Марков А.С., Цирлов В.Л., Барабанов А.В. Разработка методики испытаний межсетевых экранов по требованиям безопасности информации. // Вопросы защиты информации, 2011. № 3. С.19-24. ISSN 2073-260

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

# РАЗРАБОТКА МЕТОДИКИ ИСПЫТАНИЙ МЕЖСЕТЕВЫХ ЭКРАНОВ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

## Введение

Базовыми средствами построения любой системы сетевой защиты являются межсетевые экраны (МЭ), число различных семейств которых в настоящее время превышает несколько сотен. Существующие типовые методики тестирования МЭ носят описательный характер, что затрудняет автоматизацию и оптимизацию процессов оценки соответствия компьютерных сетей и средств межсетевой защиты. В статье рассмотрен подход к формализации методики испытаний МЭ, позволяющий определить факторы, связанные с временем, стоимостью и полной испытаний МЭ.

## Формализованное описание методики проведения испытаний

Под МЭ $\Sigma$ понимается локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС [1].

Пусть $R = \{r_i,\}$ - множество требований, предъявляемых к МЭ $\Sigma$, $T = \{t_i\}$ – множество тестовых процедур, проверяющих реализацию предъявляемых требований.

Под *методом разработки тестовых процедур* будем понимать отображение: $M: \Sigma \times R \to T$. Функция $M$ на основе требования $r_i \in R$ и информации о реализации МЭ $\Sigma$. Отметим, что функция $M$ для данного МЭ $\Sigma$ является биективным отображением.

Каждая тестовая процедура $t_i \in T$ характеризуется целью выполнения, последовательностью выполняемых действий, результатом выполнения тестовой процедуры и критерием принятия положительного решения.

*Цель испытания* содержит изложение намерения о выполнения оценки соответствия МЭ предъявляемым требованиям. *Последовательность выполняемых действий* определяет набор шагов, осуществляемых экспертом для приведения МЭ в

исходное состояние и выполнения тестовой процедуры. *Результаты выполнения тестовых процедур* фиксируются с использованием различных программных средств (ПС) проведения испытаний, таких как: средства генерации и перехвата сетевого трафика, поиска остаточной информации, проверки системы разграничения доступа. *Критерий принятия положительного решения* должен содержать эталонные результаты выполнения тестовых процедур. Введем операторы выполнения требования $F_R$ и корректности выполнения тестовой процедуры $F_C$.

Оператор выполнения требования $r_i$ для МЭ $F_R: \Sigma \times R \to \{0,1\}$:

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

Оператор корректности выполнения тестовой процедуры $t_i$ для МЭ $\Sigma$ $F_C: \Sigma \times T \to \{0,1\}$:

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

Оператор $F_C$ показывает, что для МЭ $\Sigma$ выполнение тестовой процедуры завершилось успешно: фактические результаты, зарегистрированные при выполнении теста, соответствуют эталонным значениям, указанным в описании тестовой процедуры.

*Методикой испытаний* назовем набор из пяти объектов $\mathbb{A} = \{\Sigma, R, M, F_R, F_C\}$, где $R$ - множество требований, предъявляемых к МЭ $\Sigma$, $M$ - 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 $F_R(\Sigma, r_i) \Rightarrow F_C\big(\Sigma, M(\Sigma, r_i)\big)$.

В общем виде испытания включают три стадии: планирование, тестирование, анализ результатов.

При *планировании* выполняется анализ документации и особенностей работы МЭ. Эксперты должны установить, что в технической документации разработчик декларирует соответствие МЭ требованиям $R$, то есть $F_R(\Sigma, r_i) = 1$ для $\forall r_i \in R$. На основании анализа документации, тестовых запусков МЭ и предъявляемых требований, формируется множество тестовых процедур $T = \{t_i\}$, где $t_i = M(\Sigma, r_i)$.

*Тестирование* выполняется с использованием набора тестовых процедур $T = \{t_i\}$, в результате чего для каждой тестовой процедуры определяются результаты выполнение тестовой процедуры, подлежащие регистрации.

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

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

то есть в ходе проведения испытаний установлено соответствие реальных возможностей МЭ декларируемым в документации или нормативном документе [1,2].

**Методика испытаний межсетевых экранов на соответствие требованиям безопасности информации**

Требования к МЭ по безопасности информации определены в руководящем документе Гостехкомиссии России [1], в котором указаны пять классов защищенности. Каждый класс характеризуется минимальной совокупностью требований. Рассмотрим порядок проверки для наиболее ресурсоемких требований $R = \{r_1, r_2, r_3\}$ (см. табл 1).

Таблица 1.

**Основные требования к межсетевым экранам**

| Обозначение | Требование |
|---|---|
| $r_1$ | МЭ должен обеспечивать фильтрацию на сетевом уровне. Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов. |
| $r_2$ | МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия. Дополнительно МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась. |
| $r_3$ | МЭ должен содержать средства контроля за целостностью своей программной и информационной части. |

Типовая схема испытательного стенда представляет собой два сетевых сегмента с ЭВМ, разделенных МЭ (см. рис. 1).

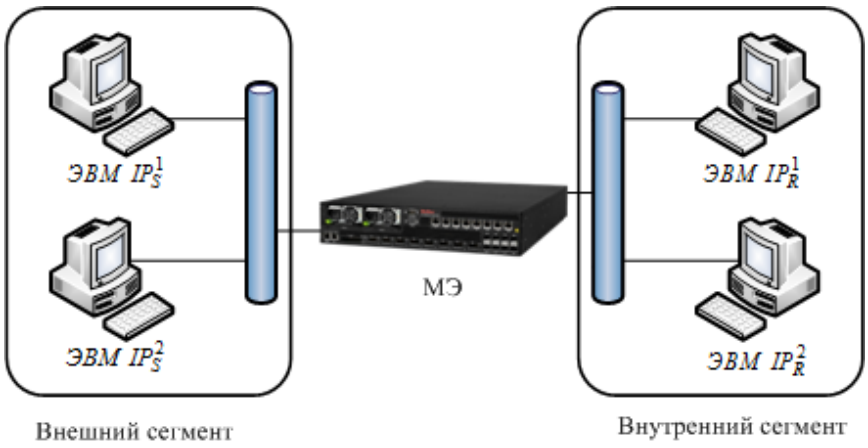


Рис. 1. Схема типового испытательного стенда тестирования межсетевого экрана

**Проверка фильтрации данных и трансляции адресов**

Цель выполнения проверки состоит в определение степени соответствия функциональных возможностей МЭ по фильтрации сетевых пакетов с учетом следующих параметров: сетевого адреса отправителя, сетевого адреса получателя. Исходными данными для формирования тестовой процедуры $t_1$ являются множество сетевых адресов, используемых в тестовых сегментах: $IP = IP_S \cup IP_R = \{IP_S^1, IP_S^2, \dots, IP_R^1, IP_R^2\}$. Предполагается, что при проведении тестирования выполняется отправление пакетов из внешнего сегмента сети (сетевые адреса вида $IP_S^i$) во внутренний сегмент (сетевые адреса вида $IP_R^j$).

Проверка включает следующие шаги:

1. Настройка правил фильтрации МЭ в соответствии с проверяемым требованием, в результате чего формируется множество запрещающих $RULE^0 = \{rule_1^0, rule_2^0, \dots\}$ и разрешающих $RULE^1 = \{rule_1^1, rule_2^1, \dots\}$ правил межсетевого экранирования, причем, каждое правило представляет собой упорядоченное множество вида $rule_k^{0/1} = (IP_S^i, IP_R^j)$, где $IP_S^i$ - сетевой адрес отправителя, $IP_R^j$ - сетевой адрес получателя.

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

3. Генерация сетевых пакетов из внешней сегмента сети во внутренний сегмент для всех возможных пар (отправитель, получатель): $packet_k = (IP_S^i, IP_R^j, payload^k)$.

4. Завершение перехвата сетевых пакетов. В результате получаем следующие множества перехваченных пакетов $PACKET^{IN} = \{packet_1^{IN}, packet_2^{IN}, \dots\}$ и $PACKET^{OUT} = \{packet_1^{OUT}, packet_2^{OUT}, \dots\}$, где $packet_k^{IN} = (IP_S^i, IP_R^j, payload^k)$ - сетевые

пакеты, перехваченные во внешнем сегменте, $packet_k^{OUT} = \left(IP_S^i, IP_R^j, payload^k\right)$ - сетевые пакеты, перехваченные во внутреннем сегменте.

5. Экспорт журнала регистрации разрешенных и запрещенных пакетов МЭ. В результате выполнения формируется множества записей о запрещении прохождения $JOUR^0 = \{journal_1^0, journal_2^0, \dots\}$ и разрешении прохождения $JOUR^1 = \{journal_1^1, journal_2^1, \dots\}$ сетевого пакета. Каждая запись имеет вид: $journal_k^{0/1} = \left(IP_S^i, IP_R^j\right)$.

Результатами выполнения тестовой процедуры являются:

1. Конфигурация МЭ – множества $\{rule_i^0\}$ и $\{rule_i^1\}$.
2. Результаты перехвата сетевых пакетов на внешнем и внутреннем интерфейсах МЭ – множества $\{packet_i^{IN}\}$ и $\left\{packet_i^{OUT}\right\}$.
3. Фрагмент журнала регистрации событий МЭ, демонстрирующий результаты фильтрации сетевых пакетов: множества $\{journal_i^0\}$ и $\{journal_i^1\}$.

В качестве критерия принятия положительного решения примем фиксацию соответствия фактических (пакеты на входном интерфейсе МЭ, пакеты на выходном интерфейсе МЭ и фрагмент журнала регистрации событий МЭ) и ожидаемых результатов (правила фильтрации МЭ):

$$\begin{cases} PACKET^{OUT} = RULE^1; \\ PACKET^{IN}/PACKET^{OUT} = RULE^0; \\ PACKET^{OUT} = JOUR^1; \\ PACKET^{IN}/PACKET^{OUT} = JOUR^0. \end{cases}$$

При проведении тестирования могут быть использованы, например, следующие ПС: *nmap, Packet Generator* (генерация сетевых пакетов), *wireshark, tcpdump* (перехват и анализ сетевых пакетов), программный комплекс *«Сканер-ВС»* (генерация, перехват и анализ сетевых пакетов) [3,4].

К МЭ предъявляются также аналогичные требования к механизмам фильтрации на других уровнях модели ISO/OSI. Для канального уровня требование выглядит следующим образом: «МЭ должен обеспечивать фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов». Методика проверки аналогична методике, представленной выше, но в качестве критериев фильтрации используются адреса канального уровня (MAC-адрес). На сетевом уровне проверяется требование по фильтрации с учетом любых значимых полей сетевых пакетов. При проведении испытаний, как правило, внимание следует уделять тестированию механизма

фильтрации с учетом следующих полей пакета сетевого уровня: адрес отправителя, адрес получателя, тип протокола верхнего (транспортного) уровня, время жизни пакета (TTL).

**Проверка механизмов идентификации и аутентификации администраторов**

Целью проверки является определение степени соответствия функциональных возможностей МЭ по идентификации и аутентификации администратора МЭ.

Будем считать, что $A$ - алфавит паролей и идентификаторов администраторов МЭ. Обозначим идентификатор администратора $id \in ID \subseteq A^*$, пароль - $pwd \in PWD \subseteq A^*$. Учетная запись администратора $adm_i \in ADM$ характеризуется следующим кортежем $adm_i = (id_j, pwd_k)$.

Введем оператор корректности учетных данных $\mathrm{F_{AUT}}\colon \mathrm{ADM} \to \{0,1\}$:

$$F_{AUT}(adm) = \begin{cases} 1, \text{ доступ на администрирование получен;} \\ 0, \text{ в противном случае.} \end{cases}$$

Предполагается, что идентификация/аутентификация выполняется с использованием сетевых протоколов с ЭВМ внутреннего сегмента сети. Тогда проверка будет включать следующую последовательность действий:

1. Включение механизма идентификации и аутентификации МЭ и создание множества учетных записей администраторов МЭ $ADM = \{adm_1, adm_2, \dots\}$.
2. Запуск ПС перехвата и анализа сетевых пакетов во внутреннем сегменте сети.
3. Выполнение запросов на идентификацию и проведение аутентификации с использованием различных сочетаний учетных данных: зарегистрированный/незарегистрированный идентификатор, верный/неверный пароль – $try_i = (id_j, pwd_k)$.
4. Генерация сетевых пакетов из внутренней сети во внешнюю (или наоборот), прохождение которых разрешается (запрещается) в соответствии с правилами фильтрации МЭ.
5. Завершение перехвата сетевых пакетов, экспорт журнала регистрации событий МЭ.
6. Анализ на предмет наличия учетных данных, передаваемых в открытом виде.

При выполнении проверки реализации локальной идентификации/аутентификации шаги 2, 5 последовательности действий не выполняются.

Результатами выполнения тестовой процедуры являются:

1. Конфигурация МЭ - множество $ADM$ учетных записей администраторов МЭ.

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

3. Результаты перехвата сетевых пакетов на внешнем и внутреннем интерфейсах МЭ.

4. Фрагмент журнала регистрации событий МЭ, демонстрирующий результаты идентификации и аутентификации

Определим критерии принятия положительного решения:

1. После ввода зарегистрированного идентификатора и пароля пользователю предоставляется доступ к средствам администрирования МЭ: $F_{AUT}(try_i) = 1 \Leftrightarrow try_i \in ADM$.

2. После ввода незарегистрированного идентификатора и/или неверного пароля пользователю отказывается в доступе к средствам администрирования МЭ: $F_{AUT}(try_i) = 0 \Leftrightarrow try_i \notin ADM$.

3. Журнал регистрации событий содержит записи о всех тестовых попытках получения доступа.

4. Попытки поиска идентификационных данных (имя пользователя, пароль) в перехваченных пакетах не дали результатов.

При проведении тестирования механизмов идентификации/аутентификации для перехвата и анализа сетевых пакетов могут быть использованы, например, программы *wireshark, tcpdump,* программный комплекс *«Сканер-ВС»* [3].

**Проверка механизмов контроля целостности**

Проверка состоит в определении степени соответствия функциональных возможностей МЭ по контролю целостности программной и информационной части МЭ.

Пусть $FILE = \{file_1, file_2, \dots, file_n\}$ - множество файлов МЭ (конфигурационные файлы, программные модули). Введем операторы нарушения целостности $F_{MOD}$ и контроля целостности файлов МЭ $F_{INT}$.

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

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

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

$$F_{INT}(file) = \begin{cases} 1, \text{ целостность файла нарушена;} \\ 0, \text{ в противном случае.} \end{cases}$$

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

1. Включение механизма контроля целостности программной и информационной части МЭ и идентификация множества файлов МЭ $FILE = \{file_1, file_2, \dots, file_n\}$.
2. Внесение изменений в файлы МЭ (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 МЭ (создание условий, при которых МЭ осуществляет контроль целостности).
4. Анализ реакции МЭ на нарушение целостности своей программной или информационной части.

Результатами выполнение тестовой процедуры следует считать:

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

В качестве критерия принятия положительного решения примем факт, что обнаружены все факты нарушения целостности:

$$F_{INT}(file_i^{\Delta}) = F_{MOD}(file_i).$$

**Рекомендации по оптимизации процедуры проведения испытаний**

Задача оптимизации процедуры проведения испытаний МЭ может быть сформулирована следующим образом. Пусть $\mathcal{T}: T \times \Sigma \to \mathbb{N}_0$ – время, затрачиваемое экспертами на выполнение оценки соответствия с использованием тестовой процедуры

$t_i \in T$ для МЭ $\Sigma$. Обозначим через отображение $C: R \times \Sigma \to \mathbb{N}_0$ – затраты на проведение тестирования реализации требований $R$ для МЭ $\Sigma$. Тогда задача оптимизации процедуры проведения испытаний МЭ формулируется следующим образом (минимизация времени тестирования МЭ при ограничениях на затраты):

$$\begin{cases} \sum_i \mathcal{T}(t_i, \Sigma) \to min, \\ \sum_i C(r_i, \Sigma) \leq C_{\text{п}}, \end{cases}$$

где $C_{\text{п}}$ – ограничения, накладываемые на затраты.

Наиболее трудоемкой частью испытаний является тестирование подсистемы управления доступом (фильтрации сетевых пакетов) МЭ. Опыт тестирования МЭ позволяет сформулировать ряд рекомендаций, позволяющих сократить эти затраты:

1. ОС тестовых ЭВМ должны загружаться со сменного носителя (CD, USB-накопитель и т. д.) и не требовать для своего функционирования установки на жёсткий диск. Это позволит сократить временные затраты на установку и конфигурирование ОС тестовых ЭВМ.

2. ПС, необходимые для проведения испытаний (например, ПС перехвата и анализа сетевого трафика или http-сервер), должны входить в состав ОС, загружаемой на тестовых ЭВМ.

3. Должна быть предусмотрена программа централизованного управления процессом генерации и анализа сетевых пакетов (программа должна входить в состав ОС, загружаемой на тестовых ЭВМ). Данная программа должна получать на вход правило фильтрации, проверяемое в ходе конкретной проверки, и необходимую информацию о конфигурации испытательного стенда. Программа должна управлять запуском и прекращением работы тестовых ПС (генерации и перехвата сетевых пакетов), собирать необходимую информацию с тестовых ЭВМ (например, список перехваченных пакетов) и выполнять анализа полученных результатов (сравнение фактических результатов с установленными правилами фильтрации). Централизованное управление и сбор информации должен происходить по компьютерным сетям, не входящим в состав внутреннего или внешнего сегментов. В целях минимизации экономических затрат управление и сбор информации может происходить с использованием беспроводных технологий передачи данных.

4. Должны быть предусмотрены средства экспорта результатов испытаний.

Указанные рекомендации позволят сократить время испытаний в части выполнения следующих процедур:

- установка ОС и необходимых ПС на ЭВМ стенда;
- запуск ПС перехвата и анализа сетевых пакетов во внутреннем сегменте сети;
- запуск ПС перехвата и анализа сетевых пакетов во внешнем сегменте сети;
- генерация сетевых пакетов из внешней сегмента во внутренний сегмент сети;
- завершение работы ПС перехвата и анализа сетевых пакетов во внутреннем сегменте сети;
- завершение работы ПС перехвата и анализа сетевых пакетов во внешнем сегменте сети;
- формирование списков пропущенных и запрещенных сетевых пакетов;
- сравнительный анализ списков пропущенных (запрещенных) сетевых пакетов и настроенных правил фильтрации МЭ.

**Выводы**

Предложенный в работе подход к формализации общего подхода и частных методик позволяет упростить автоматизацию испытаний и верификацию безопасности МЭ и компьютерных сетей в защищенном исполнении.

Автоматизация наиболее рутинных шагов (например, синхронизированный запуск ПС перехвата сетевого трафика или генерация сетевых пакетов) позволит повысить качество проводимого тестирования, снизить временные затраты, а также сократить число возможных ошибок тестирования.

Подход может быть рекомендован для проведения разного рода сертификационных испытаний средств защиты информации и аттестации объектов информатизации [5].

**Литература**

1. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности АС и ИВС / И.В.Котенко, М.М.Котухов, А.С. Марков и др. - СПб: ВУС, 2000. – 190 с.

2. Котухов М.М., Марков А.С. Методы дефектоскопии межсетевых экранов // ИБРР-99, 1999. - Часть I. – С. 64.

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

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

5. 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.