МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

УТВЕРЖДЕНЫ
руководством 8 Центра
ФСБ России
21 февраля 2008 года
№ 149/54-144

Введение

Настоящие Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (далее – Методические рекомендации) разработаны в соответствии с п. 2 постановления 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».

Методические рекомендации предназначены для операторов и разработчиков информационных систем персональных данных и охватывают вопросы защиты персональных данных с помощью криптосредств.

Методическими рекомендациями необходимо руководствоваться в случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств (за исключением случая, когда оператором является физическое лицо, использующее персональные данные исключительно для личных и семейных нужд), а также при обеспечении безопасности персональных данных при обработке в информационных системах, отнесенных к компетенции ФСБ России. В частности, Методическими рекомендациями необходимо руководствоваться в следующих случаях:

- при обеспечении с использованием криптосредств безопасности персональных данных при их обработке в государственных информационных системах персональных данных (часть 5 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»);

- при использовании криптосредств для обеспечения персональных данных в случаях, предусмотренных п. 3 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

Настоящие Методические рекомендации не распространяются на информационные системы персональных данных, в которых:

- персональные данные обрабатываются без использования средств автоматизации;

- обрабатываются персональные данные, отнесенные в установленном порядке к сведениям, составляющим государственную тайну;

- технические средства частично или целиком находятся за пределами Российской Федерации.

1 Основные термины и их определения

В настоящих Методических рекомендациях и при взаимодействии с лицензиатами ФСБ России, являющимися разработчиками криптосредств, разработчиками информационных систем персональных данных, в которых используются криптосредства, или специализированными организациями, проводящими тематические исследования криптосредств, используются следующие основные термины.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[1].

Автоматизированная система в защищенном исполнении (АСЗИ) – автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации[2].

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз[3].

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Примечание

Данное определение распространяется на любой реальный объект, в качестве которого могут выступать технические средства, программные средства, информация, информационные технологии, информационные системы, информационно-телекоммуникационные сети, здания, сооружения и т.д.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи[4].

Встраивание криптосредства – процесс подключения криптосредства к техническим и программным средствам, совместно с которыми предполагается его штатное функционирование, за исключением процесса инсталляции.

Документированные (декларированные) возможности ПО (ТС) – функциональные возможности ПО (ТС), описанные в документации на ПО (ТС).

Доступ к информации – возможность получения информации и ее использования[5].

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства[6].

Защищаемая информация – информация, для которой обладателем информации определены характеристики ее безопасности.

Инсталляция – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствие с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной системе и готовым решать определенный класс задач в определенном режиме работы[7].

Информация – сведения (сообщения, данные) независимо от формы их представления[8].

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[9].

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[10].

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[11].

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[12].

Информационно-телекоммуникационная сеть общего пользования –информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц[13].

Канал атаки – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения[14].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя[15].

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания[16].

Криптографически опасная информация (КОИ) – информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну[17].

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности».

Модель угроз – перечень возможных угроз.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Негативные функциональные возможности – документированные и недокументированных возможности программных и аппаратных компонентов криптосредства и среды функционирования криптосредства, позволяющие:

- модифицировать или искажать алгоритм работы криптосредств в процессе их использования;

- модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием криптосредства;

- получать доступ нарушителям к хранящейся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

Недокументированные (недекларированные) возможности ПО (ТС) – функциональные возможности ПО (ТС), не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение характеристик безопасности защищаемой информации[18].

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов[19].

Примечание

Так как по своей природе сведения, составляющие государственную тайну, не отличаются от всех остальных сведений, то приведенное определение можно корректно использовать для любых сведений.

Учитывая определение понятия «информация», термин «носитель информации» можно использовать в качестве синонима термину «носитель сведений».

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных[20].

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам[21].

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[22].

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности[23].

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров[24].

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[25].

Опубликованные возможности ПО или ТС – возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в СМИ, материалы конференций и других форумов, информация из сети Internet и т.д.).

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[26].

Пользователь – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

ПО – программное обеспечение.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом[27].

Специальная защита – комплекс организационных и технических мероприятий, обеспечивающих защиту информации от утечки по каналам побочных излучений и наводок.

Среда функционирования криптосредства (СФК) – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации[28].

Средство вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[29].

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства[30].

ТС – техническое средство.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства[31].

Угроза безопасности объекта – возможное нарушение характеристики безопасности объекта.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных[32].

Успешная атака – атака, достигшая своей цели.

Уровень криптографической защиты информации – совокупность требований, предъявляемых к криптосредству.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

Шифровальные (криптографические) средства:

а) средства шифрования – аппаратные, программные и аппаратно–

программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации)[33].

2 Основные положения

2.1. Работы по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (далее – информационная система) проводятся в соответствии со следующими основными документами:

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

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

- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 (далее – Положение);

- Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462) (далее – Порядок);

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382);

- 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 (ФСБ России, № 149/6/6-622, 2008);

- настоящие Методические рекомендации.

2.2. В соответствии с п. 2 Положения 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.

2.3. В соответствии с п. 12 Положения необходимым условием разработки системы защиты персональных данных является формирование модели угроз безопасности персональных данных (далее – модель угроз).

Кроме этого, в соответствии с п. 16 Порядка модель угроз необходима для определения класса специальной информационной системы.

2.4. Модель угроз формируется и утверждается оператором в соответствии с методическими документами, разработанными в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»[34].

В случае обеспечения безопасности персональных данных без использования криптосредств при формировании модели угроз используются методические документы ФСТЭК России.

В случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств при формировании модели угроз

используются методические документы ФСТЭК России и настоящие Методические рекомендации. При этом из двух содержащихся в документах ФСТЭК России и Методических рекомендациях однотипных угроз выбирается более опасная.

По согласованию с ФСТЭК России и ФСБ России допускается формирование модели угроз только на основании настоящих Методических рекомендаций.

При обеспечении безопасности персональных данных при обработке в информационных системах, отнесенных к компетенции ФСБ России, модели угроз формируются только на основании настоящих Методических рекомендаций.

2.5. В случае использования в информационной системе криптосредств при необходимости к формированию модели угроз могут привлекаться лицензиаты ФСБ России, являющиеся разработчиками криптосредств или специализированными организациями, проводящими тематические исследования криптосредств.

2.6. Модель угроз может быть пересмотрена:

- по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

3 Методология формирования модели угроз

3.1 Общие принципы

Разработка модели угроз должна базироваться на следующих принципах:

1) Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (п. 2.2 Методических рекомендаций).

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

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) Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

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

6) Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

7) Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

В случае отсутствия готовых сертифицированных криптосредств, функционально пригодных для обеспечения безопасности персональных данных при их обработке в конкретной информационной системе, на этапе аванпроекта или эскизного (эскизно-технического) проекта разработчиком информационной системы с участием оператора и предполагаемого разработчика криптосредства готовится обоснование целесообразности разработки нового типа криптосредства и определяются требования к его функциональным свойствам.

Разработка нового типа криптосредства осуществляется в соответствии с Положением ПКЗ-2005.

Различают модель угроз верхнего уровня и детализированную модель угроз.

Модель угроз верхнего уровня предназначена для определения характеристик безопасности защищаемых персональных данных и других объектов защиты (принципы 2 и 3). Эта модель также определяет исходные данные для детализированной модели угроз.

Детализированная модель угроз предназначена для определения требуемого уровня криптографической защиты.

3.2 Методология формирования модели угроз верхнего уровня

Формирование модели угроз верхнего уровня осуществляется на этапе сбора и анализа исходных данных по информационной системе в соответствии с установленным Порядком.

Для правильного определения криптосредств, необходимых для обеспечения безопасности персональных данных, дополнительно к данному этапу предъявляются следующие требования.

Определение условий создания и использования персональных данных

Должны быть описаны условия создания и использования персональных данных. Для этого определяются:

- субъекты, создающие персональные данные (в качестве такого субъекта может выступать лицо или его представитель в виде программного или технического средства);

- субъекты, которым персональные данные предназначены;

- правила доступа к защищаемой информации;

- информационные технологии, базы данных, технические средства, используемые для создания и обработки персональных данных;

- используемые в процессе создания и использования персональных данных объекты, которые могут быть объектами угроз, создающими условия для появления угроз персональным данным. Такого рода объектами могут быть, например, технические и программные средства.

Степень детализации описания должна быть достаточной для выполнения остальных требований к этапу сбора и анализа исходных данных по информационной системе.

Описание форм представления персональных данных

Персональные данные имеют различные формы представления (формы фиксации) с учетом используемых в информационной системе информационных технологий и технических средств.

Необходимо дать описание этих форм представления (форм фиксации) персональных данных. К таким формам относятся области оперативной памяти, файлы, записи баз данных, почтовые отправления и т.д.

Описание информации, сопутствующей процессам создания и использования персональных данных

На основе анализа условий создания и использования персональных данных должна быть определена информация, сопутствующая процессам создания и использования персональных данных. При этом представляет интерес только та информация, которая может быть объектом угроз и потребует защиты.

К указанной информации, в частности, относится:

- ключевая, аутентифицирующая и парольная информация криптосредства;

- криптографически опасная информация (КОИ);

- конфигурационная информация;

- управляющая информация;

- информация в электронных журналах регистрации;

- побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация;

- резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов;

- остаточная информация на носителях информации.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться приведенными выше примерами информации, сопутствующей процессам создания и использования персональных данных.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить указанный выше перечень информации, сопутствующей процессам создания и использования персональных данных, с приведением соответствующих обоснований. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

Уточнение перечня информации, сопутствующей процессам создания и использования персональных данных, должно осуществляться путем:

- исключения типов рассматриваемой информации из указанного выше перечня, которые являются избыточными в силу специфики конкретной информационной системы;

- конкретизации и детализации не исключенных типов рассматриваемой информации с учетом конкретных условий эксплуатации информационной системы;

- описания типов рассматриваемой информации, не указанных в приведенном выше перечне.

Определение характеристик безопасности

Необходимо определить характеристики безопасности не только персональных данных, но и характеристики безопасности всех объектов, которые были определены как возможные объекты угроз.

Основными (классическими) характеристиками безопасности являются конфиденциальность, целостность и доступность.

В дополнение к перечисленным выше основным характеристикам безопасности могут рассматриваться также и другие характеристики безопасности. В частности, к таким характеристикам относятся неотказуемость[35], учетность[36] (иногда в качестве синонима используется термин «подконтрольность»), аутентичность[37] (иногда в качестве синонима используется термин «достоверность») и адекватность38.

Приведенный список характеристик безопасности не является исчерпывающим. Возможность большого числа характеристик безопасности кроется в определении понятия «характеристика безопасности объекта»:

«**характеристика безопасности объекта** – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства».

Как правило, условия создания и существования реальных объектов достаточно сложны и, как следствие, к ним можно предъявить достаточно много самых различных требований.

Так как угроза безопасности объекта – возможное нарушение характеристики безопасности объекта, то перечень всех характеристик безопасности для всех возможных объектов угроз, по сути, определяет модель угроз верхнего уровня.

Например, если в информационной системе требуется обеспечить только защиту от уничтожения, целостность и доступность защищаемой информации (в качестве возможного примера такой информационной системы можно привести информационную систему школьного учителя, содержащую общедоступные персональные данные учащихся), то модель угроз верхнего уровня содержит следующий перечень угроз:

- угроза уничтожения защищаемой информации;

- угроза нарушения целостности защищаемой информации;

- угроза нарушения доступности защищаемой информации.

3.3 Методология формирования детализированной модели угроз

Согласно приведенному в Законе Российской Федерации «О безопасности» определению понятия «угроза безопасности», необходимо определить совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз. Это и есть содержание работ по созданию детализированной модели угроз.

Можно привести примеры, когда целесообразно создание моделей угроз нескольких уровней детализации.

Очевидным примером может служить объект угроз, представляющий сложную территориально распределенную автоматизированную систему, для которой условия функционирования различных составных частей системы могут существенно различаться. При анализе такой системы, как правило, используется принцип декомпозиции сложного объекта. Если же составные части системы также весьма сложны, то их анализ снова потребует использование принципа декомпозиции сложного объекта. В рассматриваемом случае целесообразно создание моделей угроз для каждого объекта, получающегося в процессе декомпозиции.

При определении угроз безопасности объекта следует различать:

- угрозы, не являющиеся атакой;

- атаки.

Рекомендуется использовать следующую структуру угроз, не являющихся атаками:

- *угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления* (землетрясения, наводнения, ураганы и т.д.);

- *угрозы социально–политического характера*: забастовки, саботаж, локальные конфликты и т.д.;

- *ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз.* Если, например, в качестве объекта угроз выступает автоматизированная система в защищенном исполнении (АСЗИ), то к таким действиям и нарушениям, в частности, относятся:

о непредумышленное искажение или удаление программных компонентов АСЗИ;

о внедрение и использование неучтенных программ;

о игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации. В частности:

- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);

- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;

- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;

- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

- *угрозы техногенного характера,* основными из которых являются:

о аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.);

о неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.;

о помехи и наводки, приводящие к сбоям в работе аппаратных средств.

Следует отметить, что, как правило, защита от угроз, не являющихся атаками, в основном регламентируется инструкциями, разработанными и утвержденными операторами с учетом особенностей эксплуатации информационных систем и действующей нормативной базы.

Как показал мировой и отечественный опыт, атаки являются наиболее опасными угрозами (что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак).

Атаки готовятся и проводятся нарушителем, причем возможности проведения атак обусловлены возможностями нарушителя. Иными словами, конкретные возможности нарушителя определяют конкретные атаки, которые может провести нарушитель.

Но тогда с учетом определения понятия «модель нарушителя» все возможные атаки определяются моделью нарушителя.

Модель нарушителя тесно связана с моделью угроз и, по сути, является ее частью. Смысловые отношения между ними следующие. В модели угроз содержится максимально полное описание угроз безопасности объекта. Модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

3.4 Методология формирования модели нарушителя

Согласно последнему из определенных в п. 3.1 Методических рекомендаций принципу (принцип 7) нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредств и СФК).

Этапы разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК

На этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК обработка персональных данных не производится. Поэтому объектами атак могут быть только сами эти средства и документация на них.

В связи с изложенным на указанных этапах возможны следующие атаки:

- внесение негативных функциональных возможностей в технические и программные компоненты криптосредства и СФК, в том числе с использованием вредоносных программ (компьютерные вирусы, «троянские кони» и т.д.);

- внесение несанкционированных изменений в документацию на криптосредство и технические и программные компоненты СФК.

Необходимо отметить, что указанные атаки:

- на этапах разработки, производства и транспортировки технических и программных средств криптосредства и СФК могут проводиться только вне зоны ответственности оператора;

- на этапе хранения технических и программных средств криптосредства и СФК могут проводиться как в зоне, так и вне зоны ответственности оператора;

- на этапе ввода в эксплуатацию технических и программных средств криптосредства и СФК могут проводиться в зоне ответственности оператора.

В связи с изложенным операторы должны предусмотреть меры контроля:

- соответствия технических и программных средств криптосредства и СФК и документации на эти средства, поступающих в зону ответственности оператора, эталонным образцам (например, оператор должен требовать от поставщиков гарантий соответствия технических и программных средств криптосредства и СФК и документации на эти средства, поступающих в зону ответственности оператора, эталонным образцам или механизмы контроля, позволяющие оператору установить самостоятельно такое соответствие);

- целостности технических и программных средств криптосредства и СФК и документации на эти средства в процессе хранения и ввода в эксплуатацию этих средств (с использованием как механизмов контроля, описанных в документации, например, на криптосредство, так и с использованием организационных и организационно-технических мер, разработанных оператором с учетом требований соответствующих нормативных и методических документов – см. п. 2.1 Методических рекомендаций).

Этап эксплуатации технических и программных средств криптосредства и СФК

Атака как любое целенаправленное действие характеризуется рядом существенных признаков. К этим существенным признакам на этапе эксплуатации технических и программных средств криптосредства и СФК вполне естественно можно отнести:

- нарушителя - субъекта атаки;

- объект атаки;

- цель атаки;

- имеющуюся у нарушителя информацию об объекте атаки;

- имеющиеся у нарушителя средства атаки;

- канал атаки.

Возможные объекты атак и цели атак определяются на этапе формирования модели угроз верхнего уровня.

При определении объектов атак, в частности, должны быть рассмотрены как возможные объекты атак и при необходимости конкретизированы с учетом используемых в информационной системе информационных технологий и технических средств следующие объекты:

- документация на криптосредство и на технические и программные компоненты СФК;

- защищаемые персональные данные;

- ключевая, аутентифицирующая и парольная информация;

- криптографически опасная информация (КОИ);

- криптосредство (программные и аппаратные компоненты криптосредства);

- технические и программные компоненты СФК;

- данные, передаваемые по каналам связи;

- помещения, в которых находятся защищаемые ресурсы информационной системы.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться приведенными выше примерами возможных объектов атак.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить указанный выше перечень возможных объектов атак с приведением соответствующих обоснований. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

Уточнение перечня возможных объектов атак должно осуществляться путем:

исключения объектов атак из указанного выше перечня, которые являются избыточными в силу специфики конкретной информационной системы;

конкретизации и детализации не исключенных объектов атак с учетом конкретных условий эксплуатации информационной системы;

описания объектов атак, не указанных в приведенном выше перечне.

С учетом изложенного модель нарушителя для этапа эксплуатации технических и программных средств криптосредства и СФК должна иметь следующую структуру:

- описание нарушителей (субъектов атак);

- предположения об имеющейся у нарушителя информации об объектах атак;

- предположения об имеющихся у нарушителя средствах атак;

- описание каналов атак.

Описание нарушителей (субъектов атак)

1) Различают шесть основных типов нарушителей: H_1, H_2, ... , H_6.

Предполагается, что нарушители типа H_5 и H_6 могут ставить работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и СФК.

Возможности нарушителя типа H_{i+1} включают в себя возможности нарушителя типа H_i (1 i 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 i 6).

2) Данный раздел модели нарушителя должен содержать:

- перечень лиц, которые не рассматриваются в качестве потенциальных нарушителей, и обоснование этого перечня (при необходимости);

- предположение о невозможности сговора нарушителей *(для всех типов нарушителей)* или предположения о возможном сговоре нарушителей и о характере сговора, включая перечисление дополнительных возможностей, которые могут использовать находящиеся в сговоре нарушители для подготовки и проведения атак *(для нарушителей типа H_4 - H_6)*.

Примечание

Данный раздел модели нарушителя имеет следующее типовое содержание.

Сначала все физические лица, имеющие доступ к техническим и программным средствам информационной системы, разделяются на следующие категории:

- *категория I – лица, не имеющие права доступа в контролируемую зону информационной системы;*

- *категория II – лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы.*

Далее все потенциальные нарушители подразделяются на:

- *внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационной системы;*

- *внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационной системы.*

Констатируется, что:

- *внешними нарушителями могут быть как лица категория I, так и лица категория II;*

- *внутренними нарушителями могут быть только лица категории II.*

Дается описание привилегированных пользователей информационной системы (членов группы администраторов), которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.

Далее следует обоснование исключения тех или иных типов лиц категории II из числа потенциальных нарушителей. Как правило, привилегированные пользователи информационной системы исключаются из числа потенциальных нарушителей.

И, наконец, рассматривается вопрос о возможном сговоре нарушителей.

Предположения об имеющейся у нарушителя информации об объектах атак

Данный раздел модели нарушителя должен содержать:

- предположение о том, что потенциальные нарушители обладают всей информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

- обоснованные ограничения на степень информированности нарушителя (перечень сведений, в отношении которых предполагается, что они нарушителю недоступны).

Примечание

Обоснованные ограничения на степень информированности нарушителя могут существенно снизить требования к криптосредству при его разработке.

При определении ограничений на степень информированности нарушителя, в частности, должны быть рассмотрены следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;

- долговременные ключи криптосредства;

- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.);

- сведения о линиях связи, по которым передается защищаемая информация;

- все сети связи, работающие на едином ключе;

- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;

- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств криптосредства и СФК;

- сведения, получаемые в результате анализа любых сигналов от технических средств криптосредства и СФК, которые может перехватить нарушитель.

Только нарушителям типа H_3 - H_6 могут быть известны все сети связи, работающие на едином ключе.

Только нарушители типа H_5 - H_6 располагают наряду с доступными в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения.

Только нарушители типа H_6 располагают все документацией на криптосредство и СФК.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться приведенным выше предположением о том, что потенциальные нарушители обладают всей информацией, необходимой для подготовки и проведения атак.

Разработчики модели угроз - специалисты в области защиты информации могут подготовить обоснованные ограничения на степень информированности нарушителя. Рекомендуется указанное ограничение делать только в случае необходимости разработки нового типа криптосредства.

Предположения об имеющихся у нарушителя средствах атак

Данный раздел модели нарушителя должен содержать:

- предположение о том, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну;

- обоснованные ограничения на имеющиеся у нарушителя средства атак.

Примечание

Обоснованные ограничения на имеющиеся у нарушителя средства атак могут существенно снизить требования к криптосредству при его разработке.

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, должны быть рассмотрены:

- аппаратные компоненты криптосредства и СФК;

- доступные в свободной продаже технические средства и программное обеспечение;

- специально разработанные технические средства и программное обеспечение;

- штатные средства.

Нарушители типа H_1 и H_2 располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК.

Дополнительные возможности нарушителей типа H_3-H_5 по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер.

Нарушители типа H_6 располагают любыми аппаратными компонентами криптосредства и СФК.

Нарушители типа H_1 могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны.

Возможности нарушителей типа H_2-H_6 по использованию штатных средств зависят от реализованных в информационной системе организационных мер.

Нарушители типа H_4-H_6 могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться только приведенными выше средствами атак.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить приведенный выше перечень средств атак. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

Описание каналов атак

С практической точки зрения этот раздел является одним из важнейших в модели нарушителя. Его содержание по существу определяется качеством формирования модели угроз верхнего уровня.

Основными каналами атак являются:

- каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами;

- штатные средства.

Возможными каналами атак, в частности, могут быть:

- каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);

- машинные носители информации;

- носители информации, выведенные из употребления;

- технические каналы утечки;

- сигнальные цепи;

- цепи электропитания;

- цепи заземления;

- канал утечки за счет электронных устройств негласного получения информации;

- информационные и управляющие интерфейсы СВТ.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться только приведенными выше основными каналами атак.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить приведенный выше перечень каналов атак. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

Определение типа нарушителя

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.

Рекомендуется при отнесении оператором нарушителя к типу H_6 согласовывать модель нарушителя с ФСБ России.

4 Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

4.1. 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 предъявляемых к криптосредствам требований, и, соответственно, шесть классов криптосредств, также обозначаемых через КС1, КС2, КС3, КВ1, КВ2, КА1.

Уровень криптографической защиты персональных данных, обеспечиваемой криптосредством, определяется оператором путем отнесения нарушителя, действиям которого должно противостоять криптосредство, к конкретному типу.

При отнесении заказчиком нарушителя к типу H_1 криптосредство 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.

4.2. Различают три уровня КС, КВ и КА специальной защиты от утечки по каналам побочных излучений и наводок при защите персональных данных с использованием криптосредств.

При отнесении нарушителя к типу H_1-H_3 должна быть обеспечена специальная защита по уровню КС, к типу H_4-H_5 – по уровню КВ, к типу H_6 – по уровню КА.

4.3. В случае принятия оператором решения о защите персональных данных в информационной системе от несанкционированного доступа в соответствии с нормативными документами ФСБ России различают шесть уровней АК1, АК2, АК3, АК4, АК5, АК6 защиты от несанкционированного доступа к персональным данным в информационных системах, определенных в порядке возрастания количества и жесткости предъявляемых к системам защиты требований, и, соответственно, шесть классов информационных систем, также обозначаемых через АК1, АК2, АК3, АК4, АК5, АК6.

При отнесении заказчиком нарушителя к типу H_1 в информационной системе должна быть обеспечена защита от несанкционированного доступа к персональным данным по

уровню АК1, к типу $Н_2$ – по уровню АК2, к типу $Н_3$ – по уровню АК3, к типу $Н_4$ – по уровню АК4, к типу $Н_5$ – по уровню АК5, к типу $Н_6$ – по уровню АК6.

5 Требования к контролю встраивания криптосредства

5.1. Встраивание криптосредств класса КС1 и КС2 осуществляется без контроля со стороны ФСБ России (если этот контроль не предусмотрен техническим заданием на разработку (модернизацию) информационной системы).

Встраивание криптосредств класса КС3, КВ1, КВ2 и КА1 осуществляется только под контролем со стороны ФСБ России.

5.2. Встраивание криптосредств класса КС1, КС2 или КС3 может осуществляться либо самим пользователем криптосредства при наличии соответствующей лицензии ФСБ России, либо организацией, имеющей соответствующую лицензию ФСБ России.

Встраивание криптосредства класса КВ1, КВ2 или КА1 осуществляется организацией, имеющей соответствующую лицензию ФСБ России.

5.3. В ходе контроля со стороны ФСБ России встраивания криптосредства могут решаться, в частности, следующие задачи:

- проверка требований документации на криптосредство, относящихся к встраиванию криптосредства, в том числе:

o анализ корректности встраивания;

o анализ правильности функционирования системы управления ключами;

- экспериментальная проверка работоспособности криптосредства и правильности выполнения возложенных на него целевых функций;

- оценка влияния технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства, на выполнение предъявляемых к криптосредству требований.

Методика и программа контроля встраивания криптосредства разрабатываются и (или) обосновываются специализированной организацией, проводящей тематические исследования криптосредства, и согласовываются с ФСБ России.

---

[1] ГОСТ 34.003-90.

[2] ГОСТ Р 51624-2000.

[3] Закон Российской Федерации "О безопасности".

[4] Федеральный закон «О персональных данных».

[5] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[6] Закон Российской Федерации "О безопасности".

[7] В. Дорот, Ф. Новиков «Толковый словарь современной компьютерной лексики», СПб., БХВ-Петербург, 2004.

[8] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[9] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[10] Федеральный закон «О персональных данных».

[11] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[12] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[13] Федеральный закон «О персональных данных».

[14] ГОСТ Р 51624-2000.

[15] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[16] Федеральный закон «О персональных данных».

[17] «Положение о разработке, производстве, реализации и шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», зарегистрировано Минюстом России (регистрационный № 6382 от 3 марта 2005 года)

[18] Данное определение является обобщением определения понятия «недокументированные (недекларированные) возможности ПО», приведенного в Руководящем документе Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларируемых возможностей» (введен в действие Приказом Председателя Гостехкомиссии России №114 от 04.06.1999).

[19] Закон Российской Федерации "О безопасности".

[20] Федеральный закон «О персональных данных».

[21] Федеральный закон «Об информации, информационных технологиях и о защите информации».

[22] Федеральный закон «О персональных данных».

[23] Федеральный закон «О персональных данных».

[24] ГОСТ Р 51275-99.

[25] Федеральный закон «О персональных данных».

[26] Федеральный закон «О персональных данных».

[27] Федеральный закон «О персональных данных».

[28] ГОСТ Р 50922-96.

[29] ГОСТ Р 50739-95.

[30] Федеральный закон «О персональных данных».

[31] Закон Российской Федерации "О безопасности".

[32] Федеральный закон «О персональных данных».

[33] Постановление Правительства Российской Федерации от 23 сентября 2002 года № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» (Собрание законодательства Российской Федерации, 2002 г., № 39, ст. 3792).

[34] Собрание законодательства Российской Федерации 2007, № 48, часть II, ст. 6001.

[35] **Неотказуемость** – способность доказать, что действие или событие произошло таким образом, что факт действия или события не может быть опровергнут (ИСО 7498–2:99 и ИСО 13888–1:2004).

[36] **Учетность**

– свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта (ИСО 7498–2:99);

– обеспечение того, что действия субъекта по отношению к объекту могут быть прослежены уникально по отношению к субъекту.

[37] **Аутентичность**

– свойство обеспечения идентичности субъекта или ресурса заявленной идентичности. Аутентичность применяется к таким субъектам как пользователи, процессы, системы и информация (ISO/IEC 13335–1:2004);

– идентичность объекта тому, что заявлено.

[38] **Адекватность** – свойство соответствия преднамеренному поведению и результатам (ISO/IEC 13335–1:2004).