О защите персональных данных

Андрей Николаевич ПРИВАЛОВ, заместитель руководителя Управления Федерального казначейства по Омской области

Дмитрий Петрович КУРМАЗОВ, начальник отдела режима секретности и безопасности информации Управления Федерального казначейства по Омской области

1 января 2011 года заканчивается срок приведения всех без исключения информационных систем персональных данных в соответствие с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Об опыте реализации норм закона в Управлении Федерального казначейства по Омской области читайте в статье.

Для выполнения требований законодательства в области обработки и защиты персональных данных в Управлении Федерального казначейства по Омской области (далее — Управление) весь объем работ был разделен на несколько этапов.

Этап первый: мониторинг персональных данных

На первом этапе был проведен мониторинг состава, содержания, а также местоположения персональных данных граждан. То есть из общей массы информации, обрабатываемой в Управлении, были выделены персональные данные с указанием таких параметров, как:

- содержание персональных данных;
- наименование документов, содержащих персональные данные;
- объем обрабатываемых персональных данных;
- вид представления (бумажный и/или электронный носитель);
- цель обработки персональных данных;
- информация о сотрудниках, имеющих доступ к персональным данным;
- номера кабинетов, в которых осуществляется обработка персональных данных;
- идентификаторы ПЭВМ, на которых осуществляется обработка персональных данных.

Полученная информация позволила сделать вывод о категории и объеме обрабатываемых в Управлении персональных данных, способах обработки (с использованием средств автоматизации или без использования таковых), определить границы информационной системы и ее структуру (конфигурацию, топологию), а также определить субъекты доступа к защищаемым ресурсам. Было установлено, что часть документов (информации) с персональными данными обрабатывается в локальной вычислительной сети Управления, а часть — исключительно на бумажных носителях.

Этап второй: классификация персональных данных и системы

На данном этапе была установлена группа субъектов, чьи персональные данные подвергаются обработке. Было выделено пять групп:

1. сотрудники Управления;
2. сотрудники отделений Управления;
3. члены семей сотрудников;
4. сотрудники сторонних организаций;
5. иные граждане.

Для установления методов и способов защиты информации была проведена классификация информационных систем персональных данных. Указанная классификация проводится государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных. Классификация проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее

введенных в эксплуатацию и (или) модернизируемых информационных систем). Порядок проведения классификации определен совместным приказом Федеральной службы по техническому и экспортному контролю (далее — ФСТЭК), ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Проведение классификации информационных систем включает в себя сбор и анализ исходных данных по информационной системе и присвоение информационной системе соответствующего класса и его документальное оформление. Для этого вначале была определена категория персональных данных, обрабатываемых в информационных системах Управления. Вышеназванный приказ выделяет четыре категории:

Категория 1 — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

Категория 2 — персональные данные, позволяющие идентифицировать субъект персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

Категория 3 — персональные данные, позволяющие идентифицировать субъект персональных данных;

Категория 4 — обезличенные и (или) общедоступные персональные данные.

Анализ персональных данных позволил сделать вывод о том, что в информационных системах Управления обрабатываются данные, которые дают возможность лишь идентифицировать субъект, а именно: в системе используются фамилия, инициалы, иные персональные данные (адрес, паспортные данные и т. д.) субъекта. Никакой дополнительной информации (не содержащейся в информационной системе) получить из обрабатываемых персональных данных невозможно. К каким-либо другим базам данных, имеющим дополнительную информацию о субъекте персональных данных, Управление подключение не производит. На основании данных аргументов было принято решение о присвоении обрабатываемым в информационной системе Управления персональным данным 3-й категории.

Также были установлены и характеристики информационной системы Управления. Во-первых, информационная система отнесена к специальной информационной системе, поскольку, вне зависимости от обеспечения конфиденциальности персональных данных, необходимо обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий). Во-вторых, информационная система Управления представляет собой комплекс автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальная информационная система). В-третьих, информационная система Управления имеет подключение к сетям связи общего пользования и сетям международного информационного обмена. В-четвертых, режим обработки персональных данных в информационной системе Управления — многопользовательский. В-пятых, информационная система Управления относится к системе с разграничением прав доступа пользователей. В-шестых, все технические средства информационной системы Управления находятся в пределах Российской Федерации.

С учетом категории информационной системы, объема обрабатываемых персональных данных (от 1 тыс. до 100 тыс. субъектов), а также указанных выше характеристик информационной системы Управления, ей был присвоен 3-й класс информационной системы персональных данных. Результаты классификации информационной системы были оформлены соответствующим актом Управления. Стоит отметить, что для данного класса информационных систем нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных.

Этап третий: определение методов и способов защиты информации

На завершающем этапе, с учетом требований и рекомендаций руководящих документов ФСТЭК России, были разработаны организационно-распорядительные документы, в которых регламентируется порядок обработки документов (информации), содержащих персональные данные, установлен круг работников Управления, допущенных к обработке такой информации, определены актуальные угрозы безопасности, выработаны и реализованы организационные и технические меры по их нейтрализации. При этом во внимание было принято то, что в соответствии с приказом ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» к методам и способам защиты информации в информационных системах относятся:

- методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от 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;
- методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа ↪

к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий.

С учетом того, что ранее был установлен 3-й класс информационной системы персональных данных Управления, было принято решение, что угрозы утечки речевой информации, а также информации, представленной в виде информативных электрических сигналов и физических полей, являются неактуальными, а сама информация от утечки по техническим каналам защите не подлежит. Поэтому применяемыми в Управлении методами и способами защиты информации от несанкционированного доступа являются следующие:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также где хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Федеральный закон «О персональных данных» направлен на обеспечение 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

Поскольку информационная система Управления имеет подключение к сетям связи общего пользования и сетям международного информационного обмена, было решено наряду с методами и способами, указанными выше, предпринять еще ряд мер по защите информации от несанкционированного доступа:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- использование средств антивирусной защиты;
- централизованное управление системой защиты персональных данных информационной системы.

На сегодняшний день все мероприятия в сфере обработки и защиты персональных данных, предписанные законодательством, в Управлении выполнены. С целью поддержания надлежащего уровня информационной безопасности производится контроль (как плановый, так и внеплановый) выполнения требований разработанных организационно-распорядительных документов, а также работоспособности применяемых средств защиты.

Следует принять во внимание, что класс информационной системы может быть в дальнейшем пересмотрен:

- на основе проведенного Управлением анализа и оценки угроз безопасности персональных данных с учетом особенностей или изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Реализация одной или нескольких угроз информационной безопасности в каком-либо управлении Федерального казначейства или в их территориальных отделениях могут повлечь негативные последствия не только для субъектов персональных данных, но также нанести ущерб репутации органам исполнительной власти России и вызвать серьезные социальные последствия. Именно по этой причине вопросам информационной безопасности в Управлении уделяется очень серьезное внимание.