Цирлов Валентин Леонидович
кандидат технических наук, доцент

Никулин Михаил Юрьевич

Правовые основы сертификации средств защиты информации

Аннотация: *в статье приведен обзор основных законодательных актов и нормативных документов, лежащих в основе сертификации средств защиты информации по требованиям безопасности информации. Рассматривается структура основных систем обязательной сертификации. Проводится сравнительный анализ правовых аспектов организации каждой из систем сертификации.*

Ключевые слова: *техническое регулирование, обязательная сертификация, защита тайн.*

Задача сертификации средств защиты информации по требованиям безопасности информации возникает при построении автоматизированных систем различного уровня во многих отраслях экономики [1]. Несмотря на то, что наиболее сложными при планировании и реализации сертификационных испытаний остаются технические аспекты, правовые особенности данного вида работ также имеют ряд нюансов и заслуживают отдельного рассмотрения.

В основе любого рода деятельности по оценке соответствия, и, в частности, сертификации средств защиты информации лежит Федеральный закон от 27.12.2002 г. №184-ФЗ «О техническом регулировании». В данном законе под подтверждением соответствия понимается документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров. В свою очередь, одной из форм подтверждения соответствия является сертификация. В области информационной безопасности под сертификацией понимают деятельность третей стороны по подтверждению характеристик средств защиты информации требованиям нормативных документов по защите информации [10].

При этом Статья 5 названного ранее Закона №184-ФЗ 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 (см. Таблицу 1), предполагают наличие различных нормативных требований для соответствующих средств защиты информации [3,4]. Впрочем, на практике большая часть перечисленных в Таблице 1 видов тайн рассматривается просто как конфиденциальная

информация, особняком стоят вопросы организации сертификационных испытаний средств защиты информации, предназначенных для защиты государственной тайны, персональных данных, а также ряда более специфических видов защищаемой информации [14].

Так, например закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной

Таблица 1

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Государственная тайна	Статья 5 Закона РФ от 21.07.1993 N 5485-1 «О государственной тайне»
	Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»
Коммерческая тайна	Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»
	Статья 12 Федерального закона от 28.11.2011 № 335-ФЗ «Об инвестиционном товариществе»
Персональные данные	Статья 7 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»
Прочие виды тайн	Соответствующие законы РФ

тайне» определяет именно сертификацию как единственную форму оценки соответствия таких средств защиты. Статья 28 Закона № 5485-1 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. Все системы сертификации имеют схожую организационную структуру, указанную на рис. 1.

В ряде случаев федеральный орган выполняет роль органа по сертификации. Как правило, схема проведения сертификации выглядит следующим образом:

Заявитель (это либо разработчик, либо другая компания, заинтересованная в проведении сертификации) подает в федеральный орган по сертификации заявку на проведение сертификационных испытаний некоторого продукта.

Федеральный орган определяет испытательную лабораторию и орган по сертификации.

Испытательная лаборатория, находясь в постоянном контакте с заявителем, проводит сертификационные испытания. Если в процессе испытаний выявляются те или иные несоответствия заявленным требованиям, то они могут быть устранены заявителем в рабочем порядке – что происходит в большинстве случаев, или

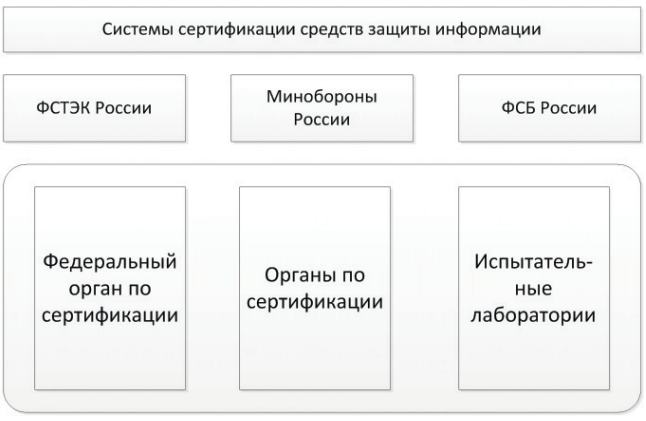

Рис.1. Обобщенная структура основных систем сертификации

же может быть принято решение об изменении требований к продукту – например, о снижении класса защищенности. Безусловно, возможен вариант, когда сертификационные испытания завершаются с отрицательным результатом.

Детальные протоколы испытаний передаются в орган по сертификации, который проводит их независимую экспертизу. Как правило, в данной экспертизе участвуют не менее двух экспертов, которые независимо друг от друга должны подтвердить, что испытания проведены корректно и в полном объеме [10].

Федеральный орган по сертификации на основании заключения органа по сертификации оформляет сертификат соответствия.

Следует сказать, что заявитель на сертификацию должен иметь лицензию на право работы в области создания средств защиты информации, а испытательная лаборатория и орган по сертификации – соответственные аттестаты аккредитации [15].

Что касается документов, на соответствие которым проводятся сертификационные испытания, то они практически идентичны во всех системах сертификации. Существуют два основных подхода к сертификации – и, соответственно, два типа нормативных документов [11].

Функциональное тестирование средств защиты информации, позволяющее убедиться в том, что продукт действительно реализует заявленные функции. Такое тестирование чаще всего проводится на соответствие конкретному нормативному документу – например, одному из руководящих документов Гостехкомиссии России. Такие документы существуют, например, для межсетевых экранов, для средств защиты от несанкционированного доступа. Если же не существует документа, которому сертифицируемый продукт соответствовал бы в полной мере, то функциональные требования могут быть сформулированы в явном виде – например, в Технических условиях, или в виде Задания по безопасности (в соответствии с положениями стандарта ГОСТ Р 15408). В системе сертификации ФСТЭК России для ряда классов СЗИ (в частности, для систем обнаружения вторжений и антивирусов) разработаны современные нормативные документы на базе «Общих критериев» [2–5].

Тестирование программного кода на отсутствие недекларированных возможностей – т.е. возможностей, не описанных или не соответствующих описанным в документации [8]. Классическим примером недекларированных возможностей являются программные закладки - внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию [7,9,13]. Выявление недекларированных возможностей предполагает проведение определенных тестов в отношении исходных текстов программного обеспечения – соответственно, предоставление исходных текстов является необходимым условием для возможности проведения сертификационных испытаний [6].

В большинстве случаев средство защиты информации должно быть сертифицировано как в части основного функционала, так и на предмет отсутствия недекларированных возможностей.

Важным моментом сертификации является выбор схемы сертификации, а именно: партии (одного или нескольких изделий) или серии (типового образца). В случае серии организация-заявитель должна дополнительно пройти спецэкспертизу по проверке возможности осуществлять производство средств защиты информации. В настоящее время Техническим комитетом по стандартизации ТК-362 «Защита информации» проводятся изыскания по формированию требований к системам менеджмента информационной безопасности в части управления безопасным производством программных СЗИ [1,16].

В заключение необходимо отметить, что на сегодняшний день фактически не существует процедуры взаимного признания сертификатов соответствия между различными системами сертификации средств защиты информации – существуют лишь единичные случаи, когда решение о возможности использования материалов испытаний, полученных в рамках работ в другой системе, принимается федеральным органом по сертификации в индивидуальном порядке. На наш взгляд, разработка системы унификации требований могла бы стать интересным направлением нормотворческой деятельности.

Литература

1. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1(1). – С.37–41.
2. Барабанов А.В., Марков А.С., Фадин А.А. Сертификация программ без исходных тек-

стов // Открытые системы. СУБД. 2011. № 4. – С.38–41.
3. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. – С.31–33.
4. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2012. Спецвыпуск №5 «Информатика и системы управления». – С.272–278.
5. Барабанов В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. – С. 48–52.
6. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1(2). – С. 40–48.
7. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). – С. 60–65.
8. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия Южного федерального университета. Технические науки. 2006. Т. 62. № 7. – С. 82–87.
9. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1(1). – С.42–48.
10. Марков А.С., Цирлов В.Л. Сертификация программ: мифы и реальность // Открытые системы. СУБД. 2011. № 6. – С.26–29.
11. Марков А.С., Цирлов В.Л., Маслов В.Г., Олексенко И.А. Тестирование и испытания программного обеспечения по требованиям безопасности информации // Известия Института инженерной физики. 2009. Т.2, №12. – С.2–6.
12. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). – С.61–64.
13. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1(2). – С. 36–39.
14. Федичев А.В., Артамошин С.А. Систематизация видов отношений и ответственности при получении доступа к информации // Вопросы кибербезопасности. 2014. № 2 (3). – С. 51–59.
15. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации // Вопросы кибербезопасности. 2013. № 1(1). – С.49–54.
16. Шахалов И.Ю., Дорофеев А.В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. – С. 4–14.