УДК 681.326

А.В. Барабанов, А.С. Марков, В.Л. Цирлов

СЕРТИФИКАЦИЯ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ ПО НОВЫМ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Приведены новые требования Федеральной службы по техническому и экспортному контролю (ФСТЭК России) к сертификации средств антивирусной защиты в соответствии с методологией стандарта «Общие критерии», обзор особенностей проведения сертификационных испытаний для основных классов средств антивирусной защиты. Рассмотрены практические рекомендации по реализации соответствующих поддерживающих процедур.

E-mail: mail@npo-echelon.ru

***Ключевые слова*:** *средства антивирусной защиты (САВЗ), сертификация САВЗ, общие критерии*

В настоящее время Федеральной службой по техническому и экспортному контролю (ФСТЭК России) подготовлен пакет новых нормативных документов, устанавливающих требования безопасности информации к средствам антивирусной защиты (САВЗ) [1]. Эти требования позволяют устранить недетерминированность процесса сертификации САВЗ, поскольку до настоящего момента требования к составу функциональных возможностей САВЗ нигде не были формализованы, и под определение сертифицированного продукта одного и того же типа могли попасть решения принципиально различного уровня. Однако введение новых документов качественно меняет содержание сертификационных испытаний по требованиям безопасности информации [2]. Анализ особенностей сертификации САВЗ в соответствии с новой нормативной базой представляет основную цель работы.

Под САВЗ понимаются программные средства, используемые в целях обеспечения защиты информации и реализующие функции обнаружения компьютерных программ или иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, либо нейтрализации средств защиты информации (вредоносные компьютерные программы, компьютерные вирусы), а также реагирования на обнаружение этих программ и информации. Как правило, обнаружение компьютерных вирусов выполняется с помощью сигнатурного метода (используется при обнаружениях известных компьютерных вирусов) и эвристического (используется при обнаружениях неизвестных компьютерных вирусов). Выделяют четыре типа САВЗ (рис. 1):

1. Тип А, предназначены для централизованного администрирования САВЗ, установленных на компонентах информационных систем (серверах, автоматизированных рабочих местах (АРМ)).

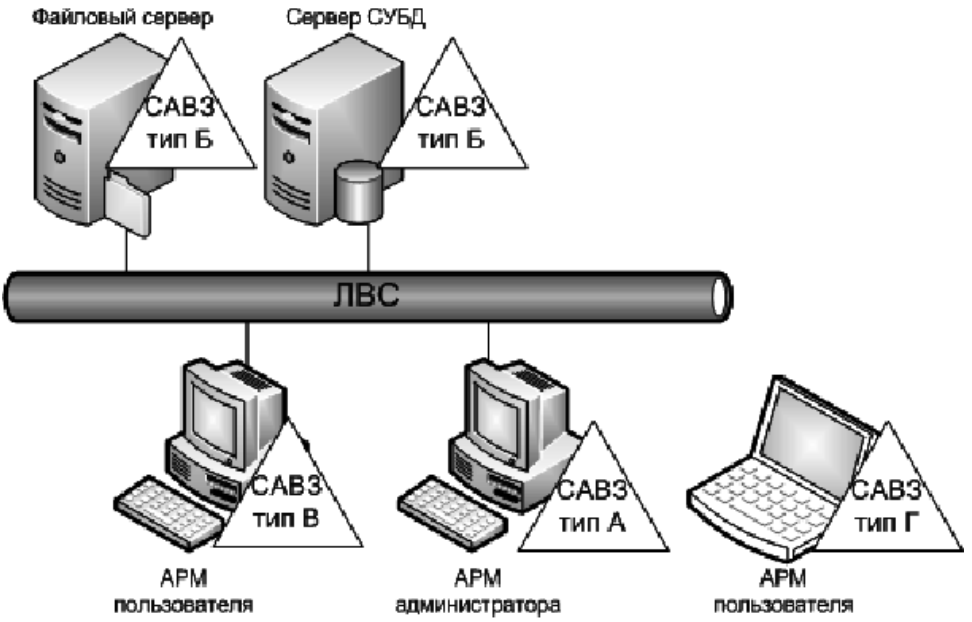

Рис. 1. Схема построения антивирусной защиты в информационной системе с применением САВЗ разных типов (СУБД — система управления базой данных; ЛВС — локальная вычислительная сеть)

2. Тип Б, применяют на серверах информационных систем.

3. Тип В, используют на АРМ информационных систем.

4. Тип Г, применяют на автономных АРМ.

Для каждого из типов САВЗ предусмотрены шесть классов защиты, требования ужесточаются от шестого класса к первому. Каждому классу защиты соответствует определенная категория информационных систем:

— САВЗ 6 класса защиты для информационных систем персональных данных 3 и 4 классов;

— САВЗ 5 класса защиты для информационных систем персональных данных 2 класса;

— САВЗ 4 класса защиты для информационных систем персональных данных 1 класса, информационных систем общего пользования 2 класса, а также для государственных информационных систем, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

— САВЗ 3, 2 и 1 классов защиты для информационных систем, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Наиболее интересной особенностью новых требований к САВЗ является то, что они разработаны в соответствии с методологией стандарта «Общие критерии» [3, 4]. Общая схема сертификации изделия по требованиям безопасности информации в соответствии с положениями этого стандарта приведена на рис. 2.

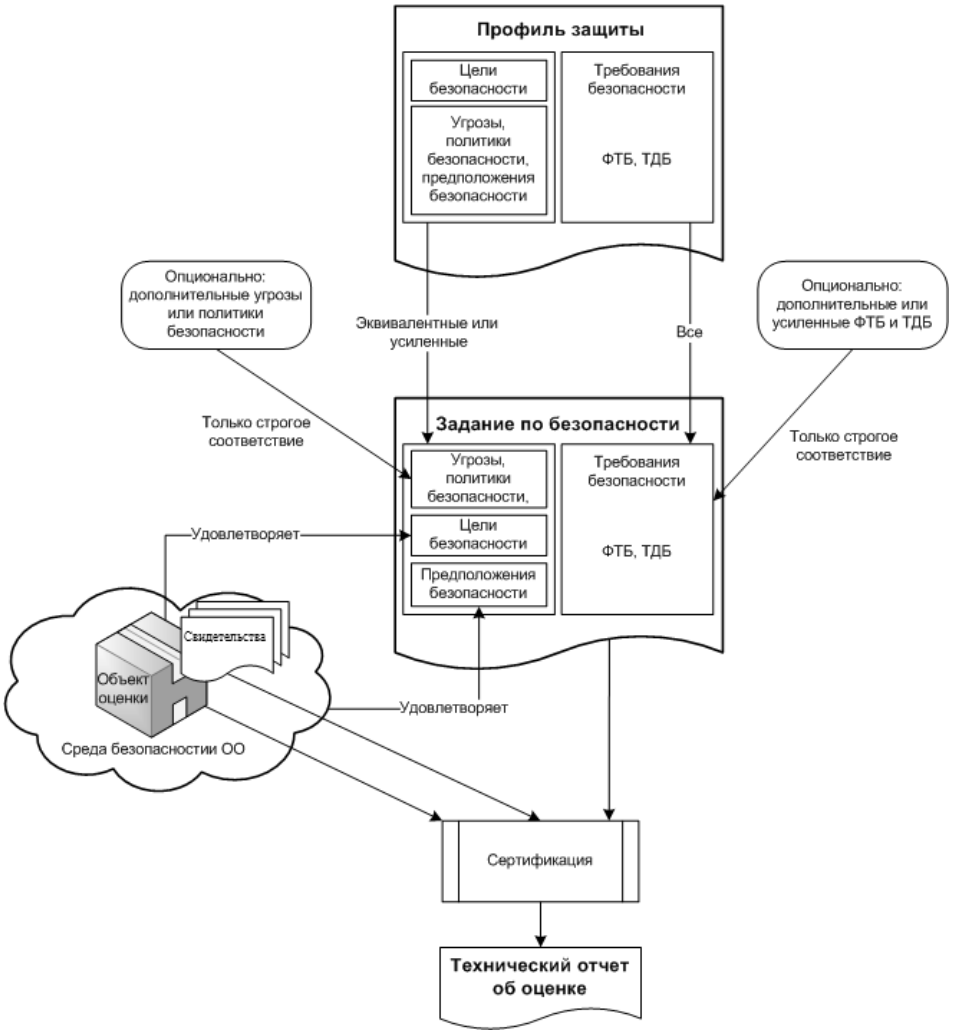

Рис. 2. Общая схема сертификации изделия по требованиям безопасности информации

Испытания ***объекта оценки*** (ОО) — в рассматриваемом случае САВЗ — проводятся на соответствие ***заданию по безопасности***, которое представляет собой структурированный и строго формализованный документ, включающий подробное описание ***функциональных требований безопасности*** (ФТБ) к объекту оценки и среде его функционирования, а также обеспечивающих мер — ***требований доверия к безопасности*** (ТДБ). При разработке задания по безопасности можно применять типовые наборы требований — ***профили защиты***. Испытательная лаборатория и орган по сертификации в свою очередь при проведении оценки используют различного рода ***свидетельства оценки*** — конструкторскую и проектную документацию на изделие, руководства пользователя и администратора, корпора-

тивные стандарты, руководства и процедуры, требования к которым также сформулированы в задании по безопасности.

Новые требования к САВЗ в явном виде определяет все функциональные требования и требования доверия, которые должны войти в соответствующие профили защиты и далее в задания по безопасности на конкретные изделия.

Состав функциональных требований безопасности к САВЗ достаточно традиционен. Кроме непосредственно возможностей по выявлению и удалению компьютерных вирусов, а также обновлению базы данных признаков компьютерных вирусов предъявляются требования к системе управления параметрами САВЗ (таблица).

Функциональные требования безопасности для САВЗ типа В класса защиты 4

Компонент	Название компонента
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MTD.1	Управление данными функций безопасности системы обнаружения вторжений
FMT_SMR.1	Роли безопасности
FAV_DET_EXT.1	Базовое обнаружение вредоносных компьютерных программ (вирусов)
FAV_MTH_EXT.1	Методы анализа
FAV_MTH_EXT.2	Выполнение проверок
FAV_ACT_EXT.1	Удаление вредоносных компьютерных программ (вирусов)
FAV_UPD_EXT.1	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

Из таблицы ясно, что часть ФТБ сформулирована в явном виде (имеют постфикс EXT). Остальные требования разработаны на основе стандартных ФТБ, приведенных во второй части стандарта ГОСТ Р ИСО/МЭК 15408—2008 [3]. Важной особенностью новых требований является то, что кроме требований к обнаружению компьютерных вирусов предъявляются требования к методам такого обнаружения (сигнатурный, эвристический).

Новый документ устанавливает требования доверия, сформулированные на основе предопределенных в третьей части стандарта ГОСТ Р ИСО/МЭК 15408–2008 оценочных уровней доверия (ОУД): САВЗ 6 класса защиты должны соответствовать усиленному ОУД 1; САВЗ 5 класса защиты — усиленному ОУД 2; САВЗ 4 класса защиты — усиленному ОУД 3; к САВЗ 3, 2 и 1 классов защиты предъявляются требования более высоких ОУД [3]. Анализ требований доверия к новым документам показывает, что заявитель должен разработать и реализовать значительное количество технологических процедур и документов, обеспечивающих безопасную (доверенную) разработку САВЗ. Например, для САВЗ 4 класса заявителем должны быть созданы и реализованы следующие основные процедуры и документы.

Уникальная маркировка — процедура уникальной маркировки каждого сертифицированного изделия.

Управление конфигурацией — система управления конфигурацией, отслеживающая представление реализации изделия, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора и документацию управления конфигурацией.

Поставка САВЗ в соответствии с разработанной процедурой — процедуры, необходимые для поддержки безопасности при распространении версий к местам использования.

Обновления базы данных признаков вредоносных компьютерных программ (вирусов) — фиксации момента получения нового типа вируса, выпуска обновления базы данных признаков за заданное время; уведомления об обновлении базы данных признаков; поставки обновления базы данных признаков пользователям; контроль целостности обновлений базы данных признаков; представления обновлений для проведения внешнего контроля; анализ влияния обновлений на безопасность САВЗ.

Задание по безопасности — документ, содержащий требования безопасности к конкретному САВЗ, а также специфицирующий функции безопасности и меры доверия, предлагаемые ОО для выполнения установленных требований.

План управления конфигурацией — описание автоматизированных инструментальных средств, используемых в системе управления конфигурацией.

Руководство по установке — описание последовательности действий, необходимых для безопасной установки, генерации и запуска САВЗ.

Функциональная спецификация — описание назначения и методов использования всех внешних интерфейсов САВЗ, неформальное описание функций безопасности САВЗ и их внешних интерфейсов.

Проект верхнего уровня — описание структуры функций безопасности САВЗ в терминах подсистем.

Руководство администратора — описание функций администрирования и интерфейсов, доступных администратору САВЗ.

Руководство пользователя — описание функций и интерфейсов, которые доступны пользователям САВЗ, не связанным с администрированием.

Документация по обновлению базы данных признаков вредоносных компьютерных программ (вирусов) — описания процедур фиксации момента появления нового типа компьютерного вируса, выпуска обновления базы данных признаков компьютерных вирусов за заданное время, уведомления об обновлении базы признаков, поставки обновления базы признаков, контроля целостности обновлений базы признаков, представления обновлений для проведения внешнего контроля; методика анализа влияния обновлений на безопасность САВЗ.

Важный момент — уточнение стандартных требований доверия для обеспечения преемственности требований к контролю отсутствия недекларированных возможностей, изложенных в руководящем документе ФСТЭК России. Например, при проведении сертификации САВЗ 4 класса защиты разработчик должен предоставить в испытательную лабораторию представление реализации функций безопасности САВЗ — исходные тексты программного обеспечения. В ходе испытаний лаборатория должна подтвердить, что исходные тексты являются необходимыми и достаточными для компиляции исполняемых файлов САВЗ (это заключение делается на основе результатов контроля полноты и отсутствия избыточности исходных текстов программного обеспечения САВЗ на уровне файлов).

Следует отметить, что в документе впервые в отечественной практике в явном виде допускается обновление базы данных признаков компьютерных вирусов (положение представлено в виде требований доверия, сформулированных в явном виде). При этом разработчик ежегодно предоставляет в испытательную лабораторию, проводившую испытания САВЗ, подробный отчет обо всех внесенных изменениях и об их возможном влиянии на безопасность системы. Такой подход позволяет значительно ускорить процедуру обновления по сравнению с традиционным подходом, требовавшим в некоторых случаях проведения инспекционного контроля после внесения каждого изменения в изделие.

Отдельного рассмотрения заслуживает вопрос трудоемкости независимого тестирования при сертификационных испытаниях по новым требованиям. Анализ, проведенный экспертами, позволяет сделать вывод о том, что плановая трудоемкость самих проводимых тестов принципиально не изменится по сравнению с традиционным подходом.

Заключение. Можно ожидать, что переход на сертификационные испытания в соответствии с изложенными в статье требованиями будет способствовать созданию рынка консалтинговых услуг в части подготовки изделий к проведению проверок [5].

СПИСОК ЛИТЕРАТУРЫ

1. Информационное сообщение о работах в области оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (ФСТЭК России, 2012). URL: http://www.fstec.ru/_razd/infsoob.pdf . Дата обращения: 1.07.2012.
2. Марков А.С., Цирлов В.Л. Сертификация программ: мифы и реальность // Открытые системы. СУБД. 2011. № 6. — С. 26–29.
3. ГОСТ Р ИСО/МЭК 15408—2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1–3. — М.: Стандартинформ, 2009. — 324 с.
4. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. — С. 31—33.
5. Матвеев В.А., Медведев Н.В., Троицкий И.И., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2011 г. // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2011. Спецвыпуск «Технические средства и системы защиты информации». — М.: Изд-во МГТУ им. Н.Э. Баумана. — С. 3—6.

Статья поступила в редакцию 4.07.2012