МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение государственного управления и местного самоуправления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Защита персональных данных в праве России: конституционно-правовой аспект

Студент Т.Е. Карташева
(И.О. Фамилия) (личная подпись)

Научный руководитель к.ю.н. В.В. Романова
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

Актуальность темы исследования. В современном мире идет постоянная работа по контролю за соблюдением прав человека, однако, важным моментом является при осуществлении одного права не нарушить другое. Научно-технический прогресс оказывает неоднозначное воздействие на права человека. Развитие современных технологий дает возможность предоставлять одни права, при этом создавая новые возможности для нарушения других, прежде всего, конституционного права гражданина «на неприкосновенность частной жизни, личную и семейную тайну» [4], закрепленное Конституцией Российской Федерации.

Право на неприкосновенность частной жизни в общем представляет собой сложный правовой институт, сочетающий в себе индивидуальные права человека, которые необходимо защищать в правовом аспекте. Конституционное право на неприкосновенность частной жизни по своему нормативному содержанию означает «неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» [4]. Развитие общественных отношений в информационной сфере сформировало новый элемент в структуре конституционного права на неприкосновенность частной жизни – права на защиту персональных данных.

Национальная безопасность Российской Федерации по большому счету зависит от обеспечения информационной безопасности, под которой понимается состояние защиты ее национальных интересов в информационной сфере, определяемое совокупностью сбалансированных интересов личности, общества и государства. В настоящее время идет активное развитие информационных технологий, создание глобальных телекоммуникационных сетей, рост скорости передачи и обработки данных, формирование электронных баз персональных данных граждан.

Базы данных о субъектах становятся предметом контроля и управления. Широкое развитие получили устройства для прослушивания, видеонаблюдение, анкетирование, тестирование и опросы. Информация о человеке рассматривается как товар. Все сведения накапливаются в электронном виде. Хранятся различные факты о человеке, о его внешности, местах пребывания, интересах, круге общения. Такие данные могут использоваться как в мирных целях, так и в преступных.

Экспертно-аналитическим центром InfoWatch было проведено исследование утечек информации. В 2019 году было зафиксировано 395 случаев утечки данных из российских компаний, а также государственных органов. Это составляет 15,7% от числа утечек данных по всему миру. В результате утечек под угрозой оказались более 172 миллионов записей персональных данных и платежной информации. По сравнению с результатами прошлого года число утечек увеличилось на 46%, а объем атакованных персональных данных вырос более чем в 6 раз. В течение семи лет Россия занимает второе место после США по объему утечек данных. В 72,1% случаев виновными в утечке информации оказались сотрудники этих же компаний, в 4,6% случаев – топ-менеджмент организаций, в 18,4% – хакеры и неизвестные лица, таким образом, подавляющее количество утечек было совершено внутренним нарушителем [37]. Персональные данные, которые были взломаны используются в различных мошеннических схемах – при оформлении кредитов, оплате товаров в Интернете и так далее.

Таким образом, в современных условиях люди теряют контроль над информацией о себе, своей личной и семейной жизни. Следовательно, интересы личности в отношении информационной безопасности должны быть выражены не только в законодательстве, но и в обеспечении реализации и эффективной защиты конституционных прав человека и гражданина на неприкосновенность частной жизни, на личную и семейную тайну при обработке персональных данных.

Факт конституционного признания права личности на неприкосновенность частной жизни – это недостаточная мера для его полной реализации в жизни. Необходимо обеспечить эффективную, прежде всего государственную защиту этого конституционного права. Эта защита должна быть выражена в деятельности уполномоченных государственных органов и должностных лиц по уважению, обеспечению и защите прав и свобод гражданина, выступающих в качестве основы правозащитного механизма.

Интеграция России в международное сообщество, глобализация экономических и социальных процессов, развитие информационных и телекоммуникационных технологий и преемственность России в области законодательства о неприкосновенности частной жизни и защите персональных данных обусловили необходимость изучения вопросов в рамках конституционно-правовых исследований в России и других странах.

Вышеизложенные обстоятельства определяют актуальность, теоретическую и практическую значимость диссертационного исследования, структуру и содержание рассматриваемых вопросов.

Степень научной разработанности темы исследования. В настоящий момент существует не так много научных работ по защите персональных данных, рассматриваемых именно в конституционно-правовом аспекте.

Ученые, занимающиеся исследованиями теоретических основ содержания конституционного права на неприкосновенность частной жизни, а также проводившие анализ действующего законодательства в данной сфере: В.В. Барбин, В.Н. Блоцкий, Н.Н. Волошкина, М.А. Грачева, В.В. Лазарев, Н.П. Лепешкин, Е.А. Миндрова, П.В. Несмелов, М.С. Петросян, И.Л. Петрухин, Д.З. Поливанова, А.В. Преснякова, И.В. Смолькова, Е.А. Филимонова и другие.

В процессе настоящего исследования изучены диссертационные работы Н.Г. Белгородцевой, Я.В. Кудашкина, Т.Д. Логиновой, М.И. Проскуряковой, Е.Ш. Рассоловой, И.С. Садиковой, Э.В. Талапиной, Ю.С.

Телиной, А.С. Федосина, М.А. Хурум, Э.А. Цадыковой, А.А. Чеботаревой и других, в которых рассматривались вопросы реализации конституционного права на неприкосновенность частной жизни.

Существующие работы в основном направлены на сравнительный анализ законодательства Российской Федерации и зарубежных стран в части защиты персональных данных или на общее теоретическое описание проблем защиты персональных данных, что во многом предопределило цели, задачи и методологические основы представленных диссертационных исследований.

Объектом исследования являются общественные отношения, возникающие в процессе формирования, реализации и защиты конституционного права гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России.

Предметом исследования являются конституционно-правовые нормы, регулирующие общественные отношения в сфере конституционного права на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных, положения, определяющие понятие персональных данных, их виды, принципы и условия обработки, правовое положение субъектов персональных данных, положения о правовой безопасности обработки персональных данных.

Целью исследования является комплексный анализ существующих нормативно-правовых актов, регулирующих отношения в области защиты персональных данных, выявление проблем при обработке персональных данных и совершенствование действующего законодательства.

Для достижения вышеуказанной цели были поставлены следующие **задачи:**

– изучить российское законодательство в области защиты персональных данных;

– провести обзор и анализ законодательства в области защиты персональных данных иностранных государств;

– проанализировать юридическую ответственность и судебную практику России в сфере защиты персональных данных;

– изучить обработку, защиту персональных данных и правовое регулирование в организациях, а также сети Интернет;

– внести предложения по изменению в нормативные правовые акты, регулирующие конституционное право на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных.

Методологическая основа исследования. В диссертации использовались общенаучные методы, частно-научные методы такие как формально-правовые – изучение правовой природы и анализ содержания конституционного права на неприкосновенность частной жизни; сравнительно-правовые – изучение состояния правового обеспечения формирования конституционного права на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах.

Практическая значимость исследования состоит в возможности использования его результатов при преподавании дисциплины «Конституционное право России», проведении дальнейших научных исследований, правотворческой деятельности.

Структура работы состоит из введения, трех глав, заключения, списка используемой литературы и используемых источников. Список используемой литературы и используемых источников включает 52 наименований, 9 из них были переведены с английского языка.

Глава 1 Конституционно-правовое регулирование персональных данных

1.1 Понятие персональных данных и защиты персональных данных

Согласно Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], «персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)» [39]. Из данного определения понятно следующее: к персональным данным относятся, к примеру, фамилия, имя, отчество, дата рождения, место рождения, место жительства, паспортные данные, номер телефона, семейное положение, религиозные убеждения, сведения о доходах, политические убеждения и другое.

Персональные данные сейчас используются практически везде: в банковской отрасли, в поликлиниках и больницах, а также школах и детских садах, университетах и других различных организациях. Из-за глобальной компьютеризации, широкого распространения электронного документооборота, практически подавляющее большинство государственных и частных организаций стали хранить и обрабатывать персональные данные в электронном виде. Это одновременно гораздо упрощает работу с большим количеством документов, но и подвергает опасности использования персональных данных преступниками в незаконных целях. В настоящий момент участились случаи взламывания баз данных различных организаций и утечек персональных данных работников или клиентов этих организаций. Мошенники используют компьютерные вирусы и похищают логины, пароли, а также данные банковских карт, более того, данные паспортов и водительских удостоверений. Особенно подвержены краже данные пользователей Интернет-магазинов, социальных сетей, онлайн-банкингов.

Обеспечить безопасность персональных данных при их обработке – это значит при хранении или обработке персональных данных не допустить такой ситуации, при которой будет возможным каким-либо образом скопировать, удалить или изменить персональные данные. Обеспечить эту безопасность, согласно Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], должен «оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными» [39]. Для достижения условия защищенности персональных данных разрабатываются и осуществляются определенные мероприятия по обеспечению их безопасности.

Обеспечение конфиденциальности персональных данных – это задача как всего государства, так и каждого пользователя в отдельности. Государство должно предоставить защиту персональных данных, потому что, согласно Конституции Российской Федерации [4], «каждый имеет 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» [4]. «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» [4]. Получается, что государство должно обеспечивать защиту данных своих граждан указанных сфер жизни от использования этих данных без их на то согласия. Если же государство не в силах защитить персональные данные каждого гражданина, оно не обеспечивает выполнение указанных положений Конституции Российской Федерации [4]. Также задачей государства является противостояние мошенникам и поиск новых путей решения и методик обеспечения безопасности персональных данных своих граждан. Данная тема

довольно динамична, мошенники изобретают каждый раз новые способы обхода средств защиты персональной информации на электронных носителях. Кроме того, и законодательство должно быть актуальным, своевременно обновляться, информация крайне быстро становится неактуальной, нужно искать и применять все новые и новые пути и способы решения данной проблемы. Одновременно с этим, если каждый гражданин будет халатно относиться к пользованию своих персональных данных, одно только государство с данной задачей не справится. Во-первых, человеку нужно быть грамотным и бдительным, когда он работает за компьютером или пользуется смартфоном. Нельзя скачивать сомнительные приложения из недостоверных источников, переходить по неизвестным неподтвержденным Интернет-ссылкам. Также нужно периодически обновлять свои пароли для доступа в Интернет-банки, социальные сети, выходить из личного аккаунта или своей электронной почты при завершении работы, использовать антивирусные программы, не сообщать свои персональные данные по телефону людям, которых человек не знает. Работники организаций должны обеспечить надежную защиту своих баз данных, своевременно проходить обучающие курсы и применять актуальное законодательство на практике. Для того, чтобы борьба с киберпреступностью была эффективной и для обеспечения защиты персональных данных каждый гражданин, каждая организация и все государство в целом должны слаженно действовать.

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] персональные данные могут быть классифицированы по степени секретности, сложности их сбора, возможности применения их третьим лицом. Они делятся на следующие виды:

- общие,
- биометрические,
- специальные,
- обезличенные.

Общие данные относятся к личной информации, которая формирует основные данные о носителе:

- фамилия, имя, отчество,
- место регистрации и проживания,
- паспортные данные,
- информация о наличии образования,
- сведения о месте работы,
- информация о полученных доходах и так далее.

Не все данные общего характера, взятые отдельно, можно отнести к информации о человеке, которая может считаться личной. Например, закон не содержит определенных толкований относительно того, можно ли считать телефонный номер физического лица одним из компонентов персональных данных. Пояснения в Роскомнадзоре показывают, что эти данные не являются информацией, которая позволила бы точно идентифицировать лицо, номер не является персональным. Но при использовании вместе с именем, фамилией, пропиской он составляет персональные данные.

Информация о человеке, которая является общей, указывается в паспорте, она заносится в военный билет, в диплом, а также в личную карточку сотрудника компании, трудовую книжку. Для использования такой информации не требуется получать от сотрудника письменного разрешения. Достаточно, чтобы лицо косвенно, поставив галочку в соответствующей графе, подтвердило право на такие действия получателю этой информации в письменном виде или онлайн-заявке.

Получение таких персональных данных очень просто, а это часто приводит к проблемам: начинаются рассылки навязчивых рекламных предложений или попытки шантажировать, подделывать кредитные заявки и многое другое.

Существуют персональные данные, которые характеризуют носителя по биологическому и физиологическому принципу. Они включают в себя:

– дактилоскопические параметры,
– анализ ДНК,
– группу крови,
– рост, цвет глаз, вес и многое другое.

Биометрические персональные данные включают информацию, полученную в результате видео- и фотосъемки с участием человека. Биометрические данные чаще всего востребованы во время лечения, при подаче заявления на работу в государственные органы, при изготовлении загранпаспортов и визовых документов. Эти данные могут быть обработаны, если у оператора есть письменное согласие от субъекта персональных данных на их обработку. «Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате» [39].

К специальным персональным данным относятся сведения, касающиеся «расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни» [39]. Эту информацию можно найти в личных файлах, медицинских записях. Они необходимы во время политических событий и используются при поступлении на службу в вооруженные силы. Для того,

чтобы третьи лица могли получить доступ и использовать эту личную информацию, требуется получить разрешение у ее владельца.

К обезличенным данным относятся общедоступные персональные данные. Такие сведения легко найти в адресных книгах, справочных документах и средствах массовой информации. Информация, которая является общедоступной, может быть легко использована заинтересованными лицами. Данные о финансовом положении политиков, государственных служащих и должностных лиц высшего звена являются общедоступными. Общедоступные персональные данные – это также те данные, которые содержатся в профилях социальных сетей, на различных сайтах объявлений. При этом владелец площадки становится оператором, ответственным за обработку данных своих пользователях.

В настоящее время принят закон, при котором граждане могут требовать удаление общедоступных персональных сведений. Лица могут устанавливать определенные условия использования таких сведений, а также запрещать передавать эти данные третьим лицам.

Кроме того, операторам запрещается размещать и распространять эти персональные данные при отсутствии согласия. К тому же, согласие требуется на каждое действие, например, передача сведений третьим лицам, размещение в открытом доступе. Невозможно получать согласие «по умолчанию», то есть просто потому, что человек заполнил свой профиль. Данное согласие на обработку персональных данных может даваться прямо оператору, либо через специальную информационную систему Роскомнадзора. Более того, операторы обязаны удалять по требованию профили их владельцев.

Оператор, которому лица предоставляют персональные сведения о себе, обязан получить разрешение на определенные действия, к примеру, на размещение данных в открытом доступе, на передачу данных третьим лицам.

До недавнего времени граждане давали разрешение на действия со своими данными, поставив одну отметку рядом с пунктом «согласен на

обработку персональных данных». Но теперь необходимо будет уточнять, какие именно данные можно публиковать, а также передавать сторонним организациям. Получается, что пользователь может устанавливать свои условия этой обработки, а также запрещать передавать персональную информацию о себе. Таким образом, граждане будут задумываться, прежде чем поставить согласие на обработку своих персональных данных и не будут публиковать о себе слишком много личной информации. Кроме этого, компаниям запрещается собирать общедоступные персональные данные из профилей социальных сетей.

Безусловно, для организаций это существенно усложняет обработку общедоступных персональных данных.

Данный закон вступил в силу 1 марта 2021 года и должен распространяться на все организации, которые работают на российском рынке.

1.2 Систематизация законодательства о персональных данных

Вопросы по соблюдению конфиденциальности персональных данных в последние годы остаются неизменными и поднимаются как в России, так и за рубежом, потому что они касаются всех граждан, независимо от их национальности и положения.

В 1981 году была принята Конвенция Совета Европы № 108 «О защите физических лиц при автоматизированной обработке персональных данных» [48], которая в 2001 году была ратифицирована Российской Федерацией. Уже тогда данный документ заложил международную основу для выполнения обработки персональных данных согласно законодательству и продолжает применяться в настоящее время: использование персональных данных только в конкретных целях и в конкретные сроки, неизбыточность и актуальность персональных данных, подвергающихся обработке, нюансы трансграничной передачи данных, защита данных, а также права граждан – владельцев

персональных данных, которые им гарантированы. Также в данном документе содержится определение персональных данных, которое было размещено в первой редакции Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39]. Согласно документу, «персональные данные означают любую информацию об определенном или поддающемся определению физическом лице (субъект данных)» [48]. После выполнения международных нормативных требований в 2012 году Россия присоединилась к Всемирной торговой организации, что с являлось целью ратификации данной Конвенции.

Страны-участницы Конвенции Совета Европы № 108 «О защите физических лиц при автоматизированной обработке персональных данных» ведут общую деятельность. В 2018 году был подписан «Протокол № 223 о внесении изменений в Конвенцию Совета Европы о защите персональных данных» [29]. Изменения учитывали появление современных технологий в области персональных данных, например, биометрическая и генетическая защита данных, новые права физических лиц в контексте алгоритмического принятия решений искусственным интеллектом, требования по защите данных на стадии моделирования информационных систем, а также обязанность ставить в известность уполномоченный надзорный орган об утечках. Граждане теперь вправе получать квалифицированную защиту своих персональных данных от надзорного органа, а российские компании, которые должны соблюдать требования европейских норм GDPR (General Data Protection Regulation – Общий регламент по защите данных), избавятся от необходимости применять дополнительные меры защиты, так как соблюдение Конвенции Совета Европы № 108 «О защите физических лиц при автоматизированной обработке персональных данных» [48] означает, что государство-участник уже в состоянии обеспечить адекватный правовой режим для защиты персональных данных.

Основным нормативным актом в области персональных данных является, прежде всего, Конституция Российской Федерации от 12 декабря

1993 года [4]. Этот документ определяет информацию о лице, которая должна быть защищена законом от наиболее общей формы нарушения. Согласно Конституции Российской Федерации, «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» [4]. А также «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» [4].

Вторым по значимости документом в области персональных данных является Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39]. Данный документ имеет схожие пункты с Конвенцией [48], но также введены дополнительные определения и требования, касающиеся обработки персональных данных. С момента издания, в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» были внесены изменения, а именно, уточнены основные постулаты о защите персональных данных, а также была запрещена первичная обработка персональных данных за пределами территории Российской Федерации. Это базовый закон, раскрывающий понятие персональных данных, дающий представление о том, как обращаться с персональными данными государственным и муниципальным учреждениям, организациям, используя или не используя средства автоматизации. Он определяет права субъекта персональных данных, обязанности оператора, а именно принципы и условия обработки персональных данных, раскрывает понятие конфиденциальности персональных данных и согласие на обработку, а также концепцию государственного контроля за обработкой персональных данных.

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [38] регулирует отношения, возникающие при обработке информации, определяет обязанности оператора, государства при работе с персональными данными и информационными системами, порядок ограничения доступа к информации.

Данный документ регулирует порядок работы с различной информацией в России, в том числе, с персональными данными. Документ содержит основные понятия и определения, используемые во всех правовых актах, связанных с защитой информации, и, среди прочего, вводит понятие информационных категорий и видов информации.

В частности, персональные данные классифицируются как информация ограниченного доступа. Согласно Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [38], «обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами» [38], поэтому государство устанавливает обязательные стандарты и правила ее обработки. К сожалению, не все виды информации с ограниченным доступом имеют такое конкретное значение - например, до сих пор нет законодательного классификатора видов тайн, можно выделить только некоторые из них: государственная, коммерческая, налоговая, банковская, аудиторская, медицинская, нотариальная, адвокатская тайна, тайна связи, следственная, судебная, инсайдерская информация и так далее [31, с. 61]. Кроме информации ограниченного доступа, в Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [38] существует еще и классификатор видов информации, доступ к которой не может быть ограничен – например, нормативные правовые акты, информация о деятельности государственных органов, состоянии окружающей среды и так далее.

Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера» [36] определяет перечень сведений, отнесенных к категории конфиденциальных.

Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [17] определяет особенности обработки персональных

данных, осуществляемой без использования средств автоматизации, меры по обеспечению безопасности персональных данных при такой обработке.

Постановление Правительства Российской Федерации от 6 июля 2008 года № 512 «Об утверждении Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» [18] устанавливает требования к материальному носителю биометрических персональных данных, его хранению, а также обязанностям, возложенным на оператора.

Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [16] установлены требования к защите персональных данных при их обработке в информационных системах и уровни безопасности данных, определены понятие информационной системы, угрозы безопасности, требования к защите от различных видов угроз.

Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 14 ноября 2011 года № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требований законодательства Российской Федерации в области персональных данных» [24] утверждает Административный регламент, которому Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций должна следовать при проверке обработки персональных данных на соответствие законодательству.

Постановление Правительства Российской Федерации от 13 февраля 2019 года № 146 «Об утверждении Правил организации и осуществления

государственного контроля и надзора за обработкой персональных данных» [22] определяет порядок организации, а также проведения плановых и внеплановых проверок лиц, являющихся операторами персональных данных, устанавливает их права, обязанности и ответственность.

Постановление Правительства Российской Федерации от 21 марта 2012 года № 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» [19], определяет перечень мер по обеспечению исполнения обязательств, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] (назначение распорядителя).

Статья 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] касается мер по обеспечению безопасности персональных данных. В данной статье определено, в частности, что «операторы должны обеспечивать уровни защиты персональных данных, установленные Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [16], что означает определенный набор требований по нейтрализации определенных угроз безопасности. Для моделирования этих угроз, то есть построения модели угрозы и модели преступника, необходимо опираться на следующие законодательные акты:

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,

– «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных

системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности».

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор, находится в подчинении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, является уполномоченным государственным органом по защите прав субъектов персональных данных.

Приказ Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных» [25] определяет свойства, характеристики обезличенных данных, методы обезличивания и требования к таким методам.

Кроме того, в 2015 году ФСТЭК России разработала проект «Методики определения угроз безопасности информации в информационных системах», который может быть использован как операторами государственных информационных систем, так и отдельными организациями.

Следует отметить, что государственные информационные системы определены в статье 13 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» как «федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов» [38].

В статье 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» говорится об обязанности государственных органов разрабатывать отраслевые модели угроз в пределах своей зоны ответственности. Такие модели угроз разработаны, например, Центральным банком Российской Федерации, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации («Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в стандартных отраслевых информационных системах» и «Модель угроз и

нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли»), Министерством здравоохранения Российской Федерации («Модель угроз типовой медицинской информационной системы типового лечебно-профилактического учреждения»).

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» возлагает на оператора информационной системы персональных данных или лицо, которое обрабатывает персональные данные от имени оператора, ответственность за безопасность персональных данных.

Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» включает в себя конкретные организационные и технические меры защиты, которые «обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора» [16], а выбор уровня зависит от категории обрабатываемых персональных данных, категории и количества субъектов персональных данных, а также от типа текущих угроз. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [16] предлагает достаточно короткий перечень мер по защите персональных данных, так как детальные меры безопасности определяются ФСТЭК России.

Персональные данные разделены на четыре категории:

– специальные – персональные данные о состоянии здоровья, национальности, расе, политических и религиозных убеждений;

– биометрические – персональные данные, характеризующие физиологические и биологические черты;

– общедоступные – персональные данные, полученные из общедоступных источников;

– иные.

«Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе» [16].

Выбор уровня защищенности персональных данных зависит от категории обрабатываемых персональных данных, типа актуальных угроз, а также от категории субъектов и количества субъектов (более или менее 100 000). Максимальный уровень защиты – 1-й, минимальный – 4-й.

ФСТЭК России разработала два документа, которые являются главным руководством всех организаций, обрабатывающих персональные данные. Приказ от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных» [27] и Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [28]. А также Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [26].

Приказ от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27] посвящен мерам защиты персональных данных для негосударственных информационных систем и содержит перечень конкретных мер по обеспечению определенного уровня защиты персональных данных. Пункт 4 позволяет операторам негосударственных информационных систем не использовать сертифицированные средства криптографической защиты информации при отсутствии актуальных угроз, а пункт 6 устанавливает трехлетний интервал для оценки эффективности применяемых мер.

Приказом от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27], а также Приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [28] предлагается аналогичный алгоритм выбора и применения мер безопасности: сначала на основе

положений соответствующего Приказа выбираются базовые меры, затем адаптируется выбранный базовый комплекс мер, что предполагает исключение не относящихся к делу «базовых» мер в зависимости от специфики используемых информационных систем и технологий. Затем адаптированный базовый комплекс мер уточняется с целью нейтрализации актуальных угроз с помощью мер, ранее не выбранных, и, наконец, уточненный адаптированный базовый комплекс дополняется мерами, установленными иными действующими нормативными правовыми документами.

Приказ от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27], пункт 10, содержит важное примечание о возможности применения оператором компенсирующих мер в случае невозможности или экономической нецелесообразности внедрения базовых мер, что дает возможность выбрать новые или обосновать использование внедренных мер по защите персональных данных. В случае использования оператором сертифицированных средств криптографической защиты информации, регулятор, в пункте 12 Приказа от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27], устанавливает требования к классам криптографической защиты информации и к используемому компьютерному оборудованию.

Также ФСТЭК устанавливает классы технических и программных средств по защите персональных данных, такие как межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты, средства доверенной загрузки, средства контроля съемных носителей, операционные системы, другое компьютерное оборудование. Существует утвержденный перечень сертифицированных средств защиты информации, который

содержится в государственном реестре сертифицированных средств защиты информации.

Приказ от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27] определяет следующие группы мер по обеспечению безопасности персональных данных, которые должны применяться в зависимости от требуемого уровня безопасности персональных данных:

«идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее – машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования

информационной системы и (или) к возникновению угроз безопасности персональных данных (далее – инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных» [27].

Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [28] устанавливает требования по обеспечению безопасности информации ограниченного доступа в государственной информационной системе, а в пункте 5 подчеркивает, что «при обработке в государственной информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119» [28]. Данный приказ обязывает операторов государственной информационной системы использовать только сертифицированные средства защиты информации и получить пятилетний сертификат соответствия требованиям защиты информации. Данный документ подразумевает следующие меры, которые должны быть приняты операторами для обеспечения защиты информации: «формирование требований к защите информации, содержащейся в информационной системе; разработка системы защиты информации информационной системы; внедрение системы защиты информации информационной системы; аттестация информационной системы по требованиям защиты информации и ввод ее в действие; обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы; обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации» [28]. В пункте 14.3 Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации,

не составляющей государственную тайну, содержащейся в государственных информационных системах» [28] говорится о необходимости создания модели угрозы и предлагается использовать «банк данных угроз безопасности информации» [28]. Также устанавливается класс безопасности для государственной информационной системы, который зависит от степени возможного повреждения свойств безопасности (конфиденциальности, целостности, доступности) и масштаба системы, который может быть федеральным, региональным или объектным.

В государственной информационной системе 1-го класса защиты должна быть защита от действий злоумышленников с высоким потенциалом, в государственной информационной системе 2-го класса – от злоумышленников с потенциалом не ниже усиленного базового (в банке данных угроз информационной безопасности их потенциал называется «средний», а в Методике определения угроз информационной безопасности в информационной системе – «базовый усиленный»), в государственной информационной системе 3-го класса – от злоумышленников с потенциалом не ниже базового (в банке данных угроз он называется низким). Так как для обеспечения информационной безопасности в государственной информационной системе могут использоваться только сертифицированные средства защиты информации, пункт 26 Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [28] описывает допустимые классы средств защиты информации, вычислительной техники и уровни контроля за отсутствием недекларированных возможностей в зависимости от класса государственной информационной системы. Пункт 27 связывает класс безопасности государственной информационной системы и уровни защищенности обрабатываемых в ней персональных данных: реализация мер по защите информации для государственной информационной системы 1-го

класса предусматривает 1, 2, 3 и 4 уровня защиты персональных данных, для 2-го класса – 2, 3 и 4 уровня защиты, для 3-го класса – 3 и 4 уровня защиты.

Меры по защите информации в государственной информационной системе почти совпадают с мерами Приказа от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27], за исключением отсутствия руководства по обнаружению инцидента и управлению конфигурацией. Эти мероприятия выполняются уже после построения системы защиты, при эксплуатации, сертифицированной государственной информационной системы.

Кроме Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [28], существует также методический документ «Меры защиты информации в государственных информационных системах» от 11 февраля 2014 года, утвержденный ФСТЭК России, в котором подробно расписаны все мероприятия по защите информации.

Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [26] «определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите

персональных данных для каждого из уровней защищенности» [26]. Класс средств криптографической защиты информации выбирается в зависимости от требуемого уровня безопасности персональных данных и типа актуальных угроз. Также данный документ предписывает соблюдение оператором обработки персональных данных определенные организационные требования – оборудование окон и дверей металлическими решетками, обеспечение безопасности носителей персональных данных, утверждение списка лиц, имеющих доступ к персональным данным.

Следует отметить, что законодательство в области защиты персональных данных является достаточно несовершенным, и в этой области существуют значительные пробелы и недостатки. В первую очередь, это связано с относительной новизной данной темы, поскольку законодательство Российской Федерации в области защиты персональных данных имеет историю не более нескольких десятилетий. Кроме того, многие трудности связаны с часто меняющимися и динамичными данными по этой теме. Сфера защиты персональных данных является новой и постоянно развивающейся, с каждым разом выявляется все больше и больше новых критериев, которые требуют закрепления в российском законодательстве. Злоумышленники постоянно изобретают новые способы взлома баз данных и хищения персональных данных граждан, что, в свою очередь, говорит о необходимости новых эффективных способах защиты, как технических, программных, так и организационных, и, соответственно, закрепленных в законодательстве. Законодательство не охватывает все нюансы защиты данных. Глобальная компьютеризация является одним из основных факторов, усугубляющих проблему, отсутствие осторожности у самих людей, их безответственность и непонимание необходимости защиты персональных данных.

Что определенно необходимо, так это намного более быстрое развитие законодательства в области защиты данных, более быстрое реагирование и принятие нормативных актов, новых правил, законов, которые охватывают

все аспекты этой области. Понимание важности и усиление действий уполномоченных органов, их контроля. Они должны осознавать, а также четко выполнять задачи, необходимые для обеспечения защиты персональных данных. Очень важно обучать сотрудников, создавать и применять современные средства защиты информации, увеличивать количество специалистов, потому что зачастую многие организации не имеют специалистов в области защиты персональных данных, а если они и существуют, то их квалификации недостаточно. Кроме того, все население должно быть информировано о важности этого вопроса и возможных способах защиты своих персональных данных. В области защиты персональных данных необходимо больше автоматизировать хранение баз данных и построить безопасную систему, чтобы никто, даже те сотрудники, которые отвечают за безопасность персональных данных, не имел никаких рычагов воздействия для доступа, изменения или удаления таких данных.

1.3 Иностранный опыт защиты персональных данных

С мая 2018 года по настоящее время в Европе одним из основных документов, обеспечивающих защиту персональных данных, является GDPR (General Data Protection Regulation – Общий регламент по защите данных) [50].

Отличается он тем, что его действие распространяется на компании, обрабатывающие персональные данные резидентов и граждан Европейского союза, а также явно нацеленные на такую обработку, вне зависимости от их местонахождения.

С помощью данного регламента компании привлекаются к ответственности, так, к примеру, за нарушение, основанное на недостаточной степени защиты данных клиентов, авиакомпания British Airways была оштрафована на 183 миллиона фунтов стерлингов.

Компания Google была оштрафована на 50 миллионов евро французским регулятором за неполное предоставление информации владельцам операционной системы Android. Также штрафам подверглись компании Uber и Facebook.

Таким образом, отсутствие офиса или представительства компании не препятствует применению GDPR [50]. В нем уже заложен принцип экстерриториальности. Если компания обрабатывает данные европейских граждан, но ее физически нет в Европе, предписания могут быть направлены им в любом случае. Но, в то же время, если компания не является резидентом Евросоюза, а также не осуществляет обработку персональных данных европейцев, действие GDPR [50] на нее не распространяется.

В регламенте [50] нет инструкций и прописанного алгоритма действий. Операторы обработки персональных данных могут выбрать стратегию защиты сами. Даются рекомендации, к примеру, как следует шифровать персональные данные при хранении, передаче и обработке. Но пошаговой инструкции в GDPR [50] по этому поводу нет. В этом состоит различие между российским и европейским подходом. В России государственные органы строго регламентируют меры защиты и условия их применения, осознавая, что операторы персональных данных сами ничего предпринимать не будут.

Еще одно важное отличие Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] от GDPR [50] – это требование о том, что базы, содержащие данные россиян, должны находиться в России. Тем не менее, Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] не имеет экстерриториального действия и не распространяется на лиц-нерезидентов России, обрабатывающих персональные данные россиян за границей.

Исходя из вышесказанного, можно сделать вывод о том, что GDPR [50] имеет более широкий спектр воздействия, чем Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], потому что позволяет

привлекать к ответственности даже те компании, которые не присутствуют в Европе, но имеют доступ к информации граждан Европейского союза.

Для возможности привлечения к ответственности иностранных компаний GDPR [50] – отличный инструмент, так как его сфера действия не имеет ограничения по национальному признаку. Хотя, объективно говоря, и с помощью Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] можно привлечь к ответственности иностранную компанию, например, при неисполнении требований о локализации данных. Но однозначно, что Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] не имеет такого широкого воздействия по привлечению иностранных компаний, обрабатывающих данные россиян за рубежом, к ответственности. Что касается штрафов за нарушение норм GDPR [50], то при незначительных нарушениях это – 2% от мирового годового оборота компании, но не более 10 миллионов евро. Если же нарушение существенное, то – 4% от мирового годового оборота, но не более 20 миллионов евро. [50]

Что касается ситуации в США, защита персональных данных пользователей регулируется отдельными отраслями. В стране нет специального федерального закона о персональных данных – его заменяют местные нормативные акты, часто действующие в отдельных штатах, и узкоспециализированные законы.

В США существует Федеральная торговая комиссия (FTC), которая контролирует соблюдение ряда законов и соглашений по защите персональных данных. Штрафы за нарушение в области защиты персональных данных составляют до 40 тысяч долларов за одно нарушение и 40 тысяч долларов за каждый последующий день незаконной обработки персональных данных после выявления такого нарушения. К примеру, Facebook была оштрафована на 5 миллиардов долларов за скандал с Cambridge Analytica, который привел к утечке личной информации 87 миллионов пользователей, не давших согласия на ее использование.

Отсутствие универсального закона о защите персональных данных в США является серьезной проблемой для страны, на территории которой расположена Кремниевая Долина, являющаяся центром крупнейших IT-компаний. Как законодатели, так и резиденты Долины, такие как Microsoft и Apple, выступают за принятие в Америке аналога GDPR [50].

В 2018 году в Калифорнии был принят закон о защите прав потребителей (California Consumer Privacy Act, или CCPA) [47], который воспроизводит некоторые пункты GDPR [50]. Некоторые представители IT-индустрии поддержали эту инициативу, назвав ее важным шагом на пути к принятию единого федерального закона о защите персональных данных.

В Бразилии действует Закон о защите данных LGPD [46]. Это аналог европейскому GDPR [50]. Согласно LGPD [46], персональные данные - это любая информация, относящаяся к физическому лицу, которое идентифицировано или может быть идентифицировано [46]. Данный документ защищает также те сведения, которые затрагивают расовую или этническую принадлежность, религию, политические убеждения, членство в различных организациях, касающихся религии или политики. В то же время, закон защищает данные о здоровье, половой жизни, генетических или биометрических параметрах, если они относятся к конкретной личности. LGPD [46] обязаны соблюдать все организации, если они собирают или обрабатывают персональные данные в Бразилии для маркетинговых целей, при этом неважно, находится данная компания в Бразилии или нет. LGPD [46] не распространяется на данные, собранные физическими лицами для личных, академических или журналистских целей, а также в целях национальной безопасности. Согласно LGPD [46] субъект данных – это физическое лицо, к которому относятся персональные данные, являющиеся объектом обработки. Субъекты данных имеют такие права в отношении своих персональных данных как право на уведомление об обработке данных и согласие на нее, доступ к своим персональным данным, исправление неточных данных, анонимизация или псевдонимизация, удаление данных,

которые были собраны или обработаны без соблюдения LGPD [46], возможность перемещать данные, раскрытие любых третьих лиц, которым передаются личные данные, доступ к информации о клиентской политике и условиям отзыва согласия, отзыв согласия.

Аргентина была признана Европейской комиссией единственной страной, которая полностью соблюдает требования по защите персональных данных в Интернете.

Южная Африка не имеет отдельного закона по защите персональных данных, тем не менее, в Конституции данной страны закреплено право на неприкосновенность частной жизни. Кроме того, Закон о защите прав потребителей 2008 года и Закон об электронных коммуникациях и сделках 2002 года содержат положения, касающиеся личной информации.

В 1776 году в Швеции был принят закон «О свободе изданий» – это закон о свободе информации. В 1949 году он был переименован на «Закон о свободе печати». В данный момент этот закон входит в Конституцию Швеции и гарантирует абсолютно всем шведским гражданам свободу получения информации от государственных органов на безвозмездной основе. Вообще скандинавских странах действует законодательство о защите компьютерных банков данных. Швеция также стала первой страной, принявшей закон «О защите частной информации, хранящейся в компьютерных базах данных».

В Китае действует большое количество актов по защите персональных данных в разных областях. Также разработано подзаконное законодательство, и большую роль играют документы рекомендательного характера.

В Саудовской Аравии нет специальных законов по защите персональных данных. В нескольких законах закреплено право на неприкосновенность частной жизни. Например, в Основном низаме правления Саудовской Аравии говорится о том, что вся переписка, равно как и все виды связи между сторонами, являются строго конфиденциальными, а их разглашение запрещено. В отсутствие применимого права суды руководствуются шариатом (исламским правом). На основании законов

шариата может быть предъявлен иск о возмещении ущерба, причиненного незаконным разглашением личной информации, если разглашение этой информации повлекло причинение ущерба лицу.

В Объединенных Арабских Эмиратах также нет специальных законов о защите персональных данных, однако, существует право на неприкосновенность частной жизни, которое закреплено в Конституции этой страны, а также в ее различных законах. Конституция ОАЭ гласит, что гражданину гарантируется свобода и конфиденциальность переписки, передачи телеграфных сообщений и других средств связи в соответствии с законом. Кроме того, некоторые права на конфиденциальность и защиту личной информации прописаны в Уголовном кодексе.

В Индии законом регулируется обработка персональных данных как правительством, так и компаниями, зарегистрированными в Индии. Он также регулирует деятельность иностранных компаний, если они обрабатывают персональные данные физических лиц в Индии. Согласно закону, граждане могут обратиться за подтверждением того, что их персональные данные были обработаны, за исправлением, заполнением или удалением их данных, за ограничением дальнейшего раскрытия их персональных данных, если в этом больше нет необходимости. Любая обработка персональных данных может быть осуществлена только на основании согласия субъекта. Персональные данные могут обрабатываться только с определенной, ясной и законной целью.

В Японии сбор и использование личной информации регулируется Законом о защите личной информации (APPI) [44]. Этот закон применяется ко всем видам обработки личной информации, но только в том случае, если речь идет об информации, принадлежащей 5 000 или более лицам. Этот закон устанавливает общие требования к полномочиям, безопасности и предоставлению информации, а также дополнительные требования к контролю для сотрудников и третьих лиц, которые обрабатывают личные данные.

В Австралии существует регулирование на федеральном и региональном уровнях. Существует также надзорный орган по защите персональных данных.

В Канаде действует Закон о защите личной информации и электронных документов (PIPEDA) [52]. Этот закон защищает персональные данные, которые содержат любую фактическую или субъективную информацию, записанную или нет, о лице, которое может быть идентифицировано. Они включают в себя не только личную информацию, такую как имя, возраст, идентификационный номер, этническое происхождение или медицинскую карту, личные дела сотрудников, кредитные записи, но и мнения, оценки, комментарии, социальный статус и дисциплинарные взыскания.

К конфиденциальным данным, не охватываемым PIPEDA [52], относятся, в частности, личные данные, обрабатываемые федеральными государственными организациями, которые подпадают под действие Закона о конфиденциальности, деловая контактная информация, используемая для общения с человеком в связи с его работой или профессией, сбор, использование или разглашение личной информации лицом исключительно в личных целях или сбор, использование или разглашение организацией личной информации в журналистских, художественных или литературных целях. Организации, согласно этому закону, должны уведомлять Комиссара Канады по вопросам конфиденциальности, если им становится известно о любых нарушениях гарантий безопасности, связанных с личной информацией, которые представляют реальную угрозу причинения значительного ущерба физическим лицам.

Компании также должны информировать лиц, затрагиваемых такими нарушениями. Организации должны в течение двух лет вести учет всех нарушений гарантий безопасности, независимо от того, были ли эти нарушения доведены до сведения канадского Уполномоченного по вопросам конфиденциальности или нет. Если организация сознательно игнорирует

требования в отношении уведомлений о нарушении данных и ведения учета, ей грозит штраф в размере до 100 000 канадских долларов.

Глава 2 Судебная и административная практика по защите персональных данных

2.1 Юридическая ответственность за нарушение норм о персональных данных

Проблема защиты персональных данных граждан в настоящее время приобрела особую остроту, по сравнению с периодом в десять лет назад. Огромное количество людей во всем мире пользуются социальными сетями и медиа-платформами, тем самым предоставляя свои персональные данные для того, чтобы иметь возможность пользоваться определенными сайтами или заказывать различные товары и услуги. Огромные объемы данных находятся в распоряжении крупных IT-компаний, и если эти данные расшифровать, то можно узнать абсолютно любые подробности о жизни человека. Защита персональных данных предусмотрена законом.

В России обработка, а также защита персональных данных регулируется несколькими нормативно-правовыми актами, в частности, Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» [39], Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» [38], Кодексом Российской Федерации об административных правонарушениях [3], Гражданским кодексом Российской Федерации [1], Уголовным кодексом Российской Федерации [35] и Трудовым кодексом Российской Федерации [34].

Административная ответственность за нарушение в области защиты персональных данных предусмотрена, прежде всего, статьей 13.11 Кодекса Российской Федерации об административных правонарушениях, а также статьями 5.39 (отказ в предоставлении информации), 13.14 (разглашение информации с ограниченным доступом) и 19.7 Кодекса Российской Федерации об административных правонарушениях (непредоставление

сведений). С 1 июля 2017 года вступили в силу поправки в статью 13.11 Кодекса Российской Федерации об административных правонарушениях, которые увеличивают размер максимального штрафа с 10 000 рублей до 75 000 рублей. Тем не менее, они не сопоставимы с европейскими. Эта сумма штрафов может быть значительной для небольших компаний, но эти штрафы не будут иметь сдерживающего эффекта для крупных игроков рынка персональных данных, которые зарабатывают большие суммы денег, торгуя персональными данными.

Размер российских штрафов, несопоставим со штрафами в соответствии с Общим регламентом по защите данных GDPR [50], где верхний предел штрафа составляет 20 миллионов евро, или 4% от мирового оборота компании-нарушителя.

«Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами» [34].

«За неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации влечет наложение административного штрафа на должностных лиц в размере от пяти тысяч до десяти тысяч рублей» [3] согласно статье 5.39 Кодекса Российской Федерации об административных правонарушениях.

Согласно части 1 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях «обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных,

несовместимая с целями сбора персональных данных, если эти действия не содержат уголовно наказуемого деяния, влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей, на должностных лиц – от пяти тысяч до десяти тысяч рублей, на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей» [3].

«Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц – от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от пятнадцати тысяч до семидесяти пяти тысяч рублей» [3] согласно части 2 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.

«Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных влечет предупреждение или наложение административного штрафа на граждан в размере от семисот до одной тысячи пятисот рублей; на должностных лиц - от трех тысяч до шести тысяч рублей; на индивидуальных предпринимателей – от пяти тысяч до десяти

тысяч рублей; на юридических лиц - от пятнадцати тысяч до тридцати тысяч рублей» [3] согласно части 3 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.

«Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц - от четырех тысяч до шести тысяч рублей; на индивидуальных предпринимателей – от десяти тысяч до пятнадцати тысяч рублей; на юридических лиц - от двадцати тысяч до сорока тысяч рублей» [3] согласно части 4 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.

«Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц – от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей – от десяти тысяч до двадцати тысяч рублей; на юридических лиц – от двадцати пяти тысяч до сорока пяти тысяч рублей» [3] согласно части 5 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.

«Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий,

обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа на граждан в размере от семисот до двух тысяч рублей; на должностных лиц – от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей – от десяти тысяч до двадцати тысяч рублей; на юридических лиц – от двадцати пяти тысяч до пятидесяти тысяч рублей» [3] согласно части 6 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.

«Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных влечет предупреждение или наложение административного штрафа на должностных лиц в размере от трех тысяч до шести тысяч рублей» [3] по части 7 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях.

«Непредставление или несвоевременное представление в государственный орган или иной уполномоченный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности, либо представление таких сведений в неполном объеме или в искаженном виде, влечет предупреждение или наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц – от трехсот до

пятисот рублей; на юридических лиц – от трех тысяч до пяти тысяч рублей.» [3] по статье 19.7 Кодекса Российской Федерации об административных правонарушениях.

Таким образом, административная ответственность в соответствии со статьей 13.11 Кодекса Российской Федерации об административных правонарушениях [3] за нарушение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] теперь дифференцирована в зависимости от совершенного правонарушения и его тяжести. Максимальный штраф для юридических лиц предусмотрен за обработку персональных данных без письменного согласия субъекта таких данных либо за обработку персональных данных с нарушением требований к составу сведений, включаемых в письменное согласие субъекта на обработку его персональных данных.

Уголовная ответственность наступает в случае «незаконного собирания или распространения сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ. Наказание при этом налагается в виде штрафа до 200 тысяч рублей, либо обязательных работ на срок до 360 часов, либо исправительных работ на срок до одного года, либо принудительных работ на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арестом на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет)» [35] согласно статье 137 Уголовного кодекса РФ. Однако, дела по этой части возбуждаются только если есть заявление потерпевшего или его законного представителя, а это условие во многом затрудняет привлечение к уголовной ответственности виновных лиц.

«То же деяние, совершенное с использованием служебного положения наказывается штрафом от 100 тысяч до 300 тысяч рублей, либо лишение

права занимать определенные должности на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет или без такового), либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет)» [35] по статье 137 Уголовного кодекса Российской Федерации.

«Незаконное публичное распространение информации, указывающей на личность лица, не достигшего 16 лет, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий грозит штрафом от 100 тысяч до 300 тысяч рублей, либо лишением права занимать определенные должности на срок от трех до пяти лет, либо принудительными работами на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет или без такового), либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет)» [35] по статье 137 Уголовного кодекса Российской Федерации.

«За неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление ему неполной или заведомо ложной информации, если это причинило вред правам и законным интересам граждан – штраф до 200 тысяч рублей, либо лишение права занимать определенные должности на срок от двух до пяти лет» [35] согласно статье 140 Уголовного кодекса Российской Федерации.

«За неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование – штраф до 200 тыс. руб., либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок» [35].

Гражданско-правовая ответственность наступает согласно статье 15 Гражданского кодекса Российской Федерации [1] в случае причинения лицу убытков в результате нарушения правил обработки его персональных данных. «Под убытками понимаются расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества, неполученные доходы, которые лицо получило бы, если бы его право не было нарушено» [1]. Наказание при этом – обязанность возместить убытки.

«Если гражданину причинен моральный вред (физические или нравственные страдания)» [1] вследствие нарушения правил обработки персональных данных налагается компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков) по статье 24 Федерального закона от 27 июля 2006 года «О персональных данных» [39], а также статье 151 Гражданского кодекса Российской Федерации [1].

Дисциплинарная ответственность наступает за «разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника» [34]. За это грозит увольнение согласно подпункту «в» пункта 6 части 1 статьи 81 Трудового кодекса Российской Федерации [34]. За иные нарушения в области персональных данных при их обработке – замечание или выговор по статье 90 и статье 192 Трудового кодекса Российской Федерации [34]. Кроме того, работник несет материальную ответственность в полном размере причиненного работодателю ущерба за разглашение сведений, составляющих охраняемую законом тайну в соответствии с пунктом 7 части 1 статьи 243 Трудового кодекса Российской Федерации [34]. Ущерб работодатель может понести, например, вследствие вынужденного возмещения им морального вреда субъекту персональных данных. В таком случае работник, виновный в нарушении законодательства о персональных

данных, должен компенсировать работодателю сумму возмещения морального вреда в соответствии со второй частью статьи 238 Трудового кодекса Российской Федерации [34].

Однако персональные данные россиян часто просачиваются в открытые источники или становятся предметом купли-продажи. Согласно исследованию Dentsu Aegis Network, только 29% россиян считают, что их персональные данные достаточно защищены. Продаются реквизиты банковских карт и счетов, счетов в социальных сетях, удаленного доступа к серверам и персональным компьютерам, а также информация из различных приложений и отсканированные копии документов. Например, копии паспорта достаточно, чтобы открыть счет или обратиться в банк за кредитом на чужое имя.

Действующий закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] позволяет физическим лицам требовать в судебном порядке возмещения имущественного и морального ущерба, причиненного в результате нарушения требований по обработке персональных данных. Основной проблемой, с которой сталкиваются физические лица при защите своих прав, является сложность доказывания размера ущерба и неготовность судов присуждать существенные суммы компенсации за моральный ущерб.

В России количество судебных дел в этой категории исчисляется десятками, что явно несопоставимо с количеством нарушений в этой области.

Другой проблемой, препятствующей эффективной защите прав субъектов персональных данных (как самостоятельно, так и со стороны государственных органов), является отсутствие физического представительства и собственности компаний-нарушителей в России, что делает невозможным реальное исполнение судебных решений. В таких случаях единственным оставшимся инструментом является блокирование сайтов компаний-нарушителей, что не всегда позволяет достичь цели защиты персональных данных.

Существует несколько прецедентов, когда крупные иностранные компании были оштрафованы в России. Например, Facebook и Twitter были оштрафованы за непредоставление информации о передаче персональных данных российских пользователей в Россию. Интернет-компании были обязаны хранить данные российских граждан на российских серверах согласно Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39].

У таких компаний как Facebook, Twitter и других представителей Кремниевой долины, нет официального представительства в России, что означает, что они формально не обязаны следовать российскому законодательству. В апреле 2019 года автономная некоммерческая организация «Цифровая экономика» выдвинула предложение о запрете компаниям, которые не имеют официального представительства в России, доступа к персональным данным россиян. Одной из главных причин называются недобросовестные условия конкуренции между иностранными и российскими IT-компаниями, так как именно к российским компаниям предъявляются требования намного более жесткие. В документе говорится о необходимости избегать ситуаций, когда иностранные компании, не выполняющие требования законодательства Российской Федерации, ограничивающего доступ к данным, будут иметь более привилегированное положение по отношению к российским компаниям, выполняющим эти требования. Эта проблема касается и Яндекса, который принадлежит компании, зарегистрированной в Нидерландах. В частности, именно поэтому в конце июля в Государственную Думу был внесен законопроект о 20% лимите на иностранное владение информационными ресурсами, который будет признан «значимым» для России. «Значимость» компании оценивается по тому, сколько активных пользователей имеет данная компания в России. При определении ресурса «значимым», предъявляется требование, что владелец данной компании должен быть зарегистрирован в России. Так, Яндекс имеет зарегистрированное юридическое лицо в России, он обязан

соблюдать российское законодательство и подчиняться требованиям Роскомнадзора.

2.2 Судебная и административная практика по защите персональных данных

В сфере защиты персональных данных судебная и административная практика по нарушению законодательства очень разнообразна. Главным вопросом при споре о персональных данных является то, считается ли эта информация персональными данными. Поскольку понятие «персональные данные» конкретно не определено в законодательстве, существует много разногласий. Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] установлено, что «персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [39]. Основным фактором, определяющим, является ли информация персональными данными – это способность идентифицировать субъекта по этой информации.

Существует много споров о том, считать ли IP-адрес персональными данными. Этот адрес идентифицирует само устройство, с которого был произведен доступ в Интернет, а не конкретного пользователя. Если знать устройство, то можно определить количество людей, которые могли бы пользоваться им, что, значительно сужает область поиска конкретного лица. Однако IP-адрес в судебной практике не имеет однозначного отношения к персональным данным.

Существует также много споров о том, должен ли образ субъекта быть признан в качестве персональных данных. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] раскрывает понятие биометрических персональных данных как физиологические данные лица, на основании которых можно его идентифицировать. В то же время, само

изображение, без ссылки на другие данные, не может быть признано в качестве персональных данных.

Также много возникает вопросов по поводу адреса электронных почт, поскольку он не дает возможности идентифицировать однозначно субъект персональных данных, он является только средством передачи этих данных. Однако, как и в случае с IP-адресом, учитывая адрес электронной почты, можно значительно сузить количество людей, причастных к этому адресу. В юриспруденции нет единого подхода к вопросу о том, следует ли считать адреса электронных почт персональными данными или нет.

Много судебных исков касаются случаев, когда конфиденциальные данные граждан публикуются в средствах массовой информации, при этом согласие на обработку персональных данных получено не было.

К примеру, случай с газетой «Лабинские вести». В данной газете были опубликованы персональные данные несовершеннолетнего ребенка, а именно, имя и информация о школе, где он учится. В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], эти данные относятся к персональным сведениям, а значит, что для их размещения требуется согласие этого гражданина или же его законных представителей. Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций вынесло руководству газеты письменное предупреждение, в котором говорилось, что при опубликовании персональной информации о гражданине без его на то согласия, учреждение нарушает законодательство о защите персональных данных. Однако, руководство данной газеты продолжило публикации персональных данных о лицах без получения их согласия на обработку персональных данных. В результате Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций обратилось с исковым заявлением в Краснодарский краевой суд с требованием запретить последующие публикации газеты «Лабинские вести». Краснодарский суд удовлетворил данное исковое заявление, поданное

Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. По моему мнению, это судебное решение является абсолютно справедливым, а также соответствующим закону. Краснодарский суд руководствовался статьей 4 Закона Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», по которой невозможно разглашение сведений, составляющих государственную или иную специально охраняемую законом тайну средствами массовой информации. К такой информации относятся, в частности, персональные данные. В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] обработка персональных данных может осуществляться только, имея письменное согласие субъекта персональных данных. Кроме этого, в соответствии со статьей 16 Закона Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», было определено, что многократные нарушения редакцией требований законодательства стали причиной для вынесения судом решения о прекращении деятельности средств массовой информации. Формулировка, которая стала ясна о персональных данных субъекта, заключалась в обеспечении их конфиденциальности [8].

Следующее дело связано с магазином. В отношении него было возбуждено административное дело. При попытке гражданина вернуть купленный товар, ему было предложено заполнить заявление. При этом в нем должны были быть указаны его персональные данные, а написание такого заявления – обязательная процедура. Этот магазин был привлечен к административной ответственности по статье 13.11 Кодекса об административных правонарушениях Российской Федерации [3], так как, в соответствии со статьей 5 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» [39], «персональные данные не должны быть избыточными по отношению к заявленным целям их обработки» [39]. Магазин подал апелляцию в Верховный Суд Российской Федерации, который

отменил принятые по этому делу решения, а также признал данный магазин невиновным. Причиной принятия этого решения послужил тот факт, что в соответствии с Постановлением Правительства Российской Федерации от 19 января 1998 года № 55 были утверждены Правила продажи отдельных видов товаров, согласно которым гражданин, который купил определенный товар мог вернуть его обратно в магазин, а затем получить обратно свои потраченные деньги. При этом продавец должен соблюдать Положение о порядке ведения кассовых операций с банкнотами и монетой Банка России на территории Российской Федерации, которое было утверждено Банком России от 12 октября 2011 года №373-П. Кассир имеет право вернуть деньги гражданину, купившему товар, если он указан в расходном кассовом ордере и при наличии документа, удостоверяющего личность, в частности, паспорта. Отсюда следует, что требование о письменном заявлении, в котором должны быть указаны фамилия, имя, отчество и данные документа, является абсолютно законным и не противоречит российскому законодательству [13].

Многочисленные жалобы были поданы в связи с нарушением требований закона о рекламе. Например, гражданин жаловался на то, что он часто получал текстовые сообщения на свой телефон с рекламой компании. Федеральная антимонопольная служба направила в эту организацию предписание с требованием указать данные владельца номера телефона, с которого были отправлены сообщения. Компания отклонила запрос и не предоставила запрашиваемую информацию, ссылаясь на законодательство о защите персональных данных, в частности, Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных» [39]. Получив отказ от данной организации в предоставлении данных, Федеральная антимонопольная служба вынесла постановление о привлечении компании к административной ответственности согласно статье 19.8 Кодекса Российской Федерации об административных правонарушениях [3]. Однако, данная организация обратилась с исковым заявлением в арбитражный суд с просьбой отменить вынесенное постановление. Арбитражный суд

удовлетворил требования компании. Суд аргументировал свое решение тем, что запрошенная информация относится к категории ограниченного доступа, а представление такой информации возможно только с получения согласия владельца этих данных. Более того, одним из доводов было то, что Федеральная антимонопольная служба не относится к органам, уполномоченным осуществлять оперативно-розыскную деятельность. При этом ни Закон о рекламе, ни Закон об оперативно-розыскной деятельности не содержат прямого указания на полномочие Федеральной антимонопольной службе запрашивать у операторов связи сведения о его абонентах. Но Верховный суд Российской Федерации с данными выводами нижестоящего суда не согласился. Верховный суд определил, что Федеральная антимонопольная служба осуществляет государственный контроль за соблюдением законодательства Российской Федерации о рекламе согласно своим полномочиям. А также, предупреждает, выявляет и пресекает нарушения физическими или юридическими лицами законодательства Российской Федерации о рекламе и возбуждает, а также рассматривает дела по признакам нарушения законодательства РФ о рекламе. Согласно изложенному, антимонопольному органу предоставляется право запрашивать документы без каких-либо ограничений по составу и объему необходимой информации. Одновременно с этим, Федеральная антимонопольная служба может запрашивать именно те документы, имеющие отношение к нарушению законодательства о рекламе и касаются деятельности определенных лиц. Неисполнение этих требований влечет за собой ответственность виновных лиц в соответствии с Кодексом Российской Федерации об административных правонарушениях [3]. Притом гарантией выполнения установленной законом защиты персональных данных является статья 35 закона о рекламе, которой установлена обязанность Федеральной антимонопольной службы по соблюдению коммерческой, служебной и иной охраняемой законом тайны, а также ответственность антимонопольного органа и его сотрудников за разглашение этих данных. Из этого получается,

что требование Федеральной антимонопольной службы соответствует действующему законодательству, и отказ организации о представлении документов был неправомерным [12].

Существуют также судебные разбирательства, которые касаются нарушений защиты персональных данных в банковском секторе. Все чаще встречаются случаи кражи баз данных, содержащих персональные данные граждан, незаконной передачи персональных данных финансовыми учреждениями третьим лицам, а также торговли персональными данными.

Рассматривалось дело, где банк заключил договор с субъектом о потребительском кредите. Определенный пункт данного договора содержал условие об уступке прав требования по данному договору, которое было обязательным, а также не включал конкретного списка третьих лиц, которым затем будут переуступлены все права, а также переданы персональные данные лица. Банк привлекли к административной ответственности согласно части 1 и 2 статьи 14.8 Кодекса Российской Федерации об административных правонарушениях [3], так как им был нарушен Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных» [39]. У лица не было варианта отказаться при представлении согласия, не был определен в данном согласии конкретный список лиц [15].

Также было дело, касающееся избыточной обработки сведений, а также ее несоответствие целям, которые были заявлены. В одном пункте кредитного договора прописали, что заемщик должен уведомить кредитора о том, что заключает (изменяет) брачный договор, о том, что изменяется состав семьи, работа или место жительства, а также о смене фамилии, об иных данных, которые могут идентифицировать лицо. Суд решил, что данный пункт кредитного договора нарушает права потребителя обязанностью по предоставлению в этот банк персональных данных, обязательность предоставления которых не установлена законодательством РФ, а также не влияет на выполнение целей кредитного договора. Данный банк был

привлечен к административной ответственности согласно части 2 статьи 14.8 Кодекса Российской Федерации об административных правонарушениях [14].

Следующее дело связано с блокировкой LinkedIn. Роскомнадзор требовал признать деятельность Интернет-ресурсов http://www.linkedin.com и http://linkedin.com по сбору, использованию и хранению персональных данных граждан Российской Федерации нарушающей требования Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] и права граждан на неприкосновенность частной жизни, личную и семейную тайну. Роскомнадзор определил, что LinkedIn Corporation нарушил Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], потому что сбор персональных сведений граждан Российской Федерации происходил без локализации баз данных. Также, через данные Интернет-ресурсы Роскомнадзор получил доступ к данным третьих лиц, которые не являлись пользователями LinkedIn, с помощью синхронизации с их электронной почтой, а также устройствами пользователей. При том, что ответчик зарегистрирован не в пределах Российской Федерации, Роскомнадзор при рассмотрении дела указывал на то, что данный Интернет-ресурс направлен все-таки на территорию Российской Федерации, так как существует русскоязычная версия сайта. Суд полностью удовлетворил требования истца и признал деятельность LinkedIn нарушающей законодательство РФ [9].

Законодательство Российской Федерации в области защиты персональных данных не идеально. Судебная практика – один из показателей. Безусловно, в большинстве споров принятые решения верные и справедливы, но есть и споры, окончательные решения по которым были приняты в соответствии с российским законодательством, но, согласно логике, а также здравому смыслу, должны быть другими. Для того, чтобы этого не происходило надо учитывать, прописывать многие моменты в законодательстве, потому что именно они, зачастую, играют главную роль.

Это и является самой сложной задачей, ведь человек не может предугадать все варианты событий.

Глава 3 Проблемы защиты персональных данных в РФ и способы их преодоления

3.1 Обеспечение защиты персональных данных в Интернете

В настоящее время глобальные информационно-телекоммуникационные сети заняли первое место в информационном обществе. Крупнейшей в мире информационно-телекоммуникационной сетью является сеть Интернет. Отсюда следует, что важным вопросом является то, чтобы обработка персональной информации обеспечивалась безопасными методами.

Сейчас во всем мире наблюдается рост Интернет-активности, вследствие этого, пользователи выкладывают большой объем данных о себе в Интернет. Важным документом, предусмотренным Федеральным законом от 27 июля 2006 года «О персональных данных» № 152-ФЗ [39] является согласие на обработку персональных данных, которое «должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом» [39]. Тем не менее, согласно указанному закону, если обработка данных происходит с целью выполнения условий договора с самим субъектом персональных данных, в этом случае у оператора нет обязательства брать такое согласие. Этим положением пользуются многие сайты в Интернете.

Вследствие того, что информационные технологии стремительно развиваются, возникают новые трудности, связанные с безопасностью обработки персональной информации, а также с получением согласия на такую обработку.

В соответствии с частью 4 статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] «равнозначным

содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью» [39].

При регистрации на большинство Интернет-ресурсов пользователю предлагается проставить отметки, таким образом дав свое согласие на обработку данных. Зачастую, без этих отметок нельзя начать пользоваться сайтом. Причем, в тех соглашениях, где заранее проставлены отметки, не означает, что субъект дал свое согласие. Требование Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] о том, что согласие обязательно должно выражаться явно, относится к обработке специальных категорий персональных данных, созданию так называемых профайлов и решению, что обработка персональных данных является полностью автоматической.

Роскомнадзор разъясняет, что при регистрации на различных социальных ресурсах граждане, согласно своим интересам и по своей воле, сообщают информацию о себе, при этом соглашаясь с правилами пользования этих социальных ресурсов. Таким образом, важной рекомендацией является сначала тщательно изучить все условия соглашений при регистрации, чтобы не допустить нарушения своих прав. Большинство сайтов ориентированы на пользователей и для их идентификации будут использовать его личную информацию, например, логин, пароль, адрес электронной почты.

Данные, которые оператор может обрабатывать без согласия субъекта, являются общедоступными. Это персональные данные, к которым с согласия гражданина предоставляется доступ общественности. Таким образом, общедоступными с письменного согласия субъекта данными могут быть фамилия, имя, отчество, адрес, дата рождения и иные данные, которые может сообщить субъект. У субъекта имеется право требовать исключить свои личные данные из общедоступных источников. Хотя, нет никаких гарантий,

что при требовании субъекта об исключении таких данных, их не обработают третьи лица.

К тому же, далеко не всегда это право может быть реализовано. К примеру, обработка персональных данных сотрудников организации осуществляется исходя из пунктов трудового договора, где согласие на обработку данных не является требованием, таким образом, возможно размещение сведений работников на официальном сайте компании в Интернете.

Гражданин имеет право требовать уточнения его данных у оператора, а также блокирования или уничтожения их тогда, когда сведений недостаточно или они не относятся к самому субъекту.

Согласно Федеральному закону от 21 июля 2014 года № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» [40] сайты, размещающие информацию, которая обрабатывается с нарушениями, обязаны быть заблокированы. Такие Интернет-сервисы вносятся в «Реестр нарушителей прав субъектов персональных данных».

Роскомнадзор, руководствуясь статьей 23 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], как уполномоченный орган по защите прав субъектов персональных данных, может «обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде» [39].

Роскомнадзор принимает меры, следуя положениям судебного акта, который вступил в законную силу, и ограничивает доступ к информации в сети, которая обрабатывается с нарушениями. Затем, после поступления в Роскомнадзор судебного решения, сайт вносится в реестр нарушителей. Данная мера способствует эффективному пресечению нарушений, а также

направлена на их профилактику, потому что только наличие реальной меры в виде блокировки ресурса мотивирует соблюдать нормы законодательства.

Все чаще возникает вопрос об идентификации пользователей в Интернете. Развитие сети способствует росту возможностей участников и методов установления уникальности ее пользователей.

В Постановлении Правительства РФ от 28 ноября 2011 года № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [20], определены ряд понятий. Идентификация участников информационного взаимодействия определяется как «сравнение идентификатора, вводимого участником информационного взаимодействия в любую из информационных систем с идентификатором этого участника в информационных системах, содержащих уникальные сведения о гражданине Российской Федерации, на ведение которых федеральные органы исполнительной власти, органы государственных внебюджетных фондов уполномочены в соответствии с федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации» [20]. Аутентификация участников информационного взаимодействия – «проверка принадлежности участнику информационного взаимодействия введенного им идентификатора, а также подтверждение подлинности идентификатора» [20]. Еще одним важным определением постановления является авторизация участников информационного взаимодействия, которое обозначает «подтверждение наличия у участника информационного взаимодействия прав на получение доступа к инфраструктуре, которая обеспечивает информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [20].

В этом постановлении именно понятие аутентификации более точно подходит по смыслу из этого определения, поэтому именно его и следует применять. В «Положении об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [11] определяется значение фразы «упрощенная идентификация физического лица» [11]. Под этой фразой понимается «установление фамилии, имени и (если иное не вытекает из закона или национального обычая) отчества, реквизитов документа, удостоверяющего личность клиента» [11]. Данные абонентов должны хранить все технические службы. Из «Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» [23], определяется то, что «оператор связи обязан своевременно обновлять информацию, содержащуюся в базах данных об абонентах оператора связи и оказанных им услугах связи. Указанная информация должна храниться оператором связи в течение 3 лет на территории Российской Федерации и предоставляться органам федеральной службы безопасности, а в случае, указанном в пункте 3 настоящих Правил, органам внутренних дел путем осуществления круглосуточного удаленного доступа к базам данных» [23].

Содержание данных сведений закреплено положениями Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [38]. Согласно этому закону, данные, которые распространяются без использования средств массовой информации, должны содержать правдивые и достоверные сведения об их владельце или о том лице, который распространяет эту информацию, в достаточных форме и объеме, для возможности идентификации данного лица. Одновременно с этим, исходя из положения Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи» [41], операторы связи должны хранить тайну, но при стремительном развитии технологий само понятие идентификации

пользователя ставится под сомнение, хотя для большинства сайтов очень важно условие идентификации своих пользователей. Если сайт отказывается от анонимности, это автоматически повышает доверие и приводит новых клиентов. Сейчас большое число Интернет-пользователей считают, что платежи в Интернете небезопасны, так как совершается множество киберпреступлений.

Особенно важным вопросом является регулирование оборота персональной информации при предоставлении государственных и муниципальных услуг.

При предоставлении таких услуг оператором, обрабатывающим персональные данные, являются органы власти. На все органы власти возложены различные задачи, и, в соответствии с этими задачами, они проводят обработку данных. Зачастую обработка персональных сведений тесно связана с предоставлением данными органами определенных услуг, оказываемых в бумажной или электронной форме. Система предоставления государственных услуг развивается и предоставляет большие преимущества обычным гражданам и различным компаниям. Одновременно с этим, эта область подразумевает и некоторые нерешенные проблемные вопросы, такие как проблема идентификации субъекта. Портал государственных услуг Российской Федерации представляет собой справочно-информационный Интернет-портал, где у каждого гражданина есть возможность заказать услугу, узнать информацию, записаться на прием и многое другое. Через него проходит огромное количество данных, безопасность которых должна быть обеспечена.

Система безопасности состоит из средств для возможности анализа содержимого, антивирусных средств, межсетевых экранов, средств мониторинга и контроля защиты данных, средств предотвращения от каких-либо несанкционированных вторжений. По требованиям ФСТЭК программное обеспечение переаттестовывается и проходит сертификацию каждый год. «Персональные данные граждан хранятся в Единой системе

идентификации и аутентификации, которая создана для обеспечения доступа к информации участников информационного взаимодействия. Сам портал и система аттестованы согласно требованиям ФСТЭК на обработку персональных данных и конфиденциальной информации» [5, с. 115]. Воплощение данных решений стало возможным благодаря сертификации ФСБ, что гарантировало соблюдение требований законодательства по защите персональных данных. Кроме этого, важным фактом является и то, что безопасность персональных сведений определяется как уровнем защиты портала, так и защищенностью самого рабочего места.

Возможность получить услугу в электронном виде удобна и экономит время, но при этом возникают и новые проблемы. Огромное число преступлений связано с незаконным использованием персональных данных. Целью таких преступлений почти всегда является похищение денежных средств с банковских счетов и из платежных систем.

В 2007 году были приняты «Правила оказания телематических услуг связи» [21]. В них прописаны все нюансы взаимоотношений между пользователями и операторами связи.

Тем не менее, серьезной проблемой является правовое регулирование Интернет-услуг, так как Интернет-технологии развиваются в разы быстрее, чем может отреагировать государство.

Важнейшей частью Интернет-пространства являются социальные сети. Отдельным вопросом стоит безопасность обработки персональных сведений в социальных сетях. Социальная сеть – это своеобразная социальная структура, узлы в которой – это пользователи, а связи – их взаимодействия друг с другом. На сегодняшний день пользователи переносят свои социальные коммуникации в сеть. Люди практически всех возрастов и обоих полов активно пользуются данными возможностями. В социальной сети есть профиль пользователя, его аккаунт, где он указывает любую информацию о себе, которую посчитает нужной. Также в ней содержатся различные группы и сообщества, объединяющие людей по интересам или другим критериям. В

них пользователь также может оставлять личную информацию. Конечно, правдивость этих данных никем не проверяется, но при регистрации гражданин передает свою электронную почту и номер мобильного телефона, с помощью которых не составит труда идентифицировать человека.

Абсолютно любой пользователь может заходить на другие аккаунты, вступать в группы и сообщества. Таким образом, любой человек может увидеть личную информацию другого человека. Эти данные могут быть использованы как мошенниками, так и исполнительными органами власти для поиска должника. Таким образом, размещенная пользователями информация при заполнении профиля может в дальнейшем его идентифицировать. Такой информацией может быть увлечения, пол, возраст, место работы и так далее. Оператор обязан публиковать на своем сайте политику обработки персональных данных, это условие содержится в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39].

Пользователь, регистрируясь в социальной сети, должен дать свое согласие о предоставлении информации. Если такого согласия не будет, он не сможет пользоваться данным сервисом. Данное требование распространено в деятельности Интернет-компаний и обусловлено спецификой информационных правоотношений в сети Интернет. Любой зарегистрированный пользователь может просмотреть информацию о других пользователях сети, например, фамилию, имя, отчество, место и дату рождения, место учебы и работы, фото, видео, друзей и список интересов.

Регистрируясь на определенном ресурсе, обычно пользователю предлагается ознакомиться с правилами и условиями обработки персональных данных. При согласии пользователь должен поставить отметку. Так как пользователь сам является собственником личной информации, он обязан ознакомиться с данными правилами, а также узнать возникают ли у него какие-либо обязательства при согласии. Данное решение не может быть заменой получения согласия, установленного действующим

законодательством Российской Федерации в сфере персональных данных. Кроме этого, необходимо самостоятельно решить, хочет ли пользователь предоставить личную информацию и какую именно. Большинством социальных сетей предусмотрена функция «приватности». С помощью нее пользователи могут сами ограничивать информацию о себе третьим лицам.

На практике организациям – собственникам социальных сетей не представляется возможным отделить персональные данные от всей информации, которую размещает пользователь. В их документации об обработке персональных данных идет разделение на персональные данные и иную предоставленную информацию.

Сбор и поиск информации производятся различными методами. Например, с помощью рассылки специальных программ или используя сервис социальных сетей. Обязательным условием должна быть необходимость разъяснений в доступной форме условия обработки и хранения персональных сведений на серверах. Необходимо предоставлять возможность отказаться от обработки своих данных. Обработка сведений, которые необходимы для предоставления услуг пользователю, должна быть только в исключительных случаях и реализована с помощью настройки каких-либо программ, либо в самом в браузере.

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] предоставляет возможность органам государственной власти запрашивать персональные сведения у различных организаций, если они имеют соответствующие полномочия. Компании, владеющие социальными сетями, получив от данных органов официальный запрос, должны предоставить нужные данные. Пользователям, активно пользующимся сетью Интернет, следует помнить о том, что выложенная информация в определенных законом случаях может быть в любой момент истребована государственными органами. Органы государственной власти достаточно часто на практике пользуются социальными сетями для поиска граждан. Более того, для этой цели были разработаны Федеральной службой судебных

приставов «Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе» [7].

Искать могут как обычных граждан, так и выявлять деятельность целых компаний. Проанализировав содержимое профиля субъекта персональных данных, судебные приставы, могут быстро определить местонахождение должника, а также его имущества. Кроме этого, изучаются Интернет-страницы его друзей, коллег, и даже родственников. Судебные приставы могут запросить информацию у Интернет-провайдеров. Таким образом, в распоряжении будет IP-адрес, по которому можно найти того или иного человека. Федеральный закон от 21 июля 1997 года № 118-ФЗ «О судебных приставах» [42] дает право получать различную информацию, если она необходима. При определении местонахождения пользователя, пристав сообщает ему о возбуждении исполнительного производства. Должники, как многие другие люди, в соцсетях оставляют много сведений о себе. На основании этих данных приставы устанавливают место работы, место жительства, а анализ информации об увлечениях и интересах, позволяет определить организации и места, где бывает должник. На практике приставы обычно используют вымышленное имя, с помощью которого получают необходимую им информацию.

В 2014 году Роскомнадзор обозначил свою позицию о создании фальшивых аккаунтов. Позиция на этот счет такова, что при создании фальшивого аккаунта используются персональные данные другого человека, а это прямое нарушение закона, так как цель создания такого аккаунта не может быть признана социально значимой. Большинство популярных социальных сетей являются сторонниками политики «реальных имен». Роскомнадзор взаимодействует с владельцами крупнейших социальных сетей по части удаления ненастоящих аккаунтов.

Смотря на опыт иностранных государств, можно привести в пример США, где существует Закон о конфиденциальности электронных коммуникаций [51]. По этому документу правоохранительным органам

можно получать доступ к электронной почте, переписке в социальных сетях без какого-либо судебного решения. Нет никаких определенных правил, закрепленных законодательно, по обеспечению безопасности обработки персональных сведений в Интернете. Операторы персональных данных должны самостоятельно принимать определенные меры по защите данных своих пользователей [51].

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] устанавливаются организационные, правовые и технические меры по защите данных своих пользователей. К примеру, к техническим требованиям, предъявляемым к операторам, относится применение сертифицированных средств защиты информации.

Одним из самых распространенных видов преступлений, совершаемых через социальные сети, являются случаи, связанные с совершением мошеннических действий против собственности граждан. Так, например, неправомерный доступ к странице пользователя социальной сети. Действия мошенника направлены на вымогательство денежных средств у друзей взломанного пользователя с помощью рассылки сообщений, где якобы он сообщает, что его банковская карта заблокирована, а он сейчас находится в тяжелой жизненной ситуации и ему срочно нужны деньги. Мошенник может попросить предоставить ему данные карточки, а также проверочный код, из смс-сообщения, либо попросить перевести определенную сумму денег на карту мошенника. Затем преступник выключает телефон, становится недоступным. Простому пользователю отследить его не реально. Предполагается, что потерпевший не станет обращаться в правоохранительные органы по поводу списания некрупной суммы.

Важно и то, что согласно Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], меры, достаточные для осуществления необходимых требований, определяются самим оператором.

Нельзя не сказать о мерах, принимаемых в Европейском союзе по обеспечению безопасности оказания услуг по обработке персональных

данных и защиты конфиденциальной информации. Директива Европейского парламента 2002/58/ЕС [49] – один из важнейших документов в отношении обработки персональных данных и защиты конфиденциальности в сфере электронных средств связи. Согласно этому документу, провайдер услуг обязан использовать нормы, которые относятся исключительно к авторизованным пользователям [49].

В настоящее время все чаще практикуется анализ работодателем профиля своего работника в соцсетях. Зачастую он обнаруживает там некорректные сообщения или фотографии. Как следствие, данного гражданина не берут на работу, либо увольняют, если он уже трудоустроен. Так, например, учительницу вынудили уволиться из-за ее фотографии в купальнике, размещенной в одной социальной сети. Примечательно, что купальник был закрытым, а сама учительница является членом Федерации зимнего плавания. Такие меры являются абсолютно противозаконными. В данном случае ущемляется конституционное право на невмешательство в личную жизнь. По статье 2 Трудового кодекса [34] и изложенным там принципам трудовых отношений, гражданин имеет право распоряжаться своими способностями к труду, выбирать профессию и род деятельности. Работники равны в своих правах и возможностях. Согласно Конституции Российской Федерации [4] у всех граждан существует право неприкосновенности частной жизни. Тем не менее, такие ситуации возникают все чаще. Работодатели просматривают социальные сети сотрудников и обнаружение непонравившейся информации может стать поводом для увольнения, но под другим предлогом.

Что же касается обработки в сети персональных данных несовершеннолетних, то на законодательном уровне практически отсутствуют какие-либо нормы.

Обоснованно считать, что необходимо обязать операторов обработки персональных данных ограничивать доступ чужих пользователей к персональным сведениям.

В каждой стране обработка персональных данных в соцсетях развивается по-разному. Владельцам Интернет-ресурсов приходится перенимать зарубежный опыт ввиду минимального правового регулирования.

3.2 Обеспечение защиты персональных данных в организациях

В российских организациях решения по защите персональной информации формируются на базе мер организационно-технического характера. Эти меры должны соответствовать, во-первых, Конституции Российской Федерации [4], во-вторых, Федеральному закону от 27 июля 2006 года №152-ФЗ «О персональных данных» [39], а также специальным требованиям регуляторов, к которым относятся Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор, Федеральная служба по техническому и экспортному контролю – ФСТЭК, Федеральная служба безопасности – ФСБ.

Роскомнадзор проверяет все организационные мероприятия, это его зона ответственности. Федеральная служба по техническому и экспортному контролю вместе со своими территориальными органами является вторым регулятором. ФСТЭК контролирует меры, проведенные в области технической защиты информационных систем обработки персональных сведений. Она проверяет технические средства защиты информации и использующиеся не криптографические методы и способы защиты персональных сведений.

Федеральная служба безопасности – это третий регулятор. Данная служба наделена обязанностью определять особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, а также предоставляет услуги по шифрованию персональной информации при ее обработке в информационных системах и осуществляет контроль в данной сфере.

Словосочетание в определении термина персональных данных «любая информация» позволяет практически все организации записать в операторы персональных данных. Государственные структуры, банки, Интернет-магазины, социальные сети – все они являются операторами персональных данных.

Ответственность за нарушение норм в сфере обработки и защиты персональной информации может быть административной, гражданско-правовой, дисциплинарной. В отдельных случаях предусмотрено также уголовное наказание.

Кроме юридической ответственности, за нарушение процедуры обращения с персональными данными можно поплатиться деловой репутацией и потерей клиентов. Таким образом, исполнение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] и соблюдение предписаний, регулирующих и контролирующих область персональных данных структур в интересах самих организаций.

В соответствии с законодательством, персональные данные разделяют на четыре категории. Учреждения организовывают систему защиты персональных сведений в зависимости от имеющейся категории.

Внедрение полноценного комплекса обеспечения защиты информационной системы персональных данных, где обрабатываются данные граждан об их расе, национальности, вероисповедании и здоровье, интимной жизни, а также политических и философских взглядах будет самым трудоемким. Данные сведения входят в категорию специальные персональные данные. Эту информацию необходимо защищать особенно внимательно.

Биологические и физиологические характеристики, по которым может быть идентифицирован субъект составляют биометрические персональные данные. К их защите также применяются высокие требования.

Организация, получившая письменное согласие от своего клиента на обработку его имени, фамилии, отчества, даты и места рождения, домашнего

адреса, рода занятий и контактной информации, становится оператором общедоступных персональных данных. По сравнению с остальными категориями, степень защиты этих данных самая низкая.

Четвертая категория – иные персональные данные – включает в себя все данные, которые не могут быть классифицированы как специальные, биометрические или общедоступные, но которые могут быть использованы для идентификации владельца данных. Защита иных персональных данных меньше, чем биометрических или специальных данных. Однако требования безопасности больше, чем в случае общедоступной информации.

В соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [16], операторы при выборе способов защиты, должны определить численность субъектов персональных данных. Разделяются информационные системы персональных данных, в которых обрабатывается менее 100 тысяч и более 100 тысяч данных субъектов.

Чтобы должным образом обеспечить безопасность обработки персональных данных, сначала необходимо выявить наиболее вероятные угрозы. Даже если организация обрабатывает лишь общедоступные данные, это совсем не значит, что защита их не так важна. Абсолютно все системы должны гарантировать защиту от незаконных операций, таких как копирование, распространение, уничтожение, блокирование или модификация. Инфраструктура для комплексной защиты информационных систем персональных данных должна учитывать вероятность существования внутреннего нарушителя. Личная информация может быть скомпрометирована любым сотрудником, как преднамеренно, так и по неосторожности. Меры, предотвращающие незаконный доступ, а также способствующие повышению надежности и отказоустойчивости информационной системы, направленные на сохранение целостности и

доступности информации внутри системы, представлены в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39]:

– необходимо выявить масштабность информационной системы и определить категорию персональных данных, сформировать угрозы безопасности;

– ввести организационно-технические способы по защите информации, которые будут согласованы со всеми уровнями безопасности;

– осуществить те способы защиты информационной системы, которые имеют сертификаты соответствия ФСТЭК или ФСБ;

– перед обработкой персональных данных провести комплексный аудит безопасности информационной системы в целом, отдельных компонентов безопасности;

– установить и реализовать систему учета носителей информации ограниченного использования;

– добавить такие функции как резервное копирование и восстановление данных системы при их модификации или удалении;

– в зависимости от должностных обязанностей и уровней доступа определить правила доступа сотрудников к персональным данным в информационной системе;

– внедрить инструменты для аудита и протоколирования действий сотрудников с персональными данными;

– непрерывно следить за соблюдением правил безопасности работы с персональными данными и осуществлением защиты аппаратного и программного обеспечения информационной системы персональных данных.

В Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] говорится о защите персональных сведений в целом. Конкретные же нормы прописаны в Приказе от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и

технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27]:

– обеспечить защиту идентификации и аутентификации пользователей, компонентов системы и персональной информации. Для исполнения данного требования необходимо сопоставить уникальные идентификаторы объектов и субъектов путем применения механизмов авторизации и разграничения прав;

– необходимо использовать определенное системное и прикладное программное обеспечение, ограничив программное окружение. Полномочия на изменение набора системных компонентов и разрешенного программного обеспечения должны быть недоступны для пользователей. Необходимо обеспечивать доступ к функциям только согласно своей роли. Это обеспечит защиту от случайного или намеренного вторжения в информационную систему;

– необходимо вести учет всех съемных носителей;

– необходимо вести непрерывное наблюдение и контролировать происходящее в системе. Вести журнал аудита и надежно его защищать;

– обязательно использовать антивирусные программные средства во избежание утечки конфиденциальной информации, а также частичного или полного выхода из строя информационной системы;

– использовать системы обнаружения и предотвращения вторжений. Это позволяет проводить анализ и выявлять незаконный доступ на уровне сети или компьютерной системы, попытки превышения полномочий или внедрения вредоносных программ, а также сразу принимать меры по устранению угроз: информировать сотрудника службы безопасности, перезагружать соединение, блокировать трафик и так далее;

– использовать системы целостности для защиты от несанкционированного изменения, повреждения информационной системы, а также восстановления поврежденных компонентов и информации;

– проводить регулярный осмотр уровня безопасности информационной системы. Развернутые программные компоненты, аппаратные средства и установленные настройки должны обеспечивать непрерывную и полную защиту процедур обработки и хранения информации в соответствии с определенным классом информационной системы.

Список мер, которые ФСТЭК предписывает соблюдать для реализации системы безопасности информационных систем персональных данных, не ограничивается несколькими положениями. Приказ от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [27] определяет требования к средствам виртуализации, каналам связи, конфигурации информационной системы персональных данных, классам компьютерного оборудования, антивирусным системам и другим параметрам защиты. При построении защищенной системы, кроме данного приказа ФСТЭК, необходимо также руководствоваться Приказом ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [26].

Невозможно разработать, а затем и внедрить полный комплекс защитных мер, не проработав нормативно-правовую базу, не имея навыков настройки технических средств и глубокого знания принципов работы программного обеспечения, осуществляющего информационную безопасность. Защита персональных данных одним сотрудником не является выполнимой задачей. Одна ошибка на любом уровне организации защиты

чревата большими штрафами со стороны регулирующих органов и потерей данных.

Работник, не обладающий компетенцией в области информационной безопасности, может изучить законодательство и затем определить какую категорию персональных данных обрабатывает его организация. Пошаговые инструкции, размещенные в свободном доступе, помогут разработать регламент информирования субъектов персональных данных о сборе информации, а также оформить уведомление в Роскомнадзор о деятельности организации в качестве оператора персональных данных. Определение ролей, разграничение доступа и фиксирование того, какие сотрудники имеют доступ и какие операции они вправе осуществлять с персональными данными, является доступной задачей для специализированного программного обеспечения.

Без участия специалиста, обладающего специальными знаниями, при разработке политики безопасности, а также при определении текущих угроз не обойтись. Процесс внедрения программно-аппаратных комплексов от выбора до активного использования программного обеспечения и оборудования требует полного понимания документации регуляторов ФСТЭК и ФСБ. Специалист должен хорошо разбираться в классах компьютерного оборудования, антивирусов и брандмауэров, а также знать, как гарантировать конфиденциальность и реализовывать отказоустойчивое подключение секторов информационных систем персональных данных.

Но даже обладающий подходящей квалификацией специалист по информационным технологиям или информационной безопасности не в силах внедрить, а тем более поддерживать в информационной системе персональных данных подсистему информационной безопасности без соблюдения некоторых условий. Деятельность, связанная со средствами технической защиты, лицензируется ФСТЭК. Так, перед оператором персональных данных стоит задача получения лицензии от этого регулятора.

Крупные компании могут позволить себе нанять штат специалистов в области информационной безопасности, затем выполнить все необходимые условия для получения лицензии ФСТЭК, и далее самостоятельно создать и поддерживать систему обеспечения защиты персональных данных.

Небольшим же организациям, которые обрабатывают персональные данные, содержать штат специалистов по информационной безопасности трудно выполнимо. Оптимальным решением в данном случае будет привлечение лицензиатов ФСТЭК. Это такие организации, которые профессионально занимаются защитой информации. Специалисты лицензиатов имеют все знания нормативной и технической базы, а также большой опыт создания комплексных систем информационной безопасности.

Рассматриваемая тема особенно актуальна, поскольку все более широкое использование компьютерных технологий и технологий обработки информации, а также увеличение объема массивов данных вызывают новые правовые проблемы, требующие от работодателей своевременного реагирования и принятия мер.

3.3 Рекомендации по совершенствованию законодательства в сфере защиты персональных данных

В настоящее время важной проблемой остается правовое регулирование персональных данных [6, с. 4], а главное – его применение на практике. Целью должно являться создание целостной системы по обработке и защите персональных данных, которая будет отвечать потребностям как отдельных субъектов, так и интересам всего государства.

Информационное общество стремительно развивается, что приводит к отставанию в правовом регулировании в этой области. При условии создания работающей нормативной базы, отвечающей полной информационной безопасности, защиты конфиденциальных данных, реализации свободного доступа к информации можно говорить о вхождении российского

информационного сообщества в мировое информационное общество. Сейчас есть основания говорить о пробелах в законодательстве о защите персональных данных.

Согласно определению, под персональными данными понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [39]. Существует мнение, что по этому определению к персональным данным можно отнести все относящиеся к нему данные, как например, марка смартфона, номер банковской карты, модель автомобиля, часто посещаемые общественные места (кафе, магазины). И если эти данные считать персональными, то и обрабатывать их нужно в соответствии с законодательством. Более того, в некоторых случаях указанное определение не позволяет однозначно ответить на вопрос, считаются ли те или иные данные персональными. Оптимальным будет решение ограниченно интерпретировать и рассматривать в качестве персональных данных только ту информацию, которая сама по себе является достаточной для идентификации гражданина. В литературе можно встретить предположение о том, что широкое определение персональных данных противоречит принципу формальных определений в правовых нормах. Такое широкое определение дает право называть персональной практически любую информацию. Это во многом затрудняет работу органов власти в области персональных данных, расширяя сферу их полномочий так, что на практике становится невозможным применение положений законодательства о персональных данных [45].

Однако, согласно пункту 1 статьи 4 Общего регламента по защите данных GDPR [50], под персональными данными понимается любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных). Это определение сопровождается комментарием, что определяемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, по его

идентификатору, например, имени, идентификационному номеру, местонахождению, онлайн-идентификатору или специфическим характеристикам. К последним относятся физические, психологические, генетические, психические, экономические, культурные и социальные характеристики субъекта [50]. Можно сделать вывод о том, что GDPR [50], как и Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], дает широкое определение персональных данных. Представляется, что только широкое определение позволяет достичь целей регулирования обработки персональных данных, главным из которых является защита частной жизни, личной и семейной тайны.

Сегодня уровень развития и проникновения в жизнь человека информационных технологий таков, что он непрерывно передает личную информацию различным организациям. Может показаться, что эта информация незначительная, но в то же время, если соединить мельчайшие кусочки этой информации при помощи компьютерных технологий, то создастся настолько полная картина образа человека, что идентифицировать его можно с легкостью. Конечно, эта информация позволяет манипулировать человеком. Чем больше личной информации о человеке собирается и обрабатывается, тем больше вероятность того, что на его жизнь можно повлиять, и тем больше вероятность того, что его права будут нарушены.

Если обратиться к преамбуле в GDPR [50], то оттуда ясно, что физических лиц можно сопоставить с их устройствами, а именно сетевыми идентификаторами, приложениями, IP-адресами, файлами cookie. Кусочки этой информации соединяются воедино и создается идентифицированный профиль человека. Профилирование – любая форма автоматической обработки персональных данных, состоящая в использовании персональных данных для оценки определенных характеристик человека, в том числе для анализа или прогнозирования его действий, экономического положения, состояния здоровья, личных предпочтений и интересов, целостности, поведения, местоположения и перемещений [50].

Исходя из вышесказанного делается вывод о том, что любая информация о человеке содержит микрочастицы идентификации, а, следовательно, должна быть защищена законом для защиты фундаментальных прав и свобод человека, включая право на неприкосновенность частной жизни. Именно поэтому широкое определение персональных данных, содержащееся в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], должно трактоваться буквально.

В том случае, если нельзя однозначно сказать о том, является ли информация персональными данными, необходимо считать ее таковой, что подтверждается определением персональных данных, представленным в GDPR [50]. Большой объем такой информации и сложность соблюдения требований законодательства о персональных данных при ее обработке не означает, что широкое определение персональных данных является размытым.

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] определяет следующие принципы обработки 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. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность,

а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.» [39] В связи с этим, включение в гражданско-правовой договор, а также в трудовой договор требования о предоставлении избыточных персональных данных является прямым нарушением закона. Тем не менее, Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] не предусматривает требуемого минимума персональных данных и, следовательно, не устанавливает юридическую ответственность за это [43]. Как следствие, на практике операторы зачастую злоупотребляют своим правом на сбор и обработку персональных данных [32, с. 132]. Кроме того, в пункте 7 статьи 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39] указано, что «хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.» [39] На практике происходит то, что организации издают локальные нормативные документы, где прописывают срок хранения персональных данных на свое усмотрение. Это может быть, как 5 лет, так и 75 лет. Возникают вопросы в обоснованности этого права. Таким образом, необходимо законодательно ограничить срок хранения персональных данных, а также ввести обязательный порядок уничтожения таких данных.

Что касается персональных данных работников организации, согласно статье 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О

персональных данных» [39], они дают письменное согласие на их обработку. При этом по нормативному документу «Требования к защите персональных данных при их обработке в информационных системах персональных данных» [16] оператором обработки персональных данных является организация или лицо, уполномоченное на это. Защита персональных данных – обязанность оператора. Информационная система при этом будет состоять из базы персональных данных, а также технических средств, обеспечивающих обработку персональных данных. Однако учреждение не может гарантировать субъекту сохранность его персональных данных. Работодатель обязан ознакомить своего работника с уровнем защиты его персональных данных и условиями информационной безопасности его персональных данных. Таким образом, на локальном уровне должен быть разработан нормативный документ об информационной безопасности персональных данных.

В соответствии с «Требованиями по защите персональных данных при их обработке в информационных системах персональных данных» [16] операторы обязаны контролировать выполнение требований безопасности, но на практике выявляется большое количество нарушений. Это говорит о том, что операторы уделяют недостаточно внимания к безопасности информационных систем.

В правоприменительной практике имеются серьезные организационные, технические, кадровые и правовые трудности. Не хватает организационной и технической базы, а также специалистов в области информационной безопасности. При совершении киберпреступлений нет специального оборудования, способного определить местоположение откуда он было совершено. Также существует сложность в определении субъекта и предмета преступления, его квалификации и сборе доказательств, подтверждающих факт преступления.

Нередко преступник является внутренним нарушителем, лицом, работающим в данной организации и имеющим доступ к персональным

данным других сотрудников. Внутри организации режим информационной безопасности часто имеет большое количество уязвимостей. Подобный внутренний саботаж в настоящее время широко распространен. Преступники внедряют ошибочные решения в процесс управления и хозяйственной деятельности, дезинформируют сотрудников и завладевают ключевой информацией. Производство дезорганизовано, интеллектуальная собственность незаконно получена. Человеческий фактор является одной из главных угроз информационной безопасности организации [33, с. 95], а незаконное использование чужой личной информации – одна из основных уязвимостей компании.

Таким образом, основной проблемой информационной безопасности персональных данных в организациях является субъективный фактор, а именно честность и соблюдение операторами всех требований, а также внимательность граждан к своим персональным данным.

Напоминание пользователям о необходимости соблюдения правил информационной безопасности должно быть основным правилом каждого оператора и работодателя. Игнорирование принципов безопасности может привести к значительным экономическим потерям [10, с. 115].

Что касается информационной безопасности в сети, пользователи размещают огромное количество персональной информации о себе, тем самым позволяя воспользоваться этой информацией злоумышленникам.

Необходимо информировать пользователей сайтов о возможности ограничить доступ к своим данным, повышать грамотность в сфере информационных технологий со школьного возраста [30, с. 37].

Одной из мер по обеспечению безопасности персональных данных при использовании Интернета является электронная подпись [2]. Эту подпись может получить любой гражданин, заплатив определенную сумму. Но в настоящий момент не каждый может это сделать. Необходимо рассмотреть возможность бесплатного обеспечения пользователей электронной подписью.

Кроме того, необходимо определить срок хранения персональной информации в организации на законодательном уровне, а также установить обязательную процедуру ее уничтожения по истечении данного срока. Ввести для работодателей обязанность ознакомления своих работников с уровнем защиты, а также условиями информационной безопасности их персональных данных.

Собственникам сайтов в Интернете, а также провайдерам необходимо уведомлять пользователей о том, что при взаимодействии с сайтами осуществляется сбор и обработка персональных данных, в ясной и понятной форме раскрывать виды и методы сбора данных, указывать конкретные цели и способы использования данных, четко и открыто объяснять возможность отказаться от согласия на сбор и использование данных, указывать конкретные условия и способы хранения личных данных, прекращать сбор и обработку в случае получения отказа, обеспечивать свободный доступ граждан для ознакомления с собранной о них информацией.

Также существует проблема с выполнением операторами обязательства уведомлять Роскомнадзор. С одной стороны, операторы подходят к выполнению этого обязательства формально, с другой стороны, само учреждение не располагает достаточными ресурсами для разбора всех поступающих уведомлений и, следовательно, нет возможности оперативного выявления рисков безопасности персональных данных и реагирования на них. В этой связи можно было бы применить зарубежную практику, заложенную в Регламенте ЕС 2016/679 [50] о защите физических лиц при обработке персональных данных, и частично отказаться от обязательства операторов уведомлять Роскомнадзор. Осуществить это можно с помощью расширения перечня, указанного в части 2 статьи 22 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [39], когда такое уведомление не требуется.

Важным вопросом остается возможность утечки персональных данных в сети Интернет. Базы персональных данных представляют большой интерес

у преступников, так как в сети широко распространена практика продажи баз данных различным компаниям. Эту проблему можно решить, разработав собственное программное обеспечение, оптимизировав систему защиты устройств пользователей, проработать и улучшить методы обнаружения и расследования эпизодов кражи баз данных, ужесточить законодательство в части наказаний за правонарушения и преступления в области защиты персональных данных.

Важным аспектом является обеспечить невозможность кражи персональной информации из закрытых баз данных, предназначенных для служебного пользования. Такая проблема есть в государственных и муниципальных учреждениях. Вероятнее всего, в данном случае присутствует незащищенность и наличие ошибок в информационных системах, несанкционированный доступ, нарушение сотрудниками правил конфиденциальности. В этом случае помогут исправить ситуацию те же рекомендации, что и при обеспечении безопасности персональных данных в сети Интернет.

Необходимо провести реформу существующего законодательства в сторону защиты прав отдельных субъектов при обработке их персональных данных в информационных системах, а не на обеспечение защиты данных в целом.

Важнейшим фактором защиты персональных данных является деятельность и ответственность самих субъектов персональных данных. Следуя определенным рекомендациям при работе в сети Интернет, пользователи могут предотвратить подавляющее большинство незаконных действий со своими данными:

– не скачивать и не устанавливать приложения и программы из непроверенных источников;

– использовать только лицензионные антивирусные программы, обновлять их до актуальной версии, периодически проверять устройство на наличие вирусов;

– использовать только лицензионное программное обеспечение на своем устройстве;

– не пользоваться общедоступными или непроверенными устройствами;

– не предоставлять личную информацию третьим лицам;

– не посещать сайты, содержащие незаконную или сомнительную информацию;

– своевременное обновлять и устанавливать необходимые подписи, способствующие сохранению безопасного доступа, отправляемые производителем.

Установление необходимого уровня утвержденных различных мер по защите информации от незаконного доступа, уничтожения, модификации, блокирования, копирования, распространения и других противоправных действий очень сложно на практике. В частности, для определения того, какую меру следует использовать, необходимо в первую очередь определить уровень ее защиты.

Когда оператор в отношении базы персональных данных установил необходимый уровень защиты, следующим уровнем регулирования является реализация как организационных, так и технических мер. Эти меры предписываются для каждого уровня защиты и регулируются соответствующим документом. Часто на практике возникает вопрос, должны ли быть сертифицированы методы защиты информации, применяемые оператором системы обработки персональных данных.

Федеральная служба по техническому и экспортному контролю России Информационным сообщением от 4 мая 2012 года № 240/24/1701 установила обязательный характер такой сертификации для защиты отдельных данных. Следует отметить, что обеспечение соответствия используемой оператором системы обработки персональных данных является достаточно трудоемким и дорогостоящим видом деятельности, так как в некоторых моментах оператор не сможет внедрить ее при отсутствии поддержки со стороны.

Необходимо продолжать совершенствовать и вносить коррективы в законодательство в этой области, используя зарубежный опыт, который подтверждает эффективность дальнейших реформ. Необходимо привлекать не только определенные ведомства, но и специалистов, занимающихся техническими вопросами в области защиты персональных данных, с целью повышения правовой безопасности обработки персональных данных.

Пространство становится виртуальным, но в этом виртуальном пространстве должны применяться правила, регулирующие обычное пространство. Сейчас любое вмешательство государства в функционирование сети ощущается пользователями как нарушение их прав, так как в настоящее время регулирование осуществляется посредством общественного контроля.

Интернет – это глобальная международная площадка, объединяющая весь мир. Следует вывод о том, что и законодательство в этой области должно быть единым и унифицированным. Необходимо избрать путь международного сотрудничества и стандартизации законодательства в данной сфере. Разработка единых правил приведет к упорядочению и единству отношений между субъектами сетевых отношений.

Безусловно, необходимо ввести должность специалиста по информационной безопасности в каждую отрасль. В каждой организации, в зависимости от ее численности, должен быть такой специалист, либо отдел по информационной безопасности. Сейчас функции такого специалиста возлагают на сотрудников отдела информационных технологий, системных администраторов, или того человека, который занимается компьютерной техникой. Но обеспечить защиту персональных данных и информации, хранящейся в организации – это колоссальный объем работы и ответственность. Эти функции не могут быть возложены как дополнительные.

Также необходимо ввести обязательный предмет в школе по компьютерной грамотности, чтобы со школьной скамьи человек имел представление о правилах поведения в Интернете, о том, как обезопасить

свои данные, не посещать подозрительные сайты и не переходить по различным ссылкам. Эти темы необходимо подробно изучать наряду с математикой или литературой. Также ввести в университеты целое направление по информационной безопасности, повышать престиж данного направления. Взять за практику обмен студентами для получения опыта между странами.

Ужесточить наказание за нарушения в области защиты персональных данных. В случае, если обработка персональных данных происходила без согласия субъекта, определить это деяние как уголовное. Штрафные санкции должны быть сопоставимы с европейскими штрафами. Для этого предлагаю в статье 5.39 Кодекса Российской Федерации об административных правонарушениях увеличить размер штрафа на должностных лиц до 100 000 рублей, в части 1 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях увеличить размер штрафа на граждан до 30 000 рублей, на должностных лиц – до 100 000 рублей, на юридических лиц – до 500 000 руб. В части 3 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях увеличить размер штрафа на граждан до одной тысячи пятисот рублей; на должностных лиц – от трех тысяч до 60 000 рублей; на индивидуальных предпринимателей – до 100 000 рублей; на юридических лиц – до 300 000 рублей. В части 4 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях увеличить размер штрафа на граждан до 20 000 рублей; на должностных лиц – до 60 000 рублей; на индивидуальных предпринимателей – до 150 000 рублей; на юридических лиц – до 400 000 рублей. В части 5 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях увеличить размер штрафа на граждан до 20 000 рублей; на должностных лиц – до 100 000 рублей; на индивидуальных предпринимателей – до 200 000 рублей; на юридических лиц – до 450 000 рублей. В части 6 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях увеличить размер штрафа для граждан до 100 000 рублей; на должностных

лиц – до 200 000 рублей; на индивидуальных предпринимателей – до 500 000 рублей; на юридических лиц – до 1 000 000 рублей. В части 7 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях увеличить размер штрафа на должностных лиц до 60 000 рублей.

Часть 2 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях переквалифицировать в статью Уголовного кодекса Российской Федерации и определить наказание в виде штрафа до 1 000 000 тысяч рублей, либо обязательных работ на срок до 360 часов, либо исправительных работ на срок до одного года, либо принудительных работ на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет), либо арестом на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет).

Учредить орган государственной власти, который будет заниматься исключительно контролем за исполнением законодательства в этой области.

Учредить международную организацию, которая будет заниматься поиском преступников, совершающих киберпреступления. Совместно с другими странами обеспечивать защиту персональных данных в сети Интернет. Утвердить международный документ, который будет действовать именно в области контроля за нарушениями в сети Интернет.

Ужесточить ответственность сотрудников, которые несерьезно относятся к защите персональных данных. Определить наказание не только в виде выговора или увольнения, но также существенного штрафа.

Определить максимальный срок хранения персональных данных субъектов, а также немедленное удаление этих данных по заявлению субъекта персональных данных.

Заключение

В настоящее время защита персональных данных является одной из острейших проблем современного мира. Необходимо установить правовые механизмы обработки и защиты персональных данных с учетом интересов как отдельно физического лица, так и всего государства. Информационное общество развивается быстро, а правовое регулирование в этой области идет медленно, оставляя нерешенными многие общественные отношения. Вступление российского информационного общества в глобальное информационное общество можно считать успешным при соблюдении ряда условий, предусмотренных нормативным законодательством, включая полную информационную безопасность, защиту конфиденциальной информации и реализацию свободного доступа к информации.

При разработке научных проблем реализации и защиты конституционных прав граждан на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России важно определить закономерности и перспективы их развития, стратегию законодательной и правоприменительной деятельности в этой сфере.

В настоящее время конституционное право на неприкосновенность частной жизни при обработке персональных данных и правовое регулирование конфиденциальности персональных и семейных данных требуют нового концептуального подхода как в связи с новыми угрозами, так и в связи с несовершенством законодательства.

В первой главе данного исследования было определено понятие персональных данных, рассмотрены их виды и особенности обработки, проведен обзор действующего российского законодательства в области защиты персональных данных, проанализированы нормативно-правовые акты, сделаны выводы об их сфере действия. Также в данной главе проведен обзор нормативно-правовых документов иностранных государств, рассмотрен их опыт реализации защиты персональных данных.

Во второй главе была изучена и проанализирована юридическая ответственность в области защиты персональных данных в Российской Федерации, изучены статьи и меры наказания при нарушении законодательства в сфере защиты персональных данных. Также был проведен обзор и анализ судебной практики России в сфере защиты персональных данных, рассмотрены конкретные примеры прецедентов и сделаны выводы по принятым решениям.

В третьей главе была проведена работа по анализу осуществления обработки и защиты персональных данных в организациях, сети Интернет, а также правового регулирования в данных областях. На основе проведенного исследования были внесены предложения по изменению нормативно-правовых актов Российской Федерации, регулирующих конституционное право на защиту персональных данных, сделаны выводы о том, как можно усовершенствовать законодательство, предложены меры по реализации защиты персональных данных как со стороны государства, так и со стороны организаций и граждан.

На основе проведенного исследования можно сформулировать ряд положений, направленных на защиту персональных данных. Исследование, проведенное в данной диссертации, имеет важное значение для правовой науки и ее применения на практике. Полученные результаты свидетельствуют о наличии проблем в законодательстве по защите персональных данных. Предлагаемые меры направлены на повышение правовой безопасности оборота персональных данных. Сформулированы основные результаты исследования.

1. Любая информация о человеке содержит мельчайшие частицы идентификации, а, следовательно, должна быть защищена законом для защиты фундаментальных прав и свобод человека, включая право на неприкосновенность частной жизни. В том случае, если нельзя однозначно сказать о том, является ли информация персональными данными, необходимо считать ее таковой.

2. Должны быть установлены правовые ограничения по сроку хранения персональных данных, а также утверждена процедура уничтожения таких данных.

3. Необходимо информировать пользователей сайтов о возможности ограничить доступ к своим данным.

4. Необходимо бесплатно предоставлять всем пользователям электронную подпись.

5. Обязать всех работодателей ввести порядок ознакомления своих работников с уровнем защиты, а также условиями информационной безопасности их персональных данных.

6. Собственникам сайтов в Интернете, а также провайдерам необходимо уведомлять пользователей о том, что при взаимодействии с сайтами осуществляется сбор и обработка персональных данных, в ясной и понятной форме раскрывать виды и методы сбора данных, указывать конкретные цели и способы использования данных, четко и открыто объяснять возможность отказаться от согласия на сбор и использование данных, указывать конкретные условия и способы хранения личных данных, прекращать сбор и обработку в случае получения отказа, обеспечивать свободный доступ граждан для ознакомления с собранной о них информацией.

7. Частично отказаться от обязательства операторов уведомлять Роскомнадзор.

8. Распространять рекомендации для пользователей при работе в сети Интернет, где будет прописано:

– не скачивать и не устанавливать приложения и программы из подозрительных источников;

– использовать только лицензионные антивирусные программы, регулярно обновлять их и периодически проверять устройства на наличие вирусов;

– использовать только лицензионное программное обеспечение на своем устройстве;

– не пользоваться общедоступными или непроверенными устройствами;

– не предоставлять личную информацию третьим лицам;

– не посещать сайты, содержащие незаконную или сомнительную информацию;

– своевременное обновлять и устанавливать необходимые подписи, способствующие сохранению безопасного доступа, отправляемые производителем.

9. Ввести должность специалиста по информационной безопасности в каждую отрасль. В каждой организации, в зависимости от ее численности, должен быть такой специалист, либо отдел по информационной безопасности.

10. Ввести обязательный предмет в школе по компьютерной грамотности. Ввести в университеты целое направление по информационной безопасности, повышать престиж данного направления. Взять за практику обмен студентами для получения опыта между странами.

11. Ужесточить наказание за нарушения в области защиты персональных данных для организаций. В случае, если обработка персональных данных происходила без согласия субъекта, определить это деяние как уголовное. Увеличить размер штрафов в несколько раз.

12. Учредить орган государственной власти, который будет заниматься исключительно контролем за исполнением законодательства в этой области.

13. Учредить международную организацию, которая будет заниматься поиском преступников, совершающих киберпреступления. Совместно с другими странами обеспечивать защиту персональных данных в сети Интернет. Утвердить международный документ, который будет действовать именно в области контроля за нарушениями в сети Интернет.

14. Ужесточить ответственность сотрудников, которые несерьезно относятся к защите персональных данных. Определить наказание не только в виде выговора или увольнения, но также существенного штрафа.

15. Определить максимальный срок хранения персональных данных субъектов, а также немедленное удаление этих данных по заявлению субъекта персональных данных.

Тот факт, что право человека на неприкосновенность частной жизни признано в Конституции, недостаточен для обеспечения его полного осуществления в жизни. Необходимо обеспечить эффективную государственную защиту данного конституционного права.

Под государственной защитой понимается деятельность уполномоченных государственных органов и должностных лиц по уважению, обеспечению и защите прав и свобод человека и гражданина, являющаяся основой правозащитного механизма.

Уровень развития цифрового пространства определяет новые условия и бросает новые вызовы, главным из которых является оптимальный баланс между развитием экономики, социальных отношений в обществе и обеспечением защиты конституционных прав граждан на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных.

Список используемой литературы и используемых источников

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СЗ РФ. – 1994. – № 32. – Ст. 3301

2. Емельянников М. Как защищать персональные данные в интернете [Электронный ресурс.] / М. Емельянников. – Режим доступа: URL: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyhdannyh/kakzaschischat-personalnye-dannye-v-internete (дата обращения: 10.09.2020)

3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. - 2002. – № 1 (часть 1). – Ст. 1

4. 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 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // СЗ РФ. – 2020. – № 31. – Ст. 4398

5. Кудашкин Я.В. Правовое обеспечение безопасности обработки персональных данных в сети Интернет / Я.В. Кудашкин. – М.: МГУ, 2019. – 199 с.

6. Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: автореферат / А.В. Кучеренко. – Челябинск: Амурский государственный университет, 2010. – 23 с.

7. Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе» (утв. ФССП РФ 30.11.2010 № 02-7) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». –
Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_110026/ (дата обращения: 10.01.2021)

8. Определение Верховного суда Российской Федерации от 24 июня 2015 г. №18-АПГ15-7. – Режим доступа: URL:

http://www.vsrf.ru/stor_pdf.php?id=1350850 (дата обращения: 12.04.2020)

9. Определение Московского городского суда от 10 ноября 2016 г. № 33-38783/2016. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOCN&n=791207#09589893671368115 (дата обращения: 14.03.2020)

10. Петров Ю.И. Защищенность как одна из наиболее актуальных характеристик современного программного обеспечения / Ю.И. Петров // Информатизация образования и науки. – 2016. – № 2(30). – С. 106–116.

11. Положение об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (утв. Банком России 19.08.2004 № 262-П) // «Вестник Банка России». – 10.09.2004. – № 54.

12. Постановление Верховного Суда Российской Федерации от 13 августа 2015 г. №302-АД15-5169. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=434452#07211060915040974 (дата обращения: 28.03.2020)

13. Постановление Верховного Суда Российской Федерации от 15 июня 2015 г. №25-АД15-3. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=433503#06914157479671139 (дата обращения: 28.03.2020)

14. Постановление Девятого арбитражного апелляционного суда от 9 октября 2017 г. № 09АП-45101/2017. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=MARB&n=1319753#0980130556366267 (дата обращения: 01.04.2020)

15. Постановление Одиннадцатого арбитражного апелляционного

суда от 27 ноября 2017 г. № 11АП-15043/2017. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=RAPS011&n=128313#024186035089524327 (дата обращения: 01.04.2020)

16. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. – 05.11.2012. – № 45. – Ст. 6257

17. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // СЗ РФ. – 22.09.2008. – № 38. – Ст. 4320

18. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» // СЗ РФ. – 2008. – № 28. – Ст. 3384

19. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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» // СЗ РФ. – 2012. – № 14. – Ст. 1626

20. Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // СЗ РФ. –

05.12.2011. – № 49. – Ст. 7284

21. Постановление Правительства Российской Федерации от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи» // СЗ РФ. – 17.09.2007. – № 38. – Ст. 4552

22. Постановление Правительства Российской Федерации от 13 февраля 2019 г. № 146 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных» // СЗ РФ. – 18.02.2019. – № 7. – Ст. 673

23. Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» // СЗ РФ. – 2005. – № 36. – Ст. 3704

24. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14 ноября 2011 г. № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требований законодательства Российской Федерации в области персональных данных» [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_124430/ (дата обращения: 10.10.2019)

25. Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ») (Зарегистрировано в Минюсте России 10.09.2013 № 29935) // Российская газета. – Федеральный выпуск №

208. – 18.09.2013

26. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_167862/ (дата обращения: 29.09.2019)

27. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // «Российская газета». – Федеральный выпуск № 107. – 22.05.2013

28. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_147084/ (дата обращения: 29.09.2019)

29. Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных СДСЕ № 223. [Электронный ресурс]. – Режим доступа: URL: https://www.coe.int/ru/web/conventions/recent-changes-for-treaties/-/conventions/treaty/223/signatures?p_auth=RtIimtHh (дата обращения: 21.06.2020*)*

30. Солдатова Г.В. Российские школьники: приватность и

безопасность в Сети: доклад [Электронный ресурс] / Г.В. Солдатова //Междунар. конф. защиты персональных данных. М.: Ренесанс Москва Монарх Центр, 08.11.2016. – Режим доступа: URL: http:://zpd-forum.com/ (дата обращения: 20.10.2020)

31. Телина Ю.С. Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах / Ю.С. Телина. – М.: ФГКОУ ВО УП РФ, 2016. – 267 с.

32. Трошина С.М., Павловская А.В. Проблемы совершенствования мер защиты персональных данных / С.М. Трошина, А.В. Павловская // Вестник Томского государственного университета. Право. – 2017. - № 23. – С. 131-143.

33. Трошина С.М., Рязанова Т.П. Человеческий фактор как угроза информационной безопасности / С.М. Трошина, Т.П. Рязанова // Вестн. Урал. финансово-юридического ин-та. – 2016. – № 2(4). – С. 93–97.

34. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 01.04.2019) // СЗ РФ. – 2002. – № 1 (ч. 1). – Ст. 3

35. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. – 1996. – № 25. – Ст. 2954

36. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. – 10.03.1997. – № 10. – Ст. 1127

37. Утечки данных. Россия. 2019 год. Аналитический центр Infowatch. [Электронный ресурс]. – Режим доступа: URL: https://www.infowatch.ru/analytics/reports/27614 (дата обращения: 05.02.2021)

38. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 31.07.2006. – № 31 (1 ч.). – ст. 3448

39. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. – 31.07.2006. – № 31 (1 ч.). – ст. 3451

40. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // СЗ РФ. – 28.07.2014. – № 30. – ст. 4243

41. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СЗ РФ. – 2003. – № 28. – ст. 2895

42. Федеральный закон от 21 июля 1997 г. № 118-ФЗ «О судебных приставах» // СЗ РФ. – 28.07.1997. – № 30. – ст. 3590

43. Шередин Р.В. Защита персональных данных: новые требования: интернет-интервью 10.01.2012 [Электронный ресурс] / Р.В. Шередин. – Режим доступа: URL: http://oblteleset.ru/2012/10-01-2012-zashhita-personalnyxdannyx-novye-trebovaniya/ (дата обращения: 02.09.2020)

44. Act on the Protection of Personal Information Act No. 57 of (2003) [Электронный ресурс]. – Режим доступа: URL: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf (дата обращения: 25.12.2020)

45. Arkhipov V., Naumov V. The Legal Definition of Personal Data in the Regulatory Environment of the Russian Federation: Between Formal Certainty and Technological Development / V. Arkhipov, V. Naumov // Computer Law & Security Review. – 2016. – No. 32. – P. 872, 877, 883, 886

46. Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019) [Электронный ресурс]. – Режим доступа: URL: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf (дата обращения: 03.01.2021)

47. California Consumer Privacy Act of 2018 [Электронный ресурс]. – Режим доступа: URL: https://oag.ca.gov/privacy/ccpa (дата обращения: 14.11.2020)

48. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981 [Электронный ресурс]. – Режим доступа: URL: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

(дата обращения: 18.08.2020)

49. Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as last amended by Directive 2009/136/EC. – OJ L 337, 18.12.2009, p. 11-36. Special edition in Croatian: Chapter 13. – Vol. 052. – P. 224-249.

50. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 «On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)» [Электронный ресурс]. – Режим доступа: URL: http://ec.europa.eu/justice/dataprotection/reform/files/regulation_oj_en.pdf (дата обращения: 04.05.2020)

51. The personal data protection bill, 2018 [Электронный ресурс]. – Режим доступа: URL: https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (дата обращения: 17.02.2020)

52. The Personal Information Protection and Electronic Documents Act (PIPEDA) 13.04.2000 [Электронный ресурс]. – Режим доступа: URL: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf (дата обращения: 14.01.2021)