УДК 004.056:621.391

МЕТОДИЧЕСКИЕ ВОПРОСЫ ОЦЕНКИ СООТВЕТСТВИЯ АППАРАТУРЫ СЕТЕЙ СВЯЗИ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

А.В. Барабанов, доцент МГТУ им. Н.Э. Баумана, к.т.н.; ab@cnpo.ru
Д.В. Лучин, заместитель генерального директора филиала ФГУП НИИР — СОНИИР, к.т.н.; dmyl@soniir.ru
А.С. Марков, доцент МГТУ им. Н.Э. Баумана, д.т.н.; a.markov@bmstu.ru
Ю.В. Рауткин, советник филиала ФГУП НИИР — СОНИИР, к.т.н.; info@soniir.ru

Разработан методический подход к проведению оценки соответствия аппаратуры сетей связи требованиям по безопасности информации, основанный на методологии метастандарта ISO 15408. Представлены результаты синтеза функциональных требований безопасности, предъявляемых к аппаратуре систем связи. Дается обоснование возможности использовать результаты синтеза как основу перспективного пакета профилей защиты аппаратуры систем связи. Предложена концептуальная модель комплекса средств защиты аппаратуры сетей связи, реализуемая в рамках сертификационных испытаний. Разработана концептуальная модель проведения сертификационных испытаний аппаратуры систем связи по требованиям безопасности информации. Показано, что предложенные модели обеспечивают детерминированность процесса испытаний и выполнение свойств повторяемости и воспроизводимости. Исследование вопросов минимизации времени проведения сертификационных испытаний показывает, что сокращение времени может быть достигнуто за счет использования покрывающих тестовых наборов.

Ключевые слова*: информационная безопасность, сети связи, безопасность телекоммуникационных систем, защита информации, оценка соответствия, сертификация, «Общие критерии», ISO 15408, требования к аппаратуре высокочастотной связи, время испытаний*

Введение. Рост угроз безопасности информации, связанных с наличием уязвимостей программно-аппаратного обеспечения аппаратуры сетей связи (СС), определяет необходимость повышения качества оценки соответствия аппаратуры СС, в том числе в области защищенности информации [1–4]. Следует отметить, что в настоящее время требования, которым должна отвечать указанная аппаратура, четко не сформулированы [5]. Например, в соответствии с отраслевыми стандартами ОАО «ФСК ЕЭС» [6], определяющими требования к аппаратуре высокочастотной связи по линиям электропередачи, данная аппаратура должна соответствовать оценочному уровню доверия 4 по требованиям ГОСТ Р ИСО/МЭК 15408 [7], но довольно много функциональных требований безопасности (ФТБ) не определено. Таким образом, задача формирования методического обеспечения анализа и синтеза множества ФТБ, предъявляемых к аппаратуре СС, а также оценки соответствия аппаратуры СС этим требованиям в настоящее время является весьма актуальной. В работе представлен методический аппарат, который эксперты испытательных лабораторий могут применять при проведении оценки соответствия аппаратуры СС требованиям по безопасности информации.

Формирование требований по безопасности информации. С учетом особенностей отечественной системы сертификации, связанных с использованием метастандарта ISO 15408 [8, 9], в рамках данной работы было принято решение об использовании аппарата «Общих критериев» при формировании множества ФТБ, предъявляемых к аппаратуре СС (рис. 1). При рассмотрении среды безопасности аппаратуры СС приводится описание следующих аспектов безопасности среды:

- описание предположений безопасности, содержащее аспекты безопасности среды, в которой аппаратура СС будет использоваться или предполагается к использованию;
- описание угроз безопасности информации, включающее все те угрозы активам, против которых требуется защита средствами аппаратуры СС или ее среды;
- описание политики безопасности организации, идентифицирующее и при необходимости объясняющее все положения политики безопасности организации или правила, которым должна подчиняться аппаратура СС.

Цели безопасности отражают заявленное намерение противостоять всем установленным угрозам безопасности информации, а также охватить все предположения безопасности и установленную политику безопасности организации. При изложении требований безопасности к аппаратуре СС должны быть определены ФТБ (например, требования к идентификации/аутентификации или разграничению доступа) и требования доверия, которым должны удовлетворять аппаратура СС и процесс ее разработки. Выбор множества ФТБ и требований доверия к безопас-

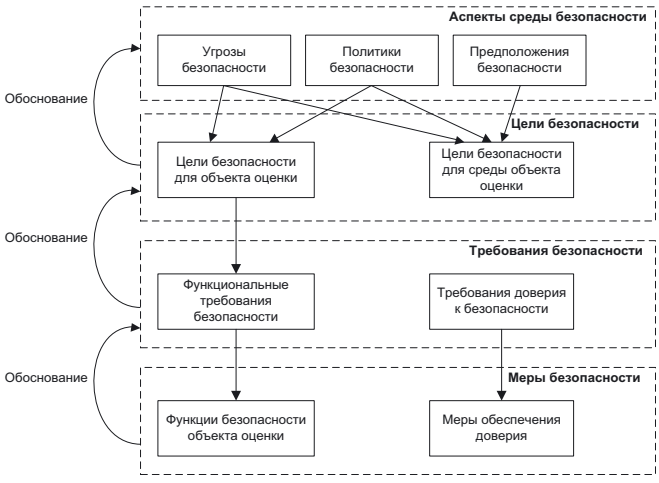

Рис. 1. **Последовательность требований**

ности осуществляется из каталогов требований, представленных во 2-й и 3-й частях стандарта «Общие критерии». С целью удовлетворения идентифицированных множеств ФТБ и требований доверия формулируются перечни функций безопасности аппаратуры СС и мер, применяемых при ее разработке. Все идентифицированные множества (аспекты среды безопасности, цели, требования, меры) должны быть согласованы друг с другом — данная информация и необходимые пояснения приводятся, как правило, в задании по безопасности.

Анализ, выполненный в рамках данного исследования, позволил сформулировать множество ФТБ, которое целесообразно предъявлять к аппаратуре СС (табл. 1).

Таблица 1. Функциональные требования безопасности к аппаратуре систем связи

Нотация по ISO 15408	Описание по ISO 15408
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FIA_ALF.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.6	Повторная аутентификация
FIA_UID.2	Идентификация до любых действий пользователя
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MTD.1	Управление данными функций безопасности аппаратуры СС
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FPT_STM.1	Надежные метки времени
FPT_TST.1	Самотестирование функций безопасности аппаратуры СС

Модель комплекса средств защиты аппаратуры сетей связи. Модель комплекса средств защиты (КСЗ) аппаратуры СС была разработана с учетом основных положений «Общих критериев». Будем рассматривать КСЗ аппаратуры СС (рис. 2) как множество объектов оценки (ОО) $\{OO_1, OO_2, \ldots, OO_w\}$, где $w \in \mathbb{N}$ — количество ОО.

Каждый объект оценки OO_i имеет набор функций безопасности $\left\{ФБ_1^i, ФБ_2^i, \ldots, ФБ_{k_i}^i\right\}$, где k_i — количество функций безопасности ОО OO_i, $i = 1,2,\ldots,w$. Под функцией безопасности будем понимать части (или часть) аппаратуры СС (ОО), обеспечивающие выполнение подмножества взаимосвязанных правил политики безопасности. В качестве примеров функций безопасности можно привести функции разграничения доступа, очистки памяти, регистрации событий, идентификации и аутентификации. Множество функций безопасности OO_i обозначим $ФБО_i$, $i = 1,2,\ldots,w$. С каждым множеством функций безопасности $ФБО_i$ связано множество интерфейсов к функциям безопасности аппаратуры СС $ИФБО_i = \left\{ИФ_1^i, ИФ_2^i, \ldots, ИФ_{z_i}^i\right\}$, где z_i — количество интерфейсов к функциям безопасности OO_i (например, графический интерфейс или внешний сетевой интерфейс). Выделение интерфейсов к функциям безопасности может быть выполнено как физически (в частности, внешний сетевой интерфейс), так и логически (интерфейс «командная строка»). С каждым интерфейсом $ИФ_k^i \in ИФБО_i$ связано множество $V\left(ИФ_k^i\right)$ значений, которые он может принимать на вход от внешнего субъекта или объекта.

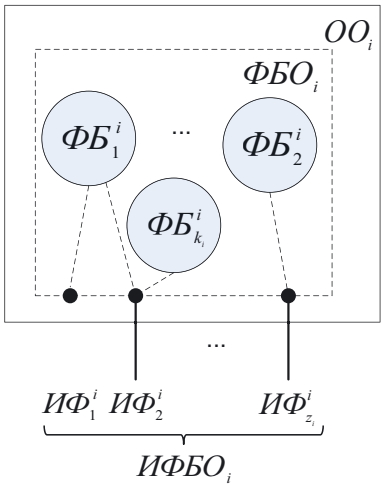

Рис. 2. **Модель комплекса средств защиты аппаратуры сетей связи**

Поскольку функции безопасности аппаратуры СС и интерфейсы к ним являются уникальными [10], множества

$$ФБС = \left\{ФБ_j^i : j = 1,2\ldots,k_i,\ i = 1,2,\ldots,w\right\};$$

$$ИФБС = \left\{ИФ_f^g : f = 1,2,\ldots,z_g, g = 1,2,\ldots,w\right\}$$

не содержат повторяющихся элементов, а следовательно, наборы функций безопасности аппаратуры СС и интерфейсов к ним могут быть представлены в виде множеств $ФБС = \{ФБ_1, ФБ_2, \ldots, ФБ_m\}$ и $ИФБС = \{ИФ_1, ИФ_2, \ldots, ИФ_b\}$ соответственно, где $m = k_1 + k_2 + \ldots + k_w$, $b = z_1 + z_2 + \ldots + z_w$. Таким образом, концептуальная модель КСЗ аппаратуры СС может быть описана кортежем $\langle ФБС, ИФБС\rangle$.

Модель сертификационных испытаний. Проведем сертификационные испытания аппаратуры сети связи, КСЗ которой описывается кортежем $\langle ФБС, ИФБС\rangle$, на соответствие множеству $ТБС = \{ТБ_1, ТБ_2, \ldots, ТБ_n\}$ требований безопасности информации, сформулированных в нотации стандарта ISO 15408, где $n \in \mathbb{N}$ — количество требований. Функциональное тестирование при проведении сертификационных испытаний производится в процессе действия оценщика ATE_IND.2.2E. Запишем шаги оценщика, выполняемые им в рамках данного действия:

- шаг оценивания ATE_IND.2–4: оценщик должен определить тестируемое подмножество функций безопасности аппаратуры СС;
- шаг оценивания ATE_IND.2–5: оценщик разрабатывает тестовую документацию для тестируемого подмноже-

ства функций безопасности, детализация которой позволяет обеспечить воспроизводимость тестов;

- шаг оценивания ATE_IND.2–6: оценщик проводит тестирование;
- шаг оценивания ATE_IND.2–7: оценщик фиксирует необходимую информацию о тестах, которые составляют подмножество тестов;
- шаг оценивания ATE_IND.2–8: оценщик проверяет, соответствуют ли все фактические результаты тестирования ожидаемым результатам тестирования.

Функциональное тестирование КСЗ аппаратуры СС выполняется для множества *ФБС*: в ходе выполнения шага оценивания ATE_IND.2–4 эксперт испытательной лаборатории идентифицирует все множество *ФБС*.

Для проведения испытаний (шаг оценивания ATE_IND.2–5) разрабатывается множество тестов $ST = \{st_1, st_2, \ldots, st_n\}$, при этом тест st_i предназначен для проверки выполнения требования $ТБ_i$ [11]. Каждый тест $st_i \in ST$ описывается:

- последовательностью выполняемых действий;
- множеством используемых при тестировании интерфейсов к функциям безопасности $S(st_i) = \{s_1^i, s_2^i, \ldots, s_{c_i}^i\} \subseteq ИФБС$ (c_i – количество интерфейсов, используемых при выполнении теста st_i);
- множеством значений, передаваемых интерфейсам в ходе тестирования $\mathfrak{V}_i = \{\langle h_1, h_2, \ldots, h_{c_i}\rangle\} = V(s_1^i) \times V(s_2^i) \times \ldots \times V(s_{c_i}^i)$;
- ожидаемыми результатами (критерий принятия положительного решения).

Последовательность действий определяется набором шагов, выполняемых экспертом испытательной лаборатории для приведения КСЗ аппаратуры СС в исходное состояние, чтобы реализовать тестовую процедуру и генерацию входной последовательности, подаваемой на вход аппаратуры СС (шаг оценивания ATE_IND.2–6). Результаты тестовых процедур регистрируются различными программными средствами (шаг оценивания ATE_IND.2–7). Критерий принятия положительного решения должен содержать эталонные результаты тестовых процедур. При тестировании для каждого кортежа множества $\mathfrak{V}_i$ выполняется необходимая последовательность действий, фактические результаты сравниваются с ожидаемыми (шаг оценивания ATE_IND.2–8), после чего принимается решение об успешном или неуспешном выполнении теста.

Введем следующие определения.

Определение 1. Предикатом успешного выполнения теста $st_i \in ST$ будем называть логическую функцию $F_{ST} : ST \to \{0,1\}$:

$$F_{ST}(st_i) = \begin{cases} 1, \ \forall \langle h_1, h_2, \ldots, h_{c_i}\rangle \in \mathfrak{V}_i : \text{тест } st_i \text{ выполнен успешнс} \\ 0, \ \text{в противном случае.} \end{cases}$$

Определение 2. Матрицей покрытия требований безопасности функциями безопасности аппаратуры СС будем называть матрицу $R = (r_{i,j}) \in \{0,1\}^{n \times m}$:

$$r_{i,j} = \begin{cases} 1, \text{ требование } ТБ_i \text{ выполняется функцией безопасности } ФБ_j; \\ 0, \text{ в противном случае.} \end{cases}$$

Определение 3. Предикатом декларации выполнения требования $ТБ_i \in ТБС$ для аппаратуры СС будем называть логическую функцию $F_R : ТБС \to \{0,1\}$:

$$F_R(ТБ_i) = \bigcup_{j=1}^{m} r_{i,j}.$$

При анализе декларации выполнения требований эксперт испытательной лаборатории должен исследовать представленную для проведения испытаний документацию на аппаратуру СС, чтобы сделать заключение, содержится ли в ней для каждого требования безопасности $ТБ_i$ приемлемое логическое обоснование того, что множество функций безопасности *ФБС* пригодно для удовлетворения данного требования.

Таким образом, концептуальная модель сертификационных испытаний аппаратуры СС характеризуется кортежем $\langle ФБС, ИФБС, ТБС, ST, F_R, F_{ST}\rangle$. Запишем основные стадии сертификационных испытаний аппаратуры СС.

1. На стадии анализа исходных данных собирается исходная информация об объекте сертификации. Рассматриваются документация на аппаратуру СС, представляемая разработчиком для проведения сертификационных испытаний, а также требования нормативных и методических документов. Выполняется анализ логической и физической структуры аппаратуры СС для определения подсистем защиты информации, функций безопасности и интерфейсов к функциям безопасности. В результате экспертами формируются модель КСЗ аппаратуры СС, которая описывается кортежем $\langle ФБС, ИФБС\rangle$, и множество тестируемых функций безопасности (шаг оценивания ATE_IND.2–4).

2. При построении матрицы покрытия требований безопасности эксперты лаборатории анализируют КСЗ аппаратуры СС и устанавливают связь между требованиями безопасности и функциями безопасности, которые обеспечивают выполнение этих требований. В результате формируется матрица $R = (r_{i,j}) \in \{0,1\}^{n \times m}$.

3. На основе анализа документации на КСЗ аппаратуры СС устанавливается, декларируется ли в ней факт выполнения того или иного требования безопасности. В результате формируется кортеж значений предиката выполнения требований $\langle F_R(ТБ_1), \ldots, F_R(ТБ_n)\rangle$.

4. На основе модели КСЗ аппаратуры СС эксперты лаборатории разрабатывают множество тестов для проведения сертификационных испытаний (шаг оценивания ATE_IND.2–5).

5. В ходе испытаний эксперты, используя разработанные тестовые процедуры, оказывают воздействие на идентифицированные интерфейсы к функциям безопасности аппаратуры СС с целью получения отклика от нее (шаг оценивания ATE_IND.2–6).

6. В отчетных материалах эксперты фиксируют следующую информацию (шаг ATE_IND.2–7):

- идентификационную информацию тестируемого режима выполнения функции безопасности;
- инструкции по подключению и настройке всего необходимого оборудования для тестирования, как это требуется для выполнения конкретного теста;
- инструкции по установке всех предварительных условий выполнения теста;
- инструкции по инициированию функции безопасности;
- инструкции по наблюдению за режимом выполнения функции безопасности;
- описание всех ожидаемых результатов и необходимого анализа, проводимого по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;
- инструкции по завершению теста;
- фактические результаты тестирования.

Эксперты лаборатории сравнивают фактические результаты теста с эталонными значениями, приведенными в описании тестовой процедуры (шаг оценивания ATE_IND.2–8). В результате формируется кортеж значений предиката успешного выполнения теста $\langle F_{ST}(st_1),\ldots,F_{ST}(st_n)\rangle$.

7. Анализ результатов проведения испытаний заключается в просмотре результатов испытаний экспертами лаборатории и руководителями групп. Для аппаратуры СС декларируется соответствие множеству ТБС требований безопасности информации, если

$$\forall i \in \{1,\ldots,n\} F_R(ТБ_i) = 1, F_{ST}(st_i) = 1 .$$

8. По результатам сертификационных испытаний оформляются технический отчет об оценке и техническое заключение, содержащее решение о соответствии/несоответствии аппаратуры СС установленным требованиям.

Минимизация времени проведения сертификационных испытаний. Оценим время проведения сертификационных испытаний, выполняемых в соответствии с разработанной моделью. В общем случае этот параметр растет экспоненциально, в зависимости от количества интерфейсов к функциям безопасности аппаратуры СС. Проведем сертификационные испытания аппаратуры СС (КСЗ которой описывается кортежем $\langle ФБС, ИФБС\rangle$) на соответствие множеству $ТБС = \{ТБ_1, ТБ_2,\ldots, ТБ_n\}$ требований безопасности информации с использованием множества тестов $ST = \{st_1, st_2,\ldots, st_n\}$ (тест st_i предназначен для проверки выполнения требования $ТБ_i$), $i \in \mathbb{N}$ — число требований. При тестировании для каждого кортежа множества $\mathfrak{P}_i = \left\{\left\langle h_1, h_2,\ldots, h_{c_i}\right\rangle\right\} = V\left(s_1^i\right)\times V\left(s_2^i\right)\times\ldots\times V\left(s_{c_i}^i\right)$ выполняется необходимая последовательность действий, где $S(st_i) = \left\{s_1^i, s_2^i,\ldots, s_{c_i}^i\right\} \subseteq ИФБС$ (c_i – количество интерфейсов, используемых при выполнении теста st_i).

Запишем время проведения тестирования:

$$\mathcal{T}_T^{ИС} = \sum_{i=1}^{n} t_i |\mathfrak{P}_i| = \sum_{i=1}^{n} t_i \prod_{j=1}^{c_i} \left|V\left(s_j^i\right)\right| \le \sum_{i=1}^{n} t_i M_i^{c_i} \approx ntM^c,$$

где n — количество тестов; t_i — время проведения теста st_i на одном наборе входных данных; $M_i = \max\left(\left|V\left(s_1^i\right)\right|, \left|V\left(s_2^i\right)\right|,\ldots, \left|V\left(s_{c_i}^i\right)\right|\right)$; $M = \max(M_1, M_2,\ldots, M_n)$; $c = \max(c_1, c_2,\ldots, c_n)$; $t = \max(t_1, t_2,\ldots, t_n)$.

Сокращение времени проведения испытаний возможно, в первую очередь, за счет уменьшения мощности проверяемого множества значений, передаваемых интерфейсам к функциям безопасности в ходе тестирования (выборочный контроль) [12]. Перечислим основные способы выборочного контроля, которые применяются в настоящее время при тестировании программного обеспечения (ПО) и использование которых во время сертификационных испытаний аппаратуры СС может быть целесообразным.

1. Тестирование с использованием случайных значений входных параметров. Значения компонент x_i входного кортежа $\hat{x} = (x_1, x_2,\ldots, x_s)$ генерируются случайным образом из областей допустимых значений $D_{x_i}^P$. Тестирование заканчивается при достижении приемлемого покрытия пространства входных значений.

2. Тестирование с разбиением области допустимых значений на эквивалентные подмножества. Области допустимых значений $D_{x_i}^P$ компонент входного кортежа разбиваются на подмножества $D_{x_{ij}}^P$, значения которых считаются эквивалентными с точки зрения функциональных особенностей тестируемого ПО. При тестировании на вход ПО в качестве компонента кортежа подается один представитель подмножества $D_{x_{ij}}^P$.

3. Тестирование граничных значений. В этом случае в первую очередь тестируются граничные значения областей допустимых значений $D_{x_i}^P$ компонент входного кортежа.

4. Тестирование, основанное на анализе рисков. Тестируются наиболее критичные функциональные возможности или требования. Приоритизация выполняется с использованием аппарата анализа рисков.

5. Тестирование на основе покрывающих наборов глубины t. При этом выполняется генерация входных кортежей, покрывающих все возможные значения подкортежей из t компонент.

Отметим, что способы 2 и 3 в большей степени ориентированы на тестирование ПО, а выборочное тестирование может с успехом использоваться как при тестировании ПО, так и при его сертификации. Тестирование на основе анализа рисков достаточно исследовано в работах российских и зарубежных ученых, при этом необходимость обеспечения повторяемости и воспроизводимости сертификационных испытаний аппаратуры СС накладывает ограничения на использование случайных выборок. С учетом данных особенностей для минимизации времени проведения испытаний целесообразно применять покрывающие наборы. Покрывающим набором глубины h для теста $st_i \in ST$ будем называть матрицу из c_i столбцов [13], таких, что в j-м столбце стоят значения из множества $V\left(s_{c_j}^j\right)$ значений, передаваемых интерфейсу в ходе тестирования, и любая комбинация возможных значений любых h-факторов встречается хотя бы в одной из ее строк. В общем случае для проведения h-факторного тестирования n входных параметров, принимающих v значений, потребуется количество тестов, пропорциональное $v^t \log n$. Отметим, что построение покрывающих наборов тестирования является NP-трудной задачей [13]. Например, при $h = 2$ (двухфакторное тестирование) на основе известных оценок размера минимальных покрывающих наборов можно получить следующую оценку мощности кортежа $\mathfrak{P}_i^* \subseteq V\left(s_1^i\right)\times V\left(s_2^i\right)\times\ldots\times V\left(s_{c_i}^i\right)$ значений, принимаемых на вход интерфейсами функций безопасности, которые используются при испытаниях:

$$\left|\mathfrak{P}_i^*\right| \approx M_i^2 \log c_i,$$

где $M_i = \max\left(\left|V\left(s_1^i\right)\right|, \left|V\left(s_2^i\right)\right|,\ldots, \left|V\left(s_{c_i}^i\right)\right|\right)$, $\left\{s_1^i, s_2^i,\ldots, s_{c_i}^i\right\}$ — множество используемых при тестировании интерфейсов к функциям безопасности.

Тогда время проведения тестирования можно оценить следующим образом:

$$\mathcal{T}_T^* \approx \sum_{i=1}^{n} t_i M_i^2 \log c_i \approx ntM^2 \log c,$$

где n — количество тестов; $M = \max(M_1, M_2,\ldots, M_n)$; $c = \max(c_1, c_2,\ldots, c_n)$; $t = \max(t_1, t_2,\ldots, t_n)$.

Таким образом, применение покрывающих наборов позволяет сократить время испытаний, поскольку размер покрывающего набора растет логарифмически от количества интерфейсов к функциям безопасности. При этом обеспечивается повторяемость и воспроизводимость испытаний.

Заключение. В ходе проведенных исследований был выполнен синтез множества функциональных требований безопасности, которые могут использоваться для задания требований безопасности информации к аппаратуре СС, например в рамках проведения испытаний. Формирование множества ФТБ осуществляется с учетом последних тенденций нормативной базы, связанных с использованием методологии метастандарта ISO 15408. Синтезированное множество ФТБ может быть положено в основу пакета профилей защиты аппаратуры СС.

Разработанные с учетом метастандарта ISO 15408 модель комплекса средств защиты аппаратуры СС и модель сертификационных испытаний аппаратуры СС обеспечивают детерминированность процесса испытаний и выполнение свойств повторяемости и воспроизводимости.

При исследовании возможностей минимизации времени проведения сертификационных испытаний выдвинуто предположение, что сокращение времени проведения испытаний может быть достигнуто за счет использования покрывающих тестовых наборов, при этом обеспечивается выполнение свойств повторяемости и воспроизводимости.

ЛИТЕРАТУРА

1. **Гордиенко В.Н.** Телекоммуникационные и вычислительные системы // Электросвязь. — 2010. — № 2. — С. 58–61.
2. **Донос А.Е.** Киберпространство под защитой РСС // Электросвязь. — 2011. — № 5. — С. 8–9.
3. **Лучин Д.В., Сподобаев М.Ю.** Системы ДКМВ радиосвязи: разработка, производство и перспективные решения // Вестник Самарского государственного аэрокосмического университета им. академика С.П. Королёва. — 2014. — № 2 (44). — С. 74–79.
4. **Марков А.С., Рауткин Ю.В., Фадин А.А.** Состояние и перспективы анализа защищенности Wi-Fi сетей // Труды НИИР. — 2012. — № 1. — С. 79–84.
5. **Чобанян В.А., Шахалов И.Ю.** Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. — 2013. — № 1(1). — С. 17–27.
6. STO-56947007–33.060.40.177–2014. ТТТ к аппаратуре высокочастотной связи по линиям электропередач.
7. **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.
8. **Барабанов А.В., Марков А.С., Рауткин Ю.В.** Оценка соответствия средств защиты информации требованиям высших оценочных уровней доверия // Труды НИИР. — 2012. — № 3. — С. 67–73.
9. **Markov A., Luchin D., Rautkin Y., Tsirlov V.** Evolution of a Radio Telecommunication Hardware-Software Certification Paradigm in Accordance with Information Security Requirements, in Proceedings of the 11th International Siberian Conference on Control and Communications (Omsk, Russia, May 21–23, 2015), SIBCON-2015, IEEE, Omsk, Russia, 2015, pp. 1–4. DOI= http://dx.doi.org/10.1109/SIBCON.2015.7147139.
10. **Зырянова Т.Ю.** Модель системы управления информационной безопасностью в условиях неопределенности воздействия дестабилизирующих факторов: автореф. дис. … канд. техн. наук. — Томск, 2008. — 25 с.
11. **Барабанов В., Марков А.С., Цирлов В.Л.** Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. — 2011. — № 3. — С. 48–52.
12. **Веряев А.С., Барабанов А.В., Марков А.С., Авезова Я.Э., Шахалов И.Ю., Цирлов В.Л.** Система оценки защищенности автоматизированных систем на основе выборочного комбинаторного контроля // Патент RUS148904, 10.09.2014, заявка № 2014136618. Бюл. № 35. — 3 с.
13. **Кулямин В.В., Петухов А.А.** Обзор методов построения покрывающих наборов // Программирование. — 2011. — № 3. — С. 3–41.

Получено 13.07.15