Введение

Современное общество все чаще встречается с информационным обменом в своей повседневной жизни. Каждый из нас регулярно сообщает о себе информацию, позволяющую напрямую или косвенно определить и идентифицировать нас. С учетом положений действующего законодательства Российской Федерации, такая информация является нашими персональными данными.

Согласно действующему Указу Президента Российской Федерации, персональные данные являются конфиденциальной информацией. Основным законом, регламентирующим вопросы в части персональных данных, является Федеральный закон №152-ФЗ от 27 июня 2006 года «О персональных данных»[1]. Согласно его положениям, персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Таким образом, все мы, как граждане своего государства, являемся субъектами персональных данных, в связи с чем, для нас становится актуальным вопрос о наших законных правах в части нашей жизни, а также законности использования этих сведений. Согласно закону «О персональных данных»[2], лица, осуществляющие любые действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных являются операторами персональных данных. Исходя из этого, в целях обеспечения выполнения

[1] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[2] Там же.

наших законных интересов и защиты нашей личной жизни необходимо знать и контролировать выполнение обязанностей, возложенных на оператора персональных данных. Защита персональных данных актуальна для большинства российских компаний, осуществляющих обработку персональных данных. Ведь под действие закона «О персональных данных»[3] попадают все организации, зарегистрированные в Российской Федерации и осуществляющие обработку персональных данных, независимо от вида отрасли, формы собственности и иных факторов.

Таким образом, защита персональных данных является одним из наиболее приоритетных направлений в существующей сфере обеспечения информационной безопасности в организациях различных форм и родов деятельности и изучение правового регулирования в области защиты персональных данных является актуальным вопросом.

Объектом дипломной работы выступают общественные отношения, связанные с защитой персональных данных.

Предметом дипломной работы является совокупность нормативных правовых актов, определяющих понятие и виды персональных данных, условия и принципы их обработки, правовое положение субъектов, участвующих в обороте персональных данных.

Цель дипломной работы – расширение и углубление научных знаний о вопросе правового регулирования отношений в области защиты персональных данных.

Для достижения поставленной цели необходимо решить следующие задачи:

- рассмотреть персональные данные как объект правовой охраны;

- рассмотреть нормативно-правовые акты в области защиты персональных данных;

---

[3] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

- изучить права субъекта и обязанности оператора при обработке персональных данных;

- рассмотреть меры по обеспечению выполнения оператором своих обязанностей;

- рассмотреть меры по обеспечению безопасности персональных данных при их обработке;

- проанализировать проблемы правового регулирования и правовой защиты персональных данных.

Методологическую основу исследования составили следующие методы: диалектический, логический, метод анализа и синтеза, сравнительно-правовой и другие.

Информационную базу дипломной работы составили законы и нормативные акты, теоретические труды таких авторов как: Баймакова И.А., Новиков А.И., Рогачев А.И., Хыдыров А.Х., Слепов О. и других.

1 Правовое регулирование в области защиты персональных данных

1.1 Персональные данные как объект правовой охраны

В соответствии с Законом № 152-ФЗ «О персональных данных»[4] персональными данными является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПДн). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПДн.

Состав и содержание персональных данных определяют операторы ПДн в зависимости от целей их обработки. Например, перечень персональных данных для популярных в последнее время систем лояльности клиентов компании, как правило, включают контактные данные, необходимые для связи с клиентами, и сведения о предоставленных услугах. Состав этих сведений не должен быть избыточен при этом оставаясь достаточным, чтобы «понимать» предпочтения клиента, его финансовые возможности, «отслеживать» его покупательскую историю и т.п.

Существуют случаи, когда цели, состав и содержание ПДн четко определяются законодательными и нормативно-правовыми актами. Это касается областей, где взаимоотношения между субъектами ПДн и операторами нуждаются в строгой регламентации. При этом в некоторых случаях субъект персональных данных обязан предоставлять оператору сведения о себе.

Например, функционирование определенных отраслей экономики связано с необходимостью обеспечения безопасности. Так, п. 5 ст. 11 ФЗ № 16 «О транспортной безопасности»[5] определяет необходимость создания единой государственной информационной системы обеспечения транспортной

[4] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

безопасности. Такая система должна состоять из централизованных баз персональных данных о пассажирах, включающих следующие данные: фамилия, имя, отчество; дата рождения; вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет); пункт отправления, пункт назначения, вид маршрута следования (беспересадочный, транзитный); дата поездки; пол; гражданство.

Регламентация состава и содержания ПДн касается отношений, связанных с трудовой деятельностью человека. Если речь идет о кадровой системе, к составу персональных данных относятся сведения, предусмотренные унифицированной формой учета кадров Т-2, утвержденной Постановлением № 1 Госкомстата России от 05.01.2004[6]. К таким сведениям относятся: фамилия, имя, отчество; дата рождения; место рождения; гражданство; номер страхового свидетельства; ИНН; знание иностранных языков; данные об образовании (номер, серия дипломов, год окончания); данные о приобретенных специальностях семейное положение; данные о членах семьи (степень родства, ФИО, год рождения, паспортные данные, включая прописку и место рождения); фактическое место проживания; контактная информация; данные о военной обязанности; данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т.п.).

Законодательство определяет различные категории персональных данных. К ним могут относиться общедоступные ПДн, специальные категории ПДн, категории ПДн, обрабатываемые в информационных системах персональных данных (далее ИСПДн), биометрические ПДн и другие.

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые в

[5] О транспортной безопасности: Федер. закон Росс. Федерации от 9 февраля 2007 г. Номер 16-ФЗ (ред. от 03.02.2014 г.) // СПС Консультант Плюс.

[6] Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты: Постановление Правительства Росс. Федерации от 5 января 2004 г. Номер 1 // СПС Консультант Плюс.

соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов[7].

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

- субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;

- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья субъекта ПДн и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну;

- обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПДн;

- обработка персональных данных осуществляется в соответствии с законодательством РФ о безопасности, об оперативно-розыскной деятельности,

[7] Слепов О. Защита персональных данных // http://www.jetinfo.ru/stati/zaschita-personalnykh#gl_3.

а также в соответствии с уголовно-исполнительным законодательством РФ или необходима в связи с осуществлением правосудия.

Выделяют следующие категории персональных данных, которые обрабатываются в ИСПДн:

- Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

- Категория 2 – персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

- Категория 3 – персональные данные, позволяющие идентифицировать субъекта ПДн;

- Категория 4 – обезличенные и (или) общедоступные персональные данные.

Категорирование персональных данных при обработке в ИСПДн может также проводиться по параметру «объем обрабатываемых персональных данных». Под этим подразумевается количество субъектов, данные которых обрабатываются в информационной системе.

Этот параметр может принимать следующие значения:

- в информационной системе одновременно обрабатываются персональные данные более чем 100000 субъектов ПДн или персональные данные субъектов ПДн в пределах субъекта РФ или РФ в целом;

- в информационной системе одновременно обрабатываются персональные данные от 1000 до 100000 субъектов ПДн или персональные данные субъектов ПДн, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования;

- в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов ПДн или персональные данные субъектов ПДн в пределах конкретной организации[8].

Такое категорирование персональных данных необходимо для определения класса ИСПДн, от которого зависят меры по обеспечению безопасности ПДн при обработке в информационных системах.

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[9]. Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством РФ о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в РФ, уголовно-исполнительным законодательством.

Исходя из определения биометрических ПДн, к ним относятся фотографии и видеизображения субъектов ПДн. Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов ПДн могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения – в системах видеонаблюдения и т.п.

---

[8] Слепов О. Защита персональных данных // http://www.jetinfo.ru/stati/zaschita-personalnykh#gl_3.

[9] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

1.2 Нормативно-правовые акты в области защиты персональных данных

Основные нормативно-правовые акты, которые регламентируют обработку персональных данных:

- Международная нормативно-правовая документация в области защиты персональных данных – Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 года)[10].

- Федеральные законы РФ:

а) Основным законом Российской Федерации, затрагивающим вопросы информационной безопасности, является Конституция, принятая 12 декабря 1993 г.[11];

б) Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»[12];

в) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[13];

г) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[14];

д) Федеральный закон Российской Федерации «О безопасности» от 28 декабря 2010 г. № 310-ФЗ[15];

---

[10] О защите физических лиц при автоматизированной обработке персональных данных: Конвенция (Страсбург, 28 января 1981 года) // СПС Консультант Плюс.

[11] Конституция Российской Федерации: принята всенар. голосованием 12 дек. 1993 г. (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[12] О коммерческой тайне: Федер. закон Росс. Федерации от 29 июля 2004 г. Номер 98-ФЗ (ред. от 12.03.2014 г.) // СПС Консультант Плюс.

[13] Об информации, информационных технологиях и о защите информации: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 149-ФЗ (ред. от 24.11.2014 г.) // СПС Консультант Плюс.

[14] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[15] О безопасности: Федер. закон Росс. Федерации от 28 декабря 2010 г. Номер 310-ФЗ // СПС Консультант Плюс.

е) Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[16];

ж) Федеральный закон от 01 июля 2011 г. № 261-ФЗ «О внесении изменений в ФЗ «О персональных данных»[17];

з) Федеральный закон от 30 ноября 2011 г. № 363-ФЗ «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных»[18];

и) Кодекс Российской Федерации об административных правонарушениях[19];

к) Трудовой кодекс РФ – Глава 14. Защита персональных данных работника[20];

л) Уголовный кодекс РФ[21];

м) Гражданский кодекс РФ Часть 1[22] и Часть 2[23].

- Указы Президента РФ:

а) Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»[24];

б) Доктрина информационной безопасности РФ 9 сентября 2000 г. № Пр-1895[25];

---

[16] Об электронной подписи: Федер. закон Росс. Федерации от 6 апреля 2011 г. Номер 63-ФЗ (ред. от 28.06.2014 г.) // СПС Консультант Плюс.

[17] О внесении изменений в ФЗ «О персональных данных»: Федер. закон Росс. Федерации от 01 июля 2011 г. Номер 261-ФЗ // СПС Консультант Плюс.

[18] О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных»: Федер. закон Росс. Федерации от 30 ноября 2011 г. Номер 363-ФЗ // СПС Консультант Плюс.

[19] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[20] Трудовой кодекс Российской Федерации (ТК РФ) от 30 декабря 2001 г. Номер 197-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

[21] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[22] Гражданский кодекс Российской Федерации (ГК РФ) Часть 1 от 30.11.1994 г. Номер 51-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[23] Гражданский кодекс Российской Федерации (ГК РФ) Часть 2 от 26.01.1996 г. № 14-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

[24] Об утверждении перечня сведений конфиденциального характера: Указ Президента Росс. Федерации от 6 марта 1997 г. Номер 188 (ред. от 23.09.2005 г.) // СПС Консультант Плюс.

[25] Доктрина информационной безопасности РФ 9 сентября 2000 г. Номер Пр-1895 // СПС Консультант Плюс.

в) Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»[26];

г) Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[27];

д) Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[28].

- Постановления Правительства РФ:

а) Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»[29];

б) Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами,

---

[26] Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела: Указ Президента Росс. Федерации от 30 мая 2005 г. Номер 609 (ред. от 01.07.2014 г.) // СПС Консультант Плюс.

[27] О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента Росс. Федерации от 17 марта 2008 г. Номер 351 (ред. от 22.05.2015 г.) // СПС Консультант Плюс.

[28] О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента Росс. Федерации от 15 января 2013 г. Номер 31с // СПС Консультант Плюс.

[29] Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: Постановление Правительства Росс. Федерации от 15 сентября 2008 г. Номер 687 // СПС Консультант Плюс.

операторами, являющимися государственными или муниципальными органами[30];

в) 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»[31].

- Нормативные и методические документы ФСТЭК России:

а) Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.[32];

б) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 14 февраля 2008 г.[33];

в) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 г.[34];

г) Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"[35];

---

[30] Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: Постановление Правительства Росс. Федерации от 21.03.2012 г. Номер 211 (ред. от 06.09.2014 г.) // СПС Консультант Плюс.

[31] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства Росс. Федерации от 1 ноября 2012 г. Номер 1119 // СПС Консультант Плюс.

[32] Положение по аттестации объектов информатизации по требованиям безопасности информации: Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. // СПС Консультант Плюс.

[33] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. // СПС Консультант Плюс.

[34] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. // СПС Консультант Плюс.

[35] Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России

д) 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”[36];

е) Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.[37]

- Методические документы ФСБ России:

а) Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ РФ от 21 февраля 2008 года)[38];

б) Приказ ФСБ России от 10.07.2014 № 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"[39];

от 11 февраля 2013 г. Номер 17 // СПС Консультант Плюс.

[36] Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК от 18 февраля 2013 г. Номер 21 // СПС Консультант Плюс.

[37] Методический документ. Меры защиты информации в государственных информационных системах: Утвержден ФСТЭК России 11 февраля 2014 г. // СПС Консультант Плюс.

[38] Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации: Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. Номер 149/54-144 // СПС Консультант Плюс.

[39] 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: Приказ ФСБ России от 10.07.2014 г. Номер 378 // СПС Консультант Плюс.

- Нормативным документом РОСКОМНАДЗОРА является Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (С изменениями, согласно постановлениям Правительства Российской Федерации от 17 марта 2010 года № 160, от 24 марта 2011 года №210, от 16 мая 2011 года № 368)[40].

- Нормативным документом Минкомсвязи России является Приказ Минкомсвязи России от 14.11.2011 № 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 требованиям законодательства Российской Федерации в области персональных данных"[41].

[40] О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: Постановление Правительства Росс. Федерации от 16 марта 2009 г. Номер 228 (ред. от 22.05.2015 г.) // СПС Консультант Плюс.

[41] 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 требованиям законодательства Российской Федерации в области персональных данных: Приказ Минкомсвязи России от 14.11.2011 г. Номер 312 (ред. от 24.11.2014 г.) // СПС Консультант Плюс.

2 Права субъекта и обязанности оператора при обработке персональных данных

2.1 Субъект персональных данных и его права при обработке персональных данных

Отношения, связанные с обработкой персональных данных, регулируются Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[42]. Согласно закона субъектом персональных данных является любое физическое лицо, которое может быть прямо или косвенно определено или определяемо при использовании персональных данных. И именно человек вправе решать когда, кому и какие данные он предоставляет, а также он вправе проконтролировать как (каким образом) обрабатываются и кому передаются его персональные данные[43].

Согласно положениям данного закона, субъект персональных данных обладает следующими правами на доступ к своим персональным данным:

- правом на получение сведений, касающихся обработки его персональных данных;

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

- правом на получение от оператора сведений, касающихся обработки его персональных данных, в доступной форме, без содержания в них персональных данных, относящиеся к другим субъектам персональных данных, за

---

[42] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[43] Баймакова И.А. Обеспечение защиты персональных данных. Методическое пособие / И.А. Баймакова, А.И. Новиков, А.И. Рогачев, А.Х. Хыдыров, 2011. С. 49.

исключением случаев, когда имеются законные основания для раскрытия таких персональных данных;

- правом на получение сведений, касающихся обработки его персональных данных, предоставляемых субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Такой запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ и должен содержать:

а) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

б) сведения о дате выдачи указанного документа и выдавшем его органе;

в) сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя;

- право на повторное обращение к оператору, в случае, если сведения, касающиеся обработки персональных данных субъекта, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу;

- право направить оператору повторный запрос в целях получения сведений, касающихся обработки персональных данных субъекта, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

- право на повторное обращение к оператору или направление ему повторного запроса в целях получения сведений, касающихся обработки персональных данных субъекта, а также в целях ознакомления с обрабатываемыми персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса;

- право потребовать от оператора представления доказательств отказа в выполнении повторного запроса;

- право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые оператором способы обработки персональных данных;

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

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

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

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

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

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

к) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами[44].

Субъект персональных данных может быть ограничен в праве на доступ к его персональным данным в соответствии с федеральными законами, в том числе если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно–розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

[44] Исаев А.С. Правовые основы организации защиты персональных данных: учебное пособие / А.С. Исаев, Е.А. Хлюпина, 2014. С. 37.

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

- обработка персональных данных осуществляется в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

В случае обработки персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации субъект персональных данных имеет право:

- давать свое согласие на обработку персональных данных, оператору. Обработка персональных данных, в выше указанных целях, без предварительного согласия со стороны субъекта персональных данных не допускается;

- отзывать свое согласие на обработку персональных данных, у оператора. Оператор обязан немедленно прекратить обработку персональных данных по требованию субъекта персональных данных.

При принятии решений на основании исключительно автоматизированной обработки персональных данных, субъект персональных данных имеет право:

- запретить принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть

принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных;

- требовать у оператора предоставления разъяснений:

а) о порядке принятия решений на основании исключительно автоматизированной обработки его персональных данных;

б) о возможных юридических последствий такого решения;

в) о порядке защиты его прав и законных интересов.

- требовать у оператора предоставления возможности заявления возражения против такого решения. В случае поступления возражений со стороны субъекта персональных данных, оператор обязан в течении 30 дней, со дня получения возражений, рассмотреть поступившие возражения и сообщить о результатах его рассмотрения.

В случае, если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[45] или иным образом нарушает его права и свободы, субъекта персональных данных имеет право:

- обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

В соответствии с частью 4, статьи 9 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[46], письменное согласие субъекта

[45] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[46] Там же.

персональных данных на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

- подпись субъекта персональных данных.

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 от 06.04.2011 № 63-ФЗ "Об электронной подписи"[47] электронной подписью.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на оператора.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

2.2 Обязанности оператора персональных данных

В соответствии с определением, приведенным в ст. 3 Федерального закона «О персональных данных», оператор персональных данных – 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[48].

Таким образом, исходя из данного определения, Федеральный закон «О персональных данных» касается всех лиц, осуществляющих обработку ПДн, ни для каких организаций, предпринимателей либо иных лиц каких-либо

[47] Об электронной подписи: Федер. закон Росс. Федерации от 6 апреля 2011 г. Номер 63-ФЗ (ред. от 28.06.2014 г.) // СПС Консультант Плюс.
[48] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

исключений не сделано. Любая организация или физическое лицо, в том числе предприниматель, осуществляющее обработку данных субъектов персональных данных является оператором персональных данных[49].

В соответствии с положениями Федерального закона № 152 "О персональных данных"[50], оператор при сборе персональных данных обязан:

- предоставить субъекту персональных данных по его просьбе следующую информацию:

а) подтверждение факта обработки персональных данных оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые оператором способы обработки персональных данных;

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

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

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

ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[51];

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

---

[49] Баймакова И.А. Обеспечение защиты персональных данных. Методическое пособие / И.А. Баймакова, А.И. Новиков, А.И. Рогачев, А.Х. Хыдыров, 2011. С. 56.

[50] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[51] Там же.

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

к) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами;

- разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[52];

- предоставить субъекту персональных данных до начала обработки таких персональных данных, в случае, если персональные данные получены не от субъекта персональных данных, следующую информацию:

а) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

б) цель обработки персональных данных и ее правовое основание;

в) предполагаемые пользователи персональных данных;

г) установленные настоящим Федеральным законом права субъекта персональных данных;

д) источник получения персональных данных.

Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

- персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

---

[52] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

- оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

- предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц[53].

В случае получения обращения и/или запроса со стороны субъекта персональных данных (или его представителя) или уполномоченного органа по защите прав субъектов персональных данных, оператор обязан:

- сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[54], субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных;

- предоставить возможность ознакомления с персональными данными относящихся к соответствующему субъекту персональных данных, при обращении субъекта персональных данных или его представителя, либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя;

- дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[55] или иного федерального закона, который являлся основанием в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или

---

[53] Исаев А.С. Правовые основы организации защиты персональных данных: учебное пособие / А.С. Исаев, Е.А. Хлюпина, 2014. С. 42.

[54] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[55] Там же.

персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя;

- безвозмездно предоставить субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

- внести изменения в персональные данные в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются неполными, неточными или неактуальными;

- уничтожить персональные данные в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

- уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

- сообщать в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

В случае нарушения законодательства при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных оператор обязан:

- осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных, в случае

выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных;

- осуществить блокирование персональных данных, относящихся к субъекту персональных данных, в случае выявления в них неточностей при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

- уточнить персональные данные и снять блокирование либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных в течение семи рабочих дней со дня представления таких сведений;

- прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора, в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, в срок, не превышающий трех рабочих дней с даты этого выявления;

- уничтожить персональные данные или обеспечить их уничтожение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, в случае, если обеспечить правомерность обработки таких персональных данных невозможно;

- уведомить субъекта персональных данных или его представителя, об устранении допущенных нарушений или об уничтожении персональных данных, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, уведомить указанный орган;

- прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае достижения цели обработки персональных данных. Данные действия должны быть реализованы в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[56] или другими федеральными законами;

- прекратить обработку персональных данных или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором,

[56] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами;

- уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных. Данные действия должны быть реализованы в срок, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами;

- осуществить блокирование персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае отсутствия возможности уничтожения таких персональных данных в течение срока, указанного в частях 3 – 5 статьи 21 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[57], и обеспечить уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

[57] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

Также в Федеральном законе от 27.07.2006 № 152–ФЗ "О персональных данных"[58] отдельно оговорены обязанности оператора по уведомлению об обработке персональных данных. До начала обработки персональных данных оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных:

- оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

а) обрабатываемых в соответствии с трудовым законодательством;

б) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

в) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством РФ, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

г) сделанных субъектом персональных данных общедоступными;

д) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

---

[58] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

е) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

ж) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

з) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами РФ, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

и) обрабатываемых в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

- уведомление, предусмотренное частью 1 статьи 22 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[59], направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

а) наименование (фамилия, имя, отчество), адрес оператора;

б) цель обработки персональных данных;

в) категории персональных данных;

г) категории субъектов, персональные данные которых обрабатываются;

[59] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

д) правовое основание обработки персональных данных;

е) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

ж) описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[60], в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

з) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

и) дата начала обработки персональных данных;

к) срок или условие прекращения обработки персональных данных;

л) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

м) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ[61];

- уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 статьи 22 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[62], а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением

---

[60] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[61] Исаев А.С. Правовые основы организации защиты персональных данных: учебное пособие / А.С. Исаев, Е.А. Хлюпина, 2014. С. 47.

[62] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными;

- на оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов;

- в случае предоставления неполных или недостоверных сведений, указанных в части 3 статьи 22 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[63], уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов;

- в случае изменения сведений, указанных в части 3 статьи 22 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[64], а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

2.3 Меры по обеспечению выполнения оператором своих обязанностей

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[65]:

- оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным

[63] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[64] Там же.
[65] Там же.

законом от 27.07.2006 № 152–ФЗ "О персональных данных"[66] и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[67] и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[68] или другими федеральными законами. К таким мерам могут, в частности, относиться:

а) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

б) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

в) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[69];

г) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[70] и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике

---

[66] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[67] Там же.
[68] Там же.
[69] Там же.
[70] Там же.

оператора в отношении обработки персональных данных, локальным актам оператора;

д) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[71], соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

е) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников[72];

- оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;

- оператор, осуществляющий сбор персональных данных с использованием информационно–телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети;

---

[71] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[72] Исаев А.С. Правовые основы организации защиты персональных данных: учебное пособие / А.С. Исаев, Е.А. Хлюпина, 2014. С. 49.

- Правительство РФ устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152–ФЗ "О персональных данных"[73] и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами;

- оператор обязан представить документы и локальные акты, указанные в части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[74] настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[75], по запросу уполномоченного органа по защите прав субъектов персональных данных.

2.4 Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

---

[73] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[74] Там же.
[75] Там же.

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных[76].

Правительство РФ с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

---

[76] Исаев А.С. Правовые основы организации защиты персональных данных: учебное пособие / А.С. Исаев, Е.А. Хлюпина, 2014. С. 51.

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Состав и содержание необходимых для выполнения установленных

Правительством Российской Федерации в соответствии с частью 3 статьи 19 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[77] требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов РФ, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных

[77] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[78], ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

Проекты нормативных правовых актов, указанных в части 5 статьи 19 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[79], подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 статьи 19 Федерального закона от 27.07.2006 № 152–ФЗ "О персональных данных"[80], подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством РФ. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности,

---

[78] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[79] Там же.
[80] Там же.

и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных[81].

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства РФ с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

---

[81] Исаев А.С. Правовые основы организации защиты персональных данных: учебное пособие / А.С. Исаев, Е.А. Хлюпина, 2014. С. 53.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3 Проблемы правового регулирования и правовой защиты персональных данных

3.1 Проблемы реализации законодательства РФ о защите персональных данных

Остановимся подробнее на отдельных проблемах, возникающих при реализации некоторых положений законодательства РФ о защите персональных данных.

В настоящее время возник вопрос о расширении понятия «персональные данные» и обеспечения защиты таковых на территории РФ, вплоть до предоставления гражданину право на сетевое забвение. Теперь стала актуальной задача защиты личного сетевого пространства каждого человека.

Помощник президента РФ Игорь Щеголев на расширенной коллегия Роскомнадзора, которая состоялась 20 апреля 2015 г. заявил: «Интернет утратил невинность. Раньше он был инструментом свободы, а теперь стал инструментом контроля. Вы теперь не потребитель, вы – продукт потребления»[82]. Таким образом, персональные данные превратились в виртуальную валюту, большое количество сервисов в Интернете потому и бесплатны, что собранные данные о пользователях можно продать значительно дороже, чем стоит сам сервис. Когда человек окружен устройствами и сервисами, собирающими, в том числе тайно, информацию о нем, нет никакой проблемы в том, чтобы узнать о его интересах и пристрастиях.

Понятие «персональные данные» нуждается в совершенствовании – теперь это понятие должно включать не только имя и реквизиты документов, но и профиль в Интернет, т.е. учетные записи пользователей онлайн-сервисов.

[82] Помощник президента высказался за пересмотр российского законодательства о защите персональных данных // http://d-russia.ru/pomoshhnik-prezidenta-vyskazalsya-za-peresmotr-rossijskogo-zakonodatelstva-o-zashhite-personalnyx-dannyx.html.

В России практика применения Федерального закона от 27 июля 2006 года «О персональных данных» № 152-ФЗ[83] показывает, что к персональным данным относят, как правило, идентификаторы субъекта персональных данных (ФИО, дата рождения и др.). Однако владельцами онлайн-сервисов накапливаются иные данные, характеризующие поведение человека, его предпочтения, перемещение со временем в пространстве, мировоззрение, связи. Такая «глубокая» идентификация личности приводит к тому, что человек и его личная жизнь становятся беззащитны, поскольку указанные сведения не подпадают под действующую практику, к их обработке и хранению особые требования не предъявляются. Необходимы меры, чтобы обеспечить защиту персональных данных граждан, регулируя их обработку в национальном сегменте сети Интернет и определяя их доступность из глобальной сети.

Это дело государства, поскольку рынок обработки данных не способен обеспечить саморегулирование. Технологический прогресс не отменяет фундаментальных прав и свобод граждан, а также обязанности государства обеспечить их безопасности без ущерба для их частной жизни.

Следует также урегулировать вопрос выдачи согласия на обработку личных данных – оно должно даваться в явном виде, а не подразумеваться.

При этом изменения в соглашениях по обработке персональных данных не должны навязываться пользователям, ранее давшим согласие на обработку персональных данных по иным правилам.

Изначально для каждого интернет-сервиса требовалось отдельное соглашение на использование персональных данных в определенных целях. Но со временем компании начали обновлять эти соглашения. Сейчас, имея один аккаунт в социальной сети, автоматически отдаются данные всей системе сервисов – и на публикацию фотографий, и на чтение поисковой системой почты, и на хранение всех поисковых запросов. Бывает, такое делается даже

[83] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

вопреки тому, что пользователь разрешает, а что запрещает владельцам онлайн-сервисов.

А также гражданин должен иметь возможность удаления в сети Интернет информацию о себе, обладать правом быть забытым.

Другая проблема реализации законодательства о защите персональных данных вытекает из условия правомерности обработки оператором персональных данных сформулированного в ч. 1 ст. 6 ФЗ «О персональных данных»[84]: обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

Реализация на практике предписания закона о получении согласия лиц на обработку их персональных данных ведет к возникновению у операторов необходимости фиксировать факт получения такого согласия, поскольку в силу ч. 3 ст. 9 ФЗ «О персональных данных»[85] обязанность предоставить доказательство получения согласия субъекта персональных данных на их обработку возлагается именно на оператора.

Некоторые исследователи обращают внимание, что операторам необходимо документально фиксировать полученное согласие субъекта и хранить этот документ на случай, если субъект вдруг решит обратиться в суд в связи с нарушением его прав[86]. Действительно, с точки зрения дальнейшей защиты своих интересов в суде для операторов наилучшей формой получения согласия субъекта персональных данных на обработку этих данных будет именно письменная форма. Однако представляется, что такая ситуация будет вести, с одной стороны, к неоправданному увеличению массива документации в организациях – операторах персональных данных, и с другой стороны – к неоправданному увеличению объема собираемых персональных данных о лице.

---

[84] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[85] Там же.
[86] Закон о ПД: некоторые проблемы реализации // http://www.psj.ru/saver_magazins/detail.php?ID=62202.

Дело в том, что Закон о персональных данных[87] предъявляет к форме письменного согласия строгие требования. Согласно ч. 4 ст. 9 Закона[88] письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

---

[87] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[88] Там же.

- подпись субъекта персональных данных.

Получается, что в конкретных случаях при оформлении письменного согласия субъекта на обработку персональных данных оператор может получить еще больше сведений о лице, чем ему требуется для целей обработки (например, при сборе персональных данных для создания телефонных справочников оператор получит еще и паспортные данные лица, занесенные в форму письменного согласия).

Существующее положение, безусловно, является основанием для уточнения содержащихся в Законе о персональных данных[89] норм, касающихся формы письменного согласия на обработку персональных данных.

Согласно части 1 ст. 9 ФЗ «О персональных данных»[90] 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. Например, с учетом развития современных технологий и сети Интернет такое согласие может быть выражено следующим образом: путем постановки «галочки» напротив строки о своем согласии на обработку персональных данных при размещении своих персональных данных в сети Интернет (например, при покупке товаров через Интернет-магазины), путем простого прохождения по определенным ссылкам и др.

Учитывая это, представляется необходимым уточнить в законе само понятие «согласие на обработку персональных данных», с тем, чтобы у операторов появилось больше возможностей для получения согласия на обработку данных различными способами, и уменьшилась необходимость собирания избыточного объема данных путем получения письменных согласий по установленной форме.

---

[89] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[90] Там же.

Другое требование законодательства о персональных данных, реализация которого вызывает большие трудности, – это требование о принятии оператором необходимых мер для защиты персональных данных от неправомерного доступа к ним и от иных неправомерных действий с этими данными (ч. 1 ст. 19 ФЗ «О персональных данных»[91]).

Согласно ч. 1 ст. 19 ФЗ «О персональных данных»[92] оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Между тем есть основания полагать, что некоторые требования к операторам по защите информационных систем персональных данных являются избыточными.

В частности, это касается требования о необходимости получения потенциальными операторами лицензии на техническую защиту конфиденциальной информации во всех случаях обработки персональных данных.

Как отмечается в литературе, содержащиеся в законодательстве о лицензировании формулировки нуждаются в уточнении. На данный момент под «технической защитой конфиденциальной информации» согласно Положению о лицензировании деятельности по технической защите конфиденциальной информации от 3 февраля 2012 г. № 79[93] понимается выполнение работ и (или) оказание услуг по ее защите от

---

[91] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[92] Там же.

[93] О лицензировании деятельности по технической защите конфиденциальной информации: Постановление Правительства Росс. Федерации от 3 февраля 2012 г. Номер 79 // СПС Консультант Плюс.

несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Регулирующие органы, руководствуясь таким определением лицензируемого вида деятельности, выдвигают требование получения потенциальными операторами лицензии на техническую защиту конфиденциальной информации даже в тех случаях, когда обработка персональных данных осуществляется для собственных нужд (например, в рамках трудовых отношений), что не вытекает из положений Закона о персональных данных[94] и не соответствует духу Федерального закона «О лицензировании отдельных видов деятельности»[95]. Если учесть, что обязанность защиты персональных данных возлагается, за малым исключением, на всех юридических лиц, то при таком подходе получение лицензии превращается в чисто фискальную функцию.

Напрашивается вывод, что положения законодательства о лицензировании требуют внесения уточнений с целью устранения обязанности операторов для всех случаев обработки персональных данных получать лицензию. Стоит также определить целесообразность введения в отношении операторов таких мер, как использование ими только сертифицированных средств защиты информации и необходимости проведения аттестации информационных систем[96].

В качестве еще одного требования к операторам Закон о персональных данных[97] устанавливает обязанность оператора до начала обработки персональных данных уведомить уполномоченный государственный орган о

---

[94] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[95] О лицензировании отдельных видов деятельности: Федер. закон Росс. Федерации от 04.05.2011 г. Номер 99-ФЗ (ред. от 31.12.2014 г.) // СПС Консультант Плюс.

[96] Закон о ПД: некоторые проблемы реализации // http://www.psj.ru/saver_magazins/detail.php?ID=62202.

[97] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

своем намерении осуществлять обработку персональных данных (ч. 1 ст. 22 ФЗ «О персональных данных»[98]).

После получения уведомления уполномоченный орган вносит сведения об операторе в реестр операторов, осуществляющих обработку персональных данных. В соответствии с действующими нормативными правовыми актами уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ (Роскомнадзор), на что указано в п. 5.1.1.4 «Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций», утвержденного Постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228[99].

Между тем Закон о персональных данных[100] закрепляет некоторые исключения из общего правила о необходимости уведомлять уполномоченный орган. Согласно ч. 2 ст. 22 ФЗ «О персональных данных»[101] уведомлять уполномоченный орган не требуется, в частности, при обработке персональных данных:

- обрабатываемых в соответствии с трудовым законодательством;

- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

---

[98] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[99] О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: Постановление Правительства Росс. Федерации от 16.03.2009 г. № 228 (ред. от 22.05.2015 г.) // СПС Консультант Плюс.

[100] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[101] Там же.

- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством РФ, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим

- сделанных субъектом персональных данных общедоступными;

- включающих в себя только фамилии, имена и отчества субъектов персональных данных;

- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами РФ, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

- обрабатываемых в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Несмотря на наличие указанных исключений, в большинстве случаев операторы все же обязаны уведомлять «Роскомнадзор» о своих намерениях

вести обработку. Поскольку практически каждое юридическое лицо сталкивается с необходимостью обработки персональных данных физических лиц, есть вероятность, что реестр операторов будет включать большую часть существующих в стране организаций.

Представляется, что изложенный в законе перечень исключений из обязанности по уведомлению «Роскомнадзора» об обработке персональных данных нуждается в уточнении. В частности, этот перечень может быть дополнен посредством включения в него случаев, при которых не требуется согласие лица на обработку его персональных данных (ведь если в конкретном случае обработка может происходить без согласия самого субъекта персональных данных, то вряд ли есть необходимость уведомлять уполномоченный орган о намерении проводить такую обработку).

Таким образом, некоторые проблемы, возникающие при реализации на практике норм Федерального закона «О персональных данных»[102] и принятых на основании него подзаконных актов свидетельствуют о необходимости совершенствования нормативной правовой базы, регулирующей отношения в области защиты персональных данных.

3.2 Проблемы применения юридической ответственности за нарушение законодательства о персональных данных

Применение административной ответственности.

Проблема применения мер ответственности за нарушение законодательства о защите персональных данных является новой как для юридической науки, так и для правоприменительной практики. Правоприменительная практика пока невелика. В то же время сегодня эта проблема, как никогда, актуальна. Закон эффективен лишь в том случае, если в

[102] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

нем заложен оптимальный механизм его реализации. Одним из самых главных элементов механизма реализации закона является институт юридической ответственности.

В Законе о персональных данных[103] часть 1 ст. 24 об ответственности сформулирована лаконично: «Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность». Поскольку указанная норма является отсылочной, то установление конкретных видов правонарушений и применение соответствующих мер ответственности должно регулироваться иными нормативными актами.

В настоящее время меры ответственности за нарушение законодательства о защите персональных данных «разбросаны» по различным отраслям законодательства – административному, уголовному, гражданскому, трудовому. Причем ни в одной отрасли они пока не систематизированы должным образом, не выделены в отдельную группу как правонарушения, посягающие на конкретный вид общественных отношений.

Меры административной ответственности за нарушения законодательства в сфере персональных данных содержатся в КоАП РФ[104].

В соответствии со ст. 2.1 КоАП[105] административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое Кодексом или законами субъектов РФ об административных правонарушениях установлена административная ответственность.

Сразу отметим, что поскольку в соответствии с п. «к» ст. 72 Конституции РФ[106] административно-правовые отношения относятся к сфере совместного ведения, то субъекты РФ вправе издавать законы, содержащие дополнительные

---

[103] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[104] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[105] Там же.

к федеральным составы административных правонарушений, т.е. субъекты РФ вправе устанавливать специальные меры ответственности за нарушения законодательства о персональных данных.

Как следует из понятия административного правонарушения, субъектами административной ответственности могут быть как физические, так и юридические лица.

Общественные отношения, связанные с защитой персональных данных, относятся преимущественно к сфере государственного управления, что обусловливает потенциально большое число составов административных правонарушений в этой сфере в будущем. В настоящее время гл. 13 «Правонарушения в области связи и информации» КоАП РФ[107] содержит несколько составов административных правонарушений, объектом которых являются отношения, связанные с оборотом и защитой персональных данных граждан.

Один из таких составов – «нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)» (ст. 13.11 КоАП РФ[108]).

Ответственность наступает в виде предупреждения или наложения штрафа на граждан – в размере от 300 до 500 руб.; на должностных лиц – от 500 до 1000 руб.; на юридических лиц – от 5000 до 10 000 руб. Если размер штрафа для юридических лиц еще можно признать существенным, то для должностных лиц он просто смехотворный.

Объектом правонарушения являются общественные отношения в области защиты персональных данных граждан. Поскольку персональные данные – это обширный массив различной информации, то предметом данного правонарушения могут являться: нарушение личной и семейной тайны,

[106] Конституция Российской Федерации: принята всенар. голосованием 12 дек. 1993 г. (ред. от 21.07.2014 г.) // СПС Консультант Плюс.
[107] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[108] Там же.

нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, распространение сведений, порочащих честь, достоинство и деловую репутацию лица, а также нарушения установленного порядка ведения деятельности операторами информационных систем, в том числе работодателями, ведущими сбор персональных данных сотрудников в рамках трудовых отношений, нарушение правил журналистской деятельности в части сбора и обработки информации о гражданах и т.п.

Данной нормой обеспечивается один из важнейших принципов работы с персональными данными – принцип обеспечения их конфиденциальности (ст. 7 Закона о персональных данных[109]).

Субъектами данного правонарушения могут быть операторы информационных систем, должностные лица уполномоченных государственных и муниципальных органов, лица, получившие на законном основании доступ к персональным данным в связи с исполнением своих профессиональных обязанностей, а также все иные физические и юридические лица, нарушившие установленный порядок оборота персональных данных.

Рассмотрим пример. Физическое лицо обратилось в банк с заявлением о предоставлении кредита. Банку были представлены необходимые сведения о лице: паспортные данные, информация о прописке, сведения о доходах и имуществе и т.п. Банк в предоставлении кредита отказал, однако на адрес и телефон заемщика стали поступать предложения от других банков. В этом случае банком было нарушено требование обеспечения конфиденциальности персональных данных, а также принцип соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора[110].

---

[109] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[110] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 84.

Таким образом, налицо состав правонарушения, предусмотренного ст. 13.11 КоАП РФ[111].

Если, напротив, банк обращается в организацию с целью проверки сведений о лице, обратившемся за кредитом: работает ли данное лицо в этой организации, какой имеет размер зарплаты и т.п., а организация предоставляет информацию о работнике без его письменного согласия, то это деяние тоже подпадает под признаки административного правонарушения, предусмотренного ст. 13.11 КоАП РФ[112].

Квалифицирующим признаком в данном правонарушении выступает совершение его должностным лицом, т.е. лицом, получившим доступ к персональным данным в связи с исполнением должностных обязанностей. Обязанность обеспечивать конфиденциальность информации может вытекать как из должностных обязанностей, так и из профессиональных (например, для священника, нотариуса).

Еще одним административным правонарушением в сфере защиты персональных данных является «Отказ в предоставлении информации» (ст. 5.39 КоАП РФ[113]). Неправомерный отказ в предоставлении информации влечет наложение административного штрафа на должностных лиц в размере от одной тысячи до трех тысяч рублей» (ст. 5.39 КоАП РФ[114]).

В данной статье речь идет об информации, предоставляемой гражданину и (или) организации, предоставление которой предусмотрено федеральными законами. Такой информацией может быть и информация персонального характера. Поэтому данная норма обеспечивает выполнение ч. 4 ст. 14 Закона о персональных данных[115], закрепляющей право субъекта персональных данных

---

[111] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[112] Там же.
[113] Там же.
[114] Там же.
[115] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

на получение сведений, касающихся подтверждения факта обработки персональных данных, ее цели и способах и т.п.

Объектом правонарушений, предусмотренных в ст. 5.39 КоАП РФ[116], являются общественные отношения, складывающиеся по поводу получения и предоставления информации гражданами. Субъектами данных правонарушений являются должностные лица.

Если персональные данные используются в целях прямого маркетинга и запрос оператору относительно источника получения и способов обработки персональных данных остается без ответа, необходимо обращаться с заявлением в Роскомнадзор, которая должна провести проверку и привлечь нарушителя к административной ответственности по данной статье.

Еще один состав, «разглашение информации с ограниченным доступом» (ст. 13.14 КоАП РФ[117]), предусматривает ответственность за разглашение конфиденциальной информации лицом, которому эта информация стала известна в связи с исполнением служебных или профессиональных обязанностей. В числе такой информации могут быть и персональные данные. Объектом правонарушения являются общественные отношения в сфере защиты информации ограниченного доступа (за исключением сведений, составляющих государственную тайну). Субъектами правонарушения являются граждане и должностные лица. Ответственность наступает в виде штрафа для граждан – в размере от 500 до 1000 руб.; для должностных лиц – в размере от 4000 до 5000 руб.

На сегодняшний день только эти три состава правонарушения, содержащиеся в КоАП РФ[118], имеют своим непосредственным объектом персональные данные личности. В совокупности они обеспечивают выполнение самых основополагающих правил – соблюдение порядка сбора и

---

[116] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[117] Там же.
[118] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

обработки персональных данных, обеспечение их конфиденциальности и осуществление права субъекта персональных данных на доступ к своим персональным данным.

Кроме того, КоАП РФ[119] содержит ряд составов правонарушений, предмет которых тесно взаимосвязан с понятием «персональные данные». В числе таких составов можно назвать правонарушения в сфере банковской деятельности, информационной безопасности и т.д. Например, «незаконные действия по получению и (или) распространению информации, составляющей кредитную историю» (ст. 5.53 КоАП РФ[120]). Данные действия влекут ответственность в виде штрафа для граждан – в размере от 1000 до 2500 руб.; для должностных лиц – от 2500 до 5000 руб. или дисквалификацию на срок до трех лет; на юридических лиц – от 30 000 до 50 000 руб.

Данный состав правонарушения был введен в Кодекс в связи с принятием Федерального закона от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»[121].

Объектом правонарушения в данном случае выступает нарушение порядка получения и распространения конфиденциальной информации – кредитной истории.

Субъектами данного правонарушения являются юридические лица – бюро кредитных историй, а также виновные должностные лица, осуществляющие организационно-распорядительные или административно-хозяйственные функции в организациях, имеющих статус бюро кредитных историй.

Закон о персональных данных[122] не выделяет в общем массиве персональных данных информацию о финансовой сфере лица. Вместе с тем эту

---

[119] Там же.
[120] Там же.
[121] О кредитных историях: Федер. закон Росс. Федерации от 30 декабря 2004 г. Номер 218-ФЗ (ред. от 28.06.2014 г.) // СПС Консультант Плюс.
[122] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

информацию можно отнести к «чувствительной», так как несанкционированный доступ к ней и разглашение фактов, характеризующих финансовое положение лица, может причинить ему немалый материальный и моральный ущерб.

Установление административной ответственности за незаконные действия по получению и (или) распространению информации, составляющей кредитную историю, обеспечивает гарантии охраны конфиденциальности информации о финансовом положении лица и тем самым способствует поддержанию правопорядка сразу в двух сферах – кредитно-финансовой и относящейся к правам и свободам человека и гражданина.

Статья 13.12 КоАП РФ устанавливает ответственность за «нарушение правил защиты информации»[123].

В частности, п. 2 указанной статьи предусмотрена ответственность за использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации[124].

Статья 19 Закона о персональных данных[125] устанавливает обязанность операторов при обработке персональных данных принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения и т.д.

Ответственность за совершение данного правонарушения заключается в наложении штрафа на граждан – в размере от 1500 до 2000 руб. с возможной конфискацией несертифицированных средств защиты; на должностных лиц – от 2500 до 3000 руб.; на юридических лиц – от 20000 до 25000 руб. с

---

[123] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[124] Там же.
[125] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

возможной конфискацией несертифицированных средств защиты. Как мы видим, штрафы достаточно существенные.

В общем этих действующих в настоящее время норм достаточно, чтобы начала складываться соответствующая правоприменительная практика, хотя очевидно, что для эффективной реализации Закона о персональных данных[126] необходима дифференциация действующих и разработка новых составов административных правонарушений.

В частности, особый правовой режим, установленный законодателем в отношении специальных категорий персональных данных, нуждается в последовательном закреплении в виде особых мер административной ответственности за незаконный сбор, хранение, использование и разглашение информации, относящейся к специальным категориям персональных данных. Наличие дополнительных квалифицирующих признаков могло бы переводить эти деяния в категорию уголовно наказуемых деяний, т.е. преступлений.

С принятием Закона о персональных данных ст. 13.11 КоАП РФ «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»[127] кажется сформулированной слишком широко, и для эффективного правоприменения в отношении таких субъектов, как операторы информационных систем, возможно, нуждается в некоторой корректировке, а именно во включении в нее некоторых квалифицирующих признаков.

Например, в Законе Испании устанавливается ответственность операторов за ведение деятельности по сбору и обработке персональных данных без соответствующего разрешения (уведомления); за осуществление данной деятельности без явно выраженного согласия субъекта персональных данных, если получение его необходимо; за нарушение правил о внесении

---

[126] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[127] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

уточнений и исправлений; за препятствование доступу субъекта персональных данных к своим персональным данным; за нарушение конфиденциальности и т.п.[128] Все эти обязанности возложены и на российских операторов. Возможно и на территории РФ установить соответствующие меры ответственности, провести дифференциацию размеров штрафов в зависимости от вида правонарушения, его субъекта, повторности и неоднократности деяния.

Особую важность представляет собой проблема выбора санкций. Разнообразный характер управленческих отношений определяет неодинаковый характер государственно-правовой реакции на их нарушение, поэтому все административные санкции делятся на три вида: административные взыскания (карательные санкции), правовосстановительные санкции и санкции реального исполнения.

Во всех рассмотренных нами составах административных правонарушений, затрагивающих права граждан в области защиты персональных данных, предусмотрены карательные санкции, а именно штрафы. В двух составах помимо штрафов установлены санкции в виде предупреждения и дисквалификации (они также носят карательный характер).

Штраф представляет собой неблагоприятное имущественное последствие для виновника нарушения, т.е. является наказанием. Помимо этого, штраф служит превентивной мерой по отношению к будущим правонарушениям.

В такой сфере, как защита прав и свобод граждан в области неприкосновенности их частной жизни и защиты персональных данных, такая мера как штраф представляется совершенно недостаточной. В случаях подобных правонарушений не менее важным, чем наказание виновного, является восстановление нарушенных прав потерпевшего. Поэтому применение в данном случае наряду с карательными санкциями (штрафами) санкций реального исполнения представляется наиболее желательным. Применительно

[128] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 89.

к защите персональных данных это означает, что виновное лицо должно восстановить установленный федеральным законодательством нарушенный порядок оборота персональных данных и обеспечить тем самым соблюдение прав субъекта персональных данных. Например, ст. 13.11 КоАП РФ[129], предусматривающая ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), в части санкции должна предусматривать восстановление нарушенных правил этой деятельности, например, обязанность виновного лица в трехдневный срок исключить незаконно полученные персональные данные потерпевшего из информационной системы и направить ему соответствующее письменное уведомление о восстановлении нарушенных прав.

Подобные санкции необходимы, в противном случае никакого серьезного эффекта, кроме пополнения соответствующего бюджета, не будет. Кроме того, для виновного лица, вынужденного не только заплатить штраф, но и затратить время и силы на восстановление нарушенного порядка, это будет дополнительным аргументом придерживаться буквы закона в будущем.

Таким образом, тех административных составов, что содержит сейчас КоАП[130], достаточно для создания первых прецедентов в области защиты персональных данных граждан, однако недостаточно для эффективной реализации Закона о персональных данных[131]. Принятие этого Закона, несомненно, требует дифференциации действующих и разработки новых составов, нацеленных на обеспечение интересов граждан в процессе оборота персональных данных. Кроме того, в настоящее время имеется настоятельная необходимость применения новых подходов к установлению санкций в указанной сфере. Цель нового подхода должна состоять в том, чтобы добиться

[129] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[130] Там же.
[131] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

не только карательного эффекта от применения санкций, но и реального исполнения невыполненной или ненадлежащим образом выполненной обязанности и восстановить нарушенные права потерпевшего.

Рассматривая вопрос об административной ответственности в сфере оборота и защиты персональных данных, нельзя обойти вниманием проблему разработки и внедрения эффективных административных процедур, обеспечивающих обжалование нарушенных прав частных лиц – физических и юридических, а также реализацию правонаделительных функций уполномоченных органов в сфере оборота и защиты персональных данных.

Частное лицо, вступая во взаимоотношения с органами публичной администрации (государственными, муниципальными органами и др.), оказывается один на один с мощнейшим аппаратом, имеющим в своем распоряжении властные, финансовые, кадровые ресурсы. Детально разработанные административные процедуры позволяют «уравновесить» правовые возможности частного лица и эффективно защищать его интересы в споре с органом публичной администрации.

Административная ответственность по российскому праву – это прежде всего ответственность, наступающая перед государством, а не перед потерпевшей стороной. Отсюда и злоупотребление карательными санкциями, и слабые правовые возможности защиты прав частных лиц. Проблема эта уже давно обсуждается специалистами, тем не менее законопроект об административных процедурах до сих пор не принят.

По общему правилу лицо, чьи права нарушены действиями или решениями органов государственной власти, органами местного самоуправления, предприятиями, учреждениями, их должностными лицами, имеет право обратиться в вышестоящий орган с обжалованием этих действий или решений, или обратиться с исковым заявлением в суд (Закон РФ «Об

обжаловании в суд действий и решений, нарушающих права и свободы граждан»[132]).

Именно этот орган наделен полномочиями рассматривать обращения и жалобы субъектов персональных данных и юридических лиц по вопросам законности обработки персональных данных, рассматривать уведомления об обработке персональных данных, вести реестр операторов и т.д. Данный орган имеет право проводить проверки, запрашивать документы, проверять соответствие деятельности оператора условиям лицензии (в части обработки и передачи персональных данных), обращаться с исковыми заявлениями в суд. Он также наделен правом законодательной инициативы. В случае нарушения прав субъекта персональных данных оператором лицо имеет право обратиться в Роскомнадзор или его территориальный орган с соответствующим обращением или жалобой либо с исковым заявлением в суд. К сожалению, четкой процедуры рассмотрения дела, порядка истребования материалов, заслушивания мнения сторон российское законодательство пока не содержит. Все это негативно сказывается на действенности и эффективности института обжалования как такового. Тем не менее именно процедура обжалования неправомерных действий считается в западных демократиях наиболее эффективной в части защиты прав и свобод частных лиц[133].

Применение уголовной ответственности.

В соответствии со ст. 24 Закона о персональных данных[134] к лицам, виновным в нарушении данного Закона, могут быть применены меры уголовной ответственности.

---

[132] Об обжаловании в суд действий и решений, нарушающих права и свободы граждан: Закон Росс. Федерации от 27 апреля 1993 г. Номер 4866-1 (ред. от 09.02.2009 г.) // СПС Консультант Плюс.

[133] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 93.

[134] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

На сегодняшний день такое понятие, как «персональные данные», в УК РФ[135] отсутствует. Соответственно нет в нем и специальных составов преступлений, предусматривающих ответственность за нарушения в сфере оборота и защиты персональных данных. Тем не менее в УК РФ[136] есть ряд статей, предусматривающих ответственность за преступления, объект посягательства которых тесно связан с персональными данными.

«Нарушение неприкосновенности частной жизни» (ст. 137 УК РФ[137]).

Данное преступление заключается в незаконном собирании или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Объектом данного преступления являются общественные отношения, обеспечивающие неприкосновенность частной жизни.

Понятия «частная жизнь» и «персональные данные» не тождественны. Однако очень часто персональные данные выступают как неотъемлемая часть сведений о частной жизни, являются личной или семейной тайной и т.д. Поэтому незаконный сбор или распространение информации о частной жизни лица могут самым непосредственным образом нарушать его права в сфере оборота и защиты персональных данных.

Характер действий правонарушителя (собирание, распространение) в совокупности с мотивацией (личная заинтересованность) в большинстве случаев предопределяют форму вины правонарушителя как прямой умысел. Субъектом преступления может быть любое лицо, достигшее возраста 16 лет, в

---

[135] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[136] Там же.
[137] Там же.

том числе и специальный субъект – лицо, наделенное соответствующими полномочиями (ч. 2 ст. 137 УК РФ[138]).

Действительно, должностные лица многих государственных органов наделены правом в рамках своей профессиональной деятельности собирать информацию о гражданах.

В настоящее время правом собирать информацию о частной жизни лица наделены, в частности, работники правоохранительных органов в рамках осуществления оперативно-розыскной деятельности.

Статья 10 Федерального закона «Об оперативно-розыскной деятельности» позволяет органам, осуществляющим оперативно-розыскную деятельность, «создавать и использовать информационные системы, а также заводить дела оперативного учета... в целях собирания и систематизации сведений, проверки и оценки результатов оперативно-розыскной деятельности, а также принятия на их основе соответствующих решений...»[139]. Характер и объем этих сведений не уточняется, однако понятно, что значительную часть их составляют персональные данные лиц, попавших в поле зрения правоохранительных органов.

Специфика оперативно-розыскной деятельности требует значительных изъятий из права на неприкосновенность частной жизни, что обусловлено прежде всего интересами общественной безопасности. Безусловно, с точки зрения защиты прав и свобод человека и гражданина данная деятельность никогда не была и не будет безупречной, поскольку эффективное ее проведение без этих ограничений вообще невозможно. С другой стороны, именно на защиту прав и свобод человека и гражданина эта деятельность и направлена.

Придерживаясь принципа приоритета прав и свобод личности в любых сферах государственной жизни, мы все-таки полагаем, что излишняя формализация оперативно-розыскной и иной правоохранительной

[138] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[139] Там же.

деятельности, даже в плане защиты персональных данных личности, может отрицательно сказаться на эффективности этой деятельности. Высокий уровень преступности в современной России не позволяет пока, к сожалению, обеспечить необходимый баланс интересов в этой области, и приходится «из двух зол выбирать меньшее». Поэтому в настоящий момент более важным является обеспечение соблюдения уже действующих норм, направленных на защиту неприкосновенности частной жизни в условиях проведения оперативно-розыскных мероприятий, чем переработка этих норм с целью усиления охраны персональных данных в указанной сфере.

В соответствии с Законом РФ от 11 марта 1992 г. № 2487-1 «О частной детективной и охранной деятельности»[140] сбор информации о гражданах может осуществляться физическими и юридическими лицами, работающими в данной сфере. Данный Закон[141] содержит множество обтекаемых формулировок и различных оговорок («сбор информации для деловых переговоров», «изучение рынка», «выяснение биографических подробностей субъекта с его письменного согласия» и т.п.), которые представляет собой серьезный «фактор риска» с точки зрения охраны конфиденциальности персональных данных. В то же время Законом[142] предусматривается обязанность частных детективов обеспечивать защиту информации, относящейся к личной жизни граждан. Грубым нарушением правил осуществления детективной деятельности являются действия, направленные против неприкосновенности частной жизни лица.

Частным детективам запрещается собирать сведения о личной жизни, религиозных и политических убеждениях отдельных граждан (п. ст. 7 Закона «О частной детективной и охранной деятельности»[143]). Видимо, имеются в виду

---

[140] О частной детективной и охранной деятельности: Закон Росс. Федерации от 11 марта 1992 г. Номер 2487-1 (ред. от 31.12.2014 г.) // СПС Консультант Плюс.
[141] Там же.
[142] Там же.
[143] О частной детективной и охранной деятельности: Закон Росс. Федерации от 11 марта 1992 г. Номер 2487-1 (ред. от 31.12.2014 г.) // СПС Консультант Плюс.

политики и иные публичные персоны. Конечно же, такая формулировка недопустима. Либо нужно распространить запрет на всех субъектов, либо перечислить конкретно тех, на кого он распространяется. Установлено, что проведение сыскных мероприятий, нарушающих гарантии неприкосновенности частной жизни, влекут применение мер ответственности, в частности по ст. 137 УК РФ[144].

«Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» (ст. 138 УК РФ[145]).

Объектом этих преступлений являются общественные отношения, связанные с охраной тайны переписки, телефонных и иных переговоров и сообщений. Преступление совершается в форме ознакомления лица с корреспонденцией и сообщениями, содержащими конфиденциальную информацию (персональные данные), без согласия субъекта персональных данных, а также без законных оснований (например, соответствующего решения суда). Субъектом данного преступления может быть любое лицо, достигшее возраста 16 лет, в том числе и специальный субъект – должностное лицо.

Статьей 138 УК РФ[146] обеспечивается конституционное право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23 Конституции РФ[147]). Заметим, что проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права граждан в данной сфере, допускается на основании судебного решения в случае наличия информации: о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно; о лицах, подготавливающих,

---

[144] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[145] Там же.
[146] Там же.
[147] Конституция Российской Федерации: принята всенар. голосованием 12 дек. 1993 г. (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

совершающих противоправное деяние, по которому производство предварительного следствия обязательно; о событиях или действиях, создающих угрозу государственной, экономической или экологической безопасности РФ[148].

В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого преступления, а также при наличии информации о событиях и действиях, создающих угрозу государственной, военной или экологической безопасности РФ, на основании мотивированного постановления одного из руководителей органов, осуществляющих оперативно-розыскную деятельность, допускается проведение оперативно-розыскных мероприятий, предусмотренных ч. 2 ст. 138 УК РФ[149], с обязательным уведомлением суда (судьи) в течение 24 часов. В течение 48 часов с момента начала проведения оперативно-розыскного мероприятия орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение.

Таким образом, как мы видим, данная деятельность довольно жестко регламентирована и поставлена под судебный контроль, что позволяет обеспечить баланс между правом гражданина на тайну коммуникаций и реализацией обязанности государства обеспечить раскрытие и пресечение преступлений.

«Отказ в предоставлении гражданину информации» (ст. 140 УК РФ[150]).

Данное преступление представляет собой неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной

---

[148] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 98.

[149] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[150] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

информации при условии, если эти деяния причинили вред правам и законным интересам граждан.

Под уголовную ответственность, предусмотренную ст. 140 УК РФ[151], подпадает и неисполнение обязанности оператором – физическим лицом или должностным лицом оператора – юридического лица по предоставлению информации субъекту персональных данных, предусмотренной ст. 18 Закона о персональных данных[152], при условии, что правам и свободам субъекта персональных данных был причинен вред.

Субъектом данного преступления может быть должностное лицо. Проблема доступа граждан к информации о деятельности государственных органов, включающая и право на доступ к своим персональным данным, содержащимся в картотеках государственных органов, лишь совсем недавно стала предметом изучения и обсуждения. Между тем во многих зарубежных странах уже давно действуют законы, регулирующие порядок доступа и получения публичной информации гражданами. Например, Закон Венгрии «О персональных данных и об опубликовании данных, представляющих общественный интерес» содержит специальную главу, устанавливающую порядок ознакомления граждан с информацией, представляющей общественный интерес. В этом Законе, в частности, предусмотрено, что «органы и лица, выполняющие функции центральных или местных органов власти…обязаны публиковать или иным образом обеспечивать общественный доступ к важнейшим данным о своей деятельности, в частности… к типам находящихся в их распоряжении данных»[153].

---

[151] Там же.

[152] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[153] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 100.

«Разглашение тайны усыновления (удочерения)» (ст. 155 УК РФ[154]). Данное преступление заключается в разглашении сведений об усыновлении (удочерении) вопреки воле усыновителя лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну.

Объектом данного преступления являются общественные отношения, обеспечивающие охрану семьи, личную и семейную тайну. Субъектом данного преступления является должностное лицо.

В настоящее время охрана персональных данных, связанных с тайной усыновления, осуществляется с помощью ст. 155 УК РФ[155].

Согласно ст. 139 СК РФ тайна усыновления ребенка охраняется законом[156]. Нормы СК РФ[157] устанавливают объем сведений, подлежащих защите, круг обязанных субъектов и основание наступления ответственности, которым является распространение сведений против воли усыновителей (несанкционированное распространение). Тайна усыновления (удочерения) относится к числу профессиональных тайн.

«Неправомерный доступ к компьютерной информации» (ст. 272 УК РФ[158]).

Данный состав преступления заключается в неправомерном доступе к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации. Объектом данного правонарушения выступают общественные отношения в сфере охраны доступа к компьютерной информации. Преступное деяние заключается в

---

[154] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[155] Там же.
[156] Семейный кодекс Российской Федерации (СК РФ) от 29.12.1995 г. Номер 223-ФЗ (ред. от 20.04.2015 г.) // СПС Консультант Плюс.
[157] Там же.
[158] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

неправомерном доступе к компьютерной информации, в результате которого эта информация становится известной виновному лицу и может быть использована им. Субъектом данного преступления может быть любое лицо, достигшее возраста 16 лет.

Компьютерной информацией, ставшей предметом преступного посягательства, могут оказаться и персональные данные лица или группы лиц, и в этом случае данный вид преступления будет представлять особую общественную опасность.

Поскольку деятельность операторов информационных систем персональных данных в большинстве случаев автоматизирована и функционирует на основе компьютерного оборудования и программ, то в будущем возможно широкое распространение преступных посягательств именно на этот объект – на компьютеризированную информацию о гражданах. В связи с этим было бы целесообразно разработать и включить в УК РФ[159] специальный состав, предусматривающий уголовную ответственность за неправомерный доступ к информационным системам персональных данных.

Состав преступления, предусмотренного ст. 272 УК РФ[160], материальный, т.е. преступление считается совершенным с момента наступления следующих последствий: уничтожение компьютерной информации блокирование информации; модификация информации; копирование информации.

Думается, что состав преступления, предусматривающий уголовную ответственность за неправомерный доступ к информационным системам персональных данных, должен быть формальным, т.е. преступление должно считаться законченным, а виновный привлекаться к ответственности независимо от наступления общественно опасных последствий. Причиной этого служит высокая степень общественной опасности деяния, а также тот факт, что совершение данного преступления возможно только с прямым

[159] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[160] Там же.

умыслом, так как случайное или неосторожное проникновение в защищенные информационные системы невозможно.

Несмотря на то что Законом о персональных данных[161] прямо предусмотрена возможность применения к виновному лицу мер уголовной ответственности, ни одного состава преступления, имеющего своим непосредственным предметом защиты персональные данные, в УК РФ[162] на сегодняшний день не существует. Это создает чисто практические трудности для правильной квалификации деяний судьями, а также лицами и органами, уполномоченными рассматривать дела об административных правонарушениях. До тех пор, пока в УК РФ[163] не появятся составы, прямо предусматривающие ответственность за нарушение законодательства о персональных данных, применение уголовной ответственности в этой сфере будет ограниченно.

Уголовно-правовая охрана необходима, но не должна становиться доминирующей. Ведь уголовные меры ответственности направлены прежде всего на наказание преступника. Однако, как уже отмечалось, в деле обеспечения защиты персональных данных важно не только наказать правонарушителя, но и восстановить нарушенное право потерпевшего.

Применение мер уголовной ответственности как наиболее сурового вида наказания, оправданно в отношении незаконного сбора и распространения информации, относящейся к специальным категориям персональных данных, т.е. сведений, касающихся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, состояния здоровья и интимной жизни, если такие действия повлекли причинение морального или материального вреда. Установление уголовно-правовой охраны данной категории информации вполне уместно в современной России, где традиции

---

[161] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[162] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[163] Там же.

уважения к частной жизни лица пока еще недостаточно укоренились. Кроме того, нужно учитывать и значительный моральный и материальный ущерб, который наносится лицу при распространении такого рода сведений.

Применение гражданско-правовой ответственности.

Статьей 24 Закона о персональных данных[164] предусмотрено, что к лицам, нарушившим требования данного Закона[165], применяются в том числе меры гражданско-правовой ответственности.

Основным признаком гражданско-правовой ответственности является ее имущественный характер, который выражается в возмещении виновным причиненных убытков. Даже в случаях, когда правонарушение затрагивает личные неимущественные права и (или) причиняет потерпевшему лицу – субъекту нарушенного гражданского права – моральный вред, применение мер гражданско-правовой ответственности будет означать присуждение потерпевшему лицу соответствующей денежной компенсации.

Вторым признаком гражданско-правовой ответственности является равноправие субъектов, т.е. ответственность по гражданскому праву представляет собой ответственность одного участника гражданско-правовых отношений перед другим, ответственность правонарушителя перед потерпевшим. Это предопределяет активную роль субъекта персональных данных. Он сам наделен правом защищать свои права и привлекать к ответственности виновного путем предъявления требований о возмещении ущерба и (или) подачи искового заявления в суд.

Третьим признаком гражданско-правовой ответственности является соответствие размера ответственности размеру причиненного ущерба или убытков[166].

---

[164] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[165] Там же.

[166] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 105.

Согласно ст. 150 ГК РФ[167] нематериальные блага, к числу которых Гражданский кодекс[168] относит жизнь и здоровье, достоинство личности, личную неприкосновенность, честь и доброе имя, деловую репутацию, неприкосновенность частной жизни, неприкосновенность жилища, личную и семейную тайну, свободу передвижения, свободу выбора места пребывания и жительства, имя гражданина, авторство, иные нематериальные блага, принадлежащие гражданину от рождения или в силу закона, неотчуждаемы и непередаваемы иным способом, защищаются в соответствии с ГК РФ[169] и другими законами в случаях и порядке, ими предусмотренными, а также в тех случаях и пределах, в каких использование способов защиты гражданских прав вытекает из существа нарушенного нематериального права и характера последствий этого нарушения.

Поскольку в ст. 150 ГК РФ[170] персональные данные личности как объект гражданско-правовой защиты не поименованы, следует рассмотреть вопрос о том, как соотносятся персональные данные личности и перечисленные в ст. 150 ГК РФ[171] неимущественные права и нематериальные блага.

Надо сказать, что нематериальные блага и неимущественные права (жизнь, здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна) охватывают широкий круг самых разнообразных проявлений человеческой жизни. Иногда персональные данные как информация (сведения, данные) об определенном или определяемом лице сами непосредственно являются нематериальным благом и неимущественным правом, подлежащим защите (например, личная или семейная тайна), а иногда они выступают опосредованным инструментом защиты этих благ и прав, например правовой

---

[167] Гражданский кодекс Российской Федерации (ГК РФ) Часть 1 от 30.11.1994 г. Номер 51-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[168] Там же.
[169] Там же.
[170] Там же.
[171] Там же.

режим конфиденциальности персональных данных обеспечивает соблюдение чести, достоинства, доброго имени индивида, а в более широком плане – неприкосновенности частной жизни.

Поскольку Закон о персональных данных[172] предусматривает гражданско-правовую защиту отношений, связанных с оборотом персональных данных, логично хотя бы в теоретическом плане считать их самостоятельным объектом гражданско-правовой защиты, так как они являются элементом права на неприкосновенность частной жизни, личную и семейную тайну и т.д.

Для возникновения обязательства по возмещению вреда (гражданско-правовой ответственности) одного факта причинения вреда недостаточно. Статья 1064 ГК РФ[173] содержит общие условия (основания), которые в совокупности с фактом причинения вреда порождают соответствующее обязательство. Условия эти следующие: противоправность деяния, причинная связь между деянием и наступившим результатом (причинение вреда) и вина причинителя.

Таким образом, если в случае виновного противоправного деяния причинен имущественный или моральный вред субъекту персональных данных, он имеет право на гражданско-правовую защиту своих прав.

Основными способами защиты неимущественных прав и благ нематериального свойства являются возмещение ущерба, компенсация морального вреда и возложение обязанности опровержения сведений, порочащих честь, достоинство и деловую репутацию граждан. Рассмотрим их поочередно.

Гражданское законодательство устанавливает принцип возмещения ущерба в полном объеме (ст. 1082 ГК РФ[174], т.е. вред может быть возмещен в

---

[172] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[173] Гражданский кодекс Российской Федерации (ГК РФ) Часть 2 от 26.01.1996 г. Номер 14-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

[174] Гражданский кодекс Российской Федерации (ГК РФ) Часть 2 от 26.01.1996 г. Номер 14-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

натуре путем предоставления вещи того же рода и качества, исправления поврежденной вещи и т.п. либо путем возмещения убытков. В соответствии с п. 2 ст. 15 ГК РФ[175] под убытками понимаются реальный ущерб (стоимость утраченного имущества, иные расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права), а также упущенная выгода (неполученные доходы, которые потерпевший получил бы при обычных условиях гражданского оборота, если бы его право не было нарушено).

Неправомерными действиями, связанными с нарушением порядка оборота и защиты персональных данных, гражданину может быть причинен не столько имущественный, сколько моральный вред. По всей видимости, в сфере оборота и защиты персональных данных именно компенсация морального вреда станет основной формой гражданско-правовой защиты указанных общественных отношений.

Как оценить вред, причиненный индивиду незаконным сбором и использованием его персональных данных, нарушением его права на доступ к персональным данным или несанкционированным разглашением конфиденциальных сведений о частной жизни? В данном случае критерием оценки будут служить моральные (нравственные) переживания лица, вызванные незаконным вмешательством в его частную жизнь, невозможностью контролировать им распространение и использование личной информации, а также психологическая травма, нанесенная лицу разглашением данных о нем личного или интимного свойства. В переводе на язык юридических терминов нравственные переживания лица вследствие нарушения тех или иных его прав и составляют моральный вред[176].

Пленум Верховного Суда РФ в постановлении от 20 декабря 1994 г. № 10 «Некоторые вопросы применения законодательства о компенсации морального

---

[175] Гражданский кодекс Российской Федерации (ГК РФ) Часть 1 от 30.11.1994 г. Номер 51-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[176] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 107.

вреда»[177] дает следующее разъяснение понятия «моральный вред»: это нравственные или физические страдания, причиненные действиями (бездействием), посягающими на принадлежащие гражданину от рождения или в силу закона нематериальные блага, такие как жизнь, здоровье, достоинство личности, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна и т.п., или нарушающими его личные неимущественные права: право на пользование своим именем, право авторства и т.д. Моральный вред, как разъясняет далее Пленум, может «заключаться в нравственных переживаниях в связи с… раскрытием семейной, врачебной тайны...»[178]. Более лаконичное определение понятия «моральный вред» содержится в ст. 151 ГК РФ[179]. В соответствии с ней моральный вред – это «нравственные или физические страдания».

Понятие «моральный вред» появилось в российском гражданском праве относительно недавно, в связи с чем среди ученых-процессуалистов нет единого мнения относительно его определения и правомерности использования самого термина «моральный вред». Некоторые ученые, например, предлагают заменить понятие «моральный вред» на более емкое и удачное понятие «психологический вред», используемое в США и Великобритании. Представляется, что различные интерпретации данного понятия в какой-то мере способствуют успешному раскрытию его содержания, однако и в настоящее время понятие «моральный вред» применяется вполне успешно, а приведенное выше разъяснение Пленума Верховного Суда РФ[180] позволяет достаточно ясно понять его содержание и очертить границы использования.

---

[177] Некоторые вопросы применения законодательства о компенсации морального вреда: Постановление Пленума Верховного Суда РФ от 20.12.1994 г. Номер 10 (ред. от 06.02.2007 г.) // СПС Консультант Плюс.

[178] Гражданский кодекс Российской Федерации (ГК РФ) Часть 1 от 30.11.1994 г. Номер 51-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[179] Там же.

[180] Некоторые вопросы применения законодательства о компенсации морального вреда: Постановление Пленума Верховного Суда РФ от 20.12.1994 г. Номер 10 (ред. от 06.02.2007 г.) // СПС Консультант Плюс.

Согласно ст. 151 ГК РФ[181], если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные имущественные права либо посягающими на принадлежащие гражданину нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации морального вреда. Таким образом, если незаконными действиями, связанными с нарушениями порядка оборота и защиты персональных данных, субъекту персональных данных причинены нравственные страдания, он имеет право на компенсацию морального вреда в денежной форме. Более того, согласно ст. 1100 ГК РФ[182] моральный вред, причиненный нарушением чести, достоинства и деловой репутации гражданина, возмещается независимо от наличия вины причинителя.

Подчеркнем, что законом выделяется лишь один вид компенсации – денежный. Определение размеров компенсации полностью зависит от решения суда, так как на уровень причиненного вреда влияет множество факторов, которые должны рассматриваться в совокупности: тяжесть деяния, степени вины нарушителя, восприимчивость психики потерпевшего, негативные последствия во внешней среде, последствия материального свойства (смена места жительства, места работы) и иные заслуживающие внимания обстоятельства. Среди таких заслуживающих внимания обстоятельств важное место занимает вопрос об имущественном положении причинителя.

Надо сказать, что проблема исполнения судебного решения в части взыскания денежных сумм в пользу потерпевшего продолжает быть актуальной. Как отмечается специалистами, механизм, предлагаемый законодателем, функционирует не слишком эффективно. Нередко на практике встречаются случаи, когда решение суда о взыскании с виновного

---

[181] Гражданский кодекс Российской Федерации (ГК РФ) Часть 1 от 30.11.1994 г. Номер 51-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[182] Гражданский кодекс Российской Федерации (ГК РФ) Часть 2 от 26.01.1996 г. Номер 14-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

определенной денежной суммы в счет компенсации морального вреда не может быть исполнено по причине отсутствия у виновного имущества и денежных средств. Складывается общая ситуация, когда из-за финансовой несостоятельности причинителя потерпевший лишается какой бы то ни было возможности компенсировать свои моральные потери. Отсутствие экономических условий делает норму закона о компенсации морального вреда во многом декларативной. Данная ситуация могла бы быть частично исправлена, если бы гражданским законодательством была предусмотрена возможность не только денежной, но и иных форм компенсации морального вреда потерпевшему. Другими словами, виновное лицо должно иметь возможность компенсировать моральный вред не только в денежном выражении, а по договоренности с потерпевшим – в ином соразмерном виде[183].

Согласно Гражданскому кодексу РФ[184] возможность компенсации морального вреда существует только в денежной форме. Вместе с тем извинение как форма компенсации морального вреда вполне могла бы стать достойной альтернативой материальному возмещению, тем более что оно в значительно большей степени способствует психологической реабилитации потерпевшего. Не будем забывать, что моральный вред потому и моральный (т.е. душевный, психологический), поскольку влияет негативно именно на душевное состояние потерпевшего. Это тем более важно, когда нарушаются права личности в области конфиденциальности личной информации.

В ст. 152 ГК РФ[185] представлен ряд способов защиты чести, достоинства и деловой репутации гражданина. Все они имеют нематериальный характер и поэтому могут быть реализованы наряду с возмещением убытков и компенсацией морального вреда. Согласно нормам этой статьи «гражданин

---

[183] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина, 2011. С. 109.

[184] Гражданский кодекс Российской Федерации (ГК РФ) Часть 2 от 26.01.1996 г. Номер 14-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

[185] Гражданский кодекс Российской Федерации (ГК РФ) Часть 1 от 30.11.1994 г. Номер 51-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

вправе потребовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности»[186], а при распространении таких сведений в средствах массовой информации – опровержение в тех же СМИ (ст. 43 Закона о СМИ[187]).

А как быть, если сведения соответствуют действительности? Значит ли это, что достоверная, но компрометирующая информация может свободно и безнаказанно распространяться любым лицом?

Разумеется, нет. Ограничения вводит Закон о персональных данных[188]. Лицо, распространившее сведения, порочащие честь и достоинство гражданина, во-первых, должно будет доказать, что эти сведения получены законным путем, т.е. что способ получения сведений не образует состава правонарушения – административного, дисциплинарного или уголовного. И во-вторых, что лицо имеет право на распространение этих сведений, т.е. не нарушает служебную, профессиональную тайну и т.п., что в отношении порочащих и компрометирующих сведений в ряде случаев представляется маловероятным. В противном случае согласно нормам Закона о персональных данных[189] виновное лицо подлежит юридической ответственности.

В судебной практике иски о компенсации морального вреда и опровержении порочащих сведений имеют достаточно широкое распространение, особенно часто они исходят от представителей политического истеблишмента. Однако следует иметь в виду, что гражданско-правовые санкции далеко не во всех случаях являются адекватными уровню наступивших для гражданина вредных последствий. Поэтому не менее

---

[186] Там же.

[187] О средствах массовой информации: Закон Росс. Федерации от 27 декабря 1991 г. Номер 2124-1 (ред. от 24.11.2014 г.) // СПС Консультант Плюс.

[188] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[189] Там же.

важными элементами системы обеспечения защиты персональных данных являются административно-правовые и уголовно-правовые санкции.

Заключение

Целью дипломной работы являлось расширение и углубление научных знаний о вопросе правового регулирования отношений в области защиты персональных данных.

Для достижения поставленной цели были решены следующие задачи: рассмотрены персональные данные как объект правовой охраны и нормативно-правовые акты в области защиты персональных данных; изучены права субъекта и обязанности оператора при обработке персональных данных; рассмотрены меры по обеспечению выполнения оператором своих обязанностей и меры по обеспечению безопасности персональных данных при их обработке; проанализированы проблемы правового регулирования и правовой защиты персональных данных.

Понятие «персональные данные» нуждается в совершенствовании – теперь это понятие должно включать не только имя и реквизиты документов, но и профиль в Интернет, т.е. учетные записи пользователей онлайн-сервисов.

Следует также урегулировать вопрос выдачи согласия на обработку личных данных – оно должно даваться в явном виде, а не подразумеваться.

А также гражданин должен иметь возможность удаления в сети Интернет информацию о себе, обладать правом быть забытым.

Необходимо уточнить в Законе о персональных данных[190] нормы, касающиеся формы письменного согласия на обработку персональных данных, поскольку в конкретных случаях при оформлении письменного согласия субъекта на обработку персональных данных оператор может получить еще больше сведений о лице, чем ему требуется для целей обработки (например, при сборе персональных данных для создания телефонных справочников оператор получит еще и паспортные данные лица, занесенные в форму письменного согласия).

---

[190] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

Необходимо уточнить в законе понятие «согласие на обработку персональных данных», с тем, чтобы у операторов появилось больше возможностей для получения согласия на обработку данных различными способами, и уменьшилась необходимость собирания избыточного объема данных путем получения письменных согласий по установленной форме.

Положения законодательства о лицензировании требуют внесения уточнений с целью устранения обязанности операторов для всех случаев обработки персональных данных получать лицензию, например, исключением может быть обработка персональных данных осуществляемая для собственных нужд (в рамках трудовых отношений). Стоит также определить целесообразность введения в отношении операторов таких мер, как использование ими только сертифицированных средств защиты информации и необходимости проведения аттестации информационных систем.

Представляется, что изложенный в законе перечень исключений из обязанности по уведомлению «Роскомнадзора» об обработке персональных данных нуждается в уточнении. В частности, этот перечень может быть дополнен посредством включения в него случаев, при которых не требуется согласие лица на обработку его персональных данных (ведь если в конкретном случае обработка может происходить без согласия самого субъекта персональных данных, то вряд ли есть необходимость уведомлять уполномоченный орган о намерении проводить такую обработку).

Проблема применения мер ответственности за нарушение законодательства о защите персональных данных является новой как для юридической науки, так и для правоприменительной практики.

В настоящее время меры ответственности за нарушение законодательства о защите персональных данных «разбросаны» по различным отраслям законодательства – административному, уголовному, гражданскому, трудовому. Причем ни в одной отрасли они пока не систематизированы

должным образом, не выделены в отдельную группу как правонарушения, посягающие на конкретный вид общественных отношений.

Меры административной ответственности за нарушения законодательства в сфере персональных данных содержатся в КоАП РФ[191]. В общем этих действующих в настоящее время норм достаточно, чтобы начала складываться соответствующая правоприменительная практика, хотя очевидно, что для эффективной реализации Закона о персональных данных[192] необходима дифференциация действующих и разработка новых составов административных правонарушений.

В частности, особый правовой режим, установленный законодателем в отношении специальных категорий персональных данных, нуждается в последовательном закреплении в виде особых мер административной ответственности за незаконный сбор, хранение, использование и разглашение информации, относящейся к специальным категориям персональных данных. Наличие дополнительных квалифицирующих признаков могло бы переводить эти деяния в категорию уголовно наказуемых деяний, т.е. преступлений.

С принятием Закона о персональных данных ст. 13.11 КоАП РФ «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»[193] кажется сформулированной слишком широко, и для эффективного правоприменения в отношении таких субъектов, как операторы информационных систем, возможно, нуждается в некоторой корректировке, а именно во включении в нее некоторых квалифицирующих признаков, например, ответственность операторов за ведение деятельности по сбору и обработке персональных данных без соответствующего разрешения (уведомления); за осуществление данной деятельности без явно выраженного

[191] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[192] Там же.
[193] Там же.

согласия субъекта персональных данных, если получение его необходимо; за нарушение правил о внесении уточнений и исправлений; за препятствование доступу субъекта персональных данных к своим персональным данным; за нарушение конфиденциальности и т.п. Возможно установить соответствующие меры ответственности, провести дифференциацию размеров штрафов в зависимости от вида правонарушения, его субъекта, повторности и неоднократности деяния.

Особую важность представляет собой проблема выбора санкций. Во всех составах административных правонарушений, затрагивающих права граждан в области защиты персональных данных, предусмотрены карательные санкции, а именно штрафы, предупреждения и дисквалификации.

Вместе с тем нельзя не отметить тот факт, что в такой сфере, как защита прав и свобод граждан в области неприкосновенности их частной жизни и защиты персональных данных, такая мера представляется совершенно недостаточной. В случаях подобных правонарушений не менее важным, чем наказание виновного, является восстановление нарушенных прав потерпевшего. Поэтому применение в данном случае наряду с карательными санкциями (штрафами) санкций реального исполнения представляется наиболее желательным. Применительно к защите персональных данных это означает, что виновное лицо должно восстановить установленный федеральным законодательством нарушенный порядок оборота персональных данных и обеспечить тем самым соблюдение прав субъекта персональных данных. Например, ст. 13.11 КоАП РФ[194], предусматривающая ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), в части санкции должна предусматривать восстановление нарушенных правил этой деятельности, например, обязанность виновного лица в трехдневный срок

[194] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

исключить незаконно полученные персональные данные потерпевшего из информационной системы и направить ему соответствующее письменное уведомление о восстановлении нарушенных прав.

Для виновного лица, вынужденного не только заплатить штраф, но и затратить время и силы на восстановление нарушенного порядка, это будет дополнительным аргументом придерживаться буквы закона в будущем.

Также есть необходимость разработки и внедрения эффективных административных процедур, обеспечивающих обжалование нарушенных прав частных лиц – физических и юридических (в частности, процедура обжалования неправомерных действий и решений органов власти), которые позволят «уравновесить» правовые возможности частного лица и эффективно защищать его интересы в споре с органом публичной администрации.

В соответствии со ст. 24 Закона о персональных данных[195] к лицам, виновным в нарушении данного Закона, могут быть применены меры уголовной ответственности.

На сегодняшний день такое понятие, как «персональные данные», в УК РФ[196] отсутствует. Соответственно нет в нем и специальных составов преступлений, предусматривающих ответственность за нарушения в сфере оборота и защиты персональных данных. Тем не менее в УК РФ[197] есть ряд статей, предусматривающих ответственность за преступления, объект посягательства которых тесно связан с персональными данными. Думается, что со временем на основе этих составов будут разработаны специальные составы, имеющие своим непосредственным объектом защиты персональные данные личности.

---

[195] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

[196] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[197] Там же.

В соответствии с Законом РФ от 11 марта 1992 г. № 2487-1 «О частной детективной и охранной деятельности»[198] сбор информации о гражданах может осуществляться физическими и юридическими лицами, работающими в данной сфере. Частным детективам запрещается собирать сведения о личной жизни, религиозных и политических убеждениях отдельных граждан (п. ст. 7 Закона «О частной детективной и охранной деятельности»[199]). Видимо, имеются в виду политики и иные публичные персоны. Конечно же, такая формулировка недопустима. Либо нужно распространить запрет на всех субъектов, либо перечислить конкретно тех, на кого он распространяется.

Статьей 140 УК РФ[200] предусмотрен отказ в предоставлении гражданину информации. Проблема доступа граждан к информации о деятельности государственных органов, включающая и право на доступ к своим персональным данным, содержащимся в картотеках государственных органов, лишь совсем недавно стала предметом изучения и обсуждения. Между тем во многих зарубежных странах уже давно действуют законы, регулирующие порядок доступа и получения публичной информации гражданами. Поэтому представляется возможным введение специальной главы в Закон о персональных данных[201], устанавливающей порядок ознакомления граждан с информацией, представляющей общественный интерес, в том числе возможно предусмотреть, чтобы органы и лица, выполняющие функции центральных или местных органов власти были обязаны публиковать или иным образом обеспечивать общественный доступ к важнейшим данным о своей деятельности, в частности к типам находящихся в их распоряжении данных.

---

[198] О частной детективной и охранной деятельности: Закон Росс. Федерации от 11 марта 1992 г. Номер 2487-1 (ред. от 31.12.2014 г.) // СПС Консультант Плюс.

[199] Там же.

[200] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

[201] О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

Статьей 272 УК РФ[202] предусмотрена ответственность за неправомерный доступ к компьютерной информации. Поскольку деятельность операторов информационных систем персональных данных в большинстве случаев автоматизирована и функционирует на основе компьютерного оборудования и программ, то в будущем возможно широкое распространение преступных посягательств именно на этот объект – на компьютеризированную информацию о гражданах. В связи с этим было бы целесообразно разработать и включить в УК РФ[203] специальный состав, предусматривающий уголовную ответственность за неправомерный доступ к информационным системам персональных данных.

Думается, что состав преступления, предусматривающий уголовную ответственность за неправомерный доступ к информационным системам персональных данных, должен быть формальным, т.е. преступление должно считаться законченным, а виновный привлекаться к ответственности независимо от наступления общественно опасных последствий. Причиной этого служит высокая степень общественной опасности деяния, а также тот факт, что совершение данного преступления возможно только с прямым умыслом, так как случайное или неосторожное проникновение в защищенные информационные системы невозможно.

Установление уголовно-правовой охраны данной категории информации вполне уместно в современной России, где традиции уважения к частной жизни лица пока еще недостаточно укоренились. Кроме того, нужно учитывать и значительный моральный и материальный ущерб, который наносится лицу при распространении такого рода сведений.

Неправомерными действиями, связанными с нарушением порядка оборота и защиты персональных данных, гражданину может быть причинен не столько имущественный, сколько моральный вред. По всей видимости, в сфере оборота и защиты персональных данных именно компенсация морального

---

[202] Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.
[203] Там же.

вреда станет основной формой гражданско-правовой защиты указанных общественных отношений. Согласно Гражданскому кодексу РФ[204] возможность компенсации морального вреда существует только в денежной форме.

Нередко на практике встречаются случаи, когда решение суда о взыскании с виновного определенной денежной суммы в счет компенсации морального вреда не может быть исполнено по причине отсутствия у виновного имущества и денежных средств. Складывается общая ситуация, когда из-за финансовой несостоятельности причинителя потерпевший лишается какой бы то ни было возможности компенсировать свои моральные потери. Отсутствие экономических условий делает норму закона о компенсации морального вреда во многом декларативной. Данная ситуация могла бы быть частично исправлена, если бы гражданским законодательством была предусмотрена возможность не только денежной, но и иных форм компенсации морального вреда потерпевшему. Другими словами, виновное лицо должно иметь возможность компенсировать моральный вред не только в денежном выражении, а по договоренности с потерпевшим – в ином соразмерном виде.

[204] Гражданский кодекс Российской Федерации (ГК РФ) Часть 2 от 26.01.1996 г. Номер 14-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

Сокращения, обозначения, термины и определения

ГК РФ – Гражданский кодекс Российской Федерации;

ИСПДн – информационная система персональных данных;

КоАП РФ – Кодекс Российской Федерации об административных правонарушениях;

МВД РФ – Министерство Внутренних Дел Российской Федерации;

Минкомсвязь – Министерство связи и массовых коммуникаций Российской Федерации;

ПДн – персональные данные;

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации;

РФ – Российская Федерация;

СК РФ – Семейный кодекс Российской Федерации;

СМИ – средства массовой информации;

ТК РФ – Трудовой кодекс Российской Федерации;

УК РФ – Уголовный кодекс Российской Федерации;

ФЗ – Федеральный закон;

ФСБ – Федеральная служба безопасности Российской Федерации;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ЭВМ – электронно-вычислительная машина.

Список использованных источников и литературы

1. О защите физических лиц при автоматизированной обработке персональных данных: Конвенция (Страсбург, 28 января 1981 года) // СПС Консультант Плюс.

2. Конституция Российской Федерации: принята всенар. голосованием 12 дек. 1993 г. (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

3. Гражданский кодекс Российской Федерации (ГК РФ) Часть 1 от 30.11.1994 г. Номер 51-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

4. Гражданский кодекс Российской Федерации (ГК РФ) Часть 2 от 26.01.1996 г. Номер 14-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

5. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. Номер 195-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

6. Семейный кодекс Российской Федерации (СК РФ) от 29.12.1995 г. Номер 223-ФЗ (ред. от 20.04.2015 г.) // СПС Консультант Плюс.

7. Трудовой кодекс Российской Федерации (ТК РФ) от 30 декабря 2001 г. Номер 197-ФЗ (ред. от 06.04.2015 г.) // СПС Консультант Плюс.

8. Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. Номер 63-ФЗ (ред. от 23.05.2015 г.) // СПС Консультант Плюс.

9. О безопасности: Федер. закон Росс. Федерации от 28 декабря 2010 г. Номер 310-ФЗ // СПС Консультант Плюс.

10. О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных»: Федер. закон Росс. Федерации от 30 ноября 2011 г. Номер 363-ФЗ // СПС Консультант Плюс.

11. О внесении изменений в ФЗ «О персональных данных»: Федер. закон Росс. Федерации от 01 июля 2011 г. Номер 261-ФЗ // СПС Консультант Плюс.

12. О коммерческой тайне: Федер. закон Росс. Федерации от 29 июля 2004 г. Номер 98-ФЗ (ред. от 12.03.2014 г.) // СПС Консультант Плюс.

13. О кредитных историях: Федер. закон Росс. Федерации от 30 декабря 2004 г. Номер 218-ФЗ (ред. от 28.06.2014 г.) // СПС Консультант Плюс.

14. О лицензировании отдельных видов деятельности: Федер. закон Росс. Федерации от 04.05.2011 г. Номер 99-ФЗ (ред. от 31.12.2014 г.) // СПС Консультант Плюс.

15. О персональных данных: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 152-ФЗ (ред. от 21.07.2014 г.) // СПС Консультант Плюс.

16. О транспортной безопасности: Федер. закон Росс. Федерации от 9 февраля 2007 г. Номер 16-ФЗ (ред. от 03.02.2014 г.) // СПС Консультант Плюс.

17. Об информации, информационных технологиях и о защите информации: Федер. закон Росс. Федерации от 27 июля 2006 г. Номер 149-ФЗ (ред. от 24.11.2014 г.) // СПС Консультант Плюс.

18. Об оперативно-розыскной деятельности: Федер. закон Росс. Федерации от 12 августа 1995 г. Номер 144-ФЗ (ред. от 21.12.2013 г.) // СПС Консультант Плюс.

19. Об электронной подписи: Федер. закон Росс. Федерации от 6 апреля 2011 г. Номер 63-ФЗ (ред. от 28.06.2014 г.) // СПС Консультант Плюс.

20. О средствах массовой информации: Закон Росс. Федерации от 27 декабря 1991 г. Номер 2124-1 (ред. от 24.11.2014 г.) // СПС Консультант Плюс.

21. О частной детективной и охранной деятельности: Закон Росс. Федерации от 11 марта 1992 г. Номер 2487-1 (ред. от 31.12.2014 г.) // СПС Консультант Плюс.

22. Об обжаловании в суд действий и решений, нарушающих права и свободы граждан: Закон Росс. Федерации от 27 апреля 1993 г. Номер 4866-1 (ред. от 09.02.2009 г.) // СПС Консультант Плюс.

23. О лицензировании деятельности по технической защите конфиденциальной информации: Постановление Правительства Росс. Федерации от 3 февраля 2012 г. Номер 79 // СПС Консультант Плюс.

24. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: Постановление Правительства Росс. Федерации от 16 марта 2009 г. Номер 228 (ред. от 22.05.2015 г.) // СПС Консультант Плюс.

25. Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: Постановление Правительства Росс. Федерации от 21.03.2012 Номер 211 (ред. от 06.09.2014 г.) // СПС Консультант Плюс.

26. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: Постановление Правительства Росс. Федерации от 15 сентября 2008 г. Номер 687 // СПС Консультант Плюс.

27. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства Росс. Федерации от 1 ноября 2012 г. Номер 1119 // СПС Консультант Плюс.

28. Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты: Постановление Правительства Росс. Федерации от 5 января 2004 г. Номер 1 // СПС Консультант Плюс.

29. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента Росс. Федерации от 17 марта 2008 г. Номер 351 (ред. от 22.05.2015 г.) // СПС Консультант Плюс.

30. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента Росс. Федерации от 15 января 2013 г. Номер 31с // СПС Консультант Плюс.

31. Об утверждении перечня сведений конфиденциального характера: Указ Президента Росс. Федерации от 6 марта 1997 г. Номер 188 (ред. от 23.09.2005 г.) // СПС Консультант Плюс.

32. Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела: Указ Президента Росс. Федерации от 30 мая 2005 г. Номер 609 (ред. от 01.07.2014 г.) // СПС Консультант Плюс.

33. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. // СПС Консультант Плюс.

34. Доктрина информационной безопасности РФ 9 сентября 2000 г. Номер Пр-1895 // СПС Консультант Плюс.

35. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. // СПС Консультант Плюс.

36. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации: Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. Номер 149/54-144 // СПС Консультант Плюс.

37. Методический документ. Меры защиты информации в государственных информационных системах: Утвержден ФСТЭК России 11 февраля 2014 г. // СПС Консультант Плюс.

38. Некоторые вопросы применения законодательства о компенсации морального вреда: Постановление Пленума Верховного Суда Росс. Федерации от 20.12.1994 г. Номер 10 (ред. от 06.02.2007 г.) // СПС Консультант Плюс.

39. 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 требованиям законодательства Российской Федерации в области персональных данных: Приказ Минкомсвязи России от 14.11.2011 г. Номер 312 (ред. от 24.11.2014 г.) // СПС Консультант Плюс.

40. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК от 18 февраля 2013 г. Номер 21 // СПС Консультант Плюс.

41. 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: Приказ ФСБ России от 10.07.2014 г. Номер 378 // СПС Консультант Плюс.

42. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11 февраля 2013 г. Номер 17 // СПС Консультант Плюс.

43. Положение по аттестации объектов информатизации по требованиям безопасности информации: Утверждено председателем Государственной технической комиссии при Президенте Росс. Федерации 25 ноября 1994 г. // СПС Консультант Плюс.

44. Баймакова И.А. Обеспечение защиты персональных данных. Методическое пособие / И.А. Баймакова, А.И. Новиков, А.И. Рогачев, А.Х. Хыдыров. – 3-е изд. – М.: ООО «1С-Паблишинг», 2011. – 268 с.

45. Галатенко В.А. Стандарты информационной безопасности. Курс лекций: учебное пособие / В.А. Галатенко. – М.: ИНТУИТ.РУ “Интернет-университет Информационных технологий”, 2011. – 264 с.

46. Гортинский А.В. Организационно-правовые основы защиты персональных данных: учебное пособие / А.В. Гортинский. – Саратов: СГУ им. Н.Г. Чернышеского, 2012. – 98 с.

47. Исаев А.С., Хлюпина Е.А. Правовые основы организации защиты персональных данных: учебное пособие / А.С. Исаев, Е.А. Хлюпина. – СПб: НИУ ИТМО, 2014. – 106 с.

48. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие/ В.Я. Ищейнов, М.В. Мецатунян. – М.: Форум, 2009. – 256 с.

49. Куняев Н.Н., Демушкин А.С., Фабричнов А.Г. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Демушкин, А.Г. Фабричнов. – М.: Логос, 2011. – 452 с.

50. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина. – М.: Статут, 2011. – 134 с.

51. Северин В.А. Комплексная защита информации на предприятии: учебник для вузов по направлению и специальности "Юриспруденция" / В.А. Северин. – М.: Издательский Дом «Городец», 2008. – 368 с.

52. Северин В.А. Правовая защита информации в коммерческих организациях: учебное пособие для вузов по специальности и направления "Юриспруденция" / В. А. Северин. – М.: АКАДЕМИЯ, 2009. – 224 с.

53. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: учебное пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2011. – 304 с.

54. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Защита персональных данных: учебное пособие / М.И. Шубинский. – СПб: НИУ ИТМО, 2013. – 77 с.

55. Гильмуллина Д.А., Чикенева И.В. О защите персональных данных в системе трудовых правоотношений / Д.А. Гильмуллина, И.В. Чикенева // Известия Оренбургского государственного аграрного университета. – 2009. – № 3 – с. 231 – 234.

56. Занин К.А. Персональные данные как объект правовой защиты в регистрационной деятельности ОВД / К.А. Занин // Вестник Воронежского института МВД России. – 2010. – № 2. – С.15 – 18.

57. Архангельская А.В. Особенности применения средств криптографической защиты информации при обработке персональных данных // http://pvti.ru/data/file/bit/2012_22/part_6.pdf.

58. Еще раз о законности передачи персональных данных // http://forum.anti-rs.ru/index.php?showtopic=7416.

59. Закон о ПД: некоторые проблемы реализации // http://www.psj.ru/saver_magazins/detail.php?ID=62202.

60. Иващук И. Актуальные вопросы защиты персональных данных // http://www.expert-solution.ru/articles/?ELEMENT_ID=244.

61. Основные законодательные и нормативно-правовые акты в области обработки персональных данных // http://59.rkn.gov.ru/directions/pd/p2314/p14648/.

62. Основные нормативно-правовые акты в области защиты персональных данных // http://www.ifru.ru/6703/.

63. Ответственность за разглашение персональных данных работника // http://hr-portal.ru/article/otvetstvennost-za-razglashenie-personalnyh-dannyh-rabotnika.

64. Персональные данные. Законодательство в области защиты персональных данных // http://www.intuit.ru/studies/courses/697/553/lecture/12444.

65. Помощник президента высказался за пересмотр российского законодательства о защите персональных данных // http://d-russia.ru/pomoshhnik-prezidenta-vyskazalsya-za-peresmotr-rossijskogo-zakonodatelstva-o-zashhite-personalnyx-dannyx.html.

66. Проблемы и перспективы реализации закона о защите персональных данных // http://www.kmis.ru/site.nsf/pages/03.09.2009.htm.

67. Проблемы реализации Федерального закона "О персональных данных" // http://www.silicontaiga.ru/home.asp?artId=9776.

68. Слепов О. Защита персональных данных // http://www.jetinfo.ru/stati/zaschita-personalnykh#gl_3.

69. Соколова О.С. Проблемы реализации Федерального закона "О персональных данных // http://www.recoveryfiles.ru/laws.php?ds=3268.

70. Споры, касающиеся незаконной обработки персональных данных // http://forum.fort-ust.ru/topic/114-spori-kasajushiesja-nezakonnoi-obrabotki-person/.

71. Судебная практика о распространении персональных данных // http://www.vl-1.ru/art/dolg/69.html.

Введение

1 Правовое регулирование в области защиты персональных данных

1.1 Персональные данные как объект правовой охраны

1.2 Нормативно-правовые акты в области защиты персональных данных

2 Права субъекта и обязанности оператора при обработке персональных данных

2.1 Субъект персональных данных и его права при обработке персональных данных

2.2 Обязанности оператора персональных данных

2.3 Меры по обеспечению выполнения оператором своих обязанностей

2.4 Меры по обеспечению безопасности персональных данных при их обработке

3 Проблемы правового регулирования и правовой защиты персональных данных

3.1 Проблемы реализации законодательства РФ о защите персональных данных

3.2 Проблемы применения юридической ответственности за нарушение законодательства о персональных данных

Заключение

Список использованных источников и литературы