DOI: 10.25586/RNU.V9187.18.11.P.139 УДК 004.056

В.А. Пиков, А.Е. Вергасова

СПОСОБ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА РОССИЙСКОЙ ФЕДЕРАЦИИ № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ» В РОССИЙСКОЙ ЧАСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

В данной статье рассмотрены базовые способы обеспечения требований безопасности обработки персональных данных в интернет-ресурсах российской части информационно-телекоммуникационной сети Интернет. Разработан способ, реализующий требования Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ (в его последней редакции), предложен ряд организационных и технических мер для обеспечения информационной безопасности интернет-ресурсов.

Ключевые слова: *персональные данные, информационная безопасность, интернет-сайт, веб-портал.*

V.A. Pikov, A.E. Vergasova

METHOD OF IMPLEMENTATION OF REQUIREMENTS OF THE FEDERAL LAW OF THE RUSSIAN FEDERATION № 152-FZ "ON PERSONAL DATA" IN THE RUSSIAN PART OF THE INFORMATION AND TELECOMMUNICATION NETWORK "INTERNET"

This article describes the basic ways to ensure the security of personal data processing in the Internet resources of the Russian part of the information and telecommunication network «Internet». The method that implements the Federal law requirements of the Russian Federation № 152 «On personal data» (as amended), the number of organizational and technical measures to ensure information security of Internet resources.

Keywords: *personal data, information security, website, web-portal.*

С конца 1970-х гг. массовое распространение персональных компьютеров и информационных сетей позволило не только автоматизировать, но и информатизировать рабочие места. Компьютеризация охватила практически все сферы жизнедеятельности людей. К сожалению, как и любое другое достижение человечества, компьютер, имея ряд преимуществ в решении задач в технических, экономических и социальных сферах, одновременно создает новые, не менее сложные.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах, наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия.

Жизненно важные интересы субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических

и других сторон деятельности (конфиденциальная коммерческая и персональная информация) была бы доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования, блокирования или уничтожения.

До 2006 г. нормативно-правовая база, регулирующая персональные данные, носила сильно разрозненный характер. В России существовало множество документов, предусматривающих различные условия и правовые основания обработки персональных данных субъектов.

За более чем 11 лет действия Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» четко выработаны принципы защиты персональных данных, значительное развитие получил институт защиты персональных данных в сети Интернет, внедрены электронные услуги, связанные с использованием собранной и накопленной информации о человеке.

Никто не будет спорить, что сегодня сфера защиты персональных данных – одна из самых динамично развивающихся областей права. Закон перенес более 16 изменений и, возможно, будет изменен еще не один раз [11].

Стоит отметить, что основной посыл Федерального закона «О персональных данных» состоит в том, что информация, содержащая любые персональные данные, не принадлежит никому, кроме самого владельца. Если какая-либо компания запрашивает эти сведения, то она должна обосновать это желание и получить разрешение от владельца либо иметь на обработку законные основания. Кроме того, такая компания должна обеспечить безопасность этой информации.

Рано или поздно с вопросом обработки персональных данных сталкивается любой интернет-предприниматель. Когда проект набирает критическую массу клиентов, приходится задумываться о том, как привести документы на сайте в порядок. Но на практике дело ограничивается лишь размещением на страницах своего интернет-представительства оферты и описаний правил работы сайта.

В этом ли состоит реализация требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?

Статья 3 вышеуказанного закона дает следующее определение.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) [2].

Стоит обратить особое внимание на словосочетание «определенному или определяемому физическому лицу». Если по информации или ее совокупности можно понять о ком речь, то перед вами то, что называют персональными данными. Если понять нельзя, то эту информацию скорее всего нельзя отнести к персональным данным.

Важно определить и оператора персональных данных. В статье 3 Федерального закона «О персональных данных» это сделано следующим образом.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Действие настоящего Федерального закона «О персональных данных» не распространяется на отношения, возникающие при (пункт 2 статьи 1 Закона):

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других

архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

4) обстоятельствах, когда предоставление, распространение, передача и получение информации о деятельности судов в Российской Федерации, содержащей персональные данные, ведение и использование информационных систем и информационно-телекоммуникационных сетей в целях создания условий для доступа к указанной информации осуществляются в соответствии с Федеральным законом от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

В Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» сказано, что оператор (владелец интернет-ресурса) вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных в случае, если:

1) персональные данные обрабатываются исключительно во исполнение требований трудового законодательства (подпункт 1 пункта 2 статьи 22 Закона);

2) персональные данные обрабатываются исключительно для исполнения договора, стороной которого является субъект персональных данных (подпункт 2 пункта 2 статьи 22 Закона);

3) персональные данные о членах общественной или религиозной организации обрабатываются самой этой организацией (подпункт 3 пункта 2 статьи 22 Закона);

4) если сам субъект персональных данных сделал их общедоступными (подпункт 4 пункта 2 статьи 22 Закона);

5) персональные данные включают в себя только фамилии, имена и отчества субъектов персональных данных (подпункт 5 пункта 2 статьи 22 Закона);

6) это необходимо в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях (подпункт 6 пункта 2 статьи 22 Закона);

7) обрабатываются персональные данные, включенные 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 (подпункт 7 пункта 2 статьи 22 Закона);

8) персональные данные обрабатываются без использования средств автоматизации (но с соблюдением требований, установленных Постановлением Правительства РФ от 15 сентября 2008 г. № 687) (подпункт 8 пункта 2 статьи 22 Закона);

9) персональные данные обрабатываются в случаях, предусмотренных законодательством Российской Федерации 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 (подпункт 9 пункта 2 статьи 22 Закона).

В настоящее время почти любой пользователь в сети Интернет оставляет о себе сведения, являющиеся персональными данными (далее – ПДн). Большинство интернет-ресурсов обрабатывает эту информацию, даже не подозревая или не обращая внимание на данное обстоятельство, нарушая законодательство Российской Федерации.

Данная тема является актуальной, потому что в Российской Федерации все больше уделяют внимание теме защите персональных данных конечных пользователей. Так в июле 2017 г. регулятор внес изменение в штраф за нарушение законодательства Российской Федерации в области обработки и защиты персональных данных и увеличил максимально допустимый штраф до 300 тыс. руб.

Целью данного исследования является проработка способа реализации требований Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в сети Интернет [2].

Термин «информация» разные научные области определяют по-разному. Однако в области защиты персональных данных принято пользоваться терминологией Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1].

С точки зрения законодательства Российской Федерации информация – это сведения (сообщения, данные) независимо от формы их представления [1].

С точки зрения защиты информации ее можно разделить на информацию ограниченного доступа и общедоступную.

Общедоступная информация – информация, доступ к которой не может быть ограничен, она подлежит распространению или предоставлению в соответствии с федеральными законами Российской Федерации.

Информацией ограниченного доступа считается информация, доступ (т.е. ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение) к которой ограничен федеральными законами. К такой информации относятся (рис. 1):

• государственная тайна;

• сведения конфиденциального характера (коммерческая тайна, врачебная тайна, служебная тайна и т.д.);

• персональные данные.

Рис. 1. Схема деления информации

Безопасность объекта определяется его отдельными свойствами, которые описываются показателями, значения которых имеют либо конкретную величину, либо находятся в определенных интервалах, поэтому в зависимости от значения этих показателей можно устанавливать разные уровни безопасности для конкретных условий существования объекта.

Таким образом, можно сделать следующие выводы.

1. Безопасность как состояние объекта определяется его свойствами для конкретных условий существования в определенное время.

2. Уровень безопасности определяется значениями или интервалами значений показателей, характеризирующих соответствующие свойства объекта.

3. Обеспечение безопасности объекта осуществляется путем проведения комплекса мероприятий, одна группа которых направлена на изменение свойств самого объекта в соответствии с изменившимися условиями его существования и определяется

как защита, а другая – против осуществляемых источником угроз воздействий или на изменение свойств источника угроз и определяется как противодействие.

Соответственно понятие защищенности объекта, его безопасности – не только качественное, но и количественное, так как мы можем говорить о так называемых «уровнях защищенности», которые в первую очередь должны определяться ценностью информации.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Следует подчеркнуть, что в то время, как информационная безопасность – это состояние защищенности информационной среды, защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Любая деятельность по обеспечению безопасности информации должна быть регламентирована законодательством (рис. 2). В области защиты персональных данных все работы осуществляются на основании ФЗ № 152-ФЗ «О персональных данных». Этот Федеральный закон устанавливает, что именно относится к персональным данным [2]. Далее следуют постановления Правительства Российской Федерации, которые описывают общие требования и рекомендации по работе с информацией ограниченного доступа [3]. Требования по защите информации определяются на основании нормативно-методической документации (далее – НМД) государственных регуляторов ФСБ России и ФСТЭК России [3; 4].

Рис. 2. Нормативно-правовая база по защите персональных данных

Построение системы защиты персональных данных состоит из таких пунктов, как:

1) описание объекта защиты и определение перечня защищаемых ресурсов;

2) классификация информационной системы по обработке персональных данных;

3) определение модели угроз;

4) создание модели нарушителя;

5) выполнение требований по защите информационной системы обработки персональных данных.

Для реализации комплексной системы защиты на всех участках обработки, хранения и передачи информации необходимо использовать организационные и технические меры защиты информации (рис. 3).

Рис. 3. Структура СЗПДн

Средства защиты информации, реализующие требования защиты ПДн, отображены в табл. 1.

Таблица 1

Средства защиты информации, реализующие требования защиты ПДн

Средство защиты информации	Примеры реализации требований
Средство межсетевого экранирования	Cisco 55xx Fortigate
Средство доверенной загрузки	Соболь 3.0 Криптон замок
Средство анализа защищенности	Xspider 7.8 Redcheck
Средство обнаружения вторжений	Рубикон Vipnet IDS
Средства антивирусной защиты	Dr.Web Kaspersky
Средства защиты от НСД	Dallas lock Secret Net

В табл. 2 отображены результаты сопоставления требований Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» требованиям для типового интернет-ресурса. Выполнение требований для интернет-ресурса представляют собой адаптированные, по сравнению с реализацией в привычных ИСПДн, рекомендации по реализации требований защиты обрабатываемых на нем персональных данных.

Таблица 2

Требования по защите ПДн для интернет-ресурса

№ п/п	Требование	Выполнение требования в интернет-ресурсе
Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»		
1	Ст. 5, ч. 1 Для каждой категории субъектов ПДн существует законное основание обработки ПДн	Для каждого субъекта персональных данных необходимо иметь законное основание обработки персональных данных. Это может быть согласие на обработку персональных данных самого субъекта или ответственного лица, либо обработка персональных данных обусловлена требованиям законодательства Российской Федерации
2	Ст. 5, ч. 2 Для каждой категории субъектов ПДн определены цели обработки ПДн	Необходимо иметь для каждой категории субъектов персональных данных понимание, зачем собираются персональные данные. Цели должны иметь обоснованный характер и нерасплывчатое определение, нести конкретику
3	Ст. 5, ч. 4 Обрабатываемые ПДн соответствуют целям обработки ПДн	Перечень персональных данных не должен быть избыточным по отношению к целям обработки персональных данных. Это значит, что при трудоустройстве или оформлении заказа запрещено собирать избыточные сведения, например, о близких родственниках
4	Ст. 9, ч. 4 Соответствие согласий на обработку ПДн требований ФЗ № 152-ФЗ	Формы согласий на обработку ПДн должны соответствовать требованиям ФЗ № 152-ФЗ. Особое внимание стоит уделять передаче персональных данных третьим лицам; необходимо максимально информативно указать перечень, цель и юридический адрес конкретного третьего лица. Как правило, в настоящее время лучшим решением является выполнение правил: одно согласие на одну цель
5	Ст. 5, ч. 3 Наличие разных баз данных ПДн, обрабатываемых с различными целями	Базы данных ПДн, обрабатываемые с различными целями, должны быть обособлены и разделены. Они не должны обрабатывать персональные данные различных субъектов при различных целях
6	Ст. 21 Обеспечение мер по удалению или уточнению неполных ПДн	Должны быть разработаны документы, регламентирующие правила уточнения и удаления информации в организации
7	Ст. 5, ч. 7 Определены сроки обработки ПДн и способы их удаления или обезличивания при достижении целей или сроков обработки	Необходимо, чтобы были определены сроки обработки персональных данных. Бессрочно персональные данные не должны обрабатываться
8	Ст. 6, ч. 3–5 Организация поручения обработки ПДн	Должны быть договорные поручения на поручения обработки персональных данных, в которых оговорены пункты об обработке персональных данных
9	Ст. 6, ч. 3 Наличие в договорах с третьими лицами положений конфиденциальности передаваемых ПДн	В договорах должна быть определена необходимость обеспечения конфиденциальности передаваемых ПДн

Продолжение таблицы

№ п/п	Требование	Выполнение требования в интернет-ресурсе
10	Ст. 18.1 Наличие обязательств о неразглашении ПДн от работников, допущенных к обработке ПДн	Работники, допущенные к обработке ПДн, должны подписывать обязательство о неразглашении ПДн
11	Ст. 16, ч. 3 Разъяснение субъекту персональных данных юридических последствий отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом	Субъекту ПДн должны разъясняться юридические последствия отказа предоставить его ПДн
12	Ст. 18, ч. 5 Обеспечение обработки персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации	Базы данных должны быть расположены на территории РФ
13	Ст. 18.1, ч. 2 Публикация в открытом доступе документа, определяющего его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных	Политика в отношении обработки персональных данных должна быть размещена на сайте и быть в открытом доступе
14	Ст. 22 Уведомление уполномоченного органа по защите прав субъектов персональных данных	Необходимо отправить уведомление в Роскомнадзор об обработке персональных данных, чтобы Роскомнадзор внес в реестр операторов, обрабатывающих ПДн
15	Ст. 18.1, ч. 1, п. 1 Назначение оператором ответственного за организацию обработки персональных данных	Должен быть назначен ответственный за организацию обработки ПДн. Назначение производится внутренним приказом
16	Ст. 18.1, ч. 1, п. 2 Издание оператором документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений	Необходимо разработать перечень необходимой документации в области обеспечения безопасности при обработке персональных данных

№ п/п	Требование	Выполнение требования в интернет-ресурсе
17	Ст. 18.1, ч. 1, п. 4 Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора	Необходимо осуществлять внутренний контроль и аудит соответствия обработки ПДн требованиям Федерального закона № 152-ФЗ «О персональных данных»
18	Ст. 18.1, ч. 1, п. 5 Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом	Должна быть проведена оценка вреда
19	Ст. 18.1, ч. 1, п. 6 Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации 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	Необходимо разработать процедуру ознакомления работников, осуществляющих обработку ПДн, с требованиями безопасности
20	Ст. 19, ч. 2, п. 1 Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных	Должна быть разработана модель угроз для каждой информационной системы персональных данных (далее – ИСПДн)
21	Ст. 19, ч. 2, п. 3 Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации	Необходимо прохождение СЗИ оценки соответствия

Окончание таблицы

№ п/п	Требование	Выполнение требования в интернет-ресурсе
22	Ст. 19, ч. 2, п. 4 Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных	Необходимо провести оценку эффективности принимаемых мер по обеспечению безопасности ПДн
23	Ст. 19, ч. 2, п. 5 Учет машинных носителей персональных данных	Должен осуществляться учет машинных носителей персональных данных
24	Ст. 19, ч. 2, п. 6 Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер	Должен быть разработан порядок обнаружения фактов несанкционированного доступа к ПДн
25	Ст. 19, ч. 2, п. 7 Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Должен быть разработан и утвержден «Регламент резервного копирования и восстановления информации ИТ-инфраструктуры»
26	Ст. 19, ч. 2, п. 8) Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных	Должны осуществляться регистрация и учет действий пользователей в ИСПДн
27	Ст. 19, ч. 2, п. 9 Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных	Должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности ПДн

Требования Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» должны быть выполнены владельцами интернет-ресурсов, если:

1) сайт позволяет производить регистрацию пользователей (даже с таким минимальным набором данных, как имя пользователя плюс адрес электронной почты); как правило, это такие интернет-ресурсы, как форумы, социальные сети, некоторые новостные сайты, интернет-магазины, блоги, сайты с частными объявлениями и многие другие;

2) сайт позволяет вносить в формы персональные данные пользователей, которые впоследствии публикуются на сайте или отправляются по электронной почте; например, если на сайте есть функция «перезвонить мне», возможность отправить быстрый заказ или подписаться на рассылку и т.п.;

3) сайт уже содержит реальные персональные данные граждан;

4) фирма (юридическое лицо или индивидуальный предприниматель) на постоянной основе занимается обработкой персональных данных граждан.

Это утверждение справедливо для:

– юридических фирм;

– регистраторов (в смысле компаний, занимающихся регистрацией юрлиц и ИП, изменениями, ликвидацией и т.д.);

– реестродержателей;

– бухгалтерских компаний, оказывающих услуги по аутсорсингу бухгалтерии и кадрового делопроизводства;

– банков, МФО и других компаний финансового сектора, работающих с данными граждан;

– медицинских учреждений;

– магазинов, салонов красоты и других подобных организаций с персональными клубными картами (это особенно популярно у сетевых магазинов косметики);

– образовательных организаций и учреждений (в том числе проводящих краткосрочные курсы или разовые тренинги);

– ТСЖ и управляющих компаний в сфере ЖКХ;

– турагентств;

– третейских судов и мн. др.;

5) компания активно работает с внештатными сотрудниками (по гражданско-правовому договору);

6) компания использует CRM или аналогичные системы;

7) во всех остальных случаях, если компания не попала под исключения, описанные выше.

Чтобы стать оператором персональных данных, во-первых, придется подготовить пакет документов, предусмотренных законодательством о персональных данных, который включает в себя более 30 наименований.

Во-вторых, следует уведомить компетентный орган – Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) о начале обработки персональных данных. После чего компания будет внесена в Реестр операторов персональных данных.

В-третьих, нужно отслеживать изменения в законодательстве о персональных данных, так как периодически придется направлять в Роскомнадзор новые уведомления и вносить коррективы в действующие внутренние положения, регламенты и другие документы [12].

Штрафы по Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» определяются статьей 24. Указанное положение ссылается на взыскания, предусмотренные законодательством. В штрафы включается и моральный вред, а также расходы, понесенные субъектом в связи с разглашением его данных.

Чтобы определить нормы законодательства по штрафам, следует рассмотреть дополнительные правовые документы. Кодекс об административных правонарушениях определяет сумму штрафа в 10 тыс. руб. Взысканию может быть подвергнуто физическое или должностное лицо (а также компания) за нарушение предписаний федерального закона. Однако с 1 июля 2017 г. последние изменения в его положения предписывают штраф до 75 тыс. руб. Также упростилась процедура их взыскания [11].

Пункт 3 статьи 13.11 КоАП РФ «невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных» влечет предупреждение или наложение административного штрафа:

– на граждан в размере от 700 до 1 500 руб.;

– на должностных лиц – от 3 000 до 6 000 руб.;

– на индивидуальных предпринимателей – от 5 000 до 10 000 руб.;

– на юридических лиц – от 15 000 до 30 000 руб.

В сети Интернет появились многочисленные онлайн-сервисы (пример: https://152фз.рф/), которые по запросу проверяют соответствие сайтов требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Все они предлагают с разной степенью автоматизации составить и разместить на интернет-сайте два документа: «Политика обработки персональных данных» и «Пользовательское соглашение», а также проверяют наличие возможности пользователям поставить «галочки» на «Согласие на обработку персональных данных» в формах обратной связи, подписки на рассылку, комментирования и т.д.

Вряд ли эти меры защитят персональные данные субъектов.

Большинство серверов крупнейших интернет-компаний находятся в Америке. «Яндекс» построил дата-центр в Рязанской области на территории девяти бывших цехов машиностроительного завода «Саста», до конца 2019 г. там будет установлено около 100 тыс. серверов. Кроме России у компании есть дата-центры в Нидерландах, США и Финляндии. У Mail.Ru Group в России пять дата-центров плюс аренда серверов за границей. В связи с новым законом, по которому российское правительство обязует компании хранить данные российских пользователей только на территории страны, ожидается, что дата-центров в России станет больше. Однако пока зарубежные интернет-компании не комментируют их будущую работу в России, и в СМИ время от времени появляется информация о том, что власти ведут переговоры с Facebook, Google, Twitter и другими интернет-гигантами. Организации и отдельные люди, которые хранят, собирают, передают или обрабатывают персональные данные, по закону относятся к операторам персональных данных. Все они с июля 2016 г. должны хранить информацию о российских пользователях на территории России. Интернет-компании, нарушающие этот закон, получат предупреждение от Роскомнадзора. Если нарушения не устранят в течение дня, компании внесут в специальный реестр, а доступ к ним по решению суда будет заблокирован.

Все-таки вернемся к защите персональных данных на просторах сети Интернет. Вот что предлагают разные источники.

1. Необходимо разместить на сайте документ, который определяет политику оператора в отношении обработки персональных данных. Законодатель указал, что доступ должен быть неограниченным, а как вы обеспечите этот доступ неограниченному кругу лиц, законодатель не указал, это должен решить для себя сам оператор. Например, можно разместить ссылку «Политика защиты и обработки персональных данных» внизу сайта, чтобы можно было увидеть ее на любой странице.

2. Обрабатывать только те категории ПДн, использование которых вы можете обосновать. Если вы запрашиваете дату рождения пользователя и ставите его в известность о том, что у вас в компании работает система скидок, связанная с возрастом клиента или есть специальная скидка в день рождения, то будет считаться, что сбор этой информации вполне обоснован.

3. Использовать собранные данные в строгом соответствии с теми целями, которые вы обозначали вашему клиенту перед тем, как он вам свои данные предоставил.

Исходя из сказанного, появляется вопрос: «Почему Роскомнадзор не отслеживает реальное положение дел по защите ПДн в российской части информационно-телекоммуникационной сети Интернет? Прослеживается формальный подход по отношению к защите ПДн.

Возможно, если крупные хостинг-компании предложат организациям тарифные планы, включающие в себя реализацию требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», то это разрешит противоречия. Хостинг с выполнением требований по защите персональных данных.

Услуга будет включать в себя не только техническое решение, но и организационное обеспечение: хостинг-компания самостоятельно проходит сертификацию, проводит аттестацию системы, а клиентам предоставляет необходимые документы.

Этой услуге всего пару лет. Ей мало кто пользуется, и она слабо развита.

По мнению сайта «Хостинг в деталях» [13], на данный момент в России подобную услугу предлагают всего семь хостинг-компаний.

Предлагаются готовые комплексные решения для информационных систем 4–2-го класса, а также специальные услуги, включая аттестацию для ИСПДн, относящихся к 1-му классу. Услуга рассчитана как на компании из сегмента малого и среднего бизнеса, имеющие информационные системы, относящиеся к 4–2-м классам, так и на крупные компании, которым логичнее будет вынести систему на аутсорсинг, чем обеспечивать выполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» своими силами.

Таким образом, для заказчика процедура приведения информационной системы в соответствие с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» упрощается, так как значительную часть работ берет на себя хостинг-компания. Перечень мероприятий по исполнению соответствующих требований включает в себя реализацию технических мер, а также решение правовых и организационных вопросов. С технической стороны клиентам предоставляют хостинговую инфраструктуру, соответствующую техническим требованиям Федерального закона, а также оказывает услуги по администрированию системы, обеспечению уровня безопасности системы и сохранности персональных данных. Известно, что требования, предъявляемые ФСТЭК к условиям эксплуатации ИСПДн, существенно отличаются в зависимости от класса системы:

– для ИСПДн 4–2-го классов использует, в основном, ту же физическую, аппаратную и программную инфраструктуру, что и для оказания услуг «обычного» хостинга; отличия заключаются в «усиленных» настройках подсистем информационной безопасности, а также в комплексе проводимых мероприятий и обязательств, которые берутся перед заказчиком, что фиксируется в расширенных, по сравнению с обычными, документах – соглашении об уровне сервиса (SLA) и соглашении о конфиденциальности (NDA);

– для ИСПДн 1-го класса действуют намного более серьезные требования, для удовлетворения которых используется сертифицированное программное обеспечение, специальные средства защиты, шифрования и т.д.; физически ИСПДн 1-го класса эксплуатируются в выделенных сегментах сети, на выделенном оборудовании; можно сказать, что предоставление хостинга ИСПДн 1-го класса при размещении на хостинге – это индивидуальный проект, включающий все этапы от аудита до аттестации.

Сейчас они готовы предложить «типовые решения» для хостинга ИСПДн 4–2-го классов.

Со временем популярность услуги среди клиентов будет расти, и хостинг-компаниями по мере накопления практического опыта в дальнейшем будут предложены типовые решения для систем 1-го класса, что позволит ускорить, упростить и удешевить процесс их аттестации при хостинге.

На страницах корпоративного блога сотрудников группы компаний «Эшелон», весьма авторитетных в области информационной безопасности, высказаны сомнения в реализуемости полноценного оказания подобной услуги и приведен такой пример (описан далее).

В личном кабинете интернет-сайта некой организации обрабатываются ПДн 1-й категории, т.е. ПДн, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, включая сведения о его здоровье. Объем персональных данных более 100 000, угрозы 1-го и 2-го типа в соответствии с моделью угроз и нарушителя признаны неактуальными. То есть мы получаем рас-

пределенную ИСПДн, состоящую из двух сегментов: офиса компании заказчика и площадки организации, предоставляющей услуги хостинга для рассматриваемого сайта. В соответствии с Постановлением Правительства № 1119 уровень защищенности ИСПДн – 2.

Чтобы выполнить все требования Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и подзаконных актов, для данного проекта было проведено небольшое исследование рынка хостинг-центров и найдена интересная, на первый взгляд, услуга: «Хостинг конфиденциальной информации».

Приводится описание услуги: «Услуга "Хостинг конфиденциальной информации" предоставляется на базе виртуального хостинга и подойдет для хранения баз данных небольших компаний, таких как интернет-магазины или предприятия бытового обслуживания.

Особенности услуги.

1. Защищенный хостинг на оборудовании, имеющем сертификат связи. При построении инфраструктуры используются серверы и телекоммуникационное оборудование ведущих мировых производителей, таких как IBM и Cisco Systems.

2. Используется аппаратно-программный комплекс шифрования "Континент 3.5", сертифицированный ФСТЭК как средство защиты от несанкционированного доступа к информации.

3. Используется сертифицированное антивирусное ПО (Антивирус Касперского 8.0 для Linux File Servers).

4. Оборудование расположено в специализированном хорошо охраняемом помещении, оборудованном системами контроля доступа и видеорегистрации.

5. Ежедневно создаются две резервные копии данных в соответствии с требованиями к ИСПДн.

6. Для каждого проекта используется отдельная база данных.

7. Ведется строгий учет носителей информации.

Наша инфраструктура позволяет построить именно ту ИСПДн, которая необходима вашему клиенту».

Создается впечатление, что вот оно – решение проблем для всех интернет-магазинов и иных сайтов с личными кабинетами!

Детальное исследование рассмотренных в предложении услуг хостинга конфиденциальной информации позволяет выполнить только ряд требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и подзаконных актов в области защиты ПДн.

Например, «веб-сервер и MySQL-сервер запущены на разных физических серверах, но на каждом из этих серверов хранятся данные многих клиентов компании». То есть на одном физическом сервере могут храниться базы данных разных клиентов, с разным уровнем конфиденциальности информации, между собой эти базы данных не отделены межсетевыми экранами. Наличие сертифицированных средств защиты и действующих сертификатов соответствия – под вопросом.

В итоге для заказчиков, которые хотят полностью и грамотно выполнить все требования по защите ПДн и не иметь никаких проблем с Роскомнадзором, указанная в примере услуга, к сожалению, не подходит. Для полноценного оказания услуги «Хостинг конфиденциальной информации» необходимо предоставлять для каждого сайта, обрабатывающего ПДн, физически выделенный сервер или использовать сертифицированные средства защиты виртуальной инфраструктуры для выделенных виртуальных серверов.

Важно грамотно обеспечить защиту ПДн при размещении сегмента ИСПДн на территории хостинг-центров [14].

В процессе данного исследования были изучены и проанализированы различные способы обеспечения безопасности в области обработки персональных данных, вы-

работаны рекомендации по соответствию требованиям безопасности. Также большое внимание уделялось анализу существующих нормативно-методических документов, а именно требований и рекомендаций по защите информации. В действующей редакции основное направление по обеспечению безопасности информации – это физическая и информационная инфраструктура объекта информатизации. В результате данные, оказавшись вне защищаемых ресурсов, не могут быть в безопасности.

Обеспечение безопасности объектов информатизации очень ресурсозатратный процесс, но крайне необходимый. Организационные меры обеспечивают дешевый способ предотвращения угроз, однако они влияют на работу, что не представляется удачным решением при проектировании обеспечения безопасности.

В ходе проведенного исследования установлено, что построение комплексной системы защиты необходимо реализовывать на всех участках обработки, хранения и передачи информации. Однако предложенные меры не были проверены на практике, что означает необходимость дальнейших исследований в области повышения уровня безопасности информации ограниченного доступа при необходимости ее передачи по незащищенным каналам связи.

Литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

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

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. 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».

5. *Рудакова Т.А.* Документооборот и информационные риски субъектов хозяйствования // NovaInfo.Ru. 2015. Т. 1. № 36. С. 72–75.

6. Cloud Infrastructure Services. URL: https://www.srgresearch.com/research/cloud-infrastructure-services

7. Discovery Research Group. URL: http://www.discoveryresearchgroup.com/

8. СЭД (рынок России). URL: http://www.tadviser.ru/index.php

9. *Мищенко В.И., Шилов А.К.* Управление рисками информационной безопасности в автоматизированных системах управления // Информационные системы и технологии. 2015. № 2 (88). С. 138–142.

10. *Anastasov I., Davcev D.* SIEM implementation for global and distributed environments // 2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014.

11. http://pd.rkn.gov.ru/press-service/news4285.htm

12. http://regforum.ru/posts/1913_a_vasha_organizaciya__operator_personalnyh_dannyh/

13. http://hosting101.ru/catalog/152-fz

14. https://s3r.ru/2013/10/zakonodatelstvo/zametka-1-hosting-konfidentsialnoy-informatsii-panatseya-ot-152-fz-ili-dengi-na-veter/

References

1. Federal’nyy zakon ot 27 iyulya 2006 g. № 149-FZ “Ob informatsii, informatsionnykh tekhnologiyakh i zashchite informatsii”.

2. Federal’nyy zakon ot 27 iyulya 2006 g. № 152-FZ “O personal’nykh dannykh”.
3. Postanovlenie Pravitel’stva RF ot 01.11.2012 № 1119 “Ob utverzhdenii trebovaniy k zashchite personal’nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal’nykh dannykh”.
4. Prikaz FSTEK Rossii ot 18 fevralya 2013 g. № 21 “Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal’nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal’nykh dannykh”.
5. *Rudakova T.A.* Dokumentooborot i informatsionnye riski sub”ektov khozyaystvovaniya // NovaInfo.Ru. 2015. T. 1. № 36. S. 72–75.
6. Cloud Infrastructure Services. URL: https://www.srgresearch.com/research/cloud-infrastructure-services
7. Discovery Research Group. URL: http://www.discoveryresearchgroup.com/
8. SED (rynok Rossii). URL: http://www.tadviser.ru/index.php
9. *Mishchenko V.I., Shilov A.K.* Upravlenie riskami informatsionnoy bezopasnosti v avtomatizirovannykh sistemakh upravleniya // Informatsionnye sistemy i tekhnologii. 2015. № 2 (88). S. 138–142.
10. *Anastasov I., Davcev D.* SIEM implementation for global and distributed environments // 2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014.
11. http://pd.rkn.gov.ru/press-service/news4285.htm
12. http://regforum.ru/posts/1913_a_vasha_organizaciya__operator_personalnyh_dannyh/
13. http://hosting101.ru/catalog/152-fz
14. https://s3r.ru/2013/10/zakonodatelstvo/zametka-1-hosting-konfidentsialnoy-informatsii-panatseya-ot-152-fz-ili-dengi-na-veter/