МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Института права
(наименование института полностью)

Кафедра «Гражданское право и процесс»
(наименование)

40.03.01 Юриспруденция
(код и наименование направления подготовки, специальности)

Гражданско-правовой
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Гражданско-правовая защита персональных данных»

Студент Г.А. Федоров _____
(И.О. Фамилия) (личная подпись)

Руководитель канд. юрид. наук, Р.Ф. Вагапов
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

АННОТАЦИЯ

Актуальность темы работы обусловлена тем, что в настоящее время вопрос обработки персональных данных находится в секторе внимания специалистов по безопасности абсолютно любой организации. В свою очередь, любой гражданин вступает во взаимоотношения с различными физическими и юридическими лицами, в результате которых образуются массивы (базы данных) персональных данных. В то же время возникают трудности в применении действующих правовых норм, регулирующих данную сферу общественных отношений.

Цель работы - провести комплексный гражданско-правовой анализ защиты персональных данных.

Для этого определяются следующие задачи:

изучить понятие персональных данных в гражданском праве;

- исследовать законодательное регулирование защиты персональных данных;

- рассмотреть понятие защиты персональных данных;

- установить методы и способы защиты персональных данных в российском гражданском праве.

Объектом исследования являются правоотношения, складывающиеся в сфере гражданско-правовой защиты персональных данных.

Предметом исследования выступают нормы, закрепляющие принципы и условия сбора персональных данных, их гражданско-правовую защиту.

Методами исследования, используемыми при написании работы стали: диалектический, сравнительный, формально-юридический, логический, системный и др.

При написании работы были использованы: нормативные правовые акты, специальная литература, материалы юридической практики. Всего использовано 40 источников. Объем работы составил 42 страницы.

Оглавление

Введение

Развитие современного общества сопровождается использованием новых информационных и коммуникационных технологий, которые активно внедряются в государственное и муниципальное управление, во все сферы экономики и банковского дела, аграрный сектор, вопросы национальной безопасности государства и правопорядка.

Потребность в использовании новых информационно-коммуникационных технологий обусловлена тем, что их применение не только меняет сам способ управления общественными процессами, позволяя значительно повысить эффективность всех сфер деятельности, но и обеспечивает прозрачность осуществляемых процедур.

Стратегия развития информационного общества в России на 2017-2030 гг. направлена на обеспечение свободного доступа граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления к информации на всех этапах ее создания и распространения[40]. Данный документ определил не только пути безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение), но и направляет на то, что применение новых технологий должно соответствовать интересам общества.

В настоящее время вопрос обработки персональных данных находится в секторе внимания специалистов по безопасности абсолютно любой организации. Трудно найти организацию, которая не обрабатывала бы персональные данные своих сотрудников или контрагентов. В свою очередь, любой гражданин вступает во взаимоотношения с различными физическими и юридическими лицами, в результате которых образуются массивы (базы данных) персональных данных. В то же время у сотрудников служб информационной безопасности возникают трудности в применении

действующих правовых норм, регулирующих данную сферу общественных отношений.

Таким образом, при персональной обработке данных в любой информационной базе имеют значение нормативно-правовые акты, их применение и соблюдение. На момент написания выпускной квалификационной работы были внесены изменения, одно из главных нововведений затронуло Положение ФЗ №152-ФЗ, дополняя его требованием с 1 января 2021 года хранения персональных данных на серверах. При сборе, в том числе посредством информационно-телекоммуникационных систем, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнения (обновление, изменение) данных граждан РФ с использованием баз, находящихся на территории РФ.

Объектом исследования являются общественные отношения, складывающиеся в сфере гражданско-правовой защиты персональных данных.

Предметом исследования выступают нормы, закрепляющие понятие, принципы и условия сбора персональных данных, их гражданско-правовую защиту.

Цель работы - провести комплексный гражданско-правовой анализ защиты персональных данных.

Для этого определяются следующие задачи:

- изучить понятие персональных данных в гражданском праве;

- исследовать законодательное регулирование защиты персональных данных;

- рассмотреть понятие защиты персональных данных;

- установить методы и способы защиты персональных данных в российском гражданском праве.

Методами исследования, используемыми при написании работы стали: диалектический, сравнительный, формально-юридический, логический, системный и др.

Теоретическую базу исследования составили труды таких авторов как: Бучакова М.А., Ворожбит Д.В., Истратова А., Козин И.С., Коломыцев М.В., Меликов У.А., Минбалеев А.В., Носок С.А., Попова Ю.П., Солдатова В.И., Соловьев В.В., Талапина Э.В. и других.

Нормативная база исследования представлена Гражданским кодексом РФ и иными федеральными законами, а также подзаконными актами.

Также при написании работы использовались материалы судебной практики.

Структура работы представлена введением, двумя главами, подразделенными на четыре параграфа, заключением и списком используемых источников.

Глава 1 Теоретический анализ института персональных данных в российском гражданском праве

1.1 Определение понятия персональных данных в гражданском праве

Важной современной тенденцией развития информационного общества и цифровой экономики является возрастание интереса к персональным данным.

Значение персональных данных настолько велико, что включает в себя различную информацию, подпадающую под понятие «персональные данные». Содержание данной информации относится к основным сферам жизнедеятельности общества: образованию, медицине, строительству, финансам и пр.

В соответствии с ч. 1 ст. 23 и ч. 1 ст. 24 Конституции РФ каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Определение понятия персональных данных закрепляется в Федеральном законе №152-ФЗ «О персональных данных»[37]. Согласно ст. 3 указанного закона персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Для установления личности субъекта персональных данных Законом «О персональных данных» установлены минимальные требования к обработке биометрических персональных данных. Однако вопрос в части информирования об утечке таких данных носит открытый характер, а это представляет существенную угрозу безопасности граждан.

Исходя из сформулированного в законе определения можно сделать вывод, что персональные данные это любая информация, которая позволяет определить личность пользователя.

Персональные данные - это любая информация о физическом лице, в частности, фамилия, имя, отчество, место и дата рождения, место проживания и регистрации, социальное, имущественное и семейное положение, профессия, образование, доходы, совершение банковских операций по счету посредством мобильного приложения, биометрическая идентификация граждан в банковской сфере, приобретение товаров и услуг в сети Интернет, получение медицинских услуг с закреплением информации об этом в соответствующих информационных файлах, возможности по отслеживанию за передвижением граждан и многое другое – все это подпадает под категорию персональных данных. При этом пароли к аккаунтам не являются персональными данными, т.к. не сообщают ничего о человеке.

Однако понятие персональных данных не конкретизировано и может возникнуть затруднение с отнесением той или иной информации об индивиде к данным, относящимся к его персоне. Ряд ученых считают необходимым рассматривать такую информацию как нематериальное благо. При этом стремительно развивающиеся технологии ведут к расширению понятия «персональные данные» с включением в него новых элементов, позволяющих идентифицировать индивида по различным параметрам: биометрическим данным, доходам, наличию собственности, уплаты налогов, наличию сведений о фактах привлечения к юридической ответственности, реквизитов банковских карт и счетов, иных сведений частной жизни и т.д.

В гражданском законодательстве нашей страны персональные данные прямо не упоминаются. На данный момент и информация не упоминается в качестве объекта гражданских прав в ст. 128 ГК РФ. Так, к объектам гражданских прав относятся вещи (включая наличные деньги и

документарные ценные бумаги), иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага[10].

Некоторые юристы восприняли законодательное исключение информации из объектов гражданского оборота в 2008 году как подтверждение необоротоспособного характера. При этом обнаруживается некоторое противоречие со ст. 5 ФЗ «Об информации, информационных технологиях и о защите информации», согласно которой информация может быть объектом гражданских отношений. Предполагается, что информация может выступать объектом гражданского оборота в части, не противоречащей специальному режиму, установленному для отдельных видов информации.

Персональные данные это тоже своего рода информация. Тогда складывается двоякая ситуация, точнее, ситуация правовой неопределенности. Получается, персональные данные пользуются смешанным правовым режимом. «С одной стороны, они в некоторой степени материализуют конституционное право человека на неприкосновенность частной жизни, а с другой стороны, являются объектом гражданских прав».

Учитывая сказанное, на законодательном уровне и среди ученых ведутся дискуссии о необходимости реформирования гражданского законодательства, касающегося персональных данных. В рамках таких обсуждений одними из ведущих являются вопросы коммерциализации персональных данных и определения понятий больших данных и (или) больших пользовательских данных.

В пользу коммерциализации, т.е. внедрения персональных данных в гражданский оборот, чаще всего приводятся следующие аргументы:

– сложившаяся практика выйдет из «серой зоны», иными словами, будет легализована;

– устранятся мешающие для построения цифровой экономики барьеры;

– у физических лиц будет формироваться более ответственное отношение к распоряжению своими персональными данными.

Ряд ученых, ратующих за включение персональных данных в объекты гражданского оборота, пишут о том, что если обезличить персональные данные, то есть устранить наличие связи информации с конкретным лицом, то такие персональные данные могут становиться предметом коммерческого оборота или, другими словами, могут рассматриваться как товар. Согласно данной позиции, коммерциализация не является посягательством на неприкосновенность частной жизни личности.

Напротив, «коммерциализация открывает возможности развития новых форм экономики, новых рынков, новой сферы для технического развития и инноваций». Однако обезличенные персональные данные, с точки зрения российского законодательств, не могут считаться товаром.

Идея торговли персональными данными по сей день воспринимается противоречащей принципам этики и основам защиты прав человека. Против звучат аргументы о невозможности коммерциализации такого нематериального блага, как человеческое достоинство, рисках легитимации недобросовестных практик обработки данных и дискриминации отдельных лиц на основе полученных о них данных.

Мы полагаем, что информация как таковая, безусловно, является объектом гражданских прав. Но информация имеет большое количество ее разновидностей. Так, персональные данные – это информация, которая не может являться объектом гражданско-правовых сделок.

Новеллой закона является введение понятия «персональные данные, разрешенные субъектом персональных данных для распространения». Так, к ним относятся «персональные данные, доступ неограниченного круга лиц к

которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном данным Федеральным законом».

Федеральным законом «О персональных данных» устанавливаются принципы и условия обработки персональных данных. Так, обработка персональных данных должна осуществляться на законной и справедливой основе.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения

персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных

Федеральным законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[38], включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях»[32], либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

Пункт 8 части 1 статьи 6 Федерального закона «О персональных данных» стал предметом рассмотрения Конституционного Суда РФ. Он определил, что данный пункт является «не противоречащим Конституции Российской Федерации в той мере, в какой он по своему конституционно-правовому смыслу в системе действующего правового регулирования:

допускает размещение на сайте в сети Интернет средством массовой информации, действующим в форме сетевого издания, персональных данных медицинского работника, ранее размещенных на основании федерального закона на официальном сайте соответствующей медицинской организации, вне зависимости от наличия на то его согласия;

предусматривает обязанность редакции такого средства массовой информации не допускать наличия на своем сайте исходящих от третьих лиц оценок, не относящихся к профессиональной деятельности медицинского работника, а равно очевидно противоправных высказываний;

предусматривает обязанность редакции такого средства массовой информации принимать меры по проверке сведений, предположительно содержащих не соответствующие действительности утверждения, порочащие честь, достоинство или деловую репутацию медицинского работника, на основании его обращения в разумные сроки, с целью их изменения либо удаления, а равно с целью опубликования в установленном законом порядке опровержения (ответа) на том же сайте, на время проверки приостанавливая доступ к соответствующему отзыву или делая пометку о его спорном характере;

не исключает возможности на основании судебного решения, вынесенного по обращению медицинского работника, установить для такого средства массовой информации - если оно допускает систематическое злоупотребление правом при размещении персональных данных медицинского работника или систематически не предотвращает такого злоупотребления правом лицами, размещающими отзывы, - запрет на распространение персональных данных медицинского работника и (или) отзывов о его профессиональной деятельности, когда иные способы защиты не смогли (не могут) обеспечить защиту его прав»[23].

- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности

средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

- обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»[34], в порядке и на условиях, которые предусмотрены указанным Федеральным законом;

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

- обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных Федеральным законом от 27 мая 1996 года N 57-ФЗ «О государственной охране»[35].

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку

персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

1.2 Законодательное регулирование защиты персональных данных

Защита персональных данных является одной из наиболее актуальных проблем для российских компаний и организаций, как коммерческих, так и государственных. В Российской Федерации защита персональных данных на законодательном уровне обеспечивается рядом Федеральных законов и нормативно-правовых документов. Так, федеральный закон №152-ФЗ «О персональных данных» был принят в 2006 году и затрагивает защиту персональных данных, обрабатываемых в государственных и коммерческих организациях. Со времени принятия данного закона прошло больше десяти лет, но до сих пор защита персональных данных, обрабатываемых или

содержащихся в информационной системе, является одной из актуальных прикладных задач как в плане усовершенствования нормативной базы, так и организации его реализации[18,49].

На сегодняшний день существует множество трудов отечественных и зарубежных ученых, монографии, материалов и периодических научных изданий по исследуемому вопросу обеспечения безопасности персональных данных, которые можно найти как в интернет-ресурсах, так и выпускаемых печатных журналах и бюллетенях. В статье Козина И.С.[14,19] предложен метод определения опасности угрозы, позволяющий подготовить перечень опасных угроз с учетом степени важности объекта защиты, в статье Соловьева В.В.[28,39] предложен способ организации схемы защиты информационной системы персональных данных. Концептуальны также труды, посвященные разработке методик маскирования персональных данных в базе данных[15,16]. Вместе с тем в рамках данной проблематики должны учитываться результаты работ таких авторов, как Минбалеев А.В. [19,4], раскрывающих также проблематику защиты персональных данных.

Нормативно-правовая основа решения данной актуальной и прикладной проблематики также значительна и фундаментальна. Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (далее - нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов

персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

Решения межгосударственных органов, принятые на основании положений международных договоров Российской Федерации в их истолковании, противоречащем Конституции Российской Федерации, не подлежат исполнению в Российской Федерации. Такое противоречие может быть установлено в порядке, определенном федеральным конституционным законом.

Ниже перечислим самые основные документальные акты, включающие и федеральную законодательную базу, и ведомственную:

- Федеральный Закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».

- Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[24].

- Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[33].

- Приказ Федеральной службы по техническому и экспортному контролю (далее ФСТЭК) № 17 от 11 февраля 2013 г. – «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[25].

- Приказ ФСТЭК № 21 от 18 февраля 2013г. – «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[26].

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (от 15 февраля 2008 г.)[1].

- Банк данных угроз безопасности информации (ФСЭК)[2].

- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»[7].

- ГОСТ РИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»[8].

Таким образом, система нормативно-правовых актов, регламентирующих понятие персональных данных и особенности их защиты представлена законами и подзаконными актами. Следует отметить, что защита персональных данных осуществляется не только нормами гражданского законодательства, а также нормами иных отраслей права.

Глава 2 Особенности защиты персональных данных в российском гражданском праве

2.1 Понятие защиты персональных данных

Сбором персональных данных информации занимаются государственные или муниципальные органы, практически любые юридические лица, а также физические лица. Согласно п. 2 ст. 3 ФЗ «О персональных данных», оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Практически любые действия, связанные с реализацией прав граждан, невозможны без процедуры передачи персональных данных. По справедливому замечанию руководителя отдела аналитики Positive Technologies Евгения Гнедина: «Всем нужно понять: все, что мы оставляем в интернете, там и останется, а возможно, будет использовано с недобросовестными целями». На «черном рынке» персональные данные стоят кратно больше, чем даже полные сведения банковской карты.

В феврале 2021 года информационный сайт РИА Новости опубликовали список «громких» утечек 2020-2021 года. Среди источников утечек оказались такие крупнейшие организации, как «Яндекс», Сбербанк, Россельхозбанк, Тинькофф банк, Райффайзенбанк, Авито, Юла и многие другие. Количество опубликованных и продаваемых данных, т.е. количество пострадавших, колеблется от нескольких до сотен тысяч. По данным РБК, в начале апреля 2021 года стало известно, что хакеры, воспользовавшись уязвимостью в дистанционной подаче первичных заявок на получение

кредита наличными, выставили на продажу данные граждан, которые обращались в банк «Дом.РФ» для оформления потребительского кредита. Записи могут содержать полный набор персональных данных, которые требуются для оформления кредита: ФИО, дата рождения, сумма и вид кредита, номер телефона, почтовый ящик, паспортные данные, ИНН, СНИЛС, домашний адрес, адрес места работы, должность, размер дохода и другие сведения. Согласно объявлению, полная база стоит 100 тыс. руб. Отдельные строки с данными за 2021 год продаются за 15 руб., за вторую половину 2020 года – 10 руб., за первую половину 2020 года – 7 руб.

Всё это говорит о том, что даже сегодня при современном уровне развития технологий ни одна организация, включая органы государственной власти, не может гарантировать абсолютную защиту личных данных от мошенников и нелегальных учреждений, которые зарабатывают деньги на торговле персональными данными на теневых рынках. Персональные данные воспринимаются как ценный экономический актив, а не что-то сугубо личное.

Вред, который может быть причинен физическому лицу в результате обработки его персональных данных, может быть субъективным и объективным. Под субъективным понимаются, например, оскорбление чести и достоинства личности, посягательства на частную, включая семейную жизнь, в том числе влияющие на самооценку индивида и т. д. Объективный вред заключается в причинении преимущественно материального ущерба. Человек должен обладать правом на информационное самоопределение: он должен самостоятельно решать, какая информация о нем и кому может быть доступна.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе,

результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В гражданском законодательстве отсутствует определение понятия защиты гражданских прав и защиты персональных данных. Мы предлагаем под защитой персональных данных понимать применение уполномоченными на то государственными органами или непосредственно самими участниками гражданских правоотношений мер, направленных на восстановление нарушенных прав или пресечение действий, создающих угрозу распространения информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Массовые утечки персональных данных в России в последнее время существенно возросли. Очевидно, утечка персональных данных возможна по объективным техническим причинам, либо по субъективным, вследствие халатности, или преследования корыстных целей сотрудников. Использование персональных данных в руках злоумышленников чревато в

преступных целях (получение кредита, незаконные сделки с недвижимостью, перевод денежных средств и прочее).

На организацию безопасности конфиденциальных данных для защиты персональных данных требуется наличие лицензии ФСТЭК. Однако, специалистов, обладающих соответствующей квалификацией, опытом работы, и требующимися знаниями крайне мало. Также необходимо специализированное помещение и соответствующее оборудование, обеспечить которое в небольших организациях не представляется возможным.

Возможности переобучать своих сотрудников, закупать дополнительное оборудование, приобретать соответствующие лицензии для обеспечения безопасности персональных данных пользователей имеет не каждый работодатель, так как расходы на приобретение необходимых технических средств защиты персональных данных, а также обслуживание системы стоит в несколько раз дороже, чем уплата штрафа[21,182].

К сожалению, приходится констатировать, что создаваемые технологии прямо противоречат действующим принципам нормативно–правовой базы, что говорит о сомнительной эффективности законодательства о защите персональных данных. Законодательство о защите персональных данных в существующем виде является все менее адекватно в соотношении с современными технологическими реалиями, и конечно, нуждается в значительной корректировке[12,37].

Таким образом, под защитой персональных данных мы предлагаем понимать применение уполномоченными на то государственными органами или непосредственно самими участниками гражданских правоотношений мер, направленных на восстановление нарушенных прав или пресечение действий, создающих угрозу распространения информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

С одной стороны новейшие технологии упростили сбор, хранение и распространение данных, а с другой стороны возросла угроза незаконного оборота данных, что является основной проблемой в цифровой информационной сфере и взаимоотношениях физических и юридических лиц.

2.2 Методы и способы защиты персональных данных в российском гражданском праве

Цифровизация общества в России с использованием новых технологий способствовала непосредственному контакту органов публичной власти с гражданами, коммерческими и иными организациями.

Проблема защиты личности от несанкционированного сбора персональных данных, злоупотреблений, возможных при сборе, обработке и распространении информации персонального характера на сегодняшний момент является достаточно актуальной для нашего государства.

Происходящие процессы использования новых информационных технологий имеют множество позитивных моментов, позволяющих оперативно и прозрачно решать управленческие задачи, оказывать различные услуги населению и пр. Одновременно они могут негативно отразиться на конфиденциальности персональных данных, основываясь на более широком подходе к исследуемой проблематике – неприкосновенности частной жизни, выступающей фундаментальным личным правом человека и гражданина[4,45].

Очевидно, что злободневные для IT-сферы вопросы коммерциализации персональных данных остаются пока без однозначных ответов и еще требуют проработки: доктринальной, законодательной, правоприменительной. Главная задача это необходимость заботиться о защите прав субъектов персональных данных.

Защита персональных данных перестает быть исключительно вопросом охраны права человека на неприкосновенность частной жизни. В цифровой экономике регулирование правового режима данных ставит более сложные задачи сочетания интересов личности и целей экономического развития.

Для защиты персональных данных логичными представляются два пути: во-первых, признание персональных данных товаром, т.е. объектом гражданских прав, и введение соответствующего нормативно-правового регулирования, и, во-вторых, признание недопустимой подобной торговли, а также борьба с ней.

Для защиты конфиденциальной информации физических лиц, разрешение вопроса нормативного правового обеспечения в целях совершенствования законодательной базы является одной из основных задач в сфере обеспечения информационной безопасности России[5,34].

С целью реализации первого направления необходимо внести соответствующие изменения в ст. 128 ГК РФ, классифицирующие объекты гражданских прав.

В России, органом, осуществляющим функции по контролю и надзору в сфере средств массовой информации, функции по контролю и надзору за соответствием обработки персональных данных, по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Президент Российской Федерации В.В. Путин на рабочей встрече с представителями Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций обратил внимание на то, что в связи с цифровизацией отечественной экономики особенно актуальным является вопрос защиты персональных данных[6].

Важным является тот аспект, что на нынешней ступени развития цифровой экономики российский законодатель придерживается

консервативного представления о персональных данных. Последние представляются как предмет, который не подлежит торгу. Персональные данные принадлежат к исключительно человеческой ценности, несмотря на тенденции во всем мире. Т.е. законодательство о персональных данных направлено на защиту, прежде всего, индивидов, а не бизнеса или государства.

Проблематика защиты персональных данных имеет немаловажное значение не только для Российской Федерации, но и для всего мирового сообщества. В европейском законодательстве персональные данные индивида и их защита рассматриваются как основное право, поскольку оно опирается и проистекает из права на защиту частной жизни[29,117]. Однако стремительная цифровизация практически всех сфер жизнедеятельности индивида приводит к тому, что информация, не подлежащая распространению и имеющая частный характер, в информационно-правовом пространстве начинает существовать по новым правилам, попадая в свободный доступ.

Осознавая возможность открытого доступа в информационное пространство персональных данных и возможные последствия их использования, Российской Федерацией в 2005 г. была ратифицирована Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[39].

К Конвенции Россия присоединилась еще в тот период, когда процессы цифровизации были в самом начале, не было отдельного законодательного акта в данной сфере, что свидетельствует об осознании значимости данной проблематики и необходимости защиты конфиденциальных сведений граждан.

Следует отметить, что в Европе процессы цифровизации и связанная с ними потребность в защите персональных данных стали происходить значительно раньше, чем в России. Так, например, вышеуказанной

Конвенцией 1981 г. в ст. 7 были установлены гарантии защиты личных сведений, хранящихся в автоматизированных файлах данных, и меры безопасности, направленные на предотвращение их случайного или несанкционированного уничтожения или случайной потери, а также направленные на недопущение незаконного доступа и обращения с ними. В мае 2018 г. в Европе был введен в действие новый документ, закрепляющий правила обработки персональных данных – Общий регламент по защите данных[20] (далее – Регламент).

В статье 4 Регламента под термином «персональные данные» понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. К информации, которая позволяет произвести идентификацию индивида, относятся: имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн, IP-адрес, данные, полученные при использовании cookie и т.д.

Новеллой Регламента стал новый подход к обработке персональных данных, предполагающий применение принципа экстерриториальности. Это обусловлено тем, что новые коммуникационные технологии, как правило, не имеют привязки к конкретной территории, что создает новый формат общения между различными субъектами, а также влияет на возможности использования конфиденциальных сведений других лиц. Высокая вероятность доступа к таким сведениям привела к усилению ответственности за нарушение правил обработки персональных данных. Так, в европейских странах штрафы к операторам, уполномоченным осуществлять обработку персональных данных, достигают 20 млн. евро (около 1,5 млрд рублей).

Достоинством Регламента является дифференцированный подход, применяемый к контролерам обработки данных, действующим в государственном и частном секторах. Дифференцированность также проявляется в разграничении категории персональных данных, как отмечалось выше, это данные разнонаправленного характера: о здоровье,

генетические и биометрические данные, электронная почта и пр. Соответственно, разные виды сведений требуют и разного подхода к ним с применением соответствующих соразмерных средств защиты. О поиске необходимого баланса публичных и частных интересов в условиях применения современных технологий и одновременно потребности в защите частной жизни свидетельствует опыт различных государств и международных организаций. В частности, в Докладе Верховного комиссара ООН по правам человека был поставлен вопрос о защите прав человека в цифровой век[11].

Применительно к Российской Федерации в условиях очевидности фактов цифровой трансформации, в основе которой лежит система управления программой «Цифровая экономика»[22], потребность в защите персональных данных является наиболее актуальной. Не случайно Закон о персональных данных определил, что лица, виновные в нарушении требований его норм, несут предусмотренную законодательством Российской Федерации ответственность. В условиях возможного открытого доступа в информационном пространстве к персональным данным в России должны действовать своевременные и адекватные меры их защиты.

Меры защиты персональных данных установлены в административном, уголовном и трудовом законодательстве, а также гражданском законодательстве.

Так, нормами административного законодательства, предусмотрена защита персональных данных на основе конституционных положений о неприкосновенности частной жизни.

Цифровизация российского общества способствует развитию законодательства о персональных данных. Его нормы становятся более обширными и гибкими по отношению к применению информационных технологий. Так, Федеральным законом от 13 июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации,

информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации»[33] был установлен новый термин – «право на забвение»[36], вводящий ограничения в отношении информации в интернете. Введение данного специфического права было связано с тем, что информация, устаревшая, потерявшая актуальность, продолжала сохраняться в интернете, и ее легко можно было выявить.

Следует отметить, что европейская практика ранее не раз сталкивалась с такими ситуациями, и разрешение их зачастую осуществлялось в судебном порядке. Большое значение в данном аспекте имеют решения Европейского Суда по правам человека (далее – ЕСПЧ). Так, например, в одном из материалов «Кэтт против Соединенного Королевства» заявительница обратилась в суд, т.к. ее личные данные хранились в базе данных полиции в картотеке «внутренние экстремисты». ЕСПЧ поддержал заявительницу, подойдя к рассматриваемому материалу с учетом всех обстоятельств дела, и признал нарушение ст. 8 Европейской конвенции. ЕСПЧ принял во внимание возраст заявителя (94 года) и отсутствие обстоятельств, касающихся совершения насилия[17].

Российские граждане аналогичным образом стали обращаться к операторам обработки персональных данных о реализации «права на забвение» по информации, касающейся их лично. Так, посредством обращения в суд был решен вопрос о непредоставлении личных сведений, связанных с преступным прошлым бизнесмена Михайлова Сергея. В 1990-е годы Михайлов был обвинен в отмывании денег в связи с солнцевской группировкой и арестован в Швейцарии. Суд присяжных оправдал Михайлова, однако информация об этих событиях в интернете была сохранена[2]. Несмотря на наличие «права на забвение», в российском законодательстве до настоящего времени возникают вопросы, связанные с

его реализацией, прежде всего фактом достоверности информации, имеющей устаревший характер.

Меры административно-правовой защиты личных сведений граждан проявляются в контрольно-надзорной деятельности, осуществляемой Роскомнадзором, и выявлении фактов незаконной деятельности в области защиты информации. КоАП РФ за нарушение законодательства в области персональных данных предусмотрена административная ответственность в отношении должностных лиц, юридических лиц (ст. 13.11, 19.7.9), однако размер штрафа был незначительным[13]. Это неоднократно отмечалось учеными, подчеркивалось несоответствие между возможными последствиями административного правонарушения в области оборота персональных данных и штрафными санкциями[27,24]. Несмотря на ужесточение санкции в КоАП РФ, проблемы, связанные с защитой персональных данных, являются неразрешенными.

С одной стороны, активизация деятельности Роскомнадзора в данной сфере способствует защите предоставляемых сведений гражданами, с другой стороны, в условиях цифровизации общества увеличивается количество операторов, осуществляющих обработку персональных данных, что порождает и рост числа нарушений.

Это, в свою очередь, усложняет надзор за ними со стороны уполномоченных органов в лице Роскомнадзора. Одновременно возникают проблемы, связанные с деятельностью иностранных компаний, действующих за пределами Российской Федерации, передающих информацию на территорию нашего государства с нарушением законодательно установленных требований. Ужесточение административных мер в отношении иностранного СМИ-агента, нарушающего закон, должно осуществляться посредством применения мер административной ответственности с назначением высокого размера штрафа и принятием

организационных мер, связанных с ограничением доступа к обработке информации[4,46].

Ответственность за распространение сведений о частной жизни лица предусмотрена статьями 137, 140, 272 Уголовного кодекса РФ[31] и предусматривает альтернативное наказание виде штрафа, исправительных работ, ареста в зависимости от тяжести совершенного деяния.

В трудовом законодательстве ответственность предусмотрена статьями 81, 90, 192. В соответствие со ст. 81 возможно расторжение трудового договора в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника[30].

Согласно ст. 90 ТК РФ лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

За совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

1) замечание;

2) выговор;

3) увольнение по соответствующим основаниям.

Федеральными законами, уставами и положениями о дисциплине для отдельных категорий работников могут быть предусмотрены также и другие дисциплинарные взыскания.

К дисциплинарным взысканиям, в частности, относится увольнение работника по основаниям, предусмотренным пунктами 5, 6, 9, или 10 части первой статьи 81, в случаях, когда виновные действия, дающие основания для утраты доверия, либо соответственно аморальный проступок совершены работником по месту работы и в связи с исполнением им трудовых обязанностей.

В гражданском законодательстве не разработана система способов защиты персональных данных. Вместе с тем, мы полагаем, что на основе ст. 12 ГК РФ, предусматривающей способы защиты гражданских, можно предложить применение отдельных из них к защите персональных данных. Так, к ним можно отнести компенсацию морального вреда.

Согласно ст. 1099 основания и размер компенсации гражданину морального вреда определяются правилами, предусмотренными Гражданским Кодексом РФ.

Моральный вред, причиненный действиями (бездействием), нарушающими имущественные права гражданина, подлежит компенсации в случаях, предусмотренных законом.

Компенсация морального вреда осуществляется независимо от подлежащего возмещению имущественного вреда.

Компенсация морального вреда осуществляется независимо от вины причинителя вреда в случаях, когда вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию.

Компенсация морального вреда осуществляется в денежной форме.

Размер компенсации морального вреда определяется судом в зависимости от характера причиненных потерпевшему физических и нравственных страданий, а также степени вины причинителя вреда в случаях, когда вина является основанием возмещения вреда. При определении размера компенсации вреда должны учитываться требования разумности и справедливости.

Характер физических и нравственных страданий оценивается судом с учетом фактических обстоятельств, при которых был причинен моральный вред, и индивидуальных особенностей потерпевшего.

Таким образом, защита персональных данных в условиях цифровизации общества основывается на сочетании частно-публичных интересов при соблюдении прав субъекта персональных данных, включающих в себя как обработку персональных данных лица только с его согласия, так и закрепление правил взаимодействия пользователей и обрабатывающих данные компаний.

Для совершенствования правового регулирования в сфере защиты персональных данных необходима классификация отдельных видов персональных данных: специальных, биометрических и других с уточнением составляющих их элементов. Это должно найти отражение в понятийном аппарате Закона о персональных данных.

Заключение

В результате проведенного исследования мы пришли к следующим выводам.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Персональные данные это любая информация, которая позволяет определить личность пользователя.

Однако понятие персональных данных не конкретизировано и может возникнуть затруднение с отнесением той или иной информации об индивиде к данным, относящимся к его персоне.

Защита персональных данных является одной из наиболее актуальных проблем для российских компаний и организаций, как коммерческих, так и государственных. В Российской Федерации защита персональных данных на законодательном уровне обеспечивается рядом Федеральных законов и нормативно-правовых документов. Защита персональных данных осуществляется не только нормами гражданского законодательства, а также нормами иных отраслей права.

Практически любые действия, связанные с реализацией прав граждан, невозможны без процедуры передачи персональных данных. Сегодня при современном уровне развития технологий ни одна организация, включая органы государственной власти, не может гарантировать абсолютную защиту личных данных от мошенников и нелегальных учреждений.

В гражданском законодательстве отсутствует определение понятия защиты гражданских прав и защиты персональных данных. Мы предлагаем под защитой персональных данных понимать применение уполномоченными на то государственными органами или непосредственно самими участниками гражданских правоотношений мер, направленных на восстановление нарушенных прав или пресечение действий, создающих угрозу

распространения информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Новейшие технологии упростили сбор, хранение и распространение данных, а с другой стороны возросла угроза незаконного оборота данных, что является основной проблемой в цифровой информационной сфере и взаимоотношениях физических и юридических лиц.

Для защиты персональных данных логичными представляются два пути: во-первых, признание персональных данных товаром, т.е. объектом гражданских прав, и введение соответствующего нормативно-правового регулирования, и, во-вторых, признание недопустимой подобной торговли, а также борьба с ней.

Для защиты конфиденциальной информации физических лиц, разрешение вопроса нормативного правового обеспечения в целях совершенствования законодательной базы является одной из основных задач в сфере обеспечения информационной безопасности России.

С целью реализации первого направления необходимо внести соответствующие изменения в ст. 128 ГК РФ, классифицирующие объекты гражданских прав.

В гражданском законодательстве не разработана система способов защиты персональных данных. Вместе с тем, мы полагаем, что на основе ст. 12 ГК РФ, предусматривающей способы защиты гражданских, можно предложить применение отдельных из них к защите персональных данных. Так, к ним можно отнести компенсацию морального вреда.

Основания и размер компенсации гражданину морального вреда определяются правилами, предусмотренными Гражданским Кодексом РФ.

Моральный вред, причиненный действиями (бездействием), нарушающими имущественные права гражданина, подлежит компенсации в случаях, предусмотренных законом.

Компенсация морального вреда осуществляется независимо от подлежащего возмещению имущественного вреда.

Компенсация морального вреда осуществляется независимо от вины причинителя вреда в случаях, когда вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию.

Компенсация морального вреда осуществляется в денежной форме.

Защита персональных данных в условиях цифровизации общества основывается на сочетании частно-публичных интересов при соблюдении прав субъекта персональных данных, включающих в себя как обработку персональных данных лица только с его согласия, так и закрепление правил взаимодействия пользователей и обрабатывающих данные компаний. Для совершенствования правового регулирования в сфере защиты персональных данных необходима классификация отдельных видов персональных данных: специальных, биометрических и других с уточнением составляющих их элементов. Это должно найти отражение в понятийном аппарате Закона о персональных данных.

Список используемой литературы и используемых источников

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008) // СПС КонсультантПлюс.
2. Банк данных угроз безопасности информации // https://bdu.fstec.ru/
3. Бизнесмен Сергей Михайлов воспользовался «правом на забвение». URL: https://www.rbc.ru/technology_ and_media/30/05/2016/574873bc9a79477bf8e5a75d (дата обращения: 04.05.2021).
4. Бучакова М.А. Персональные данные и их защита в условиях цифровизации общества // Алтайский юридический вестник. 2021. № 2 (34).
5. Ворожбит Д.В. Особенности защиты персональных данных пользователей интернетресурсов // Работы членов студенческого научного общества СЮИ ФСИН России: Сборник статей. Самара, 2019.
6. Встреча с главой Роскомнадзора Андреем Липовым. URL: http://www.kremlin.ru/events/president/ news/63874 (дата обращения: 19.12.2020).
7. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». М.: Стандартинформ, 2008.
8. ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст). М.: Стандартинформ, 2014.

9. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 N 14-ФЗ (ред. от 18.03.2019, с изм. от 28.04.2020) // Собрание законодательства РФ. 1996. N 5. Ст. 410.

10. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ (ред. от 09.03.2021) // Собрание законодательства РФ.1994. N 32. Ст. 3301.

11. Доклад Управления Верховного комиссара ООН по правам человека от 30 июня 2014 г. A/HRC/27/37 «Право на неприкосновенность личной жизни в цифровой век». URL: http://https://www.ohchr.org.

12. Истратова А. Подзаконный акт «О защите персональных данных работников» как этап развития организационно-правовых основ защиты персональных данных работника // Юрист ВУЗа. 2009.

13. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 26.05.2021) // Собрание законодательства РФ. 2002. N 1 (ч. 1). Ст. 1.

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

15. Коломыцев М.В., Носок С.А. Маскирование таблиц базы данных с использованием технологии SQL // Защита информации. 2017. №19.

16. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // Собрание законодательства РФ. 2014. N 31. Ст. 4398.

17. Кэтт (Catt) против Соединенного Королевства: постановление ЕСПЧ от 24.01.2019 // СПС КонсультантПлюс.

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

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

20. Общий регламент по защите данных // СПС Консультант Плюс

21. Попова Ю.П. К вопросу о значимости института защиты персональных данных граждан в современной России // Наука и просвещение: актуальные вопросы, достижения и инновации. Сборник статей V Международной научно-практической конференции. Пенза, 2021.

22. Постановление Правительства РФ от 02.03.2019 N 234 (ред. от 21.08.2020) «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» (вместе с «Положением о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации») // Собрание законодательства РФ. 2019. N 11. Ст. 1119.

23. Постановление Конституционного Суда РФ от 25.05.2021 N 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг» // Собрание законодательства РФ. 2021. N 22. Ст. 3915.

24. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. 2012. N 45. Ст. 6257.

25. Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных

системах» (Зарегистрировано в Минюсте России 31.05.2013 N 28608) (с изм. и доп., вступ. в силу с 01.01.2021) // Российская газета. 2013. N 136.

26. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) // Российская газета. 2013. № 107.

27. Солдатова В.И. Проблемы защиты персональных данных в условиях применения цифровых технологий // Право и экономика. 2019. № 12. С. 24-34.

28. 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.

29. Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. 2018. Т. 13. № 5.

30. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 30.04.2021) (с изм. и доп., вступ. в силу с 01.05.2021) // Собрание законодательства РФ. 2002. N 1 (ч. 1). Ст. 3.

31. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) // Собрание законодательства РФ. 1996. N 25. Ст. 2954.

32. Федеральный закон от 03.07.2016 N 230-ФЗ (ред. от 08.12.2020) «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях» // Собрание законодательства РФ. 2016. N 27 (Часть I). Ст. 4163.

33. Федеральный закон от 13.07.2015 N 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации» // Собрание законодательства РФ. 2015. N 29 (часть I). Ст. 4390.

34. Федеральный закон от 24.04.2020 N 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства РФ. 2020. № 17. Ст. 2701.

35. Федеральный закон от 27.05.1996 N 57-ФЗ (ред. от 01.04.2020) «О государственной охране» // Собрание законодательства РФ. 1996. N 22. Ст. 2594.

36. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 20.03.2021) // Собрание законодательства РФ. 2006. N 31 (1 ч.). Ст. 3448.

37. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) «О персональных данных» (с изм. и доп., вступ. в силу с 01.03.2021) // Собрание законодательства РФ. 2006. N 31 (1 ч.). Ст. 3451.

38. Федеральный закон от 27.07.2010 N 210-ФЗ (ред. от 30.12.2020) «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ. 2010. N 31. Ст. 4179.

39. Федеральный закон от 19.12.2005 N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // Собрание законодательства РФ. 2005. N 52 (1 ч.). Ст. 5573.

40. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Собрание законодательства РФ. 2017. N 20. т. 2901