УДК 004.056.5

МЕТОД ОЦЕНКИ СООТВЕТСТВИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОБЩИМ КРИТЕРИЯМ

А.В. Барабанов, **А.С. Марков**, **И.В. Найханова**

МГТУ им. Н.Э. Баумана, Москва, Россия
e-mail: mail@cnpo.ru; a.barabanov@cnpo.ru; i.naihanova@gmail.com

Рассмотрены вопросы сертификации средств защиты информации по требованиям безопасности информации и особенностям оценки соответствия продукции согласно высшим оценочным уровням доверия. Приведены свидетельства, требуемые от разработчика при выполнении сертификационных испытаний, а также особенности их оформления с использованием формальных и полуформальных стилей изложения. На основе методологии "Общих критериев" введено формальное описание процесса оценки соответствия, которое может использоваться испытательными лабораториями при планировании и проведении сертификационных испытаний в соответствии с требованиями новой нормативной базы ФСТЭК России. Рассмотрены основные методы, используемые испытательными лабораториями при проведении испытаний (экспертно-документальный метод, функциональное тестирование, статический и динамический анализ исходных текстов, тестирование проникновением), а также особенности их применения в свете новой нормативной базы. Предложены методические рекомендации по оптимизации процесса оценки соответствия, позволяющие сократить временные и материальные затраты.

Ключевые слова: общие критерии, критерии оценки безопасности информационных технологий, оценочный уровень доверия, информационная безопасность, сертификационные испытания.

TECHNIQUE FOR EVALUATION OF COMPLIANCE OF INFORMATION SECURITY MEANS WITH COMMON CRITERIA

A.V. Barabanov, **A.S. Markov**, **I.V. Naikhanova**

Bauman Moscow State Technical University, Moscow, Russia
e-mail: mail@cnpo.ru; a.barabanov@cnpo.ru; i.naihanova@gmail.com

The problems of certification of information security means according to information security requirements and the peculiarities of evaluation of output compliance with the higher evaluation assurance levels are considered. Certificates that are demanded from the developer during the conduction of certification tests as well as peculiarities of their representation using formal and semi-formal styles of writing are given. Based on Common Criteria methodology, a formal description of the compliance evaluation is introduced, which can be used in test laboratories for planning and conduction of certification tests in accordance with requirements of the new normative base of the Federal Service on Technical and Export Control of Russia. Basic methods used in test laboratories during the test conduction (expert-documental method, functional testing, static and dynamical analysis of source texts, testing by penetration), as well as peculiarities of their using in view of the new normative base are considered. The methodic recommendations on optimization of the compliance evaluation are offered, which allow the time and material expenditures to be reduced.

Keywords: common criteria, evaluation criteria for information technology security, evaluation assurance level, information security, certification testing.

В настоящее время во всех системах обязательной сертификации средств защиты информации (СЗИ) проводятся изыскания по внедрению методологии оценки соответствия, основанной на международном метастандарте ГОСТ Р ИСО/МЭК 15408. Нормативные документы, соответствующие данному стандарту, принято называть общими критериями (ОК). Популярность ОК связана с возможностью гибкого формирования необходимых требований по безопасности и качеству любого СЗИ (объекта оценки) с учетом актуальных угроз, среды разработки и функционирования, принятых политик [1–3]. В то же время внедрение ОК связано с такими трудностями, как сложность восприятия и проверка большого числа требований, указанных в дополнительной документации, в том числе нотационного вида [4]. Наиболее проблемной является оценка соответствия СЗИ, к которым предъявляются повышенные требования по безопасности. Так, опыт работы показал, что при сертификации СЗИ в соответствии с ОК и высшими оценочными уровнями доверия (ОУД) могут потребоваться весьма большие материальные и временные затраты как со стороны разработчика, так и со стороны испытательных лабораторий, нежели при сертификации, выполняемой по традиционным нормативным документам.

В настоящей статье рассмотрены особенности выполнения процедуры оценки соответствия согласно требованиям высших ОУД и предложены способы их оптимизации.

Особенности проведения процедуры оценки соответствия. Сертификация СЗИ в соответствии с требованиями ОК обычно выполняется для одного из предопределенных ОУД, которых всего семь (самый слабый – ОУД1). Наиболее авторитетными при проведении сертификации средств защиты конфиденциальной информации являются ОУД3 и ОУД4. В случае защиты информации систем высокого риска, в том числе защиты государственной тайны, применяют усиленные ОУД.

В зависимости от ОУД разработчик предоставляет данные разного объема и сложности, содержащие: задание по безопасности (ЗБ); проектную документацию; представление реализации; документацию, касающуюся жизненного цикла изделия; описание процедуры тестирования; анализ уязвимостей.

Задание по безопасности — весьма объемный документ, представленный в нотациях ОК, который может быть разработан на основе сертифицированных профилей защиты [5] или самостоятельно. Форма ЗБ принципиально не зависит от уровней ОУД.

Стиль изложения проектной документации меняется в зависимости от ОУД и может быть неформальным, допускающим использование естественного языка (ОУД4 и ниже); полуформальным – когда документы написаны в предопределенном справочном формате (ОУД5,

ОУД6); формальным, т.е. с использованием математического аппарата, позволяющего строго верифицировать правильность функционирования объекта оценки (ОУД7).

Для программных СЗИ представлением реализации является множество исходных текстов, которые предоставляются, начиная с ОУД4. На практике для исходных текстов ОУД4 и ОУД5 допускается реализация функций безопасности, декларируемых в ЗБ. Для ОУД6 и ОУД7 требуется представление полного набора исходных текстов.

Отметим, что ОУД определяет требования посредством принятия для всех этапов разработки объекта оценки (ОО) конкретной модели жизненного цикла, включая политики и процедуры устранения недостатков, правильное использование методов и инструментальных средств, а также меры безопасности для защиты среды разработки.

Тестовые процедуры — процедуры, представленные разработчиком, а также дополнительно разработанные испытательной лабораторией. При независимом тестировании СЗИ до ОУД6 включительно можно использовать подмножество тестовых процедур разработчика, но для ОУД7 все тестовые процедуры должны быть разработаны исключительно экспертами независимой испытательной лаборатории.

Что касается анализа уязвимостей, то для ОУД4 необходимо проведение независимого анализа эксплуатационной, проектной и конструкторской документации на ОО в целях определения потенциальных уязвимостей в реализации ОО. Такой анализ может базироваться на информации, приведенной в общедоступных источниках (бюллетенях), об известных уязвимостях аналогичных по назначению продуктов. Начиная с ОУД5, испытательная лаборатория должна выполнять независимый *методический анализ* уязвимостей с учетом потенциала нарушителя. Данный вид анализа является более строгим и, например, может быть основан на построении и анализе деревьев атак.

Еще один важный момент — для высоких ОУД разработчик должен провести поиск скрытых каналов для каждой политики управления информационными потоками.

В заключение следует указать, что кроме уровня ОУД на объем работ по оценке соответствия, разумеется, влияют декларированные в ЗБ функции безопасности ОО.

Формальное описание процедуры оценки соответствия. Согласно требованиям ОК, процедуру оценки соответствия можно описать следующим образом. Пусть $C = \{c_1, c_2, \ldots, c_n\}$ — множество компонент требований доверия к безопасности, предъявляемых к ОО Σ. Как правило, множество C формируется с использованием одного из предопределенных ОУД. Для каждой компоненты требования доверия c_i определено множество действий $E^{(i)} = \left\{e_1^{(i)}, e_2^{(i)}, \ldots, e_{n_i}^{(i)}\right\}$ (n_i — число действий оценщика для компоненты c_i), которые должен выполнить оценщик (как правило, аккредитованная испытательная лабора-

тория) для подтверждения соответствия ОО предъявляемой компоненте c_i. Для каждого действия оценщика $e_j^{(i)}$ разрабатывается множество $S_j^{(i)} = \left\{ s_{j\_1}^{(i)}, s_{j\_2}^{(i)}, \ldots, s_{j\_m_j^{(i)}}^{(i)} \right\}$ шагов оценивания — наименьшей структурной единицы работ по оцениванию ($m_j^{(i)}$ — число шагов оценивания для действия оценщика $e_j^{(i)}$).

В табл. 1 приведен пример действий оценщика и шагов оценивания для компоненты доверия ATE_IND.2 “Выборочное независимое тестирование”.

Таблица 1

Пример действий оценщика и шагов оценивания

Компонента доверия c_i	Действие оценщика $e_k^{(i)}$	Шаг оценивания $s_{j\_v}^{(i)}$
ATE_IND.2	ATE_IND.2.1E Оценщик должен подтвердить, что предоставленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств	ATE_IND.2-1 Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ
		ATE_IND.2-2 Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно
		ATE_IND.2-3 Оценщик должен исследовать набор ресурсов, представленных разработчиком, чтобы сделать заключение, эквивалентны ли они набору ресурсов, используемых разработчиком для функционального тестирования ФБО
	...	...
		...

Следует отметить, что разработка шагов оценивания выполняется экспертами испытательной лаборатории на основе методологии оценки безопасности информационных технологий, представленной в ГОСТ Р ИСО/МЭК 18045–2008.

По аналогии с данными работы [6] сформулируем *метод разработки шагов оценивания,* под которым будем понимать отображение $M : \Sigma \times E \to S$.

Функция M на основе действия оценщика $e_j^{(i)}$ и информации о реализации (свидетельств разработчика) ОО Σ выполняет генерацию множества шагов оценивания $S_j^{(i)}$, необходимого для проверки удовлетворения ОО множеству C компонент требований доверия к безопасности. Как правило, функция M для ОО Σ является биективным отображением.

Оператором корректности выполнения действия оценщика $e_j^{(i)} \in E^{(i)}$ для ОО Σ назовем $F_S : \Sigma \times E \to \{0, 1\}$:

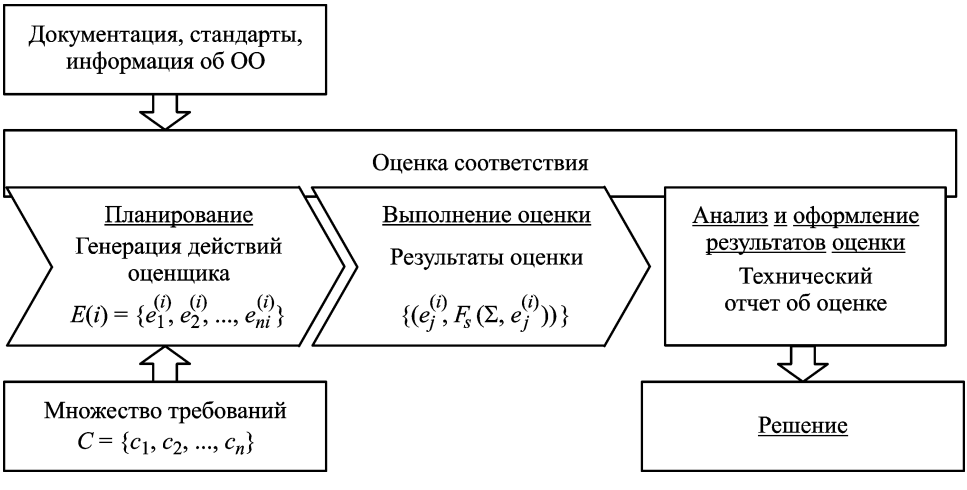
$$F_S(\Sigma, e_j^{(i)}) = \begin{cases} 1, \text{ если для } OO \ \Sigma \text{ все шаги оценивания действия } e_j^{(i)} \\ \quad \text{выполнены успешно,} \\ 0 \text{ в противном случае.} \end{cases}$$

Процедурой оценки назовем набор из четырех объектов $\mathrm{A} = \{\Sigma, C, M, F_S\}$, где C — множество компонент требований доверия к безопасности, предъявляемых к ОО Σ; M — метод разработки шагов оценивания; F_S — оператор корректности выполнения действия оценщика.

Процедура предусматривает наличие трех стадий: планирование, выполнение оценки, анализ и оформление результатов оценки (рисунок).

На стадии планирования выполняются задачи получения и анализа исходных данных для проведения оценки. На основе выполненного анализа формируются множества $E^{(i)} = \left\{e_1^{(i)}, e_2^{(i)}, \ldots, e_{n_i}^{(i)}\right\}$ действий оценщика и соответствующих им шагов оценивания. Оценка выполняется с использованием сформированного набора шагов оценивания.

Заключительная стадия предполагает выполнение анализа результатов оценки: сравнение фактических и эталонных результатов. В результате анализа получаем множество упорядоченных пар вида $\left(e_j^{(i)}, F_S(\Sigma, e_j^{(i)})\right)$. Для ОО Σ соответствие компоненте требования доверия c_i, если в ходе выполнения множества действий оценщика $E^{(i)} = \left\{e_1^{(i)}, e_2^{(i)}, \ldots, e_{n_i}^{(i)}\right\}$ для каждого получены положительные



Процедура оценки в соответствии с ОК

результаты, декларируется следующим образом:

$$\sum_{j=1}^{n_i} \left(F_S(\Sigma, e_i^{(j)}) \right) = n_i.$$

По результатам проведения оценки оформляется технический отчет об оценке. Для ОО декларируется соответствие требованиям доверия к безопасности $C = \{c_1, c_2, \ldots, c_n\}$, если $\forall i \in [1, n]$ $\sum_{j=1}^{n_i} \left(F_S(\Sigma, e_i^{(j)}) \right) = n_i$.

При проведении оценки, как правило, применяются следующие методы: экспертно-документальный; функциональное тестирование; статический и динамический анализ исходных текстов; тестирование проникновением.

Экспертно-документальный метод заключается в проверке соответствия ОО установленным требованиям на основании экспертной оценки полноты и достаточности представленных свидетельств и может использоваться для:

— анализа и проверки процессов и процедур, связанных с разработкой и реализацией ОО;

— анализа эксплуатационной документации;

— анализа разработанных функциональных тестов и полученных результатов;

— оценки соответствия параметров ОО исходным требованиям.

Функциональное тестирование заключается в проверке функций безопасности ОО с использованием специализированных тестирующих средств (применяется при независимом функциональном тестировании).

Статический анализ исходных текстов состоит в синтаксическом и семантическом анализе структуры и взаимосвязей функциональных и информационных объектов программ и построении маршрутов выполнения функциональных объектов. Динамический анализ представляет собой динамический контроль выполнения функциональных объектов (ветвей) программы (в отладочном режиме и/или с фиксацией трассы выполнения программы) и используется для детального исследования алгоритма программы [7]. Данные методы могут использоваться для выполнения:

— анализа соответствия между представлениями проекта ОО;

— анализа соответствия каждого представления проекта ОО установленным требованиям;

— анализа программных дефектов;

— проверки корректности представленных доказательств разработчика.

Тестирование проникновением заключается в санкционированной попытке обойти существующий комплекс средств защиты ОО. В ходе

тестирования оценщик играет роль злоумышленника, мотивированного на нарушение информационной безопасности.

Методические рекомендации по оптимизации процедуры оценки соответствия. Трудоемкость испытаний СЗИ по линии ОК связана, в первую очередь, с ростом числа разрабатываемых документов и дополнительных действий по оценке, выполняемых испытательной лабораторией. В данном случае задача оптимизации процедуры оценки ОО может быть сформулирована следующим образом.

Пусть $\tau : E \times \Sigma \to \mathrm{N}_0$ — время, затрачиваемое оценщиками на выполнение проверки ОО Σ с использованием действия оценщика $e_j^{(i)}$. Будем считать, что отображение вида $G : C \times \Sigma \to \mathrm{N}_0$ представляет затраты на проведение оценки ОО Σ требованиям C.

Решение задачи оптимизации может быть определено как получение минимума времени тестирования при ограничениях на затраты:

$$\sum_i \sum_j \tau\left(e_j^{(i)}, \Sigma\right) \to \min;$$
$$\sum_i G\left(c_i, \Sigma\right) \le G_M,$$

где G_M — ограничения, накладываемые на затраты.

Опыт проведения сертификационных испытаний СЗИ позволил определить ряд методических рекомендаций, существенно снижающих затраты на оценку соответствия, например (табл. 2) [8, 9]: совмещением проверок; использованием выборочного контроля, комбинаторного покрытия и средств автоматизации.

При проведении независимого функционального тестирования рекомендуется выполнять совмещение некоторых видов испытаний. Например, процедура тестирования подсистемы регистрации событий может быть совмещена с процедурой тестирования подсистемы разграничения доступа и идентификации/аутентификации [6].

Существенное сокращение работ может быть достигнуто при обосновании возможности проведения выборочного контроля, который позволяет применить процедуру проверки менее чем к 100 %-ной совокупности контролируемых элементов (например, свидетельств разработчика, тестируемых функций безопасности). При использовании методов выборочного контроля необходимо установить приоритеты проверяемых требований в целях дальнейшего определения необходимого числа тестируемых объектов [10].

Для сокращения временны́х затрат и повышения качества отчетных материалов при проведении испытаний необходимо использовать программные средства, позволяющие автоматизировать рутинные процедуры оценки соответствия. Для независимого тестирования можно использовать как инструментальные средства, широко представленные на современном рынке программного обеспечения, так и программы собственной разработки, написанные на языках сценариев (например,

perl или python), для анализа уязвимостей — сканеры безопасности, для документирования — программы типа Doxygen, для проведения анализа исходных текстов — анализаторы безопасности кода [7].

Таблица 2

Методические рекомендации по оптимизации оценки соответствия

Наименование метода	Семейство требований доверия
Совмещение отдельных видов испытаний	Независимое тестирование (ATE_IND)
Метод выборочного контроля	Представление реализации (ADV_IMP) Внутренняя структура ФБО (ADV_INT) Возможности управления конфигурацией (ALC_CMC) Функциональное тестирование (ATE_FUN) Независимое тестирование (ATE_IND) Анализ уязвимостей (AVA_VAN)
Использование программных средств при проведении функционального тестирования	Независимое тестирование (ATE_IND) Анализ уязвимостей (AVA_VAN)
Метод комбинаторного покрытия	Независимое тестирование (ATE_IND)
Использование систем документирования исходных текстов	Представление реализации (ADV_IMP)
Использование средства анализа исходных текстов программного обеспечения	Представление реализации (ADV_IMP)
Средства поиска уязвимостей	Анализ уязвимостей (AVA_VAN)

При инспекционном контроле сертифицированного ОО повторному анализу (например, в ходе выполнения независимого тестирования ATE_IND или анализа представления реализации ADV_IMP) могут подвергаться программные модули, измененные в ходе доработок. Неизменность программных модулей ОО может контролироваться испытательной лабораторией при использовании механизма электронно-цифровой подписи.

Следует отметить, что все рассмотренные методические приемы прошли апробацию в аккредитованной испытательной лаборатории, подтвердившую их эффективность [6, 8, 9].

Заключение. Рассмотренные в работе особенности процедуры оценки соответствия СЗИ требованиям высших ОУД показали, что, несмотря на все достоинства методологии ОК, очевидна сложность внедрения данного подхода как для разработчиков, так и для испытательных лабораторий. В целях повышения эффективности решения задачи оценки соответствия СЗИ разработаны формальное описание и критерии оценочных действий.

Для повышения качества отчетных материалов и сокращения затрат на выполнение рутинных процедур оценки соответствия предложен ряд методических приемов и способов.

При этом очевидно, что полный переход от сертификации СЗИ по требованиям традиционных руководящих документов к оценке соответствия по ОК повлечет за собой не только развитие нормативно-методической базы сертификации и аттестации, но и дальнейшие изыскания реализационных основ методологии ОК.

ЛИТЕРАТУРА

1. *Багаев Д.А.*, *Ланкин О.В.*, *Рогозин Е.А.* Способ определения комплексного показателя защищенности автоматизированных систем // Вопросы защиты информации. 2009. № 2. С. 8–10.
2. *Осовецкий Л.Г.*, *Суханов А.В.*, *Мануйлов Н.А.* Общие критерии: Реальность и мифы. Научно-технические аспекты // 9 НТК "Майоровские чтения". Теория и технология программирования и защиты информации. Применение вычислительной техники. СПб., 2005. С. 3–5.
3. *Статистика* внедрения "Общих критериев" в зарубежных странах / А.С. Марков и др. // Information Security / Информационная безопасность. 2006. № 1/2. С. 12–15.
4. *Грибунин В.Г.* "Общие критерии" на российской почве // Information Security / Информационная безопасность. 2005. № 1. С. 22–25.
5. *Бетелин В.В.*, *Галатенко В.А.*, *Кобзарь М.Т.*, *Сидак А.А.*, *Трифаленков И.А.* Профили защиты на основе "Общих критериев" // Аналитический обзор. JetInfo. Информационный бюллетень. 2003. № 3 (118).
6. *Барабанов А.В.*, *Гришин М.И.*, *Марков А.С.* Формальный базис и метабазис оценки соответствия средств защиты информации объектов информатизации // Изв. института инженерной физики. 2011. № 3. С. 82–88.
7. *Марков А.С.*, *Миронов С.В.*, *Цирлов В.Л.* Выявление уязвимостей программного обеспечения в процессе сертификации // Изв. Таганрогского государственного радиотехнического университета. 2006. Т. 62. № 7. С. 82–87.
8. *Барабанов А.В.*, *Марков А.С.*, *Цирлов В.Л.* Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. С. 48–53.
9. *Барабанов А.В.*, *Марков А.С.*, *Цирлов В.Л.* Разработка методики испытаний межсетевых экранов по требованиям безопасности информации // Вопросы защиты информации. 2011. № 3. С. 19–24.
10. *Барабанов А.В.* Методика оценки соответствия автоматизированных систем требованиям по защите информации от несанкционированного доступа с применением выборочного контроля // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2011. № 2. С. 104–115.

REFERENCES

1. *Bagaev D.A.*, *Lankin O.V.*, *Rogozin E.A.* The way to determine complex defense indicator of automated systems. *Vopr. Zashch. Inf.* [Probl. Inf. Prot.], 2009, no. 2, pp. 8–10 (in Russ.).
2. *Osovetskiy L.G.*, *Sukhanov A.V.*, *Manuylov N.A.* General criteria: myths and reality. Scientific and technological aspects. *Mayorovskie Chteniya: Trudy 9 Nauch. Tech. Konf. "Teoriya i tekhnologiya programmirovaniya i zashchity informatsii. Primenenie vychislitel'noy tekhniki"* [Mayorovskie Read.: Proc. 9 Sci. Tech. Conf. "Theory and technology of programming and information security. The application of computers"]. St. Petersburg, SPb Gos. Univ. Publ., 2005, pp. 3–5 (in Russ.).

3. *Markov A.S.* Statistics of general criteria implementation in foreign countries. Inf. Bezop. [Inf. Secur.], 2006, no. 1–2, pp. 12–15 (in Russ.).
4. *Gribunin V.G.* General criteria in Russia. *Inf. Bezop.* [Inf. Secur.], 2005, no. 1, pp. 22-25 (in Russ.).
5. *Betelin V.V.*, *Galatenko V.A.*, *Kobzar' M.T.*, *Sidak A.A.*, *Trifalenkov I.A.* Protection profiles based on general criteria. Analitical review. *Inf. Byull. JetInfo* [JetInfo Newsl.], 2003, vol. 118, no. 3, 32 p. (in Russ.).
6. *Grishin M.I.*, *Markov A.S.*, *Barabanov A.V.* A formal basis and metabasis for estimating the compliance of information protection means with informatization objects. *Izv. Inst. Inzh. Fiz.* [Proc. Inst. Eng. Phys.], 2011, no. 3, pp. 82–88 (in Russ.).
7. *Markov A.S.*, *Mironov S.V.*, *Tsirlov V.L.* Identification of software vulnerability in the certification process. *Izv. Taganrog. Gos. Radio Tekhn. Univ.* [Proc. Taganrog State Univ.], 2006, vol. 62, no. 7, pp. 82–87 (in Russ.).
8. *Barabanov A.V.*, *Markov A.S.*, *Tsirlov V.L.* A methodology for estimating the compliance of automated information systems with security requirements. *Spetstekhn. Svyaz'* [Spec. Equip. Commun.], 2011, no. 3, pp. 48–53 (in Russ.).
9. *Barabanov A.V.*, *Markov A.S.*, *Tsirlov V.L.* The development of a firewall testing technique to meet security requirements. *Vopr. Zashch. Inf.* [Probl. Inf. Prot.], 2011, no. 3, pp. 19–24 (in Russ.).
10. *Barabanov A.V.* A method for assessing the compliance of automated systems with the requirements to protect information from unauthorized access by using sampling inspection. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Ser. Priborostr.* [Herald of the Bauman Moscow State Tech. Univ. Ser. Instrum. Eng.], 2011, no. 2, pp. 104–115 (in Russ.).

Статья поступила в редакцию 27.02.2012

Алексей Сергеевич Марков — канд. техн. наук, доцент кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор более 120 научных работ в области качества, надежности и безопасности программных систем.
МГТУ им. Н.Э. Баумана, Россия, 105005, Москва, 2-я Бауманская ул., д. 5.

A.S. Markov — Cand. Sci. (Eng.), assoc. professor of "Information Security" department of the Bauman Moscow State Technical University. Author of more than 120 publications in the field of quality, reliability and security of software systems.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul., 5, Moscow, 105005 Russia.

Александр Владимирович Барабанов — аспирант кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор более 10 научных работ в области безопасности программного обеспечения.
МГТУ им. Н.Э. Баумана, Россия, 105005, Москва, 2-я Бауманская ул., д. 5.

A.V. Barabanov — post-graduate of "Information Security" department of the Bauman Moscow State Technical University. Author of more than 10 publications in the field of software security.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul., 5, Moscow, 105005 Russia.

Ирина Витальевна Найханова — аспирант кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор более 10 научных работ в области аудита информационной безопасности.
МГТУ им. Н.Э. Баумана, Россия, 105005, Москва, 2-я Бауманская ул., д. 5.

I.V. Naikhanova — post-graduate of "Information Security" department of the Bauman Moscow State Technical University. Author of more than 10 publications in the field of data security audit.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul., 5, Moscow, 105005 Russia.