



Персональным данным требуется отсрочка?

Эксперты в один голос говорят о противоречивости российской нормативной правовой базы по персональным данным, сложности внесения изменений в существующие информационные системы с целью приведения их в соответствие новым требованиям и ограниченности установленных законом сроков. Могут ли многочисленные операторы персональных данных рассчитывать на перенос этих сроков?



**Александр
ВАСЮНИН,**
компания
«Информзашита»

Европейский опыт

Для понимания контекста проблемы вспомним основные этапы становления законодательства о персональных данных (ПД) за рубежом.

Европейское законодательство в этой сфере уходит корнями в принятую в 1948 г. Генеральной Ассамблеей ООН «Всеобщую декларацию прав человека», ст. 12 которой гласит, что «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произ-

вольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

В 1981 г. Совет Европы принял Конвенцию о защите физических лиц при автоматизированной обработке ПД, которая исходит из того, что права и интересы личности в условиях применения новейших информационных технологий могут быть нарушены в результате несанкционированного сбора, обработки, хранения и распространения сведений персонального характера. Евросоюз стремился к тому, чтобы субъекты ПД имели четко определенные права и возможность обратиться к должностному лицу или органу, который обязан предпринять действия для их защиты. Каждой стране-члену ЕС было рекомендовано создать институт уполномоченного по защите ПД.

Следующим шагом стала Директива 95/46/ЕС Европарламента и Совета ЕС от 24.10.1995 о защите прав частных лиц применительно к обработке ПД и о свободном движении таких данных. Здесь стоит особо отметить, что Директива 95/46/ЕС рекомендует учитывать отраслевую специфику при исполнении ее требований.

В целях углубления отраслевого принципа защиты ПД, провозглашенного Директивой 95/46/ЕС, была утверждена Директива 97/66/ЕС Европарламента и Совета ЕС от 15.12.1997 об обработке ПД и защите неприкосновенности частной жизни в сфере телекоммуникаций. Она дополняет и конкретизирует правила обработки данных в информационных системах, которые собираются опе-

раторами в ходе предоставления услуг связи. Позже появилась Директива 2002/58/ЕС Европарламента и Совета ЕС от 12.07.2002 относительно обработки личных данных и защиты личной тайны в сфере электронных коммуникаций, заменившая Директиву 97/66/ЕС, которая регулировала схожую сферу отношений, но не учитывала современное состояние электронной связи.

Таким образом, европейское законодательство в области ПД идет параллельно с техническим прогрессом и учитывает современные тенденции в области технологий.

А что у нас?

В России основными побуждающими мотивами принятия закона о персональных данных явилось стремление развить положения Конституции РФ о личной тайне и неприкосновенности информации о частной жизни физического лица, а также осознание необходимости в более тесной интеграции страны в мировое и европейское сообщество.

Так, в 2005 г. Россия ратифицировала Конвенцию о защите физических лиц при автоматизированной обработке ПД и во исполнение взятых на себя обязательств в 2006 г. приняла Федеральный закон № 152-ФЗ «О персональных данных». В дополнение к закону в 2007–2008 гг. был принят целый ряд нормативных правовых актов и методических документов, после выхода которых разгорелась нешуточная дискуссия как в экспертном сообществе, так и среди представителей различных ветвей власти.

Нормативные правовые акты о персональных данных

- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утверждено Постановлением Правительства РФ от 17.11.2007 № 781).
- Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных (утверждены Постановлением Правительства РФ от 06.07.2008 № 512).
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено Постановлением Правительства РФ от 15.09.2008 № 687).

В октябре нынешнего года прошли парламентские слушания на тему «Актуальные вопросы развития и применения законодательства о защите прав граждан при обработке персональных данных», на которых были зафиксированы глубокие системные проблемы и противоречия в нормативной правовой базе, а также противоречия между государственными регуляторами и операторами ПД.

Участники слушаний указали на ориентированность нормативных правовых документов на защиту собственно ПД, а не прав граждан при их обработке в информационных системах, что противоречит Конвенции Совета Европы и закону «О персональных данных», которые в качестве своих целей устанавливают обеспечение защиты прав и свобод человека и гражданина при обработке его ПД.

Вторая проблема связана с высокими требованиями ФСТЭК России по защите информационных систем персональных данных (ИСПД), что также противоречит европейскому опыту. В частности, ст. 17 Директивы 95/46/ЕС прямо увязывает необходимые меры со стоимостью их реализации: «Государства-участники обеспечат, что контролер должен будет реализовать надлежащие технические и организационные меры для защиты персональных данных от случайного или незаконного уничтожения или случайной утраты, изменения, неправомерного раскрытия или доступа, в частности когда обработка влечет передачу данных по сети, а также от всех иных незаконных форм обработки. С учетом состояния и стоимости их реализации такие меры должны обеспечить надлежащий уровень безопасности для рисков, представленных обработкой и природой защищаемых данных».

Требования же ФСТЭК по защите ПД во многом повторяют требования по защите сведений, составляющих государственную тайну, вследствие чего операторы персональных данных должны нести серьезные расходы. К тому же методические документы ФСТЭК имеют гриф «Для служебного пользования» и не находятся в открытом доступе, что было признано неконструктивным.

Еще один момент, на который обратили внимание участники слушаний, – отсутствие учета отраслевой

специфики, из-за чего многие компании, основная деятельность которых связана с использованием больших объемов ПД, например организации телеком-сектора, попадают в сложное положение. Поэтому получила положительную оценку ведущая при участии «большой тройки» работа Инфокоммуникационного союза над проектом отраслевого стандарта по защите персональных данных в ИСПД операторов связи.

Было выдвинуто предложение внести изменения в Федеральный закон № 128-ФЗ «О лицензировании отдельных видов деятельности» для исключения необходимости получения лицензии на техническую защиту конфиденциальной информации при обработке такой информации для собственных нужд.

Но одним из главных вопросов слушаний, безусловно, была возможность переноса на год или даже на два срока приведения ИСПД в соответствие требованиям закона «О персональных данных» (согласно п. 3 ст. 25 данного закона это должно произойти 1 января 2010 г.). Аргументация понятна – методические документы государственных регуляторов были выпущены не так давно, а времени на их реализацию уже практически не осталось. Тем не менее Роскомнадзор официально заявил, что настаивает на нецелесообразности изменения срока приведения ИСПД в соответствие с законодательством. Конечно, не до конца понятны критерии, по которым регуляторы будут определять степень вреда, нанесенного субъектам ПД, однако надо отметить, что именно их обращения являются основным поводом для проверок, а статистика показывает, что число таких обращений с каждым годом неумолимо растет.



В сложившихся непростых условиях операторам ПД можно порекомендовать не игнорировать требования по защите персональных данных, ведь полное бездействие в надежде на то, что проверяющие не придут, связано с принятием повышенных рисков, а сам факт проведения работ по защите ПД и аргументированная позиция по возможным спорным вопросам помогут до некоторой степени себя обезопасить. ИКС

■ Порядок проведения классификации информационных систем персональных данных (утвержден приказом ФСТЭК РФ, ФСБ РФ, Мининформсвязи РФ от 13.02.2008 № 55/86/20).

Методические документы ФСТЭК РФ (с грифом ДСП)

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

■ Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Методические документы ФСБ РФ:

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

Когда верстался номер, стало известно, что в Госдуму внесен законопроект, предлагающий перенести срок вступления в силу п. 3 ст. 25 закона «О персональных данных» на год.