ТЕНДЕНЦИИ МЕЖДУНАРОДНОЙ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ЛИНИИ «ОБЩИХ КРИТЕРИЕВ»

[1]Барабанов А.В., [2]Марков А.С.

[1]ЗАО «НПО «Эшелон», 107023, г. Москва, ул. Электрозаводская, д. 24, e-mail:ab@cnpo.ru

[2]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана), 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1, e-mail: a.markov@bmstu.ru

В статье приведены результаты анализа текущих тенденций в ряде международной системе сертификаций средств защиты информации по линии «Общих критериев». Представлены результаты прогнозирования изменений, которые в ближайшее время могут быть внесены в основные документы, используемые для сертификации по методологии «Общие критерии». Полученные прогнозы могут быть интересны отечественным специалистам в области сертификации средств защиты информации и стандартизации в области защиты информации. Приведены рекомендации по улучшению отечественной системы сертификации.

Ключевые слова: оценка соответствия, Общие критерии, безопасность информации, сертификация средств защиты информации.

ON TRENDS IN INTERNATIONAL INFORMATION SECURITY COMMON CRITERIA CERTIFICATION SCHEME

[1]Barabanov A.V., [2]Markov A.S.

[1]NPO «Echelon», Elektrozavodskaya street, 24, 107023, Moscow Russian Federation, e-mail:ab@cnpo.ru

[2]Bauman Moscow State Technical University, 2-nd Baumanskaya, 5, 105005, Moscow, Russian Federation, e-mail: a.markov@bmstu.ru

The results of the study of current trends in the number of foreign systems certifications of information technology products for the requirements of information security held in accordance with the Common Criteria methodology are presented. The basic directions of improvement of development of Common Criteria methodology are obtained. These projections may be of interest to domestic experts in the field of information security certification and standardization. Recommendations on the improvement of the Russian Information Security Certification Scheme are presented.

Key words: conformity assessment, Common Criteria, information security, information security evaluation.

В настоящее время современное техническое регулирование отрасли информационной безопасности связывают, в первую очередь, с совершенствованием обязательной системы сертификации [1, 2]. Одним из перспективных направлений развития системы сертификации является внедрение методологии «Общих критериев», определенной стандартом ISO 15408 [3]. Указанная методология позволяет задать требования безопасности информации к различным типам изделий информационных технологий. К настоящему моменту времени ФСТЭК России разработаны и утверждены требования практически ко всем критичным с точки зрения обеспечения безопасности информации типам изделий: средства антивирусной защиты, системы обнаружения вторжений, средства контроля носителей информации, средства доверенной загрузки, операционные системы, межсетевые экраны [4]. Востребованность использования методологии «Общих критериев» связана с объективными причинами: необходимостью повышения результативности технического регулирования отечественной отрасли информационной безопасности и регламентацией национального варианта международной методологии «Общих критериев» в Российской Федерации [5]. Вместе с тем следует отметить, что методология «Общие критерии» была заложена в середине 90-ых годов двадцатого века, и принципиально ее содержание с того времени не поменялось. Понимая необходимость в кардинальном улучшении документов, рабочей технического комитета по стандартизации ISO/IEC JTC 1/SC 27 совместно с участниками соглашения о взаимном признании сертификатов соответствия (Common

Criteria Recognition Arrangement, CCRA) начата работа по кардинальному изменению стандартов и документов методологии «Общие критерии». Результатом такой работы должны стать уточненные документы серии «Общие критерии», а также соответствующие международные стандарты.

Цель проведенного исследования состояла в изучении последних тенденций международной сертификации по линии «Общих критериев» и выработке рекомендаций по улучшению отечественной системы сертификации.

В результате исследования открытой информации, публикуемой национальными системами сертификации и участниками соглашения CCRA, были выявлены следующие тенденции в международной сертификации средств защиты информации по линии «Общих критериев».

1. Выделение критичных типов средств защиты информации и программного обеспечения, разработка для них совместных профилей защиты.

2. Сертификация средств защиты информации исключительно на соответствие совместным профилям защиты и отказ от сертификации на соответствие требованиям заданий по безопасности, которые не декларирует соответствие ни одному из утверждённых профилей защиты. Совместные профили защиты разрабатываются совместно представителями различных стран, работающих в рамках международных технических комитетов. В такие международные технические комитеты, как правило, входят представители испытательных лабораторий, органов по сертификации, разработчиков и научных институтов, являющиеся специалистами в определенной области информационных технологий. Основные особенности совместных профилей защиты следующие:

- отказ от использования понятия «оценочный уровень доверия» и существенное понижение требований доверия до требований, аналогичных оценочному уровню доверия 1;
- запрет дополнения или усиления перечня требований из профиля защиты в задании по безопасности;

3. Для каждого разработанного совместного профиля защиты международные комитеты создают типовые методики испытаний, предназначенные для испытательных лабораторий и органов по сертификации.

4. Обеспечение детерминированности процедуры анализа уязвимостей, выполняемой в рамках сертификационных испытаний. В совместных профилях защиты анализ уязвимостей предлагается выполнять испытательным лабораториям исключительно на основе изучения открытых источников информации. Требования по выполнению анализа уязвимостей, например, на основе анализа исходного кода программного обеспечения с использованием методов статического или динамического анализа совместными профилями защиты не предъявляется.

5. Отдельные системы сертификации создают программы четкого отслеживания сроков сертификации (например, программа системы сертификации США «Сертификация за 90 дней»).

Следует отметить, что новый подход пока не используется повсеместно и не принят всем участниками соглашения CCRA. Так, французская, голландская и немецкая системы сертификации предполагают в дополнение к сертификации по требованиям совместных профилей защиты проводить сертификацию на соответствие повышенным требованиями доверия (так называемая «теневая сертификация»).

В Таблице 1 представлены результаты сравнения отечественной и перспективной зарубежной систем сертификации.

Таблица 1. Сравнение отечественной и перспективной зарубежной систем сертификации

Параметр	Система сертификации ФСТЭК России	Системы сертификации соглашения CCRA
Среднее время сертификации	5-6 мес.	3 мес.
Наличие требований к анализу исходных текстов	в наличии	отсутствует
Наличие типовых методик испытаний	отсутствуют	в наличии
Уровень требований доверия	сильный	слабый
Типизация средств защиты информации	от мер	от критичных процессов

По результатам анализа выполнено прогнозирование изменений в международной систем сертификации по линии «Общих критериев». Основные положения представлены далее по тексту [6].

1. Несмотря на инициативы ряда национальных систем сертификаций, связанные с отказом от использования оценочных уровней доверия, в новых версиях документов данная система должна остаться.

2. Прогнозируется, что номенклатура функциональных требований безопасности будет дополнена требованиями, характерными для современных средств защиты информации, например средств антивирусной защиты или средства защиты сред виртуализации.

3. Предполагается интеграция мер разработки безопасного программного обеспечения в номенклатуру требований доверия.

4. Действия экспертов испытательных лабораторий, описанные в «Общей методологии оценки», будут уточнены указаниями по выполнению анализа уязвимостей. Мы предполагаем, что будут определены минимальный перечень методов, используемых для идентификации перечня потенциальных уязвимостей, перечень открытых источников, который должен использоваться для формирования множества потенциальных уязвимостей.

5. Прогнозируются нововведения, ориентированные на поддержку конечных пользователей сертифицированных изделий: опубликование системами сертификации подробных технических отчетов об оценке и руководств по безопасной настройке сертифицированных продуктов.

В ходе исследования были сформулированы следующие предложения по модернизации отечественной системы сертификации.

1. Поддержка испытательных лабораторий. Уточнение действий испытательных лабораторий при проведении анализа уязвимостей и функционального тестирования с целью повышения эффективности и детерминированности этого процесса:

- разработка типовых методик функционального тестирования и тестирования проникновения;
- уточнение требований к действиям экспертов испытательных лабораторий по использованию специализированных инструментальных средств выявления уязвимостей, связанных с недостатками в реализации продуктов (недостатки исходного кода);
- определение минимального перечня открытых источников информации, анализ которых должен выполнить эксперт испытательной лаборатории при формировании множества потенциальных уязвимостей в сертифицируемом продукте;
- определение перечня инструментальных средств, используемых испытательными лабораториями при выполнении тестирования проникновения и функционального тестирования.

2. Поддержка разработчиков/заявителей на сертификацию.

- публикованные на официальном сайте систем сертификации подробных технических отчетов по результатам сертификационных испытаний с целью доведения информации о методах, используемых при проведении испытаний;
- совместное создание (разработчиком, испытательной лабораторией и органом по сертификации) и публикация руководства по установке и эксплуатации сертифицированного продукта, содержащего детальные инструкции по работе с сертифицированными функциями по безопасности.
- разработка методических указаний и шаблонов оформления необходимых свидетельств разработчика.

3. Расширение текущей номенклатуры требований доверия требованиями, выполнение которых обеспечит создание разработчиком программного обеспечения с минимальным количеством эксплуатируемых уязвимостей и формирование среды, обеспечивающей оперативное устранение выявленных в ходе эксплуатации ошибок и уязвимостей в сертифицированных продуктах ИТ [7-10].

Список литературы

1. Головин С.А. Основные принципы, заложенные в стратегию развития стандартизации информационных технологий // ИТ-Стандарт. 2014. Т. 1. № 1-1 (1). С. 1-6.

2. Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. - М.: Изд. "Вооружение. Политика. Конверсия", 1996. 280 с.

3. 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.

4. Barabanov A., Markov A. Modern trends in the regulatory framework of the information security compliance assessment in Russia based on common criteria. ACM International Conference Proceeding Series 8. "Proceedings of the 8th International Conference on Security of Information and Networks, SIN 2015" 2015, pp. 30-33.

5. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации // Оборонный комплекс - научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.

6. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30-33.

7. Барабанов А.В. Задание требований к процессу безопасной разработки программного обеспечения // ИТ-Стандарт. 2015. Т. 1. № 3-1 (4). С. 1-6.

8. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5 (13). С. 2-10.

9. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological framework for analysis and synthesis of a set of secure software development controls, Journal of Theoretical and Applied Information Technology. 2016. Vol. 88. N 1, pp. 77-88.

10. Min-Gyu Lee, Hyo-jung Sohn, Baek-MinSeong and Jong-Bae Kim A Study on Secure SDLC Specialized in Common Criteria. Advanced Science and Technology Letters Vol.93 (Security, Reliability and Safety 2015), pp.19-23.

References

1. Golovin S.A. Osnovnye printsipy zalozhennye v strategiyu razvitiya standartizatsii informatsionnykh tekhnologiy, IT-Standart. 2014. V. 1, No 1-1 (1), pp. 1-6.

2. Kostogryzov A. I., Lipaev V. V. Sertifikatsiya funktsionirovaniya avtomatizirovannykh informatsionnykh sistem. -M.: Izd. "Vooruzhenie. Politika. Konversiya", 1996, 280 p.

3. Barabanov A.V., Markov A.S., Tsirlov V.L. Otsenka sootvetstviya sredstv zashchity informatsii "Obshchim Kriteriyam", Informatsionnye tekhnologii. 2015. V. 21, No 4, pp. 264-270.

4. Barabanov A., Markov A. Modern Trends in The Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 30-33. DOI = DOI: 10.1145/2799979.2799980.

5. Markov A.S., Sheremet I.A. Teoreticheskie aspekty sertifikatsii sredstv zashchity informatsii, Oboronnyy kompleks - nauchno-tekhnicheskomu progressu Rossii. 2015, No 4 (128), pp. 7-15.

6. Barabanov A.V., Markov A.S., Tsirlov V.L. Mezhdunarodnaya sertifikatsiya v oblasti informatsionnoy bezopasnosti, Standarty i kachestvo. 2016, No 7, pp. 30-33.

7. Barabanov A.V. Zadanie trebovaniy k protsessu bezopasnoy razrabotki programmnogo obespecheniya, IT-Standart. 2015. V. 1, No 3-1 (4), pp. 1-6.

8. Barabanov A.V., Markov A.S., Tsirlov V.L. 28 magicheskikh mer razrabotki bezopasnogo programmnogo obespecheniya, Voprosy kiberbezopasnosti. 2015, No 5 (13), pp. 2-10.

9. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological framework for analysis and synthesis of a set of secure software development controls, Journal of Theoretical and Applied Information Technology. 2016. Vol. 88. No 1, pp. 77-88.

10. Min-Gyu Lee, Hyo-jung Sohn, Baek-MinSeong and Jong-Bae Kim A Study on Secure SDLC Specialized in Common Criteria. Advanced Science and Technology Letters Vol.93 (Security, Reliability and Safety 2015), pp.19-23.