В. С. Моисеев, П. И. Тутубалин, Структура и функции автоматизированной системы испытаний средств защиты информации,
Исслед. по информ., 2007, выпуск 12, 149–158

СТРУКТУРА И ФУНКЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ИСПЫТАНИЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В. С. Моисеев, П. И. Тутубалин

В доступной литературе [1-6] говорится о необходимости испытаний средств защиты информации (СЗИ), но не указываются пути реализации этого важного этапа в создании и эксплуатации СЗИ. В работе [7] говорится о необходимости получения информации о защищенности АСУ из протоколов испытаний фирм ее производителей, но не описаны подходы и методики, позволяющие сделать это.

В нашем случае объектами испытания (ОИ) являются СЗИ некоторого информационного ресурса АСУ, которые подвергаются испытаниям на информационную безопасность (ИБ).

Следуя работе [8], под автоматизированной системой испытаний (АСИ) будем понимать человеко-машинный организационно-технический комплекс, предназначенный для обеспечения максимально возможного в данных условиях уровня автоматизации испытательных работ по оценке ИБ.

Отметим, что можно выделить два вида СЗИ: программные и технические. К техническим СЗИ будем относить всевозможные аппаратные и аппаратно-программные комплексы, позволяющие предотвратить утечку и подмену конфиденциальной информации. Их подробный обзор приведен в работе [9]. Построение АСИ технических СЗИ во многом зависит от их типа и является сложной задачей. Далее мы будем рассматривать АСИ программных СЗИ.

В составе АСИ СЗИ можно выделить ряд компонент.

1) Техническое обеспечение – комплекс технических средств, обеспечивающих работу системы и выполнение возложенных на нее функций.

2) Математическое обеспечение – совокупность математических моделей и методов, лежащих в основе логических и вычислительных процессов, сопровождающих выполнение испытательных работ.

3) Программное обеспечение (ПО) – совокупность программ, обеспечивающих целевое использование АСИ СЗИ. Программное обеспечение состоит из общего (ОПО) и специального (СПО).

4) Информационное обеспечение (ИО) – совокупность исходных данных испытаний вместе с программно-аппаратными средствами управления ими.

5) Лингвистическое обеспечение (ЛО) – совокупность используемых формальных языков описания информации и алгоритмов ее обработки в процессе автоматизированных испытаний.

Важной компонентой АСИ СЗИ является персонал системы, который включает в себя администратора системы (АС) и испытателей (ИСЗИ). Структурная схема АСИ СЗИ представлена на рис. 1.

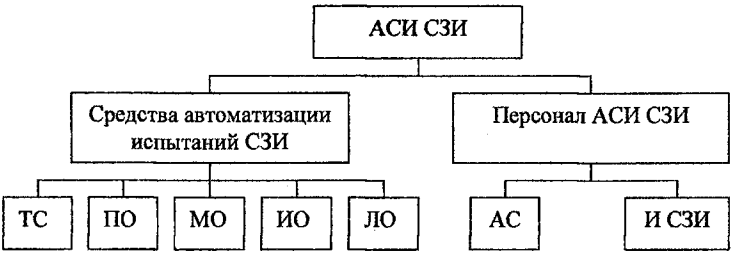

Рис. 1. Структурная схема АСИ СЗИ

Опишем компоненты АСИ СЗИ, представленные на рис. 1.

Техническое обеспечение АСИ СЗИ включает в себя компьютерные стенды, в составе которых используются технические средства формирования и реализации средств нападения на ОИ, а также обработки результатов испытаний. Структура технических средств представлена на рис. 2.

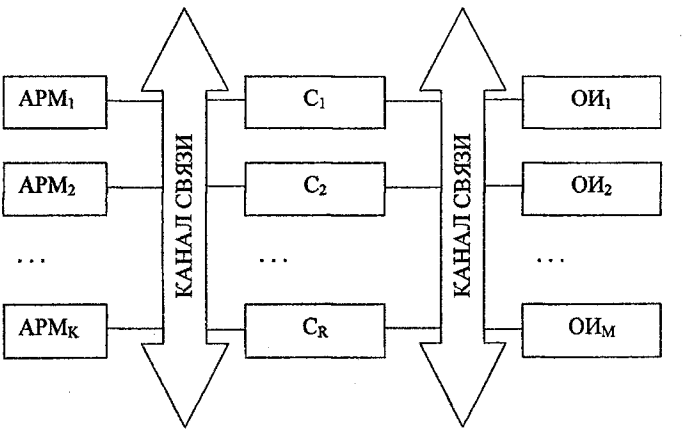

Рис. 2. Структура технических средств АСИ СЗИ

На этом рисунке приняты следующие условные обозначения.

APM_1, APM_2,..., APM_K – автоматизированные рабочие места испытателей СЗИ;

C_1, C_2,..., C_R – серверы АСИ СЗИ;

$ОИ_1$, $ОИ_2$,..., $ОИ_M$ – объекты испытания.

Рассмотрим математическое обеспечение АСИ СЗИ. Будем считать, что АСИ СЗИ работает по схеме независимых испытаний [10].

Пусть событие A – это факт выявления уязвимости тестируемого СЗИ при реализации некоторого модуля формирования атак (МФА).

Пусть n – это количество МФА, реализованных в составе АСИ СЗИ для тестирования ИБ i-го СЗИ рассматриваемой АСУ.

Допустим в n опытах событие A произошло m раз. Предполагается, что число появлений события A распределено по биномиальному закону [10], и вероятность того, что событие A появится ровно m раз в серии из n опытов, имеет вид:

$$P_{m,n} = C_n^m p^m q^{n-m},$$

где p - вероятность реализации события A, а $q = 1 - p$.

После тестирования на ИБ i-го СЗИ АСУ можно вычислить частоту появления события A, которая равна $p^* = \frac{m}{n}$.

Построим доверительный интервал $I_\beta = (p_1, p_2)$, в который частота p^* события A попадает с доверительной вероятностью β. Для этого нужно решить систему уравнений [10]:

$$\sum_{m=k}^{n} C_n^m p^m (1-p)^{n-m} = \frac{\alpha}{2}, \qquad (1)$$

$$\sum_{m=0}^{k} C_n^m p^m (1-p)^{n-m} = \frac{\alpha}{2}, \qquad (2)$$

где $\alpha = 1 - \beta$ и $k = np^*$ – число появлений события A.

Решая уравнения (1) и (2) относительно p, можно найти границы доверительного интервала p_1 и p_2. Отметим, что методы нахождения решения уравнений (1), (2) были подробно описаны в работах [10-13].

Рассмотрим случай, когда $m = 0$, то есть в n опытах событие A зафиксировано не было. В этом случае [10] p_1=0, а p_2 имеет вид:

$$p_2 = 1 - \sqrt[n]{1-\beta}.$$

В работах [10, 11] приведены формулы для расчета значений границ доверительного интервала для точечной оценки вероятности p^*. Если число испытаний сравнительно велико $n > 1000$ или $9 < npq < 100$ и $n < 1000$, тогда можно считать, что частота события p^* есть случайная величина, распределение которой близко к нормальному [10-13]. Ниже приведены формулы, позволяющие найти границы доверительного интервала для нее:

$$p_1 = \frac{p^* + \frac{1}{2}\cdot\frac{t_\beta^2}{n} - t_\beta\sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1+\frac{t_\beta^2}{n}};$$

$$p_2 = \frac{p^* + \frac{1}{2}\cdot\frac{t_\beta^2}{n} + t_\beta\sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1+\frac{t_\beta^2}{n}}; \qquad (3)$$

где $t_\beta = \arg\Phi^*(\frac{1+\beta}{2})$, Φ^* – нормальная функция распределения.

Доверительный интервал для вероятности p будет иметь вид:

$$I_\beta = (p_1, p_2).$$

Поставим задачу определения минимального значения правой границы доверительного интервала p_2 для заданного значения доверительной вероятности β. То есть какова должна быть точность оценки вероятности p при максимально возможном числе опытов n, чтобы верхняя доверительная граница для вероятности события A была равна заданному значению при отсутствии успешных реализаций события A. Решение этой задачи имеет вид [10]:

$$p_2 = 1 - \sqrt[n]{1-\beta}.$$

Построим решающие правила для оценки результатов испытаний. Пусть (p_{1i}, p_{2i}) – доверительный интервал для статистической вероятности $p_i^* = \frac{m_i}{n_i}$ нарушения ИБ i-го СЗИ АСУ, $i = \overline{1,R}$. Взаимное расположение заданного значения вероятности P_i и доверительного интервала (p_{1i}, p_{2i}) представлено на рис. 3.

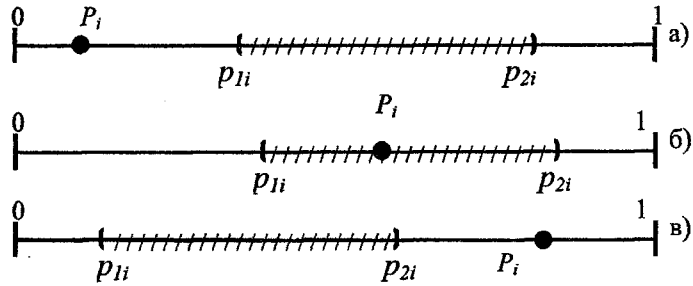

Рис. 3

Случай а) соответствует ситуации, когда значение вероятности нарушения ИБ, которое располагается в интервале (p_{1i}, p_{2i}), больше допустимого значения этой вероятности P_i. Здесь можно сделать вывод о том, что имеющиеся СЗИ не выполняют требования по ИБ для i-го элемента.

В случае б) однозначного вывода о стойкости имеющихся СЗИ сделать нельзя, так как значение вероятности нарушения ИБ, которое располагается в интервале (p_{1i}, p_{2i}), может быть как больше, так и меньше допустимого значения этой вероятности P_i.

Случай в) соответствует ситуации, при которой заданное требование по обеспечению ИБ выполняется. При этом, чем больше P_i отличается от величины p_{2i}, тем выше стойкость СЗИ к имеющимся средствам нападения.

Таким образом, имеем следующее решающее правило для оценки i-го СЗИ АСУ: «Если выполняется одно из неравенств $P_i < p_{1i}$ или $p_{1i} \le P_i \le p_{2i}$, то требования по ИБ i-го СЗИ АСУ не выполняются. При выполнении условия $P_i > p_{2i}$ i-е СЗИ обеспечивают ИБ i-го элемента АСУ с доверительной вероятностью равной β».

Построим аналогичные решающие правила (см. рис. 4) для случая отсутствия успешных реализаций нарушения ИБ АСУ, то есть когда $(p_{1i}, p_{2i}) = (0, p_{2i})$.

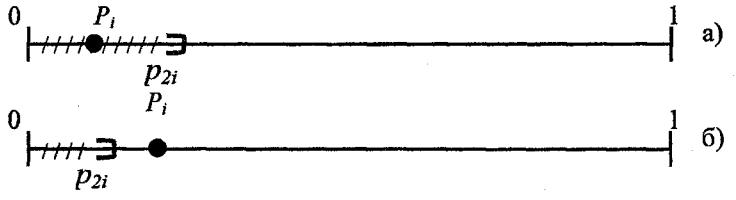

Рис. 4

В случае а) однозначного вывода о стойкости имеющихся СЗИ сделать нельзя, так как значение вероятности нарушения ИБ, которое располагается в интервале $(0, p_{2i})$, может быть и больше и меньше допустимого значения этой вероятности P_i.

Случай б) соответствует ситуации, при которой заданное требование по обеспечению ИБ выполняется.

Отметим, что если предложенные решающие правила дали отрицательные или неоднозначные выводы по выполнению требований ИБ, то производится пересмотр состава применяемых средств защиты, и испытания повторяются до удовлетворения имеющихся требований по ИБ рассматриваемого СЗИ АСУ.

Рассмотрим математические методы и алгоритмы обработки результатов работы АСИ СЗИ.

Допустим, при тестировании некоторого СЗИ АСУ S найдено множество U_S уязвимостей. Рассмотрим множество F видов компонент информации, обрабатываемой в АСУ: конфиденциальность (К), целостность (Ц) и доступность (Д). Опишем отношение взаимосвязи множеств F и U_S в виде:

$$R_S \subseteq U_S \times F, \tag{4}$$

где $F = \{K, Ц, Д\}$. Отношение (4) представляет собой бинарное отношение и может быть описано булевской матрицей вида:

$$C = [c_{ij}]_{|U(S)|\times|F|}. \tag{5}$$

Величины $M_S = |U_S|$ и $|F|$=3 определяют мощности множеств U_S и F соответственно, и первая из них является переменной.

Примем следующие условные обозначения: U_S^K - множество уязвимостей, реализация которых может привести к нарушению конфиденциальности информации, циркулирующей через тестируемое СЗИ АСУ; $U_S^Ц$ - множество уязвимостей, влияющих на целостность информации, циркулирующей через тестируемое СЗИ АСУ; $U_S^Д$ - множество уязвимостей, влияющих на доступность информации, циркулирующей через тестируемое СЗИ АСУ.

Следовательно, теперь с использованием матрицы (5) можно определить мощности каждого из множеств U_S^K, $U_S^Ц$, $U_S^Д$:

$$M_S^K = \sum_{i=1}^{M_S} c_{i1}, \quad M_S^Ц = \sum_{i=1}^{M_S} c_{i2}, \quad M_S^Д = \sum_{i=1}^{M_S} c_{i3}.$$

Далее определим точечные оценки вероятностей нарушения ИБ компонент конфиденциальности, целостности и доступности:

$$p^*_{S|K} = \frac{M_S^K}{n}, \; p^*_{S|Ц} = \frac{M_S^Ц}{n}, \; p^*_{S|Д} = \frac{M_S^Д}{n}. \tag{6}$$

Аналогично, определим точечную оценку вероятности нарушения ИБ тестируемого СЗИ АСУ:

$$p_S^* = \frac{M_S}{n}. \tag{7}$$

Далее, для каждой из найденных по формулам (6), (7) вероятностей построим доверительные интервалы с использованием формул (1), (2) или (3) в зависимости от значения параметра *npq* и количества испытаний n.

Определим интегральные характеристики защищенности компонент конфиденциальности, целостности и доступности рассматриваемой АСУ и всей системы в целом. Так как преодоление хотя бы одного из СЗИ АСУ

ведет к нарушению ИБ АСУ, можно сформировать интегральные оценки вероятностей нарушения ИБ конфиденциальности, целостности и доступности АСУ:

$$p^*_{инт|К} = 1 - \prod_{i=1}^{n}\left(1 - p^*_{i|К}\right)$$

$$p^*_{инт|Ц} = 1 - \prod_{i=1}^{n}\left(1 - p^*_{i|Ц}\right), \qquad (8)$$

$$p^*_{инт|Д} = 1 - \prod_{i=1}^{n}\left(1 - p^*_{i|Д}\right)$$

где $p^*_{i|К}$, $p^*_{i|Ц}$, $p^*_{i|Д}$ - оценки вероятностей нарушения ИБ конфиденциальности, целостности и доступности i-го СЗИ АСУ (6).

Определим оценку вероятности нарушения ИБ АСУ по аналогии с формулой (8) в виде:

$$p^*_{инт|АСУ} = 1 - \left(1 - p^*_{инт|К}\right)\left(1 - p^*_{инт|Ц}\right)\left(1 - p^*_{инт|Д}\right). \qquad (9)$$

По аналогии с нахождением доверительных интервалов для компонент конфиденциальности, целостности и доступности СЗИ АСУ, построим для каждой из найденных по формулам (8), (9) вероятностей доверительные интервалы.

Используя методику, описанную выше, и сформированные на этапе проектирования АСУ требования [14], предъявляемые как к отдельным СЗИ так и к тестируемой АСУ, можно сделать вывод о достаточной либо недостаточной степени защищенности рассматриваемой системы.

Отметим, что комплекс программ организации атак можно организовать с использованием современных сканеров уязвимостей [15]. В данной работе предлагается использовать сетевой сканер Nessus [16]. Ниже приведены его основные возможности и характеристики.

1) Модульная архитектура, в которой каждый отдельный тест выполнен в виде подключаемого модуля.

2) Клиент серверная архитектура.

3) Гибкость, которая определяется возможностью испытывать одновременно неограниченное количество объектов.

4) Адаптивность проводимых тестов. Все тесты, проводимые Nessus, координируются между собой, это позволяет ускорить процесс испытания за счет исключения тестов, которые приведут к заведомо отрицательному результату с точки зрения возможных уязвимостей в ИБ.

5) Многорежимность функционирования включает в себя специальные режимы: безопасный – режим, который не может нанести вред объекту испытания, небезопасный – режим, который может нанести вред объекту испытания, вызвав отказ в обслуживании сетевых сервисов, потерю и изменение жизненно важной для тестируемого объекта информации.

6) Возможность тестирования объектов, оснащенных средствами шифрования передаваемой информации с поддержкой протоколов SSL, HTTPS, SMTPS, IMAPS и других.

Пример обработки результатов испытаний.

Рассмотрим макетный образец АСИ СЗИ, который основан на использовании сканера безопасности Nessus и программы обработки результатов. Его структурная схема представлен на рис. 5.

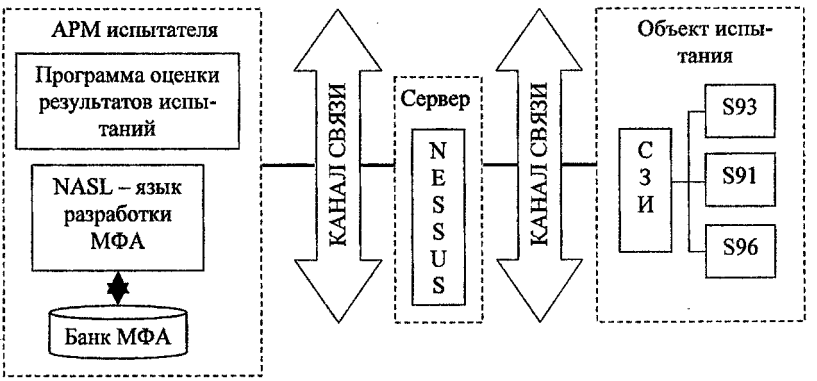

Рис. 5

Рассмотрим в качестве ОИ СЗИ группу серверов $S91$, $S93$, $S96$, работающих под управлением ОС Windows. Серверы работают под управлением ОС Windows, поэтому можно, использовать не весь набор тестов сканера безопасности Nessus, а только лишь те, которые предназначены для ОС Windows. С учетом сказанного для испытаний на ИБ было выбрано 1627 тестов. Доверительную вероятность примем равной 0,95.

Пусть заказчиком были сформированы следующие допустимые вероятности нарушения ИБ серверов АСУ и всей системы в целом, которые сведены в табл. 1.

Таблица 1.

$p_{инт\|АСУ}$	0,1		
$p_{инт\|К}$	0,05		
$p_{инт\|Ц}$	0,05		
$p_{инт\|Д}$	0,05		
Сервер	S96	S91	S93
$p_К$	0,005	0,01	0,01
$p_Ц$	0.005	0.01	0.01
$p_Д$	0.005	0.01	0.01

По окончании работы Nessus сформировал отчет, изучив который испытатель формирует таблицу, содержащую количество найденных уяз-

вимостей для каждого из серверов, и разбил их по угрозе нарушения конфиденциальности, целостности и доступности информации (табл. 2).

Таблица 2.

Сервер	S91	S93	S96
Всего	1	0	1
К	1	0	1
Ц	1	0	1
Д	0	0	0

С использованием методики, описанной выше, были найдены точечные оценки и доверительные интервалы для исходных данных табл. 2. Результат представлен в табл. 3.

Таблица 3.

Сервер	S91	S93	S96
$p^*_К$	0.0006146281	0	0.0006146281
$I^К_\beta$	(0.0006136303; 0.0006156276)	(0;0.0018396)	(0.0006136303; 0.0006156276)
$p^*_Ц$	0.0006146281	0	0.0006146281
$I^Ц_\beta$	(0.0006136303; 0.0006156276)	(0;0.0018396)	(0.0006136303; 0.0006156276)
$p^*_Д$	0	0	
$I^Д_\beta$	(0;0.0018396)	(0;0.0018396)	(0;0.0018396)

Определим интегральные точечные оценки компонент конфиденциальности, целостности, доступности и всей системы в целом с применением формул (8), (9). Результат приведен в табл. 4.

Таблица 4.

$p^*_{инт\|АСУ}$	0.0024563
$I^{АСУ}_{инт\|\beta}$	(0.0024508146; 0.0024617976)
$p^*_{инт\|К}$	0.0012289
$I^К_{инт\|\beta}$	(0.0012265939; 0.0012312104)
$p^*_{инт\|Ц}$	0.0012289
$I^Ц_{инт\|\beta}$	(0.0012265939; 0.0012312104)
$p^*_{инт\|Д}$	0
$I^Д_{инт\|\beta}$	(0;0.0018396)

Сравнив требования по ИБ, представленные в табл. 1, и доверительные интервалы, полученные в табл. 3 и 4, с использованием решающих правил, описанных выше, можно сделать заключение о том, что СЗИ тес-

тируемых серверов и система в целом удовлетворяют требованиям заказчика.

Таким образом, в результате испытаний получено подтверждение требуемого уровня ИБ СЗИ серверов рассматриваемой системы.

Литература

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

2. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М., 1992.

3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн.1. – М.: Энергоатомиздат, 1994.

4. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. Ч.1. – СПб.: Мир и семья-95, 1997.

5. Воробьев А.А. Проблемные вопросы анализа защищенности автоматизированных систем // «Актуальные проблемы информационного противоборства», сборник статей. – М.: МАКПБ, 1999. – С. 204-212

6. Воробьев А.А. Методика испытаний автоматизированных систем военного назначения на соответствие требованиям по защищенности от несанкционированного доступа // Отчет о научно-иссл. работе. Разработка временных технических условий и методик сертификационных испытаний технических, программных средств и автоматизированных систем по требованиям безопасности информации (промежуточный). Шифр – "Билетер-СП". – М., 1998.

7. Мельников Ю.Н., Готовский М.Ю. Выбор комплекса мер защиты информации на основе критерия «эффективность–стоимость» // Приборы и системы управления. – 1998. – №11. – С. 11-13.

8. Адгамов Р.И., Берхеев М.М., Заляев И.А. и др. Автоматизированные испытания в авиастроении. – М.: Машиностроение, 1989.

9. Гинатуллин И.А., Зиновьев П.А., Моисеев В.С., Иванов К.В., Тутубалин П.И. Обзор методов и средств защиты информации. – ШИФР ПМ-12-СМ-6. – Институт проблем информатики АН РТ. – Казань, 2005.

10. Вентцель Е.С. Теория вероятностей. – М.: Высшая школа, 2002.

11. Дунин-Барковский И.В., Смирнов Н.В. Теория вероятностей и математическая статистика в технике. – М.: Изд. технико-теорет.лит., 1955.

12. Манита А.Д. Теория вероятностей и математическая статистика. – М.: Издательский отдел УНЦ ДО Московского университета, 2001.

13. Феллер В. Введение в теорию вероятностей и её приложения. Т.1. – М.: Мир, 1964.

14. Моисеев В.С., Дятчин В.В., Тутубалин П.И. Расчет вероятностных характеристик информационной безопасности разрабатываемых автоматизированных систем // Тез. докл. 3-й междунар. научно-практ. конф. "Инфокоммуникационные технологии глобального инф. общества". – Казань, 2005. – С. 113-114.

15. Марков А., Ермолаев С. Инструментальные средства аттестации программных ресурсов объектов информатизации // Information Security. – 2004. – №4. – С. 4-17.

16. Документация по настройке и эксплуатации сетевого сканера безопасности Nessus. http://www.nessus.org