Практический опыт проведения сертификации по «Общим критериям»

***Марков А.С.**, канд.техн.наук, ст.науч.сотр., CISSP;*
***Цирлов В.Л.**, CISSP*

С переходом систем обязательной сертификации средств защиты информации (СЗИ) на использование нормативного аппарата ГОСТ Р ИСО/МЭК 15408-2002 «ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (более известный как «Общие критерии») связывалось и до сих пор связывается множество надежд. Основные из них относятся к ожидаемому отказу от устаревших руководящих документов (РД) Гостехкомиссии России.

Известно, что «Общие критерии» задумывались как метастандарт, направленный на создание гибких и динамичных нормативных и технологических документов (профиль защиты, задание по безопасности), включающих как требования по безопасности, так и требования к качеству изделия. Стандарт, кроме решения задач унификации систем сертификации и адекватности требований к объекту сертификации, должен был решать насущные задачи сертификации, в первую очередь: сократить время сертификации версий программ, обеспечить информированность участников сертификации, снизить затраты вообще при заданной достоверности результата самой сертификации [2].

Первый опыт сертификации двух продуктов (сетевого сканера XSpider 7 по ОУД3 и межсетевого экрана CheckPoint по ОУД1), а также участие в ряде НИР по тематике «Общих критериев» позволил авторам получить ряд независимых практических результатов, направленных на преодоление трудностей, связанных с новизной данного направления. К слову сказать, у авторов имеется твердая уверенность в возможности решения теоретических проблем нормативной базы в рамках данного направления, например, возможность использования аппарата «Общих критериев» в процессе контроля отсутствия недекларированных возможностей затронута в [1].

В докладе будут рассмотрены достоинства «Общих критериев», как универсальность, гибкость, масштабируемость, международный характер стандарта, изначально позволяющий несколько упростить процедуру сертификации СЗИ зарубежного производства. При этом важно осветить трудности, возникшие в ходе реальной жизни при проведении первичных

сертификационных испытаний продуктов по «Общим критериям», и соответственно раскрыть пути их преодоления. Отметим некоторые из них.

1. Возрастание первоначальной трудоёмкости сертификационных испытаний. Разработчик (или заявитель) при проведении первичной сертификации в соответствии с «Общими критериями» должен выполнить весьма значительный объём работ. В абсолютном большинстве случаев заявители и разработчики испытывают трудности при подготовке полноценных материалов для проведения сертификации по «Общим критериям» и не имеют реальной возможности подготовить соответствующие материалы. В результате подготовка материалов отдаётся на откуп специалистам сертификационной лаборатории, что не всегда легитимно с точки зрения методологии проведения сертификационных испытаний.

2. Неопределённый статус сертификации. В настоящее время сертификация по «Общим критериям» должна проводиться пока для продуктов, предназначенных для обработки конфиденциальной информации. Одновременно продукты такого рода могут проходить сертификацию на соответствие традиционным РД Гостехкомиссии России – и поскольку последний вариант является гораздо более быстрым и дешевым, у потребителя нет мотивации для проведения сертификации по требованиям «Общих критериев». Кроме того, в процессе аттестации или сертификации АС имеется неясность при трактовке статуса сертифицированных по «Общим критериям» продуктов, если они декларируются как СЗИ, входящие в состав автоматизированной системы.

3. Неоднозначность толкования определённых положений «Общих критериев». В докладе будут прокомментированы моменты, допускающие неоднозначное толкование со стороны экспертов, а именно:

- полнота отчётной документации;
- язык описания предположений, угроз, политик и целей безопасности;
- выбор оценочного уровня доверия;
- функциональные требования безопасности и требования доверия, формулируемые в явном виде;
- детализация краткой спецификации объекта оценки;
- ссылки на профили защиты;
- глубина логического обоснования разделов профилей защиты и заданий по безопасности.

Отметим, что перечисленные трудности ни в коей мере не умаляют достоинства «Общих критериев» - безусловно, наиболее эффективного оценочного стандарта из всех ныне существующих в данной области. В качестве базовых подходов к решению указанных проблем можно предложить следующие меры:

- перманентный отказ от проведения сертификационных испытаний СЗИ на соответствие традиционным РД Гостехкомиссии России;
- формирование *широкого рынка* независимых консалтинговых услуг по подготовке продукции к сертификации по требованиям «Общих критериев»;
- разработка полноценной системы сопутствующей методической документации, регламентирующей практические аспекты реализации отдельных положений «Общих критериев».

Литература

1. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия ТРТУ, 2006. - № 7. - С. 82-87.

2. Леденко С.А., Марков А.С. и□ др□ Статистика внедрения «Общих критериев» в зарубежных странах // InformationSecurity, 2006. - № 1-2. - С.12-15.