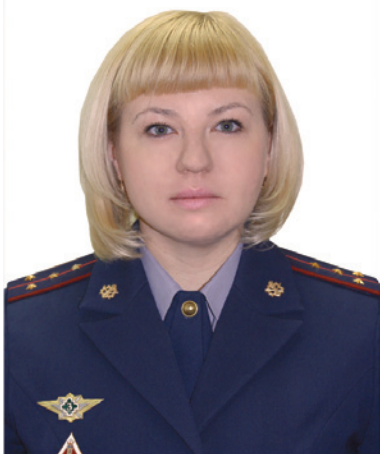

Система сертификации средств защиты информации в Российской Федерации

Бочкарева Татьяна Олеговна,
старший инженер отдела аттестации объектов информатизации центра технической защиты и обработки информации ФКУ НИИИТ ФСИН России, капитан внутренней службы

Основной задачей режима обработки информации ограниченного доступа является обеспечение ее информационной безопасности. Главная цель создания системы защиты информации — ее надежность. Понимая важность этого направления и обладая определенной ответственностью перед обществом, государство на законодательном уровне ввело контроль качества технических, криптографических, программных и других средств, которые могут использоваться для защиты информации ограниченного доступа. Указанный контроль осуществляется посредством сертификации средств защиты информации.

Под сертификацией понимается форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров [1]. Сертификация средств защиты информации прежде всего подразумевает проверку их качественных характеристик для реализации основной функции — защиты информации на основании государственных стандартов и требований по безопасности информации.

Статья 5 Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании» ставит особняком вопросы технического регулирования в отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну.

Тем самым, различные виды сведений, отнесенных к категории ограниченного доступа, предполагают наличие нормативных документов для соответствующих средств защиты информации.

Так например, закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне» определяет сертификацию как единственную форму оценки соответствия средств защиты информации. Статья 28 Закона гласит, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. При этом организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Тем самым детализация требований по организации соответствующих систем сертификации возложена, соответственно, на ФСТЭК России, ФСБ России и Минобороны России.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам.

Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции.

Целями создания системы сертификации являются:

- реализация требований Закона Российской Федерации «О государственной тайне»;
- реализация требований государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам;
- создание условий для качественного и эффективного обеспечения потребителей сертифицированной техникой защиты информации;
- обеспечение национальной безопасности Российской Федерации в информационной сфере;
- содействие формированию рынка защищенных информационных технологий и средств их обеспечения;
- формирование и осуществление единой научно-технической и промышленной политики в информационной сфере с учетом современных требований по про-

тиводействию техническим разведкам и технической защите информации.

К средствам защиты информации относятся технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, и иной информации ограниченного доступа, в которых эти средства реализованы, а также средства контроля эффективности защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Вместе с тем средства антивирусной защиты являются элементом систем защиты информации информационных систем, функционирующих на базе вычислительных сетей или на базе автономных рабочих мест, и применяются совместно с другими средствами защиты информации от несанкционированного доступа к информации в информационных системах [5].

Обязательной сертификации подлежат средства защиты информации:

- предназначенные для защиты сведений, составляющих государственную тайну, а также другой информации с ограниченным доступом, подлежащей защите в соответствии с действующим законодательством;
- систем управления экологически опасными производствами, объектами, имеющими важное оборонное или экономическое значение и влияющими на безопасность государства;
- средства общего применения, предназначенные для противодействия техническим разведкам.

Согласно положениям пункта 8 статьи 14 Федерального закона «Об информации, информационных технологиях и о защите информации», технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

В настоящее время одним из основных руководящих документов по сертификации средств защиты информации является Положение о сертификации средств защиты информации, утвержденное постановлением Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации».

Организационную структуру системы сертификации образуют:

- федеральный орган по сертификации средств защиты информации;
- центральный орган системы сертификации средств защиты информации;
- органы по сертификации средств защиты информации;
- испытательные центры (лаборатории);
- заявители.

При этом процедура сертификации средств защиты информации может быть представлена следующими этапами:

1. Подача заявки в орган по сертификации средств защиты информации.

Законодательством Российской Федерации предусмотрена возможность сертификации средств защиты информации отечественного производства и признание зарубежного сертификата средств защиты информации. Важным условием сертификации средств защиты информации изготовителем является обязательность наличия у него лицензии на соответствующий вид деятельности. Согласно пункту 8 Положения о сертификации средств защиты информации, изготовитель для получения сертификата должен направить в орган по сертификации средств защиты информации заявку на проведение сертификации, к которой могут быть приложены схема ее проведения, государственные стандарты и иные нормативные и методические документы, требованиям которых должны соответствовать сертифицируемые средства защиты информации. В случае необходимости признания зарубежного сертификата, изготовитель направляет его копию и заявку на признание сертификата в федеральный орган по сертификации.

Заявка оформляется на бланке заявителя и заверяется печатью.

2. Проверка и рассмотрение представленных документов.

При сертификации средств защиты информации орган по сертификации в месячный срок после получения заявки направляет изготовителю решение о проведении сертификации с указанием схемы ее проведения, испытательной лаборатории, осуществляющей испытания средств защиты информации, и нормативных документов, требованиям которых должны соответствовать сертифицируемые средства защиты информации.

Если изготовитель обратился в федеральный орган по сертификации с заявкой о признании зарубежного сертификата, то в срок не позднее одного месяца после получения указанных документов федеральный орган по сертификации извещает его о признании сертификата или необходимости проведения сертификационных испытаний.

3. Назначение и проведение сертификации средств защиты информации по выбранной схеме.

Основными схемами проведения сертификации средств защиты информации являются:

- для единичных образцов средств защиты информации — проведение испытаний этих образцов на соответствие требованиям по защите информации;
- для серийного производства средств защиты информации — проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований.

Кроме того, Положением о сертификации средств защиты информации допускается предварительная проверка производства по специально разработанной программе. Сертификация импортируемых средств защиты информации проводится по тем же правилам, что действительны и для отечественных СЗИ.

Согласно указанному Положению, сроки проведения испытаний устанавливаются договором между изготовителем и испытательной лабораторией.

4. Принятие решения о выдаче сертификата, о признании зарубежного сертификата или об отказе в его выдаче или признании.

В соответствии с пунктом 6 Положения о сертификации средств защиты информации, испытательные лаборатории по результатам проведенных сертификационных испытаний средств защиты информации оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации средств защиты информации и изготовителям.

При несоответствии результатов испытаний требованиям нормативных и методических документов по защите информации орган по сертификации средств защиты информации принимает решение об отказе в выдаче сертификата и направляет изготовителю мотивированное заключение.

Согласно пункту 9 Положения о сертификации средств защиты информации, «в случае несогласия с отказом в выдаче сертификата изготовитель имеет право обратиться в центральный орган системы сертификации, федеральный орган по сертификации или в Межведомственную комиссию для дополнительного рассмотрения полученных при испытаниях результатов».

5. Оформление сертификата и его выдача изготовителю.

Экспертное заключение вместе с техническим заключением, материалами сертификационных испытаний, комплектом необходимой технической и эксплуатационной документации на средство защиты информации направляется в федеральный орган по сертификации.

После согласования технических условий или формуляра на средства защиты информации и присвоения сертификату регистрационного номера федеральный орган по сертификации оформляет сертификат и выдает его заявителю. Срок действия сертификата не может превышать пяти лет.

Таким образом, получение заявителем сертификата дает ему право получить в федеральном органе по сертификации лицензию на применение знака соответствия. Владелец лицензии (изготовитель средства защиты информации) осуществляет маркирование средств защиты информации знаком соответствия в порядке, установленном правилами системы сертификации, и несет ответственность за поставку маркированных средств защиты информации.

Федеральный орган по сертификации обеспечивает участников сертификации необходимой информацией о деятельности системы сертификации, включающей:

- перечень средств защиты информации (их сертифицированных параметров), на которые выданы сертификаты;
- перечень средств защиты информации (их сертифицированных параметров), на которые действие сертификатов аннулировано;
- перечень органов по сертификации;
- перечень испытательных центров (лабораторий);
- перечень органов по аттестации объектов информатизации;
- перечень нормативных документов, на соответствие требованиям которых проводится сертификация средств защиты информации,
- и методических документов по проведению сертификационных испытаний.

Система сертификации Российской Федерации коренным образом отличается от систем, принятых в других странах. Каждый экземпляр сертифицированного средства защиты информации имеет пакет документов государственного образца о том, что данный продукт является сертифицированным, включая голографический специальный защитный знак соответствия с уникальным номером, который идентифицирует данный экземпляр средства защиты информации в системе государственного учета сертифицированных продуктов.

Список используемых источников:

1. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»;
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне»;
4. Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации»;
5. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России 20.03.2012 № 28.