Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 6 (133)/2004

МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПО ОБЩИМ КРИТЕРИЯМ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПО ОБЩИМ КРИТЕРИЯМ

Марк Кобзарь, Алексей Сидак
ООО "Центр безопасности информации"

СОДЕРЖАНИЕ

1 История вопроса

В 1990 году под эгидой Международной организации по стандартизации (ИСО) и при содействии в дальнейшем государственных организаций США, Канады, Великобритании, Франции, Германии и Нидерландов были развернуты работы по созданию международного стандарта (исторически сложившееся название — Общие критерии) в области оценки безопасности информационных технологий (ИТ). Разработка этого стандарта преследовала следующие основные цели:

- Унификация национальных стандартов в области оценки безопасности ИТ;
- Повышение уровня доверия к оценке безопасности ИТ;
- Сокращение затрат на оценку безопасности ИТ на основе взаимного признания сертификатов.

Общие критерии были призваны обеспечить взаимное признание результатов стандартизованной оценки безопасности на мировом рынке ИТ.

Официальный текст международного стандарта ISO/IEC 15408 [1-3] издан 1 декабря 1999 года. Изменения, внесенные в стандарт на завершающей стадии его принятия, учтены в версии 2.1 Общих критериев (ОК), идентичной стандарту по содержанию. В 2002 году на основе аутентичного текста ISO/IEC 15408 был принят российский стандарт ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» [4-6].

В поддержку стандарта под эгидой ИСО разработан целый ряд нормативно-методических документов. Среди них:

- Руководство по разработке профилей защиты и заданий по безопасности [7];
- Процедуры регистрации профилей защиты [8];
- Общая методология оценки безопасности информационных технологий [9-10].

Что касается первых двух документов, то их аналоги уже есть в России в виде руководящих документов, одобренных в январе 2004 года коллегией Гостехкомиссии России. Настоящая статья посвящена последнему из перечисленных (но далеко не последнему по значению) документу — «Общая методология оценки безопасности информационных технологий» (ОМО).

Общая методология оценки по ОМО — документ, сопровождающий ОК. В ОМО описываются основные действия, которые необходимо выполнить оценщику при проведении оценки безопасности ИТ с использованием критериев и свидетельств оценки, определенных в ОК. ОМО предназначена, главным образом, для оценщиков, использующих ОК, и экспертов органов по сертификации, подтверждающих действия оценщиков. ОМО может быть использована также заявителями на проведение оценки для получения исходной информации, разработчиками продуктов и систем ИТ, профилей защиты (ПЗ) и заданий по безопасности (ЗБ), а также другими сторонами, заинтересованными в обеспечении безопасности ИТ.

Основным лейтмотивом создания ОМО явилась унификация на международном уровне способов и приемов проведения оценки по ОК в целях взаимного признания оценок и, таким образом, устранения накладных расходов, связанных с дублированием оценок продуктов ИТ и профилей защиты.

Несколько слов о взаимном признании оценок. В 1998 году правительственными организациями Канады, Франции, Германии, Великобритании и США было подписано соглашение о взаимном признании оценок (The International Mutual Recognition Arrangement — MRA), полученных на основе Общих критериев. В соответствии с этим Соглашением стороны намеревались признавать сертификаты на продукты и системы ИТ, полученные в странах, присоединившихся к Соглашению, если они получены на основе применения Общих критериев и выданы организациями, удовлетворяющими требованиям Соглашения. Установленные в MRA правила позволяли присоединиться к Соглашению как в виде участника, только признающего сертификаты, выданные в соответствии с ОК, так и в виде участника, выдающего эти сертификаты.

В мае 2000 года представителями уже четырнадцати стран (Канады, Франции, Германии, Великобритании, США, Нидерландов, Италии, Греции, Испании, Швеции, Норвегии, Финляндии, Австралии и Новой Зеландии) было подписано более универсальное (по сравнению с MRA) соглашение CCRA (Arrangement of the Recognition of Common Criteria Certificates in the field of Information Technology Security). Соглашение CCRA значительно расширяет возможности присоединения новых стран-участниц. В 2001 году к соглашению CCRA присоединился Израиль, в 2002 году — Австрия, в 2003 году — Турция, Венгрия и Япония.

Согласно CCRA признание сертификатов ОК должно базироваться на уверенности в том, что оценка безопасности ИТ проводилась с использованием принятых методов оценки безопасности ИТ. В соглашении CCRA в качестве документа по методам оценки определена ОМО.

2 Существующие версии Общей методологии оценки безопасности информационных технологий

Выход первой версии ОМО датирован августом 1999 года. Соответствующий документ носит название «Common Methodology for Information Technology Security Evaluation» и состоит из двух частей:

- Часть 1: Introduction and General Model (Часть 1. Введение и общая модель) [9];
- Часть 2: Evaluation Methodology (Часть 2. Методология оценки) [10].

Отличительной особенностью ОМО версии 1.0 (Часть 2 ОМО) является то, что структуризация действий и шагов оценивания проведена по оценочным уровням доверия (ОУД1-ОУД4).

В то же время отметим, что в ПЗ/ЗБ для продуктов и систем ИТ редко когда какой-либо ОУД используется в «чистом» виде (без компонентов доверия, его дополняющих). Как правило, используется именно ОУД усиленный (то есть некоторый ОУД+), для оценки по которому до конца непонятно, как использовать часть 2 ОМО, то есть как из нее «вырывать» отдельные составляющие (соответствующие дополнительным по отношению к конкретному ОУД компонентам доверия) и как эти составляющие интегрировать в ту часть ОМО, которая относится к конкретному ОУД.

Часть 1 рассматриваемой версии ОМО появилась намного раньше, чем часть 2, а именно в

1997 году, то есть даже раньше, чем версия 2.0 ОК, положенная в основу международного стандарта ISO/IEC 15408. Это привело к тому, что между частями ОМО есть некоторые противоречия, которые следует разрешать в пользу части 2 ОМО и этой частью необходимо руководствоваться. Разработчиками ОМО предполагалось актуализировать часть 1 ОМО и объединить ее с частью 2 ОМО.

В апреле 2002 года вышла ОМО версии 1.1a (не в полном объеме) под названием «Evaluation Methodology for the Common Criteria for Information Technology Security Evaluation».

Новая версия ОМО претерпела ряд существенных изменений:

1. В отличие от предыдущей, указанная версия ОМО [11] не разделена на две части.
2. Структуризация действий и шагов оценивания проведена не по ОУД, а по видам деятельности, соответствующим классам доверия ОК.
3. Существенной переработке в настоящее время подвергаются следующие главы ОМО:
   - глава 3 «Оценка ПЗ»;
   - глава 4 «Оценка ЗБ»;
   - глава 12 «Вид деятельности AVA» (анализ уязвимостей).
4. Добавлены следующие главы:
   - глава 5 «Пакеты доверия»;
   - глава 13 «Поддержка доверия» (AMA).
5. Добавлен подраздел 10.4 «Оценка устранения недостатков» (компоненты семейства ALC_FLR не входят ни в один ОУД и могут быть использованы для дополнения предопределенных ОУД).

ОМО, как и ОК, является динамично развивающимся документом. В версии 1.1a структура ОМО изменена таким образом, чтобы впоследствии охватить все компоненты доверия из части 3 ОК. В рассматриваемом документе учтены также все относящиеся к ОМО интерпретации, выпущенные после выхода версии 1.0 ОМО.

Разработчики ОМО при ее создании руководствовались следующими принципами:

- **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.

Эти принципы нашли отражение при описании представленных в методологии видов деятельности по оценке.

Между структурой ОК (класс — семейство — компонент — элемент) и структурой ОМО (вид деятельности — подвид деятельности — действие — шаг оценивания) была установлена прямая взаимосвязь. Рис. 1 иллюстрирует соответствие между такими конструкциями ОК, как классы, компоненты и элементы действий оценщика, и рассматриваемыми в ОМО видами деятельности, подвидами деятельности и действиями. Вместе с тем, некоторые шаги оценивания ОМО могут прямо следовать из требований ОК, содержащихся в элементах действий разработчика, содержания и представления свидетельств.

В ОМО термин «Вид деятельности» («activity») используется для описания применения класса доверия из части 3 ОК.

Для описания применения компонента доверия из части 3 ОК используется термин «Подвид деятельности» («sub-activity»). Заметим, что семейства доверия прямо не рассматриваются в ОМО, поскольку при проведении оценки всегда используется только один компонент доверия из применяемого семейства.

В свою очередь, с элементом действий оценщика из части 3 ОК связан термин «Действие» («action»). Эти действия или сформулированы в явном виде как действия оценщика, или неявно следуют из действий разработчика (подразумеваемые действия оценщика) в рамках компонентов доверия из части 3 ОК.

Термин «Шаг оценивания» («work unit») описывает неразделимый фрагмент работы по оценке. Каждое действие в ОМО включает один или несколько шагов оценивания, которые сгруппированы по элементам содержания и представления или действий разработчика соответствующего компонента из части 3 ОК. Шаги оценивания представлены в ОМО в том же порядке, что и элементы ОК, из которых они следуют.

Шаги оценивания содержат обязательные действия, которые оценщик должен выполнить, чтобы прийти к заключению.

Текст, сопровождающий шаги оценивания, содержит дальнейшие разъяснения использования формулировок ОК при оценке. Хотя сопроводительный текст не предписывает обязательные ме-

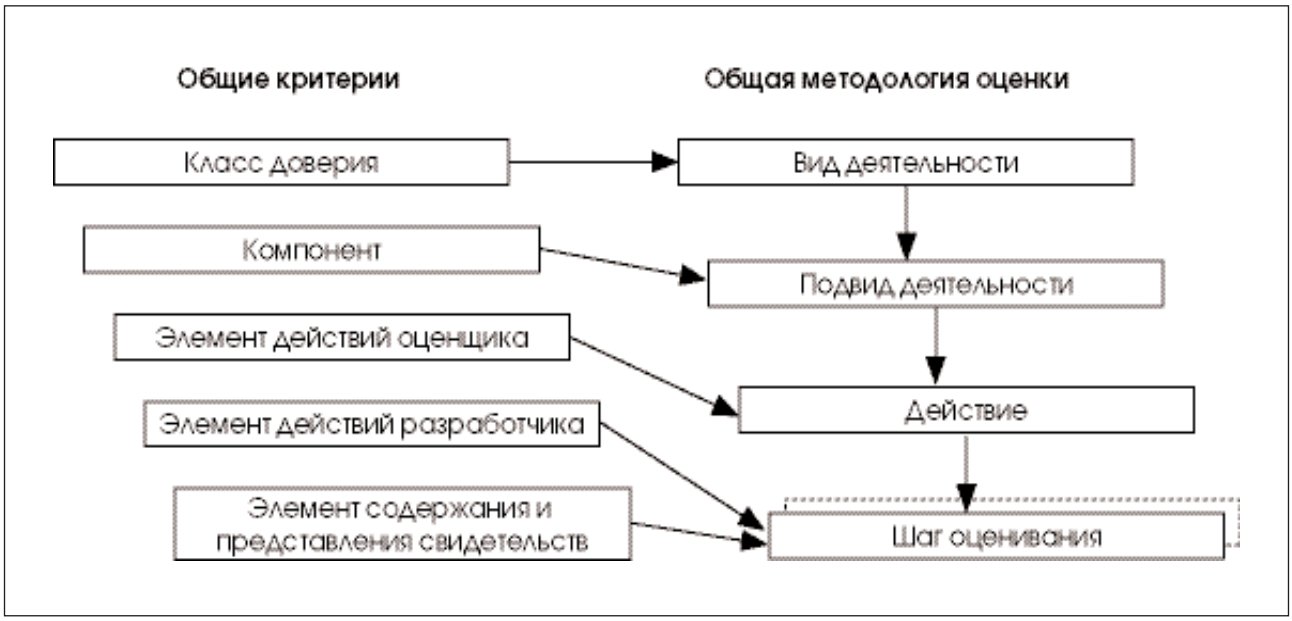

Рис. 1. Соотношение структур ОК и ОМО

ры, он дает представление о том, что ожидается от оценщика при удовлетворении обязательных аспектов шагов оценивания.

ОМО разбита на следующие главы:

Глава 1 *«Введение»* описывает цели, структуру, соглашения и терминологию документа.

Глава 2 *«Процесс оценки и соответствующие задачи»* описывает задачи, которые относятся ко всем видам деятельности по оценке (задачи получения исходных данных для оценки и оформления результатов оценки).

Глава 3 *«Оценка ПЗ»* описывает методологию оценки ПЗ, основанную на классе APE части 3 ОК.

Глава 4 *«Оценка ЗБ»* описывает методологию оценки ЗБ, основанную на классе ASE части 3 ОК. В ОМО не предусмотрено отдельного документа для оформления результатов оценки ЗБ.

Глава 5 *«Пакеты доверия»* представляет обзор выбора и/или конструирования пакетов компонентов доверия.

Главы 6-13 описывают методологию оценивания по классам и компонентам, приведенным в ОК.

Глава 14 *«Общие указания по оценке»* содержит те общие правила оценки (при выборке, анализе непротиворечивости, учете зависимостей, посещении объектов), которые применяются при оценивании более чем по одному классу доверия из ОК.

Приложение А *«Глоссарий»* содержит сокращения, а также словарь терминов и ссылки, используемые в ОМО.

Приложение Б *«Сфера ответственности системы оценки»* содержит перечень вопросов, которые оставлены для решения в системах оценки.

Приложение В *«Границы ОО»* представляет описание терминов, применяемых для идентификации сущности, подлежащей оценке.

Приложение Г *«Запрос на интерпретацию ОМО»* содержит краткое изложение способа подачи запроса на интерпретацию ОМО.

Особенность перерабатываемых глав ОМО состоит в том, что их разработчики помещают проекты этих глав в Интернет на сайт www.commoncriteria.org, объявляют срок приема замечаний и дополнений к ним и впоследствии выпускают эти главы с учетом мнений широкого круга специалистов из разных стран.

3 Процесс оценки

3.1 Общая модель оценки

Согласно ОМО, процесс оценки состоит из выполнения оценщиком задачи получения исходных данных для оценки, подвидов деятельности по оценке и задачи оформления результатов оценки. Рис. 2 дает общее представление о взаимосвязи этих задач и подвидов деятельности по оценке.

Общая модель оценки предусматривает наличие следующих ролей: заявитель, разработчик, оценщик и орган оценки.

Заявитель инициирует оценку, то есть является заказчиком оценки и отвечает за обеспечение оценщика свидетельствами оценки.

Разработчик предъявляет объект оценки (ОО) и отвечает за представление свидетельств, требуемых для оценки (например, проектной документации), от имени заявителя.

Оценщик принимает свидетельства оценки от разработчика от имени заявителя или непосред-

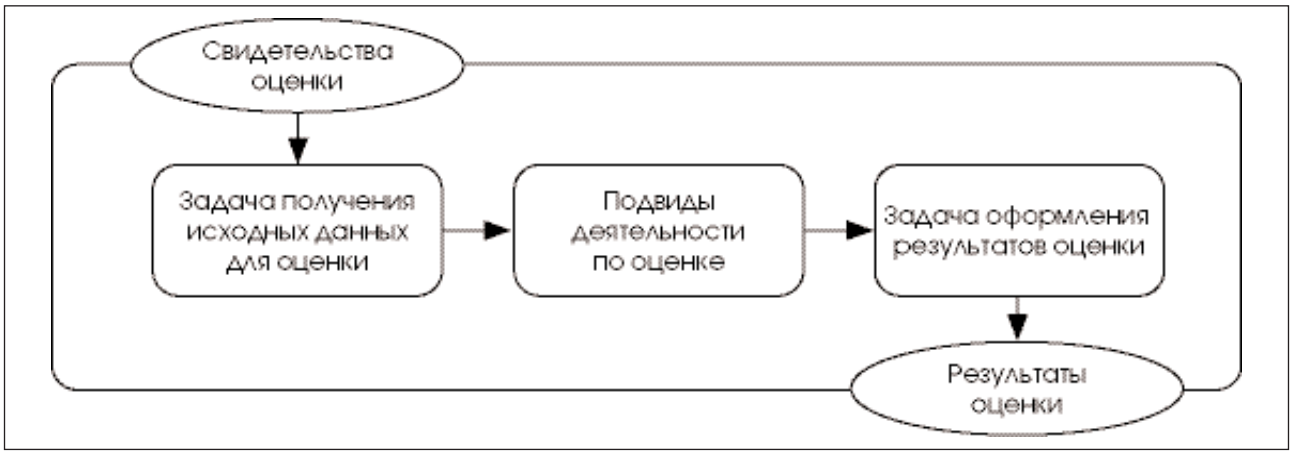

Рис. 2. Общая модель оценки

ственно от заявителя, выполняет подвиды деятельности по оценке и представляет результаты оценки органу оценки.

Орган оценки организует и поддерживает систему оценки, контролирует процесс оценки и выпускает отчеты о сертификации, а также выдает сертификаты, основываясь на результатах, представленных оценщиками.

Для предотвращения негативного влияния на оценку предусматривается определенное разделение ролей, то есть роли, описанные выше, должны выполняться разными организациями. Исключение — возможность выполнения роли разработчика и роли заявителя одной и той же организацией. Кроме того, в некоторых случаях, например, при оценке по ОУД 1, участие разработчика может не требоваться. В этом случае сам заявитель должен представить оценщику как объект оценки, так и необходимые свидетельства оценки.

В ходе проведения оценки оценщик может получить доступ к коммерческой информации заявителя и разработчика (например, информации о конструкции ОО или специализированных инструментальных средствах), а также к информации, являющейся в соответствии с действующим законодательством информацией ограниченного доступа. В этих случаях от оценщика потребуется поддержание конфиденциальности предоставленных ему свидетельств оценки.

Подвиды деятельности по оценке варьируются в зависимости от того, оценивается ПЗ или ОО. Кроме того, при оценке ОО выбор подвидов деятельности зависит от специфицированных в ЗБ требований доверия.

3.2 Особенности выполнения количественных оценок

В настоящее время общеупотребительным подходом к построению критериев оценки безопасности ИТ является использование совокупности определенным образом упорядоченных качественных требований к функциональным механизмам обеспечения безопасности, их эффективности и доверия к реализации.

Качественные критерии применимы для оценки большей части механизмов обеспечения безопасности ИТ, а также оценки выполнения требований доверия к безопасности изделий ИТ. Несмотря на это, ОМО предусматривает возможность проведения, там где это применимо, количественных оценок с использованием соответствующих качественных показателей.

Чтобы корректно использовать количественный показатель, он должен иметь объективную интерпретацию, однозначную зависимость от отдельных аспектов безопасности. Поэтому количественные критерии целесообразно использовать для оценки таких механизмов безопасности, как парольная защита, контрольное суммирование и т.п.

3.2.1 Анализ стойкости функций безопасности, как пример выполнения количественных оценок

В ОК и ОМО применение количественных показателей предусматривается при анализе стойкости функций безопасности ОО, реализованных вероятностными и/или перестановочными механизмами.

В процессе анализа оценщик определяет минимальный потенциал нападения, требуемый нарушителю, чтобы осуществить нападение, и приходит к заключению относительно возможностей ОО противостоять нападению. В табл. 1 демонстрируются и далее описываются взаимосвязи между анализом СФБ и потенциалом нападения.

Анализ стойкости функции безопасности ОО выполняется только для функций безопасности, реализуемых вероятностными или перестановочными механизмами, за исключением тех из них, которые основаны на криптографии. Более того, при

Уровень СФБ	Адекватная защита от нарушителя с потенциалом нападения:	Недостаточная защита от нарушителя с потенциалом нападения:
высокая СФБ	высокий	Не применимо – успешное нападение за пределами практически возможного
средняя СФБ	умеренный	высокий
базовая СФБ	низкий	умеренный

Табл. 1. Стойкость функции безопасности и потенциал нападения

анализе предполагается, что вероятностный или перестановочный механизм безопасности реализован безупречно и что функция безопасности используется при нападении с учетом ограничений ее проекта и реализации. Как показано в табл. 1, уровень СФБ также отражает нападение, описанное в терминах потенциала нападения, для защиты от которого спроектирована функция безопасности.

Потенциал нападения является функцией от мотивации, компетентности и ресурсов нарушителя.

При анализе стойкости функции безопасности предполагается наличие уязвимости в механизмах реализации этой функции безопасности ОО. Чтобы нарушитель мог использовать уязвимость, ему необходимо ее сначала идентифицировать, а затем только использовать. Это разделение может показаться тривиальным, но является существенным.

В ходе анализа потенциала нападения, требуемого для использования уязвимости, необходимо учитывать следующие факторы:

а) **Идентификация:**
   1) время, затрачиваемое на идентификацию уязвимости;
   2) техническая компетентность специалиста;
   3) знание проекта и функционирования ОО;
   4) доступ к ОО;
   5) аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для анализа.

б) **Использование:**
   1) время, затрачиваемое на использование уязвимости;
   2) техническая компетентность специалиста;
   3) знание проекта и функционирования ОО;
   4) доступ к ОО;
   5) аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для использования уязвимости.

Фактор **«Время»** — это время, обычно затрачиваемое нарушителем на непрерывной основе, чтобы идентифицировать или использовать уязвимость. Данный фактор может иметь следующие значения: «за минуты» (при нападении идентификация и использование уязвимости занимает менее получаса); «за часы» (менее чем за день); «за дни» (менее, чем за месяц) и «за месяцы» (нападение требует, по меньшей мере, месяца).

Фактор **«Компетентность специалиста»** относится к уровню общих знаний прикладной области или типа продукта (например, операционной системы, протоколов Интернета). Идентифицированными уровнями компетентности являются следующие:

а) *«Эксперты»* хорошо знакомы с основными алгоритмами, протоколами, аппаратными средствами, структурами и т.п., реализованными в типе продукта или системы, а также с применяемыми принципами и концепциями безопасности;
б) *«Профессионалы»* хорошо осведомлены в том, что касается режима безопасности продукта или системы данного типа;
в) *«Непрофессионалы»* слабо осведомлены, по сравнению с экспертами или профессионалами, и не обладают специфической компетентностью.

Фактор **«Знание ОО»** указывает на определенный уровень знаний об ОО. Оно отличается от общей компетентности, хотя и связано с ней. Идентифицированными уровнями знания ОО являются следующие:

а) *«Отсутствие информации»* об ОО, кроме его назначения;
б) *«Общедоступная информация»* об ОО (например, полученная из руководства пользователя);
в) *«Чувствительная информация»* об ОО (например, сведения о внутреннем содержании проекта).

«Доступ к ОО» также является важным фактором и имеет отношение к фактору «Время». Идентификация или использование уязвимости могут требовать продолжительного доступа к ОО, что может увеличить вероятность обнаружения. Некоторые нападения могут требовать значительных автономных усилий и лишь краткого доступа к ОО для использования уязвимости. Доступ также может быть необходим непрерывный или в виде нескольких сеансов.

Фактор **«Аппаратные средства/программное обеспечение ИТ или другое оборудование»** указывает на оборудование, которое требуется для идентификации или использования уязвимости.

Название фактора	Диапазон	Значение при идентификации уязвимости	Значение при использовании уязвимости
Затрачиваемое время	< 0.5 часа	0	0
	< 1 день	2	3
	< 1месяц	3	5
	> 1месяц	5	8
	Не практично	*	*
Компетентность	Непрофессионал	0	0
	Профессионал	2	2
	Эксперт	5	4
Знание ОО	Отсутствие информации	0	0
	Общедоступная информация	2	2
	Чувствительная информация	5	4
Доступ к ОО	< 0.5 часа или не обнаруживаемый доступ	0	0
	< 1 день	2	4
	< 1 месяц	3	6
	> 1 месяц	4	9
	Не практично	*	*
Оборудование	Отсутствует	0	0
	Стандартное	1	2
	Специализированное	3	4
	Заказное	5	6

* Означает, что нападение невозможно в пределах тех временных рамок, которые были бы приемлемы для нарушителя. Любое значение «*» указывает на противостояние нарушителю с высоким потенциалом нападения.

Табл. 2. Вычисление потенциала нападения

В качестве значений данного фактора рассматриваются следующие виды оборудования:

а) *стандартное оборудование* — это оборудование либо для идентификации уязвимости, либо для нападения, которое легко доступно нарушителю. Это оборудование может быть частью самого ОО (например, отладчик в операционной системе) или может быть легко получено (например, программное обеспечение, загружаемое из Интернета);

б) *специализированное оборудование* не является общедоступным нарушителю, но может быть приобретено нарушителем без значительных усилий. Оно может включать покупку небольшого количества оборудования (например, анализатора протоколов) или разработку более сложных сценариев и программ нападения;

в) *заказное оборудование* — это оборудование, которое либо может потребовать его специальной разработки (например, очень сложное программное обеспечение), либо настолько специализированное, что его распространение контролируется и, возможно, даже ограничено, либо очень дорогое оборудование. Использование сотен персональных компьютеров, связанных через Интернет, как правило, относится к этой категории.

В табл. 2 значениям (диапазонам значений) рассмотренных факторов поставлены в соответствие числовые значения по двум аспектам: идентификации уязвимости и использованию уязвимости.

При определении потенциала нападения для данной уязвимости из каждого столбца (столбцы 2 и 3 табл. 2) для каждого фактора следует выбрать определенное значение (10 значений). При выборе значений должна учитываться предопределенная среда ОО. Выбранные 10 значений суммируются, давая итоговое значение. Это значение затем сверяется с таблицей 3 для определения рейтинга уязвимости и соответственно по таблице 1 — уровня СФБ. Полученный уровень стойкости функции безопасности говорит о том, нарушителю с каким потенциалом противостоит ОО.

Диапазон значений	ОО противостоит нарушителю с потенциалом нападения:
< 10	Нет рейтинга
10-17	Низкий
18-24	Умеренный
> 25	Высокий

Табл. 3. Рейтинг уязвимостей

Когда значение фактора оказывается близким к границе диапазона, то оценщику следует подумать об использовании значения, усредняющего табличные. Например, если для использования уяз-

1. Ограничения на цифровые пароли:

FIA_SOS.1	**Верификация секретов**
FIA_SOS.1.1	ФБО должны предоставить механизм для верификации того, что **пароли** отвечают следующей метрике качества: • цифровой пароль должен быть не менее четырех и не более шести цифр; • последовательные числовые ряды (типа 7,6,5,4,3) не допускаются; • повторение цифр не допускается (каждая цифра должна быть уникальной).

2. Характеристики блокировки терминала:

FIA_AFL.1 (1)	**Обработка отказов аутентификации**
FIA_AFL.1.1	ФБО должны обнаруживать, когда произойдет (очередная) неуспешная попытка аутентификации (для данного терминала с момента последней попытки или с момента последнего сброса счетчика неудачной аутентификации).
FIA_AFL.1.2	При **обнаружении** неуспешной попытки аутентификации ФБО должны увеличить значение счетчика неудачной аутентификации на единицу. При этом сброс (обнуление) счетчика неудачной аутентификации осуществляется через пять минут.
FIA_AFL.1 (2)	**Обработка отказов аутентификации**
FIA_AFL.1.1	ФБО должны обнаруживать, когда произойдет (шесть) неуспешных попыток аутентификации (для данного терминала с момента последней попытки или с момента последнего сброса счетчика неудачной аутентификации).
FIA_AFL.1.2	При достижении **счетчиком неуспешных попыток аутентификации** числа неуспешных попыток аутентификации, определенного **в элементе FIA_AFL.1.1**, ФБО должны выполнить блокирование терминала на один час.

Рис. 3. Функциональные требования безопасности как источник для расчета стойкости функции безопасности

вимости требуется доступ к ОО в течение одного часа или если доступ обнаруживается очень быстро, то для этого фактора может быть выбрано значение между 0 и 4.

Для конкретной уязвимости может возникнуть необходимость сделать несколько проходов (Табл. 2) для различных сценариев нападения (например, попеременно использовать разные значения компетентности в сочетании с определенными значениями факторов времени или оборудования). При этом ориентироваться нужно на наименьшее значение, полученное для этих проходов.

В случае уязвимости, которая уже идентифицирована и информация о которой общедоступна, значения *«при идентификации уязвимости»* нарушителем (столбец 3 табл. 2) следует выбирать, исходя из раскрытия этой уязвимости в общедоступных источниках, а не из начальной ее идентификации нарушителем.

3.2.2 Пример анализа стойкости функции безопасности

Рассмотрим пример анализа СФБ для гипотетического механизма цифрового пароля.

Информация, полученная из ЗБ и свидетельств проекта, показывает, что идентификация и аутентификация предоставляют основу для управления доступом к сетевым ресурсам с терминалов, расположенных далеко друг от друга. Управление физическим доступом к терминалам каким-либо эффективным способом не осуществляется. Управление продолжительностью доступа к терминалу каким-либо эффективным способом не осуществляется. Уполномоченные пользователи системы подбирают себе свои собственные цифровые пароли для входа в систему во время начальной авторизации использования системы и в дальнейшем — по запросу пользователя. Система содержит ограничения на цифровые пароли, выбираемые пользователем. Эти исходные данные получены на основе анализа функциональных требований безопасности из ЗБ (Рис. 3).

Предполагается, что пароли состоят не менее чем из четырех символов, являющихся цифрами. Все цифры должны быть различны. Кроме того, запрещается использовать "явно неслучайные" пароли, представляющие собой последовательно возрастающие или убывающие совокупности цифр (1234, 8765 и т.п.), и не должны быть связаны каким-либо способом с конкретным пользователем, например, с датой рождения.

Число возможных значений цифровых паролей рассчитывается следующим образом:

а) Допуская самый плохой вариант сценария, когда пользователь выбирает число, состоящее только из четырех цифр, число перестановок цифрового пароля (предполагая, что каждая цифра уникальна) равно:
$7*8*9*10 = 5040$

б) Число возможных увеличивающихся рядов — семь, как и число убывающих рядов. После от-

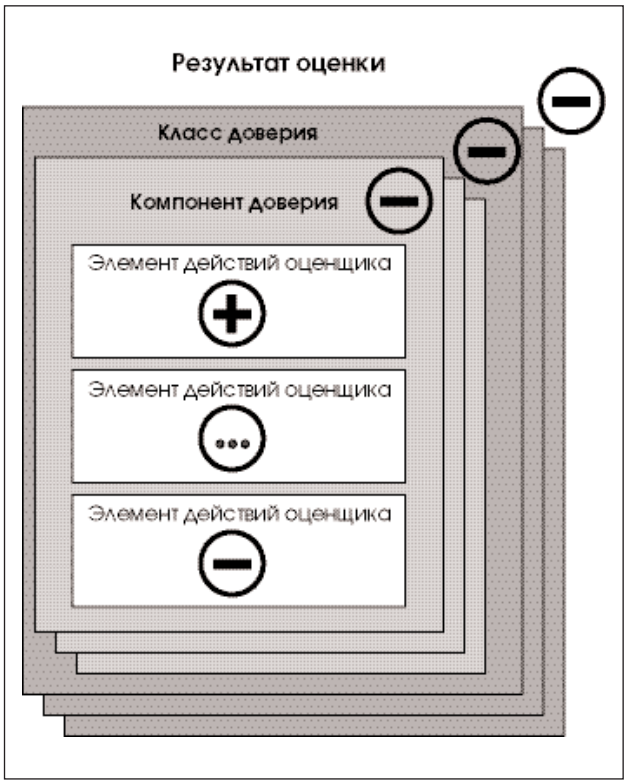

Рис. 4. Пример правила формирования заключения

брасывания этих рядов число возможных значений цифровых паролей равно:

$5040 - 14 = 5026$

Основываясь на дополнительной информации (Рис. 4) в механизме цифрового пароля спроектирована характеристика блокировки терминала. После шестой подряд неудачной попытки аутентификации терминал блокируется на один час. Счетчик неудачной аутентификации сбрасывается через пять минут; таким образом, нарушитель в лучшем случае может осуществить пять попыток ввода цифрового пароля каждые пять минут или 60 вводов цифрового пароля в час.

В среднем нарушитель должен был бы ввести 2513 цифровых комбинаций до ввода правильного цифрового пароля. Как результат, в среднем, успешное нападение произошло бы чуть меньше, чем за

$$\frac{2513 \text{ мин}}{60 \text{ мин/час}} \approx 42 \text{ часа}$$

Используя подход, описанный в п. 3.2.1, следует выбирать значения факторов при идентификации, минимальные из каждой категории (все 0), так как существование уязвимости в рассматриваемой функции очевидно. Основываясь на приведенных выше вычислениях, для непрофессионала является возможным нанести поражение механизму в пределах дней (при получении доступа к ОО) без использования какого-либо оборудования и без знания ОО, что в соответствии с таблицей 2 (для использования уязвимостей) дает значение 11. Получив результирующую сумму — 11, потенциал нападения, требуемый для осуществления успешной атаки, определяется, по меньшей мере, как умеренный.

Поскольку механизм цифрового пароля является стойким к нарушителю с низким потенциалом, то этот механизм цифрового пароля соответствует уровню «базовая СФБ» (Табл. 1).

3.3 Правила формирования заключения по результатам оценки

При выполнении работы по оценке оценщик делает заключения относительно выполнения требований ОК. Наименьшая структурная единица ОК, по которой делается заключение — элемент действий оценщика. Заключение по выполняемому элементу действий оценщика из ОК делается в результате выполнения соответствующего действия из ОМО и составляющих его шагов оценивания.

В ОМО различаются три взаимоисключающих вида заключения:

а) условиями *положительного* заключения являются завершение оценщиком элемента действий оценщика из ОК и определение, что при оценке требования к ПЗ, ЗБ или ОО выполнены. Для элемента условием положительного заключения является успешное завершение всех шагов оценивания, составляющих соответствующее действие из ОМО;

б) условиями *отрицательного* заключения являются завершение оценщиком элемента действий оценщика из ОК и определение, что при оценке требования к ПЗ, ЗБ или ОО не выполнены;

в) все заключения являются *неокончательными* до выдачи *положительного* или *отрицательного* заключения.

Общее заключение положительно тогда и только тогда, когда все составляющие заключения положительны. В примере, показанном на рис. 4, заключение для одного из элементов действий оценщика отрицательно, поэтому заключения для соответствующего компонента доверия, класса доверия и общее заключение также отрицательны.

В результате оценки ОО должна быть установлена степень доверия тому, что ОО соответствует требованиям, а именно:

а) отвечают ли специфицированные функции безопасности ОО функциональным требованиям и, следовательно, эффективны ли они для достижения целей безопасности ОО;

б) правильно ли реализованы специфицированные функции безопасности ОО.

Отметим, что хотя ОМО и предусматривает возможность выполнения количественных оценок, результирующая оценка безопасности ИТ имеет качественное выражение.

3.4 Оформление результатов оценки

Основные выходные результаты оценки оформляются в виде сообщений о проблемах (если это необходимо при выполнении оценки) и технического отчета об оценке (ТОО). Для сообщения о проблеме (СП) и ТОО ОМО определяет лишь содержание минимально необходимой информации и не препятствует включению в эти сообщения (отчеты) дополнительной информации, которая может требоваться в рамках конкретной системы оценки.

Стандартизованное представление результатов оценки облегчает достижение универсального принципа повторяемости и воспроизводимости результатов.

3.4.1 Подготовка СП

СП предоставляют оценщику механизм для запроса разъяснений (например, от органа оценки о применении требований) или для определения проблемы по одному из аспектов оценки (например, запрос на корректировку ЗБ, направляемый заявителю оценки).

Таким образом, СП может использоваться оценщиком как один из способов выражения потребности в разъяснении, либо для отражения результата оценки при отрицательном заключении (окончательном или неокончательном).

Оформляя СП, оценщик должен привести в нем следующую информацию:

а) идентификатор оцениваемого ПЗ или ОО;
б) ссылку на задачу/подвид деятельности по оценке, при выполнении которой/которого была выявлена проблема;
в) суть проблемы;
г) оценку серьезности проблемы (например, приводит к отрицательному заключению, задерживает выполнение оценки или требует решения до завершения оценки);
д) идентификационную информацию организации, ответственной за решение проблемы;
е) рекомендуемые сроки решения проблемы;
ж) влияние на оценку отрицательного результата решения проблемы.

Адресаты рассылки СП и процедуры обработки ими сообщений зависят от характера содержания конкретных сообщений и от указаний со стороны системы оценки.

Основными типами СП являются СП органу оценки и заявителю, но в рамках системы оценки СП могут также различаться по содержанию.

3.4.2 Подготовка ТОО

Результаты оценки отражаются в ТОО, в котором оценщик представляет техническое обоснование сделанных им заключений. Минимальные требования к содержанию ТОО определены в ОМО.

Кроме того, в рамках системы оценки могут устанавливаться дополнительные требования к структуре, содержанию и форме представления информации в ТОО.

При изложении информации в ТОО необходимо исходить из того, что тот, кто будет знакомиться с данным документом, имеет представление об общих концепциях информационной безопасности, ОК, ОМО и подходах к оценке безопасности ИТ.

Основная цель ТОО — помочь органу оценки провести независимую экспертизу и подтвердить результаты оценки.

В ОМО предусмотрены две разновидности ТОО:

- ТОО по результатам оценки ПЗ;
- ТОО по результатам оценки ОО.

Рассмотрим их подробнее.

3.4.2.1 Технический отчет об оценке профиля защиты

Содержание ТОО, отражающего результаты оценки ПЗ, представлено на рис. 5.

В разделе **«Введение»** ТОО оценщик должен привести следующую информацию:

- идентификационную информацию системы оценки, требуемую для однозначной идентификации системы, в рамках которой проводилась оценка ПЗ;
- название, дату составления и номер версии ТОО;
- название, дату составления и номер версии ПЗ;
- идентификационную информацию разработчика ПЗ;
- идентификационную информацию заявителя оценки ПЗ;
- идентификационную информацию оценщика, то есть организации, ответственной за проведение оценки ПЗ и за формирование заключений по результатам оценки.

В разделе **«Оценка»** ТОО оценщик должен привести следующую информацию:

- ссылки на критерии, методологию, технологии и инструментальные средства оценки, использованные при оценке ПЗ;
- сведения о каких-либо ограничениях, имевших место в процессе оценки ПЗ или при обработке результатов этой оценки, а также о предположениях, сделанных в процессе оценки, которые повлияли на ее результаты.

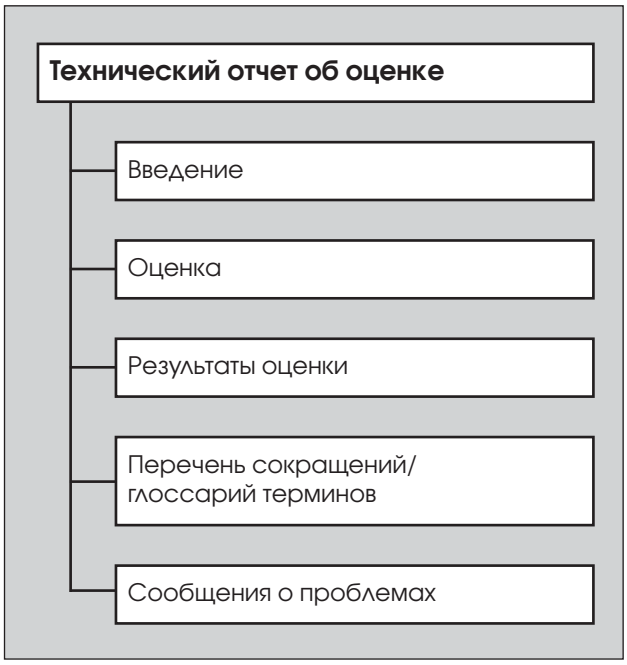

Рис. 5. Содержание ТОО по результатам оценки ПЗ

Кроме того, оценщик может включить в ТОО информацию о каких-либо правовых или законодательных аспектах оценки ПЗ, организации работ по оценке, информацию, связанную с обеспечением конфиденциальности материалов оценки, а также другую информацию.

В разделе **«Результаты оценки»** ТОО оценщик должен привести заключение по каждому из компонентов доверия, определяющих вид деятельности APE «Оценка ПЗ», как результат выполнения соответствующих действий ОМО и составляющих их шагов оценивания. Каждое такое заключение должно сопровождаться надлежащим обоснованием.

В разделе «Выводы и рекомендации» ТОО оценщик должен изложить выводы по результатам оценки ПЗ, установив, является ли ПЗ полным, непротиворечивым, технически правильным и, следовательно, пригодным для изложения требований к ОО, предполагаемому для оценки.

Результат оценки ПЗ в целом должен формулироваться как «соответствие/несоответствие» [4].

При положительном результате оценки должна быть указана степень, с которой можно доверять тому, что ПЗ соответствуют требованиям ОК. Должно поясняться соотношение с функциональными требованиям из части 2 ОК, требованиями доверия из части 3 ОК, как это указано ниже:

а) **соответствие части 2 ОК** — ПЗ соответствует части 2 ОК, если функциональные требования основаны только на функциональных компонентах из части 2 ОК;

б) **расширение части 2 ОК** — ПЗ соответствует расширению части 2, если функциональные требования включают функциональные компоненты, не содержащиеся в части 2;

в) **соответствие части 3 ОК** — ПЗ соответствует части 3 ОК, если требования доверия представлены в виде ОУД из части 3 ОК или пакета требований доверия, включающего только компоненты доверия из части 3 ОК;

г) **усиление части 3 ОК** — ПЗ соответствует усилению части 3 ОК, если требования доверия представлены в виде ОУД или пакета требований доверия и включают другие компоненты доверия из части 3 ОК;

д) **расширение части 3 ОК** — ПЗ соответствует расширению части 3 ОК, если требования доверия представлены в виде ОУД, дополненного требованиями доверия не из части 3 ОК, или пакета требований доверия, который включает требования доверия, не содержащиеся в части 3 ОК, или полностью состоит из них.

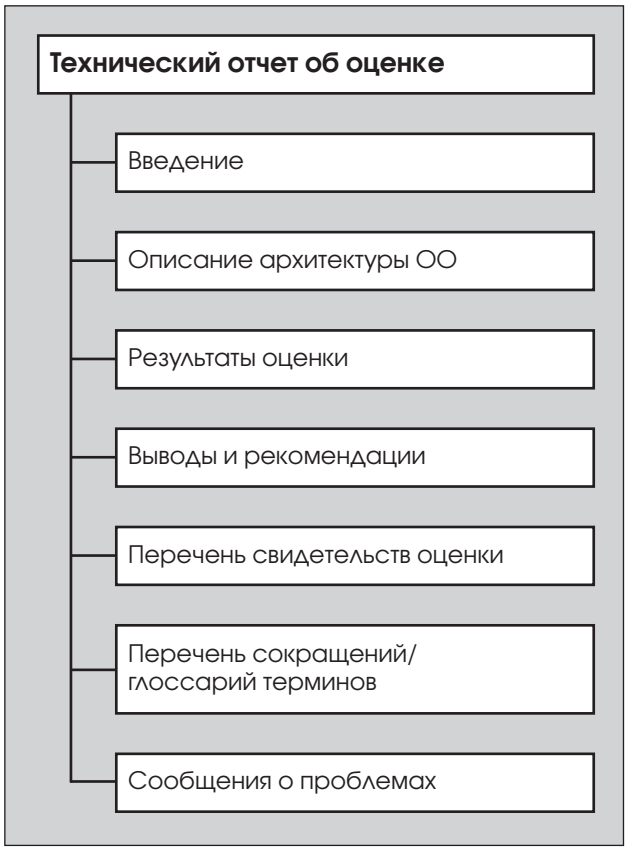

Рис. 6. Содержание ТОО при оценке ОО

Кроме того, в данном разделе ТОО оценщик имеет возможность поместить рекомендации, которые могут оказаться полезными для органа оценки. Эти рекомендации могут иметь отношение к недостаткам ПЗ, обнаруженным в процессе оценки, или касаться тех свойств ПЗ, которые представляются особенно полезными.

В разделе **«Перечень сокращений/глоссарий терминов»** ТОО оценщик должен привести перечень всех сокращений, используемых в ТОО, а также глоссарий используемых терминов. При этом нет необходимости в ТОО повторять определения терминов, имеющихся в глоссариях ОК или ОМО.

В разделе **«Сообщения о проблемах»** ТОО оценщик должен привести полный перечень СП, выпущенных в процессе оценки, а также их текущий статус. Для каждого СП в перечне следует привести идентификатор СП, а также его название или аннотацию.

3.4.2.2 Технический отчет об оценке объекта оценки (продукта или системы ИТ)

Содержание ТОО, отражающего результаты оценки ОО, представлено на рис. 6.

В разделе **«Введение»** ТОО оценщик должен привести следующую информацию:

- идентификационную информацию системы оценки, требуемую для однозначной идентификации системы, в рамках которой проводилась оценка ОО;
- название, дату составления и номер версии ТОО;
- информацию управления конфигурацией ОО (например, наименование и номер версии) для того, чтобы орган оценки мог определить, что именно подвергалось оценке;
- название, дату составления и номер версии ЗБ для того, чтобы орган оценки мог определить, на соответствие чему проводилась оценка, и подтвердить правильность заключений, сделанных оценщиком.
- ссылку на ПЗ (если ЗБ содержит утверждение о соответствии ОО требованиям одного или нескольких ПЗ). Такая ссылка должна содержать информацию, которая бы уникально идентифицировала соответствующие ПЗ (например, название, дату составления и номер версии);
- идентификационную информацию разработчика ОО, то есть организации, ответственной за создание ОО;
- идентификационную информацию заявителя оценки ОО, то есть организации, ответственной за предоставление оценщику свидетельств оценки;
- идентификационную информацию оценщика, то есть организации, ответственной за проведение оценки ОО и за формирование заключений по результатам оценки.

В разделе **«Описание архитектуры ОО»** ТОО оценщик должен привести высокоуровневое описание ОО и его главных компонентов, основанное на свидетельстве оценки, указанном в семействе доверия ОК «Проект верхнего уровня» (ADV_HLD), если компонент доверия из этого семейства был включен в ЗБ, и по нему выполнялась оценка.

Основное назначение рассматриваемого раздела ТОО состоит в указании степени архитектурного разделения главных компонентов ОО.

В разделе **«Оценка»** ТОО оценщик должен привести следующую информацию:

- ссылки на критерии, методологию, технологии и инструментальные средства оценки, использованные при оценке ОО;
- сведения о каких-либо ограничениях, имевших место в процессе оценки ОО или при обработке результатов этой оценки, а также о предположениях, сделанных в процессе оценки, которые повлияли на ее результаты.

Кроме того, оценщик может включить в ТОО информацию о каких-либо правовых или законодательных аспектах оценки ОО, организации работ по оценке, информацию, связанную с обеспечением конфиденциальности материалов оценки, а также другую информацию.

В разделе **«Результаты оценки»** ТОО для каждого вида деятельности по оценке ОО оценщик должен привести следующую информацию:

- название рассматриваемого вида деятельности;
- заключение по каждому из компонентов доверия, определяющих рассматриваемый вид деятельности, как результат выполнения соответствующих действий ОМО и составляющих их шагов оценивания;
- обоснование каждого сделанного заключения, показывающее в какой мере свидетельства оценки удовлетворяют или не удовлетворяют требованиям. Обоснование должно содержать описание выполненной работы, методов и процедур, применявшихся при получении результатов.

В разделе **«Выводы и рекомендации»** ТОО оценщик должен изложить выводы по результатам оценки ОО об удовлетворении ОО требованиям ЗБ.

Результат оценки ОО в целом должен формулироваться как «соответствие/несоответствие».

При положительном результате оценки должна быть указана степень, с которой можно доверять тому, что ОО соответствуют требованиям ОК. Должно поясняться соотношение с функциональными требованиями из части 2 ОК, требованиями доверия из части 3 ОК или же непосредственно с ПЗ, как это указано ниже [4]:

a) **соответствие части 2 ОК** — ОО соответствует части 2 ОК, если функциональные требования основаны только на функциональных компонентах из части 2 ОК;

б) **расширение части 2 ОК** — ОО соответствует расширению части 2 ОК, если функциональные требования включают функциональные компоненты, не содержащиеся в части 2 ОК;
в) **соответствие части 3 ОК** — ОО соответствует части 3 ОК, если требования доверия представлены в виде ОУД из части 3 ОК или пакета требований доверия, включающего только компоненты доверия из части 3 ОК;
г) **усиление части 3 ОК** — ОО соответствует усилению части 3 ОК, если требования доверия представлены в виде ОУД или пакета требований доверия и включают другие компоненты доверия из части 3 ОК;
д) **расширение части 3 ОК** — ОО соответствует расширению части 3 ОК, если требования доверия представлены в виде ОУД, дополненного требованиями доверия не из части 3 ОК, или пакета требований доверия, который включает требования доверия, не содержащиеся в части 3 ОК, или полностью состоит из них;
е) **соответствие ПЗ** — ОО соответствует ПЗ только в том случае, если он соответствует всем частям этого ПЗ.

Кроме того, в данном разделе ТОО оценщик имеет возможность поместить рекомендации, которые могут оказаться полезными для органа оценки. Эти рекомендации могут иметь отношение к недостаткам продукта ИТ, обнаруженным в процессе оценки, или касаться тех его свойств, которые представляются особенно полезными.

В разделе **«Перечень свидетельств оценки»** оценщик должен привести следующую информацию относительно каждого свидетельства оценки:

- идентификатор составителя (например, разработчик, заявитель);
- название;
- уникальную ссылку (например, дату составления и номер версии).

В разделе **«Перечень сокращений/глоссарий терминов»** ТОО оценщик должен привести перечень всех сокращений, используемых в ТОО, а также глоссарий используемых терминов. При этом нет необходимости в ТОО повторять определения терминов, имеющихся в глоссариях ОК или ОМО.

В разделе **«Сообщения о проблемах»** ТОО оценщик должен привести полный перечень СП, выпущенных в процессе оценки, а также их текущий статус. Для каждого СП в перечне следует привести идентификатор СП, а также его название или аннотацию.

3.4.3 Управление выходными материалами оценки

Оценщик представляет органу оценки ТОО, а также все СП, выпущенные в процессе оценки. Договорными отношениями может быть предусмотрено предоставление ТОО заявителю или разработчику. Но если ТОО включает чувствительную для оценщика информацию (информацию о «ноу-хау» и, в первую очередь, о приемах и методах оценки), то такую информацию оценщик вправе изъять до передачи ТОО заявителю или разработчику.

4 Применение Общей методологии оценки безопасности информационных технологий в России

Рассматривая перспективы вступления России в CCRA, следует отметить, что данное соглашение устанавливает для своих участников необходимость проведения работ в направлении единообразной интерпретации ОК и ОМО. Результатом такой работы в России стал выпуск ГОСТ Р ИСО/МЭК 15408-2002 [4-6] и соответствующего РД Гостехкомиссии России [12-14]. Что касается ОМО, то работа по подготовке российского аналога в настоящее время ведется (и весьма активно) специалистами ООО «Центр безопасности информации», Центра «Атомзащитаинформ» и ЦНИИАТОМИНФОРМ Минатома России при поддержке экспертов международной рабочей группы по Общим критериям.

С принятием в России ГОСТ Р ИСО/МЭК 15408 (идентичного международному стандарту ISO/IEC 15408) появилась возможность и настоятельная необходимость его использования для оценки безопасности продуктов и систем ИТ.

Провести оценку своих продуктов в соответствии с Общими критериями выразили желание как российские, так и зарубежные компании. Проведение таких оценок потребовало разработки соответствующих типовых методик оценки, предназначенных для использования испытательными лабораториями. Основой таких рабочих методик стала, конечно же, ОМО.

При разработке типовых методик оценки текст ОМО, сопровождающий шаги оценивания, подвергался структуризации. По сути, он разбивался на подшаги, которые должен выполнить оценщик, с четким описанием ожидаемых результатов после каждого шага и критериями досрочного завершения некоторых шагов.

В ОМО подвиды деятельности следуют согласно алфавиту. Но при этом нужно учитывать, что между соответствующими компонентами ОК имеются зависимости. Кроме того, зависимости имеются и между некоторыми шагами оценивания, относящимися к разным действиям оценщика и даже разным подвидам деятельности.

С учетом этих зависимостей всю деятельность по оценке целесообразно представлять в виде сетевых моделей (Е-сетей), определяющих порядок следования подвидов деятельности в рабочих методиках оценки. Такое представление деятельности по оценке позволяет распараллелить усилия оценщиков, а следовательно, достичь существенного сокращения продолжительности оценки.

Имея сетевое представление большинства из используемых пакетов доверия и разработав правила корректной композиции этих сетевых представлений, мы можем в короткие сроки разрабатывать рабочие программы и методики оценки продуктов и систем ИТ.

Разработанные специалистами ЦБИ типовые методики сертификационных испытаний по Общим критериям, которые уже использовались при сертификации отечественного межсетевого экрана «Z-2» (разработчик — ЗАО «Инфосистемы Джет»), операционной системы Microsoft® Windows® XP Professional Service Pack 1a (разработчик — корпорация Microsoft), межсетевого экрана Symantec™ Enterprice Firewall, Version 7.0.4 (разработчик — корпорация Symsntec), будут использоваться и в дальнейшем при сертификации других продуктов и систем ИТ.

5 Перспективы развития Общей методологии оценки безопасности информационных технологий

В заключение рассмотрим перспективы развития ОМО. История ОМО неразрывно связана с историей самих Общих критериев (Рис. 7). В настоящее время официальными документами Соглашения CCRA являются версия 2.1 ОК и версия 1.0 ОМО. В то же время, несмотря на то, что ОК уже давно (с 1999 года) нашли свое воплощение в стандарте ИСО, ОМО стала рассматриваться в качестве возможного документа (технического отчета) этой международной организации только два года назад.

ОК используются с 1998 года.

- Версия 1.0 ОМО (часть 2), соответствующая версии 2.1 ОК, выпущена в августе 1999 года и включает методологию оценки для ОУД 1-4.
- Версия 1.1а ОМО (апрель 2002 года) – предварительный проект для использования в качестве основы для документа ИСО. Структурирована по классам требований доверия из части 3 ОК, включает интерпретации.
- Версия 2.2 ОК и версия 1.2 ОМО планируются к выпуску в 2004 году.

Это будут официальные версии, куда войдут итоговые интерпретации, но ОМО будет все еще оставаться в формате 'ОУД'.

- Промежуточные версии 2.3 ОК и 1.3 ОМО планируются к выпуску также в 2004 году. Части 1 и 3 ОК будут существенно изменены в части классов ASE/APE. Изменения появятся и в классе AVA.
- Выпуск версии 3.0 ОК/ОМО запланирован в 2006 году. В ней предусматривается:
  - полная ревизия части 3 ОК;
  - учет интерпретаций в части 2 ОК;
  - учет влияния частей 2 и 3 на часть 1 ОК;
  - ОМО, соответствующая пересмотренной части 3 ОК и дополнительно включающая методологию оценки:
    - по меньшей мере, для компонентов ОУД 5;
    - для компонентов семейства ALC_FLR;
    - для класса AMA.

Рис. 7. Перспективы развития ОК и ОМО

Начиная с версии 1.1а ОМО, вносимые изменения уже влияют не только на ОМО, но и на ОК. С этого момента ОМО и ОК начинают «жить» вместе, разработчики ОК и ОМО предполагают синхронизировать их версии по номеру и по дате выпуска. Несмотря на рассмотренные выше достоинства новой версии ОМО, она так и останется какое-то время экспериментальной (неофициальной).

Новыми же официальными документами CCRA станут, скорее всего, ОК версии 2.2 и ОМО версии 1.2, которые, по сути, будут технической редакцией ОК версии 2.1 и ОМО версии 1.0 соответственно. В них войдут итоговые интерпретации (принятые CCRA изменения и дополнения в текущие версии ОК и ОМО), но ОМО так и останется структурированной по ОУД.

Появление промежуточных версий ОК (версия 2.3) и ОМО (версия 1.3), уже структурирован-

ной не по ОУД, ожидается в конце 2004 года. Но эти документы также, скорее всего, не станут официальными документами CCRA, будут подвергнуты апробации и дальнейшей доработке и ориентировочно в 2006 году получат новый (уже единый) номер версии — 3.0. Именно ОК/ОМО версии 3.0 планируется как основа нового издания стандарта ИСО, а также как официальные документы Соглашения CCRA.

Что касается России, то в настоящее время подготовлен проект РД Гостехкомиссии России «Общая методология оценки безопасности информационных технологий» [15] и проект «Типовой методики оценки профилей защиты и заданий по безопасности» [16].

При этом отметим, что в ОМО рассмотрены не все вопросы, связанные с оценкой безопасности ИТ, и это обуславливает необходимость дальнейшей разработки дополнительных руководств для всех участников оценки: заявителей, разработчиков, испытательных лабораторий и органа по сертификации, а также руководства по сопровождению сертификатов соответствия продуктов и систем ИТ требованиям безопасности информации.

ЛИТЕРАТУРА

1. Information technology — Security techniques — Evaluation Criteria for IT Security. Part 1: Introduction and general model. ISO/IEC 15408-1: 1999.
2. Information technology — Security techniques — Evaluation Criteria for IT Security. Part 2: Security functional requirements. ISO/IEC 15408-2: 1999.
3. Information technology — Security techniques — Evaluation Criteria for IT Security. Part 3: Security assurance requirements. ISO/IEC 15408-3: 1999.
4. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель.
5. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности.
6. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности.
7. Guide for Production of Protection Profiles and Security Targets. ISO/JTC1/SC27/N2449. DRAFT v0.9, January 2000.
8. Information technology — Security techniques — Protection Profile registration procedures. ISO/IEC 15292: 2001.
9. Common Evaluation Methodology for Information Technology Security Evaluation. Part 1: Introduction and general model, version 0.6, 19 January 1997.
10. Common Evaluation Methodology for Information Technology Security Evaluation. Part 2: Evaluation Methodology, version 1.0, August 1999.
11. Evaluation Methodology for the Common Criteria for Information Technology Security Evaluation, version 1.1a, 19 April 2002.
12. Руководящий документ — Безопасность информационных технологий — Критерии оценки безопасности информационных технологий — Часть 1: Введение и общая модель, Гостехкомиссия России, 2002.
13. Руководящий документ — Безопасность информационных технологий — Критерии оценки безопасности информационных технологий — Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002.
14. Руководящий документ — Безопасность информационных технологий — Критерии оценки безопасности информационных технологий — Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.
15. Руководящий документ — Безопасность информационных технологий — Общая методология оценки безопасности информационных технологий, Гостехкомиссия России, 2004 (проект).
16. Безопасность информационных технологий — Типовая методика оценки безопасности профилей защиты и заданий по безопасности, Гостехкомиссия России, 2004 (проект).

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Овчинникова Г.Ю. *(galya@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**