А. В. Архангельская

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В связи с вступлением в силу в 2011 г. Федерального закона «О внесении изменений в Федеральный закон "О персональных данных"» [1], ужесточившего требования к операторам персональных данных в части их технической защиты, ведется много дискуссий и споров о его применении на практике. Поэтому видится необходимым уделить внимание некоторым особенностям применения средств криптографической защиты информации (СКЗИ) при защите персональных данных.

Безопасность обработки персональных данных с использованием СКЗИ обеспечивают операторы персональных данных, а также лица, которым на основании договора с оператором персональных данных поручены их обработка и/или оказание услуг по организации и обеспечению безопасности их обработки в некоторой информационной системе с использованием СКЗИ.

Перечислим основные документы, в соответствии с которыми должны проводиться работы по обеспечению с помощью СКЗИ безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПД) с использованием средств автоматизации:

1) Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2];

2) Федеральный закон № 152-ФЗ «О персональных данных» [3];

3) Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных № 781 [4];

4) Порядок проведения классификации информационных систем персональных данных [5];

5) Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) [6];

6) 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 (Типовые требования) [7];

7) Методические рекомендации ФСБ России «По обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (Методические рекомендации) [8];

8) Постановление Правительства РФ «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» [9].

Ответственность за соответствие проводимых мероприятий по организации обработки персональных данных с использованием СКЗИ лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также Типовым требованиям возлагается на операторов персональных данных, которые должны обеспечивать комплексную защиту персональных данных, в том числе посредством применения некриптографических средств защиты информации.

Обязанностями оператора персональных данных являются следующие:

1) разработка для каждой ИСПД модели угроз безопасности персональных данных при их обработке;

2) построение на ее основе системы безопасности персональных данных, обеспечивающей нейтрализацию всех выявленных угроз;

3) обоснование необходимости использования СКЗИ для обеспечения безопасности персональных данных;

4) установка и ввод в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к ним;

5) проверка готовности СКЗИ к использованию;

6) обучение лиц, использующих СКЗИ, работе с ними;

7) поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним, носителей персональных данных;

8) учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных;

9) контроль за соблюдением условий использования СКЗИ, указанных в эксплуатационной и технической документации к ним;

10) разбор и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования СКЗИ, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, снижающим уровень их защищенности;

11) разработка и принятие мер по предотвращению возможных опасных последствий указанных видов нарушений;

12) описание организационных и технических мер, которые оператор персональных данных обязуется осуществлять при обеспечении безопасности персональных данных с использованием СКЗИ.

Пользователи СКЗИ допускаются к работе с ними по решению, утверждаемому оператором персональных данных. При наличии двух или более пользователей СКЗИ обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

Контроль за организацией, обеспечением функционирования и безопасности СКЗИ, предназначенных для защиты персональных данных при их обработке в ИСПД, осуществляется в соответствии с действующим законодательством Российской Федерации и возлагается на оператора персональных данных и ответственного пользователя СКЗИ.

При разработке системы защиты персональных данных оператор персональных данных должен сформировать модель угроз безопасности персональных данных (далее – модель угроз), причем в случае использования СКЗИ в информационной системе к формированию модели угроз могут привлекаться лицензиаты ФСБ, являющиеся разработчиками СКЗИ или специализированными организациями, проводящими тематические исследования СКЗИ.

Перечислим основные принципы формирования модели угроз (рис. 1):

1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных.

2. Необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных, т. е. прямые угрозы, так и угрозы, создающие условия для появления прямых угроз, т. е. косвенные угрозы.

3. Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4. СКЗИ штатно функционируют совместно с техническими и программными средствами, способными повлиять на выполнение предъявляемых к СКЗИ требований и образующими среду функционирования СКЗИ.

5. Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СКЗИ не может обеспечить защиту информации от раскрытия лицами, имеющими право на доступ к этой информации).

6. Нарушитель может действовать на различных этапах жизненного цикла СКЗИ и среды их функционирования.

7. Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться СКЗИ, сертифицированные в системе сертификации ФСБ.

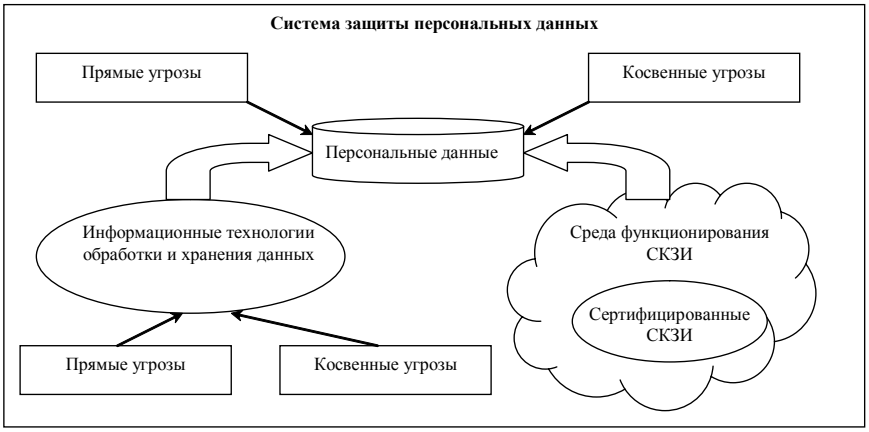

Рис. 1. Принципы формирования модели угроз безопасности персональных данных

В случае отсутствия готовых сертифицированных СКЗИ, подходящих для обеспечения безопасности персональных данных при их обработке в конкретной информационной системе, на этапе эскизного проекта разработчиком информационной системы с участием оператора персональных данных и предполагаемого разработчика СКЗИ готовится обоснование целесообразности разработки нового типа СКЗИ и определяются требования к его функциональным свойствам.

При разработке модели угроз составляются модель угроз верхнего уровня и детализированная модель угроз. Первая предназначена для определения характеристик безопасности защищаемых персональных данных и других объектов защиты и определяет исходные данные для детализированной модели угроз, вторая — для определения требуемого уровня криптографической защиты.

Формирование модели угроз верхнего уровня осуществляется на этапе сбора и анализа исходных данных по информационной системе, при этом для правильного выбора СКЗИ,

которые следует применять для обеспечения безопасности персональных данных, выполняются следующие действия:

1) определяются условия создания и использования персональных данных;

2) описываются формы представления персональных данных;

3) описывается информация, сопутствующая процессам создания и использования персональных данных, являющаяся объектом угроз и вследствие этого требующая защиты;

4) определяются характеристики безопасности не только персональных данных, но и всех объектов, которые могут являться возможными объектами угроз.

При формировании детализированной модели угроз необходимо определить совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

Помимо модели угроз должна быть разработана модель нарушителя, в которой учитывается, какие конкретные возможности нарушителя могут привести к конкретным атакам. Модель нарушителя должна содержать описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, и об ограничениях на эти возможности, тогда как в модели угроз указывается максимально полное описание угроз безопасности объекта.

Модель нарушителя для этапа эксплуатации технических и программных средств СКЗИ и среды их функционирования должна иметь следующую структуру:

1) описание нарушителей (субъектов атак);

2) предположения об имеющейся у нарушителя информации об объектах атак;

3) предположения об имеющихся у нарушителя средствах атак;

4) описание каналов атак.

Методические рекомендации различают шесть основных типов нарушителей: H_1, H_2, ... , H_6, причем возможности нарушителя типа H_{i+1} включают в себя возможности нарушителя типа H_i, $1 \le i \le 5$. Если внешний нарушитель обладает возможностями по созданию способов подготовки атак, аналогичными соответствующим возможностям нарушителя типа H_i, за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне, то этот нарушитель также будет обозначаться как нарушитель типа H_i, $2 \le i \le 6$.

Приведем основные свойства нарушителей, принадлежащих указанным типам:

1. Нарушитель типа H_1 располагает только доступными в свободной продаже аппаратными компонентами СКЗИ и среды их функционирования и может использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны.

2. Нарушитель типа H_2 располагает возможностями по использованию штатных средств, которые зависят от реализованных в информационной системе организационных мер.

3. Нарушителю типа H_3 могут быть известны все сети связи, работающие на едином ключе. Дополнительные возможности нарушителей типа $H_3 - H_5$ по получению аппаратных компонентов СКЗИ и среды их функционирования зависят от реализованных в информационной системе организационных мер.

4. Нарушитель типа H_4 может проводить лабораторные исследования СКЗИ, используемых за пределами контролируемой зоны информационной системы.

5. Нарушитель типа H_5 может проводить работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды их функционирования, он также располагает наряду с доступной в свободной продаже документацией на СКЗИ и среду их функционирования исходными текстами прикладного программного обеспечения.

6. Нарушитель типа H_6 располагает всей документацией и любыми аппаратными компонентами СКЗИ и среды их функционирования.

Нарушитель относится к типу H_i, если среди предположений о его возможностях есть предположение, относящееся к нарушителям типа H_i, и нет предположений, относящихся только к нарушителям типа H_j, $j > i$. Нарушитель относится к типу H_6 в информационных системах, в которых обрабатываются наиболее важные персональные данные, нарушение характеристик безопасности которых может привести к особо тяжелым последствиям.

Методические рекомендации различают шесть уровней — КС1, КС2, КС3, КВ1, КВ2, КА1 — криптографической защиты персональных данных, не содержащих сведений, составляющих государственную тайну, определенных в порядке возрастания количества и жесткости требований, предъявляемых к СКЗИ, и, соответственно, шесть классов СКЗИ, имеющих те же обозначения.

Уровень криптографической защиты персональных данных, которую обеспечивают СКЗИ, определяется оператором персональных данных путем отнесения нарушителя, действиям которого должны противостоять СКЗИ, к конкретному типу.

При отнесении заказчиком нарушителя к типу H_1 СКЗИ должно обеспечить криптографическую защиту по уровню КС1, к типу H_2 — КС2, к типу H_3 — КС3, к типу H_4 — КВ1, к типу H_5 — КВ2, к типу H_6 — КА1.

Обобщая приведенные в настоящей статье сведения об особенностях применения СКЗИ для защиты персональных данных, приведем перечень документов, которые должны быть разработаны в этом случае:

1) модель угроз безопасности персональных данных при их обработке в ИСПД и модель нарушителя;

2) эксплуатационная и техническая документация на используемые СКЗИ;

3) заключение о возможности эксплуатации СКЗИ;

4) журнал учета используемых СКЗИ;

5) журнал учета технической документации к СКЗИ;

6) журнал учета носителей персональных данных;

7) приказ о назначении лиц, допущенных к работе с СКЗИ;

8) документ, устанавливающий порядок обеспечения безопасности персональных данных при помощи СКЗИ;

9) документ, устанавливающий порядок организации контроля за соблюдением условий использования СКЗИ;

10) документ, устанавливающий порядок хранения носителей персональных данных.

Таким образом, при разработке системы защиты персональных данных ключевую роль играет модель угроз и созданная на ее основе классификация нарушителей, и при использовании СКЗИ необходимо проанализировать возможности нарушителей безопасности и сопоставить применяемые средства с определенными нормативными документами уровнями криптографической защиты персональных данных, не содержащих сведений, составляющих государственную тайну.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон Российской Федерации «О внесении изменений в Федеральный закон “О персональных данных”» от 25 июля 2011 г. № 261-ФЗ.

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

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

4. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждено постановлением Правительства Российской Федерации 17 ноября 2007 г. № 781.

5. Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 г., регистрационный номер 11462).
6. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждено ФСБ 9 февраля 2005 г.
7. 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, утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г.
8. Методические рекомендации ФСБ России «По обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21 февраля 2008 г. № 149/54-144.
9. Постановление Правительства РФ «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» от 29 декабря 2007 г. № 957 (с изменениями от 21 апреля, 24 сентября 2010 г.).