ФОРМАЛИЗАЦИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ К СРЕДСТВАМ АНАЛИЗА ЗАЩИЩЕННОСТИ

***Веряев Александр Сергеевич**, заместитель директора департамента программных разработок по НИОКР НПО «Эшелон», г.Москва*
E-mail: a.veryev@cnpo.ru
***Фадин Андрей Анатольевич**, CISSP, Главный конструктор ЗАО «НПО «Эшелон», г. Москва*
E-mail: a.fadin@cnpo.ru

В статье приведено краткое описание решения задачи разработки и формализации требований к средствам анализа защищенности (САЗ). Произведена типизация САЗ, выделены основные угрозы, нейтрализацию которых должны обеспечивать данные средства. На основе методологии ГОСТ ИСО/МЭК 15408 разработаны как функциональные требования безопасности, так и требования доверия к САЗ.

Ключевые слова: средства анализа защищенности, уязвимость, статический и динамический анализ исходных текстов программного обеспечения, ГОСТ ИСО/МЭК 15408, Общие критерии.

SECURITY REQUIREMENTS FORMALIZATION FOR SECURITY ASSESSMENT TOOLS

***Andrey Fadin**, CISSP, Chief Structural Engineer, (Moscow, NPO Echelon)*
E-mail: a.fadin@cnpo.ru
***Alexander Veryaev**, Deputy Head of Development Department (R&D), (Moscow, NPO Echelon)*
E-mail: a.veryev@cnpo.ru

Abstract. The paper presents the short description of the solution to the issue of creation and formalization requirements for security assessment tools (SAT). The SAT typing has been performed, major threats, counteraction to which SAT must carry out, have been highlighted. Security Functional and Assurance Requirements have been formulated on the basis of the ISO/IEC 15408 approach.

***Keywords**: security assessment tools, vulnerability, software source code static and dynamic analysis, ISO/IEC 15408, Common Criteria.*

Введение

Периодический, проводимый на постоянной основе контроль и анализ защищенности информационных систем (ИС) необходим для предупреждения возможных злоумышленных действий, направленных на уничтожение или повреждение информации или нарушение нормального функционирования средств обработки и передачи информации.

Для реализации контроля и анализа защищенности существует большое количество видов программных и программно-аппаратных комплексов (средств анализа защищенности - САЗ), работающих на различных принципах: от анализа свойств и параметров конфигурации программного обеспечения до непосредственной имитации действий злоумышленника.

Для эффективного анализа и синтеза САЗ необходимо развивать нормативно-правовую базу в области оценки качества работы таких комплексов. Для этого в свою очередь необходимо разработать четкие требования, на соответствие которым САЗ будут проверяться.

Подход к решению задачи формирования требований

Целью настоящей статьи является попытка сформировать набор формализованных требований безопасности к САЗ, опираясь на подход, используемый ФСТЭК России при разработке современных требований к средствам защиты информации (СрЗИ) [7].

С учетом последних тенденций в системе сертификации программного обеспечения (ПО) в России [1, 3, 6] разработку требований к САЗ целесообразно проводить с учетом методологии, предлагаемой ГОСТ ИСО/МЭК 15408 и широко известной как «Общие критерии» [4-13].

Данная методология позволяет сформулировать требования к САЗ, с учетом их типов и классов защиты. Классы защиты САЗ формируются на основе применения САЗ в ИС (таблица 1) [12].

Все существующие САЗ по функциональным возможностям можно условно поделить на 2 типа:

– сканеры безопасности;

– специализированные комплексы анализа защищенности информации.

Сканеры безопасности выполняют функции выявления уязвимостей, проверки целостности и доступности пользовательской информации, контроля соблюдения политик безопасности, контроля остаточной информации и т. п., т. е. выполняют широкий спектр анализов безопасности ИС [8].

Специализированные комплексы анализа защищенности информации в свою очередь могут представлять собой средства проведения статического или динамического анализа как при наличии исходных кодов, так и при их отсутствии.

Используемый подход позволит сформулировать серию профилей защиты, на основании которых разработчики (изготовители) САЗ могут подготовить необходимое задание по безопасности.

Формирование требований к средствам анализа защищенности

В результате анализа применимости объекта оценки (ОО, в данном случае - САЗ) можно выделить следующие основные угрозы, нейтрализацию которых должны обеспечить данные средства [2]:

– преднамеренный несанкционированный доступ или специальные воздействия на информацию с использованием известных уязвимостей программного обеспечения как со стороны внутреннего, так и со стороны внешнего нарушителя;

– преднамеренный несанкционированный доступ или специальные воздействия на информацию с использованием неизвестных уязвимостей программного обеспечения как со стороны внутреннего, так и со стороны внешнего нарушителя.

Для нейтрализации вышеперечисленных угроз, а также с целью устойчивого безопасного функционирования ОО (удовлетворение политикам безопасности) предъявляются требования безопасности. В ИСО 15408 (в части 2 и 3) фактически представлены каталоги требований безопасности следующих типов:

– функциональные требования безопасности (ФТБ), предъявляемые к функциям безопасности ОО;

– требования доверия к безопасности, которые предъявляются к технологии и процессу разработки, эксплуатации и оценки ОО и призваны гарантировать адекватность реализации механизмов безопасности.

Предлагается в качестве функциональных требований безопасности использовать следующий состав ФТБ к САЗ (таблицы 2-4).

Таблица 1. *Классы защиты САЗ*

1-3 классы	Информационные системы, в которых обрабатываются сведения, составляющие государственную тайну
4 класс	Государственные информационные системы, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну. Информационные системы персональных данных при необходимости 1го уровня защищенности персональных данных (1 класса).
5 класс	Информационные системы персональных данных при необходимости обеспечения 2-го уровня защищенности персональных данных (2 класса)
6 класс	Информационные системы персональных данных при необходимости обеспечения 3-го и 4-го уровней защищенности персональных данных (3 и 4 классов)

Таблица 2. *Стандартные ФТБ к САЗ*

Условное обозначение семейства	Наименование функциональной возможности
FAU_ARP	Автоматическая реакция аудита безопасности
FAU_GEN	Генерация данных аудита безопасности
FAU_SAR	Просмотр аудита безопасности
FAU_STG	Хранение данных аудита безопасности
FIA_UAU	Аутентификация пользователя
FIA_UID	Идентификация пользователя
FMT_MOF	Управление отдельными функциями ФБО
FMT_MSA	Управление атрибутами безопасности
FMT_MTD	Управление данными ФБО
FMT_SMR	Роли управления безопасностью

Таблица 3. *Дополнительные ФТБ для сканеров безопасности*

Условное обозначение семейства	Наименование функциональной возможности
FSS_SCN_EXT	Сканирование портов
FSS_IDE_EXT	Идентификация операционных систем и активных сетевых сервисов
FSS_VUL_EXT	Анализ уязвимостей
FSS_DAT_EXT	Поиск остаточной информации
FSS_CSC_EXT	Контроль целостности информационных объектов
FSS_CLS_EXT	Классификация уязвимостей
FSS_REC_EXT	Генерация рекомендаций по устранению уязвимостей
FSS_REP_EXT	Генерация отчетов
FSS_UPD_EXT	Обновление баз уязвимостей и компонентов САЗ

Таблица 4. *Дополнительные ФТБ для специализированных комплексов анализа защищенности информации*

Условное обозначение семейства	Наименование функциональной возможности
FCA_VUL_EXT	Статический анализ исходных текстов
FCA_REP_EXT	Генерация отчетов
FCA_UPD_EXT	Обновление баз программных ошибок и компонентов САЗ
FCA_DAS_EXT	Дизассемблирование
FCA_DYN_EXT	Динамический анализ
FCA_CLS_EXT	Классификация уязвимостей
FCA_REC_EXT	Генерация рекомендаций по устранению уязвимостей

Кроме стандартных ФТБ для САЗ (таблица 2) предлагается использовать ряд дополнительных ФТБ как для сканеров безопасности (таблица 3), так и для специализированных комплексов анализа защищенности информации (таблица 4).

Семейства FSS_SCN_EXT и FSS_IDE_EXT содержат требования к сканерам безопасности по возможности обнаружения открытых портов и идентификации заданных операционных систем с сетевыми сервисами, соответствующими обнаруженным открытым портам. Семейство FSS_VUL_EXT содержит требования по возможности обнару-

***Таблица 5**. ребования доверия к СА3 для ОУД 1-3*

Класс ИСПДн	ОУД	Дополнительные компоненты доверия к безопасности
ИСПДн 1го уровня защищенности	3	ADV_IMP.2 «Полное отображение представления реализации ФБО» ADV_TDS.3 «Базовый модульный проект» ADV_FSP.4 «Полная функциональная спецификация» ALC_TAT.1 «Полностью определённые инструментальные средства разработки» ALC_CMC.4 «Поддержка генерации, процедуры приёмки и автоматизация» ALC_FLR.1 «Базовое устранение недостатков» AVA_VAN.4 «Методический анализ уязвимостей» AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность СА3»
ИСПДн 2го уровня защищенности	2	ALC_FLR.1 «Базовое устранение недостатков» AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность СА3»
ИСПДн 3го уровня защищенности	1	AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность СА3»

жения уязвимостей различных типов, например, переполнение буфера, SQL-инъекция, межсайтовое выполнение скриптов. Семейства FSS_CLS_EXT FSS_REC_EXT идентифицируют требования по возможности осуществления классификации обнаруженных уязвимостей и выдаче рекомендаций по их устранению соответственно. Семейство FSS_DAT_EXT содержит требования к идентификации информации на запоминающем устройстве, оставшейся после формального удаления данных.

Для специализированных комплексов анализа защищенности информации характерными являются требования по возможности проведения статического анализа (FCA_VUL_EXT) и динамического анализа исходных текстов (FCA_DYN_EXT). Кроме того целесообразно в случае отсутствия исходных текстов СА3 требовать наличие возможности провести анализ программы в отсутствии исходных текстов [4]. Семейство FCA_DAS_EXT идентифицирует требование по преобразованию двоичного кода в текст программы на языке ассемблера, что дает возможность его дальнейшего анализа. Семейства FCA_CLS_EXT и FCA_REC_EXT, как и в случае со сканерами безопасности, предъявляют требования по возможности осуществления классификации обнаруженных уязвимостей и выдаче рекомендаций по их устранению.

Важным семейством требований как в том, так и в другом случае является семейство, отвечающие за обновление базы данных уязвимостей FSS_UPD_EXT для сканеров безопасности и базы данных программных ошибок FCA_UPD_EXT для специализированных комплексов анализа защищенности информации.

Как следует из таблицы 1, СА3, используемые для защиты информации конфиденциального характера, будут соответствовать ОУД1-ОУД3. Пример предлагаемых требований доверия к классам защиты СА3, предназначенных для защиты персональных данных, представлен в таблице 5.

Следует отметить добавление для всех ОУД дополнительного требования доверия AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность СА3», которое позволяет удостовериться в неизменности функций безопасности СА3 после внесения изменений в ОО путем обновления базы данных уязвимостей/программных ошибок, а также компонентов СА3 [12].

Выводы

В статье приведены результаты разработки функциональных требований безопасности и требований доверия к СА3. Формирование требований осуществлялась на базисе метастандарта “Общие критерии” с учетом назначения и функциональных характеристик СА3.

Выделены два типа СА3: сканеры безопасности и специализированные комплексы анализа защищенности информации. Первые выполняют преимущественно функции обнаружения известных уязвимостей, а использование вторых направлено на поиск ошибок в программном коде. В соответствии с их назначением основными требованиями к ним являются возможность сканирования ПО на наличие уязвимостей и проведение статического, а также динамического анализа исходных текстов.

Сформированы и другие дополнительные семейства ФТБ, относящиеся к поиску остаточной информации, контролю целостности, классификации уязвимостей, генерации отчетов, в том числе содержащих рекомендации по устранению выявленных уязвимостей и к другим важным с точки зрения безопасности функциональным возможностям СА3.

Литература:

1. Барабанов А., Марков А., Цирлов В. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31-33.
2. Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых в вредоносных компьютерных программ // Вопросы кибербезопасности. 2014. № 4 (7). С. 41-48.
3. Барабанов А.В., Гришин М.И., Марков А.С., Цирлов В.Л. Формирование требований по безопасности информации к DLP-системам // Вопросы радиоэлектроники. 2013. Т. 3. № 2. С. 67-76.
4. 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.
5. 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.
6. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации. // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2012. № S5. С. 272.
7. 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.
8. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. № 3 (51). С. 56-61.
9. Шалаевский О.Н., Малыхина Г.Ф. Онтологическая модель безопасности измерительных информационных технологий на базе Общих критериев // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010, 5 (108), 186-192.
10. Юдичев Р.М., Горюнов М.Н. Оценка и ранжирование функциональных возможностей средств защиты среды виртуализации // Автоматизация и управление в технических системах. 2015. № 1 (13). С. 92-100.
11. Higaki W. H. Successful Common Criteria Evaluations: A Practical Guide for Vendors. CreateSpace. 2010. 282 p.
12. Markov A.S., Fadin A.A., Veryaev A.S. Formalization of Requirements for Security Analysis Tools of Information Systems. Proceedings of the 3rd International Conference «Information Technologies for Intelligent Decision Making Support» (May 18-21), Ufa, Russia, 2015, Vol. 1, pp. 116-118.
13. Merkow M. S., Breithaupt J. Computer Security Assurance Using the Common Criteria. Thomson Delmar Learning, 2005. 278 p.

References:

1. Barabanov A., Markov A., Tsirlov V. Sertifikatsiya sistem obnaruzheniya vtorzheniy, Otkrytye sistemy. SUBD, 2012, No 3, pp. 31-33.
2. Barabanov A.V., Grishin M.I., Kubarev A.V. Modelirovanie ugroz bezopasnosti informatsii, svyazannykh s funktsionirovaniem skrytykh v vredonosnykh komp'yuternykh programm, Voprosy kiberbezopasnosti, 2014, No 4 (7), pp. 41-48.
3. Barabanov A.V., Grishin M.I., Markov A.S., Tsirlov V.L. Formirovanie trebovaniy po bezopasnosti informatsii k DLP-sistemam, Voprosy radioelektroniki, 2013, Vol. 3, No 2, pp. 67-76.
4. Barabanov A.V., Markov A.S., Rautkin Yu.V. Otsenka sootvetstviya sredstv zashchity informatsii trebovaniyam vysshikh otsenochnykh urovney doveriya, Trudy Nauchno-issledovatel'skogo instituta radio, 2012, No 3, pp. 67-73.
5. Barabanov A.V., Markov A.S., Tsirlov V.L. Otsenka sootvetstviya sredstv zashchity informatsii "Obshchim kriteriyam", Informatsionnye tekhnologii, 2015, Vol. 21, No 4, pp. 264-270.
6. Barabanov A.V., Markov A.S., Tsirlov V.L. Sertifikatsiya sredstv antivirusnoy zashchity po novym trebovaniyam bezopasnosti informatsii., Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya: Priborostroenie, 2012, No S5, pp. 272.
7. Markov A, S., Tsirlov V. L., Barabanov A. V. Metody otsenki nesootvetstviya sredstv zashchity informatsii / Ed. A, S.Markov. M.: Radio i svyaz', 2012. 192 p.
8. Markov A.S., Fadin A.A. Sistematika uyazvimostey i defektov bezopasnosti programmnykh resursov, Zashchita informatsii. Insayd, 2013, No 3 (51), pp. 56-61.
9. Shalaevskiy O.N., Malykhina G.F. Ontologicheskaya model' bezopasnosti izmeritel'nykh informatsionnykh tekhnologiy na baze obshchikh kriteriev, Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikatsii. Upravlenie, 2010, 5 (108), pp. 186-192.
10. Yudichev R.M., Goryunov M.N. Otsenka i ranzhirovanie funktsional'nykh vozmozhnostey sredstv zashchity sredy virtualizatsii, Avtomatizatsiya i upravlenie v tekhnicheskikh sistemakh, 2015, No 1 (13), pp. 92-100.
11. Higaki W. H. Successful Common Criteria Evaluations: A Practical Guide for Vendors. CreateSpace, 2010. 282 p.
12. Markov A.S., Fadin A.A., Veryaev A.S. Formalization of Requirements for Security Analysis Tools of Information Systems. Proceedings of the 3rd International Conference «Information Technologies for Intelligent Decision Making Support» (May 18-21), Ufa, Russia, 2015, Vol. 1, pp. 116-118.
13. Merkow M, S., Breithaupt J. Computer Security Assurance Using the Common Criteria. Thomson Delmar Learning, 2005. 278 p.