Что делать с персональными данными?

Для реализации Федерального закона «О персональных данных» утвержден «Порядок проведения классификации информационных систем персональных данных». Что нам это дает? К чему обязывает?

В. В. Разувайкин, *директор по развитию направления «Персональные данные» Компания «Информзащита»*

Немного предыстории.

27 июля 2006 года вышел Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой персональных данных государственными и муниципальными органами власти, юридическими и физическими лицами, с использованием средств автоматизации (а в некоторых случаях и без). Цель такого регулирования – обеспечение защиты прав и свобод человека при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Законом вводится термин «Оператор», под трактовку которого подпадает любое юридическое лицо (а также и физические), которое хранит и обрабатывает персональные данные других физических лиц (врезка 1). Любое!

Согласно закону, при обработке персональных данных именно Оператор обязан принимать все **необходимые организационные и технические меры**, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Обеспечение безопасности персональных данных при их обработке – один из важнейших вопросов, для решения которых и был принят этот закон. И тут же возникает закономерный вопрос: какие именно меры в таком случае следует принимать? Какие из них являются необходимыми, а какие – не обязательны?

Закон отвечает на этот вопрос так: «*Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных*».

Разматываем клубок дальше. Какие же требования к обеспечению безопасности персональных данных устанавливает Правительство РФ? В ответ на этот пункт закона Правительство РФ Постановлением № 781 от 17.11.2007 утвердило «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», которым устанавливается следующее: «*Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.*

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации».

Сразу видно, что одними техническими решениями дело не ограни-

чивается. Требуются еще и организационные меры, что логично и естественно. По мере же углубления в требования оказывается, что с организационными мерами сложностей будет не меньше, чем с техническими средствами защиты. К тому же требования к методам и способам защиты персональных данных в информационных системах, согласно Постановлению № 781, должны устанавливаться ФСТЭК России и ФСБ России в соответствии с классификацией таких информационных систем.

Помимо вышесказанного еще ряд положений Постановления заслуживают того, чтобы мы заострили на них внимание.

- Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор.
- Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.
- Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
- При обработке персональных данных в информационной системе должно быть обеспечено:
  а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
  б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;
  в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
  г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
  д) постоянный контроль за обеспечением уровня защищенности персональных данных.
- Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

Все указанные требования по обеспечению защиты обрабатываемых персональных данных должны выполняться в соответствии с классификацией таких систем. Классифицировать же свои информационные системы персональных данных (ИСПД) должны сами Операторы таких систем, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Для этого и предназначен совместный Приказ ФСТЭК, ФСБ и Мининформсвязи № 55/86/20 от 13.02.08 «Об утверждении порядка проведения классификации информационных систем персональных данных», опубликованный в «Российской газете» 12 апреля этого года.

Утвержденный Порядок описывает проведение классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, которые позволяют осуществлять обработку таких персональных данных с использованием средств автоматизации (врезка 2).

Классифицирование осуществляют сами Операторы, учитывая следующие исходные данные.

1. Категория обрабатываемых в информационной системе персональных данных (определяется в зависимости от конкретного содержания персональных данных).
2. Объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе).
3. Заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе (конфиденциальность, защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).
4. Структура информационной системы (автономная, локальная, распределенная).
5. Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям

Врезка 1

Определения из закона «О персональных данных»

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.

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.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

международного информационного обмена.
6. Режим обработки персональных данных (однопользовательские или многопользовательские).
7. Режим разграничения прав доступа пользователей информационной системы.
8. Местонахождение технических средств информационной системы (в РФ, за пределами РФ, частично за пределами РФ).

Присвоение информационной системе соответствующего класса должно быть документально оформлено самими Операторами персональных данных (государственными и муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных).

Совместный Приказ ФСБ РФ, ФСТЭК РФ и Мининформсвязи РФ, с одной стороны, упорядочил классификацию ИСПД, с другой – добавил множество новых вопросов к уже существующим. Например, разделение на типовые и специальные ИСПД, задаваемое самим Оператором ПД, исходя из требуемых мер безопасности ПД. Для типовых ИСПД требуется обеспечить только конфиденциальность ПД. Если же требуется обеспечить еще хотя бы одну характеристику безопасности ПД (защиту от изменения, или блокирования, или уничтожения, или иных НСД), то это уже – специальная ИСПД. Сложно представить себе информационную систему, лишенную всякой защиты от хотя бы несанкционированных изменений хранимых данных. Опять же классификация по данному Порядку возможна только для типовых ИСПД. Для специальных же ИСПД класс необходимо определять по методическим документам, разрабатываемым ФСТЭК РФ и ФСБ РФ. Не знаю, что разрабатывает ФСБ РФ, но ФСТЭК РФ разработал четыре методических документа и защитил их грифом ДСП, что сильно затрудняет самостоятельную классификацию специальных ИСПД.

Многие подобные вопросы требуют разъяснения. Но ясно одно – уже есть с чем работать и вряд ли стоит ожидать первых административных санкций, чтобы начинать задумываться о безопасности персональных данных, с которыми вы работаете. Более того, в конце марта вышел Приказ Россвязьохранкультуры о создании единого реестра всех владельцев и операторов информационных систем персональных данных. Другими словами, так или иначе, но закон начал работать.

Итак – что можно и нужно делать прямо сейчас Операторам ИСПД? Ждать, пока наступит ясность или когда придет Россвязьохранкультуры с проверкой? Конечно же, нет. Есть некоторые шаги, которые ясно определены уже сейчас, и их срочно нужно выполнять. Не можно, а именно нужно! С чего же начать?

Итак, строго следуя нормативным актам в том виде, какие они есть сейчас, можно выделить следующие шаги.

Первый шаг – выявить все свои ИСПД.

Второй шаг – определить назначение ИСПД и круг лиц, работающих с данной ИСПД, описать все это документально.

Третий шаг – классифицировать свои ИСПД в соответствии с Порядком классификации.

Четвертый шаг – создать (описать) модель угроз для каждой конкретной ИСПД, описать средства защиты, разработать ряд нормативных документов (таких как инструкция о порядке обработки ПД, регламент доступа в зону обработки ПД и т. д.).

Пятый шаг – поставить в известность Россвязьохранкультуру о наличии ИСПД и о присвоенном ей классе.

Шестой шаг – обеспечить техническими и организационными мерами требуемый уровень безопасности для каждой конкретной ИСПД в соответствии с ее классом (для вновь создаваемых систем – во время их разработки, для уже существующих – согласно Закону, до 01.01.2010).

Седьмой шаг – при необходимости сертифицировать систему защиты ИСПД или саму ИСПД во ФСТЭК РФ, получить лицензию на деятельность по технической защите информации.

Восьмой шаг – готовиться к проверке Россвязьохранкультуры.

Конечно, существует и альтернатива – воспользоваться услугами серьезной компании, которая много лет занимается услугами в сфере информационной безопасности. Ее специалисты помогут пройти все эти шаги и не дадут свернуть в сторону: разработать комплекс как организационных мер, так и технических решений по защите персональных данных, а при необходимости и пройти сертификацию (аттестацию) во ФСТЭК России. ■

Врезка 2

Порядком проведения классификации информационных систем персональных данных определены 4 класса информационных систем персональных данных (ИСПД):

- 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.