

Особенности сертификации продуктов и ИТ-систем на основе Общих критериев

Применение Общих критериев при проведении сертификации продуктов и систем информационных технологий по требованиям безопасности информации имеет ряд особенностей по сравнению с применяемыми ранее нормативными документами Гостехкомиссии (ФСТЭК) России образца 1992 года. Обзору этих особенностей и посвящена данная статья.

А. А. Сидак, к. т. н., с. н. с.,
начальник научно-методического отдела
Центра безопасности информации
sidak@bk.ru

Основные особенности

1. Оценка проводится не на соответствие универсальным требованиям руководящих документов Гостехкомиссии (ФСТЭК) России или разработанным разработчиком технических условий, а на соответствие так называемым заданиям по безопасности (табл. 1), содержащим как исходные предпосылки (угрозы безопасности, предположения, политику безопасности организации), так и собственно требования безопасности, выполняемые объектом оценки, и его функциональные возможности. Задание по безопасности (ЗБ) создается разработчиком продукта или системы информационных технологий (ИТ), как правило, в соответствии с выбранным профилем защиты (ПЗ), содержащим необходимый объем требований для данного типа изделий ИТ.

2. Оценка проводится на основе Общей методологии оценки, содержащей порядок действий (по шагам) для всех видов и подвидов деятельности по оценке. Сочетание Общих критериев (ОК) и Общей методологии оценки (ОМО) обеспечивает возможность единого подхода к оценке и получения объективных и повторяемых результатов (см. врезку).

3. Основная работа по подготовке исходных данных для оценки (табл. 2) – свидетельств, содержащих проектную, тестовую, эксплуатационную документацию, свидетельств их полноты, непротиворечивости, безопасности и др., возлагается на разработчика.

4. Основной задачей оценщика является независимая, объективная оценка безопасности объекта оценки в соответствии с заявленным оценочным уровнем доверия путем проведения активного исследования представленных свидетельств и независимого тестирования объекта оценки (ОО). Практический опыт подготовки и проведения сертификационных испытаний свидетельствует о том, что сроки и качество проведения испытаний во многом зависят от качества подготовки разработчиком (заявителем) свидетельств оценки и особенно задания по безопасности, что является простой задачей.

5. По результатам испытаний оценщик составляет технический отчет об оценке (рис. 1), на основе которого орган по сертификации выпускает публичный отчет о сертификации (рис. 2) продукта или системы информационных технологий и выдает соответствующий сертификат.



Табл. 1. Содержание задания по безопасности

№	Наименование раздела
1	ВВЕДЕНИЕ ЗБ
1.1	Идентификация ЗБ
1.2	Аннотация ЗБ
1.3	Соответствие Общим критериям
2	ОПИСАНИЕ ОБЪЕКТА ОЦЕНКИ
3	СРЕДА БЕЗОПАСНОСТИ ОБЪЕКТА ОЦЕНКИ
3.1	Угрозы безопасности
3.2	Политика безопасности организации
3.3	Предположения безопасности
4	ЦЕЛИ БЕЗОПАСНОСТИ
4.1	Цели безопасности для объекта оценки
4.2	Цели безопасности для среды
5	ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ
5.1	Функциональные требования
5.2	Требования доверия
5.3	Требования безопасности для среды ИТ
6	КРАТКАЯ СПЕЦИФИКАЦИЯ ОБЪЕКТА ОЦЕНКИ
6.1	Функции безопасности объекта оценки
6.2	Меры доверия
7	УТВЕРЖДЕНИЕ О СООТВЕТСТВИИ ПЗ
7.1	Ссылка на ПЗ
7.2	Уточнение ПЗ
7.3	Дополнение ПЗ
8	ОБОСНОВАНИЕ
8.1	Обоснование целей безопасности
8.2	Обоснование требований безопасности
8.3	Обоснование краткой спецификации объекта оценки
8.4	Обоснование утверждения о соответствии ПЗ

Табл. 2. Состав исходных материалов, предъявляемых разработчиком изделия при проведении оценки по ОК

№ п/п	Исходные данные	Оценочный уровень доверия (EAL)						
		1	2	3	4	5	6	7
1	Задание по безопасности	+	+	+	+	+	+	+
2	Модель политики безопасности объекта оценки (модель защиты)	-	-	-	+	+	=	=
3	Функциональная спецификация	+	=	=	+	+	=	+
4	Проект верхнего уровня (эскизный проект)	-	+	+	=	+	+	+
5	Проект нижнего уровня (технический проект)	-	-	-	+	=	+	=
6	Представление реализации (исходные тексты программ)	-	-	-	+	+	+	=
7	Свидетельство анализа соответствия между краткой спецификацией объекта оценки и функциональной спецификацией	+	=	=	=	+	=	+
8	Свидетельство анализа соответствия между функциональной спецификацией и проектом верхнего уровня	-	+	=	=	+	=	+
9	Свидетельство анализа соответствия между проектом верхнего уровня и проектом нижнего уровня	-	-	-	+	+	=	+
10	Свидетельство анализа соответствия между проектом нижнего уровня и представлением реализации	-	-	-	+	+	=	+
11	Руководство администратора	+	=	=	=	=	=	=
12	Руководство пользователя	+	=	=	=	=	=	=
13	Процедуры безопасной инсталляции, генерации и запуска	+	=	=	=	=	=	=
14	Документация определения жизненного цикла	-	-	-	+	+	=	+
15	Документация инструментальных средств разработки	-	-	-	+	+	+	=
16	Документация безопасности разработки	-	-	+	=	=	+	=
17	Документация управления конфигурацией	-	+	+	+	+	+	=
18	Процедуры поставки	-	+	=	+	=	=	+
19	Объект оценки, предназначенный для поставки	+	+	=	=	=	=	=
20	Тестовая документация	-	+	=	=	=	+	=
21	Процедуры тестирования	-	+	=	=	=	=	=
22	Свидетельство анализа покрытия тестами	-	+	+	=	=	+	=
23	Свидетельство анализа глубины тестирования	-	-	+	=	+	=	+
24	Свидетельство анализа возможности неправильного применения руководств	-	-	-	+	=	=	=
25	Свидетельство анализа утверждений о стойкости функций безопасности	-	+	=	=	=	=	=
26	Свидетельство анализа уязвимостей	-	+	=	+	+	+	=
27	Свидетельство анализа скрытых каналов	-	-	-	-	+	+	=

Обозначения:

«-» – не требуется;

«+» – требуется, требуется с дополнениями;

«=» – требования совпадают с требованиями предыдущего уровня.

Принципы ОМО

- Объективность** – результаты оценки основываются на фактических свидетельствах и не зависят от личного мнения оценщика.
- Беспристрастность** – результаты оценки являются непредубежденными, когда требуется субъективное суждение.
- Воспроизводимость** – действия оценщика, выполняемые с использованием одной и той же совокупности поставок для оценки, всегда приводят к одним и тем же результатам.

- Корректность** – действия оценщика обеспечивают точную техническую оценку.
- Достаточность** – каждый вид деятельности по оценке осуществляется до уровня, необходимого для удовлетворения всех заданных требований доверия.
- Приемлемость** – каждое действие оценщика способствует повышению доверия, по меньшей мере, пропорционально затраченным усилиям.

Технический отчет об оценке	
Введение	
Описание архитектуры ОО	
Оценка	
Результаты оценки	
Выводы и рекомендации	
Перечень свидетельств оценки	
Перечень сокращений/гlossарий терминов	
Сообщение о проблемах	

Рис. 1. Содержание технического отчета об оценке

Отчет о сертификации	
Аннотации	
Идентификация	
Политика безопасности	
Предложения и пояснения области использования	
Информация по архитектуре	
Документация	
Тестирования продукта ИТ	
Оцениваемая конфигурация	
Комментарии/рекомендации оценщика	
Приложения	

Рис. 2. Содержание отчета о сертификации

Практические результаты сертификации продуктов и систем информационных технологий на основе Общих критериев

Впервые в России по Общим критериям был сертифицирован межсетевой экран «Z-2» серия В, разработчиком которого является ЗАО «Инфосистемы Джет» (Москва). Сертификация меж сетевого экрана проводилась на соответствие заданию по безопасности, где был заявлен весьма высокий оценочный уровень доверия (ОУД) 4+. Процесс сертификации этого продукта растянулся примерно на восемь месяцев, из них подготовка и проведение оценки в испытательной лаборатории Центра безопасности информации отняли шесть с половиной месяцев. Сравнительно более продолжительный срок подготовки и проведения испытаний (по сравнению с сертификацией МЭ «Z-2» серия В по РД Гостехкомиссии при Президенте Российской Федерации для МЭ) объясняется отсутствием у разработчика аналогов задания по безопасности, документов свидетельств и опыта их разработки, а у оценщиков – отработанных методик и опыта проведения испытаний в соответ-

ствии с Общей методологией оценки (рабочие методики обрабатывались в ходе проведения испытаний), а также опыта разработки итоговых документов (в частности, технического отчета об оценке).

Особенностью сертификации следующего продукта, занявшей около пяти месяцев (операционной системы Windows XP Professional Service Pack 1) по Общим критериям являлось отсутствие возможности получения от разработчика (заявителя) полного комплекта документации (проектной, тестовой) и свидетельств. Поэтому сертификация осуществлялась по сравнительно низкому оценочному уровню доверия (ОУД 1+), минимально необходимому для использования продукта при обработке конфиденциальной информации.

Далее испытательной лабораторией Центра безопасности информации были проведены сертификационные испытания программного продукта корпорации Symantec – меж сетевого экрана Symantec Enterprise Firewall v.7.0.4. Испытания включали контроль отсутствия недекларированных возможностей по соответствующему РД Гостехкомиссии России для 4-го уровня контроля и проводились на основе анализа исходных текстов программ у разработчика в городе Waltham (США). Параллельно разработчиком был подготовлен и представлен в испытательную лабораторию (впервые для зарубежных ИТ-продуктов) полный комплект исходных свидетельств, включая проектную, тестовую, эксплуатационную документацию, документацию управления конфигурацией и обеспечения безопасности разработки, свидетельство анализа уязвимостей и др. Представленные исходные данные были необходимы для оценки продукта по самому высокому для обычных коммерческих продуктов оценочному уровню доверия ОУД 4. Процесс сертификации этого продукта занял примерно четыре месяца.

Полный перечень ИТ-продуктов, сертифицированных в России по Общим критериям, представлен в табл. 3.

№ п/п	Сертификат	Продукт	Задание по безопасности	ОУД
1	№ 806 (13.11.2003)	МЭ «Z-2», серия В (производство)	ДЖЕТ.Z-2.B.3Б	4+ (усиленный)
2	№ 844 (22.01.2004)	MS Windows XP Prof. SP1a (300 экз.)	MS.Win_XP_SP1a.3Б	1+ (усиленный)
	№ 844/1 (28.06.2004)	(производство)	MS.Win_XP_SP1a.3Б	
	№ 844/2 (03.12.2004)	(производство)	MS.Win_XP.3Б	
3	№ 908 (17.05.2004)	Symantec Enterprise Firewall 7.0.4 (200 экз.)	Sym.SEF_7.0.4.3Б	4
4	№ 925/1 (30.11.2004)	Aladdin eToken Pro (производство)	ALD.ETN-SL.3Б	1+ (усиленный)
5	№ 941 (29.07.2004)	CSP VPN Gate, версия 1.1 (50 экз.)	S-Terra. VPN_Gate_1.1.3Б	3
	№ 941/1 (01.03.2005)	CSP VPN Gate, версия 2.0 (150 экз.)	S-Terra. VPN_Gate_2.0.3Б	
	№ 941/2 (29.07.2004)	CSP VPN Client, версия 2.0 (300 экз.)	S-Terra. VPN_Client_2.0.3Б	
6	№ 998 (24.03.2005)	СУБД Microsoft SQL Server 2000 Enterprise Edition	MS.SQL_Srv_Ent.3Б	1+ (усиленный)
7	№ 1017 (25.05.2005)	ОС Microsoft Windows 2003 Server Enterprise Edition	MS.Win_Srv2003_Ent.3Б	1+ (усиленный)
8	№ 1019 (24.05.2005)	OEM-версия ОС Microsoft Windows XP Professional	MS.Win_XP.3Б	1+ (усиленный)

Табл. 3. Перечень продуктов, сертифицированных в России по Общим критериям