Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет
(Национальный исследовательский университет)»
Институт открытого и дистанционного образования
Кафедра «Управление и право»

РАБОТА ПРОВЕРЕНА
Рецензент
Начальник отдела информационных
технологий администрации КГО
Челябинской области
_____Е.С. Суслов
18.06.2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой
_____ А.А. Демин
22.06.2018 г.

Правовое регулирование защиты персональных данных

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ЮУрГУ – 40.03.01.2018.31998.ПЗ.ВКР

Руководитель работы
доцент кафедры УиП
_____ Н.Г. Деменкова
20.06.2018 г.

Автор работы
студент группы ДО-550
_____ А.А. Сошин
20.06.2018 г.

Нормоконтролер
ст. преподаватель кафедры УиП
_____ Е.Н. Бородина
21.06.2018 г.

Челябинск 2018

АННОТАЦИЯ

Сошин А.А. Правовое регулирование защиты персональных данных. – Челябинск: ЮУрГУ, ДО-550, 63 с., библиогр. список – 53 наим., 8 л. плакатов ф. А4.

Объектом исследования в данной работе является комплекс общественных отношений, складывающихся в процессе правового регулирования защиты персональных данных.

Цель работы – исследование, выявление и разрешение актуальных теоретических и практических проблем правового регулирования защиты персональных данных, научное обоснование предложений по разработке и совершенствованию законодательства в данной сфере.

В работе рассмотрены теоретико-правовые основы института персональных данных, в том числе историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в Российской Федерации, нормативно-правовые основы и понятие персональных данных, их виды. Во второй главе изучен правовой статус субъектов, участвующих в обороте персональных данных. В третьей главе выявлены особенности и проблематика защиты персональных данных в государственных органах.

Результаты работы имеют практическую значимость и могут применяться для защиты персональных данных в государственных органах.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы. В начале 21 века бурное развитие сети Интернет и компьютерных технологий повлекло за собой соответствующие изменения в использовании и хранении персональных данных. Применение компьютеров в значительной степени облегчило работу многих государственных органов: появилась возможность не осуществлять ввод данных каждый раз при обращении в тот или иной орган государственной власти, а фиксировать подобную информацию однократно, т.е. при первом обращении. Уточнения же в ней можно осуществлять по мере изменения, к примеру, при переезде гражданина в другой город, смене фамилии и др.

Обратной стороной данных позитивных изменений в документообороте оказалась его малая защищенность. В открытом доступе и в продаже на рынках появлялись информационные базы различных государственных органов (государственной автоинспекции, паспортных столов и др.), содержащие персональные данные граждан Российской Федерации. Данные базы и содержащиеся в них сведения могли стать основой совершения противоправных и преступных действий, поэтому в 2006 году принимается федеральный закон № 152 «О персональных данных». Его принятие в значительной степени позволило урегулировать отношения, связанные с обработкой персональных данных.

Однако на сегодняшний день органы государственной власти взяли курс на создание электронного правительства, которое предполагает предоставления набора государственных услуг при минимальном взаимодействии между государством и гражданином, посредством использования цифровых технологий. Тем самым накапливаются огромные массивы информации, включающей полные персональные данные граждан Российской Федерации, разглашение или утрата которых может наносить серьезный ущерб органам государственной власти и личности каждого гражданина.

По итогам 2017 года Роскомнадзором было проведено 1640 плановых проверок, в том числе 333 – в отношении государственных органов, муниципальных органов, организующих и (или) осуществляющих обработку персональных данных. Проведено также 99 внеплановых проверок. По результатам мероприятий выдано 619 предписаний об устранении выявленных нарушений, в том числе порядка 100 – в отношении государственных органов. Кроме того, территориальными органами Роскомнадзора за 2017 год было направлено в суды порядка 7 тыс. протоколов об административных правонарушениях, а также наложено административных штрафов на сумму почти 6 млн. руб. за типичные нарушения Закона о персональных данных и принятых на его основе позаконных актов [1].

[1] Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) [Электронный ресурс]/ Режим доступа: https://rkn.gov.ru/press/annual_reports/

Исходя из вышесказанного, повышается актуальность вопросов, связанных с повышением эффективности защиты персональных данных от утечки, несанкционированного доступа и других проблем, связанных с обеспечением безопасности обработки и хранения персональных данных граждан Российской Федерации.

В работе использованы труды теоретиков права, а также специалистов в области отраслевых юридических наук: С.А. Авакьян, С.С. Алексеева, Г. В. Атаманчук, Д.Н. Бахрах, С.Ю. Головиной, Ю.И. Гревцова, О.С. Иоффе, Е.А.Керимовой, М.Ю. Романовской, О.С. Соколовой, А. Токаренко, Ю. Травкина, Е.Н. Трубецкой, А.С. Федосина, Р.О. Халфиной, В.Н. Храпанюка, М.Д. Шаргородского, Г.Ф. Шершеневича и др.

Значительная роль в развитии представлений о механизме правового регулирования института персональных данных принаждлежит Ф.А. Абаеву, А.Г. Арешеву, Д.С. Власову, С.В. Гуде, Н.Г. Беляевой, А.Л. Доходову, В.П. Иванскому, В.Я. Ищейнову, А.А. Малюк, А.В. Морозову, Д.Ю. Писареву, К.М. Саматову, В.А. Сергиевич, Л.А. Сергиенко и другим.

Диссертационные исследования по темам, связанным защитой персональных данных, проводились Н.Г. Белгородцевой, И.Л. Вельдер, А.В. Дворецким, А.В.Кучеренко, О.Б. Просветовой, Н.И. Петрыкиной, А.С. Маркевич.

Целью является исследование, выявление и разрешение актуальных теоретических и практических проблем правового регулирования защиты персональных данных, научное обоснование предложений по разработке и совершенствованию законодательства в данной сфере.

Задачи работы.

1. Изучить современные тенденции развития и историко-правовые предпосылки формирования института персональных данных в Российской Федерации.
2. Рассмотреть понятие, виды и правовую природу института персональных данных.
3. Определить общую характеристику правового понятия «субъект персональных данных».
4. Изучить права и обязанности субъектов, участвующих в обороте персональных данных.
5. Выявить особенности защиты персональных данных в государственных органах.
6. Проанализировать проблемы защиты персональных данных в государственных органах.

Объектом исследования в данной работе является комплекс общественных отношений, складывающихся в процессе правового регулирования защиты персональных данных.

Предметом исследования выступает совокупность правовых норм, регулирующих отношения в сфере защиты персональных данных.

Методологическую основу исследования составили общенаучные методы, в том числе индукция, дедукция, анализ, синтез, аналогия, абстрагирование, и

частно-научные методы, в том числе сравнительно-правовой, формально-юридический, историко-правовой, метод конкретного правового анализа.

Теоретическую основу исследования составили фундаментальные труды и содержащиеся в них положения общей теории государства и права, литература по гражданскому законодательству РФ, судебная практика.

Нормативной базой исследования стали Конституция Российской Федерации, федеральные конституционные законы, федеральные законы, международные правовые акты о правах человека в сфере защиты персональных данных, Указы Президента Российской Федерации, Постановления Правительства Российской Федерации и ведомственные приказы в области защиты информации.

Научная новизна исследования заключается в практических рекомендациях, предлагаемых автором в качестве устранения проблем правовой защиты персональных данных.

Теоретическая значимость исследования заключается в том, что сформулированные автором теоретические выводы, практические рекомендации и предложения вносят определенный вклад в правовую науку, систематизируют научные знания по вопросам правового регулирования защиты персональных данных, а также могут быть использованы в дальнейших научных изысканиях.

Практическое значение исследования состоит в том, что сформулированные в нем выводы и предложения могут быть использованы в ходе дальнейшего реформирования правовых основ защиты персональных данных.

Структура исследования определена его целью и задачами и состоит из введения, трех глав, заключения, библиографического списка, приложений. В первой главе рассмотрены историко-правовые предпосылки формирования института персональных данных, теоретико-правовые основы института персональных данных, в том числе современные тенденции развития института персональных данных в Российской Федерации, нормативно-правовые основы и понятие персональных данных, виды. Во второй главе изучен правовой статус субъектов, участвующих в обороте персональных данных. В третьей главе выявлены особенности и проблематика защиты персональных данных в государственных учреждениях. В заключении подведены итоги исследования. Библиографический список содержит перечень источников, использованных при подготовке данной работы.

1 ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ИНСТИТУТА ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1 Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в Российской Федерации

Развитие социума невозможно без совершенствования правового статуса личности, без получения человеком на каждой новой ступени развития дополнительных прав и свобод, постоянно расширяющихся от одной исторической эпохи к другой. Сложившаяся благодаря такому поступательному движению система прав и свобод человека и гражданина к настоящему моменту представляет собой органическое единство, в котором одни права зачастую раскрывают содержание других, гарантируют их. Так, например, право на неприкосновенность частной жизни нельзя рассматривать в отрыве от права на защиту персональных данных от неправомерных посягательств.

Вопрос роли и места института персональных данных в системе права на текущем этапе является недостаточно изученным и очень актуальным. Стоит отметить, что в юридической науке практически полностью отсутствуют работы, направленные на его изучения, даже несмотря на особую значимость изучаемого института с практической точки зрения. На наш взгляд, возможными причинами послужили следующие. Во-первых, большинство экспертов и специалистов защиту персональных данных понимают только как техническую задачу, которая включает следующие аспекты: защита от несанкционированного доступа и от кражи, защита от утечки информации по техническим каналам и так далее. В данной позиции происходит изменение полюса внимания в исключительно техническую область. Стоит отметить, что защита персональных данных – это, прежде всего, защита прав субъекта (физического лица). А именно, того лица, которое владеет и предоставляет свои персональные данные частной организации либо государственному органу.

Во-вторых, нормы, которые регулируют обработку персональных данных приянто считать частью института неприкосновенности частной жизни, что также может являться возможной причиной.

Впервые право на неприкосновенность частной сферы как юридическая категория зародилось в США. В английском языке все ее стороны обозначаются единым термином «privacy», который не имеет буквального эквивалента в русском языке. В 1890 году американские юристы Сэмюэл Уоррен и Луис Брандейс изложили суть данного понятия. Они определили ее как «the right to be alone», что в прееводе означает – право быть забытым, право быть оставленным в покое или право быть предоставленным самому себе[2]. С. Уоррен и Л. Брандейс утверждали, что серьезную опасность для приватности представляет угроза со

[2] Саматов, К.М. Персональные данные как институт права/К.М. Саматов// В сборнике: Новые вопросы в современной науке Материалы Международной (заочной) научно-практической конференции. под общей редакцией А.И. Вострецова. – 2017. – С. 297.

стороны методов ведения бизнеса и новых изобретений. Данный тезис они изложили в своей статье «Право на приватность» [3].

Функционирование американских судов сыграло большую роль в формировании права на частную жизнь. Например, в 1965 году в деле Griswold vs Connecticut судья Верховного суда США Дуглас вывел право на неприкосновенность из первых пяти поправок к Конституции США. Он признал, что данные поправки «защищают различные аспекты неприкосновенности частной жизни». «Мы имеем дело с правом на неприкосновенность частной жизни, которое старше, чем Билль о правах» - произнес судья Верховного суда США Дуглас вынося решение суда[4].

Справедливость приведенных выводов особенно актуальна в условиях технической революции и научно-технического прогресса, которые особенно сильно проявляются в последние 20 лет. Изобретение новейших способов и средтв сбора, хранения и обработки данных, касающихся как личной жизни индивидов так и их публичной деятельности, послужило причиной возникновения новой категории нарушений в области прав на неприкосновенность частной жизни. Ранее они не были известны юридической науке.

Рожденная в США концепция о неприкосновенности оказала большое влияние на формирование сегодняшней системы прав и свобод человека. Несмотря на существующее великое множество международных соглашений, число универсальных международно-правовых принципов на самом деле относительно невелико. Сосредоточенные главным образом в трех универсальных документах – Всеобщей декларации прав человека (ст.12), Международном пакте о гражданских и политических правах 1966 года (ст.17), Конвенции о защите прав и основных свобод – они занимают главенствующее в иерархии норм международного права положение[5].

Всеобщая Декларация прав человека была утверждена Генеральной Ассамбеей ООН 10 декабря 1948 года. Статья 12 Декларации закрепила что, никто не может подвергаться неосновательному вмешательству в его частную жизнь. Также было закрплено право на неприкосновенность жилища, тайну переписки, честь и репутацию. Указанные права говорят о защите человека от различного рода вмешательств.

«Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции» [6]. В 1950 году Европейской конвенцией была закреплена данная норма в 8 статье о защите прав и свобод человека. Имменно данные акты

---

[3] Саматов, К.М. Персональные данные как институт права/К.М. Саматов// В сборнике: Новые вопросы в современной науке Материалы Международной (заочной) научно-практической конференции. под общей редакцией А.И. Вострецова. – 2017. – С. 297.

[4] Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 122.

[5] Сергиевич, В.А. Проблемы становления и развития института «право быть забытым»/ В.А. Сергиевич, И.В. Шугурова//Отечественная юриспруденция. – 2016. – № 12 (14). – С. 18..

[6] Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS № 108) (заключена в г. Страсбурге, 28 января 1981 г.). // «Бюллетень трудового и социального законодательства РФ», №4, 2014

поспособствовали признанию неотъемлемым правом каждого человека права на неприкосновенность частной жизни.

С точки зрения юридической техники между данными документами имеются некоторые разночтения. Так, в Декларации и в Пакте даны формулировки более общего плана: не допустимо вмешательство в личную и семейную жизнь. В Конвенции же представлены отдельные уточнения благодаря отраженной двуединой концепции права на неприкосновенность частной жизни – «либертарианской» от англ. «liberty – свобода» и «дигнитарианской» от американского английского «dignity – достоинство» [7].

Непреодолимых противоречий между ними нет, просматривающаяся граница разделения проходит лишь по субъектам потенциального вмешательства: первая нацелена в большей степени на защиту личного пространства человека от посягательств государства в лице его органов, а вторая – на охрану от вторжения физических и юридических лиц. И все-таки процесс развития этих принципов нельзя считать завершенным – на их основе формируется следующий, более конкретный и формально определенный пласт международного правопорядка.

Первоначально на проблему защиты рассматриваемой разновидности прав обратила ОЭСР, принявшая в 1980 году Директиву о защите неприкосновенности частной жизни и международных обменов персональными данными. В дальнейшем эти принципы были детализированы в Конвенции Совета Европы «Об охране личности в отношении автоматизированной обработки ПД». Целью Конвенции № 108 Совета Европы «О защите индивидуумов (частных лиц) при автоматизированной обработке персональных данных»[8] является правовая защита личности при автоматической обработке персональной информации. Статья 2 Конвенции содержит определение персональных данных: «персональные данные» означают любую информацию об определенном или поддающемся определению физическом лице («субъект данных») [9]. Это определение достаточно широко и дает возможность странам, ратифицировавшим Конвенцию, возможность для трактовки и трансформации его для применения в национальном законодательстве не только при автоматизированной обработке персональных данных[10].

В 2001 году был принят дополнительный протокол к 108 конвенции Совета Европы, который содержит требование ко всем государствам-членам СЕ о соблюдении адекватного уровня защиты настоящей категории законных интересов. С этой целью в Конвенции определен ряд положений.

---

[7] Сергиевич, В.А. Проблемы становления и развития института «право быть забытым»/ В.А. Сергиевич, И.В. Шугурова//Отечественная юриспруденция. – 2016. – № 12 (14). – С. 19.

[8] Конвенция Совета Европы № 108 от 28 января 1981 года «О защите индивидуумов (частных лиц) при автоматизированной обработке персональных данных» // Справочно-правовая система «КонсультантПлюс».

[9] Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS № 108) (заключена в г. Страсбурге, 28 января 1981 г.). // «Бюллетень трудового и социального законодательства РФ», №4, 2014

[10] Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 122-126.

1. Устанавлены требования, согласно которым основными принципами в отношении персональных данных являются: добросовестность и законность получения, определенность и законность целей сбора, точность, целевое использование персональных данных, обновляемость, определенности сроков хранения.

2. Определены те категории персональных данных, обработка которых возможна в случае, когда национальное право предусмотрело надлежащие гарантии в данной сфере. К таким персональным данным Конвенция относит сведения о национальной принадлежности, политических либо религиозных взглядах или иных убеждениях, данные о здоровье, судимости и т. д.

3. Для предотвращения случайного или несанкционированного уничтожения персональных данных, нелегального и несанкционированного доступа, распространения, уничтожения и т. д., Конвенция содержит требования о соблюдении надлежащих мер безопасности при их хранении.

4. В Конвенции предусмотрены различные гарантии для физических лиц по контролю над своими персональными данными [11].

Согласно Директиве 95/46/ЕС о защите прав частных лиц применительно к обработке персональных данных и свободном движении таких данных, которая была принята 24 октября 1995 года, под персональными данным понимается любая информация зафиксированная на любом носителе, которая так или иначе связана с субъектом персональных, позволяет его индентифицировать. В данную категорию попадают такие категории данных, как имена, почтовые и электронные адреса физических лиц[12].

В Директиве 95/46/ЕС установлены ключевые принципы защиты информации, которые ложаться в основу деятельности «контролеров данных». Контролеры данных – это лица или организации, которые определяют цели и способы обработки персональных данных.

Всего в Директиве установлено восемь ключевых принципов. Главный принцип заключается в справедливости обработки персональных данных. Суть указанного принципа заключается в том, что субъект персональных данных имеет право получать информацию о том, кто является контролером данных, для каких целей производится обработка и использование персональных данных, а также он должен предоставить согласие на использование персональных данных. Данные права он реализует до того, как предоставит контролеру персональные данные. В связи с чем предварительное уведомление может включать в себя любую информацию, необходимую в конкретных условиях, чтобы сбор и обработка персональных данных были бы справедливы.

Кроме того, в число основных принципов входят такие как:

четкость и законность целей для сбора и обработки персональных данных;

---

[11] Конвенция Совета Европы № 108 от 28 января 1981 года «О защите индивидуумов (частных лиц) при автоматизированной обработке персональных данных» // Справочно-правовая система «КонсультантПлюс».

[12] Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 122-126.

обязательное соответствие объема запрашиваемых персональных данных тем целям, в котрых предполагается их использование;

установлен срок хранения персональных данных – он не должен превышать срок, который необходим для обработки данных в соответствии с указанными целями;

принцип доступности к персональным данным субъекта этих данных для их дальнейшего изменения, уточнения или удаления;

принцип создания необходимых технических и организационных мер для обеспечения защиты данных от незаконной или несанкционированной обработки, случайной утраты или разрушения[13].

В 2012 году право на неприкосновенность частной сферы получило свое настоящее название, когда Европейская комиссия подготовила проект Регламента «О защите персональных данных», который вносил изменения в Директиву 1995 года и адаптировал ее к применению. Сущностью одного из таких изменений стало детальное описание процедуры исполнения «права быть забытым», которое нашло свое отражение в судебной практике, несмотря на то, что сам Регламент в силу не вступил. Реформа «О защите персональных данных» должна была устранить излишние административные процедуры и снизить затраты на ведение документации благодаря принятию единого документа, который даст возможность вести бизнес на едином внутреннем рынке ЕС[14].

Впервые данный институт нашел свое применение в решении Суда Европейского Союза от 13.05.2014. по делу Гонсалеса о требовании к поисковой системе Google привести в соответствие с современным положением дел предоставлнную несколько лет назад газетой информацию о гражданине. Поскольку устаревшая информация не соответствовала действительности и приносила ущерб деловой репутации гражданина. Суд в своем решении обязал поискового оператора Google удалить выдачу в результате поиска информацию относительно Гонсалеса, несоответствующую действительности, однако на информацию, размещенную на сайте газеты это требование не распространялось.

Таким образом, Суд постановил, что поисковые операторы должны по запросу удалять с серверов устаревшие, не соответствующие действительности или утратившие актуальность личные данные. Данное решение вызвало серьезные споры между пользователями сети Интернет и субъектами, непосредственно обеспечивающими ее деятельность. Так исполнительный директор Google Ларри Пейдж высказал опасения, что данное решение может стать оружием в недобросовестной конкуренции и в дальнейших перспективах снизит темпы развития инноваций[15].

[13] Алямкин, С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты/ С.Н. Алямкин // Мир науки и образования. – 2016. – № 4 (8). – С. 4.

[14] Алямкин, С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты/ С.Н. Алямкин // Мир науки и образования. – 2016. – № 4 (8). – С. 4.

[15] Алямкин, С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты/ С.Н. Алямкин // Мир науки и образования. – 2016. – № 4 (8). – С. 4.

Последствием вступления судебного решения по делу Гонсалеса в силу стало ежедневное поступление более чем 10 тысяч запросов только в поисковую систему Google. Данный прецедент дал возможность защитить схожие правоотношения, например The New York Times жаловалась на то, что поиск Google сохраняет в кэш-памяти их содержание. По мнению владельцев газеты, это нарушает авторские права.

Окружной суд США штата Невада постановил, что кэши компании Google не нарушают авторских прав, однако европейский судебный прецедент может изменить взгляд юридического сообщества на эту проблему. Все спорные случаи будут передаваться в государственные органы, занимающиеся защитой информации.

Итак, вышеперечисленные этапы являются основными в становлении нормативной системы защиты персональных данных в Европе. Становление Евросоюза и принятие национальных законов стран-участниц ЕС явилось завершающей ступенью его формирования. Институт направлен на регулирование вопросов защиты персональных данных.

В России в дореволюционный период лишь частично на уровне законодательства были утверждены и закреплены элементы права на неприкосновенность. Тайна корреспонденции была закреплена в Телеграфном уставе в 1876г. и Почтовом уставе в 1857г. На основе Уложения о наказаниях уголовных и исправительных 1845г., Уголовного Уложения 1903 г. происходило уголовно-правовая защита тайны корреспонденции. В частности, в ст.ст. 162–170 Уголовного Уложения 1903 г. устанавливался запрет на вмешательство должностных лиц при осуществлении ими правосудия в личную и семейную жизнь человека.

Подход к проблеме прав человека после революции в 1917 года существенно изменился. Ранее действующая Конституция РСФСР 1918 года в свой состав включала раздел, носящий название «Декларация прав трудящегося и эксплуатируемого народа». Эта декларация номинативно была посвящена правам человека, однако, но в ней не были закреплены даже элементарные права: личные, политические, экономические, культурные. Данный аспект являлся существенным недостатком вышеназванной декларации. В состав «Декларация прав трудящегося и эксплуатируемого народа» вошли только право уравнивающее землепользование, эмбарго на эксплуатацию, право трудящихся в хозяйствовании, освобождение трудящегося народа из-под ига капитала.

Вновь принятая в 1924 году Конституция СССР не содержала Декларации прав. В данной Конституции было установлено право на единое союзное гражданство, национальную свободу и равенство. Указанный перечень исчерпывал права человека. При этом, отдельная глава Конституции посвящалась подразделению, которое нарушало все человеческие права: организации по борьбе с политическими и экономическими контрреволюционерами, шпионами и бандитизмом Объединенного государственного политического управления. Данное подразделение в указанный период времени занималось репрессиями.

О правах и обязанностях граждан в СССР начали говорить впервые в преддверии массовых репрессий 1937–1938гг. С этого момента появляется отдельная глава в Конституции СССР, закрепляющая достаточный перечень личных прав и свобод граждан. Глава была введена 5 декабря 1936 года. К включенным в нее правам были отнесены свобода совести (ст. 124), неприкосновенность личности (ст. 127), неприкосновенность жилища и тайна корреспонденции (ст. 128);

Стоит отметить, что в практическом смысле включение указанных прав было лишь формальным, однако, теоретически этот факт можно считать значительным достижением советского права.

22 ноября 1991 была принята Декларация прав и свобод человека и гражданина непосредственно Верховным Советом РСФСР. Именно данный документ содержит первое упоминание права на неприкосновенность частной жизни в качестве самостоятельного права. Декларация прав и свобод человека включала запрет на сбор и использование, хранение и распространение информации о частной жизни человека без его согласия. Указанная норма права нашла последующее отражение в принятой всенародным голосованием Конституции 1993 года.

20 февраля 1995 года был принят Федеральный закон «Об информации, информатизации и защите информации» № 24–ФЗ. В нем понятие о персональных данных утверждалось на законодательном уровне. К персональным данным, согласно закону, относятся сведения о фактах, событиях и обстоятельствах жизни гражданина, которые позволяют отождествлять так или иначе его личность. Данное понятие закреплено в 2 статье. Рассматриваемый закон также утверждал общие принципы, которыми следует руководствоваться при сборе и использовании информации о гражданах. В свою очередь, ФЗ № 24 закрепил конфиденциальный характер персональных данных.

Еще до принятия Директивы Европейского Парламента и Совета Европы 95/46/ЕС 24 октября 1995 г. «О защите личности в отношениях обработки персональных данных и свободном обращении этих данных» началось составление специального закона о защите личной информации. Законопроект находился в разработке в Комитете по информационной политике и связи Государственной Думы РФ с 1998 года. К участию была привлечена рабочая группа специалистов в сфере информационного законодательства. Первоначально законопроект носил название «Об информации персонального характера». Но указанная инициатива в Госдуме так и не была рассмотрена[16].

Аналогичная группа экспертов была сформирована спустя два года в Совете Безопасности РФ. Она занималась подготовкой законопроекта, принятого впоследствии в качестве Федерального закона «О персональных данных» от 27.07.2006 г. № 152–ФЗ.

[16] Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 123.

Вступление в мае 2013 года в законную силу Федерального закона от 07.05.2013 № 99–ФЗ обусловило обновление трудового законодательства. Согласно данному закону был внесен ряд изменений в 86 и 90 ТК РФ, а также утратила силу ст. 85 ТК РФ. Основной причиной приятия данного закона послужило исполнение Российской Федерацией ряда обязательств, очерченных в рамках Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Указанная Конвенция содержит требования о том, что «каждая Сторона принимает необходимые меры в рамках своего национального законодательства с целью ввести в действие основополагающие принципы защиты данных не позднее момента вступления Конвенции в отношении нее в силу»[17].

В ст. 85 Трудового кодекса было описано понятие персональных данных работника. Под ними понималась информация, нужная работодателю в связи с трудовыми отношениями, которая касалась конкретного работника. Данная статья из ТК РФ была исключена. Теперь работодатели для понимания содержания персональных данных полностью должны руководствоваться определением, котрое содержит закон «О персональных данных». Согласно указанному закону, понятие «персональные данные» включает любую информацию, которая прямо или косвенно относится определенному или определяемому физическому лицу, т.е. субъекту персональных данных.

Усиление охраны и защиты персональных данных ограниченного доступа также предусмотрено в изменениях. К ним отнесены:

– сведения о политических, религиозных и других убеждениях работника;
– сведения о профсоюзной деятельности работника;
– сведения о его членстве в общественных объединениях.

Без согласия субъекта персональные данные не могут обрабатываться.

Таким образом, по результатам данной части исследования можно сказать, что Зарубежный опыт и история становления института персональных данных в значительной степени сказались на тенденциях и особенностях развития данного института в России. Наша страна в полной мере восприняла международные тенденции. Был учтен зарубежный накопленный правовой опыт. Кроме того, значительное внимание было уделено общественным реалиям российской жизни, произошедшим политическим преобразованиям, а также общим актуальным направлениям развития права. Особенно стоит отметить, что в России с учетом национальных условий реализации правовых норм были использованы возможности изменения и преобразования ключевого акта международного уровня анализируемой сферы – 108 Конвенции Совета Европы о защите прав физических лиц в отношении персональных данных 1981 года. Данный факт подтверждает готовность государства и в дальнейшем развивать институт персональных данных и обеспечивать его эффективное функционирование.

[17] Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 122.

1.2 Понятие, правовая природа и виды персональных данных

В теории права персональные данные определяются как «информация зафиксированная на любом материальном носителе о конкретном человеке, которая отождествлена или может быть отождествлена с ним». Российское законодательство также закрепило максимально широкое понимание термина «персональные данные». В Федеральном законе № 152–ФЗ «персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[18]. Предыдущая редакция Закона содержала конкретный и в то же время открытый перечень персональных данных. К ним были отнесены сведения о фамилии, имени, отчествв, дате и месте рождения, адресе, семейном и социальном положении, имущественном положении, образовании, профессии, доходах, другая информация.

В настоящее время институт «персональных данных» в России регулируется рядом нормативных актов. При этом, практически во всех законах присутствуют нормы о правах граждан – субъектов персональных данных, хотя и с различной степенью разработанности. Во многих актах закреплены нормы об ответственности за нарушения в работе с персональными данными.

В первую очередь, неприкосновенность частной жизни гарантируется Конституцией Российской Федерации, а персональные данные являются важнейшей составляющей частной жизни. Статья 23 Конституции гарантирует каждому «право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» [19]. В Статье 24 Конституции установлен запрет на «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия» [20].

Также для развития нормы о неприкосновенности частной жизни и в связи с ратификацией Российской Федерацией ряда международных актов, в Трудовой Кодекс была включена глава 14 «Защита персональных данных». В ней определяются общие положения защиты персональных данных работника: понятие, требования, особенности хранения, передачи, права работников и ответственность за нарушение норм[21].

Кроме того, в качестве нормативно-правового источника защиты персональных данных, следует выделить ФЗ №149 «Об информации,

---

[18] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 29.07.2017) // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451. 94

[19] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // «Собрание законодательства РФ», 04.08.2014, №31, ст. 4398

[20] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 21.07.2014 № 11-ФКЗ). // «Собрание законодательства РФ», 04.08.2014, №31, ст. 4398

[21] Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (ред. от 05.02.2018). // «Собрание законодательства РФ», 07.01.2002, №1 (ч. 1), ст. 3. 93

информационных технологиях и защите информации». Необходимо отметить, что действующее трудовое законодательство нацелено на обеспечение безопасности персональных данных, как в частном секторе, так и на государственной службе.

Помимо Конституции РФ, основным законом, регулирующим обработку персональных данных различными субъектами, является Федеральный закон «О персональных данных» от 27.07.2006 года № 152–ФЗ (далее – закон 152–ФЗ). Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к персональным данным в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных.

Не попадают под сферу регулирования закона 152–ФЗ следующие действия:

– обработка чужих персональных данных физическими лицами для собственных нужд (личных и семейных), при условии, что такая обработка не нарушает права владельца персональных данных;

– действия по организации архивов, которые попадают в сферу регуляции законодательства об архивном деле в РФ;

– обработка персональных данных, которые содержат сведения, отнесенные в соответствии с действующим законодательством РФ, к государственной тайне;

– персональные данные, относящиеся к деятельности судов, предоставленные в порядке, закрепленном соответствующими законодательными актами[22].

Федеральный закон № 152–ФЗ «О персональных данных» описывает организационно-правовые механизмы защиты персональной информации любого физического лица. Однако в отношении данных закон не указывает, распространяются ли его нормы на персональные данные работников.

Отметим, что в отличие от работников частного сектора, в отношении защиты персональных данных государственных гражданских служащих действуют дополнительные нормативные акты. Так, п. 4. ст. 42 № 79–ФЗ «О государственной гражданской службе Российской Федерации» устанавливает условия получения и обработки персональных данных, доступа субъекта к данным, а также их передача третьим лицам. При этом при работе с персональными данными с использованием средств автоматизации и технических средств необходимо руководствоваться Постановлением от 17.11.2007 г. № 781.

Таким образом, вышеуказанные правовые нормы регулируют общественные отношения, связанные с обработкой персональных данных и их защитой. Можно говорить, что данные нормы имеют отличительные черты, присущие самостоятельному правовому институту.

«Система права – совокупность правовых форм, внутренне упорядоченная по отношениям, обеспечивающим относительную самостоятельность и единство

[22] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 29.07.2017). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451. 94

этой совокупности, которое выражается в ее интегральных, обеспечительных и координационных свойствах и функциях» [23]. Указанное определение охватывает существенные признаки, как системы права, так и ее подсистем: отраслей, подотраслей, институтов.

Теория права не имеет единого подхода к тому, какие критерии лежат в основе выделения составляющих элементов системы права. Ряд авторов допускают выделение главных оснований, среди которых предмет и метод регулирования, а также дополнительные критерии, которые включают функции и отраслевые принципы. Данный подход объективно учитывает воздействие общественных отношений на систему права. Исходя из того, что право выстает средством регулирования общества и социума, оно не может быть отделено от указанных отношений.

Право как система включает различные подсистемы, или структурные элементы, в том числе отрасль, подотрасль, институт, субинститут и норма права. С.С. Алексеев в качестве основных признаков института права указывает:

1) «самостоятельность регулятивного воздействия на определенные общественные отношения;

2) юридическую однородность норм, выраженную в специфической группе понятий, общих положений, терминов;

3) своеобразие юридической конструкции, которое выражается в следующем: наличие комплекса «равноправных» нормативных предписаний, юридическая разнородность предписаний, наличие устойчивых закономерных связей, создающих из отдельных предписаний специфическую юридическую конструкцию» [24].

По мнению Е.А. Киримовой, признаки правового института как структурного элемента системы права составляют:

– специфичный способ правового регулирования;
– относительная самостоятельность;
– наличие или принципиальная возможность формирования общих понятий в рамках видовых явлений [25].

Используя в качестве основы теорию права, можно проанализировать институт персональных данных. Предметом института персональных данных являются общественные отношения, связанные с их обработкой. Данная обработка может производиться муниципальными и государственными органами, юридическими и физическими лицами. В процессе обработки могут применяться средства автоматизации, включая информационно-телекоммуникационные сети и вычислетельную технику. Также обработка может производиться без различных средств автоматизации. Однако обязательным является защита от неправомерного

[23] Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 122-126.

[24] Алексеев, С.С. Государство и право: учебное пособие/ С.С. Алексеев. – М.: Проспект, 2015. – С.53.

[25] Керимова, Е.А. Правовой институт: автореф. дис. … канд. юрид. наук./ Е.А. Керимова. – Саратов, 1998. – С.33.

доступа к персональным данным, уничтожения или их блокирования, что подразумевает конфиденциальность, целостность и доступность информации.

Институт персональных данных оперирует достаточно широким набором понятий. Например, в статье 3 Федерального закона «О персональных данных» раскрыто содержание ключевых определений, в число которых входит само понятие персональных данных, понятие оператора, понятие обработки персональных данных, содержание понятий «автоматизированная обработка персональных данных», «обезличивание персональных данных», «информационная система персональных данных», «трансграничная передача персональных данных» и многие другие.

Помимо этого, институт персональных данных и всю связанную с ним сферу в настоящее время можно считать относительно обособленной. Она располагает широким спектром источников, которые включают различные нормы материального права на уровне федеральных законов и нормы процессуального права на уровне подзаконных нормативных актов. Они описывают все процедуры, которые входят в состав обязательных при обработке персональных данных оператором с целью защиты обрабатываемой информации.

В статье 5 закона «О персональных данных» устанавливлены шесть ключевых принципов, лежащих в основе обработки персональных данных. К числу таковых относятся.

1. Добросовестность обработки персональных данных, законность способов и целей их обработки.

2. Цели обработки персональных данных должны соответствовать тем целям, которые были заранее определены и заявлены при их сборе. Также полномочия оператора должны соответстветствовать всем заявленным параметрам.

3. Объем персональных данных, способ обработки и характер обрабатываемых персональных данных должен соответствовать целям обработки.

4. Недопустимой является обработка данных, которые являются избыточными по отношению к заявленным при сборе данных целям. Достоверность и достаточность персональных данных для целей обработки являются обязательным требованием.

5. Объединение информационных баз персональных данных, которые были созданы для несовместимых между собой целей, является недопустимым.

6. Форма хранения персональных данных должна позволять определять субъекта этих данных. Кроме того, срок хранения данных не должен превышать сроки, определенные целями их обработки. Персональные данные должны быть уничтожены после того, как будут достигнуты цели их обработки, а также при отсутствии необходимости в их достижении [26]. ЭТО

Все вышеперичесленные принципы обработки персональных данных должны применяться во всех видах правоотношений. В их состав могут быть включены и

[26] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 29.07.2017) // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451. 94

гражданские, и трудовые, и процессульные павоотношения. Также принципы применяются независимо от оператора, осуществляющего обработку.

Стоит отметить, что институт защиты персональных данных ипользует по большей части императивный метод регулирования. Данный вывод базируется на анализе перечисленных в ст.5 ФЗ–152 принципов и условий, а также на основе анализа подзаконных и иных НПА, которые были изданы в соответствии с указанным законом.

Таким образом, рассморев весь объем правовых норм, которые регулируют общественные отношения в области обработки и защиты персональных данных, можно утверждать, что она имеет все признаки, которые характеризуют ее как самостоятельный правовой институт, обладающий отличительными чертами.

Обращение к классификации позволит определить место указанного института в системе права России. Право делится на частное и публичное, материальное и процессуальное. Институт персональных данных можно отнести к публичной отрасли права, что подтверждает анализ, проведенный выше. При этом, ряд норм указанного института можно найти в трудовом праве, которое традиционно относится к частной отрасли [27].

Исходя из вышесказанного, институт защиты персональных данных связан с регулированием общественных отношений, относящиеся к нескольким отраслям права, т.е. находящиеся на стыке отраслей, поэтому, институт персональных данных следует рассматривать в качестве самостоятельного межотраслевого института права.

Выводы по разделу 1

Таким образом, по итогам теоретической части исследования можно сделать ряд выводов. Для российской действительности институт персональных данных является относительно новым. Он пришел из института тайны частной жизни, являясь адаптацией так называемого права быть оставленным в покое.

Зарубежный опыт и история становления института персональных данных в значительной степени сказались на тенденциях и особенностях развития данного института в России. Наша страна в полной мере восприняла международные тенденции. Был учтен зарубежный накопленный правовой опыт. Кроме того, значительное внимание было уделено общественным реалиям российской жизни, произошедшим политическим преобразованиям, а также общим актуальным направлениям развития права. Особенно стоит отметить, что в России с учетом национальных условий реализации правовых норм были использованы возможности изменения и преобразования ключевого акта международного уровня анализируемой сферы – 108 Конвенции Совета Европы о защите прав физических лиц в отношении персональных данных 1981 года. Данный факт подтверждает готовность государства обеспечивать эффективное

[27] Сергиевич, В.А. Проблемы становления и развития института «право быть забытым»/ В.А. Сергиевич, И.В. Шугурова//Отечественная юриспруденция. – 2016. – № 12 (14). – С. 18-20.

функционирование института персональных данных, а также способствовать его развитию.

Персональные данные представляют собой информацию, зафиксированную на любом материальном носителе о конкретном человеке, которая отождествлена или может быть отождествлена с ним. Нормативно-правовая база защиты персональных данных включает международное законодательство, Конституцию Российской Федерации, Федеральные законы, в том числе Федеральный закон от № 152–ФЗ «О персональных данных», Федеральный закон № 149–ФЗ «Об информации, информационных технологиях и о защите информации», различные подзаконные акты.

Институт персональных данных регулирует общественные отношения, которые относятся к нескольким отраслям права. С одной стороны, институт персональных данных можно отнести к публичной отрасли права, с другой стороны – ряд норм указанного института можно найти в трудовом праве, которое традиционно относится к частной отрасли. Следовательно, институт персональных данных регулирует отношения, находящиеся на стыке отраслей, поэтому его следует рассматривать как межотраслевой.

2 ПРАВОВОЙ СТАТУС СУБЪЕКТОВ, УЧАСТВУЮЩИХ В ОБОРОТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Общая характеристика правового понятия «субъект персональных данных»

Ключевой целью ФЗ РФ № 152–ФЗ «О персональных данных» является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных. Данная цель также включает защиту прав на неприкосновенность частной жизни, личную и семейную тайны. Обращаясь к ст.3 ФЗ РФ № 152–ФЗ «О персональных данных» можно сформулировать определение персональных данных. «Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация» – персональные данные.

Действующее законодательство выделяет несколько видов персональных данных, в числе которых общедоступные, обезличенные, специальные и другие.

Общедоступные персональные данные – это данные, доступ к которым производиться с согласия субъекта персональных данных. На эту категорию персональных данных не распространяется принцип конфиденциальности. Доступ к ним предоставляется неограниченному кругу лиц. Если рассматривать более подробно принцип конфиденциальности, то в данном аспекте он включает в себя тайну фамилии, имени, отчества, год и место рождения, адрес, абонентский номер, сведения о профессии и иные. Источники информации – адресные книги, справочники, и т.п. Общедоступные персональные данные могут быть исключены из общедоступных источников в любое время, но по требованию субъекта персональных данных. Требование может быть со стороны уполномоченных государственных органов либо утверждено решением суда.

К категории специальных персональных данных относятся данные, которые касаются национальной либо расовой принадлежности, философских убеждений, религиозных убеждений, политических взглядов, состояния здоровья, интимной жизни. Обработка специальных персональных данных допускается только в следующих случаях:

– имеется согласие субъекта персональных данных на обработку этих данных;
– допускается обработка общедоступных персональных данных;
– допускается обработка данных, относящихся к состоянию здоровья субъекта, когда получение его согласия на обработку не представляется возможным;
– допускается обработка данных, относящихся к состоянию здоровья субъекта, когда она производится лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– обработка специальных персональных данных допускается в случаях, когда это необходимо в соответствии с требованиями законодательства Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия [28].

Вся информация, которая составляет персональные данные, по своей сути является неоднородной. Ее можно подразделить на номинативную и иную. Номинативной является информация, позволяющая идентифицировать конкретное лицо (фамилия, имя, отчество, пол, серия и номер паспорта, дата и место рождения и т. п.). Неноминативная информация может включать сведения о доходах и месте работы, политических убеждениях и медицинских заболеваниях, наличии судимости и т. п.[29].

Особое место среди номинативных персональных данных занимают биометрические персональные данные, т.е. сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность. Специфика биометрических персональных данных связана с тем, что большинство их разновидностей трудно поддаются изменению. Так, например, обычному человеку будет проблематично изменить свой основные характеристики отпечатков пальцев, либо сетчатки глаза, не говоря уже о ДНК. Указанные особенности человека, ввиду их стабильности, представляют определенную ценность для государства, например, биометрические персональные данные могут использоваться государственными органами в целях выявления и предотвращения преступлений, идентификации человека[30].

В зависти от необходимости обработки персональных данных в соответствии с требованиями законодательства предлагается следующая классификация. Она включает три группы данных.

1. Первая группа включает персональные данные, которые обрабатываются с момента государственной регистрации рождения как юридического факта. К ним относятся такие данные, как имя, дата и место рождения.

2. Вторая группа включает совокупность персональных данных, обработка которых производится начиная с момента внесения записи в соответствующие документы. Совокупность сведений этой группы включает соответствующие персональные данные о профессии, образовании, семейном положении, доходах и другие.

3. Третья группа включает персональные данные, обработка которых производится в силу прямого указания закона, дополнительное оформление их не

[28] Параскевов, А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом/ А.В. Параскевов // Научный журнал КубГАУ. – 2015. – №110(06). – С. 2.

[29] Саматов, К.М. Персональные данные как институт права/К.М. Саматов// В сборнике: Новые вопросы в современной науке Материалы Международной (заочной) научно-практической конференции. под общей редакцией А.И. Вострецова. – 2017. – С. 296.

[30] Кривогин, М.С. Правовой режим биометрических персональных данных/М.С. Кривогин// Проблемы современной науки. – 2015. – №10 (40) – С. 126-129.

требуется. К числу таких персональных данных относятся сведения о социальном и имущественном положении, расовой и национальной принадлежности, данные о политических взглядах, религиозных или философских убеждениях, данные об интимной жизни, некоторые биометрические данные [31].

Двумя основными участниками правоотношений, которые складываются в рамках оборота персональных данных, являются субъект персональных данных (физическое лицо) и оператор, осуществляющий обработку персональных данных. Рассмотрим подробнее характеристику каждого участника.

В основе правореализационных процессов лежит наличие в структуре правоотношения субъекта персональных данных. Это придает норме права регулирующий статус общественных отношений. Одной из основных категорий, как информационного права, так и теории права является субъект права. Можно сформулировать общее понятие субъекта права – физическое или иное лицо, наделенное законом обязанностями и правами, способное сознательными действиями и решениями осуществлять права, принадлежащие ему и исполнять обязанности[32]. Субъект права должен обладать таким качеством, как правосубъектность, благодаря которому он может выступать участником правоотношений по своему усмотрению или в силу закона.

Многие авторы в юридической литературе разграничивают категории «субъекта правоотношений» и «субъекта права». Данные категории не являются идентичными, например субъектом права является потенциальный участник, находящийся в статическом, «неподвижном» состоянии до вступления в правоотношение[33]. Субъект права, который реализуется с помощью правосубъектности, является субъектом правоотношений и находится в динамике.

С точки зрения науки, различие понятийного аппарата субъекта права и субъекта правоотношений происходит глубоко и всесторонне, исследуются особенности явлений правовой природы. С практической точки зрения разграничение понятий происходит при исследовании эффективности правового регулирования общественных отношений и реализации своих возможностей субъектами права[34].

Изучая правоотношения в рамках оборота персональных данных, можно сделать вывод, что любое физическое лицо, не зависимо от каких-либо критериев с наличием информации, является субъектом права. Правоотношения в сфере персональных данных являются личными абсолютными правами человека. Реализация личных абсолютных прав человека происходит в рамках конкретного правоотношения с помощью конкретного субъекта.

---

[31] Кучеренко, А.В. Понятие и признаки оператора, осуществляющего обработку персональных данных /А.В. Кучеренко // Альманах современной науки и образования. Тамбов: Грамота. – 2009. – №12 (31). – Ч.2. – С. 59.

[32] Кучеренко, А.В. Понятие и признаки оператора, осуществляющего обработку персональных данных /А.В. Кучеренко // Альманах современной науки и образования. Тамбов: Грамота. – 2009. – №12 (31). – Ч.2. – С. 59.

[33] Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 122.

[34] Вышеславова, Т.Ф. Дифференциация персональных данных работников // НаукаПарк. – 2015. – № 9 (39). – С.133.

Проблематика заключается в том, что ФЗ «О персональных данных» не содержит конкретного, обобщенного, официально закрепленного понятия субъекта персональных данных. Действующий Закон не разграничивает участников правоотношений, не выделяет четких критериев. Закон не регламентирует наличие у субъектов персональных данных таких критериев как, например, возраст, гражданство, объем дееспособности и правоспособности. Проблема закрепления понятийного аппарата в действующем законе препятствует решению многих важных вопросов.

Главным обстоятельством допуска участника к участию в качестве субъекта является возраст. Возрастной признак разграничивает деликтоспособность, дееспособность и способность лица иметь специальные права. Стоит отметить, что законодатель не сделал ссылку в Законе на наличие ограничения по возрасту. Законом установлены границы возраста, при наступлении которых участник правоотношений имеет право на реализацию принадлежащих ему прав. Открытым остается вопрос о наличии у субъекта совокупности персональных данных.

Можно сформулировать ряд вопросов, на которые достаточно сложно дать ответ.

1. В какой момент возникают права на защиту персональных данных?

2. Момент возникновения права на защиту персональных данных совпадает с моментом возникновения дееспособности гражданина?

3. Имеет ли возможность несовершеннолетний гражданин реализовывать право на защиту персональных данных в полной мере?

Сравним право на защиту отдельных видов персональных данных, которые содержаться в ФЗ «О персональных данных» и ряде других законов. Ст.19 Гражданского Кодекса РФ и ст.ст. 58, 59 Семейного Кодекса РФ предусмотрено, что гражданин имеет право на имя, отчество и фамилию. Гражданский Кодекс РФ указывает на такое обстоятельство, что объектом охраны является имя, полученное человеком при рождении. Имя получает функцию охраны только после государственной регистрации рождения гражданина, заявление о котором делается не позднее одного месяца после рождения.

В соответствии с ФЗ «Об актах гражданского состояния» в случае, если ребенок был подкинут или найден, имя должно быть присвоено не позднее семи дней со дня обнаружения ребенка. Действующее законодательство предусматривает присвоение ребенку имени в момент составления акта о его рождении. На наш взгляд, реализация права на защиту имени не связана с моментом его возникновения. Гражданский Кодекс лишь делает ссылку на то, что имя гражданина, как и иные виды нематериальных благ, неотчуждаемо и непередаваемо иным способом.

Субъект персональных данных наделен рядом прав, а именно на получение информации, которая касается обработки его персональных данных, например:

– цели обработки персональных данных;
– правовые основания обработки персональных данных;

– подтверждение факта обработки персональных данных оператором;
– цели, применяемые оператором в ходе обработки персональных данных;
– способы обработки персональных данных;
– наименование и место нахождения оператора;
– сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона.
– данные, находящиеся в обработке, относящиеся к соответствующему субъекту персональных данных, источник получения персональных данных;
– сроки хранения и сроки обработки персональных данных;
– порядок осуществления субъектом прав, предусмотренных законом.
– информацию об осуществленной трансграничной передаче данных;
– наименование, имя, фамилию, отчество лица, осуществляющего обработку персональных данных.

В соответствии с федеральными законами предусмотрено ограничение права субъекта персональных данных на доступ к его данным, в том числе если:
– содержатся персональные данные, полученные в ходе оперативно-розыскной деятельности, осуществляемой в целях обороны страны, безопасности государства и охраны правопорядка;
– обработка персональных данных производиться органами, которые осуществили задержание подозреваемого субъекта;
– доступ персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

Таким образом, на основе проведенного анализа характеристики правового понятия «субъект персональных данных», можно сделать вывод, что любое физическое лицо, не зависимо от каких-либо критериев—наличия информации, является субъектом права.. Проблематика заключается в том, что ФЗ «О персональных данных» не содержит конкретного, обобщенного, официально закрепленного понятия субъекта персональных данных. Действующий Закон не разграничивает участников правоотношений, не выделяет четких критериев.

Среди субъектов персональных данных особое место занимает оператор, организующий и (или) осуществляющий обработку персональных данных. Согласно Федеральному закону «О персональных данных» «Оператор персональных данных – государственный или муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных» [35].

При этом «обработкой» персональных данных считаются «действия (операции) с персональными данными, включая их сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,

[35] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 29.07.2017). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451. 94

распространение (в том числе передачу), обезличивание, блокирование и уничтожение» [36].

Любое лицо (физическое, юридическое) после получения доступа к персональным данным, даже не производящее обработку этих данных, а только осуществляющее организацию данного процесса, является оператором. Данное утерждение следует из определения оператора, установленного ФЗ «О персональных данных». При этом, именно оператор отвечает за законность и качество обработки персональных данных третьих лиц[37].

Стоит отметить, что любая организация в ходе своей деятельности обрабатывает информацию персонального характера:

– органы власти – о лицах, выступающих участниками регулируемых отношений, заявителях и т. п.;

– юридические лица – о клиентах, сотрудниках, потенциальных партнерах, контрагентах и т. д.

Соответственно, субъектами, несущими ответственность за соблюдение режима персональных данных, являются все юридические лица, а также органы власти.

Виды персональной информации, обрабатываемой физическими лицами, являются более разнообразными. С течением времени значительная совокупность персональных данных других физических лиц накапливается у любого гражданина. Не всегда данная информация попадает под дейтсвие ФЗ «О персональных данных». Примером могут служить те случаи, когда обработка персональных данных физическим лицом производится для семейных или личных нужд (п. 1 ч. 2 ст.1).В данном случае стоит отметить, что законодатель не раскрывает содержание понятия «личные и семейные нужды». Можно предположить, что введение в текст закона данных терминов подразумевает использование персональных данных иных лиц не для извлечения прибыли. Однако такое использование может приводить к получению выгод иного характера. К числу иных выгод могут быть онесены стремление вырасти по карьерной лестнице и занять новую должность, укрепление авторитета и улучшение деловой репутации.

Интересным является опыт зарубежных стран в определени оператора, осуществляющего обработку персональных данных. Например, согласно Закону Японии «О защите персональной информации» (2003 г.), оператором может выступать организация с численностью персональных данных не менее пяти тысяч сотрудников. Эти данные в обязательном порядке используются для осуществления предпринимательской деятельности. Не имеют право создавать базы данных орагнизации, которые обладают меньшим числом данных сотрудников. Исходя из вышесказанного, можно утверждать, что законы Японии

[36] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 29.07.2017). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451. 94

[37] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 29.07.2017) // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451. 94

не распространяется на правительственные учреждения и местные органы управления, независимые местные и административные корпорации.

Согласно Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», субъект, который определяет цель и средства обработки персональных данных, является «контролером». Данная Директива вводит дополнительно такой субъект анализируемых правоотношений, как «обработчик». Им является непосредственно обрабатывающее персональные данные физическое или юридическое лицо, официальный орган, агентство или иной орган. Обработчик осуществляет и реализует указанные действия по поручению контролера.

Введение дополнительного субъекта можно назвать оправданным, поскольку операторы зачастую не имеют административных, технических и/или материальных ресурсов, которых было бы достаточно для самостоятельного осуществления или организации обработки персональных данных. Что касается России, возможность осуществлять обработку персональных данных не самим оператором, а третьим лицом на основании договора в законодательстве предусмотрена в ч. 4 ст. 6 ФЗ «О персональных данных». В данном случае, третье лицо по сути, выполняет функции «обработчика».

Понятие «оператор информационной системы» практически идентично понятию «оператору, осуществляющему автоматизированную обработку персональных данных». Данное понятие фигурирует в Федеральном законе «Об информации, информационных технологиях и о защите информации» [38]. Юридическое лицо или гражданин, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных – является оператором информационной системы.

Обязанности оператора информационной системы:

– своевременное обнаружение на фактов несанкционированного что доступа к тот информации;

– предотвращение это несанкционированного доступа как к информации по и (или) но передачи ее они лицам, не ты имеющим права из на доступ мы к информации; за

– постоянный контроль вы за обеспечением так уровня защищенности же информации и от пр.

– предупреждение еще возможности неблагоприятных бы последствий нарушения уже порядка доступа для к информации.

Законодатель не устанавливает четких целей осуществления и (или) организации оператором обработки персональных данных. Операторы самостоятельно устанавливают их. Кроме того, цели могут быть конкретизированы в различных профильных нормативно-правовых актах.

[38] Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 23.04.2018). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3448.

Следует заметить, что ключевым условием развития указанных правоотношений является четкое заблаговременное определение цели сбора персональных данных. При этом запрет на использование собранной информации в целях, которые не соответствуют первоначально заявленным, также обязательно[39].

Целями обработки персональных данных могут быть:

– статистические или иные научные цели (при условии обязательного обезличивания персональных данных);

– исполнение договора, одной из сторон которого является субъект персональных данных;

– защита жизни, здоровья или иных жизненно важных интересов субъекта персональных данных;

– доставка почтовых отправлений организациями почтовой связи, осуществление операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, рассмотрение претензий пользователей услугами связи;

– профессиональная деятельность журналиста и другие.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) обязана вести соответствующий реестр операторов, осуществляющих обработку персональных данных. Включение в даный реестр является добровольным. Основанием включения выступает уведомление об обработке (о намерении осуществлять обработку) персональных данных, направленное в территориальное управление Роскомнадзора.

Проблема заключается в том, что наличие оператора в Реестре не гарантирует законность его действий. Также, перечисленные выше процедуры не являются взаимозависимыми. Обязательность включения оператора в указанный реестр, например, при проведении государственной регистрации юридического лица или индивидуального предпринимателя, при внесении изменений в учредительные документы уже существующих организаций, могла бы послужить решению указанной проблемы. Указанная мера может способствовать снижению нарушений в сфере обработки и защиты персональных данных, а также позволит решить ряд проблем правоприменительной практики.

Таким образом, федеральный закон № 152–ФЗ дает легитимное определение оператора, организующего и (или) осуществляющего обработку персональных данных. Оператор – физическое либо юридическое лицо, имеющее доступ к чужим персональным данным. Он самостоятельно может не проводить обработку персональных данных, а может являться только организатором этого процесса. Оператор отвечает за легитимность и качество процесса обработки персональных данных. Закон делит операторов на несколько категорий: физические лица, индивидуальные предприниматели, юридические лица, муниципальные органы, государственные органы. Субъект права – базовая категория права. Любое лицо

[39] Кучеренко, А.В. Понятие и признаки оператора, осуществляющего обработку персональных данных /А.В. Кучеренко // Альманах современной науки и образования. Тамбов: Грамота. – 2009. – №12 (31). – Ч.2. – С. 60.

является субъектом права, не приобретая этот статус самостоятельно и единовременно, а только из признания данного статуса государством. Говоря иначе, объем правосубъектности лица, который участвует в обороте персональных данных, определяется формулировкой положений законодательства. Данный факт положен в основу всего правореализационного процесса в сфере обработки персональных данных. На данный момент в связи с вышесказанным существует потребность законодательного закрепления точных характеристик и четких критериев, которые лягут в основу определения статуса оператора, осуществляющего обработку персональных данных.

2.2 Права и обязанности субъектов, участвующих в обороте персональных данных

Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и о защите информации» относит персональные данные к конфиденциальной информации[40]. Законодательство расценивает действия по обработке персональных данных как фактор, оказывающий существенное влияние на неприкосновенность частной жизни, личную и семейную тайну. В соответствии со ст. 7 федерального закона № 152–ФЗ «операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом»[41]. Тем самым гарантируется конфиденциальность персональных данных, что означает законодательное обеспечение режима их тайны.

Все права, предоставленные субъекту персональных данных, возникают у субъекта единовременно. Стоит отметить, что реализация каждого права субъекта персональных данных зависит от этапа развития правоотношения, связанного с обработкой персональных данных. По мнению автора Кучеренко А.В. классификация прав субъекта персональных зависит от времени их реализации и включает три группы.

1. Группа прав, которые субъект персональных данных может реализовать до начала их обработки. К правам данной группы могут быть отнесены следующие: давать согласие на обработку, право дать согласие включить в общедоступные источники персональные данные, право получать сведения об операторе данных.

2. Группа прав, которые субъект персональных данных может реализовать во время обработки данных. В состав прав данной группы влкючается право иметь доступ к обрабатываемым персональным данным, право направить оператору запрос о наличии сответствующих данных у оператора, право требовать от оператора уточнения, блокирования и уничтожения персональных данных. Кроме

[40] Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 23.04.2018) // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3448.

[41] Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 23.04.2018). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3448.

того, в данную группу входят права отзывать согласие на обработку персональных данных и требовать исключения персональных данных из общедоступных источников, право обращаться в Роскомнадзор как в Уполномоченный орган по защите прав субъектов персональных данных в случае их нарушения.

3. Группа прав, которые субъект персональных данных может реализовать после их обработки. В состав данной группы включено право обжаловать в судебном порядке неправомерные действия оператора, право обращаться в Роскомнадзор как в Уполномоченный орган по защите прав субъектов персональных данных в случае их нарушения [42].

Наличие согласия субъекта персональных данных на их обработку является общим правилом обработки персональных данных в Российской Федерации. Согласие на обработку персональных данных может быть дано субъектом персональных данных самостоятельно или его представителем в любой форме, которая позволяет подтвердить факт его получения, если иное не установлено федеральным законом.

Любые иные исключения должны быть регламентированы федеральными законами. Согласие субъекта на обработку персональных данных не является необратимым и может быть отозвано. Стоит отметить, что в данном случае, субъект, чьи персональные данные обрабатываются, не должен выполнять какие-либо условия или объяснять причины такого решения. О принятом решении субъект персональных данных должен уведомить оператора. Право отзыва согласия на обработку персональных данных не распространяется на случаи их обработки, установленные федеральными законами. Однако имеются ситуации, в которых субъект обязан предоставить свои персональные данные, данное регламентировано федеральными законами. Например, когда субъект подает налоговую декларацию [43]. В случае, если обработка персональных данных выполняется без разрешения субъекта и является незаконной, оператор обязан немедленно прекратить данную обработку.

Субъект персональных данных обладает правом потребовать от оператора уточнить или заблокировать персональные данных, а ткже уничтожить их. Данное право реализуемо, если персональные данные, которыми располагает оператор, неполные, устаревшие, неточные либо если они получены незаконно, также не являются необходимыми для заявленной цели обработки. Срок внесения изменений и удаления данных составляет семь рабочих дней с момента обращения субъекта персональных данных либо его законного представителя, что соответствует нормам ч. 3 ст. 20 ФЗ–152. Оператор персональных данных обязан

[42] Кучеренко, А.В. Понятие и признаки оператора, осуществляющего обработку персональных данных /А.В. Кучеренко // Альманах современной науки и образования. Тамбов: Грамота. – 2009. – №12 (31). – Ч.2. – С. 59-60

[43] Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 29.07.2017) // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451. 94

уведомить субъекта персональных данных о всех изменения и предпринятых им мерах[44].

Субъект, в чьих интересах ведется обработка персональных данных, имеет право обжаловать действие или бездействие оператора, осуществляемого данную обработку. Статьей 17 федерального закона № 152–ФЗ закреплено право субъекта персональных данных на обжалование действий или бездействия оператора в т. ч. на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Так, А. обратилась в суд с иском к ООО о взыскании компенсации морального вреда в виду обработки персональных данных с нарушением требований закона. Судом было установлено, что А. неоднократно получала почтовые отправления от ООО с указанием о том, что выиграла приз, а также получала каталоги товаров, которые реализует ответчик, в поступающей корреспонденции содержались ее персональные данные - фамилия, имя, отчество, место регистрации и проживания, согласия на размещение указанных данных истец не давала. Разрешая заявленные требования, суд указал, что моральный вред истцу подлежит возмещению, поскольку доказательств ознакомления истца с Положением ответчика о порядке обработки персональных данных клиентов ООО, а также о согласии истца на обработку персональных данных ответчиком представлено не было[45].

По другому делу Л.Д. обратилась в суд с исковым заявлением к банку о взыскании компенсации морального вреда. В обоснование иска указала, что заключила с банком кредитный договор на приобретение автомобиля, кредитный договор был обеспечен договором залога автомобиля и страхованием приобретенного по кредиту имущества от гибели. Для осуществления своих целей банком, в нарушение требований Федерального закона № 152–ФЗ от 27.07.2006 года «О персональных данных», без письменного согласия истца, долговому агентству были переданы ее персональные данные: имя, фамилия и отчество, дата рождения; паспортные данные, домашний адрес, номера рабочего, домашнего и мобильного телефона, информация о последнем известном банку месте работы. В результате данных действий банка, на номер сотового телефона истца ежедневно, как в рабочие, так и в выходные дни, поступали телефонные звонки от долгового агентства с требованиями погашения перед банком задолженности, что лишало ее возможности добросовестно работать, нарушало ее покой и отдых, причиняло моральные страдания.

Рассматривая спор и принимая решение о частичном удовлетворении исковых требований, суд первой инстанции исходил из установленного факта, что на передачу персональных данных истца банком в долговое агентство требовалось получение письменного согласия Л.Д., однако, данного согласия банком получено не было. Действия банка по передаче персональных данных истца противоречат

---

[44] Добрикова Е. Информационно-правовой портал Гарант. Обязанности оператора при обработке персональных данных [Электронный ресурс]// Режим доступа: http://www.garant.ru/actual/persona/obyazannosti/#ixzz5EKshkqBU.

[45] Апелляционное определение Московского городского суда от 10.08.2015 по делу № 33-28318/2015 // Справочно-правовая система «КонсультантПлюс»

требованиям статьи 857 Гражданского кодекса РФ, статье 26 Федерального закона «О банках и банковской деятельности», положениям Конституции РФ, что является основанием для удовлетворения требований истца о взыскании с ответчика компенсации морального вреда.

Апелляционная инстанция нашла заслуживающими внимания доводы жалобы о несогласии с размером денежной компенсации морального вреда, определенной ко взысканию судом. При определении размера компенсации морального вреда суд учел содержание и количество писем (2 письма) от долгового агентства. Однако, судебная коллегия считает, что размер компенсации морального вреда, определенный судом, не соответствует характеру нравственных страданий истца, степени вины ответчика, а также требованиям разумности и справедливости, при этом судебная коллегия исходит из фактических обстоятельств дела. Исходя из изложенного, судебная коллегия нашла необходимым изменить решение суда, увеличив размер компенсации морального вреда[46].

Таким образом, субъект персональных данных имеет право принимать предусмотренные действующим законом меры по защите своих прав. Операторы, которые нарушили законодательство о персональных данных, несут уголовную, дисциплинарную, административную ответственность.

Уголовное законодательство предусматривает следующий перечень статей за нарушение законодательства: ст.ст.137, 272 Уголовного Кодекса РФ. УК РФ провозгласив одной из своих задач охрану прав и свобод человека и гражданина от преступных посягательств, в диспозиции ст.137 УК РФ установил, что незаконное собирание или распространение сведений о частной жизни лица (за исключением общедоступной информации), составляющих его личную или семейную тайну, без его согласия служит основанием для привлечения к уголовной ответственности. Однако, как и повелось – у каждого правила есть свое примечание. Таковым является Федеральный закон РФ «Об оперативно-розыскной деятельности» № 144–ФЗ, вынужденно приоткрывающий неприкосновенный занавес тайны личных сведений субъектов, в отношении которых имеются достоверные свидетельства о подготовке, совершении или совершенном противоправном деянии, которое также может создавать угрозу государственной, экологической и т. д. безопасности Российской Федерации, таким образом исключая возможную ответственность должностных лиц по ч.2 ст.137 УК РФ.

Сам же потерпевший также вправе предпринимать активные действия по защите своих законных интересов путем обжалования вынесенных решений в судебном порядке или же в Уполномоченный орган по защите персональных данных. Последний, в свою очередь, имеет подтвержденную возможность обращаться с исковым заявлением и представлять интересы субъектов персональных данных в уголовном судебном разбирательстве.

[46] Апелляционное определение Новосибирского областного суда от 21.01.2014 по делу № 33-383/2014 // Справочно-правовая система «КонсультантПлюс».

Стоит отметить, что отнюдь не все отношения попадают под охрану исключительно ст. 137 УК РФ. При определенных условиях, когда непосредственно задействованы электронные средства обработки информации, неправомерные действия могут быть квалифицированы и по ст.272 УК РФ. Такое деяние, в сущности, является двухобъектным посягательством. При уголовно-правовой оценке действия лица будут образовывать разнообъектную идеальною совокупность по ст.137 и ст. 272 УК РФ. Субъект осуществляет посягательство, с одной стороны, на отношения по поводу обеспечения целостности и сохранности компьютерной информации. А с другой – на конституционные права неприкосновенности частной жизни. Объективная сторона состава преступлений обеих статей тоже имеет отличительные черты. Следует обратить внимание на вытекающее обстоятельство: доступ будет являться неправомерным, не только если лицо не имеет права на таковой, но и если, имея соответствующее разрешение, оно осуществит его помимо установленного порядка[47].

Административные правонарушения предусмотрены ст.ст. 5.39, 13.11, 13.14 КоАП РФ. Стоит отметить, что 1 июля 2017 года вступил в силу Федеральный закон от 07.02.2017 № 13–ФЗ, который внес поправки в ст. 13.11 КоАП. В частности, он расширил перечень оснований для привлечения к административной ответственности за незаконную обработку персональных данных и увеличил штрафы. В частности, именно такое основание, как обработка персональных данных без получения согласия их субъекта, предусматривает самые крупные штрафы для всех категорий нарушителей – до 75 000 руб.

Дисциплинарная ответственность предусмотрена ст. 192 Трудового Кодекса РФ. В соответствии со ст. 192 ТК РФ 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: замечание, выговор, увольнение по соответствующим основаниям.

Оператор, как субъект персональных данных наделен определенными обязанностями.

Первое, что должен сделать оператор, это уведомить соответствующий орган – Роскомнадзор – о производстве обработки персональных данных лица. Оператор обязан направить данное уведомление до начала обработки данных и указать в нем наименование, адрес оператора, категории персональных данных, цель обработки, правовое основание обработки данных, категорию субъектов, которые подлежат обработке, наименование физического или юридического лица, дату и сроки обработки персональных данных.

Существуют ситуации, при которых уведомление Роскомнадзора не требуется. Таковым может быть обработака персональных данных работников работодателем. Также в случаях заключения договоров с клиентом не требуется уведомлять Роскомнадзор, если сведения используются организацией

[47] Латухина, В.С. Международные и национальные стандарты уголовно-правовой защиты персональных данных/ В.С. Латухина // Экономика. Социология. Право. – 2017. – №.4. – С. 76.

исключительно в целях данного договора и не передаются иным третьим лицам без согласия субъекта персональных данных. При оформлении единоразового пропуска для доступа на территорию операторатора персональных данных и при обработке общедоступных персональных данных не требуется уведомление Роскомнадзора. Если оператором используются только ФИО субъекта и другие аспекты. Данные положения определены в ч. 2 ст. 22 закона о персональных данных [48].

Обязанностью опреатора является обеспечение конфиденциальности персональных данных. Он не должен распространять какие-либо известные ему сведения о персональных данных субъекта без согласия лица, в отношении которого ведется обработка персональных данных. Это является основной обязанностью оператора. Без письменного согласия работника работодатель не может сообщить персональные данные какой-либо третьей стороне. Кроме того, необходимо предупреждать третьи лица о том, что передаваемые персональные данные работников могут использоваться только в тех целях, для которых они переданы. Пердача персональных данных работников допустима только в пределах одной организации, у одного индивидуального предпринимателя, что должно быть обусловлено одним локальным нормативным актом. Ознакомление с данным актом работника под подпись является обязательным (ст. 88 ТК РФ)[49].

Обязанностью оператора является принятие мер по обеспечению безопасности персональных данных. С данной обязанностью тесно связана дургая - по осуществлению внутреннего контроля за соблюдением требований по защите персональных данных. В ст. 22.1 закона о персональных данных определено, что с целью выполнения указанных обязанностей в организации должно быть назначено ответственное лицо. В полномочия и закрепленные обязанности указанного лица входит непосредственный внутренний контроль за тем, как оператор и его работники соблюдают требования о защите персональных данных. Ответственное лицо обязано информировать работников о всех изменениях в законодательстве о персональных данных, доводить до их сведения его положения иположения локальных актов, связанных с вопросами обработки персональных данных. Также в обязанности лица, ответственного за обработку персональных данных у оператора, входит организация и прием обращений от субъектов персональных данных. С этой целью дополнительно могут применяться и использоваться различные технические меры, обеспечивающие безопасность обработки персональных данных. Ответственное лицо обязано издавать все документы, в которых определена политика компании в области обработки персональных данных.

---

[48] Добрикова Е. Информационно-правовой портал Гарант. Обязанности оператора при обработке персональных данных [Электронный ресурс]// Режим доступа: http://www.garant.ru/actual/persona/obyazannosti/#ixzz5EKshkqBU.

[49] Добрикова Е. Информационно-правовой портал Гарант. Обязанности оператора при обработке персональных данных [Электронный ресурс]// Режим доступа: http://www.garant.ru/actual/persona/obyazannosti/#ixzz5EKshkqBU.

В ч. 2 ст. 18.1 закона о персональных данных определяется публичность политики обработки персональных данных организации. Способом, который в наибольшей степени позволяет сделать данный документ доступным, является размещение на официальном сайте оператора. Если данный аспект не выполним, то бумажный вариант политики может быть размещен в любом месте, которое является доступным для посетителей организации. Это могут быть специальные информационные доски либо отдельные «кармашки». Те операторы, которые производят сбор персональных данных через Интерент, в обязательном порядке размещают политику на официальном сайте. При этом, должен быть обеспечен доступ к данной политике. Роскомнадзор разместил на своем сайте рекомендации, позволяющие составить политику в области обработки персональных данных.

Стоит отметить, что на предприятии должно быть два документа, связанных с обработкой персональных данных, которые не следует путать. Так, политика обработки персональных данных распространяет свое действие и предназначена для тертьих лиц – клиенты, контрагенты и др. Положение о защите, хранении, обработке и передаче персональных данных работников – иной документ, выступающий в роли локального акта, распространяет свое действие на работников организации. Требования публичности на него не распространяются, но обязательно необходимо под роспись ознакомить с ним каждого сотрудника компании (ст. 22 ТК РФ)[50].

Обязанностью оператора является локализация персональных данных. Оно заключается в том, что все операторы, осуществляющие обработку персональных данных, должны делать это при помощи тех баз данных, которые хранятся в России. Требование вступило в действие с 1 сентября 2015 года и закреплено в ч. 5 ст. 18 закона о персональных данных. Среди операторов и различных специалистов указанная норма вызвала большое количество споров и стало резонансным. Это связано с неоднозначностью формулировок, которые вызвали вопросы даже у экспертов. Не было ясно, на какие точно персональные данные и на каких операторов распространено действие требования, допустимо ли производить одновременно обработку данных на российском и иностранном сервере, как определяеся гражданство субъекта и многие другие.

В большинстве своем указанные вопросы были раскрыты Роскомнадзором до вступления новых требований в действие. В частности, вопрос определения гражданства лица, персональные данные которого обрабатываются оператором, был отнесен к самостоятельному ведению оператора. Он сам должен решить, каким образом будет определяться гражданство, либо применяться требование о локализации к персональным данным всех субъектов. Также Роскомнадзор разъяснил положение о том, что записанные на в российскую базу данных персональные данные в дальнейшем могут проходить обработку на иностранной базе данных.

[50] Добрикова Е. Информационно-правовой портал Гарант. Обязанности оператора при обработке персональных данных [Электронный ресурс]// Режим доступа: http://www.garant.ru/actual/persona/obyazannosti/#ixzz5EKshkqBU.

Обязанность оператора обеспечивать запись и хранение, систематизацию и накопление, а также обновление и изменение персональных данных российских граждан при помощи тех баз данных, которые расположены в России, должна быть в обязательном порядке закреплена как в политике обработки персональных данных, так и в Положении о защите персональных данных работников. В указанных документах также должно быть определено место нахождения указанных баз данных[51].

Оператор прекращает обработку персональных данных в следующих случаях: когда достигнута цель обработки персональных данных, а также, когда от субъекта данных поступил отказ в их обработке. Срок, который закреплен законодательно для прекращения обработки, составляет 30 дней. В дополнительном соглашении такой срок может изменяться, что указано в ч. 4-5 ст. 21 закона о персональных данных

Таким образом, деление прав субъекта персональных данных производится на три категории. Они включают такие составляющие, как права субъекта персональных данных, которые он может реализовать до обработки, в процессе обработки данных и после их обработки. Помимо возможности отозвать свое согласие на обработку персональных данных субъект имеет еще целый ряд прав, о которых важно знать. В том числе лицо, чьи персональные данные обрабатываются, имеет право получать любую информацию, касающуюся этого, будь то данные оператора (его наименование и место нахождения), перечень обрабатываемых данных, сроки их обработки и хранения и др. Субъект, в чьих интересах ведется обработка персональных данных, имеет право обжаловать действие или бездействие оператора, осуществляющего данную обработку и т. д.

Оператор, который производит обработку персональных данных, должен выполнять ряд обязанностей. К их числу относятся: уведомление об обработке персональных данных соответствующего органа, обеспечение безопасности персональных данных при их обработке, получение согласия субъекта на обработку его персональных данных и другие.

Выводы по разделу 2

На основе проведенного анализа характеристика правового понятия «субъект персональных данных», можно сделать вывод, что любое физическое лицо, не зависимо от каких-либо критериев с наличием информации, является субъектом права. Проблематика заключается в том, что ФЗ «О персональных данных» не содержит конкретного, обобщенного, официально закрепленного понятия субъекта персональных данных. Действующий Закон не разграничивает участников правоотношений, не выделяет четких критериев

[51] Добрикова Е. Информационно-правовой портал Гарант. Обязанности оператора при обработке персональных данных [Электронный ресурс]// Режим доступа: http://www.garant.ru/actual/persona/obyazannosti/#ixzz5EKshkqBU.

Федеральный закон № 152–ФЗ дает легитимное определение оператора, организующего и (или) осуществляющего обработку персональных данных. Оператор – физическое либо юридическое лицо, имеющее доступ к чужим персональным данным. Он самостоятельно может не проводить обработку персональных данных, а может являться только организатором этого процесса. Оператор отвечает за легитимность и качество процесса обработки персональных данных. Закон делит операторов на несколько категорий: физические лица, индивидуальные предприниматели, юридические лица, муниципальные органы, государственные органы.

Субъект права – базовая категория права. Любое лицо является субъектом права, не приобретая этот статус самостоятельно и единовременно, а только из признания данного статуса государством. Говоря иначе, объем правосубъектности лица, который участвует в обороте персональных данных, определяется формулировкой положений законодательства. Данный факт положен в основу всего правореализационного процесса в сфере обработки персональных данных. На данный момент в связи с вышесказанным существует потребность законодательного закрепления точных характеристик и четких критериев, которые лягут в основу определения статуса оператора, осуществляющего обработку персональных данных.

Деление прав субъекта персональных данных производится на три категории. Они включают такие составляющие, как права субъекта персональных данных, которые он может реализовать до обработки, в процессе обработки данных и после их обработки. Помимо возможности отозвать свое согласие на обработку персональных данных субъект имеет еще целый ряд прав, о которых важно знать. В том числе лицо, чьи персональные данные обрабатываются, имеет право получать любую информацию, касающуюся этого, будь то данные оператора (его наименование и место нахождения), перечень обрабатываемых данных, сроки их обработки и хранения и др. Субъект, в чьих интересах ведется обработка персональных данных, имеет право обжаловать действие или бездействие оператора, осуществляемого данную обработку и т. д.

Оператор, который производит обработку персональных данных, должен выполнять ряд обязанностей. К их числу относятся: уведомление об обработке персональных данных соответствующего органа, обеспечение безопасности персональных данных при их обработке, получение согласия субъекта на обработку его персональных данных и другие.

3 ОСОБЕННОСТИ И ПРОБЛЕМАТИКА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННЫХ ОРГАНАХ

3.1 Особенности защиты персональных данных в государственных органах

Особенности защиты персональных данных в государственных органах заключаются в том, что аспекты данной сферы могут быть рассмотрены с нескольких позиций. В первую очередь, государственные органы выступают в роли работодателя. При прохождении государственной службы служащие предоставляют в кадровые службы государственных органов конфиденциальные документы, содержащие персональные данные, которые отражают личную или семейную жизнь. Эти данные содержатся в паспорте, трудовой книжке, военном билете, дипломе и т. д., а также в документах, раскрывающих характер правоотношений с государством: назначение на должность, аттестационный лист, сведения о доходах/расходах и другое.

Правовое регулирование обработки и защиты персональных данных государственных гражданских служащих, помимо Закона № 152–ФЗ и гл. 14 Трудового кодекса РФ, осуществляется также Федеральным законом от 27.07.2004 № 79–ФЗ «О государственной гражданской службе Российской Федерации», Федеральным законом от 30.11.2011 № 342–ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» и рядом подзаконных актов:

Указом Президента РФ от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» (далее – Положение о персональных данных госслужащего);

– постановлением Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

– постановлением Правительства РФ от 21.03.2012 № 211 «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» (далее – Постановление № 211) и др[52].

На локальном уровне порядок обработки и защиты персональных данных госслужащих утверждается соответствующими государственными органами и подлежит официальному опубликованию. К примеру, утверждены следующие Положения о персональных данных.

[52] Обработка персональных данных государственных гражданских служащих [Электронный ресурс]// Режим доступа: https://www.pro-personal.ru/article/1083852-qqe-m12-obrabotka-personalnyh-dannyh-gosslugagih

1. Положение об организации работы с персональными данными федеральных государственных гражданских служащих Министерства финансов Российской Федерации, заместителей руководителей Федеральных служб, находящихся в ведении Министерства финансов Российской Федерации, руководителей их территориальных органов, назначаемых на должность Министром финансов Российской Федерации, утв. приказом Минфина России от 04.07.2011 № 75н;

2. Положение о работе по обработке персональных данных в Министерстве энергетики Российской Федерации, утв. приказом Минэнерго России от 11.11.2008 № 166.

3. Положение о работе с персональными данными государственного гражданского служащего ФСТ России и ведении его личного дела, утв. приказом ФСТ России от 07.11.2008 № 441-к.

4. Положение об организации работы с персональными данными федерального государственного гражданского служащего Управления делами Президента Российской Федерации, утв. приказом Управления делами Президента РФ от 28.07.2011 № 451 и другие[53].

Требования к обработке, хранению и передаче персональных данных государственного гражданского служащего во многом совпадают с требованиями, предусмотренными гл. 14 ТК РФ. Как и в трудовых правоотношениях, персональные данные госслужащего:

1) должны быть получены только у него лично;

2) должны обрабатываться нанимателем только в целях, предусмотренных законом;

3) не могут обрабатываться, если речь идет о политических, религиозных и иных убеждениях и частной жизни служащего, о его членстве в общественных объединениях, в том числе в профессиональных союзах;

4) могут передаваться третьей стороне только с письменного согласия государственного служащего;

5) защищаются за счет средств нанимателя;

6) не могут являться основой для принятия конкретных решений, если получены исключительно в результате автоматизированной обработки[54].

Кроме того, государственные служащие в процессе реализации должностных обязанностей вступают во взаимоотношения с различными предприятиями, организациями, учреждениями, гражданами. В результате у них накапливаются данные о конкретном индивиде, начиная с самых простых (фамилии, имени, отчества, даты и места рождения и т. п.) и заканчивая очень специфическими (сведениями о заболеваниях, судимостях, размерах доходов, имуществе и пр.). При этом гражданин не желает, чтобы сведения о нем становились известны широкому кругу лиц.

---

[53] Обработка персональных данных государственных гражданских служащих [Электронный ресурс]// Режим доступа: https://www.pro-personal.ru/article/1083852-qqe-m12-obrabotka-personalnyh-dannyh-gosslugagih

[54] Салтыкова, О.П. Проблемы организации работы с персональными данными на гражданской службе/ О.П. Салтыкова//Агрофорсайт. – 2017. - №2. – С.1-9

Таким образом, в органах государственной власти защита персональных данных происходит по двум направлениям: организация работы с персональными данными государственных служащих и организация работы с персональными данными граждан[55].

Организация работы с персональными данными на государственной службе предусматривает решение двух основных задач. Первая задача связана с правовыми вопросами владения информацией, т. е. с правами лиц определять, при каких условиях, когда и кому может быть передана относящаяся к ним информация. Вторая задача связана с безопасностью, т.е. с защитой информации от случайного или преднамеренного (несанкционированного) ее раскрытия, изменения или разрушения. При этом под данными, содержащимися в банках данных, понимаются именно фактические данные, а не мнения тех или иных лиц, включая должностных лиц компетентных органов.

В Федеральном законе №152 рассмотрены вопросы хранения, обработки и защиты данных, а также введена классификация по объему и типу хранимых данных. В зависимости от объема и типа персональных данных меняются и требования к защите информации. К примеру, обезличенной и общедоступной информации присваивается четвертый класс защищенности данных. В четвертом классе защищенности нарушение целостности или утечки данных не влечет за собой возникновения негативных последствий для субъектов персональных данных. Также в данном законе вводится понятия оператора данных, под которым понимается орган государственной или муниципальной власти организующий обработку и хранение соответствующих персональных данных.

Во втором и третьем классе защищенности находится информация, при утечке или утрате которой могут возникать негативные последствия для субъектов персональных данных.

Самый высший класс защищенности – первый – присваивается информации, связанной с персональными данными, поступающими по линии социального развития и здравоохранения. Естественно, утечка таких данных или нарушение безопасности ведет к сильным негативным последствиям для субъекта персональных данных (см. табл. 1).

В табл. 1 можно увидеть, что классификация по основанию класса защиты меняется в зависимости от 2 факторов: а) количества персональных данных граждан и б) ее объема. Соответственно в органах государственной власти для защиты данных в первую очередь создается модель угроз, и используется соответствующее программное обеспечение для защиты персональных данных. Если в 4 классе комплекс мер по защите информации определяется только оператором, то в следующих классах защиты требуется обязательная сертификация со стороны Федеральной службы по техническому и экспертному

[55] Салтыкова, О.П. Проблемы организации работы с персональными данными на гражданской службе/ О.П. Салтыкова//Агрофорсайт. – 2017. - №2. – С.1-9.

контролю[56], которая предполагает получение оператором лицензии для ведения деятельности по обработке персональных данных.

Таблица 1 – Классификация объектов защиты персональных данных по классу защищенности

№	Категория	Объем 3 (<1 000, организация)	Объем 2 (1 000-100 000, отрасль, город)	Объем 1 (>100 000, субъект Федерации)
1	обезличенные, общедоступные	К-4	К-4	К-4
2	идентификационные	К-3	К-3	К-2
3	идентификационные и присутствует дополнительная информация	К-3	К-2	К-1
4	медицинские, оциальные	К-1	К-1	К-1

Порядок действий по защите информации в государственных органах предполагает прохождение следующих шагов:

1) отправка уведомления в уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных с использованием средств автоматизации;
2) сбор данных, обследование системы;
3) классификация оператором, класса защиты обрабатываемых данных;
4) построение модели угроз актуальной для данной информационной системы;
5) разработка технического задания на систему для защиты персональных данных организации;
6) проектирование защиты персональных данных организации;
7) внедрение системы защиты персональных данных;
8) выполнение требований по инженерной защите помещения, пожарной безопасности, санитарной, экологической норме эксплуатации;
9) аттестация в соответствии с требованиями безопасности;
10) повышение уровня образования и обучение сотрудников работе с персональными данными граждан;
11) сопровождение и доработка системы защиты персональных данных[57].

Данная последовательность шагов в определенной мере гарантирует эффективную работу с информацией и поддержание соответствующего ей уровня защиты.

Методы защиты персональных данных регламентированы в приказе Федеральной службы по Экспертному контролю[58]. Более детально о методах защиты говорится в объединенном приказе нескольких ведомств[59].

[56] Постановление правительства Российской Федерации «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17 ноября 2007г. // http://www.klerk.ru/doc/93135

[57] Власов, Д.С. Защита персональных данных в автоматизированных системах обработки информации органов государственной власти / Д.С. Власов // Успехи современной науки. – 2016. – Том 8. – №12. – С. 34.

В порядке конкретизации можно отметить следующее. Так, для защиты рабочих мест используется только программное обеспечение отечественного производителя. Данное требование связанно с тем, что государственные органы безопасности не могут проверить иностранного производителя защитных средств на предмет недокументированных способов работы. Для защиты персональных рабочих и серверов отвечающих за обработку персональных данных используют следующие типы защиты:

1) локальные системы защиты от несанкционированного доступа, предполагающие защиту рабочих мест пользователей от незаконного копирования служебной информации или персональных данных пользователей участвующие в обработке;

2) опечатку компьютера и установку средств по шифрованию и защиты системного блока от несанкционированного доступа;

3) использование средств криптографической защиты;

3) использование защищенных каналов связи;

4) использование внутренних сетей без выхода в сеть Интернет;

5) применение средств антивирусной защиты.

В качестве средств криптографической защиты в органах государственной власти используется программный комплекс Крипто-про, позволяющий производить санкционированный доступ к программам по обработке персональных данных.

Изначально же от несанкционированного доступа должны защищать сервер данных и рабочие места пользователей. Для этих целей на рабочие места пользователей устанавливают специальные аппаратные устройства, которые защищают компьютер от возможного вскрытия и модификации данных. Одним из наиболее известных таких устройств в Российской Федерации является аппаратно-программный комплекс «Соболь».

Следующим уровнем после защиты компьютера выступает защита компьютера от копирования с помощью встроенных средств операционной системы с использованием съемных носителей информации, таких как DVD, флеш-накопитель, переносные жесткие диски. Данную задачу решает программный комплекс Secret-Net. Он позволяет хранить и использовать данные, которые подвергаются риску незаконного копирования. Данная система позволяет также интегрироваться в сетевую доменную структуру организации[60].

Известно, что крупные организации зачастую имеют связанную, многоуровневую доменную структуру организации хранения данных. Также внутри организации могут использоваться дополнительно межсетевые экраны и антивирусное программное обеспечение. Антивирусное программное

---

[58] Приказ Федеральной службы по техническому и экспортном контролю «об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» от 5 февраля 2010 года №58. // https://rg.ru/2010/03/05/da№№ye-dok.html.

[59] Приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. №55/86/20 // http://dehack.ru/zak_akt/№pbaza/prikaz_55-86-20

[60] Власов, Д.С. Защита персональных данных в автоматизированных системах обработки информации органов государственной власти / Д.С. Власов // Успехи современной науки. – 2016. – Том 8. – №12. – С. 33-36.

обеспечение, в первую очередь, необходимо для защиты рабочих мест от возможного вторжения программных вирусов. Некоторые типы вирусов созданы специально для кражи персональных данных, поэтому защита от такого типа угроз также является приоритетной. Для использования в Российской Федерации разрешено в использовании органами государственной власти антивирусное программное обеспечение создаваемое в Лаборатории Касперского. На компьютерах, которые используются отдельно для работы в сети Интернет, возможно использование альтернативных антивирусных средств распространяемых бесплатно, – с открытыми исходными кодами. Реестр разрешенных программ ведется органами государственной власти при соответствующем разрешении и приказов Федеральной службы безопасности Российской Федерации[61].

Использование защиты на персональных рабочих местах и серверах, которые обрабатывают персональные данные, не гарантирует от потери или утечки данных. В дополнении к перечисленным методам защиты применяется организация шифрованных каналов связи. Шифрованные каналы связи предполагают их защиту от несанкционированного доступа, и шифрованию трафика передаваемого по данным каналам.

Известно, что на сегодняшний день уровень обработки и качество предоставляемых электронных услуг государством напрямую связаны с защитой персональных данных граждан. Так, в 2015 году Российская Федерация в рейтинге внедрения электронного правительства, который ведет Организация Объединенных наций, находится на 27 месте. Причем Российская Федерация поднялась за год на 30 позиций, подтянувшись к таким развитым странам, как Италия и Германия. Это, в свою очередь, предполагает и дальнейшее развитие средств телекоммуникации, методов защиты информации, что является ключевой задачей по защите прав и свобод граждан нашей страны[62].

Таким образом, основные особенности защиты персональных данных в государственных органах заключаются в том, что организация работы с персональными данными происходит по двум направлениям: персональные данные государственных служащих и работа с персональными данными граждан. С учетом развития электронного правительства, особенно актуальными являются вопросы защиты накопленных данных граждан. В органах государственной власти для защиты данных в первую очередь создается модель угроз, и используется соответствующее программное обеспечение для защиты персональных данных.

[61] Власов, Д.С. Защита персональных данных в автоматизированных системах обработки информации органов государственной власти / Д.С. Власов // Успехи современной науки. – 2016. – Том 8. – №12. – С. 35.

[62] Власов, Д.С. Защита персональных данных в автоматизированных системах обработки информации органов государственной власти / Д.С. Власов // Успехи современной науки. – 2016. – Том 8. – №12. – С. 36.

3.2 Проблемы защиты персональных данных в государственных органах

С целью выявления нарушений в области защиты прав субъектов персональных данных уполномоченный орган (Роскомнадзор) проводит проверки (Приложение А). В результате проведенных проверок отмечно сокращение количества предписаний об устранении выявленных нарушений в области защиты персональных данных (Приложение Б). Также сократилось число административных протоколов, направленных в суды по результатам плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных (Приложение В). Тем не менее, сумма наложенных административных штрафов по результатам плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных составляет порядка 6 млн. руб. (Приложение Г).

Итак, анализ статистики и судебной практики демонстрирует, что нарушения прав субъектов персональных данных продолжаются.Рассмотрим наиболее частые нарушения, которые встречаются при организации работы с персональными данными на государственной гражданской службе.

Как демонстрирует сложившиеся практика организации работы с персональными данными на гражданской службе, одним из нарушений является ситуация, при которой нормативным правовым актом государственного органа, регламентирующим порядок работы с персональными данными, не определена политика государственного органа в отношении обработки персональных данных. А также отсутствует лицо, ответственное за организацию обработки персональных данных, либо данные лица не имеют специальных знаний в области защиты прав субъектов персональных данных. Государственные органы ссылаются на то, что такое лицо определено внутренним распоряжением. Однако из буквального текста большинства приказов следует, что лицо, ответственное за работу с персональными отвечает лишь за сбор и хранение данных, но не за их обработку. Данные нарушения неоднократно отмечались в решениях судов, но чаще всего отмечаются в небольших муниципальных образованиях.

Например, прокуратурой Наримановского района Астраханской области 20.04.2016 года с 09.00 часов до 14.30 часов проведена проверка по факту нарушения законодательства о персональных данных в деятельности администрации МО «Волжский сельсовет». В ходе проверки было установлено, что администрацией МО «Волжский сельсовет» не назначены лица, ответственные за организацию обработки персональных данных, отсутствует лист ознакомления с Постановлением администрации МО «Волжский сельсовет» от 21.05.2013 № 113 «Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования «Волжский сельсовет». Выявлены нарушения ч. 2 ст. 18.1 Закона № 152, которым установлена обязанность оператора, являющегося юридическим лицом, по изданию документов определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных

данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Руководствуясь ст. 29.10 КоАП РФ, суд главу администрации муниципального образования «Волжский сельсовет» Иманову Ж.П. признал виновной в совершении административного правонарушения, предусмотренного ст. 13.11 КоАП РФ и назначил наказание в виде предупреждения[63].

Ряд нарушений выявлен в области защиты персональных данных государственных служащих. На государственной гражданской службе кадровыми службами реализуется целый ряд кадровых технологий, такие как, конкурс на замещение вакантных должностей гражданской службы, кадровый резерв и другие, которые предполагают работу с персональными данными, и в том числе с биометрическими данными. Сложившаяся практика демонстрирует, что достаточно часто происходят ситуации нарушений требований Федерального закона «О персональных данных». В этом смысле актуальными для деятельности кадровых служб государственных органов будет Постановление Пятнадцатого арбитражного апелляционного суда от 14 марта 2014 г. № 15АП–22502/2013 в котором указывалось, что «использование фотоизображения работника для его идентификации согласно ч. 1 ст. 11 Федерального закона «О персональных данных» является обработкой биометрических персональных данных. Такая обработка допускается только с письменного согласия субъекта персональных данных. Письменное согласие на обработку биометрических персональных данных, как правило, не берется. Сбор и хранение в документах по кадровому учету копии страниц паспортов гражданских служащих должно производиться с учетом требований Федерального закона «О персональных данных», а обработка персональных данных не должна превышать объем обрабатываемых персональных данных, установленный Конституцией Российской Федерации и Федеральным законом «О государственной гражданской службе в Российской Федерации».

В Постановлении Седьмого арбитражного апелляционного суда от 27 июня 2012 г. № 07АП–4482/12 была указана следующая позиция: «В соответствии с пунктами 1, 2 статьи 5 Закона «О персональных данных» 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.

В Постановлении Федерального арбитражного суда Северо-Кавказского округа от 21 апреля 2014 г. № Ф08–1921/14 по делу № А53–13327/2013 суд сделал вывод о том, что для идентификации личности при приеме на работу достаточно фамилии, имени и отчества, при условии предъявления лицом документа, удостоверяющего личность, в котором содержатся все необходимые сведения. «Хранение копий паспорта, страниц военного билета, свидетельства о

[63] Постановление от 18 мая 2016 г. по делу № 5-454/2016///Справочно-правовая система «КонсультантПлюс»

заключении брака, свидетельства о рождении ребенка на рабочем месте превышает объем обрабатываемых персональных данных работника, действующим законодательством не предусмотрено, нарушает права и свободы гражданина, снижает уровень прав и гарантий работника, противоречит федеральному законодательству. При проведении проверки управление сделало правильный вывод о том, что учреждение производит обработку избыточных персональных данных, по сравнению с теми, которые определены к заявленным целям их обработки, что является нарушением части 5 статьи 5 Закона № 152 – ФЗ[64]. Представляется, что решение Федерального арбитражного суда Северо-Кавказского округа должно заинтересовать органы государственной власти, поскольку прием документов граждан при проведении конкурса на замещение вакантной должности гражданской службы, а следовательно, вытекающие из этого процедуры работы с персональными данными претендентов далеко не всегда идеальны.

В судебной практике встречаются и спорные ситуации, которые обусловлены спецификой кадровой работы на государственной гражданской службе. Так, например, согласно федеральному законодательству все документы, представленные претендентами при поступлении на государственную службу, подлежат обязательной проверке кадровыми службами, что подразумевает запросы, которые направляются в различные организации. Решениями Верховного суда РФ ограничение доступа к персональным данным распространено также и на государственные органы, если иное не предусмотрено законодательством. Так, например, в деле от 4 марта 2016 г. № 307–АД15–18844 суд исходил из отсутствия в действиях общества события вменяемого ему административного правонарушения, поскольку отказ общества в предоставлении антимонопольному органу информации, содержащей персональные данные физического лица, в отсутствие его согласия на их обработку и передачу, является правомерным[65].

Аналогичное решение было принято и в 2015 году: оно содержится в Постановлении Верховного Суда РФ от 30 марта 2015 г. № 302–АД15–1225. По материалам Постановления суд оставил без изменения ранее принятые по делу судебные акты, которыми удовлетворено требование о признании незаконным и отмене постановления о привлечении к административной ответственности за непредставление или несвоевременное представление антимонопольному органу сведений, либо представление заведомо недостоверных сведений, поскольку в предоставлении запрашиваемых сведений было правомерно отказано в связи с тем, что они относятся к персональным данным абонентов и не могут быть предоставлены. Следовательно, все запросы, направленные на проведение проверки предоставленных при поступлении на государственную службу

[64] Постановление Федерального арбитражного суда Северо-Кавказского округа от 21 апреля 2014 г. № Ф08-1921/14 по делу № А53-13327/2013//// Справочно-правовая система «КонсультантПлюс»

[65] Постановления Верховного Суда РФ от 4 марта 2016 г. № 307-АД15-18844// Справочно-правовая система «КонсультантПлюс»

документов (сведений) должны проводиться с учетом требований действующего законодательства.

В 2013 году по Постановлению Верховного Суда РФ от 7 октября 2013 г. № 94–АД13–1 суд отменил принятые судебные акты и прекратил производство по делу о невыполнении законных требований прокурора, поскольку требование прокурора о представлении сведений о доходах, об имуществе и обязательствах имущественного характера служащих и членов их семей влечет

незаконное разглашение персональных данных без согласия субъекта персональных данных;

несоблюдение режима конфиденциальности в случаях передачи персональных данных без согласия субъекта персональных данных;

несоблюдение права субъекта персональных данных на получение информации, касающейся обработки его персональных данных[66].

Ряд проблем касается персональных данных граждан, которые накоплены государственными учреждениями. Кроме того, стоит отметить отсутствие норм, регламентирующих сбор, обработку и раскрытие персональных данных государственными структурами всех уровней. Например, по делу № 33–5960, судом было установлено, что государственное учреждение в нарушение требований Федерального закона от 27 июля 2006 г. № 152–ФЗ «О персональных данных» совершило действия, направленные на раскрытие полученных персональных данных истца неопределенному кругу лиц, путем размещения в общественном месте в качестве образца заявления о выдаче дубликата страхового свидетельства, содержащего персональные данные истца в открытом виде, без согласия последнего. Разрешая заявленные требования, суд первой инстанции, руководствуясь статьями 3, 7, 17, 24 Федерального закона от 27.07.2006 № 152–ФЗ «О персональных данных», статьями 151, 1101 ГК РФ, установив факт размещения в общедоступном месте в качестве образца персональных данных истца, пришел к обоснованному выводу о частичном удовлетворении исковых требований, взыскав с ответчика компенсацию морального вреда[67].

Фактически ситуация, которая сложилась на текущий момент, приводит к безнаказанности ряда лиц, превращающих государственные базы персональных данных в источник извелечения прибыли и коммерческого оборота. Располагая определенными финансовыми ресурсами, любое лицо имеет возможность получить базу данных из абсолютно любой сферы, в которую будут включены сведения на миллионы жителей России, и не только.

Актуальным подтверждением данного суждения может являться факт утечки персональных данных из Федеральной службы по контролю за оборотом наркотиков (ФСКН) после ее расформирования в 2016 году. База включала сведения о пациентах психоневрологических диспансеров, о ВИЧ-инфицированных, о склонных к суициду, алко- и наркозависимых. В данном

[66] Постановление Верховного Суда РФ от 7 октября 2013 г. № 94-АД13-1// Справочно-правовая система «КонсультантПлюс»

[67] Определение Приморского краевого суда от 14.07.2014 по делу №33-5960 // Справочно-правовая система «КонсультантПлюс»

случае угроза информационной безопасности распространилась не только на тех, чьи сведения были в базе данных, а также на их непосредственное окружение: родственников, друзей, коллег[68].

Практика настоящего времени имеет обратный характер – государственные структуры не только не защищают персональные данные от утечки на черные рынки, а напротив – благоприятствуют данным событиям. Не всегда данные факты происходят целенаправленно, тем не менее – ситуация остается очень сложной. Принятый летом 2016 года противоречащий Конституции РФ так называемый «пакет Яровой» обязывает всех операторов связи хранить трафик всех граждан России в течение полугода и метаданные – в течение трех лет, делая эти данные легкой добычей для хакеров.

Таким образом, несмотря на постоянное совершенствование законодательной базы, регулирующей использование персональных данных, в государственных органах регулярно совершаются нарушения и преступления в отношении прав субъектов персональных данных. Наиболее часто выявляются следующие нарушения:

1) нормативным правовым актом государственного органа, регламентирующим порядок работы с персональными данными, не определена политика государственного органа в отношении обработки персональных данных, либо отсутствуют в учреждениях лица, ответственные за организацию обработки персональных данных;

2) государственными учреждениями запрашиваются избыточные сведения персонального характера;

3) в государственных учреждениях не соблюдается право субъекта персональных данных на получение информации, касающейся обработки его персональных данных;

4) в государственных учреждениях происходит обработка персональных данных в целях, не совместимых с целями, для которых они были изначально собраны и другие.

Правовые проблемы являются не единственными. Их сопровождают такие аспекты, как нехватка денежных средств на проведение работ по защите персональных данных, низкий уровень информатизации, недостаток квалифицированных сотрудников и т.д. Система защиты персональных данных в государственных учреждениях является комбинацией технических и технологических мер, а также мер по ее организации и администрированию. Общие технологические требования к обеспечению безопасности установлены действующим законодательством, однако в отношении организационных мер в законе ничего не сказано. Тем не менее, безопасность информационных систем возможна только в случае эффективной взаимосвязи технической и

[68] Тимиршаяхов, С.Ю. Правовые проблемы защиты информации при обработке персональных данных/ С.Ю. Тимиршаяхов, Ю.В. Тимиршаяхова // В сборнике: Правозащитная деятельность в современной России: проблемы и их решение Сборник научных трудов III Международной научно-практической конференции. – 2017. – С. 747.

организационной составляющей[69]. Как отмечается специалистами по информационной безопасности, камнем преткновения любой, даже самой технически совершенной, автоматизированной информационной системы являются профессионализм и ответственность обслуживающего ее персонала. При построении автоматизированных информационных систем необходимо учитывать человеческий фактор и иметь подсистему разграничения доступа к информации.

Нельзя не отметить и проблему правовой грамотности населения в сфере персональных данных. Нередко граждане, не осознавая последствий, добровольно предоставляют свои персональные данные и дают согласие на их обработку третьим лицам.

В качестве способов совершенствования деятельности по защите персональных данных можно рассмотреть следующие направления.

1. Во-первых, законодательно ограничить перечень сведений, запрашиваемых операторами или работодателями, а также срок хранения персональных данных и ввести обязательную процедуру их уничтожения после истечения срока хранения;

2. Во-вторых, обязать государственные учреждения вести процедуру ознакомления сотрудников с уровнем защиты и условиями обеспечения информационной безопасности персональных данных;

3. В-третьих, разработать систему безвозмездного предоставления каждому пользователю доступной электронной подписи, гарантирующей ее целостность и подлинность.

4. Кроме того, необходимо дополнительное финансирование защиты персональных данных в государственных учреждениях, а также необходимо обучение персонала на курсах повышения квалификации по информационной безопасности.

5. Повышение правовой грамотности населения и квалификации операторов, осуществляющих обработку персональных данных.

Перечисленные проблемы, в первую очередь носят системный характер и требуют решения органами исполнительной власти на федеральном и региональном уровнях. При принятии соответствующих мер выстроится гибкая универсальная система информационного обмена между государственными учреждениями, которая будет являться эффективным инструментом по повышению доступности и качества оказываемых государственных и муниципальных услуг населению.

Выводы по разделу 3

Основные особенности защиты персональных данных в государственных органах заключаются в том, что организация работы с персональными данными

[69] Крюкова, Д.Ю., Актуальные проблемы правового регулирования оборота и защиты персональных данных в России/ Д.Ю. Крюкова, Ю.В. Мокрецов // Вестник института: преступление, наказание, исправление. – 2017. – № 2 (38). – С. 35.

происходит по двум направлениям: персональные данные государственных служащих и персональные данные граждан. С учетом развития электронного правительства, особенно актуальными являются вопросы защиты накопленных данных граждан. В органах государственной власти для защиты данных в первую очередь создается модель угроз, и используется соответствующее программное обеспечение для защиты персональных данных. Однако анализ судебной практики демонстрирует, что нарушения прав субъектов персональных данных со стороны государственных учреждений продолжаются. Основными проблемами в данном случае являются такие, как отсутствие политики государственного органа в отношении обработки персональных данных либо отсутствуют лица, ответственные за организацию обработки персональных данных. Также государственными учреждениями запрашиваются избыточные сведения персонального характера, зачастую не соблюдается право субъекта персональных данных на получение информации, касающейся обработки его персональных данных.

Перечисленные проблемы, в первую очередь носят системный характер и требуют решения органами исполнительной власти на федеральном и региональном уровнях.

В качестве способов совершенствования деятельности по защите персональных данных можно предложить такие направления, как законодательное ограничение перечня сведений, запрашиваемых операторами или работодателями, срок хранения персональных данных. Следует ввести обязательную процедуру уничтожения персональных данных после истечения срока хранения и ряд других.

При принятии соответствующих мер выстроится гибкая универсальная система информационного обмена между государственными органами, которая будет являться эффективным инструментом по повышению доступности и качества оказываемых государственных и муниципальных услуг населению.

ЗАКЛЮЧЕНИЕ

Таким образом, по результатам исследования можно сделать ряд выводов.

Для российской действительности институт персональных данных является относительно новым. Он пришел из института тайны частной жизни, являясь адаптацией так называемого права быть оставленным в покое.

Зарубежный опыт и история становления института персональных данных в значительной степени сказались на тенденциях и особенностях развития данного института в России. Наша страна в полной мере восприняла международные тенденции. Был учтен зарубежный накопленный правовой опыт. Кроме того, значительное внимание было уделено общественным реалиям российской жизни, произошедшим политическим преобразованиям, а также общим актуальным направлениям развития права. Особенно стоит отметить, что в России с учетом национальных условий реализации правовых норм были использованы возможности изменения и преобразования ключевого акта международного уровня анализируемой сферы – 108 Конвенции Совета Европы о защите прав физических лиц в отношении персональных данных 1981 года. Данный факт подтверждает готовность государства и в дальнейшем развивать институт персональных данных и обеспечивать его эффективное функционирование.

Персональные данные представляют собой информацию, зафиксированную на любом материальном носителе о конкретном человеке, которая отождествлена или может быть отождествлена с ним. Нормативно-правовая база защиты персональных данных включает международное законодательство, Конституцию Российской Федерации, Федеральные законы, в том числе Федеральный закон от № 152–ФЗ «О персональных данных», Федеральный закон № 149–ФЗ «Об информации, информационных технологиях и о защите информации», различные подзаконные акты.

Институт персональных данных регулирует общественные отношения, относящиеся к нескольким отраслям права. С одной стороны он относится к публичной отрасли права, при этом его нормы находят свое отражение и в такой традиционно отнесенной к частному праву отрасли как трудовое. Следовательно, институт персональных данных регулирует отношения, находящиеся на стыке отраслей, поэтому его следует рассматривать как межотраслевой.

Сегодня законодатель определяет множество видов персональных данных: обезличенные, общедоступные, специальные и другие. Следует отметить, что информация, составляющая персональные данные неоднородна. Ее можно подразделить на номинативную и иную. Номинативной является информация, позволяющая идентифицировать конкретное лицо (фамилия, имя, отчество, пол, серия и номер паспорта, дата и место рождения и т. п.). К неноминативной относится информация о доходах, месте работы, политических убеждениях, медицинских заболеваниях, наличии судимости и т. п.

На основе проведенного анализа характеристика правового понятия «субъект персональных данных», можно сделать вывод, что любое физическое лицо, не зависимо от каких-либо критериев с наличием информации, является субъектом права. Правоотношения в сфере персональных данных являются личными

абсолютными правами человека. Проблематика заключается в том, что ФЗ «О персональных данных» не содержит конкретного, обобщенного, официально закрепленного понятия субъекта персональных данных. Действующий Закон не разграничивает участников правоотношений, не выделяет четких критериев

Оператор – физическое либо юридическое лицо, имеющее доступ к чужим персональным данным. Он самостоятельно может не проводить обработку персональных данных, а может являться только организатором этого процесса. Оператор отвечает за легитимность и качество процесса обработки персональных данных. Закон делит операторов на несколько категорий: физические лица, индивидуальные предприниматели, юридические лица, муниципальные органы, государственные органы. Субъект права – базовая категория права. Любое лицо является субъектом права, не приобретая этот статус самостоятельно и единовременно, а только из признания данного статуса государством. Говоря иначе, объем правосубъектности лица, который участвует в обороте персональных данных, определяется формулировкой положений законодательства. Данный факт положен в основу всего правореализационного процесса в сфере обработки персональных данных. На данный момент в связи с вышесказанным существует потребность законодательного закрепления точных характеристик и четких критериев, которые лягут в основу определения статуса оператора, осуществляющего обработку персональных данных.

Деление прав субъекта персональных данных производится на три категории. Они включают такие составляющие, как права субъекта персональных данных, которые он может реализовать до обработки, в процессе обработки данных и после их обработки. Помимо возможности отозвать свое согласие на обработку персональных данных субъект имеет еще целый ряд прав, о которых важно знать. В том числе лицо, чьи персональные данные обрабатываются, имеет право получать любую информацию, касающуюся этого, будь то данные оператора (его наименование и место нахождения), перечень обрабатываемых данных, сроки их обработки и хранения и др. Субъект, в чьих интересах ведется обработка персональных данных, имеет право обжаловать действие или бездействие оператора, осуществляемого данную обработку и т. д.

Оператор, который производит обработку персональных данных, должен выполнять ряд обязанностей. К их числу относятся: уведомление об обработке персональных данных соответствующего органа, обеспечение безопасности персональных данных при их обработке, получение согласия субъекта на обработку его персональных данных и другие.

Основные особенности защиты персональных данных в государственных органах заключаются в том, что организация работы с персональными данными происходит по двум направлениям: персональные данные государственных служащих и персональные данные граждан. С учетом развития электронного правительства, особенно актуальными являются вопросы защиты накопленных данных граждан. В органах государственной власти для защиты данных в первую очередь создается модель угроз, и используется соответствующее программное обеспечение для защиты персональных данных. Однако анализ судебной

практики демонстрирует, что нарушения прав субъектов персональных данных со стороны государственных учреждений продолжаются. Наиболее часто выявляются следующие нарушения:

1) нормативным правовым актом государственного органа, регламентирующим порядок работы с персональными данными, не определена политика государственного органа в отношении обработки персональных данных, либо отсутствуют в учреждениях лица, ответственные за организацию обработки персональных данных;

2) государственными учреждениями запрашиваются избыточные сведения персонального характера;

3) в государственных учреждениях не соблюдается право субъекта персональных данных на получение информации, касающейся обработки его персональных данных;

4) в государственных учреждениях происходит обработка персональных данных в целях, не совместимых с целями, для которых они были изначально собраны и другие.

В качестве способов совершенствования деятельности по защите персональных данных можно рассмотреть следующие направления.

1. Во-первых, законодательно ограничить перечень сведений, запрашиваемых операторами или работодателями, а также срок хранения персональных данных и ввести обязательную процедуру их уничтожения после истечения срока хранения;

2. Во-вторых, обязать государственные учреждения вести процедуру ознакомления сотрудников с уровнем защиты и условиями обеспечения информационной безопасности персональных данных;

3. В-третьих, разработать систему безвозмездного предоставления каждому пользователю доступной электронной подписи, гарантирующей ее целостность и подлинность.

4. Кроме того, необходимо дополнительное финансирование защиты персональных данных в государственных учреждениях, а также необходимо обучение персонала на курсах повышения квалификации по информационной безопасности.

5. Повышение правовой грамотности населения и квалификации операторов, осуществляющих обработку персональных данных.

Перечисленные проблемы, в первую очередь носят системный характер и требуют решения органами исполнительной власти на федеральном и региональном уровнях. При принятии соответствующих мер выстроится гибкая универсальная система информационного обмена между государственными органами, которая будет являться эффективным инструментом по повышению доступности и качества оказываемых государственных и муниципальных услуг населению.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6–ФКЗ, от 30.12.2008 № 7–ФКЗ, от 21.07.2014 № 11–ФКЗ). // Собрание законодательства РФ. – 2014. – № 31. – ст. 4398.
2. «Всеобщая декларация прав человека» (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета – 1995. – № 67.
3. Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS № 108) (заключена в г. Страсбурге, 28 января 1981 г.). // Бюллетень трудового и социального законодательства РФ. – 2014. – № 4.
4. Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. // СЗ РФ. – 2001. – № 2.
5. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14–ФЗ (ред. от 23.05.2018) // Российская газета. – № 23 – № 27.
6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195–ФЗ (ред. от 23.04.2018) // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – ст. 1.
7. Трудовой кодекс Российской Федерации от 30.12.2001 № 197–ФЗ (ред. от 05.02.2018) // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – ст. 3. 93
8. Уголовный кодекс Российской Федерации от 13.06.1996 № 63–ФЗ (ред. от 23.04.2018) // Российская газета. – 1996. – № 113–№ 118.
9. Закон РФ от 21.07.1993 № 5485–1 «О государственной тайне» (ред. от 26.07.2017) // Российские вести. – 1993. – № 189.
10. Федеральный закон от 20.02.1995 № 24–ФЗ «Об информации, информатизации и защите информации» // Российская газета. – 1995. – № 39.
11. Федеральный закон от 27.07.2004 № 79–ФЗ «О государственной гражданской службе Российской Федерации» (ред. от 28.12.2017) // Российская газета. – 2004. – № 12.
12. Федеральный закон от 15.07.1995 № 101–ФЗ «О международных договорах Российской Федерации» (ред. от 12.03.2014) // Российская газета. – 1995. – № 140.
13. Федеральный закон от 12.08.1995 № 144–ФЗ «Об оперативно-розыскной деятельности» (ред. от 06.07.2016 № 374–ФЗ) // Российская газета. – 1995. – № 160.
14. Федеральный закон от 19.12.2005 № 160–ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // Собрание законодательства РФ. – 2005. – № 52 (1 ч.) – ст. 5573.
15. Федеральный закон от 27.07.2006 № 152–ФЗ «О персональных данных» (ред. от 29.07.2017) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – ст. 3451. 94

16. Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 23.04.2018) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – ст. 3448.
17. Федеральный закон от 27.12.2002 № 184–ФЗ «О техническом регулировании» (ред. от 29.07.2017) // Российская газета. – 2002. – № 245.
18. Федеральный закон от 07.07.2003 № 126–ФЗ «О связи» (ред. от 18.04.2018) // Собрание законодательства РФ. – 2003. – № 28. – ст. 2895.
19. Федеральный закон от 29.07.2004 № 98–ФЗ «О коммерческой тайне» (ред. от 18.04.2018) // Собрание законодательства РФ. – 2004. – № 32. – ст. 3283.
20. Федеральный закон от 22.10.2004 № 125–ФЗ «Об архивном деле в Российской Федерации» (ред. от 28.12.2017) // Собрание законодательства РФ. – 2004. – № 43. – ст. 4169.
21. Указ Президента РФ от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» (ред. от 01.07.2014). // Российская газета. – 2005. – № 120.
22. Распоряжение Президента РФ от 10.07.2001 № 366–рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных». // Собрание законодательства РФ. – 2001. – № 29. – ст. 3011.
23. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Российская газета. – 2008. – № 200. – Ст. 95.
24. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Российская газета. – 2012. – № 256.
25. Определение Приморского краевого суда от 14.07.2014 по делу № 33–5960 // Справочно-правовая система «КонсультантПлюс».
26. Постановление Верховного Суда РФ от 7 октября 2013 г. № 94–АД13–1// Справочно-правовая система «КонсультантПлюс».
27. Постановления Верховного Суда РФ от 4 марта 2016 г. № 307–АД15–18844// Справочно-правовая система «КонсультантПлюс».
28. Постановление Федерального арбитражного суда Северо-Кавказского округа от 21 апреля 2014 г. № Ф08–1921/14 по делу № А53–13327/2013// Справочно-правовая система «КонсультантПлюс».
29. Постановление от 18 мая 2016 г. по делу № 5–454/2016 //Справочно-правовая система «КонсультантПлюс».
30. Абаев, Ф.А. Историко-правовые предпосылки формирования и современные тенденции развития института персональных данных в трудовом праве / Ф.А. Абаев// Пробелы в российском законодательстве. Юридический журнал. – 2013. – С. 122–126.

31. Авакьян, С. А. Конституционное право России. Учебный курс: учеб. пособие/ С.А. Авакьян. – М.: Норма, 2014. – 864 с.
32. Алексеев, С.С. Государство и право: учебное пособие/ С.С. Алексеев. – М.: Проспект, 2015. – 152 с.
33. Алямкин, С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты/ С.Н. Алямкин // Мир науки и образования. – 2016. – № 4 (8). – С. 4.
34. Власов, Д.С. Защита персональных данных в автоматизированных системах обработки информации органов государственной власти / Д.С. Власов // Успехи современной науки. – 2016. – Том 8. – № 12. – С. 33-36.
35. Вышеславова, Т.Ф. Дифференциация персональных данных работников // НаукаПарк. – 2015. – № 9 (39). – С.133-139.
36. Гиляров, Е.М. Основные направления международно-правового регулирования отношений в сфере персональных данных / Е.М. Гиляров, А.А. Воронина// Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2013. – № 4-1 (30). – С. 58-62.
37. Гуде, С.В. Защита персональных данных в Российской Федерации: исторический аспект и современное состояние / С.В. Гуде, П.В. Арбузов, А.Г. Карпика // Юристъ-Правоведъ. – 2015. – № 2 (69). – С. 93-97.
38. Егошина, Г.Г. Модернизация конституционно-правового регулирования защиты персональных данных в Европе: усиление региональной интеграции / Г.Г. Егошина // Теория и практика общественного развития. – 2014. – № 3. – С.156–159.
39. Исакова, Л.В. Международно-правовое регулирование защиты персональных данных работников / Л.В. Исакова, К.Е. Статуева// Новый университет. Серия: Экономика и право. – 2015. – № 4. – С. 39-44.
40. Керимова, Е.А. Правовой институт: автореф. дис. … канд. юрид. наук./ Е.А. Керимова. – Саратов, 1998. – 126 с.
41. Кривогин, М.С. Правовой режим биометрических персональных данных/ М.С. Кривогин// Проблемы современной науки. – 2015. – № 10 (40) – С. 126-129.
42. Крюкова, Д.Ю., Актуальные проблемы правового регулирования оборота и защиты персональных данных в России/ Д.Ю. Крюкова, Ю.В. Мокрецов // Вестник института: преступление, наказание, исправление. – 2017. – № 2 (38). – С. 34-38.
43. Кучеренко, А.В. Понятие и признаки оператора, осуществляющего обработку персональных данных /А.В. Кучеренко // Альманах современной науки и образования. Тамбов: Грамота. – 2009. – №12 (31). – Ч.2. – С. 59-60.
44. Латухина, В.С. Международные и национальные стандарты уголовно-правовой защиты персональных данных/ В.С. Латухина // Экономика. Социология. Право. – 2017. – № 4. – С. 76-80.

45. Параскевов, А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом/ А.В. Параскевов // Научный журнал КубГАУ. – 2015. – № 110(06). – С. 2–15.
46. Саматов, К.М. Персональные данные как институт права/К.М. Саматов// В сборнике: Новые вопросы в современной науке Материалы Международной (заочной) научно-практической конференции. под общей редакцией А.И. Вострецова. – 2017. – С. 296-301.
47. Сергиевич, В.А. Проблемы становления и развития института «право быть забытым»/ В.А. Сергиевич, И.В. Шугурова//Отечественная юриспруденция. – 2016. – № 12 (14). – С. 18-20.
48. Терещенко, Л.К. Модернизация информационных отношений и информационного законодательства: монография/ Л.К. Терещенко. – М.: НИЦ ИНФРА-М: ИЗиСП, 2013. – 227 с.
49. Тимиршаяхов, С.Ю. Правовые проблемы защиты информации при обработке персональных данных/ С.Ю. Тимиршаяхов, Ю.В. Тимиршаяхова // В сборнике: Правозащитная деятельность в современной России: проблемы и их решение Сборник научных трудов III Международной научно-практической конференции. – 2017. – С. 747–750.
50. Усманова, Е.Ф. Проблемы и особенности формирования правовой культуры в современном правовом государстве / Е.Ф. Усманова// Инновационные тенденции, социально-экономические и правовые проблемы взаимодействия в международном пространстве. Саранск. – 2016. – С. 235–237.
51. Обработка персональных данных государственных гражданских служащих. – https://www.pro-personal.ru/article/1083852-qqe-m12-obrabotka-personalnyh-dannyh-gosslugagih
52. Обязанности оператора при обработке персональных данных. – http://www.garant.ru/actual/persona/obyazannosti/#ixzz5EKshkqBU
53. Отчеты о деятельности Уполномоченного органа по защите прав субъектов персональных данных. – https://rkn.gov.ru/personal-data/reports/

ПРИЛОЖЕНИЕ А

Сведения о количестве плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных[70] Динамика представлена на рисунке А.1.

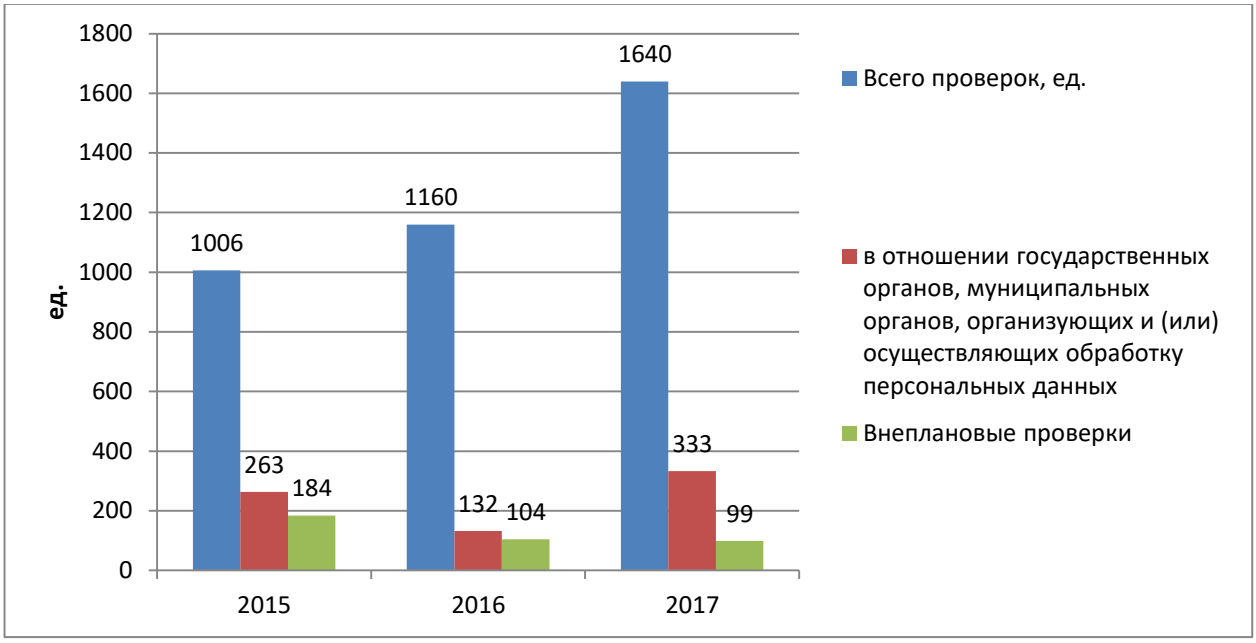

Рисунок А.1 – Динамика числа плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных

[70] По данным Отчета о деятельности Уполномоченного органа по защите прав субъектов персональных данных [Электронный ресурс]/ Режим доступа https://rkn.gov.ru/personal-data/reports/

ПРИЛОЖЕНИЕ Б

Сведения о количестве выданных предписаний в результате плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных [71]

Динамика представлена на рисунке Б.1.

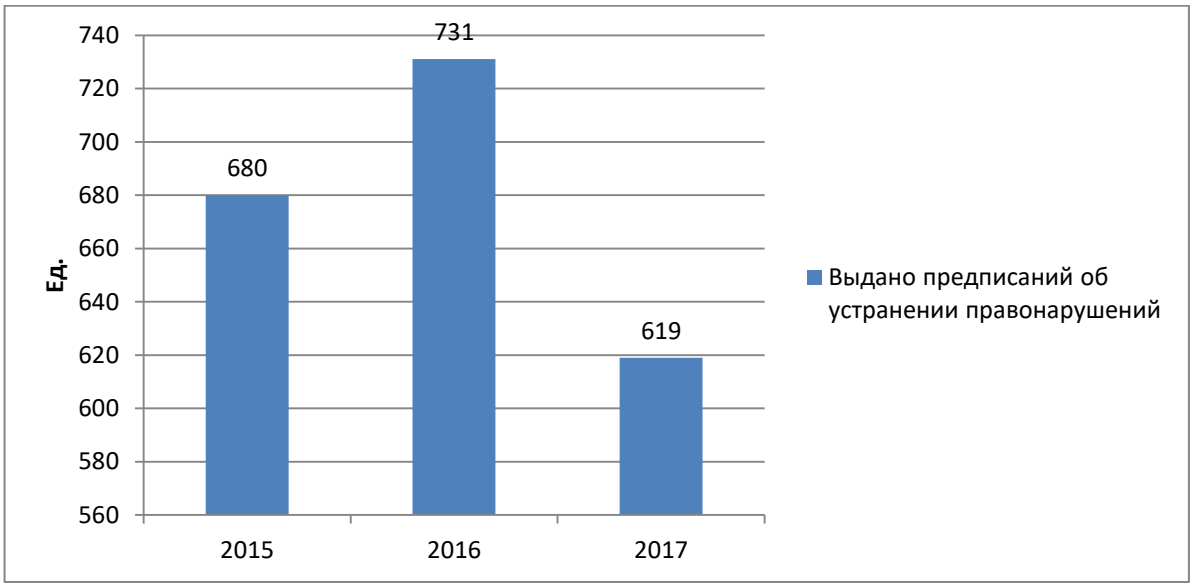

Рисунок Б.1 – Динамика числа выданных предписаний в результате плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных

[71] По данным Отчета о деятельности Уполномоченного органа по защите прав субъектов персональных данных [Электронный ресурс]/ Режим доступа https://rkn.gov.ru/personal-data/reports/

ПРИЛОЖЕНИЕ В

Сведения о количестве административных протоколов, направленных в суды по результатам плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных [72]

Динамика представлена на рисунке В.1.

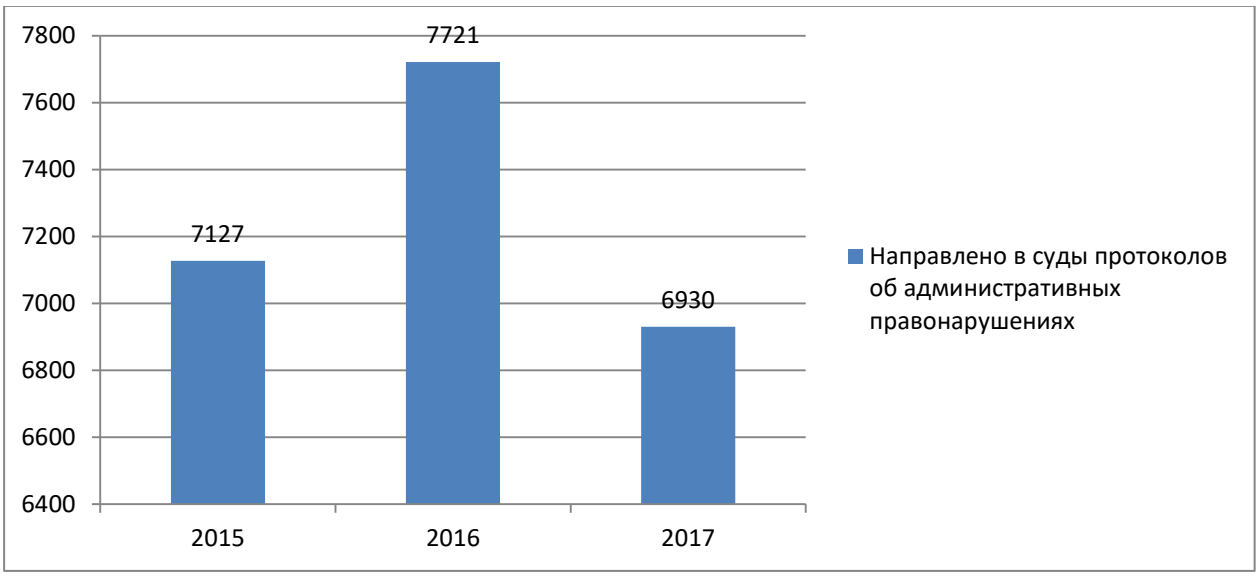

Рисунок В.1 – Динамика числа административных протоколов, направленных в суды по результатам плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных

[72] По данным Отчета о деятельности Уполномоченного органа по защите прав субъектов персональных данных [Электронный ресурс]/ Режим доступа https://rkn.gov.ru/personal-data/reports/

ПРИЛОЖЕНИЕ Г

Сведения о сумме наложенных административных штрафов по результатам плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных [73]

Динамика представлена на рисунке Г.1.

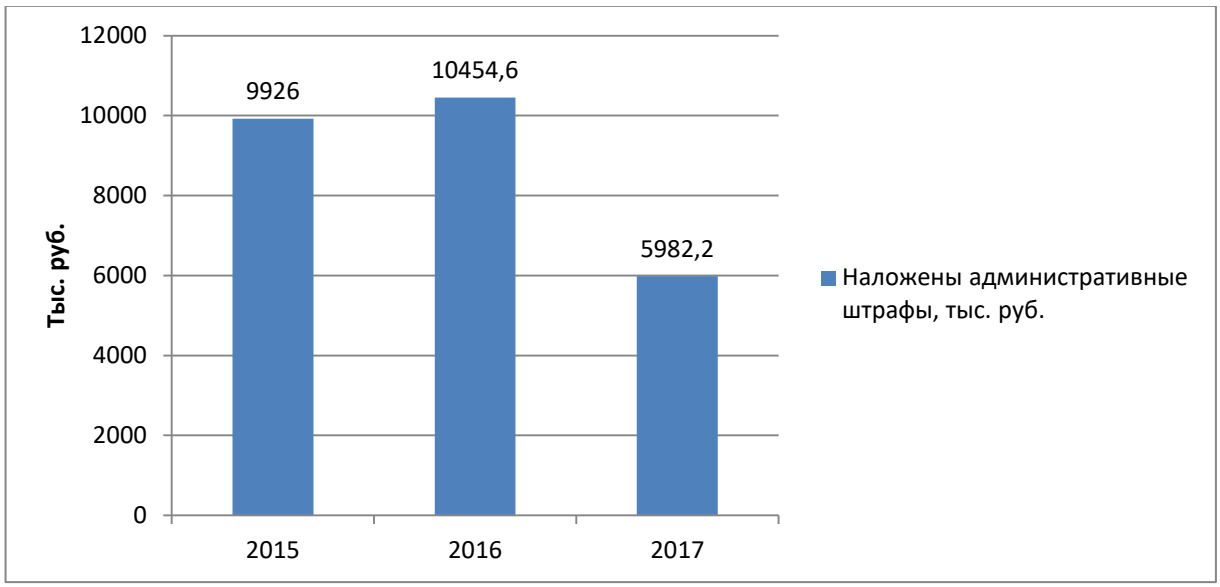

Рисунок Г.1 – Динамика суммы наложенных административных штрафов по результатам плановых и внеплановых проверок, проведенных Роскомнадзором в области защиты прав субъектов персональных данных

[73] По данным Отчета о деятельности Уполномоченного органа по защите прав субъектов персональных данных [Электронный ресурс]/ Режим доступа https://rkn.gov.ru/personal-data/reports/