках обращения вы должны изложить суть проблемы и оставить свое полное имя и адрес для получения официального ответа.

Для того чтобы подготовиться к проверке соблюдения законодательства об обработке персональных данных, можно возложить обязанности по контролю за соблюдением этого законодательства на службу внутреннего контроля. Определив функции проверки в положении об этой услуге, можно гарантировать, что она проводится регулярно, что позволит компании быть готовой к приезду инспекторов. Если служба внутреннего аудита не обладает

такими полномочиями, то аудит проводится специально сформированной комиссией, в которую при необходимости могут входить внешние эксперты. Это особенно актуально, если компания подлежит проверке со стороны ФСТЭК.

В дополнение к основным принципам проверки соблюдения прав субъектов персональных данных, включены следующие аспекты:

- Контроль программного обеспечения, проверка наличия сертификатов ФСТЭК РФ и их актуальности, законности приобретения программного обеспечения, а также наличия платежных документов.
- Наличие функционирующей системы контроля доступа пользователей к информационным ресурсам, содержащим персональные данные, с учетом принципа разграничения прав доступа.
- Ведение журнала действий пользователя.

Результатом проведенных контрольных мероприятий должны стать рекомендации по подготовке к аудиту. Если бюджет организации не позволяет внедрить программное обеспечение, рекомендованное агентством, в нормативных документах предусмотрены компенсационные меры, и проверяющие органы должны предложить организации, какие из этих мер могут быть использованы.(Павлова, 2021)

Внешний и внутренний контроль направлены на защиту прав граждан на неприкосновенность персональных данных, конфиденциальность личной жизни и семейных тайн. Организации должны самостоятельно проводить проверки для оценки соответствия своей деятельности законодательству.

2.4. Риски и угрозы

Вся деятельность лиц, имеющих доступ к охраняемым законом информационным ресурсам с персональной информацией, должна основываться на нормах, установленных "Моделью". В рамках "Модели" существуют четыре категории субъектов, которые могут нанести ущерб охраняемым законом интересам:

- Граждане России, преследующие свои личные цели.
- Иностранные разведывательные службы.
- Другие иностранные организации, будь то террористические или коммерческие структуры.
- Преступные группировки.

Шаги, предпринимаемые этими субъектами и направленные на нарушение безопасности и целостности защищаемых информационных ресурсов, могут нанести ущерб интересам личности, общества и государства.

Государственное учреждение разработало модель действий для различных типов нарушителей. Согласно этому документу, посягательства могут осуществляться следующими способами:

- Перехват или копирование информации, передаваемой по каналам связи, с целью ее незаконного распространения или использования вопреки закону.
- Несанкционированный доступ к базам данных, содержащим паспортные данные, адреса, истории болезни и другую информацию. Этот доступ используется не только для копирования или незаконного распространения данных, но и для изменения, уничтожения или искажения важных параметров. Нарушители используют специальные программы и технические средства для осуществления деструктивных действий, часто у операторов нет готовых решений для решения задач, созданных с использованием современных технологий. (Меликов, 2015)

ФСТЭК разработала собственную модель угроз с уверенностью в том, что каждый оператор сможет разработать свои собственные методы защиты персональных данных при их обработке в информационных системах персональных данных. Для этого необходимо эффективно использовать различные материальные средства хранения и передачи, в том числе:

- Компьютеры;
- Информационные комплексы;
- Сети;

- Системы и устройства для передачи, приема и обработки информации, такие как аудио- и видеотехника, а также телевизионные устройства;
- Средства копирования и дублирования;
- Программное обеспечение, включая операционные системы и программы для управления базами данных и информационными массивами;
- Программное обеспечение, обеспечивающее безопасность информационных систем персональных данных.

Владельцы оборудования и сетей несут ответственность за работоспособность и безопасность своих систем.

ФСТЭК, разрабатывая свою модель угроз, была уверена, что каждый оператор сможет разработать свои собственные методы защиты персональных данных при их обработке в информационных системах персональных данных. Для этого необходимо грамотно использовать различные материальные средства хранения и передачи, к которым относятся:

- Компьютеры
- Информационные системы
- Сети
- Системы и средства передачи, приема и обработки информации, такие как устройства передачи звука, усиления звука и средства создания телевизионного изображения
- Средства тиражирования и копирования
- Программное обеспечение, включая операционные системы и программы для управления базами данных и массивами информации
- Программы, обеспечивающие безопасность информационных систем персональных данных

Владельцы оборудования и сетей несут ответственность за работоспособность и безопасность этих систем. Каждый субъект рынка, включенный в реестр, должен быть не только готов в любой момент пройти проверку Роскомнадзора, но и решать задачи, которые не предусмотрены

действующей нормативной документацией и представляют новые вызовы. (Меликов, 2015) Некоторые из этих задач включают:

- Разработка собственных моделей угроз, учитывающих конкретные потребности каждого оператора, обрабатывающего персональные данные. Разные лица могут преследовать разные цели при нарушении информации, относящейся, например, к государственным служащим и тем, кто интересуется медицинскими картами пенсионеров.
- Анализ и мониторинг текущей ситуации в области защиты баз персональных данных от внешнего вторжения.
- Разработка собственной системы защиты баз данных и нейтрализации потенциальных угроз на основе методов и рекомендаций, применимых к каждой отдельной системе.
- Систематическое осуществление мер, направленных на предотвращение несанкционированного доступа третьих лиц к базам данных, для которых не было предоставлено разрешение на доступ к этой информации и ее обработку.
- Организация технической системы защиты средств обработки данных с целью исключения любого воздействия на них, которое может привести к их повреждению или уничтожению.
- Постоянный контроль качества защиты.

Модель предлагает изучить основные уязвимости систем безопасности, текущие типы угроз и доступные способы обеспечения информационной безопасности. Федеральная служба постоянно отслеживает новые виды угроз и вносит изменения в свои рекомендации.

Чтобы эффективно бороться с угрозами, необходимо полностью понимать их происхождение, серьезность и другие связанные с ними параметры. ФСТЭК предлагает классификацию угроз, которая поможет в решении этой проблемы. В рамках своей модели агентство определяет угрозу как сочетание внешних и внутренних факторов или условий, которые позволяют злоумышленникам сознательно или бессознательно получить доступ

к защищаемой информации, что может привести к ее несанкционированному использованию. Эти действия могут включать:

- Уничтожение (стирание из памяти компьютера)
- Блокирование доступа к информации;
- Распространение среди ограниченного или широкого круга лиц;
- Изменение информации;
- Копирование информации
- Любые иные действия, не предусмотренные установленными правилами обработки информации в системах персональных данных.

Риски могут быть связаны как с личностью, произвольными действиями третьих лиц, так и с несанкционированными техническими сбоями, связанными с ошибками или невнимательностью персонала. Сочетание факторов и условий будет иметь индивидуальный характер для каждой отдельной системы и будет зависеть от характеристик конкретной информационной системы персональных данных, окружающей среды и методов распространения информационных сигналов, а также технических и других возможностей, доступных потенциальным источникам угроз. (Салихов, 2021)

Существует несколько характеристик информационных систем персональных данных (интернет-провайдеров), которые влияют на появление новых угроз и рисков:

- Объем и содержание информации, содержащейся в базе данных.
- Структура и конфигурация системы.
- Подключение системы к сетям передачи информации общего пользования или сетям для трансграничного обмена данными.
- Доступность и качество систем защиты.
- Режим обработки персональных данных.
- Многоуровневая система доступа, которая предоставляет различные уровни полномочий и задач для доступа к данным.
- Физическое местоположение технических устройств и режим их защиты от незаконного вмешательства.

При этом особое внимание уделяется свойствам среды передачи сигнала. Часто доступ к защищенной информации можно получить, используя линии подключения к электрическим сетям или собирая информацию об изменениях электромагнитного излучения.

По-прежнему существует возможность использования аудиоустройств для подслушивания и записи аудиоинформации.

При анализе источников угроз необходимо изучать различные типы угроз, такие как угрозы, связанные со злоупотреблением служебным положением, технические, программные и физические угрозы. Реализация каждой угрозы происходит на практике, когда существует канал доступа между субъектом, намеревающимся совершить противоправное деяние, и охраняемым объектом, который открывает возможность для несанкционированного, сознательного или случайного доступа к объекту..

При анализе угроз, связанных с обработкой персональных данных и исходя из разнообразия возможностей доступа к информации, модель выделяет следующие классы угроз (таблица 1)

Таблица 1

Таблица 1 – Анализ угроз (Шумекева, 2018)

Угрозы	**Анализ**
Внутренние угрозы (инсайдерские)	Эти риски возникают, когда внутренний пользователь, имеющий доступ к информационным системам в рамках своего служебного положения, работы в компании или государственной структуре, может похитить или изменить данные.
Внешние	В этом случае субъект угрозы получает несанкционированный доступ к защищаемому объекту, используя возможности общедоступных сетей.
Технические	Эти угрозы возникают при использовании аппаратных закладок и программ, разработанных для кражи электронной информации

Таким образом, модель идентифицирует указанные классы угроз, связанных с обработкой персональных данных, и основана на различных методах получения доступа к информации

Необходимо тщательно проанализировать все виды угроз, связанных с обработкой персональных данных. Это требует изучения личностей сотрудников, имеющих доступ к базам данных, а также уделение внимания технической безопасности средств хранения и обработки данных с использованием специализированного программного обеспечения, DLP-систем и SIEM-систем.

Модель также предлагает классификацию угроз, основанную на различных типах используемого оборудования.:

1. Угрозы безопасности персональных данных, обрабатываемых на рабочих местах, которые не подключены к Интернету.
2. Угрозы данным, обрабатываемым на рабочих местах, подключенных к Интернету.
3. Угрозы информационным массивам, обрабатываемым в локальных сетях, не подключенных к Интернету.
4. Угрозы массивам данных, которые обрабатываются в локальных сетях предприятий и организаций, имеющих доступ в Интернет.
5. Угрозы безопасности персональных данных, обрабатываемых в распределенных сетях операторов, включая международные сети обмена информацией (Яковец, 2014).

Кроме того, модель угроз безопасности предлагает классификацию, относящуюся к различным типам технических средств, которые используются для доступа к защищенным информационным массивам.:

1. Использование вредоносных программ, вирусов, червей и аналогичных инструментов, созданных в незаконных целях.
2. Утечка данных по техническим и физическим каналам.
3. Другие специальные методы воздействия.

Модель угроз также выявляет уязвимости систем безопасности и технических средств, используемых конкретным оператором:

1. Уязвимости системного программного обеспечения.
2. Уязвимости прикладного программного обеспечения.
3. Уязвимости, связанные с возможностью использования аппаратных закладок.
4. Уязвимости, связанные с использованием средств связи и протоколов передачи информации.
5. Уязвимости, связанные с техническими каналами передачи данных (например, телефонными сетями, сетями электроснабжения). (Терещенко, 2018)

Чтобы выявить эти уязвимости, необходимо регулярно проводить аудиты безопасности и систем защиты информации. Помимо анализа возможностей доступа нарушителей к компьютерным средствам обработки информации, следует также иметь в виду, что потенциальную угрозу может представлять практически любое офисное техническое устройство. Модель безопасности классифицирует такие устройства следующим образом:

1. Рабочие станции.
2. Отдельные устройства обработки информации (принтеры, копировальные аппараты, звукозаписывающая аппаратура, оборудование видеонаблюдения).
3. Коммуникационные сети.

Опыт показывает, что большая часть конфиденциальной информации утекает по техническим каналам передачи данных. Сигналы передаются через определенные физические носители, могут быть акустическими или электромагнитными и могут быть перехвачены с помощью встроенных устройств и других методов. Эти устройства могут перехватывать данные, передаваемые посредством электромагнитного излучения, а также акустическую и визуальную информацию. Защита от этого метода перехвата осуществляется путем ограничения доступа к охраняемому объекту.

Для организации практически невозможно полностью защитить персональные данные от своих собственных сотрудников. Существует несколько способов, которыми данные могут быть повреждены:

- Стандартное программное обеспечение, которое может предоставить доступ к операционной среде.
- Создание нестандартных условий работы, позволяющих искажать данные и изменять их.
- Вредоносное ПО.
- Угрозы, связанные с удаленным доступом.
- Комбинированные угрозы.

Для борьбы с этими угрозами необходимо установить программное обеспечение безопасности и регулярно контролировать рабочие станции. Роскомнадзор также проводит проверки системных операторов на предмет соблюдения требований и выдает предписания по повышению уровня безопасности. В большинстве случаев это не требует значительных финансовых вложений. Стандартные меры безопасности и соблюдение инструкций позволяют сохранить до 90% данных. Каждая из перечисленных угроз может иметь различные последствия, начиная от незначительных и заканчивая катастрофическими. Операторы персональных данных обязаны обеспечивать условия обработки данных, которые предотвращают нанесение ущерба интересам отдельных лиц или общества в целом. (Салихов, 2021)

В итоге стоит отметить, что существует ряд методов и подходов к защите персональных данных, которые играют важную роль в обеспечении их конфиденциальности и безопасности.

Шифрование является одним из основных методов защиты персональных данных. Он позволяет преобразовать данные в непонятный для посторонних вид, требующий специального ключа для расшифровки. Это помогает предотвратить несанкционированный доступ к данным, даже если они попадут в чужие руки.

Применение сильной аутентификации, такой как пароли, биометрические данные или двухфакторная аутентификация, позволяет контролировать доступ к персональным данным. Управление доступом позволяет определить, какие пользователи или группы пользователей имеют право просматривать, изменять или удалять определенные данные.

Физическая безопасность играет важную роль в защите персональных данных. Это включает ограничение доступа к серверным помещениям, использование видеонаблюдения, систем контроля доступа и других физических мер для предотвращения несанкционированного доступа к хранилищам данных.

Сотрудники, работающие с персональными данными, должны быть обучены и осведомлены о правилах и процедурах защиты данных. Это включает соблюдение политик безопасности, понимание рисков и угроз, а также знание процедур реагирования на инциденты безопасности.

Проведение регулярных аудитов и мониторинга системы позволяет обнаруживать потенциальные уязвимости и аномалии в обработке персональных данных. Это помогает реагировать на возможные инциденты безопасности и принимать соответствующие меры по устранению уязвимостей.

Соблюдение законодательства и нормативных требований в области защиты персональных данных является неотъемлемой частью методов защиты. Это включает соблюдение требований по хранению, передаче и обработке данных, а также информирование субъектов данных о целях и условиях обработки их персональных данных.

Все эти методы взаимодействуют и комплексно обеспечивают защиту персональных данных от угроз и несанкционированного доступа. Эффективная защита данных требует постоянного мониторинга, обновления и совершенствования методов, учета новых угроз и использования передовых технологий в области информационной безопасности.

ГЛАВА 3 СОЗДАНИЕ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Одним из обязательств компании в соответствии со статьей 18.1 Закона о персональных данных № 152 является своевременная подготовка документов о персональных данных (локальных актов), а также проведение систематического внутреннего аудита защиты персональных данных. С другой стороны, не менее важно принять меры по подготовке документов и грамотно организовать учет и хранение персональных данных.

Вот перечень документов, которые необходимо подготовить (Лебедев, 2018):

1. Приказ о назначении ответственного за безопасность персональных данных. Назначение ответственного за обеспечение безопасности персональных данных осуществляется по указанию руководителя в соответствии с пунктом 14 "Требований к защите персональных данных при их обработке в информационных системах персональных данных", утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.Ответственный за обеспечение безопасности персональных данных выполняет функции администратора безопасности при обработке персональных данных оператором. Он руководствуется утвержденной инструкцией в своей деятельности.

2. Согласие на обработку персональных данных, разрешенных субъектом для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор должен выдать согласие на распространение персональных данных отдельно от других согласий на обработку этих данных, предоставленных субъектом. До получения такого согласия оператор обязан предоставить субъекту возможность определить, какие персональные данные из списка категорий, указанных в согласии, будут обрабатываться. То есть оператор предоставляет субъекту список, содержащий конкретные персональные

данные, подлежащие обработке (например, при приеме на работу - паспортные данные, полное имя, адрес и т.д.). Из этого списка субъект должен выбрать данные, которые могут быть распространены. Если согласие на обработку данных не предусматривает разрешения на их распространение, оператор обрабатывает данные без права их распространения. Молчание или бездействие лица не считается согласием на обработку указанных данных. Требования к содержанию такого согласия устанавливаются Роскомнадзором (пункт 9 статьи 9, статья 23 Федерального закона № 152).

3. Приказ об утверждении перечня персональных данных. Утверждается список персональных данных, которые обрабатываются в информационных системах персональных данных оператора. В приказе приводится перечень конкретных персональных данных, которые хранятся и обрабатываются оператором, а также устанавливается срок, по истечении которого определенные данные из этого списка должны быть удалены.

4. Последствия отказа предоставить персональные данные. Целью настоящего документа является информирование субъекта персональных данных о правовых последствиях, которые могут возникнуть в случае отказа от предоставления персональных данных. Особое внимание уделяется разъяснению того, что обработка персональных данных необходима работодателю при заключении трудового договора.

5. Приказ о допуске к обработке персональных данных. Этим приказом утверждается перечень должностей сотрудников, которым необходим доступ к персональным данным для выполнения их официальных обязанностей. Ответственный за организацию обработки персональных данных проводит обучение сотрудников, назначенных в соответствии с данным приказом.

6. Политика конфиденциальности. Каждый оператор, который собирает персональные данные пользователей через свой веб-сайт, должен разместить на нем Политику конфиденциальности. Этот документ разработан для обеспечения прозрачности процессов обработки персональных данных и

обычно состоит из следующих разделов: общие положения, основания и условия обработки персональных данных, права пользователей при обработке их персональных данных, цели обработки персональных данных, виды обрабатываемых данных, информация о передаче персональных данных третьим лицам сторонам, информация о безопасности персональных данных, а также информация об операторе и возможности связаться с ним.

7. Соглашение о неразглашении информации, содержащей персональные данные. В этом документе определены определенные обязанности работника оператора, который имеет доступ к персональным данным. Одна из таких обязанностей состоит в соблюдении режима конфиденциальности персональных данных.

8. Правила осуществления внутреннего контроля.

9. Положение об обработке и защите персональных данных является одним из основных внутренних документов оператора. В нем определяется содержание обрабатываемых персональных данных, категории субъектов, чьи персональные данные обрабатываются, сроки их обработки и хранения, а также процедура уничтожения таких данных после достижения целей обработки или по другим законным причинам.

10. Информированное согласие пользователя сайта

11. Перечень форм, содержащих персональные данные. В этом документе указаны образцы типовых форм, которые оператор использует для содержания персональных данных.

12. Правила рассмотрения запросов субъектов персональных данных содержит порядок учета (регистрации) и рассмотрения запросов от субъектов персональных данных или их уполномоченных представителей определяется правилами обработки таких запросов.

13. В соответствии с правилами внутреннего контроля устанавливается процедура проверки соблюдения требований законодательства о персональных данных и локальных актов, принятых оператором, касающихся защиты персональных данных при обработке таких данных.

14. Договор поручения на обработку персональных данных обработчика персональных. Обработчиком обычно является организация, которая обрабатывает данные от имени оператора, например, поставщик облачных услуг или компания по аутсорсингу бухгалтерского учета. Необходимо заключить соглашение об уступке с обработчиком. В этом договоре должен быть указан перечень операций, которые обработчик будет выполнять с персональными данными, цели обработки и обязательство соблюдать конфиденциальность персональных данных.

15. Приказ об утверждении перечня информационных систем персональных данных (ИСПДн) определяет назначение основной системы обработки персональных данных. Например, это может быть автоматизация кадрового учета или процессов расчета заработной платы. В документе также указаны категории и объем персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

16. Порядок хранения бумажных носителей персональных данных устанавливает места хранения документов, бланков и других материальных носителей, содержащих персональные данные. Лицо, ответственное за организацию обработки персональных данных, проверяет сохранность материальных носителей и обеспечивает соответствие утвержденных мест хранения.

17. Приказ об определении контролируемой территории определяет границы контролируемой зоны информационных систем персональных данных. В пределах установленных границ ответственные лица, отвечающие за организацию обработки и безопасность персональных данных, осуществляют контроль за обработкой этих данных и обеспечивают их безопасность.

18. Инструкции лица, ответственного за организацию обработки персональных данных регламентирует работу лица, ответственного за организацию обработки персональных данных, устанавливает зону ответственности, права и обязанности этого лица. Он осуществляет внутренний контроль за соблюдением оператором законодательства о персональных

данных. Назначение лица, ответственного за организацию обработки персональных данных, производится путем издания приказа руководителем.

19. Инструкция по учету персонала, имеющего доступ к персональным данным в информационных системах персональных данных (ИСПДн), устанавливает порядок учета таких лиц, правила их допуска к работе с персональными данными, а также порядок прекращения такого доступа.

20. Инструкция по проведению инструктажа лиц, допущенных к работе в ИСПДн. Целью её является обеспечение безопасности персональных данных. Настоящая инструкция определяет порядок инструктажа сотрудников, ответственных за организацию обработки персональных данных, с целью обеспечения безопасности персональных данных.

21. Инструкции лица, ответственного за обеспечение безопасности персональных данных определяет основные функции, обязанности, права и ответственность лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных. Назначение лица, ответственного за обеспечение безопасности персональных данных, осуществляется путем издания соответствующего приказа руководителем.

22. Инструкции по резервному копированию и восстановлению определяют действия, связанные с функционированием технических и программных средств автоматизированной информационной системы (АИС) и системы защиты персональных данных.

23. Инструкции по учету и хранению съемных носителей определяют порядок работы с такими носителями. Данная инструкция является обязательной для всех лиц, которым разрешен доступ к обработке персональных данных в соответствии с приказом о допуске к обработке персональных данных. Лица, допущенные к обработке персональных данных, должны ознакомиться с инструкциями, подтвердив свое согласие подписью.

24. Инструкция пользователя информационной системы персональных данных (ИСПДн) на случай возникновения нештатных ситуаций необходима

для определения возможных нештатных ситуаций, связанных с функционированием информационных систем персональных данных, а также мер и средств для поддержания непрерывности работы и восстановления работоспособности ИСПДн после нештатных ситуаций. Целью данного документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.

25. Инструкции по организации антивирусной защиты в информационных системах персональных данных (ИСПДн) разработаны в целях защиты персональных данных в информационных системах персональных данных от несанкционированного копирования, модификации и уничтожения под воздействием вирусов и другого вредоносного программного обеспечения.

26. Журнал регистрации запросов субъектов персональных данных ведется оператором в качестве меры, направленной на обеспечение выполнения оператором обязанности по уточнению, блокированию, уничтожению персональных данных при обращении к нему субъекта персональных данных. Документ разработан в соответствии с правилами рассмотрения запросов от субъектов персональных данных.

27. Журнал прохождения первичного инструктажа сотрудниками ведется оператором в качестве меры, направленной на фиксацию прохождения первичного инструктажа сотрудниками, допущенными к обработке персональных данных на основании приказа о допуске к обработке персональных данных.

28. Журнал учета съемных носителей, содержащих персональные данные ведется оператором в качестве меры, направленной на обеспечение сохранности съемных носителей персональных данных. Съемные носители с личными данными (флэш-карты, внешние жесткие диски, мобильные устройства и т.д.) необходимо хранить в сейфах, если личные данные на самом носителе не зашифрованы.Документ предназначен, например, для учета таких

носителей и разработан в соответствии с инструкциями по учету и хранению съемных носителей.

29. Журнал прав доступа к ИСПДн ведется оператором в качестве меры, направленной на учет лиц, допущенных к работе с персональными данными, их должности, объема прав и времени доступа. Он создается и поддерживается в актуальном состоянии оператором на основании приказа о допуске к обработке персональных данных, а также инструкций по регистрации лиц, допущенных к работе с персональными данными в информационных системах персональных данных (ИСПДн).

30. Журнал регистрации нарушений и восстановления работоспособности ведется оператором в качестве меры, направленной на фиксацию событий сбоя оборудования или ИСПДн, даты и времени обнаружения события, причин нарушения, информации о мерах, принятых для восстановления работоспособности оборудования или ИСПДн.

31. Журнал учета проверок контролирующими органами ведется оператором в качестве меры, направленной на обеспечение исполнения оператором обязанности по предоставлению информации по запросу уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзора) и других органов.

32. Реестр средств защиты информации ведется оператором в качестве меры, направленной на учет средств защиты информации, эксплуатационной и технической документации к ним, а также лиц, устанавливающих средства защиты информации.

33. Форма запроса на уточнение персональных данных была разработана на основании статьи 14 Закона "О персональных данных" № 152-ФЗ, согласно которой субъект персональных данных имеет право, а оператор обязан уточнить обрабатываемые персональные данные такого субъекта, то есть внести определенные коррективы к ним по запросу субъекта персональных данных

34. Форма запроса на наличие и ознакомление с персональными данными была разработана на основании статьи 14 Закона "О персональных данных" № 152-ФЗ, согласно которой субъект персональных данных имеет право, а оператор обязан предоставлять информацию, касающуюся обработки персональных данных такого субъекта, в частности, такую, как факт обработки, основания и цели обработки, методы обработки, срок хранения персональных данных.

35. Форма запроса на блокирование персональных данных была разработана на основании статьи 14 Закона "О персональных данных" № 152-ФЗ, согласно которой субъект персональных данных имеет право, а оператор обязан заблокировать персональные данные такого субъекта по его требованию, за исключением случаев, предусмотренных законом. Под блокировкой понимается преднамеренное создание невозможности доступа и использования персональных данных.

36. Форма запроса на уничтожение персональных данных была разработана на основании статьи 14 Закона "О персональных данных" № 152-ФЗ, согласно которой субъект персональных данных имеет право, а оператор обязан уничтожить персональные данные такого субъекта, за исключением случаев, предусмотренных законом.

37. Форма запроса с отзывом согласия на обработку персональных данных была разработана на основании статей 5 и 21 Закона "О персональных данных" № 152-ФЗ, согласно которым субъект персональных данных имеет право, а оператор обязан прекратить обработку персональных данных такого субъекта по его требованию.

38. Форма уведомления об отказе во внесении изменений в персональные данные субъекта предназначена для информирования субъекта персональных данных в случае непредоставления им необходимых документов, подтверждающих запрашиваемые изменения, о невозможности внесения изменений в его персональные данные в форме уведомления об устранении неправомерных действий с персональными данными. Кроме того, данная форма

предназначена для информирования субъекта персональных данных в случае нарушения обработки его персональных данных о том, что нарушения были устранены оператором.

39. Форма уведомления органа по защите прав субъектов персональных данных предназначена для информирования государственного органа по защите прав субъектов персональных данных о существенных условиях обработки персональных данных, осуществляемой оператором, таких как цели обработки, основания для обработки, виды персональных данных.

40. Акт оценки потенциального вреда субъектам персональных данных предназначен для формализации результатов оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований законодательства о персональных данных.В документе для каждой категории субъектов персональных данных (сотрудники, клиенты, заявители и т.д.) и для каждого способа обработки персональных данных указана присвоенная степень вреда (низкая, умеренная, средне-значимая, высокая, чрезвычайно высокая). Серьезность ущерба обычно зависит от возможности идентификации, объема персональных данных и количества субъектов персональных данных.

41. Акт определения уровня защиты персональных данных является одним из документов, содержащих информацию о внедренных требованиях к защите персональных данных. Акт определения уровня защиты персональных данных составляется для каждой информационной системы персональных данных (ИСПДн).Структура этого документа включает в себя: персональные данные, обрабатываемые в ИСПДн, объем обрабатываемых персональных данных, тип текущих угроз для ИСПДн, уровень безопасности персональных данных.

42. Акт уничтожения персональных данных фиксирует процедуру уничтожения персональных данных и должен соответствовать правилам, установленным законом: после процесса уничтожения информация не должна подлежать восстановлению. В то же время сам процесс должен осуществляться

специальной комиссией, созданной именно для таких случаев. После завершения процедуры составляется акт, подписываемый членами комиссии и руководителем.

43. Модель угроз безопасности. Настоящий документ был создан с целью выполнения обязательства, предусмотренного пунктом 1 части 2 статьи 19 Закона № 152-ФЗ "О персональных данных", по выявлению угроз безопасности персональных данных.

При подготовке этого документа рекомендуется использовать следующие документы в качестве руководства:

- Постановление Правительства Российской Федерации от 01.10.2012 № 1119;
- Методика определения фактических угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Федеральной службой по техническому и экспортному контролю 14.02.2008);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Федеральной службой по техническому и экспортному контролю 15.02.2008).

В итоге, отметим, что создание документации по защите персональных данных является неотъемлемой частью эффективной системы управления информационной безопасностью. Она позволяет организациям и операторам данных установить политику и процедуры, обеспечивающие конфиденциальность, целостность и доступность персональных данных. Документация по защите персональных данных является основой для проведения аудитов, мониторинга и анализа системы защиты данных. Она облегчает процесс проверки соответствия системы безопасности требованиям и выявления потенциальных уязвимостей или нарушений. Создание документации по защите персональных данных является важным шагом в обеспечении безопасности и конфиденциальности персональных данных, а

также демонстрирует готовность и стремление организации к соблюдению законодательных и этических норм, касающихся защиты персональных данных.

ГЛАВА 4 РЕАЛИЗАЦИЯ БАЗЫ ДАННЫХ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Внедрение базы данных для защиты персональных данных в информационных системах включает в себя несколько важных аспектов. Вот несколько рекомендаций и методов, которые можно использовать при создании такой базы данных:

1. Определение структуры данных.

2. Идентификация персональных данных. База данных должна содержать следующие типы персональных данных: имя, адрес, номер телефона, адрес электронной почты и дату рождения пользователей.

Пример структуры таблицы "Пользователи":

- Идентификатор пользователя (уникальный идентификатор)
- Имя пользователя (строка)
- Адрес (строка)
- Номер телефона (линия)
- Адрес электронной почты (строка)
- Дата рождения (date)

3. Классификация данных. В соответствии с требованиями законодательства, возможно классифицировать данные на основе их конфиденциальности и деликатности.

Пример классификации данных:

- Общедоступные данные: Имя пользователя
- Конфиденциальные данные: адрес, номер телефона, адрес электронной почты
- Строго конфиденциальные данные: Дата рождения

Классификация данных помогает установить соответствующие меры безопасности и права доступа.

4. Определение взаимосвязей между данными.Здесь надо установить взаимосвязь между таблицей "Пользователи" и другими таблицами,

содержащими связанные данные. Например, таблица "Заказы", которая содержит информацию о заказах пользователей.

Пример взаимосвязи между таблицами:

- Таблица "Пользователи" связана с таблицей "Заказы" с помощью общего идентификатора пользователя.
- Это позволяет связывать данные, обеспечивая целостность и удобный доступ к связанным информационным блокам.

1. Аутентификация и авторизация

- **Рекомендация**. Внедрите систему аутентификации, которая требует от пользователей предоставления уникальных учетных данных, таких как логин и пароль, для получения доступа к базе данных. Используйте хэширование паролей для обеспечения безопасности хранения паролей.
- **Пример реализации.** Создайте таблицу "Пользователи" с полями, включающими хэш логина и пароля. При попытке входа в систему пользователь будет проверен на соответствие хэшу логина и пароля перед доступом к базе данных.

2. Шифрование данных:

- **Рекомендация.** Используйте механизмы шифрования для защиты конфиденциальности персональных данных во время их хранения и передачи. Используйте надежные алгоритмы шифрования, такие как AES (AdvancedEncryptionStandard) или RSA (Rivest-Shamir-Adleman).
- **Пример реализации.** При хранении персональных данных в базе данных используйте шифрование для защиты конфиденциальности. Например, вы можете зашифровать поле с номером телефона пользователя перед сохранением его в базе данных и расшифровать его для использования при получении данных.

3. Ведение журнала и мониторинг

- **Рекомендация.** Включите механизмы регистрации событий и мониторинга для обнаружения несанкционированного доступа или ненормальной активности в базе данных. Регулярно проверяйте журналы

событий и анализируйте их, чтобы выявить потенциальные угрозы или нарушения безопасности.

- **Пример реализации.** Разработайте систему, которая записывает все важные события, связанные с доступом к базе данных, изменениями данных или попытками несанкционированного доступа. При возникновении подозрительных событий отправляйте уведомления администраторам или службам безопасности.

Кроме того, следует учитывать дополнительные рекомендации по безопасности, такие как регулярные обновления системы, использование исправлений безопасности, ограничение физического доступа к серверам баз данных и обеспечение резервного копирования данных для восстановления

4. Политика безопасности:

- **Рекомендация**. Разработать документ "Политика безопасности", определяющий общие принципы и требования к защите персональных данных в базе данных. Укажите меры, которые следует принять для обеспечения конфиденциальности, целостности и доступности данных.

- **Пример реализации.** В политике безопасности укажите, что доступ к базе данных должен быть ограничен только авторизованными сотрудниками, аутентификация должна осуществляться с использованием уникальных учетных записей и паролей. Также укажите, что резервное копирование данных должно осуществляться регулярно, а доступ к резервным копиям должен быть ограничен. Определите процедуры устранения нарушений безопасности, включая обязательное уведомление о нарушениях и расследование инцидентов.

5. Процедуры контроля доступа

- **Рекомендация**: Разработайте процедуры управления доступом к базе данных, описывающие процессы создания и удаления учетных записей пользователей, управления правами доступа и аудита доступа.

- **Пример реализации**: Разработайте процедуру создания новых учетных записей пользователей, которая будет включать в себя процесс

проверки идентификации и присвоения соответствующих прав доступа. Также разработайте процедуру удаления учетных записей при прекращении или истечении срока действия доступа. Определите процесс управления правами доступа, включая процедуру запроса изменений прав и процедуру пересмотра прав доступа с определенной периодичностью.

6. План реагирования на инциденты:

- **Рекомендация.** Разработайте план реагирования на инциденты, который определяет процедуры и обязанности по устранению нарушений безопасности и инцидентов, связанных с персональными данными.
- **Пример реализации**: В плане реагирования на инциденты укажите, какие действия следует предпринять при обнаружении нарушений безопасности или утечек персональных данных. Определите команду ответственных лиц, которые будут расследовать инциденты и реагировать на них.

Реализация этих мер будет зависеть от конкретных требований организации и используемых инструментов. Важно обратиться к современным методам и инструментам обеспечения безопасности баз данных, таким как шифрование данных, системы контроля доступа и мониторинга, а также регулярное обновление политик и процедур в соответствии с меняющимися угрозами и законодательством в области защиты персональных данных.

Выбор базы данных для хранения и защиты персональных данных зависит от различных факторов, включая требования к безопасности, масштабируемость, производительность, доступность и бюджет организации. Вот несколько популярных типов баз данных, которые обычно используются для хранения персональных данных:

1. Реляционные базы данных (RDBMS) широко используются и имеют хорошую поддержку безопасности данных. Они обеспечивают механизмы шифрования, контроля доступа и аудита, а также предоставляют возможности для разработки политик безопасности и управления правами доступа.

2. Базы данных NoSQL обеспечивают гибкость и масштабируемость при хранении и обработке больших объемов данных. Они также могут предоставлять средства безопасности, включая шифрование и контроль доступа, но функциональность может варьироваться в зависимости от конкретной реализации.

3. Облачные платформы предлагают различные базы данных с функциональностью защиты персональных данных. Однако следует понимать, что оператор несет ответственность за данные, а представители облака - нет.

4. Гибридные решения. Иногда, в целях обеспечения безопасности и соблюдения требований законодательства о защите персональных данных, может возникнуть необходимость в объединении различных баз данных. Например, вы можете использовать реляционную базу данных для хранения конфиденциальных персональных данных и базу данных NoSQL для обработки и хранения более общей информации.

При выборе базы данных для хранения и защиты персональных данных рекомендуется провести тщательный анализ требований организации, обратиться к руководящим документам и рекомендациям, касающимся безопасности данных, а также учитывать ограничения и возможности каждого конкретного решения. Также важно следовать современным стандартам и передовой практике защиты персональных данных.

В заключение, реализация базы данных для защиты персональных данных играет решающую роль в обеспечении конфиденциальности, целостности и доступности информации о пользователях.

База данных предоставляет структурированное и централизованное хранилище для персональных данных, где информация может быть управляема и контролируема. Это позволяет упорядочить данные и обеспечить единый и точный источник информации о пользователях.

Реализация базы данных для защиты персональных данных является необходимым шагом для обеспечения безопасности и конфиденциальности информации о пользователях. Это помогает предотвратить утечку данных,

минимизировать риски нарушений безопасности и обеспечить соблюдение законодательных требований, связанных с персональными данными.

ЗАКЛЮЧЕНИЕ

В заключение, стоит отметить, что понятие персональных данных и системы защиты информации играют важную роль в современном информационном обществе. Персональные данные представляют собой информацию, относящуюся к конкретному лицу, которая может быть использована для его идентификации. Защита персональных данных имеет особое значение, поскольку неправомерное их использование может привести к нарушению приватности и угрозам для личной жизни.

Правовое регулирование защиты персональных данных осуществляется на государственном уровне и направлено на обеспечение конфиденциальности и безопасности таких данных. Многие страны принимают законодательные акты, которые определяют права и обязанности операторов и субъектов персональных данных, а также устанавливают меры и процедуры для обеспечения их защиты.

В современных условиях, с увеличением объема и сложности обработки персональных данных, становится все более важным обеспечение надежной системы защиты информации. Это включает в себя применение технических и организационных мер, направленных на предотвращение несанкционированного доступа, утечки и повреждения персональных данных.

В целом, правовое регулирование защиты персональных данных и развитие систем защиты информации являются важными аспектами в современном информационном обществе. Это позволяет обеспечить конфиденциальность, приватность и безопасность персональных данных, способствуя доверию и эффективному функционированию цифровой экономики и общества.

Стоит отметить, что существует ряд методов и подходов к защите персональных данных, которые играют важную роль в обеспечении их конфиденциальности и безопасности.

Все методы взаимодействуют и комплексно обеспечивают защиту персональных данных от угроз и несанкционированного доступа. Эффективная защита данных требует постоянного мониторинга, обновления и совершенствования методов, учета новых угроз и использования передовых технологий в области информационной безопасности.

В итоге, отметим, что создание документации по защите персональных данных является неотъемлемой частью эффективной системы управления информационной безопасностью. Она позволяет организациям и операторам данных установить политику и процедуры, обеспечивающие конфиденциальность, целостность и доступность персональных данных. Документация по защите персональных данных является основой для проведения аудитов, мониторинга и анализа системы защиты данных. Она облегчает процесс проверки соответствия системы безопасности требованиям и выявления потенциальных уязвимостей или нарушений. Создание документации по защите персональных данных является важным шагом в обеспечении безопасности и конфиденциальности персональных данных, а также демонстрирует готовность и стремление организации к соблюдению законодательных и этических норм, касающихся защиты персональных данных.

Реализация базы данных для защиты персональных данных играет решающую роль в обеспечении конфиденциальности, целостности и доступности информации о пользователях.

База данных предоставляет структурированное и централизованное хранилище для персональных данных, где информация может быть управляема и контролируема. Это позволяет упорядочить данные и обеспечить единый и точный источник информации о пользователях.

Реализация базы данных для защиты персональных данных является необходимым шагом для обеспечения безопасности и конфиденциальности информации о пользователях. Это помогает предотвратить утечку данных, минимизировать риски нарушений безопасности и обеспечить соблюдение законодательных требований, связанных с персональными данными.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Законодательство РФ

1. Доктрина информационной безопасности Российской Федерации от 09.09.2000 № ПР-1895 // Российская газета. – 2000. – 28 сент. (Утратил силу.)
2. Доктрина информационной безопасности Российской Федерации утверждена Указом Президента РФ от 05.12.2016 г. № 646 // Российская газета. – 2016. – 6 дек.
3. Конституция (Основной закон) Российской Федерации от 12.12.1993 // Российская газета. – 1993. – 25 дек.
4. О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ // Российская газета. – 2006. – 29 июля.
5. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: федер. закон от 19.12.2005 № 160-ФЗ // СЗ РФ. – 2005. – № 52 (ч. 1). – Ст. 5573.
6. Об информации, информатизации и защите информации: федер. закон от 20.02. 1995 № 24-ФЗ // СЗ РФ. – 1995. – № 8. – Ст. 609.
7. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // СЗ РФ. – 2006. – № 31. – Ст. 3448.
8. Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014).

9. Об утверждении перечня сведений конфиденциального характера: указ Президента Российской Федерации от 06.03. 1997 № 188 // СЗ РФ. – 1997. – № 10. – Ст. 1127.

10. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203 // Российская газета. – 2017. – 10 мая.

11. Бачило, И.Л. Персональные данные в структуре информационных ресурсов. Основы правового регулирования /И.Л. Бачило, Л.А. Сергиенко, Б.А. Кристальный., А.Г. Арешев // Информационное право. - 2016. - № 3. - С. 50-55.

12. Бойкова О.Ф. Защита персональных данных: касается всех! Практическое пособие. Выпуск № 142 / Бойкова Ольга Феоктистовна. - М.: Либерея, 2018. - 950 с.

13. Болик, В.Н. О правомерности законодательных ограничений конституционного права на неприкосновенность частной жизни / В.Н. Болик., А.М. Туркиашвили А.М. // Законы России: опыт, анализ, практика. - 2015. - № 7. - С. 78 - 84.

14. Бондаренко, К.А. Взаимосвязь признаков индивидуального трудового договора и особенностей договорного регулирования трудовых отношений / К.А. Бондаренко // Трудовое право в России и за рубежом. 2015. — № 3. — С. 23 — 27.

15. Бондаренко, Э.Н. Конфиденциальная информация в трудовых отношениях. / Э.Н. Бондаренко, Иванов ДВ. - СПб.; Издательство «Юридический центр-Пресс». – 2014. - 213 с

16. Бурдов, С.Н. К вопросу о возможностях совершенствования нормативно правового режима конфиденциальной информации / С.Н. Бурдов // Государство и право. 2015. № 5. - С. 103-105.

17. Буркова А.Ю. Определение понятия "персональные данные" // Право и экономика. - 2015. - № 4. - С. 20 - 24

18. Буркова, А.Ю. Локализация баз данных на территории Российской Федерации: первые толкования // Законодательство и экономика. 2015.- № 9.- С. 59 - 64.

19. Власов Д.С. Защита персональных данных в автоматизированных системах обработки информации органов государственной власти // Успехи современной науки. 2016. Т. 8. - № 12. - С. 33-38.

20. Выговская, И.Г. Трудовое право России: учебник / И.Г. Выговская, С.В. Колобова, О.С. Королькова и др.; под общ. ред. М.В. Преснякова, С.Е. Чаннова. - Саратов: Поволжский институт управления им. П.Л. Столыпина, 2014.- 288 с.

21. Гадельшин А.А., Степанов М.М. COOKIE-ФАЙЛЫ как объект персональных данных и способ нарушения конфиденциальности персональных данных//Вопросы российской юстиции. 2021. - № 16. - С. 516-531.

22. Головина, С.Ю. Конституционные принципы и права в сфере труда и их конкретизация в трудовом законодательстве России // Российский юридический журнал. - 2015. - № 1. - С. 132 - 145.

23. Дроменко А.Ю. Информационные права граждан Российской Федерации и защита персональных данных в сети «Интернет» // ScienceTime. - 2016. - № 2 (26). - С. 203-206.

24. Дудко И.Г. Защита персональных данных кандидата в избирательном процессе // Проблемы права. - 2017. - № 5 (64). - С. 26-31.

25. Журавлев, М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. - 2017. - №4. - С. 35 - 38.

26. Загородников, С.Н. Чужие тайны и их защита: нормативно правовые аспекты / С.Н. Загородников, Максимов Д.А. // Российский следователь. - 2014. - № 3.- С. 40.

27. Иванов А.А. Хранение персональных данных за рубежом с точки зрения российского права // Закон. - 2015. - № 1. - С. 134 - 143.

28. Катунцева М.О. Конституционное право на информацию и проблема защиты персональных данных в социальных сетях // В книге: Конституционные права и свободы человека и гражданина в РФ: проблемы реализации и защиты Материалы межвузовского студенческого круглого стола.- 2016. - С. 31-37.

29. Козин И.С. Метод определения опасности угрозы персональным данным при их обработке в информационной системе. // Известия СПбГЭТУ «Лэти». – 2017. – №10. – С. 19-26.

30. Костомаров К.В., Качанова Е.А. Банк России в сфере защиты персональных данных клиентов коммерческих банков: экономический и юридический аспекты. Монография / Екатеринбург, 2015. - 321 с.

31. Кутенков Ю.И. Понятие персональных данных работника в российском трудовом праве // Азиатско-тихоокеанский регион: Экономика, политика, право. - 2015. - № 4 (37). - С. 116-133.

32. Лебедев, В.М. Трудовое право: Учебник / В.М. Лебедев, Д.В. Агашев, А.А. Белинин, А.В. Дворецкий; Под ред. В.М. Лебедева. - М.: Норма: НИЦ Инфра-М, 2018. - 464 с.

33. Меликов У.А. Гражданско-правовая защита персональных данных // Вестник УрФО. Безопасность в информационной сфере. – 2015. – № 4 (18). – С. 49-53.

34. Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. - 2012. - № 2 (4). - С. 4-9.

35. Павлова И.Ю.Соотношение правового регулирования банковской тайны и персональных данных гражданина в свете новелл законодательства о персональных данных //Государственная служба и кадры. - 2021. - № 3. - С. 43-47.

36. Салихов Д.Р. Пандемия и персональные данные: как распространение новой коронавирусной инфекции бросает новые вызовы

персональным данным //Конституционное и муниципальное право. - 2021. - № 3. - С. 46-50.

37. Соловьев В.В. Улучшение защищенности распределенной информационной системы персональных данных на основе технологии VPN и терминального доступа // Информационные технологии и проблемы математического моделирования сложных систем. – 2017. – №18. – С. 39-44.

38. Терещенко, Л.К. Правовой режим персональных данных и безопасность личности /Л. К. Терещенко //Закон. -2018.- №6.- С. 37 -43.

39. Трофимова, И.А. Обработка и хранение персональных данных/ И.А. Трофимова // Делопроизводство.- 2015. - № 3. - С. 107 - 110.

40. Шумекеева Г. Б. Защита персональных данных как одна из проблем современного мира / Право: современные тенденции : материалы VI Междунар. науч. конф. (г. Краснодар, октябрь 2018 г.). - Краснодар : Новация, 2018. - С. 47-49.

41. Яковец, Е.Н. Своеобразие состава защищаемой конфиденциальной информации / Е.Н. Якрвец // Право и кибербезопасность. - 2014. - № 2. - С. 51 - 58.

42. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). –

43. (https://rkn.gov.ru/). – Загл. с экрана.

44. Портал персональных данных уполномоченного органа по защите прав субъекта субъектов персональных данных – (http://pd.rkn.gov.ru/). – Загл. с экрана.

45. ФСТЭК России – Федеральная служба по техническому и экспортному контролю – (http://fstec.ru/). – Загл. с экрана.

46. EUR-Lex.europa.eu. – (http://eur-lex.europa.eu/). – Загл. с экрана.