

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОРГАНИЗАЦИИ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Ю.С.Балабан
*Руководитель испытательной лаборатории
ЗАО НПЦ «Модуль»*

Сертификационные испытания средств защиты информации (СЗИ) в системе сертификации Министерства обороны Российской Федерации проводятся с учетом требований следующих основных руководящих и нормативно-методических документов:

- Постановления Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;
- «Положения о системе сертификации средств защиты информации Министерства обороны Российской Федерации по требованиям безопасности информации», введенного в действие приказом Министра обороны Российской Федерации;
- Постановления Государственного комитета Российской Федерации по стандартизации и метрологии (Госстандарта России) от 23 августа 1999 года № 44 «Об утверждении Правил по сертификации «Оплата работ по сертификации продукции и услуг».

Испытательной лабораторией проводятся два типа работ, а именно, сертификационные испытания продукции и инспекционный контроль.

Сертификационные испытания включают в себя следующие основные работы:

- рассмотрение руководством ИЛ заявки;
- получение Решения органа по сертификации СЗИ;
- назначение руководителей работ, экспертиза документов, приложенных к Решению;
- выбор, согласование и утверждение исполнителей по отдельным видам работ из штатных сотрудников и лиц, привлекаемых по договорам;
- подготовка комплекта договорных документов на проведение сертификационных испытаний;
- согласование комплекта договорных документов с заявителем, заключение договора на проведение сертификационных испытаний;
- отбор образцов продукции;
- разработка Программы проведения сертификационных испытаний;
- разработка Методик проведения сертификационных испытаний;
- согласование и утверждение разработанных документов;
- проведение сертификационных испытаний;
- оформление протоколов и технических заключений по результатам испытаний.

Кроме того, осуществляется экспертиза документов и проверка производства. При проведении экспертизы по документам проводятся прием, входной контроль и регистрация документов, собственно экспертиза комплекта документов, прилагаемых к заявке, и подготовка экспертного заключения по заявке.

В процессе инспекционного контроля проводятся следующие работы:

- оформляется акт отбора образца. При отборе образца составляется перечень комплектов продукции, на которые будет распространяться продленный сертификат;
- осуществляется передача продукции с документацией на нее заявителем в испытательную лабораторию с составлением акта приема-передачи;
- разрабатываются проекты программы и методик инспекционного контроля;
- согласовываются проекты программы и методик инспекционного контроля с заявителем и органом по сертификации с последующим утверждением разработанных документов органом по сертификации;
- проводятся проверки в части документации, в том числе факта отражения в документации изменений и доработок; влияния изменений, внесенных в продукцию; показателей защищенности; функциональных возможностей продукции; соответствия исходных текстов предъявленному загрузочному коду и т.д.; оформляются протоколы инспекционного контроля, техническое заключение и акт инспекционного контроля;
- предоставляются итоговые документы заявителю и органу по сертификации;
- возвращается испытательной лабораторией продукция с документацией на нее заявителю с составлением акта приема-передачи.

К основным организационным проблемам, возникающим при проведении сертификации продукции по требованиям безопасности информации, относятся следующие.

Руководящие указания по конструированию должны определять перечень допустимых технических средств, на которых ведется разработка программного обеспечения, а также версию операционной системы, средств разработки, перечень библиотечных модулей. Отсутствие документированных сведений может оказаться проблемой при оформлении акта идентификации среды разработки.

Отсутствие действующих сертификатов соответствия требованиям безопасности информации на составные компоненты продукции является существенной проблемой при проведении испытаний. Поэтому необходимо Разработчику продукции уже на этапе проектирования определиться, кто и как будет предъявлять заимствованные составные компоненты на сертификацию. Если на заимствованные компоненты имеются сертификаты соответствия требованиям безопасности информации, то следует убедиться, что сертифицированные заимствованные компоненты по своим характеристикам безопасности информации могут использоваться в составе комплексного продукта, с учетом его характеристик безопасности информации. У разработчика (Заявителя сертификационных испытаний) в обязательном порядке должны иметься копии сертификатов соответствия на составные (заимствованные) компоненты.

Сертификация продукции в целом предполагает и сертификацию составных изделий. Заявка на сертификацию продукции в целом может завершиться выдачей ряда сертификатов, в том числе и на составные компоненты (если это реально требуется и отдельно оговаривается в техническом заключении испытательной лаборатории по результатам сертификационных испытаний). Поэтому, наличие сертифицированных составных компонентов при подаче Заявки на сертификацию продукции в целом является не обязательным условием. Сертификация составных частей в одной лаборатории при последующей сертификации продукции в целом в другой лаборатории потребует больших временных и материальных затрат.

Следующая проблема - отсутствие документации на изделие в объеме требований системы сертификации. Согласно действующим нормативным документам, при выполнении ОКР Исполнитель утверждает у Заказчика перечень рабочей конструкторской и эксплуатационной документации, впускаемой в рамках ОКР. Однако, если в ТТЗ на ОКР задается последующая сертификация продукции на соответствие требованиям безопасности информации, необходимо учесть, что для сертификации продукции требуются отдельные документы, наличие которых устанавливается положениями ГОСТ и иных нормативных документов в области сертификации и защиты информации, которые могут быть не указаны в перечне, согласованном Заказчиком.

Принципиальной проблемой принятой процедуры сертификации является отсутствие учета политики безопасности использования программного продукта в рамках объекта информатизации. Необходимо решать проблемы организации сертификации программных продуктов с постоянно изменяющимся кодом или, например, когда неизвестен правообладатель продукта или фрагментов кода, разработчик находится за рубежом и распространяет продукт бесплатно.

Кажется также спорным вопрос проведения сертификационных испытаний АС по соответствию реальных и декларируемых в документации функциональных возможностей в рамках «Системы сертификации средств защиты информации Министерства обороны Российской Федерации по требованиям безопасности информации». В этом случае часто дублируются работы при проведении государственных и сертификационных испытаний. Наверное, целесообразно засчитывать, если это возможно, результаты проведенных государственных испытаний, и не проводить такие работы в сертификационных испытаниях.

К финансовым проблемам проведения сертификационных испытаний продукции относятся следующие.

Значительные временные задержки в оплате проведенных ИЛ работ, так как в договоре на проведение испытаний почти всегда присутствует фраза, что «Заказчик выплачивает аванс (или полный расчет за работу) в размере до 50% от стоимости работ, при условии получения денежных средств от Генерального заказчика». Получение денежных средств от Генерального заказчика может затягиваться на долгие месяцы.

Следующая проблема заключается в занижение реальной стоимости работ по сертификационным испытаниям продукции. ИЛ самостоятельно в соответствии с действующим законодательством определяет трудоемкость и стоимость работ. При этом следует руководствоваться действующими нормативно-методическими документами, имея ввиду, что цена работ (по данным мировой практики) при проведении сертификационных испытаний составляет в среднем 15 процентов от стоимости разработки продукции. При расчете стоимости сертификационных испытаний следует помнить про устранение замечаний, выявленных в процессе сертификационных испытаний, которые могут приводить не только к корректировке РКД и эксплуатационной документации, но и к разработке новой версии программного обеспечения, и, следовательно, дополнительным испытаниям.