ПУБЛИЧНО-ПРАВОВЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

АНАЛИЗ НОРМ ПРАВА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ МЧС РОССИИ

А.Д. Катаржнов, кандидат технических наук.
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики.
С.Б. Хитов.
Санкт-Петербургский университет ГПС МЧС России.
Е.В. Кусов.
Войсковая часть № 42842

Проведен анализ законодательства Российской Федерации в области обеспечения персональных данных, обрабатываемых в информационных системах МЧС России. Рассмотрены основные направления совершенствования государственной политики в области обеспечения безопасности персональных данных, требования основных нормативно-правовых актов Российской Федерации в данной области.

Ключевые слова: информация, информационная система, информационная безопасность, персональные данные, безопасность персональных данных, нормативно-правовой акт, государственная политика

ANALYSIS RUSSIAN LEGAL NORMS IN THE DOMAIN OF PERSONAL DATA SECURITY PROCESSED IN THE INFORMATION SYSTEMS OF EMERCOM OF RUSSIA

A.D. Katarzhnov.
Saint-Petersburg national research university of information technologies, mechanics and optics.
S.B. Khitov. Saint-Petersburg university of State fire service of EMERCOM of Russia.
E.V. Kusov. Military unit № 42842

The article is dedicated analysis Russian legal norms in the domain of personal data security, processed in the information systems of EMERCOM of Russia. Also in the article are considered the basic directions of state policy improvement in the area of personal data security, requirements of main legal regulatory acts of Russia in this domain.

Keywords: information, information system, information security, personal data, personal data security, legal regulatory act, state policy

С ростом применения в деятельности органов управления, подразделений, организаций и учреждений системы МЧС России информационных и управляющих систем различного назначения возрастает и острота проблемы обеспечения безопасности субъектов

информационных отношений, защиты их прав и законных интересов, а также хранящейся и обрабатываемой в подобных системах информации, в том числе персональных данных.

В МЧС России в рамках Федеральной целевой программы «Пожарная безопасность в Российской Федерации на период до 2017 года», утвержденной Постановлением Правительства Российской Федерации от 30 декабря 2012 г. № 1481, отмечено: «Предусмотрено создание системы безопасности связи в главных управлениях МЧС России и на объектах подразделений федеральной противопожарной службы МЧС России» [1]. Данная система состоит из объектовых комплексов безопасности связи, на которые возлагаются функции по обеспечению защиты информационных ресурсов и персональных данных, обрабатываемых в информационных системах.

Построение комплексов осуществляется по следующим направлениям:

– организационно-методическое обеспечение – комплекс организационных и методических мероприятий, которые регламентируют вопросы обработки информации ограниченного доступа, в том числе персональных данных, и являются необходимыми для соответствия требованиям законодательства Российской Федерации в области защиты информационных ресурсов, содержащих персональные данные;

– техническое обеспечение – комплекс программных и программно-аппаратных средств защиты информации, обеспечивающий выполнение технических требований к системе защиты информации, в том числе к системе защиты персональных данных.

При выполнении мероприятий организационно-методического обеспечения должны выполняться требования нормативных правовых актов Российской Федерации в области обеспечения безопасности персональных данных.

В Доктрине информационной безопасности России [1], являющейся составной частью национальной безопасности России, утвержденной Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895, был сделан вывод о неудовлетворительной организации защиты собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Такое положение дел в области обеспечения информационной безопасности Российской Федерации, в том числе в области обеспечения безопасности персональных данных, привело к совершенствованию политики государства в указанной области (рис. 1), созданию нормативной правовой базы и усилению государственного регулирования правового обеспечения безопасности (рис. 2) персональных данных.

В основу организации защиты персональных данных как информации ограниченного доступа положен принцип разделения прав и обязанностей между субъектами обеспечения защищенности этой информации: государством, предприятиями, учреждениями, организациями и отдельными гражданами.

Государство как основной субъект обеспечения защиты информации через свои органы законодательной, исполнительной и судебной властей обеспечивает:

– создание системы правовых норм, регулирующих отношения в области защиты информации;

– проведение единой технической политики, разработку требований и методических рекомендаций по защите информации;

– разработку государственных программ по защите информации;

– общий контроль за состоянием защиты информации.

Предприятия, учреждения и организации независимо от формы собственности, а также отдельные граждане, выполняющие работы, связанные с использованием информации ограниченного доступа, включая обработку персональных данных должны обеспечить их защиту.

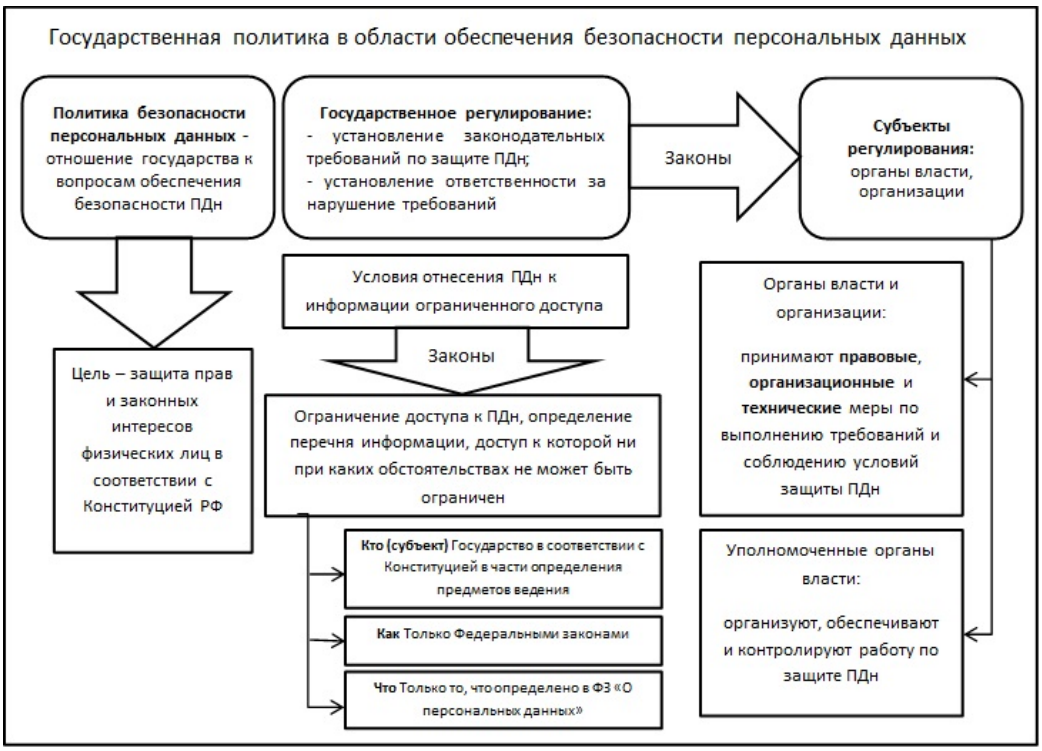

Рис. 1. **Государственная политика в области обеспечения безопасности персональных данных**

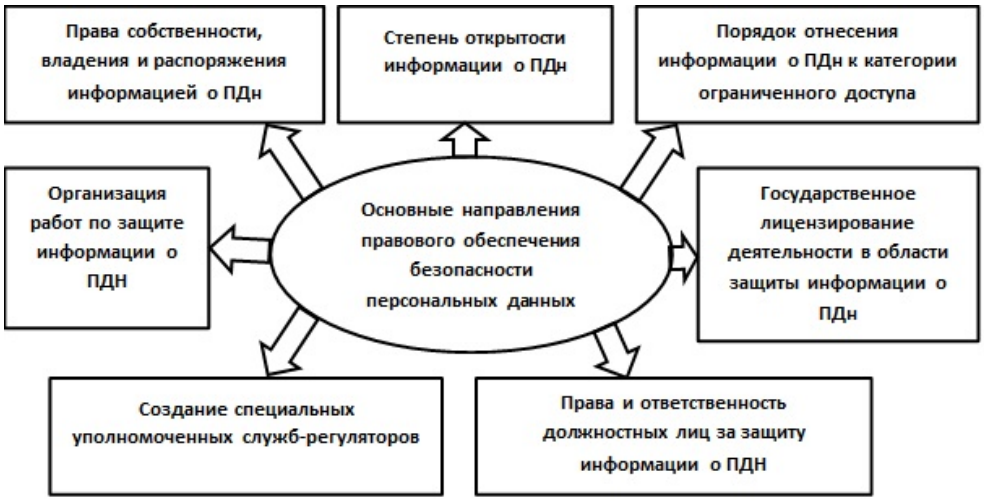

Рис. 2. **Основные направления правового обеспечения безопасности персональных данных**

Особенностями персональных данных как объектов защиты является:

– личная тайна гражданина охраняется Конституцией Российской Федерации. Разглашение этой тайны, то есть бесконтрольное распространение персональных данных во времени и пространстве, может нанести значительный материальный и моральный ущерб физическому лицу;

– понятие личной тайны близко примыкает к семейной тайне, к которой относятся тайна усыновления, тайна отцовства, тайна наследственного заболевания и др. При этом семейная тайна или тайна нескольких физических лиц, членов семьи не тождественна личной тайне по составу защищаемых сведений;

– личная тайна и персональные данные являются «первичными» тайнами, а профессиональные виды тайн (например, врачебная, банковская тайна – «вторичными»);

– персональные данные входят во многие виды тайн (государственная, личная, семейная, коммерческая, банковская, врачебная и т.п.) и должны защищаться с учетом требований по их защите.

Принятие и ратификация Российской Федерацией Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, возложили на страну обязательства по приведению в соответствие с нормами европейского законодательства деятельности в области защиты прав субъектов персональных данных.

Первым шагом в реализации вышеназванных обязательств со стороны России стало принятие Федерального закона Российской Федерации от 27 июля 2006 г. «О персональных данных» (ФЗ РФ № 152-ФЗ) [3]. Указанный Закон направлен на реализацию конституционных положений, закрепляющих право каждого на неприкосновенность частной жизни и свободу информации, а также на воплощение в жизнь международных обязательств Российской Федерации. В этой связи не случайно, что в качестве основополагающих принципов обработки персональных данных законодатель определил соответствие способа обработки и объема обрабатываемых данных с законными целями, определенными оператором до начала обработки, а также недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных (ИСПДн).

ФЗ РФ № 152-ФЗ (п. 1 ст. 1), в настоящее время действующего с последними изменениями, внесенными Федеральным законом Российской Федерации от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» (ФЗ РФ № 261-ФЗ), регулируются отношения, связанные с обработкой персональных данных, осуществляемые федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами (муниципальные органы), юридическими лицам и физическими лицами с использованием средств автоматизации, в том числе, в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Внесение ФЗ РФ № 261-ФЗ [4] поправок существенно изменило редакцию ФЗ РФ № 152-ФЗ в части:

– терминологии (персональные данные, биометрические персональные данные, обезличивание, обработка, автоматизированная обработка, трансграничная передача, условия обработки персональных данных);

– условий обработки персональных данных без согласия субъекта персональных данных;

– условий обработки специальных категорий персональных данных;

– условий трансграничной передачи персональных данных;

– условий ограничения и не предоставления доступа субъекта к его персональным данным.

– контроля и надзора за выполнением требований по защите персональных данных со стороны ФСТЭК и ФСБ России;

– содержания уведомления об обработке персональных данных в Роскомнадзор.

– возмещения морального вреда субъекту персональных данных независимо от возмещения имущественного вреда и понесенных убытков.

Кроме этого, в новую редакцию Закона внесены следующие дополнения:

1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом (ст. 18.1):

– публикации политики об обработке персональных данных;

– предоставление оператором Роскомнадзору доказательств реализации мер по защите персональных данных.

2. Меры по обеспечению безопасности персональных данных при их обработке (переработка правил) ст. 19.

3. Назначение оператором лица, ответственного за организацию обработки персональных данных (ст. 21.1).

Действие ФЗ РФ № 152-ФЗ распространяется на юридических и физических лиц, обрабатывающих персональные данные.

В ст. 3 ФЗ РФ № 152-ФЗ определено понятие «оператора персональных данных» – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, определяющие цели и содержание обработки персональных данных.

Таким образом, оператором персональных данных будет являться любая организация, осуществляющая даже простую систематизацию, накопление или только хранение персональных данных. Органы управления, подразделения, организации и учреждения системы МЧС России как минимум осуществляют сбор, систематизацию, хранение и уточнение сведений о своих сотрудниках. При этом практически во всех из них, на сегодняшний день применяются те или иные информационные системы – автоматизированная информационно-управляющая система Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (АИУС РСЧС), ИС «Делопроизводство», АИС «Монолит» и многие другие. С учетом вышеизложенного органы управления, подразделения, организации и учреждения системы МЧС России являются операторами персональных данных и обязаны выполнять требования российского законодательства в области обеспечения безопасности персональных данных, прежде всего – требования ФЗ РФ № 152-ФЗ.

Основополагающим понятием в ФЗ РФ № 152-ФЗ является понятие «персональные данные», под которыми понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). Так, к числу основных документов, содержащих персональные данные сотрудника (работника) МЧС России, должны быть отнесены:

– служебный контракт (трудовой договор);

– приказ (распоряжение) о приеме на службу (работу);

– приказы (распоряжения) об изменении условий служебного контракта (трудового договора), его прекращении;

– приказы (распоряжения) о поощрениях и дисциплинарных взысканиях, примененных к сотруднику (работнику);

– трудовая книжка.

К составу персональных данных сотрудника (работника) можно отнести сведения, предусмотренные унифицированной формой учета кадров Т-2, утвержденной Постановлением Госкомстата Российской Федерации от 5 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты» [5].

К таким сведениям относятся:

– фамилия, имя, отчество;

– дата 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.).

В соответствии со ст. 4 ФЗ РФ № 152-ФЗ законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов (рис. 3). Вопросы обработки персональных данных, так или иначе, затрагивают 75 международных договоров, подписанных Россией, 13 кодексов, более 100 законов и 250 актов Правительства Российской Федерации.

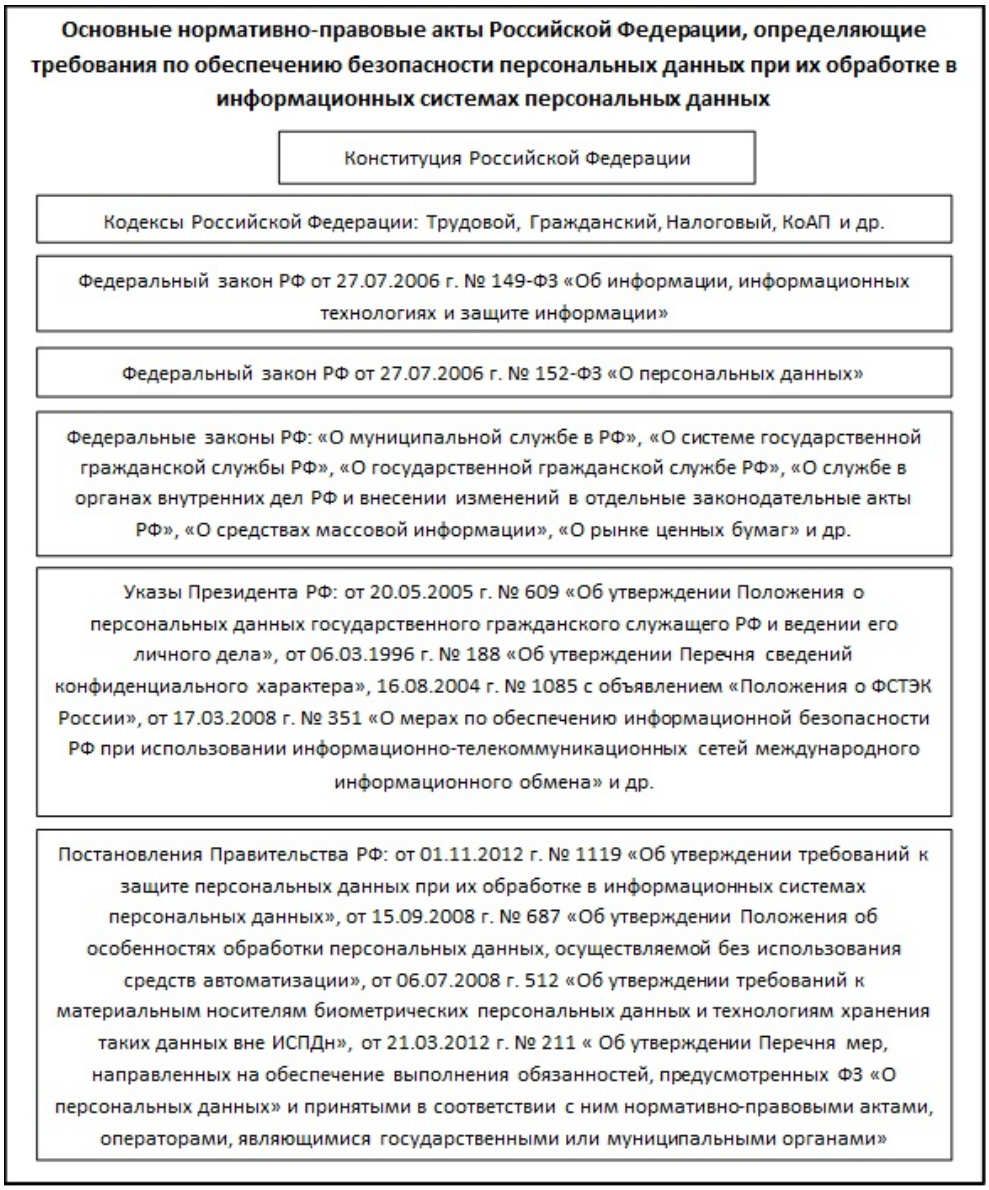

Рис. 3. **Основные нормативно-правовые акты Российской Федерации, определяющие требования по обеспечению безопасности персональных данных при их обработке в ИСПДн**

На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

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

Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора. ФЗ РФ № 152-ФЗ определены принципы (ст. 5) и условия (ст. 6) обработки операторами персональных данных, необходимость обеспечения их конфиденциальности при обработке (ст. 7), установлены правила обработки персональных данных предусматривающие получение согласия субъекта персональных данных (ст. 9). Законом определено, что порядок получения согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг в форме электронного документа, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

Кроме требований ФЗ РФ № 152-ФЗ оператору при обработке персональных данных необходимо учитывать и требования других нормативных правовых актов. Так, Трудовым кодексом Российской Федерации (ТК РФ) [6] (ст. 86) установлены следующие общие требования при обработке персональных данных работника и гарантии их защиты:

– обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

– при определении объема и содержания обрабатываемых персональных данных работника, работодатель должен руководствоваться Конституцией Российской Федерации, ТК РФ и иными федеральными законами, в том числе ФЗ РФ № 152-ФЗ;

– все персональные данные работника работодатель должен получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

– работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

– работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением ряда случаев, предусмотренных ТК РФ или федеральными законами;

– при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональные данные работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

– защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном кодексом Российской Федерации, и иными федеральными законами, в том числе ФЗ РФ № 152-ФЗ;

– работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

– работники не должны отказываться от своих прав на сохранение и защиту тайны;

– работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Согласно ст. 87 ТК РФ порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований ТК РФ, ФЗ РФ № 152-ФЗ и иных федеральных законов. Таким образом, в организациях должно быть разработано и утверждено «Положение о порядке хранения и использования персональных данных работников». Статья 88 ТК РФ устанавливаются строгие требования к порядку передачи персональных данных работника.

Согласно ст. 2 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ФЗ РФ № 149-ФЗ) [7] распространением информации называются действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Одним из видов распространения персональных данных является обнародование персональных данных в средствах массовой информации. В соответствии со ст. 2 Федерального закона Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» [8] массовой информацией называются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы. Под средством массовой информации понимается периодическое печатное издание, радио-, теле-, видеопрограмма, кинопрограмма, иная форма периодического распространения массовой информации.

Распространение персональных данных может происходить и в форме их размещения в информационно-телекоммуникационных сетях. В ст. 2 ФЗ РФ № 149-ФЗ определено, что информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Примером информационно-телекоммуникационной сети является сеть Интернет.

Постановлением Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» [9] устанавливается, что операторы федеральных государственных информационных систем, созданных или используемых в целях реализации полномочий федеральных органов исполнительной власти и содержащих сведения, указанные в перечне сведений о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети Интернет», при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям, доступ к которым не ограничен определенным кругом лиц, обязаны обеспечить:

– защиту информации, содержащейся в информационных системах общего пользования, от уничтожения, изменения и блокирования доступа к ней;

– постоянный контроль возможности доступа неограниченного круга лиц к информационным системам общего пользования;

– восстановление информации, измененной или уничтоженной вследствие несанкционированного доступа к ней, в течение не более 8 ч.;

– использование при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям средств защиты информации, прошедших оценку соответствия (в том числе в установленных случаях сертификацию), в порядке, установленном законодательством Российской Федерации.

Операторы информационных систем общего пользования и операторы связи обязаны обеспечивать информационную безопасность при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям.

В ст.ст. 18.1, 19 ФЗ РФ № 152-ФЗ, в настоящее время действующего с последними изменениями, внесенными ФЗ РФ № 261-ФЗ установлены меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом. При этом оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.

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.

Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с ч. 3 ст. 19 ФЗ РФ № 152-ФЗ 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, а также контроль и надзор за их выполнением, устанавливаются и осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России), и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий (ФСТЭК России).

Вышеуказанные требования 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 в настоящее время установлены Приказом ФСТЭК России от 18 февраля 2013 г. № 21.

Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [10] утверждены требования к защите персональных данных при их обработке в информационных системах персональных данных

и установлены уровни защищенности персональных данных при их обработке в информационных системах персональных данных.

Конкретные требования по нейтрализации выявленных угроз безопасности и требования к защитным механизмам определяются после определения уровня угроз безопасности персональным данным при их обработке в ИСПДн на основе построения модели и определении актуальных угроз на основании нормативных и методических документов ФСТЭК и ФСБ России.

Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [11] устанавливаются и требования к обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации. Обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. Важно учитывать, что при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне ИСПДн установлены Постановлением Правительства Российской Федерации от 6 июля 2008 г. № 512. Указанные требования должны применяться при использовании материальных носителей, на которые осуществляется запись биометрических персональных данных, а также при хранении биометрических персональных данных вне ИСПДн.

Особенности порядка получения, обработки, хранения, передачи и любого другого использования персональных данных государственных гражданских служащих Российской Федерации установлены «Положением о персональных данных государственного гражданского служащего РФ и ведении его личного дела», утвержденного Указом Президента Российской Федерации от 30 мая 2005 г. № 609 [12]. В соответствии с указанным Положением руководители государственных органов обязаны:

– обеспечить защиту персональных данных государственных гражданских служащих Российской Федерации, содержащихся в их личных делах, от неправомерного их использования или утраты за счет средств государственных органов в порядке, установленном федеральными законами;

– определить лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных государственных гражданских служащих Российской Федерации в государственном органе и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

При выполнении требований законодательства Российской Федерации при защите информации ограниченного доступа, к которой относятся и персональные данные, необходимо учитывать и другие руководящие документы ФСТЭК (Гостехкомиссии) России. Основными из них являются:

– РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» 1992 г.

– РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» 1992 г.

– РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» 1997 г.

– РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники» 1992 г.

– РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» 2001 г.

– РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» 2002 г.

– «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР – К)» 2002 г.

За последнее время было принято еще несколько нормативных актов по защите персональных данных:

– Закон Российской Федерации «О внесении изменений в некоторые законодательные акты РФ в связи с принятием Федерального закона Российской Федерации «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

– Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных»;

– Приказ Роскомнадзора от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных»;

– Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

– Приказ ФСБ России от 10 июля 2014 г. № 378 г. «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».

Решение задач по реализации требований, рассмотренных выше нормативных, методических и других руководящих документов в области обеспечения безопасности персональных данных при выполнении мероприятий организационно-методического обеспечения в рамках создания системы безопасности связи в главных управлениях МЧС России и на объектах подразделений федеральной противопожарной службы МЧС России позволяет успешно обеспечить защиту информационных ресурсов, служебной информации, информации ограниченного распространения, а также персональных данных, обрабатываемых в информационных системах МЧС России.

Литература

1. Об утверждении Федеральной целевой программы «Пожарная безопасность в Российской Федерации на период до 2017 г.»: Постановление Правительства Рос. Федерации от 30 дек. 2012 г. № 1481. URL: http://www.mchs.gov.ru/document/369038 (дата обращения: 22.01.2015).

2. Доктрина информационной безопасности Российской Федерации (утв. Президентом Рос. Федерации от 9 сент. 2000 г. Пр-1895). Доступ из информ.-правового портала «Гарант».

3. О персональных данных: Федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ // Рос. газ. 2006. № 4131.

4. О внесении изменений в Федеральный закон Рос. Федерации «О персональных данных»: Федер. закон Рос. Федерации от 25 июля 2011 года № 261-ФЗ // Рос. газ. 2011. № 5538.

5. Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты: Постановление Госкомстата Рос. Федерации от 5 янв. 2004 г. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Трудовой кодекс Рос. Федерации № 197-ФЗ // Рос. газ. 2001. № 2868.

7. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ // Рос. газ. 2006. № 4131.

8. О средствах массовой информации: Закон Рос. Федерации от 27 дек. 1991 г. № 2124-1. URL: http://www.rg.ru/1991/12/27/smi-zakon.html (дата обращения: 24.01.2015).

9. Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям: Постановление Правительства Рос. Федерации от 18 мая 2009 г. № 424 // Рос. газ. 2009. № 4916.

10. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства Рос. Федерации от 1 нояб. 2012 г. № 1119 // Рос. газ. 2012. № 5929.

11. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: Постановление Правительства Рос. Федерации от 15 сентября 2008 г. № 687 // Рос. газ. 2008. № 4757.

12. Положение о персональных данных государственного гражданского служащего РФ и ведении его личного дела: Указ Президента Рос. Федерации от 30 мая 2005 г. № 609 // Рос. газ. 2005. № 3789.