электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 681.3.06

Разработка методики испытаний средств антивирусной защиты в соответствии с новыми требова ниями ФСТЭК России

***Ларионцева Е.А.**, студент*
кафедра «Информационная безопасность»,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана

***Стельмашук Н.Н.**, студент*
кафедра «Информационная безопасность»,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана

Научный руководитель: Марков А. С., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

Введение

Для обеспечения информационной безопасностикак крупных предприятий, так и отдельных пользователей, а также для предотвращения возможных угроз интересам субъектов информационных отношений необходимо использовать определенные средства защиты. Одним из распространенных видов угроз являются компьютерные вирусы. Для успешной борьбы с ними и другими вредоносными программными объектами необходимо четко представлять себе особенности связанных с ними угроз.

Вирусом называется специально созданный программный код, способный самостоятельно распространяться в компьютерной среде. Можно выделить следующие несколько типов вирусов:файловые вирусы, загрузочные вирусы, стелс-вирусы, шифрующиеся вирусы, полиморфные вирусы**Ошибка! Закладка не определена.**, почтовые вирусы и другие.

Каждый из типов вирусов имеет свои особенности и характерные черты, знание которых позволяет минимизировать вероятность проникновения компьютерного вируса на рабочий компьютер или корпоративную интрасеть иобеспечить максимальную защиту персональных данных. Поэтому с целью обнаружения, удаления вирусов, а также предотвращения возможного заражения файлов на персональном компьютере (далее ПК) используются средства антивирусной защиты (далее САВЗ). Под САВЗ понимаются программные средства защиты информации от шпионских и вредоносных программ, позволяющие предотвратить потенциальные последствия от разрушающих воздействий на информацию, несанкционированного доступа к персональным данным, хищения, модификации или незаконного распространения конфиденциальной информации.

При проведении сертификационных испытаний САВЗ важным аспектом является четкая формулировка основного функционала сертифицируемого средства и определение типа сертификации. В данной работе будет рассмотрен пример составления методики проведения испытаний на основании профиля защиты средств антивирусной защиты типа Г для шестого класса защиты ИТ.САВЗ.Г6.ПЗ.

20 марта 2012 г. приказом ФСТЭК России N 28 утверждены Требования к средствам антивирусной защиты, которые вступили в действие с 1 августа 2012 г. До недавнего времени анализ и синтез САВЗ был ограничен отсутствием нормативной и методической базы, однако данный недостаток был устранен с выходом новых документов ФСТЭК России, включающих профили защиты по САВЗ [1,2]. Разработка новой методики испытаний САВЗ согласно начальным требованиям к САВЗ и представляет основное содержание работы. При этом предложенная методика строится как математическая модель, что является развитием методического аппарата, предложенного в работах некоторых авторов, ранее затрагивавших данную тематику, а именно, [3,4].

2. Математическое описание методики проведения испытаний САВЗ.

Первым этапом построения *методики проведения испытаний САВЗ* является создание математической модели программного средства, в данном случае – средства антивирусной защиты. Введем условные обозначения. В профиле защиты ИТ.САВЗ.Г6.ПЗ предъявлено 10 функциональных требований и 8 требований доверия для САВЗ, сертифицируемых в соответствии с данным документом. Поэтому обозначим $Fn=\{fn_1,fn_2,\ldots,fn_{10}\}$ – множество данных функциональных требований к объекту оценки $GЭ$ (далее ОО), множество $D=\{d_1, d_2, \ldots,d_9\}$–множество требований доверия. Пусть $T=\{t_1, t_2, \ldots, t_i, \ldots\}$ – множество тестов (испытаний), проводимых в процессе сертификации.

Зададим отображение $G: GЭ\times D \rightarrow T$. Данный закон ставит в соответствие требованиям доверия множество тестовых испытаний, проводимых над объектом $GЭ$. Назовем это отображение *схемой составления тестовых испытаний*.Одно из требований доверия, а именно «Тестирование», включает в себя множество функциональных требований, основанных на функциональных компонентах.

Далее необходимо определить набор параметров, определяющих методику проведения испытаний САВЗ. Данные параметры являются элементами множества тестовых испытаний. К ним отнесем: формулировку требования, цель испытаний, порядок проведения испытаний, условие принятия положительного решения. Так как некоторые пункты проверки нуждаются в дополнительных пояснениях, то дополнительным

элементом может быть пункт «комментарии к выполнению проверки», являющийся опционным.

Введем дополнительные отображения: $F_1: D \times T \to \{0,1\}$ и $F_2: ҒƆ \times D \to \{0,1\}$. Первое отображение характеризует соответствие корректности проводимых испытаний требованию, предъявляемому профилем защиты, второе – соответствие полноты выполнения проверки над объектом оценки желаемому результату. Таким образом, если некоторое испытание t_i соответствует требованию доверия d_j и получен требуемый результат, то F_1 будет отображением в 1, в противном случае – в 0. Аналогично для отображения F_2: если для объекта оценки $ҒƆ$ проверка требования d_k является функционально полной, данное отображение принимает значение 1, иначе – 0.

Итак, методика проведения испытаний САВЗ – это множество **Ψ,** состоящее из 6 элементов: $\Psi\ (ҒƆ, D, T, G, F_1, F_2)$. Элементы данного множества – это $ҒƆ$ - объект оценки, D – множество требований доверия к ОО, T – множество тестовых испытаний, проводимых в ходе сертификации ОО, G–схема составления тестовых испытаний, F_1, F_2 – отображения, характеризующие корректность и полноту проведения испытаний.

3. Составление методики проведения испытаний САВЗ.

Основными этапами проведения сертификационных испытаний САВЗ, отражаемыми в методики, являются следующие:

1) *Условия, объем, методы и порядок проведения испытаний.* На данном этапе определяются требования к испытательному стенду, на котором будут проводиться испытания, объем испытаний, структуризация программы и метода испытаний, а также выделяются особые условия проведения тестирования.

2) В*ыполнение тестовых испытаний над объектом оценки ҒƆ.*Осуществляется выполнение тестов $t_i \epsilon T$.

3) *Анализ полученных результатов.* Заключительный этап тестирования, когда осуществляется сравнение полученных результатов с эталонными. Данное требование считается выполненным, если

$$\begin{cases} F_1(\boldsymbol{f_i}, \boldsymbol{t_i}) \to \mathbf{1} \text{ для} \forall \boldsymbol{t_i} \epsilon \boldsymbol{T}, \forall \boldsymbol{f_i} \epsilon F_1 \\ F_2(\mathrm{W}, \boldsymbol{t_i}) \to \mathbf{1} \text{ для} \forall \boldsymbol{t_i} \epsilon \boldsymbol{T} \end{cases}$$

Далее приведены основные этапы и методы проведения тестовых испытаний для САВЗ типа «Г» по шестому классу защиты, предназначенных для применения на автономных автоматизированных рабочих местах. Основными угрозами, для противостояния которым используются САВЗ типа «Г», являются угрозы, связанные с внедрением в автономные автоматизированные рабочие места вирусов со съемных машинных носителей информации.

Рассмотрим несколько предъявляемых к САВЗ требований доверия, то есть элементов множества ***D*.** Функциональные требования, описанные в рассматриваемом профиле защиты, основаны на функциональных компонентах из ГОСТ Р ИСО/МЭК 15408–2. Требования доверия основаны на компонентах требований доверия из ГОСТ Р ИСО/МЭК 15408–3.Сертификационные испытаний по проверке соответствия САВЗ требованиям профиля защиты проводится на стенде испытательной лаборатории, монтируемом в соответствии с требованиями эксплуатационной документации. Конфигурация стенда может быть различной в зависимости от типа и класса защиты тестируемого САВЗ, однако на рисунке 1 приведена наиболее общая модель для тестирования ОО.

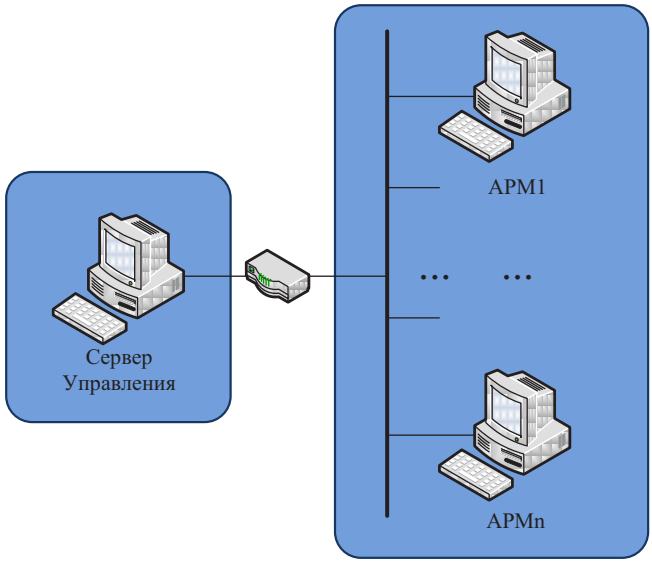

Рисунок 1. Модель стенда: общий вид испытательного стенда

На сервере управления расположен некоторый Центр Управления, с помощью которого задаются все необходимые настройки антивирусной защиты на рабочих станциях $АРМ_1$ – $АРМ_n$. На $АРМ_1$ – $АРМ_n$ соответственно установлено некоторое клиентское программное обеспечение, необходимое для осуществления связи с сервером.

4. Методика проверки соответствия ОО требованиям доверия

Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналогичный опыт или специфический опыт. Однако ОК обеспечивают доверие с использованием активного исследования. Активное исследование – это оценка продукта или системы для определения его свойств безопасности [3].Рассмотрим методики проверки некоторых требований.

4.1 Проверка наличия ролевого разграничения доступа.

При выполнении испытаний необходимо убедиться, что функции безопасности объекта (ФБО) поддерживают ролевое разграничение доступа, то есть обеспечивают наличие ролей пользователя, администратора и других. Кроме того ФБО должны быть способны ассоциировать пользователей с ролями.

Введем следующие обозначения: пусть $Rp=\{rp_1, \ldots, rp_t\}$ представляет собой множество ролей описанных в требованиях к тестируемому САВЗ, $R=\{r_1, \ldots, r_t\}$ множество ролей, поддерживаемых системой, а $U=\{u_1, \ldots, u_w\}$ множество пользователей тестируемого САВЗ. Отображение $\Psi: R \rightarrow U$ будем называть соотношением пользователей с ролями.

При проведении тестирования выполняются перечисленные ниже действия:

1. Анализ документации на САВЗ, выявление поддерживаемых ролей.
2. Создание пользователей $u_1, \ldots, u_t$.
3. Присвоение каждому пользователю u_i роли r_i $(i=1 \ldots t)$
4. Осуществление проверки наличия полномочий роли r_i для каждого пользователя u_i.

Критерий принятия положительного решения. Проверка считается выполненной успешно, если в ходе анализа документации выявлено, что множество ролей R, поддерживаемых САВЗ, совпадает с множеством R_p – ролей заданных в требованиях к системе, или включает его в себя, то есть $R \subseteq R_p$. В результате присвоения ролей каждому пользователю заданно отображение $\Psi: R \rightarrow U$, причем каждый пользователь обладает только полномочиями присвоенной ему роли.

4.2 Базовое обнаружение компьютерных вирусов

При выполнении испытаний необходимо убедиться, что ФБО могут выполнять обнаружение компьютерных вирусов в файловых областях носителей информации**.** Порядок проведения испытания следующий.

1. Настройка правил реагирования САВЗ на обнаружение предполагаемых вирусов на различных носителях информации. Примерами правил могут быть следующие: удаление обнаруженных вирусов, занесение зараженных объектов в карантин, игнорирование зараженных объектов и так далее.

2. Добавление нового устройства, содержащего зараженные объекты (например, внешнего USB-устройства, CD диска).

2. Фиксирование реакции САВЗ на зараженные объекты. В результате САВЗ должны применить к зараженным объектам действия, заданные ранее администратором безопасности. Данные об обнаруженных угрозах должны быть занесены в соответствующие журналы регистрации событий.

4.Экспорт журнала регистрации САВЗ. Анализ полученных результатов.

Критерий принятия положительного решения. Проверка считается выполненной успешно, если зафиксировано соответствие фактических (реагирование САВЗ на зараженные объекты **в** файловых областях носителей информации) и ожидаемых результатов (соответствие полученных результатов заранее установленным правилам реагирования).

4.3 Обработка объектов, подвергшихся воздействию

При выполнении испытаний необходимо убедиться, что ФБО при обнаружении вирусов выполняют удаление их из файлов, системных областей носителей информации. Порядок проведения испытания следующий.

1. Настройка правил реагирования САВЗ на обнаружение предполагаемых вирусов. Для каждого типа вирусных программ задание типа реагирования, например, «Удалять», «Игнорировать», «В карантин», «Информировать» и так далее. При необходимости с целью задания папки или диска, исключаемого из области проверки, настройка исключаемых путей, не подвергающихся контролю со стороны САВЗ, а также времени сканирования.

2. Применение заданных настроек к рабочим станциям, участвующим в процессе испытаний.

3. На рабочей станции осуществление копирования зараженных файлов с внешнего носителя на жесткий диск.

4. Регистрация реакции САВЗ на произведенные действия. Осуществление проверки успешного удаления (игнорирования, помещения в карантин и других действий) в соответствии с созданными правилами. Экспорт журнала регистрации САВЗ. Анализ полученных результатов.

Критерий принятия положительного решения. Проверка считается выполненной успешно, если зафиксировано предотвращение распространения вирусной инфекции в защищаемой локальной сети в соответствии с заданными правилами реагирования.

4.4 Обновление базы данных компьютерных вирусов.

При выполнении испытаний необходимо убедиться, что ФБО обеспечивают получение и установку обновлений базы данных компьютерных вирусов локально без применения средств автоматизации. Порядок проведения испытания следующий.

1. В локальной вычислительной сети (ЛВС) организации, эксплуатирующей САВЗ, определение ЭВМ, участвующих в процедуре обновления – тестовая ЭВМ и локальный сервер обновлений.

2. Настройка локального сервера обновлений на получение файлов сигнатур компьютерных вирусов с сервера обновлений. При необходимости задание времени осуществления обновлений баз данных вирусов.

3. Сохранение обновлений, полученных с сервера.

4. Обновление сигнатур компьютерных вирусов тестовой ЭВМ полученными файлами. Осуществление проверки полученных обновлений на тестовой ЭВМ.

Критерий принятия положительного решения. Проверка считается выполненной успешно, если САВЗ обладают средствами обновления баз правил компьютерных вирусов.

4.5 Методы анализа.

При выполнении испытаний необходимо убедиться, что ФБО способны выполнять проверки с целью обнаружения вирусов в объектах с использованием сигнатурных методов. Порядок проведения испытания следующий.

1. Настройка проверок САВЗ на предполагаемые вирусные воздействия.

2. При использовании сигнатурного анализа, осуществляется выбор сигнатур вторжения из имеющегося в САВЗ списка, согласно которым будет осуществляться обнаружение аномалий в системе. Для описания набора используемых сигнатур введем множество $Sg= \{Sg_1, Sg_2, \ldots Sg_n\}$,где Sg_i–элементы множества сигнатур из базы данных сигнатур вирусов в САВЗ. Тогда множество проверок САВЗ $Rules=\{Rule_1, Rule_2, \ldots Rile_n\}$.

Критерий принятия положительного решения. Проверка считается выполненной успешно, если зафиксировано соответствие фактических (результаты проверок САВЗ и фрагменты журнала регистрации событий) и ожидаемых результатов (соответствие сигнатурным/эвристическим правилам обнаружения вирусов САВЗ) при тестировании САВЗ.

5. Методы оптимизации

Задача оптимизации испытаний объекта оценки может быть представлена следующим образом. Пусть ξ: $Ǥ \times \Psi \rightarrow N_0$ – время, затрачиваемое оценщиками на выполнение проверки ОО, где Ψ – множество действий, необходимых для проведения испытаний, N_0 –множество натуральных чисел с 0. Отображение вида σ: $S \times Ǥ \rightarrow N0$ – характеризует затраты на проведение испытаний. Тогда задача минимизации времени тестирования при ограничениях на затраты может быть представлена как:

$$\begin{cases} \sum_{i} \xi(\Omega, \psi_i) \rightarrow min \\ \sum_{i} \sigma(s_i, \Omega) \leq \sigma_0 \end{cases}$$

В формуле σ_0 – ограничения, накладываемые на затраты. В контексте описанных выше методик тестирования оптимизация подразумевает частичную автоматизацию процесса испытания, например, автоматическое внесение объектов тестовой вирусной базы в множество проверяемых объектов.

Заключение

В данной работе была описана математическая модель оценки соответствия САВЗ *6 класса согласно требованиям профиля защиты* ИТ.САВЗ.Г6.ПЗ, а так же рассмотрены особенности и методы проведения сертификационных испытаний на соответствие им. В статье рассмотрены и структурированы методы и способы, применяемые при проведении тестовых испытаний в испытательной лаборатории, позволяющие производить проверки с наименьшими затратами и трудоемкостью, что существенно снижает не только время проведения испытаний, но и их стоимость.

Список использованной литературы

1. Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа Г шестого класса защиты ИТ.САВЗ.Г6.ПЗ // Официальный сайт ФСТЭК России. URL: http://fstec.ru/_docs/pz_c6.doc (дата обращения 18.02.13)
2. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31-33.
3. 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.
4. Барабанов А.В, Гришин М.И., Марков А.С. Формальный базис и метабазис оценки соответствия средств защиты информации объектов информатизации// Известия Института инженерной физики. 2011, № 3. С.82-88.