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.

УДК 004.05; 681.3

А.В.Барабанов, А.С.Марков, В.Л.Цирлов

Об оценке соответствия средств защиты информации сообразно «Общим критериям»

Аннотация. Статья посвящена анализу системы сертификации средств защиты информации, проводимой в соответствии с методологией «Общих критериев» и ISO 15408. Проведен анализ статистики в области отечественной и международной сертификации средств защиты информации по требованиям безопасности информации. Дан краткий обзор новых пакетов нормативных методических документов ФСТЭК России. Показаны проблемные вопросы сертификации по линии «Общих критериев», касающиеся разработчиков изделий, а также испытательных лабораторий. Предложены пути преодоления трудностей, связанных с внедрением методологии «Общих критериев». Рассмотрены перспективы внедрения методологии «Общих критериев» в нашей стране и за рубежом.

Ключевые слова: безопасность информации, сертификация, средство защиты информации, общие критерии, методология общих критериев, критерии оценки безопасности информационных технологий, ИСО 15408, ИСО 18045, оценка соответствия

Введение

Последние два года ознаменовались выходом новых пакетов нормативных документов ФСТЭК России, касающихся оценки соответствия средств защиты информации (СЗИ) требованиям метастандарта ГОСТ ИСО/МЭК 15408, релевантного международной методологии «Общих критериев» (ОК). Указанные документы конкретизировали классический подход использования ОК для оценки соответствия ряда СЗИ в нашей стране. Ожидается постепенный переход от традиционных руководящих документов ФСТЭК России к новым документам для широкого класса современных и перспективных СЗИ.

Несмотря на накопленный опыт использования методологи ОК по линии ФСТЭК России, в смежных российских системах сертификации СЗИ указанный подход не получил пока глубокой проработки. Анализу потенциала развития подхода по линии ОК посвящена данная статья.

Историческая ретроспектива

В нашей стране система сертификации СЗИ по требованиям безопасности информации берет начало с 1995 года[1]. В основу организации сертификационных и аттестационных испытаний были положены нормативные документы директивного плана, касающиеся детерминированных требований к функциям безопасности, в частности, автоматизированных систем, комплексных СЗИ от несанкционированного доступа (НСД) и, чуть позже, межсетевых экранов (МЭ). С развитием информационных технологий и новых классов угроз информационной безопасности (ИБ) остро стал вопрос создания универсальной, гибкой и адаптивной системы нормативных документов, учитывающей типы СЗИ, среды функционирования и уровни защиты информации, но обеспечивающей повторяемость результатов испытаний [1-3]. С этой целью Технический комитет ТК-362 обеспечил перевод соответствующих международных стандартов (см.рис.1), а в рамках системы ФСТЭК России была инициирована апробация методологии ОК [4-7].

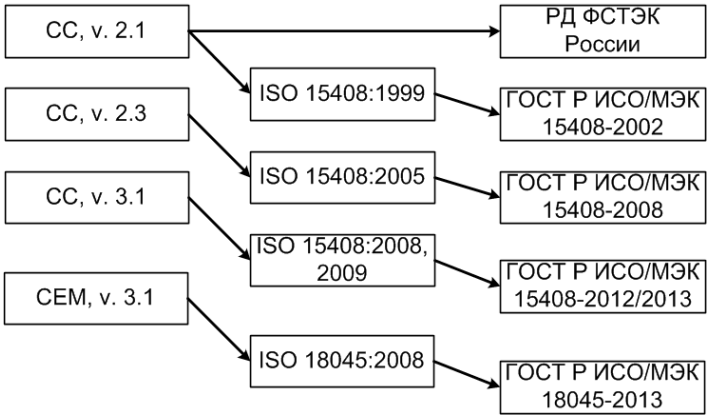

Рис. 1. Соответствие международных и национальных стандартов

Принципиально новым этапом внедрения методологии ОК в нашей стране стало утверждение пакетов требований для отдельных типов СЗИ, начиная с 2012 года [8]. Согласно новому подходу, для каждого типа СЗИ принимается нормативный правовой акт, содержащий требования по защите информации и устанавливающий классы защиты, содержащие минимальный набор требований. Для каждого типа СЗИ утверждаются профили защиты, которые являются основой для создания задания по безопасности, на соответствие которому и проводится сертификация конкретного изделия (рис. 2).

[1] См. Постановление Правительства РФ 1995 № 608

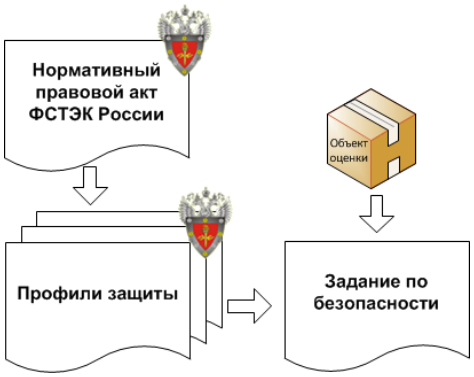

Рис. 2. Новый порядок задания требований по безопасности информации

В период 2012-2013 гг. были утверждены требования к системам обнаружения вторжений (СОВ) [9], средствам антивирусной защиты (САВЗ) [10] и средствам доверенной загрузки, а в ближайшее время ожидается принятие документов по DLP [11], средствам защиты среды виртуализации, средствам ограничения программной среды, средствам управления доступом, средствам управления потоками информации, средствам защиты каналов передачи информации, средствам контроля удаления информации, средствам идентификации и аутентификации, МЭ, средствам анализа защищенности (САЗ) и др.

В соответствии с этим перед испытательными лабораториям и разработчиками СЗИ возникла задача апробации новых документов, меняющих сложившиеся методики работ, а следовательно и трудозатраты [5]. Рассмотрим общие тенденции внедрения методологии ОК в нашей стране в сравнении с международной системой Common Criteria.

Задачи исследования

В основу проведенного анализа положены данные, представленные на сайте ФСТЭК России[2], портале международной системы сертификации Common Criteria[3], а также полученные в ходе авторских испытаний СЗИ и экспертизы материалов испытаний по линии ОК.

С точки зрения целей анализа важно было оценить:

- объемы и рост работ по оценке соответствия СЗИ;
- классы актуальных и перспективных СЗИ;
- долю импортной продукции в России;
- перспективы серийного производства в России;
- лидирующие компании в области создания СЗИ;
- открытие исходного кода и предоставление среды компоновки;
- оценочные уровни доверия, достижимые при сертификации на практике;
- распределение затрат испытательной лаборатории.

Общие тенденции оценки соответствия по линии «Общих критериев»

Проведенный анализ показал, что сертификация по линии ОК имеет устойчивый рост в мире и постепенно набирает оборот в нашей стране.

Первое, что бросается в глаза, - это то, что объемы сертификации в России не уступают международным, что объясняется государственной важностью результатов оценки соответствия СЗИ требованиям по безопасности информации, видимо, по причине зависимости от технологий иностранных производителей (рис.3). В то же время количество сертификаций в России в соответствии с международной методологией ОК невелико (рис.4).

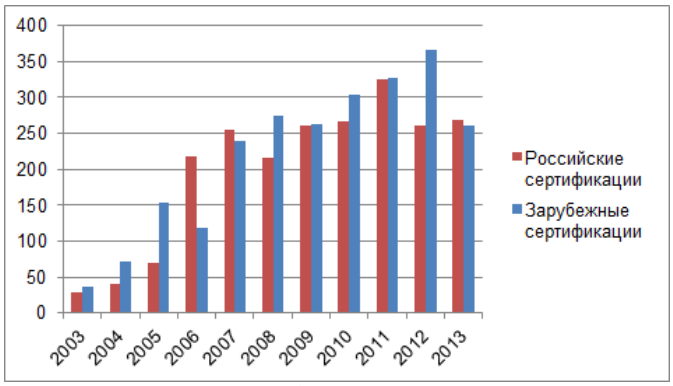

Рис. 3. Количество сертификаций по линии ФСТЭК России

[2] www.fstec.ru
[3] www.commoncriteriaportal.org

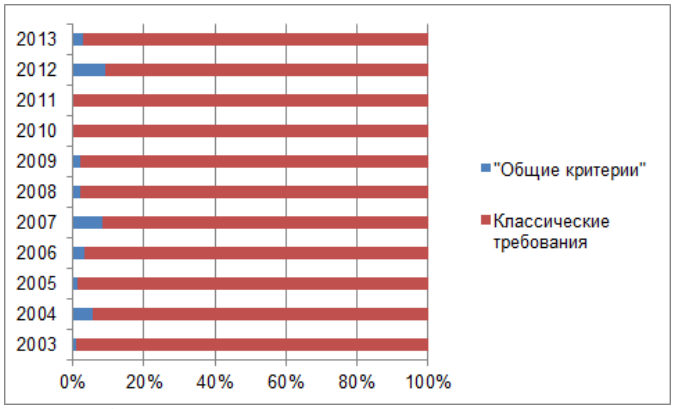

Рис. 4. Распределение числа сертификаций по традиционным документам и методологии «Общих критериев» в России

На рис. 5 представлено распределение числа сертификаций типов СЗИ в России (за период 2011-2013 гг.), а именно: МЭ, СЗИ от НСД, программного обеспечения (ПО) со встроенными СЗИ, ПО общего назначение (ОН), которое не содержит встроенных функций по защите информации, ПО, используемого в вычислительных сетях (ВС), кроме МЭ, операционных систем (ОС), САЗ, САВЗ, систем управления базами данных (СУБД) и СОВ. Очевидно, развитие защищенных сетевых технологий обусловило лидерство сертификации МЭ.

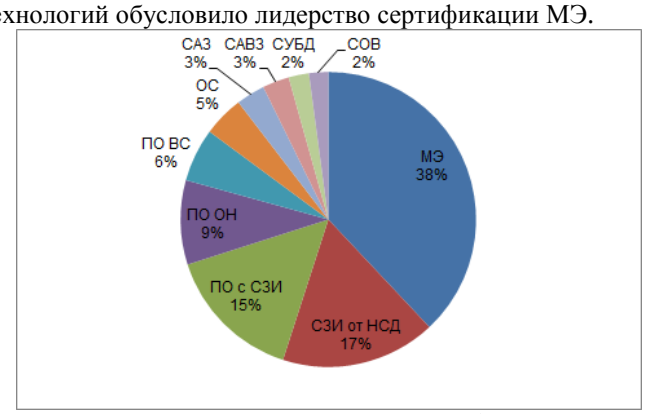

Рис. 5. Распределение по типам средств защиты информации в России

Аналогичный анализ, выполненный в отношении международной системы сертификации Common Criteria, позволил выявить актуальные зарубежные ИТ-решения в защищенном исполнении, а именно (рис.6):

- ПО, используемое в смарт-картах;
- многофункциональные устройства (например, принтеры);
- сетевое ПО (маршрутизаторы, коммутаторы).

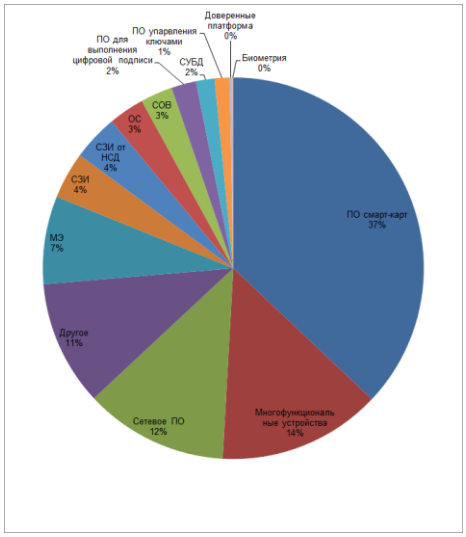

Рис. 6. Распределение по типам средств защиты информации в системе Common Criteria

Распределение числа испытаний СЗИ по схемам сертификации «серия» («типового образца») и «партия» (включая единичные устройства) по линии ФСТЭК России представлено на рис. 7.

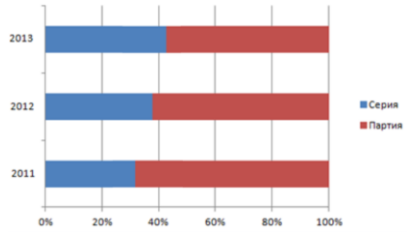

Рис. 7. Распределение по схемам сертификации в России

Распределение числа сертификаций СЗИ российского и импортного производства в системе ФСТЭК России за период 2011-2013 гг. представлено на рис. 8.

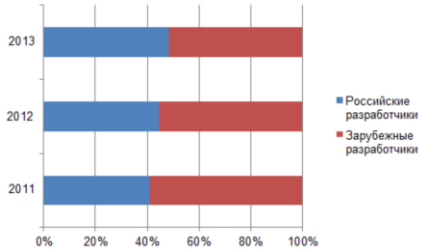

Рис. 8. Сертификации продукции российского и зарубежного производства в России

После вступления в силу нормативных правовых актов, задающих требования безопасности информации в нотации ОК, как отечественные так и зарубежные разработчики стали проводить сертификации в России по новым требованиям. Первые сертификации по новым требованиям были проведены зарубежными компаниями McAfee и TrendMicro. Среди отечественных разработчиков, получивших сертификаты соответствия ФСТЭК России, - «Код безопасности» и «Лаборатория Касперского».

На рис. 9 и 10 представлены иностранные и российские организации-разработчики СЗИ, наиболее часто сертифицируемые в системе сертификации ФСТЭК России за период 2011-2013 гг. Например, рис. 9 косвенно демонстрирует значимую роль продукции американской компании CISCO в создании информационной инфраструктуры нашей страны.

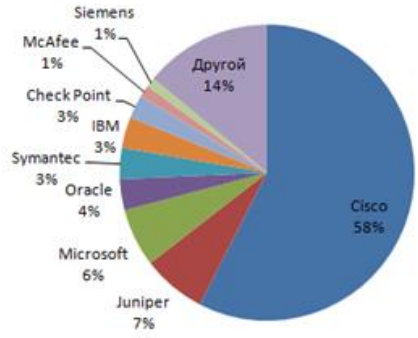

Рис. 9. Иностранные разработчики, продукция которых сертифицируется ФСТЭК России

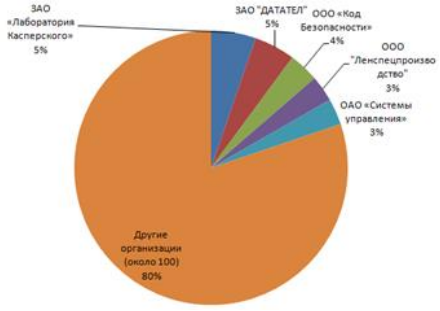

Рис. 10. Российские разработчики, продукция которых сертифицируется ФСТЭК России

Соответствующая статистика по разработчикам СЗИ, прошедших сертификацию в международной системе Common Criteria, представлена на рис. 11.

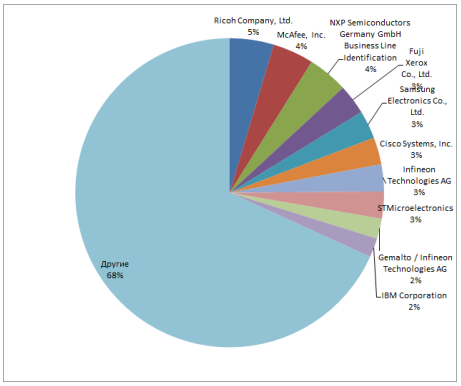

Рис. 11. Разработчики, продукция которых сертифицируется в системе Common Criteria

Соотношение числа сертификаций СЗИ, проводимых с предоставлением исходных программных кодов за период 2011-2013 гг., представлено на рис. 12. Как известно, гарантированные оценки уровня безопасности программных систем можно получить только при доступе к исходному коду [9]. Поэтому отставания нашей страны в этом плане должно настораживать.

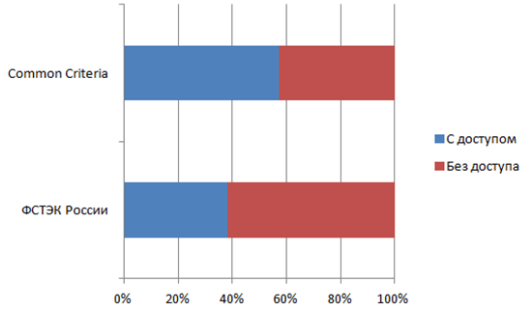

Рис.12. Соотношение сертификаций в зависимости от доступа к исходным текстам программ

Распределение числа отечественных и международных сертификаций в зависимости от оценочного уровня доверия (ОУД), подтверждение которому проверялось в ходе испытаний, представлено на рисунках 13 и 14. Как известно, уровню защиты информации, составляющей государственную тайну, соответствует ОУД4+ (усиленный) [9].

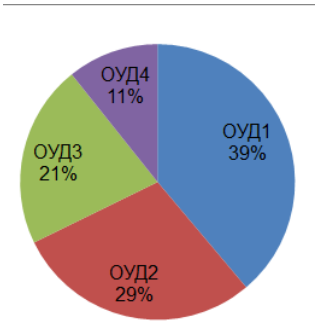

Рис. 13. Соотношение числа сертификаций в зависимости от ОУД во ФСТЭК России

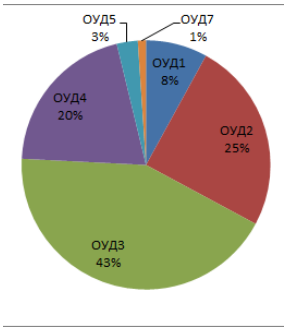

Рис. 14. Соотношение числа сертификаций в зависимости от ОУД в системе Common Criteria

Опыт работы испытательной лаборатории

Отдельного рассмотрения заслуживает вопрос оценки трудоемкости независимого тестирования при проведении сертификационных испытаний по новым требованиям. Анализ, проведенный авторами, исходя из опыта испытательной лаборатории, позволил сделать вывод о том, что плановая трудоёмкость самих проводимых тестов принципиально не изменилась по сравнению с традиционным подходом. На рис. 15 представлен сравнительный анализ затрат на испытания систем обнаружения вторжений (СОВ) на соответствие техническим условиям (ТУ) и нормативным документам (НД).

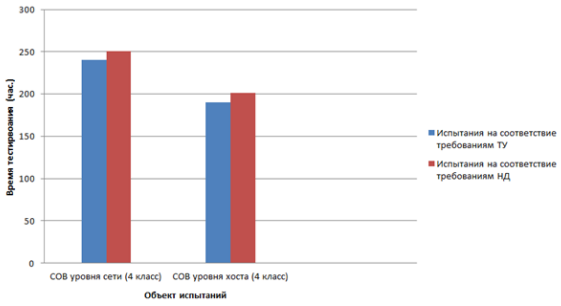

Рис. 15. Сравнительный анализ временных затрат при проведении независимого тестирования систем обнаружения вторжений

Анализ затрат на проверки СЗИ по методологии ОК показал следующее распределение трудоемкости работ (по убыванию) по требованиям новой нормативной базы (рис.16):

- анализ проектной документации на объект сертификации (ADV[4]);
- проведение независимого тестирования (ATE);
- анализ жизненного цикла объекта сертификации (ALC);

[4] Нотации указаны в соответствии с ISO 15408-3: 2009.

- анализ задания по безопасности (ASE);
- анализ эксплуатационной документации (AGD);
- проведение независимого тестирования на проникновение (AVA).

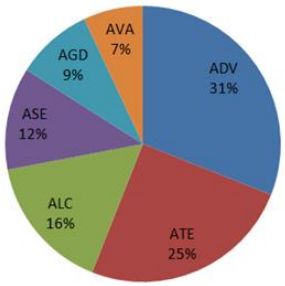

Рис. 16. Распределение затрат испытательной лаборатории при сертификации по требованиям новой нормативной базы

Зарубежные тенденции

Представленный в работе анализ был бы не полным, если не отметить альтернативное направление развития международной системы сертификации по Common Criteria. Например, с 2012 г. National Information Assurance Partnership (NIAP) - организация, регулирующая сертификацию СЗИ в США - инициировало коренную реформу системы сертификации по схеме ОК. Основные преобразования следующие:

1. Отказ от понятия «оценочный уровень доверия». Опыт проведения сертификации по классическим ОК показал, что во многих случаях невозможно обеспечить повторяемость и воспроизводимость сертификационных испытаний (даже при сертификации на ОУД3 или ОУД4). Предлагаемые новые профили защиты содержат упрощенные требования доверия, сформулированные на основе «классического» ОУД2. Такая тенденция была авторами предсказана девять лет назад [1].
2. Для обеспечения повторяемости результатов профили защиты дополняются типовыми методиками испытаний, причем, как для требований доверия, так и для функциональных требований безопасности.
3. Справочная информация (например, обоснования требований или целей безопасности) вынесена в приложение к профилям защиты.
4. Профили защиты разрабатываются техническими комитетами, в которые, как правило, входят представители разработчиков.
5. Создаются базовые профили защиты и пакеты расширений базового профиля защиты (Extended Package). Например, базовый профиль защиты на сетевое устройство задает функции безопасности, характерные для всех сетевых устройств (идентификация и аутентификация администратора, регистрация событий и т.д.), а пакет расширения базового профиля защиты содержит требования, характерные для конкретного типа СЗИ на базе сетевых устройств (например, МЭ или СОВ).

К реформе присоединились «коронованные территории»: Великобритания, Австралия, Канада.

Заключение

Проведенный анализ статистики в области «Общих критериев» позволил отметить ряд положительных моментов в сфере разработки и оценки соответствия СЗИ в нашей стране, а именно:

1. Стимулирование серийного производства продукции, выражающегося в постепенном уходе от сертификации по схеме «партия» к схеме «серия» ввиду того, что новые нормативные правовые акты ФСТЭК России требуют от заявителей поддержки сертифицированного ПО СЗИ на всех стадиях жизненного цикла.
2. Повышение реальной безопасности программных систем, так как утверждение новых нормативных правовых актов вводит обязательность выполнения процедуры «оценки уязвимостей» по всем классам защиты. Напомним, что при сертификации по традиционным руководящим документам поиск уязвимостей не являлся обязательной процедурой и выполнялся только энтузиастами в области сертификации СЗИ. Например, авторами были выявлены уязвимости в 50% зарубежных и отечественных СЗИ.
3. Повышение доверия к программной продукции, в первую очередь, иностранного производства, что связано с постепенным открытием испытательным лабораториям доступа к исходным текстам со стороны крупных мировых разработчиков ПО.
4. Возможность для разработчиков модифицировать и обновлять свои продукты между сертификациями, представляя необходимые свидетельства об отсутствии влияния обновлений на сертифицированные функции безопасности. Это связано с тем, что впервые в российских нормативных документах формализовано понятие «инспекционного контроля» с использованием требований класса АМА «Поддержка доверия», то есть новые профили защиты (утверждаемые ФСТЭК России) содержат требования доверия к безопасности, касающиеся возможной модификации программной продукции.
5. Концептуальная возможность интеграции и внедрения передовых иностранных ИТ-решений, которые прошли сертификацию по Common Criteria, то есть, когда иностранные разработчики уже разработали подобные рабочие документы и понимают процесс сертификации по новым требованиям ФСТЭК России.

В то же время надо отметить, что новые нормативные документы ФСТЭК России ввиду новизны потребуют доработки организационной и методической базы лабораторий и разработчиков, например:

1. Первые сертификации по линии ОК показали начальное увеличение интеллектуальных затрат у разработчиков отечественной продукции. Это связано с тем, что даже при сертификации на наиболее привлекательный 4-ый класс защиты (не связанный с защитой государственной тайны) требуется достичь ОУД3, а требуемые свидетельства разработчика являются относительно новыми: корреляции с национальными стандартами практически нет, нет и методических документов регуляторов для разработчиков СЗИ.

2. Недостаток реального опыта и методической информации приведет к неспособности всем без исключения аккредитованным лабораториям проводить испытания продукции по новым требованиям в самом ближайшем времени. Как вариант, возможно введение практики аккредитации испытательных лабораторий по наивысшему классу защиты (ОУД), по которому лаборатория может проводить испытания.

В заключение можно сделать вывод, что сертификация СЗИ по линии «Общих критериев» имеет устойчивые перспективы в нашей стране: внедрение методологических и концептуальных основ неизбежный процесс, как минимум, в ближайшей перспективе.

Литература

1. Статистика внедрения «Общих критериев» в зарубежных странах / А.С.Марков и др. // Information security. 2006. № 1/2. С. 12-15.
2. Barabanov A.V., Markov A.S., Tsirlov V.L. Russian IT Security Certification Scheme: Steps Toward Common Criteria Approach // 15th International Common Criteria Conference ICCC-2014 (9-11 September, 2014, New Delhi, India). 2014. P. 1-11.
3. Merkow M.S., Breithaupt J. Computer Security Assurance Using the Common Criteria. Thomson Delmar Learning, 2005. 278 p.
4. Higaki W.H. Successful Common Criteria Evaluations: A Practical Guide for Vendors. CreateSpace. 2010, 282 p.
5. Багаев Д.А. Требования к информационной безопасности автоматизированных систем на основе применения общих критериев // Вопросы защиты информации. 2009. № 2. С. 6-8.
6. Барабанов А.В., Марков А.С., Рауткин Ю.В. Оценка соответствия средств защиты информации требованиям высших оценочных уровней доверия // Труды Научно-исследовательского института радио. 2012. № 3. С. 67-73.
7. Дровникова И.Г., Никитин А.А. Требования к безопасности информационных технологий автоматизированных систем на основе применения общих критериев // Технологии техносферной безопасности. 2013. № 3 (49). С. 24.
8. Сидак А.А. Композиционный подход к формированию требований к изделиям, реализующим функции безопасности в информационных системах. Семейства профилей защиты // Стратегическая стабильность. 2013. № 3 (64). С. 40-42.
9. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под ред. А.С. Маркова. М.:Радио и связь, 2012. 192 с.
10. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31-33.
11. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации. // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2012. Спецвыпуск №5 "Информатика и системы управления". С.272-278.
12. Барабанов А.В., Гришин М.И., Марков А.С., Цирлов В.Л. Формирование требований по безопасности информации к DLP-системам // Вопросы радиоэлектроники. 2013. №2. С. 67-76.

A.V.Barabanov, **A.S.Markov**, **V.L.Tsirlov**

The conformity assessment of information security solutions according to the Common Criteria

Abstract. The information security certification in accordance with the Common Evaluation Methodology and ISO 15408 is analyzed. The analysis of statistics in the field of domestic and international certification of information security solutions are done. The overview of the new package of regulatory guidance documents FSTEC Russia is done. The certification issues through the Common Criteria for developments and testing laboratories is shown. The ways to overcome the difficulties associated with the implementation of Common Criteria are suggested. The prospects for implementation of the Common Criteria in Russian and in the world are marked.

Keywords: information security, certification, information security tool, common criteria, common evaluation methodology, criteria for information technology security evaluation, ISO 15408, ISO 18045, conformity assessment

Reference

1. Markov A.S. and etc. Statistika vnedreniya «Obshchikh kriteriyev» v zarubezhnykh stranakh, Information Security (in Russian), 2006, N 1/2, pp. 12-15.
2. Alexey Markov, Alexander Barabanov, Valentin Tsirlov. Russian IT Security Certification Scheme: Steps Toward Common Criteria Approach, 15th International Common Criteria Conference (ICCC-2014), New Delhi, India, 2014, pp.1-11.
3. Mark S. Merkow, Jim Breithaupt, Computer Security Assurance Using the Common Criteria. Thomson Delmar Learing, 2005, 278 p.
4. Wesley Hisao Higaki, Successful Common Criteria Evaluations: A Practical Guide for Vendors, CreateSpace, 2010, 282 p.
5. Bagayev D.A. Trebovaniya k informatsionnoy bezopasnosti avtomatizirovannykh sistem na osnove primeneniya obshchikh kriteriyev, Voprosy zashchity informatsii, 2009. N 2, pp. 6-8.
6. Barabanov A.V., Markov A.S., Rautkin Yu.V. Otsenka sootvetstviya sredstv zashchity informatsii trebovaniyam vysshikh otsenochnykh urovney doveriya, Trudy Nauchno-issledovatelskogo instituta radio, 2012, N 3, pp. 67-73.
7. Drovnikova I.G., Nikitin A.A. Trebovaniya k bezopasnosti informatsionnykh tekhnologiy avtomatizirovannykh sistem na osnove primeneniya obshchikh kriteriyev, Tekhnologii tekhnosfernoy bezopasnosti, 2013, N 3 (49), pp. 24.
8. Sidak A.A. Kompozitsionnyy podkhod k formirovaniyu trebovaniy k izdeliyam, realizuyushchim funktsii bezopasnosti v informatsionnykh sistemakh. semeystva profiley zashchity, Strategicheskaya stabilnost, 2013, N 3 (64), pp. 40-42.
9. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviya sredstv zashchity informatsii, By ed. A.S.Markov, Moscow, Radio i svyaz, 2012, 192 p.
10. Barabanov A.V., Markov A.S., Tsirlov V.L. Sertifikatsiya sistem obnaruzheniya vtorzheniy, Otkrytyye sistemy. SUBD (Open Systems Journal), 2012, N 3, pp. 31-33.
11. Barabanov A.V., Markov A.S., Tsirlov V.L. Sertifikatsiya sredstv antivirusnoy zashchity po novym trebovaniyam bezopasnosti informatsii, Vestnik MGTU im. N.E. Baumana. Ser. «Priborostroyeniye», 2012, Spetsvypusk N 5 "Informatika i sistemy upravleniya", pp.272-278.
12. Barabanov A.V., Grishin M.I., Markov A.S., Tsirlov V.L. Formirovaniye trebovaniy po bezopasnosti informatsii k DLP-sistemam, Voprosy radioelektroniki, 2013, N 2, pp. 67-76.