Разработка методики испытаний систем обнаружения вторжений в соответствии с положениями новой нормативной базы

Подготовили: студентки МГТУ им. Н. Э. Баумана,

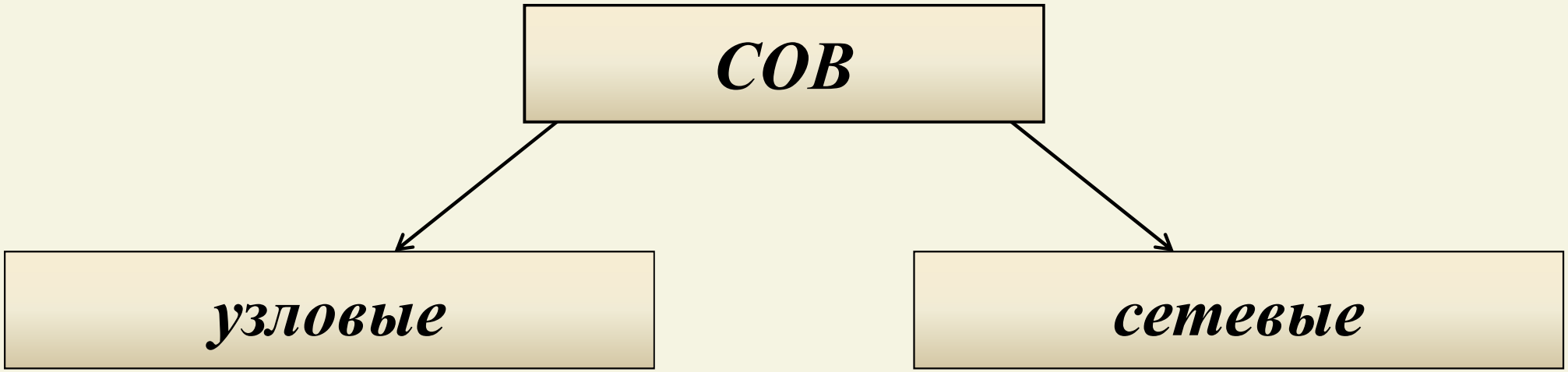
кафедра «Информационная безопасность»

Ларионцева Е. А.

Стельмашук Н. Н.

Введение

Система обнаружения вторжений (СОВ) – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней

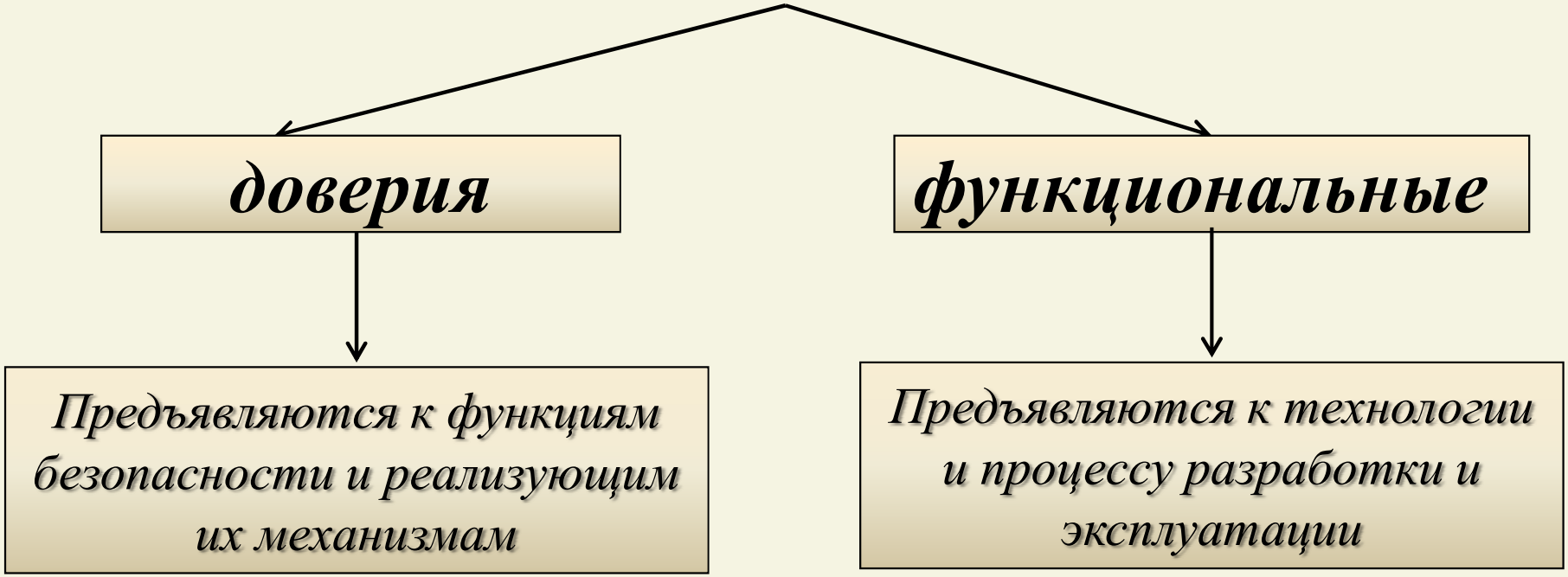


Сертификация СОВ

Основание для сертификации - новый руководящий документ ФСТЭК России, определяющий состав стандартных и специальных функциональных компонентов СОВ, устанавливаемых в соответствие с ГОСТ Р ИСО/МЭК 15408-2, зависящих от типа СОВ и класса защиты.

Методика проведения испытаний СОВ

В соответствии со стандартом «Общие критерии оценки защищённости информационных технологий» (Common Criteria for Information Technology Security Evaluation) существует 2 вида требований безопасности:



Математическое описание методики проведения испытаний СОВ

$F=\{f_1,f_2,\ldots,f_{14}\}$ – множество функциональных требований к объекту оценки Ω

$S=\{s_1, s_2, \ldots, s_7\}$– требования доверия к безопасности объекта оценки Ω

Определим набор параметров.

$E=\{e_1, e_2, \ldots, e_i, \ldots\}$ множество испытаний, при помощи которых выполняется проверка требований

Отображение M: $\Omega \times S \rightarrow E$ - метод составления тестовых испытаний для объекта оценки Ω

Математическое описание методики проведения испытаний СОВ

Методика проведения испытаний СОВ – это кортеж **Θ{Ω, S, E, M, C_1, C_2, T},** где:

Ω - объект оценки**,**

S **–**требований доверия к безопасности**,**

E **–** множество испытаний, проводимых над СОВ,

M **–** метод составления тестовых испытаний,

C_1, C_2– отображения, характеризующие корректность выполняемых проверок и полноту результата.

T **–** множество дополнительных программных/аппаратных средств, используемых для проведения тестовых испытаний.

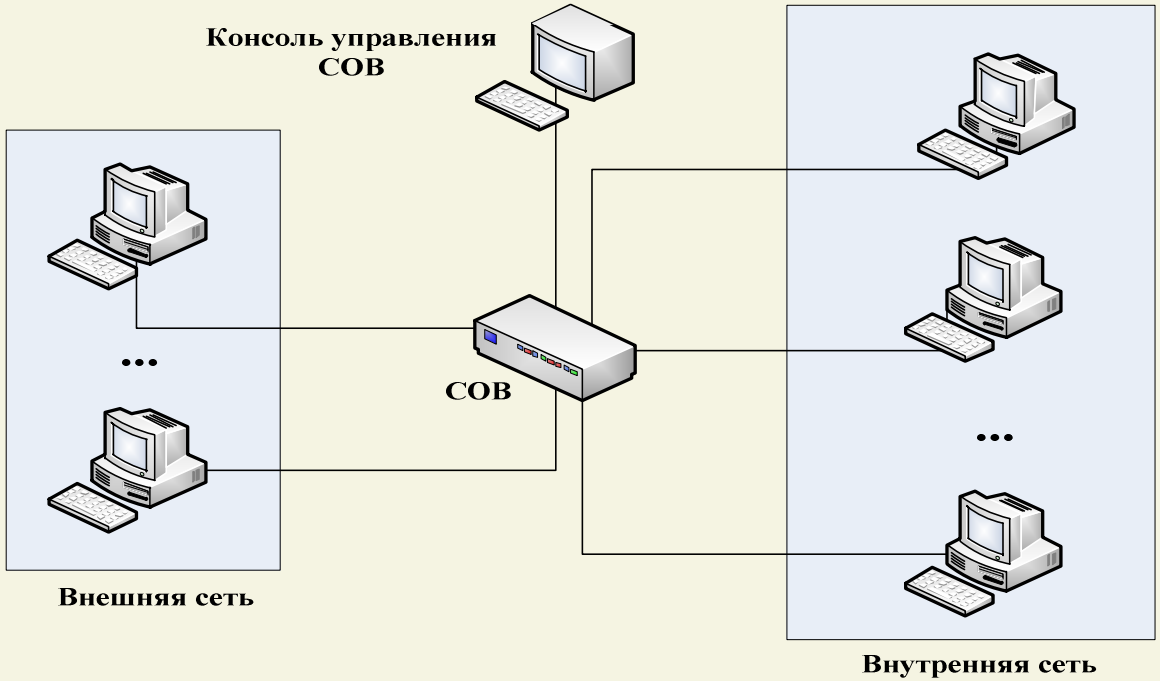
Этапы методики проведения испытаний СОВ

- ✓ **Идентификация объекта испытаний Ω, среды испытаний и планирование тестовых процедур**
- ✓ **Непосредственно выполнение тестовых испытаний над объектом оценки Ω**
- ✓ **Анализ полученных результатов**

Разработка общей и частных методик

Объект испытаний – система обнаружения вторжений уровня узла (расположена на отдельном узле)

Проверка соответствия СОВ требованиям профиля защиты проводится на испытательном стенде

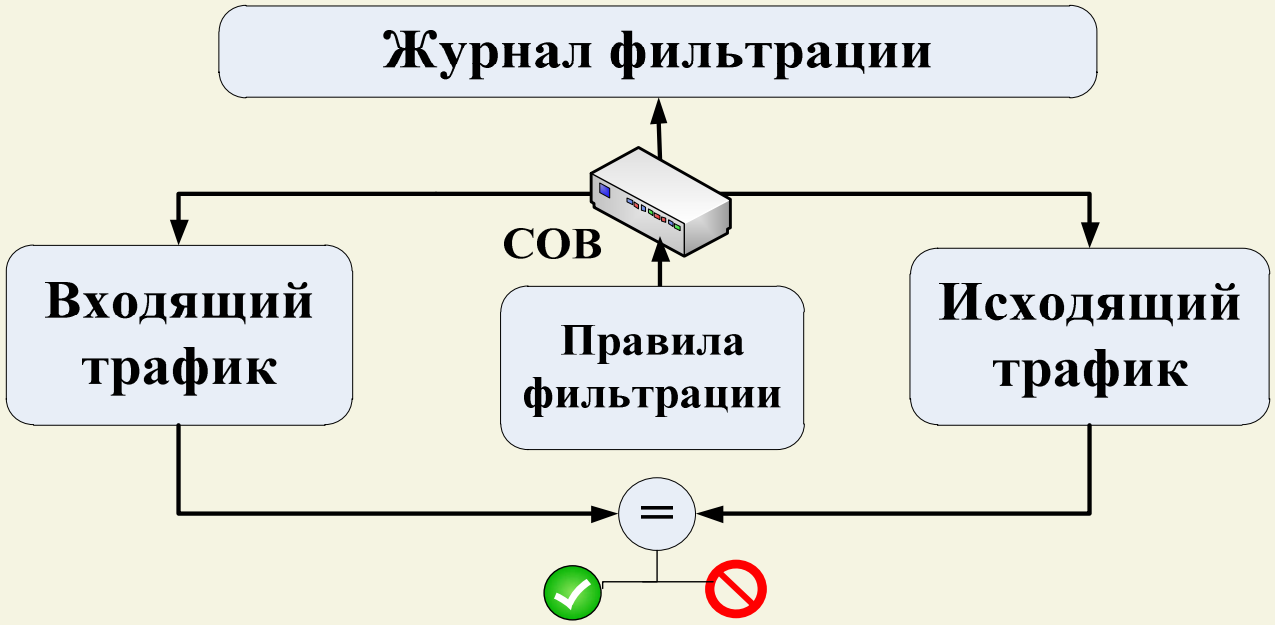


Методика проверки соответствия СОВ некоторым требованиям профиля защиты

1. Проверка базового анализа данных СОВ

Цель :

Определение соответствия СОВ требованиям по реализации средств анализа данных



Методика проверки соответствия СОВ некоторым требованиям профиля защиты

Порядок проведения испытания:

1)Настройка правил обнаружения СОВ: определение набора правил $R=\{R_1,...R_n\}$.

2) Генерация пакетов от IP_s^m к $IP_d^p i$, IP_s^m –адрес отправителя, IP_d^p –получателя.

3) Завершение перехвата сетевых пакетов. Образуются 2 множества:

$A_+ = \{A_{+1}..A_{+k}\}$ – пропущенных и $A_- = \{A_{-1}...A_{-s}\}$ – заблокированных атак.

4) Экспорт журнала регистрации разрешенных и запрещенных пакетов.

Критерий принятия положительного решения:

Зафиксировано соответствие фактических и ожидаемых результатов при тестировании СОВ.

Методика проверки соответствия СОВ некоторым требованиям профиля защиты

2. Проверка методов анализа

Цель :

Определение соответствия СОВ функциональным требованиям по реализации методов анализа данных.

Порядок проведения испытания:

1)Настройка правил реагирования СОВ: определяется набор Rules={$Rule_1$, …$Rule_n$}.

2) Генерация атак из внешней сети во внутреннюю.

3) Экспорт журнала регистрации. Формируется 2 множества записей $J_+ = \{J_{+1}…J_{+k}\}$ – зарегистрированных пропущенных атак и $J_- = \{J_{-1}…J_{-s}\}$ –заблокированных.

Критерий принятия положительного решения:

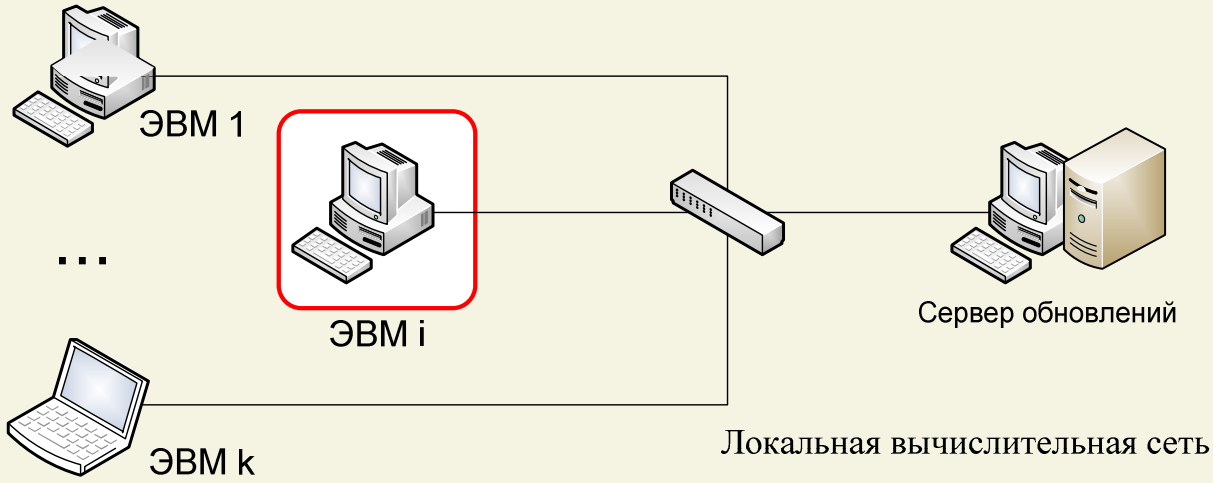
Зафиксировано наличие средств реагирования СОВ при обнаружении вторжений.

Методика проверки соответствия СОВ некоторым требованиям профиля защиты

3. Проверка наличия средств обновления СОВ

Цель :

Определение степени соответствия СОВ функциональным требованиям по наличию средств обновления СОВ.



Критерий принятия положительного решения:

СОВ обладает средствами обновления баз правил.

Методы оптимизации испытаний СОВ

$$\begin{cases} \sum_i \xi(\Omega, \psi_i) \to min \\ \sum_i \sigma(s_i, \Omega) \leq \sigma_0 \end{cases}$$

отображение ξ: $\Omega \times \Psi \to N_o$ – время, затрачиваемое на выполнение проверки ОО,

Ψ – множество действий, необходимых для проведения испытаний,

No – множество натуральных чисел с нулем,

отображение σ: $S \times \Omega \to No$ – затраты на проведение испытаний ОО,

σ_o – ограничения, накладываемые на затраты.

Заключение

Основная проблема:

при проведении тестирования организации сталкиваются с существенным ростом временных и материальных затрат, связанным с увеличением числа действий, необходимых для достижения определенного уровня доверия к разрабатываемой СОВ.

Итоги:

В работе предложены некоторые методические подходы, позволяющие наиболее оптимально проводить трудоемкие испытания и сократить затраты на проведение оценки соответствия СОВ новой нормативной документации ФСТЭК России.

Спасибо за внимание!