Инструментальные средства проведения испытаний систем по требованиям безопасности информации

В соответствии с «Доктриной информационной безопасности Российской Федерации» обеспечение безопасности информационных ресурсов от несанкционированного доступа представляет собой одну из составляющих национальных интересов России в информационной сфере. Это определяет необходимость выполнения специальных действий по оценке соответствия средств защиты информации от несанкционированного доступа, используемых при построении автоматизированных систем (АС), требованиям нормативных и иных документов по защите информации. В данной статье рассматриваются инструментальные средства и методы, которые могут быть использованы при проведении функционального тестирования систем и комплексов защиты по требованиям безопасности информации в соответствии с требованиями руководящих документов.

А. Барабанов
МГТУ им. Н. Э. Баумана

Испытания средств защиты информации от несанкционированного доступа

Как известно, руководящий документ (РД) «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) устанавливает 7 классов защищенности средств защиты информации (СЗИ) от несанкционированного доступа (НСД) на базе перечня показателей защищенности и совокупности описывающих их требований. Рассмотрим общий порядок проведения испытаний СЗИ от НСД на соответствие требованиям РД [1], предъявляемым к дискреционному принципу контроля доступа, а также к механизму очистки внешней памяти.

Проверка реализации требований к дискреционному принципу контроля доступа

Порядок проведения данной проверки в общем случае выглядит следующим образом (рис. 1).

1. Создание тестовых субъектов (например, пользователей) $S = \{S_1, S_2, ..., S_i, ..., S_n\}$ и объектов доступа (например, объектов файловой системы) $O = \{O_1, O_2, ..., O_i, ..., O_n\}$.

2. Настройка правил разграничения доступа субъектов испытываемого СЗИ от НСД к тестовым защищаемым объектам. Данная операция заключается в настройке матрицы доступа. Строка матрицы доступа соответствует субъекту S_i, а столбец – объекту O_j. На пересечении строки и столбца указаны права доступа $r_v \in R$ соответствующего субъекта к данному объекту.

3. Тестирование фактического наличия права r_k у субъекта S_j по отношению к объекту O_l (тестирование настроек СЗИ от НСД).

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

Для автоматизации процесса проверки реализации данного требования РД [1] могут быть использованы программы семейств «Ревизор», «НКВД» или программы, написанные на языках сценариев (например, Perl или Python).

Проверка реализации требований к механизму очистки внешней памяти

Порядок проведения данной проверки в общем случае выглядит следующим образом.

1. Настройка механизма очистки внешней памяти тестируемого СЗИ от НСД в соответствии с информацией, приведенной в эксплуатационной документации.

2. Создание тестовой последовательности символов на внешнем накопителе ЭВМ, на которой установлено тестируемое СЗИ от НСД.

3. Определение сектора накопителя, в котором располагается тестовая последовательность символов: данный сектор определяется путем поиска тестовой последовательности на накопителе с использованием

специализированного программного обеспечения (ПО).

4. Удаление созданного действием 2 файла путем применения штатных средств гарантированного удаления информации СЗИ от НСД.

5. Выполнение анализа сектора внешнего накопителя, определенного действием 3, на предмет наличия в нем созданной ранее последовательности символов (выполняется с помощью специализированного программного обеспечения).

6. Если тестовая последовательность не обнаружена, эксперт испытательной лаборатории (ИЛ) выносит вердикт о соответствии тестируемого СЗИ от НСД требованию РД [1] к очистке внешней памяти.

При проведении проверки реализации данного требования РД [1] могут быть использованы программный комплекс «Средство анализа защищенности

«Сканер-ВС» (ПК «Сканер-ВС»), программы семейств Terrier, «НКВД».

Испытания межсетевых экранов

Требования к СЗИ от НСД, обеспечивающим безопасное взаимодействие сетей ЭВМ посредством управления межсетевыми потоками информации, предъявляет РД [2] «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997). Наиболее трудоемкие требования с точки зрения процесса поведения сертификационных испытаний предъявляются к функциям управления доступом (фильтрация данных и трансляция адресов).

Порядок проведения данных проверок в общем случае выглядит следующим образом (рис. 2).

1. Настройка правил фильтрации МЭ в соответствии с проверяемым требованием РД [2].

2. Запуск ПО перехвата и анализа сетевых пакетов во внутреннем и внешнем сегментах сети.

3. Генерация сетевых пакетов из внутренней сети во внешнюю (или наоборот), прохождение которых

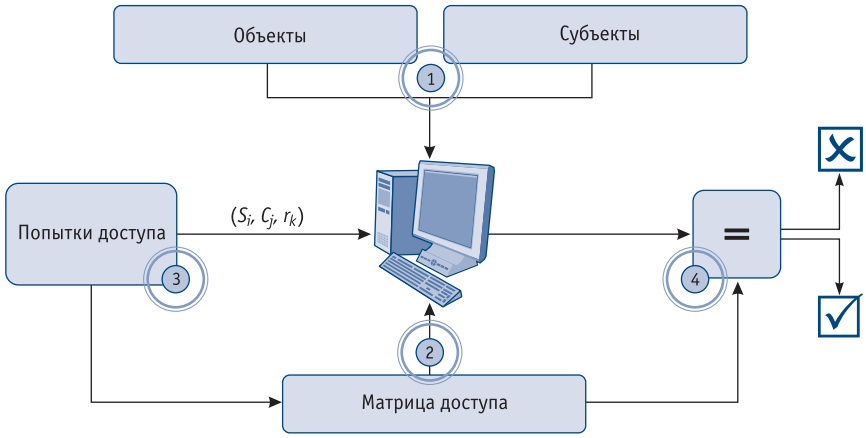

Рис. 1. ***Порядок тестирования реализации требований к дискреционному принципу контроля доступа***

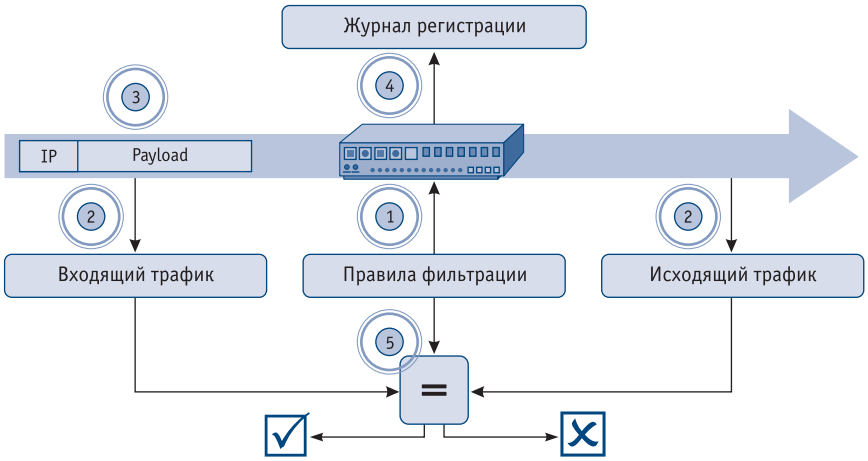

Рис. 2. ***Порядок тестирования функций управления доступом МЭ***

разрешается (запрещается) в соответствии с правилами фильтрации межсетевого экрана.

4. Завершение перехвата сетевых пакетов, экспорт журнала регистрации разрешенных и запрещенных пакетов МЭ.

5. Исходя из полученных данных, эксперт ИЛ делает вывод о соответствии или несоответствии фактических (пакеты на входном интерфейсе МЭ, пакеты на выходном интерфейсе МЭ и фрагмент журнала регистрации событий МЭ) и ожидаемых результатов (правила фильтрации МЭ) тестирования. При их соответствии выносится вердикт о том, что МЭ отвечает требованию РД [2].

При проведении тестирования реализации требования РД [2] к функциям управления доступом могут быть использованы, например, следующие программы: *nmap, Packet Generator* (генерация сетевых пакетов), *wireshark, tcpdump* (перехват и анализ сетевых пакетов), ПК «Сканер-ВС» (генерация сетевых пакетов, перехват и анализ сетевых пакетов).

Анализ защищенности автоматизированных систем

Обязательный анализ защищенности АС выполняется в форме аттестации или сертификации на соответствие руководящего документа Гостехкомисии [3]. В ходе проведения проверки анализируются фактические настройки СЗИ АС, их соответствие требованиям нормативных документов и эксплуатационной документации АС. Основное отличие от процедуры испытаний СЗИ заключается в том, что проверяемая АС должна быть настроена в соответствии с требованиями нормативных документов до начала проведения испытаний. Задача эксперта ИЛ (или органа по аттестации) заключается в анализе текущих настроек СЗИ АС и их влияния на безопасность информации, обрабатываемой в АС.

НОВОСТИ

При проведении анализа защищенности могут применяться программные продукты, используемые для проведении испытаний СЗИ по требованиям безопасности информации. Более подробную информацию о методах и инструментальных средствах, используемых при проведении анализа защищенности АС, можно найти в работе [4].

Возможность применения инструментального комплексов проведения испытаний

В качестве инструментального комплекса испытаний удобно воспользоваться средством анализа защищенности «Сканер-ВС», позволяющим проводить большое количество типов проверок в соответствии с требованиями руководящих документов. Варианты использования программного комплекса (ПК) «Сканер-ВС» при проведении функционального тестирования систем и комплексов защиты по требованиям безопасности информации приведены далее по тексту.

1. РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992):
- генерация сетевых пакетов с необходимым для проведения испытаний набором атрибутов;
- перехват и анализ сетевых пакетов.

2. РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1997):
- проверка механизма очистки внешней памяти.

3. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992):
- проверка очистки освобождаемых областей внешней памяти;
- проверка подсистемы межсетевого экранирования;
- поиск уязвимостей в ресурсах сети;
- локальный аудит паролей учетных записей ОС.

ПК «Сканер-ВС» обладает рядом заметных достоинств.

1. ***Полнота инструментария.*** ПО, входящее в состав ПК «Сканер-ВС», позволяет проводить широкий диапазон проверок систем и комплексов защиты по требованиям РД ФСТЭК России и приказов Министра обороны Российской Федерации.

2. ***Простота использования.*** ПК «Сканер-ВС» представляет собой носитель информации, который запускает свою собственную среду (операционная система, производная от Linux) с предустановленным тестовым ПО. Это позволяет сократить временные расходы экспертов ИЛ на поиск, установку и настройку ПО, применяемого при проведении испытаний, в том числе и операционной системы, под которой функционирует тестовое ПО.

3. ***Сертификаты соответствия.*** ПК «Сканер-ВС» является сертифицированным в системах сертификации СЗИ ФСТЭК России и Минобороны России средством контроля эффективности применения СЗИ.

ЛИТЕРАТУРА

1. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – Гостехкомиссия России, 1992.

2. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. – Гостехкомиссия России, 1997.

3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Гостехкомиссия России, 1992.

4. Марков А. С., Ермолаев С. А. Инструментальные средства аттестации программных ресурсов объектов информатизации // Information Security. 2004, №№ 4–5.