УДК 004.05

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

А. С. Марков, д-р техн. наук
АО «НПО «Эшелон», Москва, Россия

И. А. Шеремет, д-р техн. наук
Российский фонд фундаментальных исследований, Москва, Россия

Рассмотрены теоретические вопросы оценки соответствия средств защиты информации требованиям по безопасности информации. Кратко представлен понятийный аппарат сертификации средств защиты информации. Предложено рассматривать сертификацию как целенаправленный процесс (операцию), результативность которого определяется показателями безопасности объекта оценки и безопасности программной среды. Рассмотрены директивная и риск-ориентированная парадигмы сертификации средств защиты информации. Доказана состоятельность риск-ориентированной парадигмы сертификации с точки зрения ее результативности. Сформулированы характерные особенности перспективной парадигмы сертификации средств защиты информации. Рассмотрены особенности методов испытаний программных средств защиты информации. Показаны некоторые пути обеспечения полноты результатов испытаний с учетом современных реестров дефектов и уязвимостей безопасности, а также методологии "Общих критериев". Приведена краткая статистика апробации предложенных подходов.

Ключевые слова: информационная безопасность, защита информации, техническое регулирование, оценка соответствия, подтверждение соответствия, результативность, эффективность, ИТ-изделие, парадигма, риск-ориентированный подход, директивный подход, целенаправленный процесс, операционная безопасность.

Индустрия информационной безопасности (ИБ) в развитых странах подлежит государственному техническому регулированию. Основу технического регулирования ИБ составляет оценка соответствия средств защиты информации (СЗИ) требованиям по безопасности информации, которая в нашей стране проводится в форме обязательной сертификации СЗИ. Ввиду длительности и крайне высокой трудоемкости выполнения проверок современных ИТ-изделий вопросы сертификации СЗИ лежат в плоскости постоянного переосмысления и совершенствования. Степень государственной важности работ по сертификации СЗИ пропорциональна уровню зависимости страны от технологий зарубежного производства и развития новых методов информационного противоборства.

Марков Алексей Сергеевич, старший научный сотрудник.
E-mail: mail@cnpo.ru
Шеремет Игорь Анатольевич, профессор, заместитель директора Российского фонда фундаментальных исследований по научной работе.

Статья поступила в редакцию 20 августа 2015 г.

Проблематика сертификации СЗИ также отмечена и в "Приоритетных проблемах научных исследований в области обеспечения информационной безопасности Российской Федерации".

Понятийный аппарат сертификации средств защиты информации

Под СЗИ будем понимать ИТ-изделие, применительно к которому задекларированы функции защиты ресурсов системы от угроз конфиденциальности, целостности и доступности.

Сертификация СЗИ по требованиям безопасности информации представляет собой обязательное независимое подтверждение соответствия СЗИ требованиям нормативных документов по безопасности информации с учетом правил и компетенции федеральных органов*. Участниками сертификации являются: организация-заявитель, испытательная лаборатория, орган по сертификации, федеральный орган.

Следует назвать ключевые принципы сертификации СЗИ:

* Минобороны России, ФСБ России, ФСТЭК России.

1. Независимость, которая обеспечена работой 3-их сторон — аккредитованной испытательной лабораторией и аккредитованным органом по сертификации, которые также контролируются федеральным органом.

2. Обязательность, что продиктовано современной законодательной базой*.

3. Документальная подтвержденность в виде сертификата соответствия, в котором приведены выполненные требования, период действия документа, идентификационные характеристики сертифицированного изделия.

4. Техническая законченность сертифицированного изделия, которое подлежит маркировке и имеет фиксированные значения показателей целостности (например, контрольные суммы).

В настоящее время в области ИБ приняты две схемы сертификации: партии изделий (одно или несколько изделий) и серийного производства. В последнем случае сертификация изделия включает дополнительную экспертизу (аттестацию) его производства.

Основной же процедурой сертификации являются сертификационные испытания, программа, методики и результаты (протоколы, отчеты, заключения, акты) которых подлежат поэтапной внешней экспертизе. Заявитель на сертификацию (им может быть разработчик, изготовитель или поставщик) должен иметь соответствующие лицензии, а испытательная лаборатория и орган по сертификации дополнительно и аттестаты аккредитации, т. е. подлежать специальным экспертизам и аккредитациям.

Таким образом, сертификация СЗИ представляет собой *многоуровневый комплекс проверок принципиального характера, обладающий известной долей субъективизма*. Очевидно, что при сертификации превалируют экспертные методы исследования и принятия решений, эффективность которых, как известно, зависит от степени их регламентации и автоматизации.

Проблематика сертификации СЗИ должна рассматриваться на различных методологических уровнях (процедурном, методическом, технологическом, документальном и инструментальном), при этом как вид деятельности сертификация находится в непрерывном взаимодействии с другими составными частями оценки соответствия, а именно: испытаниями и контролем**.

* См. Постановления Правительства РФ 1995 г. № 608 и 2010 г. № 330.

** ISO/IEC 17000: 2004.

Эффективность сертификации средств защиты информации

Оценку эффективности сертификации СЗИ будем рассматривать как операцию, представляющую целенаправленный процесс [1, 2]. В этом случае легко показать, что эффективность сертификации СЗИ порождается совокупностью свойств: результативностью, ресурсоемкостью, оперативностью, т. е. ее можно оценить с помощью следующего e-мерного вектора:

$$E_{\langle e\rangle} = \left\langle S_{\langle s\rangle}, R_{\langle r\rangle}, T_{\langle t\rangle} \right\rangle,$$

где $S_{\langle s\rangle}, R_{\langle r\rangle}, T_{\langle t\rangle}$ — векторные показатели результативности, ресурсоемкости и оперативности;

e — размерность векторного показателя ($e = s + r + t$).

Требования по безопасности информации в международной практике делят на требования по безопасности объекта оценки и требования по безопасности среды*. В нашей стране, что касается ИТ-изделий, указанные требования трансформируются в требования по защищенности информации от несанкционированного доступа (НСД) и в требования по безопасности программ — отсутствию недекларированных возможностей (НДВ).

Тогда показатель результативности имеет следующий вид:

$$S_s = \left\langle S^{(\text{нсд})}_{s_{\text{нсд}}}, S^{(\text{ндв})}_{s_{\text{ндв}}} \right\rangle,$$

где s — размерность векторного показателя $(s = s_{\text{нсд}} + s_{\text{ндв}})$.

Формализованное описание цели сертификации можно описать критерием пригодности:

$$E_{\langle e\rangle} \in \left\{ E^{\text{д}}_e \right\},$$

где $\left\{ E^{\text{д}}_e \right\}$ — область допустимых значений показателя $E_{\langle e\rangle}$ качества результатов сертификации.

В условиях априорной неопределенности факторов сертификации можно использовать вероятность наступления события, которая характеризует степень его объективной возможности при заданном комплексе условий:

$$P_{\text{ц}} = P\left(\hat{E}_{\langle \text{в}\rangle} \in \left\{ \hat{E}^{\text{д}}_{\langle \text{в}\rangle} \right\} \right),$$

где $P_{\text{ц}}$ — вероятность достижения целей сертификации.

* ISO/IEC 15408-1: 2009.

В идеале конечной целью всей деятельности по сертификации СЗИ является обеспечение безопасности ресурсов объекта информатизации, в частном случае — автоматизированной системы (АС). В то же время показатели безопасности информации СЗИ жестко заданы в нормативных документах. Как известно, нормативные документы являются отражением текущей *доктрины информационной безопасности*. Сказанное позволяет сформулировать ряд теоретических положений.

Утверждение 1 ("Закон отставания"). Уровень результативности сертификации СЗИ отстает от уровня реальной результативности СЗИ на величину отставания нормативно-методических документов от актуальных требований $\left\{S^{\text{д}}_{\langle s\rangle}\right\} \Big/ \left\{S^{\text{д}'}_{\langle s'\rangle}\right\}$.

Можно привести доказательство этого утверждения, используя индуктивный метод. Например, в системе может быть задан пароль длиной лишь в 6 символов (с энтропией близкой к нулю), но это будет соответствовать текущим нормативным требованиям. Или другой показательный пример: эксперт подтвердил, что, на его взгляд, избыточность в программном коде условно приемлема, что, согласно современной нормативной базе, соответствует категоричному выводу об отсутствии НДВ в средствах защиты конфиденциальной информации.

В теоретическом плане возникает вопрос: как определить расстояние между уровнем результативности сертификации и уровнем результативности собственно СЗИ? Рассмотрим вначале парадигмы сертификации СЗИ по требованиям безопасности информации.

Директивная парадигма сертификации

Генезис указанной парадигмы связан со специальными документами прошлого тысячелетия, основанными на методологии *Orange Book** [3]. Несмотря на ветхость, эта парадигма показывала свою состоятельность в течение длительного времени, а в ряде федеральных систем актуальна и сейчас.

Отметим показатели результативности сертификации $S_{\langle s\rangle}$, соответствующие указанной парадигме в настоящее время в нашей стране:

- показатель защищенности информации от несанкционированного доступа $S^{(\text{нсд})}_{\langle s_{\text{нед}}\rangle}$, заданный таблично в руководящих и специальных документах, касающихся средств вычислительной техники, автоматизируемых систем, межсетевых экранов и других;
- показатель отсутствия недекларированных возможностей $S^{(\text{ндв})}_{\langle s_{\text{ндв}}\rangle}$, заданный таблично в руководящем документе по контролю отсутствия НДВ в программном обеспечении СЗИ (рис. 1).

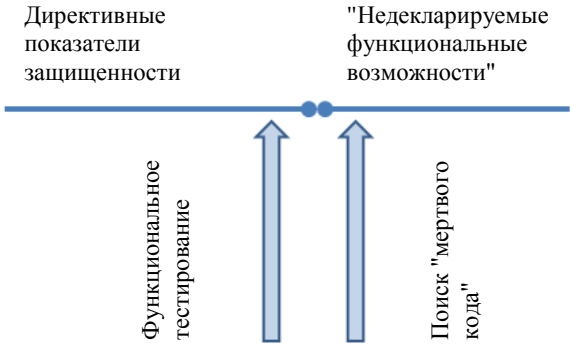

Рис. 1. Факторы и методы директивной сертификации

В первом случае проводится процедура подтверждения (путем функционального тестирования) заданных качественных показателей (например, факта, что пароль должен содержать не менее 6 символов). Если все частные (булевы) показатели подтверждены при проверках, то делается вывод о соответствии СЗИ нормативно-методическому документу в части заданного класса защиты информации [4].

Во втором случае, в соответствии с нормативным документом проводится так называемый статический, а при необходимости и динамический анализ исходного кода, выражающийся в компиляции и нисходящей декомпозиции программы (сборе и прогоне маршрутов программ и т. п.). Предполагается, что по завершению декомпозиционных процедур следует сделать экспертный вывод о полном *отсутствии* НДВ [5].

Несмотря на то, что указанные методы сертификации имеют ряд существенных косвенных достоинств (главным образом, "детерентального" характера [6]), следует сделать критический анализ директивной доктрины в связи с новыми геополитическими и технологическими условиями.

Основными особенностями данной доктрины являются:

- множество показателей защищенности имеют жестко детерминированный вид, т. е. могут не иметь нагрузки для безопасности реального объекта информатизации;

* DoD 5200.28-STD: 1983.

• полнота тестирования формально не определена, т. е. *обоснование достоверности* носит весьма субъективный характер;

• методический аппарат испытаний опирается на теорию надежности, т. е. малоэффективен при поиске ошибок, связанных с редко используемыми входными данными (например, злонамеренных программных закладок);

• статичность сертификации, т. е. независимая проверка изделия не проводится до следующей пересертификации (решение на которую, как показывает практика, мало зависит от инцидентов в области ИБ) или инспекционного контроля.

Эти особенности затрудняют строгую формальную оценку степени разрыва между уровнями результативности сертификации и результативности СЗИ (см. утверждение 1), однако четко обуславливают ряд негативных моментов.

Утверждение 2. В рамках директивной парадигмы может возникнуть ситуация, когда увеличение времени и стоимости испытаний СЗИ не приводит к повышению его безопасности, а с течением времени эксплуатации СЗИ его степень безопасности уменьшается:

$$\begin{cases} \forall(T, R \to \infty)\exists S \nrightarrow S' \\ \lim\limits_{t\to\infty} S \setminus S'(t) \to \infty \end{cases},$$

где T, R, S — обобщенные показатели эффективности сертификации СЗИ;
S' — обобщенный показатель результативности СЗИ;
t — время эксплуатации изделия.

Доказательство утверждения можно выполнить, используя индуктивные методы. Например, *fuzzing*-тестирование современной операционной системы предполагает запуск последней до миллиарда раз. Очевидно, что испытательная лаборатория на этапе сертификации не имеет возможности найти уязвимости, опираясь на методы из теории надежности. Совершенно очевидно, что при дальнейшей эксплуатации сложного ИТ-изделия в нем будут обнаружены ошибки, связанные с безопасностью системы.

Еще пример, структурная декомпозиция программ (сбор и контроль всех маршрутов) является обязательной и чрезвычайно трудоемкой процедурой, в то же время не связанной напрямую с поиском и локализацией дефектов безопасности (за исключением "мертвого кода").

Следствие 1. Испытания СЗИ, основанные исключительно на аппарате теории надежности, приводят к снижению результативности сертификации СЗИ по причине отвлечения экспертов испытательной лаборатории (ИЛ) на трудоемкие проверки, мало релевантные с безопасностью информации.

Следует отметить, что повышение результативности директивного подхода может осуществляться путем детализации механизмов (мер и средств) защиты информации, что, конечно, позволит учесть наиболее известные классы угроз ИБ для абстрактного объекта информатизации.

Риск-ориентированная парадигма сертификации

Как известно, альтернативным директивному подходу в области ИБ является *риск-ориентированный* подход. Опираясь на его концепцию, следует определить основные факторы безопасности программных систем:

• *дефекты безопасности программ*, локализация которых может составить уязвимость;

• *уязвимости*, реализация которых может представлять угрозу,

• *угрозы* ИБ, определяющие риски,

• *риски* ИБ, характеризующие уровень безопасности системы (объекта информатизации).

Каждому фактору безопасности можно сопоставить классы соответствующих проверок, например:

• методы структурного анализа безопасности программ, направленные на выявление дефектов и известных уязвимостей;

• методы функционального тестирования (от пентестов до комплексного анализа уязвимостей), ориентированные на определение угроз, в том числе связанных с идентифицированными уязвимостями;

• объектовый анализ рисков, связанный с актуальными угрозами конкретным ресурсам системы.

Здесь важно отметить, что идеальный риск-ориентированный подход по ИБ носит нисходящий вид, а именно: от решаемых функциональных задач к конкретным механизмам безопасности. Например, в рамках планирования непрерывности деятельности (в мировой практике известного, как *Business Impact Analysis* — BIA [6]) или оценки риска могут быть сформулированы объектовые требования по ИБ, на основании которых выполняется синтез комплекса СЗИ, функции безопасности и безопасность программной среды которых подтверждены в необходимой степени.

Исходя из системного подхода, можно усилить концепцию указанной парадигмы сертификации СЗИ. Во-первых, сертификацию целесообразно рассматривать как неотъемлемую часть

непрерывной оценки соответствия, что подразумевает использование результатов приемочных *испытаний* (в том числе в случае последующей модификации изделия) и определение последующего периодического инспекционного *контроля*. Во-вторых, определяя показатели полноты проверок, обеспечиваем качественно новый уровень сертификации, а именно ее *доказательность*.

Определим черты альтернативной парадигмы сертификации СЗИ:

- ориентация на факторы информационной безопасности;
- определение полноты проверок (обеспечение доказательности уровня безопасности);
- динамичность и непрерывность.

Такой подход имеет ряд преимуществ:

- сертификация ограничена только областью ИБ, т. е. исключает трудоемкие (зачастую и невыполнимые) проверки по качеству и надежности, в том числе дублируемые собственно разработчиком изделия;
- ориентация на факторы безопасности, включая именно источники уязвимостей и угроз (т. е. дефекты безопасности), существенно повышает результативность сертификации в смысле повышения безопасности ресурсов АС;
- итоговые объектовые проверки на конкретной АС направлены на защиту только от актуальных угроз, т. е. согласуются с моделью реальных угроз (рис. 2).

$$\begin{cases} S(t) \rightsquigarrow S_{\max} \\ T \le T_{\text{тр}} \\ R \le R_{\text{тр}} \end{cases},$$

где T, R, S — обобщенные показатели эффективности сертификации СЗИ;
t — время эксплуатации изделия.

Можно предложить доказательство данного подхода, опираясь на индуктивно-дедуктивные методы. Например, базовые классы факторов безопасности, а именно: дефекты безопасности, уязвимости, угрозы и риски, инвариантны, значения их показателей подлежат непрерывному контролю. Эффективность контроля зависит от полноты и ранжирования проверочных процедур, которые, в свою очередь, находятся в постоянном развитии, т. е. подлежат управлению.

Следствие 2. Риск-ориентированный подход удобен для обоснования инкрементальной сертификации, когда ИТ-изделие имеет динамически меняющийся код.

Это особенно важно, когда оценке соответствия подлежат изделия, требующие непрерывного изменения кода, например, с целью срочных обновлений или исправлений, касающихся функционала ИБ. Подобная ситуация возникает и с интегрированными в изделие базами активных данных по ИБ, например, антивирусными базами, базами уязвимостей или базами шаблонов компьютерных атак. Придерживаясь риск-ориентированного подхода, можно оценить (и отслеживать) сегмент реальных рисков, связанных с модификацией программ и баз данных, и принять обоснованные решения (провести обработку риска) по периодичности инспекционного контроля программных дополнений или пересертификации изделия.

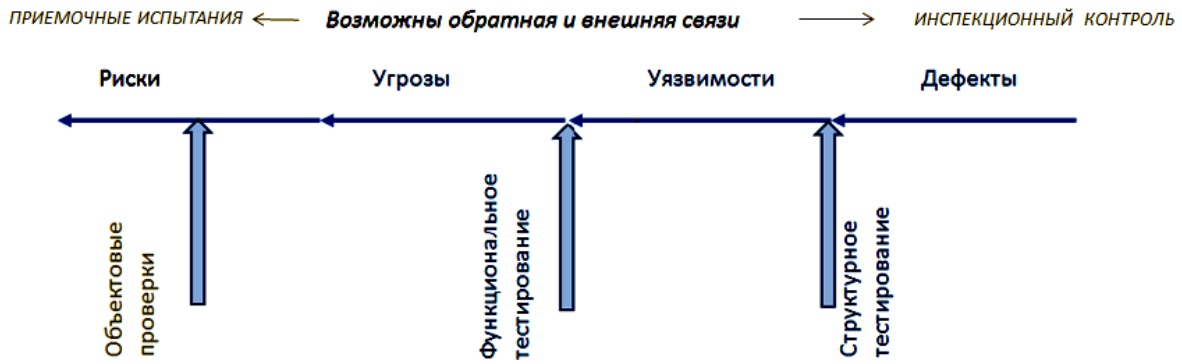

Рис. 2. Факторы безопасности и методы тестирования

В итоге, налицо достижение эффекта значительного повышения результативности, зачастую при снижении ресурсоемкости и повышении оперативности.

Утверждение 3. Использование риск-ориентированного подхода позволяет обеспечить заданный уровень эффективности сертификации СЗИ по требованиям безопасности информации:

Опираясь на рассматриваемые факторы безопасности, можно представить показатель результативности сертификации СЗИ как совокупность показателей безопасности ИТ-изделия на разных этапах его жизненного цикла, например:

$$S_{\langle S\rangle} = \left\langle S^{(\text{рск})}_{\langle s_{\text{рск}}\rangle}, S^{(\text{узв})}_{\langle s_{\text{узв}}\rangle} \right\rangle,$$

где $S^{(\text{рск})}_{\langle s_{\text{рск}}\rangle}, S^{(\text{узв})}_{\langle s_{\text{узв}}\rangle}$ — показатели уровня рисков системы (объекта информатизации) и уровня уязвимости продукта (средства).

В данном случае можно уточнить *утверждение 1* для любых парадигм сертификации СЗИ и сформулировать следующие теоретические положения.

Утверждение 4. Степень результативности сертификации продукта (технического средства) может быть оценена числом N — опубликованных (нормированных) уязвимостей, найденных и оставшихся в продукте в период действия сертификата (с учетом периодического инспекционного контроля для их устранения).

Следствие 3. В рамках экспертизы материалов испытаний должна быть подтверждена полнота спектра выявляемых уязвимостей и дефектов (источников уязвимостей).

Следствие 4. Степень результативности сертификации зависит от определения в эксплуатационной документации возможности и порядка обновления продукта в случае опубликования уязвимости.

Утверждение 5. Степень результативности сертификации системы (аттестации объекта информатизации) может быть определена степенью увеличения риска ΔR ресурсам системы, связанного с возникшими и оставшимися угрозами и уязвимостями за период действия сертификата (с учетом инспекционного контроля).

Следствие 5. В рамках экспертизы материалов испытаний должна быть подтверждена полнота соответствия механизмов безопасности СЗИ актуальным угрозам.

Замечание. В условиях неопределенности указанные в *утверждениях 4* и *5* показатели носят вероятностный характер.

Методы тестирования программных средств защиты информации

Как отмечалось, и требования, и виды сертификационных испытаний, и реализующие их методы тестирования делятся на два класса.

В случае проверки защищенности информации от НСД используется метод функционального тестирования (метод "черного ящика"), когда проводятся тесты на соответствие заданным нормативным требованиям. Например, директивному подходу соответствуют руководящие документы Гостехкомиссии России, от которых отталкиваются все отечественные системы сертификации с момента их основания.

Риск-ориентированному подходу может соответствовать международная методология *Common Criteria* (*ISO* 15408), согласно которой формируется *задание по безопасности* в виде полуформальных нотаций для конкретного СЗИ [7]. Это упрощает выполнение отображения реестра значимых угроз на функции безопасности, реализуемых синтезируемым комплексом СЗИ. Методологии *Common Criteria* придерживается 25 стран, но в России методология имеет локальное развитие под эгидой интенсивных изысканий ТК-362 и ФСТЭК России. Указанный подход, конечно, не лишен недостатков, например, отмечается сложность понимания данного подхода и увеличение трудоемкости как документальной подготовки изделия, так и проведения испытаний. В некоторых странах наблюдается трансформация основ *Common Criteria* в направлении кибербезопасности и снижения сложности [8].

Достоверная проверка безопасности программного кода, как известно, возможна только путем применения структурных методов ("белого ящика"). Директивному подходу соответствует метод структурной нисходящей декомпозиции программ, ориентированный на выявление "мертвого кода" и регламентированный известным руководящим документом Гостехкомиссии России по контролю отсутствия НДВ. Говоря о риск-ориентированных методах, следует отметить, что они направлены на выявление источников угроз, т. е. актуальных классов дефектов безопасности, наиболее известными из которых являются:

- тестирование по моделям представления программ (прикладная верификация) [9, 10];
- эвристический (сигнатурный) анализ потенциально опасных фрагментов программ [11].

К достоинству тестирования по моделям относят высокую степень автоматизации выявления некорректностей кодирования (нефункциональных ошибок) [12]. Второй подход позволяет учесть полный спектр известных классов дефектов безопасности, но в большей степени зависим от квалификации экспертов: как при написании эвристик, так и при анализе потенциально опасного фрагмента кода. Заметим, указанные подходы не претендует на ис-

ключительность, так как на практике интересен синтез возможных методик выявления конкретного класса дефектов по критериям быстродействия и уровней ошибок I и II рода. К примеру, международный стандарт *ISO/IEC TR* 20004 предлагает методики выявления известных уязвимостей, опубликованных в открытых бюллетенях по безопасности. Разумеется, такой подход усилит эффективность структурного тестирования, например, при первичном анализе заимствованных компонент.

В то же время следует указать, что полноту учета полного спектра дефектов обеспечивает именно эвристический анализ, так как он не накладывает ограничений на классы выявляемых дефектов.

Краткая статистика по апробации методов тестирования по безопасности

Некоторые из отмеченных выше методов, которые укладываются в концепцию риск-ориентированного подхода, прошли апробацию в ряде испытательных лабораторий.

Что касается структурных методов, то имеется статистика использования эвристического подхода к выявлению дефектов и уязвимостей. Полнота спектра выявляемых дефектов обеспечена поддержкой актуальных классификаторов *CWE* (*Common Weakness Enumeration*) и *HP Fortify*. Как показала статистика испытаний, большинство критических уязвимостей выявлено указанным способом (рис. 3) [11].

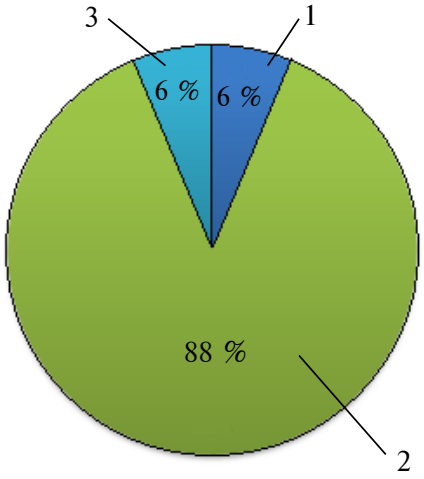

Рис. 3. Примерное соотношение результативности методов тестирования:
1 — функциональное тестирование ("черный ящик");
2 — структурный анализ ("белый ящик");
3 — реверс-инжиниринг

Исследование функциональных методов связано с получением положительных результатов внедрения методологии *Common Criteria*. Успешное завершение ряда сертификаций по линии ФСТЭК России показало перспективность данного направления в целом. В частности, на рис. 4 показано, что трудоемкость испытаний по линии *Common Criteria* соизмерима с трудоемкостью традиционных испытаний для случая проверки СЗИ невысоких оценочных уровней доверия (ОУД). Ожидается, что разница будет нивелироваться с развитием методической базы испытаний [8].

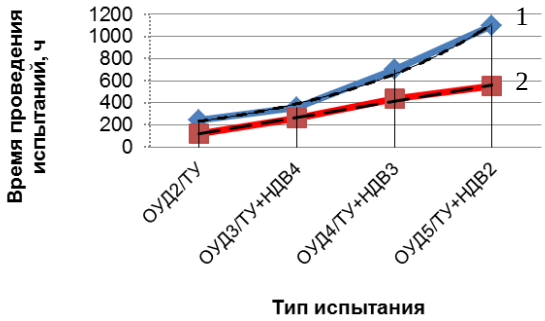

Рис. 4. Сравнение времени проведения испытаний:
1 — испытания по линии *Common Criteria*; 2 — испытания по линии *Orange Book*

Выводы

Дан ряд новых теоретических положений, касающихся концептуальных вопросов развития сертификации СЗИ, в том числе сделаны следующие выводы:

1. Сертификация СЗИ представляет собой сложный многомерный комплекс процедур, опирающийся на экспертные методы тестирования и принятия решений, что в первую очередь подразумевает обеспечение и контроль полноты целевых проверок для оценки достоверности результата собственно сертификации. Это требует создания и развития соответствующих современных методов, технологий, методик и инструментальных средств сертификации СЗИ.

2. Сертификацию СЗИ целесообразно рассматривать как целенаправленный процесс, эффективность которого может быть определена показателями результативности, оперативности и ресурсоемкости, при этом показатели результативности включают как показатели безопасности объекта оценки, так и его среды. В то же время динамизм и сложность ИТ-изделий приводит к объективному отставанию уровня эффективности и результативности сертификации СЗИ от текущих требований в области ИБ. Цен-

тральным системообразующим принципом повышения эффективности сертификации СЗИ, включая уменьшение указанного разрыва, является строгая ориентация системы сертификации на актуальные факторы безопасности информации, включая их источники (такие, как дефекты безопасности), а не на показатели качества функционирования систем вообще.

3. В работе показано, что современная парадигма сертификации СЗИ должна обладать свойствами: непротиворечивости (при строгом соответствии целевой задаче безопасности информации), непрерывности и системности, полноты и доказательности. В этом плане на основе анализа современных директивного и риск-ориентированного подходов в области ИБ показаны предпосылки к эволюции современной парадигмы сертификации СЗИ в направлении к риск-ориентированному подходу. Однако переход к указанному подходу сопряжен с серьезным переосмыслением всей системы оценки соответствия в области ИБ, так как подразумевает нисходящее формирование требований от функциональных задач к функциям безопасности. На переходном этапе имеет место быть квази риск-ориентированный подход, в рамках которого выполняется директивная детализация мер защиты, отображающихся на восходящую модель угроз.

4. Последние изыскания испытательных лабораторий по внедрению современных методов, соответствующих риск-ориентированному подходу и отвечающих требованиям по полноте, показали их перспективность. В частности, полнота проверки безопасности ИТ-изделия может быть обеспечена путем поддержки известных баз уязвимостей и реестров дефектов безопасности. Полнота безопасности объекта информатизации подтверждается проверкой соответствия актуальных угроз (отвечающих заданным рискам) и функций безопасности синтезируемого комплекса СЗИ, для чего удобно использовать элементы методологии *Common Criteria*.

ЛИТЕРАТУРА

1. **Петухов Г. Б., Якунин В. И.** Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. — М.: АСТ, 2006. — 504 с.
2. **Юсупов Р. М., Заболотский В. П.** Концептуальные и научно-методологические основы информатизации. — СПб: Наука, 2009. — 542 с.
3. **Барсуков В. С., Дворянкин С. В., Шеремет И. А.** Безопасность связи в каналах телекоммуникаций // Технологии электронных коммуникаций. 1992. Т. 20. — 122 с.
4. **Костогрызов А. И., Липаев В. В.** Сертификация функционирования автоматизированных информационных систем. — М.: Изд. "Вооружение. Политика. Конверсия", 1996. — 280 с.
5. **Осовецкий Л. Г.** Технология выявления недекларированных возможностей при сертификации промышленного программного обеспечения по требованиям безопасности информации // Вопросы кибербезопасности. 2015. № 1 (9). С. 60 —64.
6. **Stewart J. M., Chapple M., Gibson D.** CISSP: Certified Information Systems Security Professional Study Guide, 7th Edition. Sybex. 2015. — 1104 p.
7. **Higaki W. H.** Successful Common Criteria Evaluations: A Practical Guide for Vendors. CreateSpace Independent Publishing Platform. 2010. — 282 p.
8. **Барабанов А. В., Марков А. С., Цирлов В. Л.** Оценка соответствия средств защиты информации "Общим критериям" // Информационные технологии. 2015. Т. 21. № 4. С. 264 —270.
9. **Аветисян А. И., Белеванцев А. А., Чукляев И. И.** Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20 —28.
10. **Ковалев В. В., Компаниец Р. И., Новиков В. А.** Верификация программ на основе соотношений подобия // Труды СПИИРАН. 2015. № 1. С. 233—245.
11. **Марков А. С., Цирлов В. Л.** Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1(1). С.42—48.
12. **Baier C., Katoen J. P.** Principles of model checking // MIT Press. 2008. — 984 p.

THEORETICAL ASPECTS OF INFORMATION SECURITY CERTIFICATION

A. S. Markov
JSC "NPO "Echelon", Moscow, Russia

I. A. Sheremet
Russian Foundation for Basic Research, Moscow, Russia

The theoretical questions of information security compliance assessment are considered. The terminology basis for information security certification is briefly presented. It is proposed to consider the certification as a purposeful process (operation), the effectiveness of which is measured by indicators of security of the evaluation object and programming environment. The directive paradigm and risk-oriented paradigm for information security certification are considered. The consistency of the risk-oriented paradigm of certification from the viewpoint of its effectiveness is proved. The characteristic features of a promising paradigm for information security certification are formulated. The features of software security testing methods are reviewed. Some of the ways to ensure the completeness of the test results with current registers of the defects and security vulnerabilities as well as the Common Criteria methodology are shown. A brief statistics of testing the proposed approaches are given.

Keywords: information security, data protection, technical regulations, conformity assessment, compliance assessment, performance, efficiency, IT product, paradigm, risk-based approach, directive approach, purposeful process, operation security.

Bibliography — 12 references. *Received August 20, 2015*