Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь, 2011. № 3. С.48-53. ISSN 2075-7298

А.В.Барабанов, А.С.Марков, В.Л.Цирлов

НПО «Эшелон», г.Москва

Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации

Введение

Обязательная оценка соответствия автоматизированных систем (АС) требованиям безопасности информации проводится в форме аттестации объектов информатизации или сертификации средств защиты информации (СЗИ) [1]. Кроме того, процедура оценки соответствия может применяться на этапах приемо-сдаточных испытаний, внутреннего аудита и контроля эффективности защиты информации. Базовым документом, в котором определены требования к подсистемам безопасности АС, является руководящий документ Гостехкомиссии России [2]. Существующие типовые методики аттестационных или сертификационных испытаний носят описательный характер, что затрудняет автоматизацию и оптимизацию процессов оценки соответствия АС. При этом исследования показывают, что более половины средств, выделяемых на разработку АС в защищенном исполнении, тратится именно на этапы испытаний и внедрения системы.

В статье рассмотрен подход к формализации методики оценки соответствия АС, позволяющий определить факторы, связанные с временем, стоимостью и полной испытаний АС.

Формализованное описание методики проведения испытаний

Под АС, согласно ГОСТ 34.003-90, будем понимать систему, состоящую из персонала и комплекса средств автоматизации его деятельности, реализующую информационную технологию выполнения установленных функций. Таким образом, АС представляет собой совокупность следующих объектов: средства вычислительной техники, программное обеспечение, каналы связи, информация на различных носителях, персонал и пользователи системы, эксплуатационная и организационно-распорядительная документация.

Пусть $R = \{r_i\}$ - множество требований, предъявляемых к АС Σ, $T = \{t_i\}$ – множество тестовых процедур, проверяющих реализацию требований. Каждая тестовая процедура $t_i \in T$ характеризуется следующими элементами: цель выполнения, объекты проверки (факторы оценки соответствия), последовательность выполняемых действий, критерий принятия положительного решения.

Под *методом разработки тестовых процедур* будем понимать отображение $M: \Sigma \times R \to T$ [3]. Функция M на основе требования $r_i \in R$ и информации о реализации АС Σ, подлежащего процедуре оценки соответствия, выполняет генерацию тестовой процедуры $t_i \in T$, выполняемой для проверки удовлетворения АС требованию $\mathrm{r}_i \in R$. Отметим, что функция M для данной АС Σ является биективным отображением.

Введем операторы выполнения требования F_R и корректности выполнения тестовой процедуры F_C для данных $\Sigma,\ r_i,\ t_i$.

Оператор выполнения требования r для АС Σ $F_R: \Sigma \times R \to \{0,1\}$:

$$F_R(\Sigma, r_i) = \begin{cases} 1, \text{ если требование } r_i \text{ выполнено для } \Sigma; \\ 0, \text{ в противном случае.} \end{cases}$$

Оператор корректности выполнения тестовой процедуры t для АС Σ $F_C: \Sigma \times T \to \{0,1\}$:

$$F_C(\Sigma, t_i) = \begin{cases} 1, \text{ если тест } t_i \text{ выполнен успешно для } \Sigma; \\ 0, \text{ в противном случае.} \end{cases}$$

Методикой оценки соответствия АС назовем набор из пяти объектов $\mathbb{A} = \{\Sigma, R, M, F_R, F_C\}$, где R - множество требований, предъявляемых к АС Σ, M - метод разработки тестовых процедур, F_R и F_C операторы выполнения требования и корректности

выполнения тестовой процедуры соответственно, а также для $\forall r_i \in R$ справедливо $F_R(\Sigma, r_i) \Rightarrow F_C\big(\Sigma, M(\Sigma, r_i)\big)$.

Методика предусматривает наличие трех стадий: планирование, тестирование и анализ результатов.

На стадии *планирования* выполняется анализ документации и особенностей работы АС. Перед началом проведения тестирования эксперты должны установить, что в документации на объект испытаний (например, в задании по безопасности на АС) декларируется соответствие АС требованиям R, то есть $F_R(\Sigma, r_i) = 1$ для $\forall r_i \in R$. На основании данных, полученных в ходе анализа документации, тестовых запусков АС и предъявляемых требований, формируется множество тестовых процедур $T = \{t_i\}$, где $t_i = M(\Sigma, r_i)$.

Тестирование АС выполняется с использованием набора тестовых процедур $T = \{t_i\}$. В результате тестирования для каждой тестовой процедуры определяются результаты выполнение тестовой процедуры t_i, подлежащие регистрации. При проведении оценки соответствия АС, как правило, применяются следующие методы: экспертно-документальный метод, метод опроса и инструментальный метод.

На стадии *анализа* фактических и эталонных значений получают множество упорядоченных пар вида $\big(t_i, F_C(\Sigma, t_i)\big)$. Для АС Σ декларируется соответствие требованиям $R = \{r_i\}$, если:

$$\sum_{i=1}^{n} \Big(F_R(\Sigma, r_i) \cdot F_C\big(\Sigma, M(\Sigma, r_i)\big)\Big) = n,$$

то есть в ходе проведения испытаний установлено соответствие реальных возможностей АС по декларируемым в документации или нормативном документе.

Методика испытаний автоматизированной системы на соответствие требованиям безопасности информации

Руководящий документ Гостехкомиссии России [2] устанавливает классификацию АС, подлежащих защите от несанкционированного доступа (НСД) к информации, и задаёт требования по защите информации в АС различных классов. Рассмотрим формализованный порядок проверки для следующих наиболее ресурсоемких требований $R_{IS} = \{r_1, r_2, r_3\}$ [2]:

–*требование* r_1: должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

–*требование* r_2: должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

–*требование* r_3: должна быть обеспечена целостность программных средств защиты информации от НСД, а также неизменность программной среды.

Перед началом проведения тестирования эксперты должны установить, что в технической документации (например, в задании по безопасности на АС) на объект испытаний декларируется соответствие АС требованиям R_{IS}, то есть $F_R(\Sigma, r_i) = 1$ для $\forall r_i \in R_{IS}$.

Частная методика проверки механизмов идентификации и аутентификации субъектов доступа

Проверка выполняется с целью контроля организационных мероприятий, которые позволяют удовлетворить требования к парольной политике, анализа установленных параметров функционирования средств идентификации и аутентификации, контроля корректности функционирования механизмов идентификации и аутентификации, а также контроля процедуры смены паролей пользователями.

Введем определения, используемые при описании тестовой процедуры. Пусть A - алфавит паролей и идентификаторов субъектов доступа (пользователей АС). Обозначим идентификатор пользователя $id \in ID \subseteq A^*$, пароль - $pwd \in PWD \subseteq A^*$. Учетная запись субъекта доступа $s_i \in S$ характеризуется следующим кортежем $s_i = (id_j, pwd_k)$. Введем оператор корректности учетных данных $F_{AUT}: S \to \{0,1\}$:

$$F_{AUT}(s_i) = \begin{cases} 1, \text{ выполнен вход в систему;} \\ 0, \text{ в противном случае.} \end{cases}$$

При проверке корректности реализации механизмов идентификации и аутентификации может быть использована следующая тестовая процедура.

Тогда проверка будет включать следующую последовательность действий:

1. Проверить наличие эксплуатационных документов на АС, в которых регламентирован порядок проведения парольной защиты АС. Проверить наличие следующих положений:

−требования к сложности паролей (длина, сложность);

−обязанности администратора безопасности по реализации парольной политики АС (генерация паролей, распределение паролей);

−обязанности пользователей по реализации парольной политики АС (генерация паролей, смена паролей).

2. Определить установленные СЗИ от НСД в АС значения для следующих параметров: минимальная длина пароля, сложность пароля (алфавит паролей), максимальный срок действия пароля, максимальное число неудачных попыток входа пользователей в АС, после которого осуществляется блокировка работы пользователя, реакция АС на превышение максимального числа неудачных попыток входа пользователя.

3. Произвольным образом выбрать несколько АРМ и выполнить запросы на идентификацию и проведение аутентификации с использованием различных сочетаний учетных данных: зарегистрированный/незарегистрированный идентификатор, верный/неверный пароль – $try_i = (id_j, pwd_k)$.

4. Под учетными записями пользователей произвести попытки установить пароль, не соответствующий нормативным требованиям [2]. Для этого осуществить:

−попытку установить пароль, длина которого менее 6 символов;

−попытки установить пароль, состоящий исключительно из цифр, либо только из букв.

Результатами выполнения тестовой процедуры, подлежащей регистрации, являются:

1. Положения документации на АС относительно реализации и сопровождения системы парольной защиты.

2. Конфигурация СЗИ от НСД АС в части реализации парольной защиты.

3. Полученные результаты тестовых запросов на идентификацию и аутентификации - множество $\{F_{AUT}(try_i)\}$.

4. Полученные результаты тестовых попыток изменения паролей.

В данном случае критериями принятия положительного решения являются следующие:

1. В нормативных документах организации, эксплуатирующей АС, установлены требования (сложность, минимальная длина) к паролям пользователей рассматриваемой АС соответствующие нормативным требованиям [2].

2. В нормативных документах организации, эксплуатирующей АС, описана процедура действий администратора безопасности по реализации парольной политики АС (процедуры генерация паролей, распределение паролей);

3. Настройки СЗИ от НСД выполнены таким образом, что длина пароля для пользователей АС не может быть менее 6 символов, а установленные ограничения сложности не позволяют использовать пароли, состоящие из однотипных символов.

4. После ввода зарегистрированного идентификатора и пароля пользователю предоставляется доступ к АС: $F_{AUT}(try_i) = 1 \Leftrightarrow try_i \in S$.

5. После ввода незарегистрированного идентификатора и/или неверного пароля пользователю отказывается в доступе к АС: $F_{AUT}(try_i) = 0 \Leftrightarrow try_i \notin S$.

6. Все попытки установить пароль, не соответствующий нормативным требованиям, завершились неудачно.

Частная методика проверки средств управления доступом

Целью проверки является определение степени соответствия фактических настроек системы дискреционного разграничения доступа требуемым настройкам, определенным в матрице доступа. Исходными данными для формирования тестовой процедуры являются: множество возможных субъектов доступа $S = \{S_i\}$, множество защищаемых объектов $O = \{O_i\}$, конечное множество прав доступа $P = \{P_i\}$ и матрица доступа.

Последовательность выполняемых действий следующая:

1. Идентификация субъектов (например, пользователей) $S = \{S_i\}$ и объектов доступа (например, объектов файловой системы) $O = \{O_i\}$.

2. Идентификация матрицы доступа субъектов к защищаемым объектам.

3. Для каждой тройки $(S_i, O_j, P_k) \in S \times O \times P$ выполнение тестирования фактического наличия права P_k у субъекта S_i по отношению к объекту O_j (тестирование настроек СЗИ АС).

4. Сравнение фактических прав доступа с требуемыми правами, определенными в матрице доступа.

Результаты выполнение тестовой процедуры, подлежащие регистрации:

1. Матрица доступа субъектов к защищаемым объектам.

2. Фактически результаты тестирования системы дискреционного разграничения доступа.

В качестве критерия принятия положительного решения имеем полученное соответствие фактических и декларируемых прав доступа, определенных в матрице доступа.

Частная методика проверки механизмов контроля целостности

Целью выполнения процедуры является определение степени соответствия функциональных возможностей СЗИ от НСД АС по контролю целостности программных СЗИ от НСД.

Пусть $FILE = \{file_i\}$ - множество файлов СЗИ от НСД (конфигурационные файлы, программные модули). Введем операторы нарушения целостности F_{MOD} и контроля целостности файлов СЗИ от НСД F_{INT}.

Оператор нарушения целостности $F_{MOD}: FILE \to \{0,1\}$:

$$F_{MOD}(file) = \begin{cases} 1, \textit{ целостность файла нарушена при проведении испытаний}; \\ 0, \textit{ в противном случае.} \end{cases}$$

Оператор контроля целостности файлов СЗИ от НСД $F_{INT}: FILE \to \{0,1\}$:

$$F_{INT}(file) = \begin{cases} 1, \textit{зафиксировано нарушение целостности файла}; \\ 0, \textit{ в противном случае.} \end{cases}$$

Обозначим $FILE^{\Delta} = \{file_1^{\Delta}, file_2^{\Delta}, \dots, file_n^{\Delta}\}$ - множество файлов СЗИ от НСД, модифицированных в ходе проведения испытания. При этом выполняется модификация файла $file_i$ в файл $file_i^{\Delta}$. При проверке корректности реализации механизма контроля целостности может быть использована следующая тестовая процедура.

Последовательность выполняемых действий следующая:

1. Идентификация множества файлов СЗИ от НСД $FILE = \{file_1, file_2, \dots, file_n\}$.

2. Внесение изменений в файлы (изменение конфигурации, подмена (модификация) исполняемых файлов и т. п.) – получение множества измененных файлов $FILE^{\Delta} = \{file_1^{\Delta}, file_2^{\Delta}, \dots, file_n^{\Delta}\}$.

3. Инициализация проверки целостности файлов СЗИ от НСД (создание условий, при которых СЗИ от НСД осуществляет контроль целостности).

4. Анализ реакции СЗИ от НСД на нарушение целостности своей программной или информационной части.

Результаты выполнение тестовой процедуры, подлежащие регистрации, являются:

1. Множество файлов $FILE = \{file_1, file_2, \dots, file_n\}$.
2. Множество модифицированных файлов $FILE^{\Delta} = \{file_1^{\Delta}, file_2^{\Delta}, \dots, file_n^{\Delta}\}$.
3. Реакции СЗИ от НСД на нарушение целостности: $F_{INT}(file_1^{\Delta}), F_{INT}(file_2^{\Delta}), \dots, F_{INT}(file_n^{\Delta})$.

Критерием принятия положительного решения является факт, СЗИ от НСД обнаружены все факты нарушения целостности:

$F_{INT}\left(file_i^{\Delta}\right) = F_{MOD}(file_i)$ для $\forall i \in [1, n]$.

Способы оптимизации процедуры оценки соответствия

Из представленных частных методик следует, что основной проблемой, с которой сталкиваются организации при проведении оценки соответствия, является рост временных и материальных затрат. Например, при проведении проверки механизма дискреционного разграничения доступа необходимо выполнить $|S| \cdot |O| \cdot |P|$ типовых операций. В общем случае можно показать, что время $\mathcal{T}_{\Sigma}$, затрачиваемое на проведение испытаний, носит экспоненциальный характер роста:

$$\mathcal{T}_{\Sigma} \sim n \cdot \mathcal{v}^{\mathcal{w}},$$

где n – число проверяемых требований, $\mathcal{w}$ - число факторов тестирования (например, «учетная запись пользователя»), $\mathcal{v}$ – число возможных значений фактора тестирования.

Задача оптимизации процедуры проведения оценки соответствия АС может быть сформулирована следующим образом.

Пусть отображение вида $\mathcal{T}: T \times \Sigma \to \mathbb{N}_0$ – это время, затрачиваемое экспертами на выполнение оценки соответствия АС Σ с использованием тестовой процедуры t_i, а отображение $C: R \times \Sigma \longrightarrow \mathbb{N}_0$ – затраты на проведение оценки соответствия АС Σ требованиям R. Задача оптимизации может выглядеть следующим образом (минимизация времени тестирования при ограничениях на затраты):

$$\begin{cases} \sum_i \mathcal{T}(t_i, \Sigma) \to min, \\ \sum_i C(r_i, \Sigma) \le C_M, \end{cases}$$

где C_M – ограничения, накладываемые на затраты.

В качестве методов, позволяющих решить задачу оптимизации, могут быть предложены следующие.

1. *Совмещение отдельных видов испытаний*. При проведении оценки соответствия рекомендуется выполнять совмещение некоторых видов испытаний. Например, процедура тестирования подсистемы регистрации событий может быть совмещена с процедурой тестирования подсистемы разграничения доступа и идентификации/аутентификации. Совмещение отдельных видов испытаний позволит существенно сократить временные затраты на процедуру оценки соответствия.

2. *Применение методов выборочного контроля при проведении испытаний*. Выборочный контроль предполагает применение процедуры проверки менее чем к 100% совокупности проверяемых элементов (выборка) при использовании экспертно-документального метода, метода опроса или инструментального метода. Например, при тестировании подсистемы дискреционного разграничения доступа, проверка может быть выполнена только для некоторой совокупности ячеек матрицы доступа, выбранной случайным образом, а вывод о соответствии АС требованию нормативного документа [2] сделан в том случае, если проверка была выполнена успешно для всей выборки. Размеры тестируемых выборок могут быть определены исходя из гипергеометрического распределения, описывающего вероятность того, что в выборке из N различных объектов, отобранных из генеральной совокупности, ровно K объектов являются несоответствующими установленному требованию. Отметим, что при использовании методов выборочного контроля необходимо выполнять определение приоритетов проверяемых требований с целью дальнейшего определения необходимого количества тестируемых объектов.

3. *Использование программных средств тестирования*. Для сокращения временных затрат при проведении испытаний необходимо использовать программные средства, позволяющие автоматизировать процедуру тестирования. Могут использоваться как инструментальные средства, широко представленные на современном рынке программного обеспечения, так и программы собственной разработки, написанные на языках сценариев [4-8].

Заключение

Рассмотренное в работе решение задачи формализации процессов оценки соответствия АС позволяет упростить автоматизацию аттестационных и сертификационных испытаний АС в защищенном исполнении.

Основной проблемой, с которой сталкиваются организации при проведении оценки соответствия, является рост временных и материальных затрат, связанный, в первую очередь, с большим количеством проверяемых объектов. Предложенные методические приемы позволяют сократить затраты на проведение оценки соответствия АС и решить задачу минимизация времени оценки соответствия при заданных ограничениях на затраты.

Концептуальный подход к формализации процедуры оценки соответствия может быть рекомендован для проведения разного рода испытаний средств защиты информации, аттестации объектов информатизации, а также аудита систем безопасности [9-12].

Список литературы

1. Правовое обеспечение информационной безопасности / С.В.Дворянкин, В.А.Минаев, М.М.Никитин, С.В.Скрыль, Н.С.Хохлов, А.П.Фисун, - М.: Маросейка, 2008. 368 с.

2. Руководящий документ. Автоматизированные системы защита от несанкционированного доступа к информации классификация автоматизированных систем и требования по защите информации // Сборник руководящих документов по защите информации от несанкционированного доступа. М.: Гостехкомиссия России, 1998. С. 16-32.

3. Gourlay J.S. A Mathematical Framework for the Investigation of Testing // IEEE Transactions on Software Engineering. 1983. Vol. SE-9, №. 6. P. 686-709.

4. Ермолаев С.А., Марков А.С., Инструментальные средства аттестации программных ресурсов объектов информатизации: Часть 1. // Information Security/Информационная безопасность. 2004. № 4. С.58-59.

5. Ермолаев С.А., Марков А.С., Инструментальные средства аттестации программных ресурсов объектов информатизации: Часть 2. // Information Security/Информационная безопасность, 2004. № 5. С.58-61.

6. Марков А.С., Цирлов В.Л., Миронов С.В. Аттестация без проблем: об использовании сетевых сканеров безопасности при аттестации АС // Information Security/Информационная безопасность. 2005. № 3. С. 44-45.

7. Марков А.С., Миронов С.В., Цирлов В.Л. Опыт тестирования сетевых сканеров уязвимостей // Информационное противодействие угрозам терроризма, 2005. № 5. - С. 109-122.

8. Барабанов А.В. Инструментальные средства проведения испытаний систем по требованиям безопасности информации // Защита информации. Инсайд. 2011. №1. С. 2-4.

9. Марков А.С., Цирлов В.Л., Маслов В.Г., Олексенко И.А. Тестирование и испытания программного обеспечения по требованиям безопасности информации // Известия Института инженерной физики, 2009. Т. 2. № 12. С. 2-6.

10. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия Южного федерального университета, 2006. Т. 62. № 7. С. 82-87.

11. Колесников Д.В., Петров А.Ю., Храмов В.Ю. Методика оценки защищенности специального программного обеспечения при проведении испытаний автоматизированных систем // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2010. № 1. С. 74-79.

12. Дорофеев А.В. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд, 2010. №6. С. 2-3.