27 июля 2006 г. был принят Федеральный Закон № 152-ФЗ «О персональных данных» для обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Одной из причин принятия данного закона послужили многочисленные факты краж баз персональных данных в государственных и коммерческих структурах, их повсеместная продажа.

Что означает термин «персональные данные»?

Определение персональных данных (ПДн) встречалось и до принятия закона, например, в «Перечне сведений конфиденциального характера», утвержденном *указом Президента РФ № 188* от 6 марта 1997 г.:

К конфиденциальной информации относятся: сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Однако закон дополнил его. Теперь, согласно *ФЗ-152*, персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Таким образом, персональные данные — это, прежде всего, паспортные данные, сведения о семейном положении, сведения об образовании, номера ИНН, страхового свидетельства государственного пенсионного страхования, медицинской страховки, сведения о трудовой деятельности, социальное и имущественное положение, сведения о доходах. Такие данные есть практически в каждой организации.

При поступлении на работу — это данные отдела кадров работодателя, которые работник указывает в личной карточке, автобиографии, других документах, заполняемых при заключении трудового договора.

При поступлении ребенка в детский сад, школу, институт, другие образовательные учреждения также заполняется множество анкет и форм, в которых указываются данные как ребенка (например, данные свидетельства о рождении), так и его родителей (вплоть до места работы, занимаемой должности).

При прохождении лечения в медицинских учреждениях необходимо указать не только паспортные данные, но и сведения о льготах, медицинских страховках, сведения о предыдущих лечениях, результаты анализов. Во многих медицинских учреждениях амбулаторные/стационарные карты дублируются в электронном виде.

И все эти данные, согласно нынешнему законодательству, подлежат

защите. С чего начать защиту, и нужна ли она вообще?

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания (*ФЗ-152*).

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и(или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (*ФЗ-152*).

Информационная система персональных данных (ИСПДн) — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств (*ФЗ-152*).

Обработка персональных данных — это действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,

распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (*ФЗ-152*).

Оператор при обработке ПДн должен принимать все необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Что же необходимо сделать, чтобы защитить персональные данные?

Прежде всего, необходимо определить, какие информационные системы ПДн есть и какого типа ПДн в них обрабатываются.

Классификация информационной системы персональных данных

Для того чтобы понять, насколько проблема защиты ПДн существенна, а также для выбора необходимых методов и способов защиты ПДн, оператору нужно провести классификацию ИСПДн. Порядок классификации определен *приказом ФСТЭК России, ФСБ России и Мининформсвязи России № 55/86/20 от 13 февраля 2008 г*.

Итак, оператор формирует комиссию (приказом руководителя организации), которая после анализа исходных данных принимает решение о присвоении ИСПДн соответствующего класса. В ходе классификации определяются:

- категория обрабатываемых персональных данных;
- объем обрабатываемых персональных данных;
- тип информационной системы;
- структура информационной системы и местоположение ее технических средств;
- режимы обработки персональных данных;
- режимы разграничения прав доступа пользователей;
- наличие подключений к сетям общего пользования и (или) сетям международного информационного обмена.

Согласно *приказу № 55/86/20*, все информационные системы (ИС) делятся на типовые и специальные.

Типовые информационные системы — информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы — информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

На практике выходит, что типовых ИС практически нет, поскольку в большинстве случаев помимо конфиденциальности необходимо обеспечить также целостность и доступность информации. Кроме того, в обязательном порядке к специальным системам должны быть отнесены:

- информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;
- информационные системы, в которых предусмотрено 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.

Итак, по результатам анализа исходных данных комиссия присваивает системе персональных данных соответствующий класс:

класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Результаты классификации оформляются Актом классификации ИСПДн, в котором указываются тип ИСПДн (типовая, специальная), присвоенный ИСПДн класс и условия, на основании которых было принято решение.

Как уже было сказано, классификация необходима для дальнейшего выбора методов и средств защиты ПДн, обрабатываемых в ИСПДн, поскольку в документах ФСТЭК и ФСБ каждому классу устанавливаются свои требования по защите ИСПДн.

Согласие субъекта ПДн на обработку

Далее необходимо перейти к обработке этих данных, но перед тем, как их обработка будет законной, необходимо получить согласие субъекта персональных данных на обработку (закон тем самым предотвращает незаконный сбор и использование персональных данных):

Статья 6 ФЗ-152:

Обработка персональных данных может осуществляться оператором с согласия субъектов ПДн, за исключением случаев:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Итак, если наш случай обработки ПДн предусмотрен частью 2 статьи 6 ФЗ-152, то получение согласия необязательно.

Также необходимо руководствоваться *Трудовым Кодексом, Глава 14*. Например, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия (*Статья 86 часть 4 ТК*).

В соответствии со *статьей 9 ФЗ-152* получать согласие субъекта персональных данных на обработку его персональных данных необходимо в письменной форме. Письменное согласие субъекта персональных данных должно включать:

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

– наименование (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;

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

– срок, в течение которого действует согласие, а также порядок его отзыва.

Положение, регламентирующее порядок обработки и защиты ПДн

Итак, оператор получил (если это необходимо) согласие на обработку персональных данных — персональные данные можно обрабатывать. Но, согласно *Трудовому кодексу* и *ФЗ-152* необходимо разработать (если есть, доработать в соответствии с ФЗ) положение, регламентирующее порядок хранения, обработки и защиты персональных данных. Давайте условно назовем его Положение по обеспечению безопасности персональных данных. Положение по обеспечению безопасности персональных данных — это внутренний (локальный) документ организации. Строгой формы данного документа нет, но он должен удовлетворять требованиям *ТК* и *ФЗ-152,* а, следовательно, в нем должно быть указано:

– цель и задачи в области защиты персональных данных;

– понятие и состав персональных данных;

– в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные;

– как происходит сбор и хранение персональных данных;

– как они обрабатываются и используются;

– кто (по должностям) в пределах фирмы имеет к ним доступ;

– принципы защиты ПДн, в том числе от несанкционированного доступа;

– права работника в целях обеспечения защиты своих персональных данных;

– ответственность за разглашение конфиденциальной информации, связанной с персональными данными работников.

Положение по обеспечению безопасности персональных данных утверждается руководителем организации или уполномоченным им лицом, вводится в действие приказом руководителя. Работодатель обязан ознакомить работника с Положением под подпись.

Список лиц, допущенных к обработке ПДн

Кроме того, необходимо оформить список лиц, допущенных к обработке ПДн, т.е. перечень тех (по должностям), кому доступ к ПДн необходим для выполнения служебных обязанностей. В первую очередь это сотрудники кадровой службы, поскольку они собирают и формируют данные о работнике, а также сотрудники бухгалтерии. Помимо того, доступ к этим сведениям могут получить руководители структурных подразделений (например, начальники отделов) — и это также необходимо отразить в списке. Однако все они вправе запрашивать не любые данные, а только те, которые необходимы для выполнения конкретных трудовых функций (например, чтобы рассчитать льготы по налогам, бухгалтерия получит не все сведения о работнике, а только данные о количестве его иждивенцев). Поэтому целесообразно прописать перечень информационных ресурсов, к которым пользователи допущены.

Список лиц, допущенных к обработке ПДн можно оформить в виде приложения к Положению по обеспечению безопасности персональных данных или отдельным документом, утвержденным руководителем.

Уведомление Роскомнадзора

Далее в соответствии со *статьей 22 ФЗ-152* оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов ПДн (на сегодняшний день это — Федеральная служба по надзору в сфере связи, информационных технологий и

массовых коммуникаций (Роскомнадзор)) о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных *частью 2 статьи 22 ФЗ-152*:

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

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) 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;

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

4) являющихся общедоступными персональными данными;

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

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

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

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

Требования к уведомлению указаны в *части 3 статьи 22 ФЗ-152*. Форму уведомления об обработке (о намерении осуществлять обработку) персональных данных можно заполнить в электронном виде на сайте Роскомнадзора: https://pd.rkn.gov.ru/operators-registry/notification/form/

Теперь можно приступать к обработке персональных данных, параллельно решая самый сложный и проблемный вопрос — обеспечение безопасности персональных данных при их обработке.

Обеспечение безопасности персональных данных при их обработке

Мероприятия по защите информации трудоемки и могут привести к значительным финансовым затратам, что обусловлено необходимостью:

– получать (по необходимости) лицензию на деятельность по технической защите конфиденциальной информации ФСТЭК России;

– привлекать лицензиата ФСТЭК России для осуществления мероприятий по созданию системы защиты ИСПДн и/или ее аттестации по требованиям безопасности информации;

– отправлять сотрудников, ответственных за обеспечение безопасности информации, на курсы повышения квалификации по вопросам защиты информации и/или нанимать специалистов по защите информации;

– устанавливать сертифицированные по требованиям ФСТЭК средства защиты информации (СрЗИ), сертифицированные ФСБ средства криптографической защиты информации (СКЗИ) в зависимости от класса ИСПДн.

Что-то можно сделать самим, а где-то лучше довериться специалистам. Но защитить персональные данные необходимо, так или иначе.

Статья 19, ФЗ-152:

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или

случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Помимо *ФЗ-152* требования и рекомендации по обеспечению защиты персональных данных устанавливают:

- «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено постановлением Правительства РФ № 781 от 17 ноябрям2007 г.
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено постановлением Правительства РФ № 687 от 15 сентября 2008 г.
- «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утверждены постановлением Правительства РФ № 512 от 6 июля 2008 г.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом Гостехкомиссии России № 282 от 30 августа 2002 г. (ДСП)

Лицензия — получать или не получать?

Законодательство, а также документы ФСТЭК говорят нам следующее:

Статья 16, часть 6 ФЗ-149 «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.:

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17, часть 1, п.11 ФЗ-128 «О лицензировании отдельных видов деятельности» от 8 августа 2001 г.:

В соответствии с настоящим Федеральным законом лицензированию подлежат следующие виды деятельности: деятельность по технической защите конфиденциальной информации.

Постановление Правительства РФ № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» от 15 августа 2006 г.

Под технической защитой конфиденциальной информации понимается комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Основные мероприятия

ФСТЭК Пункт 3.14

В соответствии с положениями Федерального закона № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1, 2 и 3 (распределенные системы) классов должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке.

Так же на вопрос о необходимости лицензии отвечал начальник отдела Управления ФСТЭК России НАЗАРОВ Игорь Григорьевич на круглом столе, проведенном журналом «Connect! Мир связи» (http://www.connect.ru/article.asp?id=9406):

Вопрос: Нужно ли операторам, обрабатывающим персональные данные в ИСПДн, получение лицензии на техническую защиту конфиденциальной информации?

Игорь Назаров: В соответствии с документами ФСТЭК лицензия необходима операторам ПДн, которые самостоятельно проводят такие мероприятия по информационным системам 1, 2 класса и территориально распределенным системам 3 класса, как правило, это большие

государственные информационные системы. При этом для поликлиник, детских садов, аптек и т.п., имеющих ИСПДн 3 и 4 классов, получение таких лицензий не требуется.

В соответствии с постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, если оператор ИСПДн заключает договор на проведение соответствующих мероприятий в части защиты информации (ПДн) с уполномоченным лицом — лицензиатом ФСТЭК России, иметь лицензию ему не обязательно.

Итак, для небольших организаций более экономически-выгодным вместо получения лицензии ФСТЭК по ТЗКИ для проведения мероприятий по обеспечению безопасности ПДн (создание системы защиты ИСПДн, аттестация) будет привлечение лицензиата ФСТЭК, который проведет все необходимые работы.

Для крупных организаций (таких как операторы связи, крупные банки и т.п.) — выгоднее самим получить лицензию и выполнить все необходимые работы.

Порядок предоставления лицензии на осуществление деятельности по технической защите конфиденциальной информации определен *«Положением о лицензировании деятельности по технической защите конфиденциальной информации»* (утверждено постановлением Правительства РФ от 15 августа 2006 г. № 504). Требования для получения лицензии:

а) наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;

б) наличие у соискателя лицензии (лицензиата) помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;

в) наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;

г) использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;

д) использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;

е) наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю.

Этапы создания СЗПДн

Согласно *Основным мероприятиям* по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, выпущенными ФСТЭК, создание системы защиты персональных данных (СЗПДн) состоит из следующих этапов:

1 Предпроектная стадия

1.1 обследование объекта информатизации:

- установление необходимости обработки ПДн в ИСПДн;
- определение перечня ПДн, подлежащих защите;
- определение условий расположения ИСПДн относительно границ контролируемой зоны (КЗ);
- определение конфигурации и топологии ИСПДн в целом и ее отдельных компонентов; физических, функциональных и технологических связей как внутри ИСПДн, так и с другими системами различного уровня и назначения;

- определение технических средств и систем, используемых в защищаемой ИСПДн, условий их расположения;
- определение общесистемных, специальных и прикладных программных средств, используемых в защищаемой ИСПДн;
- определение режима обработки информации в ИСПДн в целом и в отдельных компонентах;
- проведение классификации ИСПДн;
- определение степени участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой;
- определение и составление перечня уязвимостей и угроз безопасности информации, оценка актуальности угроз безопасности информации;
- разработка частной модели угроз.

1.2 разработка технического задания на создание СЗПДн, которое должно содержать:

- обоснование необходимости разработки СЗПДн;
- исходные данные ИСПДн в техническом, программном, информационном и организационном аспектах;
- класс ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

2. Стадия проектирования и реализации СЗПДн

2.1 разработка проекта на создание СЗПДн;

2.2 разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;

2.3 закупка сертифицированных средств защиты информации;

2.4 разработка и реализация разрешительной системы доступа пользователей и персонала к обрабатываемой в ИСПДн информации;

2.5 установка и настройка СрЗИ;

2.6 определение подразделений и лиц, ответственных за эксплуатацию средств защиты информации, обучение назначенных лиц специфике работ по защите ПДн;

2.7 разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации (положений, приказов, инструкций и других документов);

2.8 выполнение других мероприятий, направленных на защиту информации.

3. Стадия ввода в действие СЗПДн

3.1 опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

3.2 приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта;

3.3 оценка соответствия ИСПДн требованиям безопасности информации — аттестация (декларирование) по требованиям безопасности информации.

4. Техническое обслуживание и сопровождение системы защиты информации

Организационно-распорядительная документация по защите ПДн Помимо технических решений создаваемой системы защиты персональных данных,

оператор должен обеспечить разработку организационно-распорядительных документов, которые будут регулировать все возникающие вопросы по обеспечению безопасности ПДн при их обработке в ИСПДн и эксплуатации СЗПДн. Таких документов достаточно много, основные из них:

1. Положение по обеспечению безопасности ПДн — в начале статьи мы уже касались назначения и состава этого документа. На всякий случай повторим — в нем должно быть указано:

– цель и задачи в области защиты персональных данных;

– понятие и состав персональных данных;

– в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные;

– как происходит сбор и хранение персональных данных;

– как они обрабатываются и используются;

– кто (по должностям) в пределах фирмы имеет к ним доступ;

– принципы защиты ПДн, в том числе от несанкционированного доступа;

– права работника в целях обеспечения защиты своих персональных данных;

– ответственность за разглашение конфиденциальной информации, связанной с персональными данными работников.

2. Для организации системы допуска и учета лиц, допущенных к работе с ПДн в ИСПДн, — Список лиц, допущенных к обработке ПДн (перечень по должностям тех, кому доступ к ПДн необходим для выполнения служебных обязанностей) и Матрица доступа (должна отражать полномочия пользователей по выполнению конкретных действий в отношении конкретных информационных ресурсов ИСПДн — чтение, запись, корректировка, удаление). Оба документа утверждаются руководителем.

3. Частная модель угроз (если ИСПДн несколько, то модель угроз разрабатывается на каждую из них) — разрабатывается по результатам предварительного обследования. ФСТЭК России предлагает *Базовую модель* угроз безопасности персональных данных при их обработке в информационных системах персональных данных, согласно которой при создании частной модели должны быть рассмотрены:

– угрозы утечки информации по техническим каналам;

– угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к ИСПДн, реализующих угрозы непосредственно в ИСПДн. При этом необходимо в качестве потенциальных нарушителей рассматривать легальных пользователей ИСПДн;

– угрозы несанкционированного доступа, связанные с действиями нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Разработанная модель угроз утверждается руководителем.

4. На основании утвержденной модели угроз ИСПДн необходимо разработать требования по обеспечению безопасности ПДн при их обработке в ИСПДн. Требования, как и модель угроз, — это самостоятельный документ, который должен быть утвержден руководителем организации.

Для разработки модели угроз и требований оператору целесообразно привлекать специалистов организаций-лицензиатов ФСТЭК.

5. Инструкции в части обеспечения безопасности ПДн при их обработке в ИСПДн.

6. Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

Кроме того, до проведения всех мероприятий по защите ПДн оператор должен назначить должностное лицо или (если ИСПДн достаточно велика) структурное подразделение, ответственные за обеспечение безопасности ПДн. Решение о назначении оформляется приказом руководителя. Задачи, функции и полномочия должностного лица (подразделения), ответственного за обеспечение безопасности ПДн, определяются внутренними организационно-распорядительными документами (должностными инструкциями, регламентами).

Что обязательно сертифицировать, а что нет?

Часто возникает заблуждение, что все используемое программное обеспечение (ПО), должно быть сертифицировано, а сертификация стоит дорого и занимает много времени.

Однако ни в одном из документов по регулированию вопросов защиты ПДн не сказано, что должно быть сертифицировано все ПО. Сертифицированы по требованиям ФСТЭК России должны быть средства защиты информации, но никак не системное, прикладное или специальное ПО, не участвующее в защите ИСПДн.

Игорь Назаров: …сертификация по контролю отсутствия НДВ касается функционала безопасности, именно средств защиты, а не всего программного обеспечения, которое используется в информационной системе (http://www.connect.ru/article.asp?id=9406).

Сегодня документы ФСТЭК, которые можно посмотреть на сайте Федеральной службы по техническому и экспортному контролю, говорят нам по этому поводу следующее:

Рекомендации…

В ИСПДн должны использоваться только сертифицированные по требованиям безопасности информации технические средства и системы защиты.

Основные мероприятия…

Пункт 4.2: …в ИСПДн должен проводиться контроль на наличие недекларированных возможностей в программном и программно-аппаратном обеспечении и анализ защищенности системного и прикладного программного обеспечения.

Пункт 4.3: Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации, в том числе и встроенных в общесистемное и прикладное программное обеспечение), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ.

Таким образом, сертифицировать системное и прикладное ПО, если оно не участвует в процессе защиты информации, не нужно — это можно делать по желанию оператора.

Практика создания систем защиты ПДн показывает, что необходимо использовать лицензионное программное обеспечение (системное, прикладное и специальное ПО) и сертифицированные средства защиты информации и антивирусной защиты (это могут быть СрЗИ от НСД, антивирусные продукты, межсетевые экраны, средства обнаружения вторжений, средства анализа защищенности, соответствующие определенному классу). Если в ИСПДн устанавливаются криптографические средства защиты информации (СКЗИ), то они также должны быть сертифицированы по требованиям ФСБ России.

Следует отметить, что устанавливать сертифицированные СрЗИ имеет право только лицензиат ФСТЭК, а СКЗИ — лицензиат ФСБ.

Аттестация

Финальным этапом создания системы защиты ИСПДн должна стать аттестация (декларирование соответствия) — комплекс организационно-технических мероприятий, в результате которых посредством специального документа — Аттестата соответствия (Заключения) подтверждается, что ИСПДн соответствует требованиям стандартов или иных нормативно-методических документов по безопасности информации. Наличие действующего Аттестата соответствия дает право обработки информации с соответствующим уровнем конфиденциальности на период времени, установленный в Аттестате соответствия.

Вопрос: Кто может аттестовать рабочие места на соответствие требованиям законодательства и нормативных документов в области персональных данных?

Игорь Назаров: Аттестацию ИСПДн на соответствие требованиям по безопасности информации имеют право проводить лицензиаты ФСТЭК, которые имеют лицензию на деятельностьпотехническойзащитеконфиденциальнойинформации (http://www.connect.ru/article.asp?id=9406).

Аттестация предусматривает комплексную проверку (аттестационные испытания) ИСПДн в реальных условиях эксплуатации с целью оценки соответствия принятого комплекса мер защиты требуемому уровню безопасности ПДн.

В общем виде аттестация ИСПДн по требованиям безопасности информации включает в себя следующие этапы:

– анализ исходных данных по аттестуемой ИСПДн;

– проведение экспертного обследования ИСПДн и анализ разработанной документации по обеспечению безопасности ПДн на соответствие требованиям нормативных и методических документов;

– проведение комплексных аттестационных испытаний ИСПДн в реальных условиях эксплуатации с использованием специальной аппаратуры контроля и программных средств контроля защищенности от несанкционированного доступа;

– анализ результатов комплексных аттестационных испытаний, оформление и утверждение Заключения и Аттестата соответствия по результатам аттестации.

Важным моментом является то, что в случае изменения условий и технологии обработки ПДн оператор обязан известить об этом организацию-лицензиата, проводившую аттестацию ИСПДн. После чего организация-лицензиат принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты ИСПДн.

Ответственность и риски за неисполнение требований закона

При неисполнении требований по обеспечению безопасности ПДн у оператора могут возникнуть риски гражданско-правовых исков со стороны клиентов или работников.

Что в свою очередь может повлиять на репутацию компании, а также привести к принудительному приостановлению (прекращению) обработки ПДн, привлечению компании и (или) ее руководителя к административной или иным видам ответственности, а при определенных условиях — к приостановлению действия или аннулированию лицензий. Кроме того, согласно ФЗ, лица, виновные в нарушении требований, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность (*статья 24 ФЗ-152*):

Дисциплинарная (Трудовой кодекс Российской Федерации, статьи 81, 90, 195, 237, 391);

Административная (Кодекс Российской Федерации об административных правонарушениях, статьи 5.27, 5.39, 13.11–13.14, 13.19, 19.4–19.7, 19.20, 20.25, 32.2);

Уголовная (Уголовный кодекс Российской Федерации, статьи 137, 140, 155, 171, 183, 272, 273, 274, 292, 293).

Государственная политика в области защиты персональных данных регламентируется следующими нормативными актами:

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

Федеральный закон от 21 июля 2014 г. N 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях;

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

Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

Федеральный закон № 353-ФЗ «О потребительском кредите (займе)»;

Правовыми основаниями для обработки ПД являются Трудовой кодекс РФ, Налоговый кодекс РФ.

Статья 1

Статья 1 Федерального закона № 242-ФЗ дополнила Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) новой статьёй 15.5 «Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных».

Нумерация вводимой статьи в контексте правовой конструкции Федерального закона № 149-ФЗ указывает на установление законодателем особого порядка ограничения доступа к информации, содержащей персональные данные.

Выделение вопроса ограничения доступа к персональным данным в отдельный порядок обусловлено, прежде всего, тем, что иные режимы ограничения, предусмотренные Федеральным

законом № 149-ФЗ, связаны с информацией, распространение которой на территории Российской Федерации прямо запрещено законодательством Российской Федерации.

Распространение же персональных данных профильным законом не запрещено, но должно осуществляться в соответствии с требованием конфиденциальности, установленным статьей 7 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее-Федеральный закон №152-ФЗ).

Нет смысла в данном комментарии подробно описывать порядок ограничения доступа к персональным данным, поскольку он концептуально не отличается от аналогичных порядков блокировки, установленных статьями 15.1-15.4 Федерального закона № 149-ФЗ.

При этом следует выделить следующие его особенности.

В соответствии с частью 1 комментируемой статьи создана автоматизированная информационная система «Реестр нарушителей прав субъектов персональных данных» (далее-Реестр нарушителей), целью которой является ограничение доступа к информации в сети «Интернет», обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных.

Основанием для внесения в Реестр нарушителей доменного имени, URL-адреса интернет-страницы, законодателем установлено вступившее в законную силу решение суда о признании деятельности по распространению информации, содержащей персональные данные, нарушающей требования Федерального закона №152-ФЗ, а также права субъекта персональных данных на неприкосновенность частной жизни, личную и семейную тайну.

Основанием для запуска процедуры ограничения доступа к Интернет-ресурсу может стать не только сбор персональных данных, осуществляемый с нарушением статьи 2 комментируемого закона, но и обработка персональных данных субъектов персональных данных в отсутствие правовых оснований: согласие субъекта персональных данных на обработку его персональных данных, отсутствие законодательно возложенных на оператора функций, полномочий и обязанностей, предусматривающих распространение персональных данных в сети Интернет, предоставление доступа неограниченному кругу лиц к общедоступным персональным данным в целях и объеме, отличных от цели и объема их первоначального сбора.

В силу имеющихся отдельных прецедентов следует отдельно остановиться на вопросе распространения в сети Интернет персональных данных, содержащихся в архивных документах.

Норма ч. 2 ст. 1 Федерального закона № 152-ФЗ содержит исключительные виды обработки документов Архивного фонда Российской Федерации и других архивных документов, содержащих персональные данные, а именно: хранение, комплектование, учет и использование персональных данных, на которые Федеральный закон № 152-ФЗ не распространяется.

В указанном перечне видов обработки персональных данных отсутствует такой вид обработки как «распространение». На основании п. 5 ст. 3 Федерального закона № 152-ФЗ действия, направленные на раскрытие персональных данных неопределенному кругу лиц, определяются как распространение персональных данных. Таким образом, на деятельность, связанную с распространением, в том числе в сети Интернет, архивных документов, содержащих персональные данные, действие Федерального закона № 152-ФЗ распространяется в полной мере.

1.Так, частью 1 комментируемой статьи законодателем внесены изменения в статью 18 «Обязанности оператора при сборе персональных данных» Федерального закона №152-ФЗ, согласно которым для оператора персональных данных установлена совершенно новая обязанность осуществлять при сборе персональных данных определенные виды обработки персональных данных в базах данных, которые находятся на территории России.

Комментируемая норма содержит четкий закрытый перечень видов обработки персональных данных, а именно: запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, которые оператор

обязан осуществлять с использованием баз данных, находящихся на территории Российской Федерации.

При определении понятия «база данных» следует учитывать, что в законодательстве Российской Федерации существует много понятий баз данных, тем не менее, все они сводятся к одному общему значению, согласно которому база данных - это упорядоченный массив данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных). Так, например, базой данных можно считать таблицу в формате Excel, word, в которой содержатся персональные данные граждан.

При этом единственным законным признаком, которым должна обладать база данных, является ее место нахождения – территория Российской Федерации.

Долгое время существовал спор можно ли считать предметом регулирования комментируемого закона базу данных, сформированную на бумажных носителях, при последующем внесении указанных сведений в информационную систему персональных данных.

Существующая позиция основывается на принципе, согласно которому обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. В связи с этим внесение персональных данных в информационную систему персональных данных, используемую в целях, аналогичных сбору данных на бумажных носителях, следует рассматривать как единый процесс, реализация которого должна осуществляться в строгом соответствии с требованиями части 5 статьи 18 Федерального закона №152-ФЗ. Разделение указанного единого процесса на отдельные действия законодательством Российской Федерации в области персональных данных не предусмотрено. Таким образом, отдельные виды обработки персональных данных, предусмотренные частью 5 статьи 18 Федерального закона №152-ФЗ, в том числе сбор персональных данных на бумажных носителях с последующим их внесением в электронную базу данных, должны осуществляться как единый процесс в правовом поле законодательной нормы, обязывающей хранить персональные данные на территории Российской Федерации.

Понятие «оператор» содержится в статье 3 Федерального закона № 152-ФЗ, под которым понимается 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. Таким образом, в свете применения комментируемой нормы, оператором является лицо, осуществляющее сбор персональных данных, либо поручившее его третьему лицу на основании договора поручения.

В отношении отнесения той или иной информации к персональным данным следует руководствоваться п. 1 ст. 3 Федерального закона № 152-ФЗ, согласно которому персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Таким образом, отнесение указанного перечня информации к персональным данным возможно при условии соответствия данной информации положениям Федерального закона № 152-ФЗ.

Реализация обязанности «при сборе данных» означает, что оператор должен их получать непосредственно у первоисточника, то есть у субъекта персональных данных или его представителя. В таком случае речь идет о сборе информации, а не о случаях передачи данных третьему лицу для обработки в каких-либо целях.

Так, оператор, получив данные субъекта, обязан обеспечить их запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение с использованием баз данных, находящихся в России.

Указанные виды обработки данных представляют собой единый процесс формирования и поддержания базы данных в актуальном состоянии. Образно говоря, можно сказать, что законодатель вводит правило, согласно которому формирование и актуализация баз персональных данных российских граждан должны осуществляться на территории России.

Так, база данных, сформированная посредством сбора персональных данных, должна находиться на территории России и актуализироваться также на территории России.

Обращаем Ваше внимание на то, что в первом полугодии 2019 г. был произведен анализ сайтов общеобразовательных учреждений Республики Бурятия, в ходе, которого выявлены нарушения законодательства о персональных данных:

- отсутствие на сайте в свободном доступе политики в отношении обработки персональных данных;

- отсутствие возможности у посетителя сайта дать свое согласие на обработку персональных данных при направлении им обращений, вопросов, отзывов в адрес учреждения с использованием информационно-телекоммуникационных сетей.

В связи с чем Управление Роскомнадзора по Республике Бурятия требует привести в соответствие принадлежащие общеобразовательным учреждениям республики сайты до конца 2019 г.

Еще одна обязанность операторов – регистрация в Реестре операторов, осуществляющих обработку персональных данных, и что не мало важно - поддержание представленной информации в актуальном состоянии.

Вместе с тем, одним из типичных нарушений как раз является нарушение требований ч. 3 ст. 22 ФЗ «О персональных данных» - представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения.

Кроме того, в соответствии со ст. 19.7 КоАП РФ непредставление или несвоевременное представление в государственный орган, осуществляющий государственный контроль (надзор), сведений (информации), представление которых предусмотрено законом или представление таких сведений (информации) в неполном объеме или в искаженном виде влечет предупреждение или наложение административного штрафа.

Если в Вашей организации происходит какая-либо обработка персональных данных, то Вы однозначно являетесь Оператором персональных данных, даже если обработка подразумевает под собой просто хранение документов или Вы обрабатываете ПД только своих сотрудников (для начисления заработной платы или кадрового учета). Таким образом, Вам необходимо перед началом осуществления своей деятельности направить Уведомление о намерении обрабатывать персональные данные в Управление Роскомнадзора. Заполнить его Вы можете на сайте - Роскомнадзор по Республике Бурятия/электронные формы заявлений/заполнить форму информационного письма.

Либо, если Вы уже предприняли данные действия, однако в Вашем Уведомлении было недостаточно сведений, либо они были заполнены некорректно, Вам необходимо приступить к заполнению информационного письма на вышеуказанном сайте - Роскомнадзор по Республике Бурятия/электронные формы заявлений/заполнить форму информационного письма.

Целями обработки персональным данных является основание их обработки, если Вы обрабатываете ПД своих клиентов – Вы используете их для осуществления своей деятельности, если начисляете заработную плату и ведете кадровый учет – Вы делаете это для осуществления трудовых отношений (согласно действующему законодательству).

Средствами обработки являются предметы, с помощью которых в Вашей организации достигается безопасность и сохранность при обработке ПД (это может быть запираемый шкаф, сейф, сигнализация, кнопка охраны, пароли доступа на ПК и прочее).

Описание мер, предусмотренных ст. 18.1 и 19 (152 ФЗ), согласно которым необходимо назначить лицо, ответственное за организацию обработки персональных данных, создать нормативно-правовые внутренние локальные акты по обработке ПД.

Сведениями об обеспечении безопасности будет являться все действия, предпринятые Вашей организацией для обеспечения безопасности при автоматизированной и неавтоматизированной обработке персональных данных (включая ознакомление работников с нормативными актами, необходимыми при обработке персональных данных).

Ответственным лицом за организацию обработки персональных данных необходимо назначить работника, который будет обеспечивать весь процесс работы с персональными

данными, включая подготовку нормативных внутренних актов, распределение работы с персональными данными, организацию их хранения.

Количество информационных систем зависит от каждой конкретной организации.

Адрес ЦОДа – фактический адрес центра обработки данных, где происходит их обработка. (Собственный ЦОД - да). Если же больницы направляют информацию в Министерство Здравоохранения, а школы в Министерство образования, это необходимо указывать в информационном письме как 2 адреса местонахождения базы данных, один из которых адрес организации, другой - адрес Министерства.

Перейдем к части проведения плановых и внеплановых проверок Управления Роскомнадзора и обеспечения Вашей подготовки к ним.

При проведении плановых проверок Управлением за 2 недели готовится приказ о проведении проверки и в Ваш адрес приходит уведомление.

Вся информация, указанная в Вашем Уведомлении о намерении осуществлять обработку должна соответствовать действительности.

Перечень документов, представление которых необходимо для достижения целей и задач при проведении плановой выездной проверки в сфере обработки персональных данных указывается в Приказе о проведении проверки, и его можно получить у сотрудников Управления.

По результатам проверки Управлением составляется справка и акт о результатах проверки.

В случае выявления нарушений выдается предписание об устранении выявленного нарушения, а также может быть составлен протокол об административном правонарушении, как в отношении юридического лица, так и должностного лица (ответственного за организацию обработки персональных данных).

Специалисты Управления всегда готовы провести консультацию по заполнению уведомлений и информационных писем, а также по вопросам проведения проверок.

Закон о «защите персональных данных» содержит в себе следующие требования.

Во-первых, каждый оператор должен придерживаться принципов обработки данных, а это значит, что необходимо:

- определить законное основание обработки персональных данных; конкретную и законную цель обработки; содержание и объем персональных данных, в соответствии с целью сбора персональных данных; срок хранения персональных данных;
- исключить избыточность персональных данных;
- обеспечить точность персональных данных, их достаточность, актуальность по отношению к целям обработки.

Во-вторых, определить условия обработки персональных данных, которые закреплены в ч. 1 ст. 6 ФЗ «О персональных данных». Т.е. оценить следующие обстоятельства: обработка персональных данных обусловлена требованиями закона, договора или есть необходимость получения согласия на обработку персональных данных. Определиться, при каком условии обработка персональных данных будет легитимной.

В-третьих, соблюдать конфиденциальность персональных данных, а именно не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Очевидно, что, нарушая режим конфиденциальности, оператор несет не только репутационные риски, но и может быть привлечен к ответственности.

Статьей 13.11 КоАП РФ предусмотрено несколько видов ответственности такие как:

- использование персональных данных в непредусмотренных законодательством целях;
- обработка личных сведений без согласия субъекта ПДн;
-нарушение режима доступа к политике организации по обработке ПДн;
- сокрытие от субъекта ПД информации о целях, сроках и способов сбора, хранения и обработки информации, о третьих лицах, которые будут работать с личными сведениями по поручению Оператора и т.д.;

-отказ оператора заблокировать или уничтожить ПД согласно ст.21 ФЗ-152 (неправомерная обработка, неточность, достижение цели, отзыв согласия субъектом, блокирование, в случае невозможности уничтожить в срок);

-отсутствие средств автоматизации для хранения ПДн, хранение только в бумажном виде. Если такой оператор допустил утечку, уничтожение, несанкционированное копирование или распространение ПДн;

- несоблюдение или нарушение процедуры обезличивания сотрудниками гос. и муниципальных органов.

Максимальный (суммированный) штраф, предусмотренный ст. 13.11. КоАП РФ в новой редакции с июля 2017 г. – 75000 рублей.

Кроме того, не стоит забывать про иные виды ответственности, предусмотренные российским законодательством, в том числе уголовную.

В-четвертых, оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Статьей 18.1 ФЗ «О персональных данных» установлено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Указанная статья содержит примерный перечень мер, который фактически является необходимым минимумом. С реализации следующих мер необходимо начать:

1) назначить лицо, ответственное за организацию обработки персональных данных;

2) разработать документы, определяющих политику оператора в отношении обработки персональных данных и другие локальные акты по вопросам обработки персональных данных;

3) применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 ФЗ «О персональных данных»;

4) осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценить вред, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;

6) ознакомить работников, 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, и (или) обучение указанных работников.

Немаловажен тот факт, что 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.

Обеспечить неограниченный доступ – значит не стеснять субъекта персональных данных таким обстоятельством, как, например – регистрация на сайте для ознакомления с данным документом.

Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать указанный документ в соответствующей информационно-телекоммуникационной сети, а также обеспечить возможность доступа к нему с использованием средств соответствующей информационно-телекоммуникационной сети.

Обработка персональных данных

Политика обработки ПД и локальные нормативные акты по вопросам обработки должны быть опубликованы. Политика и сведения о мерах по защите ПД размещаются на сайте, где ведётся обработка ПД, а также там могут быть размещены и пользовательское соглашение, и условия использования сервисов. Можно опубликовать общую политику на несколько сайтов, но внутри неё должна быть градация.

Для обработки персональных данных необходимо получить согласие субъекта ПД. В согласии должны быть указаны адрес или данные основного документа, удостоверяющего личность субъекта, наименование или ФИО и адрес оператора ПД, перечень ПД, на обработку которых дается согласие и способ отзыва согласия на обработку ПД. При составлении текста согласия можно использовать типовые формы на сайте РКН. Срок действия согласия может быть ограничен сроком или достижением цели.

Указание в согласии нескольких целей допустимо, в том числе на сбор файловой информации cookie (кроме биометрии, спецкатегории и трансграничной передачи на территорию неадекватных по защите ПД стран). На период принятия решения о трудоустройстве нужно получать согласие на обработку ПД от соискателя и его близких родственников, если требуется информация о них. При действии субъектов ПД в интересах третьих лиц нужно их согласие, доверенность (например, при оформлении туристического пакета).

При опубликовании фотографий и иной информации о сотрудниках на сайте нужно их согласие. Это не распространяется на учителей и работников государственных органов, но при любом превышении минимального перечня ПД из закона их согласие тоже нужно получать.

Для передачи персональных данных работников внутри российской группы компаний нужно получать их письменное согласие, а внутри международной группы компаний – письменное согласие и договор-поручение со штаб-квартирой. Одно согласие работника с указанием каждого контрагента даётся для одной цели обработки ПД.

При передаче ПД работников третьи лица, привлекаемые по договору поручения, могут объединены в одно согласие (если цель обработки ПД единая). Третьи лица, привлекаемые по договору поручения, подают уведомления об обработке ПД, кроме ч. 2 ст. 22 ФЗ «О ПД». У оператора нет обязанности предоставлять третьему лицу, привлекаемому по договору поручения, сведения о правовых основаниях обработки ПД.

После достижения целей обработки персональных данных необходимо их уничтожить и оформить акт об уничтожении. Частым нарушением этого требования является обработка ПД соискателей после принятия решения об отказе в устройстве на работу (при отсутствии внешнего кадрового резерва, кроме госслужащих) и обработка ПД в информационной системе персональных данных по истечении сроков, указанных в законе. Порядок уничтожения ПД должен быть указан в локальных актах.

Обязанности оператора

Необходимо предоставлять в Роскомнадзор уведомления об обработке ПД. В уведомлении указывается только одно ответственное лицо, и даются его почта и телефон. Если контактные данные меняются, об этом нужно обязательно уведомить РКН.

Если иностранное юридическое лицо имеет представительство на территории РФ, то можно подать уведомление, а если нет, то уведомление подавать не нужно. Однако требования о локализации такая организация обязана выполнить (базы данных по обработке ПД должны находиться на территории РФ). Кроме того, раз в два года проводятся проверки в отношении таких иностранных компаний.

Чтобы не было нарушений в виде предоставления неполных или недостоверных сведений, рекомендуется проводить внутри организации аудит деятельности оператора по обработке ПД и следить, чтобы ответственное за заполнение уведомления отраслевое подразделение отражало информацию не только о своей деятельности (кадры, бухгалтерия). В организации должны быть планы или материалы проверочных мероприятий, подтверждающие внутренний контроль/аудит ПД (акты, протоколы, докладные записки).

Популярное нарушение - неполный перечень целей обработки ПД. Например, в целях обработки персональных данных часто забывают указать организацию пропускного режима и подбор персонала.

Понятие “база данных” трактуется сотрудниками РКН по внутреннему убеждению, например, любая таблица в Word – это тоже база данных.

Адреса всех баз персональных данных обязательно должны быть указаны в формате 123456, Москва г., ул. ___, д. ___, стр. ___, в том числе базы данных сайта и информационной системы персональных данных оператора. Также необходимо помнить, что база ПД – это не только информационные системы (сервер, центр обработки данных), но и места, где находятся материальные носители (жёсткие диски, картотеки).

При использовании для хранения облачной инфраструктуры требуется договор-поручение с провайдером. Облачная инфраструктура обеспечивает доступ, а эти действия означают обработку, даже не имея самого доступа к ПД.

После прекращения обработки персональных данных или при изменении информации, содержащейся в уведомлении, необходимо предоставить сведения об этом в Роскомнадзор в течение 10 дней.

Согласно ФЗ №152 “О персональных данных”, в организации должно быть лицо, ответственное за организацию обработки ПД. Нарушением является назначение на эту должность нескольких лиц или отсутствие данного полномочия в должностном регламенте. Можно указать полномочия ответственного лица в трудовом договоре или в приказе о назначении лица и наделении полномочиями, но лучше сделать это отдельно в должностной инструкции.

Работников оператора, непосредственно осуществляющие обработку ПД, обязаны быть ознакомлены с положениями законодательства РФ. Для подтверждения этого формируется лист ознакомления работников с положениями законодательства РФ, соответствующие положения включаются в трудовой договор с работником, проводятся курсы для работников (с получением документов) и внутренние обучающие мероприятия. Ознакомление работников с законодательством в электронном виде не в полной мере отвечает требованиям ст. 86 ТК РФ.

Также должен быть утверждён перечень лиц, осуществляющих обработку ПД, либо имеющих к ним доступ.

Составы правонарушений ст. 13.11 КоАП РФ (нарушение законодательства РФ в области персональных данных)

•Ч. 1 ст. 13.11 КоАП: включение избыточного объема данных, неправомерное размещение изображения гражданина на сайте, неправомерная обработка работодателем ПД близких родственников, неправомерная обработка ПД в целях продвижения товаров, работ, услуг;

•Ч. 2 ст. 13.11 КоАП: публикация статьи в интернете, которая содержит инфо в большом объеме со специальной категорией ПД без согласия гражданина, письменная форма согласия не соответствовала ч. 4 ст. 9 ФЗ;

•Ч. 3 ст. 13.11 КоАП: нет политики обработки ПД на сайте;

•Ч. 4 ст. 13.11 КоАП: нереализация права субъекта на получение информации, которая относится к обработке его ПД;

•Ч. 5 ст. 13.11 КоАП: нарушение сроков по уточнению, блокированию, уничтожению ПД;

•Ч. 6 ст. 13.11 КоАП: невыполнение обязанностей по соблюдению условий, обеспечивающих сохранность материальных носителей (например, неправильная утилизация медицинских амбулаторных карт).

Основные проблемы при взаимодействии проверяющих лиц с операторами в рамках проведения плановых/внеплановых проверок

1.Отсутствие уполномоченного представителя оператора;

2.Отсутствие документа, подтверждающего полномочия сотрудников на представление интересов оператора и взаимодействие с проверяющими лицами (доверенность, приказ);

3.Назначение в качестве уполномоченных представителей оператора лиц, не обладающих достаточными профессиональными знаниями;

4.Отказ в предоставлении запрашиваемой информации и документации;

5.Отказ в предоставлении доступа в помещения оператора, где осуществляется обработка ПД;

6.Отказ в предоставлении доступа к оборудованию оператора;

7.Неумышленное затягивание сроков проведения проверки (продление сроков – это дополнительная административная нагрузка).

При этом важно помнить, что должностные лица РКН:

1.Не осуществляют консультирование проверяемого лица;

2.Не предоставляют проект акта проверки для предварительного ознакомления представителем проверяемого лица;

3.Не дают пояснений относительно причин или оснований квалификации отдельных действий оператора как нарушающих ФЗ «О ПД», их можно получить только при обжаловании акта;

4.Не продлевают, в том числе и по письменному обращению проверяемого лица, контрольные сроки исполнения предписания об устранении нарушений.

Роскомнадзор дал разъяснения по закону о персональных данных в форме вопросов и ответов:

Что такое Уполномоченный орган по защите прав субъектов персональных данных и на кого возложена реализация этих функций?

Уполномоченный орган — федеральный орган исполнительной власти, осуществляющий функции контроля и надзора в сфере информационных технологий и связи. В настоящее время, в соответствии с постановлением Правительства от 16 марта 2009 года № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» данная функция возложена на Роскомнадзор.

Кто может являться оператором персональных данных?

В соответствии с п. 2 ст.3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.При этом операторами указанные органы и лица являются независимо от включения в реестр операторов, осуществляющих обработку персональных данных, который ведет Роскомнадзор.

В каких случаях операторами не должна обеспечиваться конфиденциальность персональных данных?

В соответствии с ч. 2 ст.7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обеспечения конфиденциальности персональных данных не требуется:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

В каких случаях для обработки персональных данных не требуется согласия субъекта персональных данных?

Согласно ч. 2 ст.6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» согласия субъекта персональных данных не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

1.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;(п. 1.1 введен Федеральным законом от 25.11.2009 № 266-ФЗ)

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Кто должен запрашивать согласие работников предприятия на обработку персональных данных при их передаче для обработки другому оператору?

Получить согласие работника на передачу его персональных данных для обработки другому оператору должна администрация предприятия, на котором работает субъект персональных данных.

В каких случаях оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных?

В соответствии с ч.1 ст.22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. Исключение составляют случаи, предусмотренные ч.2 комментируемой статьи, при обработке персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) 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;

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

4) являющихся общедоступными персональными данными;

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

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

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

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.Уведомление должно быть направлено в письменной форме и подписано должностным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации

Образец формы уведомления об обработке персональных данных и методические рекомендации по его заполнению размещены на официальном сайте Роскомнадзора: https://pd.rkn.gov.ru/operators-registry/notification/form/

Кроме того, на портале Персональные данные реализована функция по заполнению уведомлений об обработке персональных данных в электронной форме.

Вправе ли физическое лицо представлять персональные данные своих близких родственников?

Предоставление физическим лицом оператору персональных данных близких родственников возможно только при наличии письменного согласия указанных лиц либо в случаях, установленных федеральными законами.

Если при обработке персональных данных организацией нарушаются мои права, куда я могу обратиться за защитой?

Вы вправе обратиться в ближайшее территориальное управление Роскомнадзора. Адреса и контактные телефоны указаны на официальном сайте Роскомнадзора.

Какая ответственность предусмотрена за нарушения оператором требований Федерального закона «О персональных данных»?

Ст.24 Федерального закона «О персональных данных» определяет ответственность за нарушение данного Федерального закона, которая выражается в виде уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.Административная ответственность за нарушение настоящего Федерального закона наступает за:

— неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, либо несвоевременное предоставление таких документов и материалов, непредставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации (ст.5.39 КоАП РФ);

— нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст.13.11 КоАП РФ);

— разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность) (ст.13.14 КоАП);

— непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде (ст.19.7 КоАП РФ).

Кроме того, за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, и неправомерный доступ к охраняемой законом компьютерной информации российским законодательством предусмотрена уголовная ответственность, предусмотренная ст.137, 272 УК РФ.

Вправе ли кредитная организация обрабатывать персональные данные физических лиц, получивших отказ в предоставлении кредита? Возможно ли хранить формы анкет-заявок на получение кредита в формате цифровых копий?

Персональные данные субъектов персональных данных, полученные кредитной организацией при рассмотрении заявок на получение кредита, в случае отрицательного решения кредитной организации подлежат уничтожению в срок, не превышающий трех рабочих дней с даты принятия соответствующего решения.

Обращаем Ваше внимание, что типовые формы документов, характер информации в которых предполагает или допускает включение в них персональных данных, могут храниться в формате цифровых копий при соблюдении требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Возможно ли получение согласия на обработку персональных данных по телефону?

Получение согласия на обработку персональных данных по телефону, посредством СМС-сообщений действующим законодательством Российской Федерации не установлено.

Что является доказательством получения согласия на обработку персональных данных при покупке товаров в интернет-магазинах?

При заполнении вэб-формы заявки на покупку товара на сайте интернет-магазина в информационно-телекоммуникационной сети «Интернет» критерием, свидетельствующим о получении оператором согласия субъекта персональных данных на обработку его персональных данных, является файл электронной цифровой подписи.

Кроме того, предложение оператора о продаже товара в отдельных случаях может рассматриваться как публичная оферта. Таким образом, субъект персональных данных, акцентируя указанную оферту, тем самым осуществляет конклюдентные действия, выражающие его волю и согласие на обработку его персональных данных, предоставленных при заполнении заявки на покупку товаров.

Вправе ли оператор запрашивать сведения о судимости?

В соответствии с ч.3 ст.10 Федерального закона «О персональных данных» обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Какие иностранные государства обеспечивают адекватную защиту персональных данных?

До начала осуществления трансграничной передачи персональных данных оператор, осуществляющий обработку персональных данных (далее — Оператор) на территории Российской Федерации, обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

Критериев, определяющих адекватность защиты прав субъектов персональных данных на территории иностранного государства, действующим законодательством Российской Федерации не предусмотрено.Оператору, осуществляющему трансграничную передачу персональных данных, необходимо руководствоваться законодательством иностранного государства, на территорию которого осуществляется передача персональных данных, законодательством Российской Федерации в области защиты прав субъектов персональных данных, а также международными нормативными актами, в том числе Конвенцией о защите прав физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года ETS № 108 с учетом перечня стран, подписавших и ратифицировавших данную Конвенцию. Это Австрия, Бельгия, Болгария, Дания, Великобритания, Венгрия, Германия, Греция, Ирландия, Испания, Италия, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Финляндия, Франция, Чехия, Швеция, Эстония.

Вторая группа, которые могут претендовать на статус стран, обеспечивающих адекватную защиту персональных данных, это страны, имеющие общенациональные нормативные правовые акты в области защиты персональных данных и уполномоченный надзорный орган по защите прав субъектов персональных данных. Это Андорра, Аргентина, Израиль, Исландия, Канада, Лихтенштейн, Норвегия, Сербия, Хорватия, Черногория, Швейцария, Южная Корея, Япония.

Распространяются ли требования Федерального закона «О персональных данных» на юридическое лицо иностранного государства?

Требования Федерального закона «О персональных данных» распространяются на представительства юридических лиц иностранных государств, осуществляющих деятельность по обработке персональных данных на территории Российской Федерации.

Является ли веб-сайт информационной системой обработки персональных данных?

Согласно пункту 9 статьи 3 Федерального закона «О персональных данных» информационная система персональных данных — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.В случае соответствия веб-сайта указанным требованиям он является информационной системой.

Как документально оформить факт уничтожения персональных данных субъекта?

Порядок документальной фиксации уничтожения персональных данных субъекта определяется оператором персональных данных самостоятельно. Уничтожение персональных данных субъекта осуществляется комиссией либо иным должностным лицом, созданной (уполномоченным) на основании приказа Оператора. Наиболее распространенными способами документальной фиксации уничтожения персональных данных субъекта является оформление соответствующего акта о прекращении обработки персональных данных либо регистрация факта уничтожения персональных данных в специальном журнале. Типовая форма акта и журнала утверждаются самим Оператором.

Существуют ли стандарты или рекомендации по исполнению Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» операторами?

Да, такие документы, разработанные отдельными представителями операторского сообщества, существуют:

— стандарты и рекомендации в области стандартизации Банка России;

— концепция защиты персональных данных в информационных системах персональных данных оператора связи;

— методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости.

Наличие у программы сертификата соответствия ФСТЭК не решает проблемы защиты ПДн. Существует множество средств защиты информации и сценариев их использования. Для построения эффективной и адекватной системы защиты персональных данных важно понимать принципы и порядок реализации мер, направленных на обеспечение безопасности ПДн.

Важно! Защита персональных данных — это комплекс мероприятий, направленных на обеспечение безопасности персональных данных, и внедрение системы защиты является лишь одним из этапов обеспечения безопасности.

Рекомендации по защите персональных данных

Не стоит забывать о поддержании созданной системы защиты ПДн в актуальном состоянии. Периодически необходимо проверять актуальность организационно-распорядительной документации, обновлять модель угроз и контролировать обеспечение установленного уровня защищенности ПДн.