УДК 004.56 doi: 10.26102/2310-6018/2019.24.1.036

В.Л. Токарев, А.А. Сычугов

МЕТОД АУДИТА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

ФГБОУ ВО «Тульский государственный университет»
Тула, Россия

Проведен анализ существующей в настоящее время нормативной базы и методик анализа защищенности информационных ресурсов. Отмечено, что в основе методик лежит использование технических методов анализа, которые предполагают применение как активного, так и пассивного тестирования системы защиты информации. Еще одним существующим вариантом решения данной задачи является применение экспертных оценок. Однако, оба подхода являются трудоемкими и, зачастую, субъективными. На основе теории нечетких множеств предложена математическая модель аудита защищенности автоматизированных систем, на основании которой предложен соответствующий метод. Рассмотрены нечеткие модели как инструмент для проведения аудита автоматизированных систем, обрабатывающих конфиденциальную информацию. В качестве примера использования предложенного метода рассматривается оценка одного из аспектов информационной безопасности - защищенность доступа к конфиденциальной информации в автоматизированной системе. Предлагаемый метод позволит эффективно использовать полученные оценки для решения задачи обеспечения безопасности информации в автоматизированных системах. Основным преимуществом метода является то, что он не требует проведения сложных процедур тестирования, расчета вероятностей, привлечения и подбора экспертов и др. и может быть использован для оценивания большинства различных аспектов информационной безопасности.

Ключевые слова: информационная безопасность, защищенность доступа, оценивание, нечеткие множества

Введение

Типовая методика [1,2] анализа защищенности информационных ресурсов предприятия включает: изучение исходных данных (организационная структура и функциональная схема автоматизированной системы, обрабатывающей конфиденциальную информацию, структура используемого программного обеспечения, наличие и характер взаимодействия с другими автоматизированными системами и др.); оценивание рисков, связанных с осуществлением угроз безопасности в отношении информационных ресурсов; анализ политики безопасности предприятия и организационно-распорядительной документации по обеспечению информационной безопасности и оценку их соответствия требованиям существующих нормативных документов; анализ конфигурационных файлов маршрутизаторов и прокси-серверов, почтовых

и DNS-серверов; сканирование внешних сетевых адресов локальной сети, внутренних ресурсов локальной сети; анализ конфигурации серверов и рабочих станций с помощью специализированных средств.

Обобщая перечисленное, можно заметить, что в основе указанной методики лежит использование технических методов анализа, которые предполагают применение как активного, так и пассивного тестирования системы защиты информации [3,4]. Активное тестирование заключается в эмуляции действий потенциального злоумышленника, а пассивное тестирование предполагает анализ конфигурации операционных систем и приложений по соответствующим шаблонам. Тестирование может производиться вручную или с использованием специализированных программных средств. В любом случае, это трудоемкий процесс, и он не всегда возможен в реальных условиях по разным причинам.

Альтернативным подходом к оцениванию защищенности информационных ресурсов является использование метода экспертных оценок. В его основе лежит понятие профиля защиты стандарта ISO/IEC 15408 [5]. Но проблема в том, что формально описать вероятности отдельных угроз, атак, эффективности отдельных мер безопасности очень сложно из-за недостатка требуемой информации. Использование таких вспомогательных мер, как анкетирование субъектов отношений [6], построение графа, вершинами которого являются модули защиты и защищаемые объекты, а ребрами – возможные пути продвижения нарушителя [7], уясняют задачу, но не упрощают ее решение.

Материалы и методы

Для снижения сложности указанной задачи, без потери объективности получаемых оценок, предлагается использовать для оценивания защищенности информационных ресурсов нечеткие модели реляционного типа [8]. Предлагаемый метод основан на следующих утверждениях.

Утверждение 1. Защищенность автоматизированной системы, как информационного ресурса, зависит от выполнения требований к защите, предусмотренных современными стандартами [1]. При этом можно выделить следующие три уровня защищенности:

- высокий уровень обеспечивается выполнением полностью всех предусмотренных требований;
- частичная защищенность обеспечивается в случае не выполнения хотя бы одного требования или выполнения хотя бы одного требования частично (не полностью);
- полная незащищенность определяется в случае невыполнения всех требований, предусмотренных стандартами.

Пусть $X = \{x_1, x_2 ... x_L\}$ - полный конечный набор требований, безусловное выполнение которого обеспечит высокий уровень защищенности; $y \in [0...1]$ - величина, характеризующая уровень защищенности: $y = 1$ - высокий уровень защищенности; $y = 0$ - полностью незащищенная система. Очевидно, что уровень защищенности есть величина непостоянная, то есть справедливо: $y = f(t, X_\tau)$, где X_τ - некоторый набор требований, выполняемых в текущий момент времени $t = \tau$.

Из утверждения 1 с учетом введенных обозначений следует, что основой оценивания защищенности может быть отношение:

$$R : A(x) \to B(y) \quad (1)$$

где $A(x)$ - множество вариантов совокупностей выполненных требований X_i по защите информационного ресурса, $B(y)$ - вектор значений защищенности, определенных на отрезке [0,…,1], каждое из которых соответствует одному варианту совокупностей выполненных требований X_i.

На основании утверждения 1 задачу оценивания защищенности автоматизированной системы формально можно представить следующим образом.

$$\Pi(X_\tau, t) \to y(t) \quad (2)$$

где $\Pi(X_\tau, t)$ – оператор выполнения некоторой совокупности требований X_τ в рассматриваемый интервал времени $t = \tau$.

Утверждение 2. Поскольку ни полнота выполнения требований, ни уровень защищенности не могут быть оценены в четких количественных шкалах (абсолютных, относительных) то отношение $R : A(x) \to B(y)$ может быть нечетким, в котором

$x = (x_1, x_2, \ldots, x_n)$ – вектор нечетких входных переменных, совокупностей выполненных требований $x_i \in X$;

y – нечеткая выходная переменная, принимающая значения оценки защищенности, $y \in Y$;

$A=\{A_{ij}, \ i=1,...,n; \ \ j=1,...,m\}$ - множество j-х термов i-й лингвистической переменной «ОЦЕНКА ВЫПОЛНИМОСТИ ТРЕБОВАНИЙ В РАССМАТРИВАЕМЫЙ ИНТЕРВАЛ ВРЕМЕНИ», определенных на X с функциями принадлежности $\mu_{A_{ij}}(x_i) \in [0,....1]$ для $i=1,...,n$;

B = $(b_1, b_2, \ldots, b_m)$- множество термов лингвистической переменной «ОЦЕНКА ЗАЩИЩЕННОСТИ В РАССМАТРИВАЕМЫЙ ИНТЕРВАЛ

ВРЕМЕНИ», определенных на Y с функциями принадлежности $\mu_{b_j}(y) \in [0,....1]$ для $j=1,...,m$.

Из утверждения 2 следует, что нечеткое отношение $\tilde{R}_i$ i для одного заключения b_i можно представить в виде:

$$\tilde{R}_i = \underset{j=1}{\overset{m}{\times}} A_{ij} \to b_i, \tag{3}$$

где «×» - символ декартова произведения.

В целом нечеткое отношение R может быть представлено объединением $R = \bigcup_{i=1}^{N} \tilde{R}_i$ нечетких отношений $\tilde{R}_i$ или:

$$R = \bigcup_{i=1}^{N} \left(\underset{j=1}{\overset{m}{\times}} A_{ij} \to b_i \right) \tag{4}$$

Такое отношение можно представить как модель процедуры оценивания защищенности или как базу правил отображения $\tilde{A} \to \tilde{B}$, в котором

$$\tilde{A} = \bigcup_{i=1}^{N} \left(\underset{j=1}{\overset{m}{\times}} A_{ij} \right); \quad \tilde{B} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix}. \tag{5}$$

Наличие такой модели позволяет получить нечеткое множества B по результатам измерения (оценки) A выполнения множества требований $x \in X$ в рассматриваемый интервал времени $t = \tau$:

$$B = A \circ R = \bigcup_{i=1}^{N} \left(\left(\underset{j=1}{\overset{m}{\times}} A_{ij} \right) \circ \left(\left(\underset{j=1}{\overset{m}{\times}} A_{ij} \right) \to b_i \right) \right), \tag{6}$$

где символ «о» означает операцию композиции нечеткого множества A и нечеткого отношения R, результатом которого будет

$$\mu_B(y) = \sup_{x \in X} \{ min[\mu_A(x), \mu_R(x,y)] \} \tag{7}$$

На основе предложенной математической модели можно предложить следующий метод оценки защищенности автоматизированной системы.

Шаг А. Определение модели $\tilde{R}$ в виде базы правил (4).

Для этого: а) определяются категории (группы) требований $\{x_i\}$ к мерам и средствам защиты информационного ресурса; б) затем

определяются совокупности (подгруппы) требований $\{x_{ij}\}$, реализующие каждую отдельную i-ю группу требований и соответствующие переменные $x_{ij} \in X$; в) определяется необходимое количество m уровней защищенности.

Шаг Б. Выполнение фаззификация полученных переменных: получение функций принадлежности нечетких множеств A_{ij} на множестве значений переменных X и нечетких множеств b_i на множестве значений переменных Y. Примером результата выполнения этой процедуры могут быть функции принадлежности нечетких множеств A_{ij} и b_i, графическое представление которых приведено на Рисунках 1 и 2.

Значения базовых переменных x и y представлены в шкале [0,0;….;0,1]. Термы (нечеткие множества) входных лингвистических переменных обозначены как: ОН –«очень низкое значение»; Н–«низкое значение»; С–«среднее значение»; В–«высокое значение». Соответствующие функции принадлежности имеют трапецеидальную форму.

Термы выходных лингвистических переменных обозначены как: b_0 - «отсутствие защищенности»; b_{15} - «высокая защищенность», остальные $b_1, b_2, \cdots b_{13}, b_{14}$ соответствуют промежуточным значениям защищенности информационного ресурса. Соответствующие функции принадлежности имеют треугольную форму.

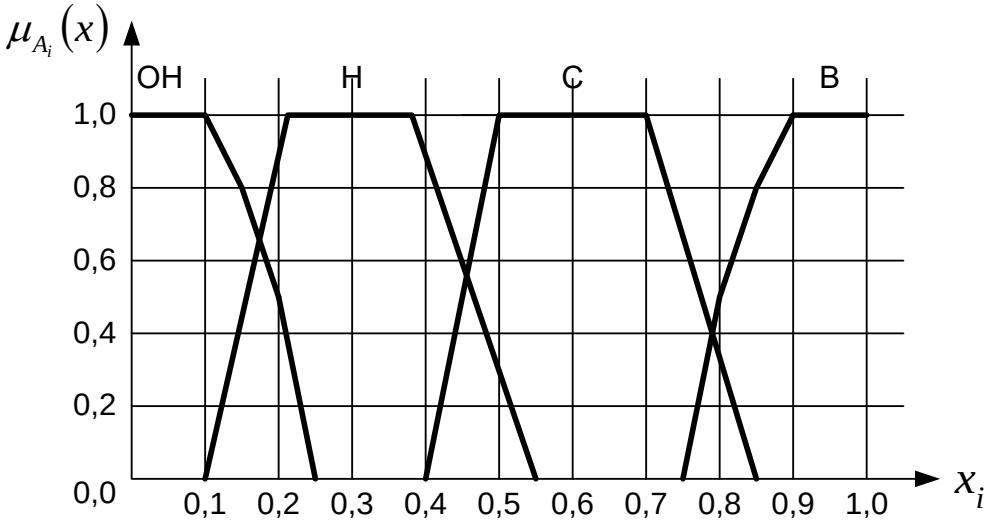

Рисунок 1 – Нечеткие множества входных лингвистических переменных

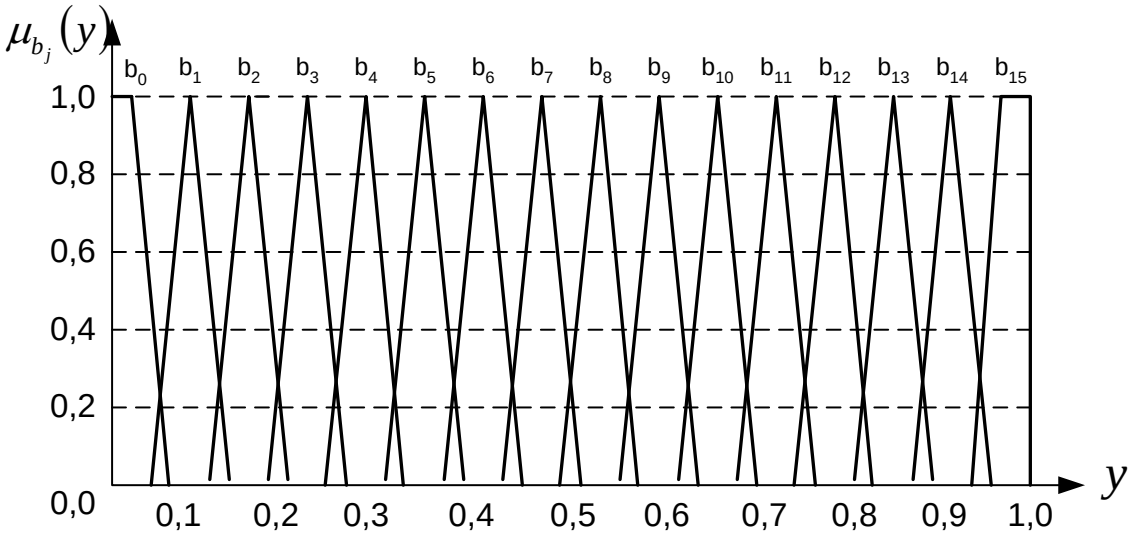

Рисунок 2 – Нечеткие множества выходной лингвистической переменной

Шаг В. После этого определяются, исходя из утверждения 1, отношения (3) полученных нечетких множеств, на основе которых выстраивается база правил – модель оценивания защищенности (2).

Количество m правил (3), отражающих отношения $\tilde{R}_i$ равно количеству выходных нечетких множеств $b_i \subseteq B$. Общий вид получаемой модели $\tilde{R}$:

$$\begin{aligned} &1.\,(x_1 \in A_{11}) \wedge (x_2 \in A_{12}) \wedge \cdots \wedge (x_n \in A_{1n}) \to b_0 \\ &2.\,(x_1 \in A_{11}) \wedge (x_2 \in A_{12}) \wedge \cdots \wedge (x_n \in A_{1n}) \to b_1 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &m.\,(x_1 \in A_{11}) \wedge (x_2 \in A_{12}) \wedge \cdots \wedge (x_n \in A_{1n}) \to b_{m-1} \end{aligned} \qquad (8)$$

Такую модель удобно для программной реализации представить в виде $m \times n$-матрицы, в которой m - число правил, n – число рассматриваемых категорий (групп) требований.

Шаг Г. Получение нечеткого множества $\hat{b}$ и значения функции принадлежности $\mu_B(y)$, используя выражения (7) . Этот шаг выполняется по следующему алгоритму.

1. Определяются значения переменных $x_{ij} \in X$ для каждой группы требований, как отношения числа выполняемой требований конкретной (одной из девяти) группы к общему числу требований данной группы.

2. Выполняется фаззификация полученных значений получением значений $\mu_{\tilde{A}'_{ij}}(x_i)$ и образуя предпосылки $\underset{j=1}{\overset{m}{\times}} \tilde{A}'_{ij}$ для каждого правила (8).

3. Определяется степень истинности каждой предпосылки каждого правила

$$a_j = min\left\{ \underset{j=1}{\overset{m}{\times}} \tilde{A}'_{ij}, \quad i = 1,\ldots,N \right\} \qquad (9)$$

4. Определяется степень истинности заключения по каждому правилу

$$\mu_{\hat{b}_j}(y) = min\left\{\alpha_j, \mu_{\tilde{R}}(x,y)\right\}, \quad j = 1,\ldots,m \qquad (10)$$

5. Выполняется аккумулирование полученных значений $\mu_{\hat{b}_j}(y)$ по всем правилам:

$$\mu_{\tilde{B}}(y) = \sup_{x \in X} \left\{\mu_{\tilde{B}'_j}(y), \quad j = 1,\ldots,m\right\} \qquad (11)$$

Шаг Д. Выполняется дефаззификация полученной функции принадлежности $\mu_{\tilde{B}}(y)$

$$y' = \frac{\sum_{p=1}^{q} y_p \mu_{\tilde{B}'}(y)}{\sum_{p=1}^{q} \mu_{\tilde{B}'}(y)}, \qquad (12)$$

где q – число элементов y_p в области Y, размеченной для вычисления «центроида»; y' - проекция на ось выходной переменной центра области.

Результаты и обсуждение

В качестве примера использования предложенного метода рассматривается оценка одного из аспектов информационной безопасности - защищенность доступа к конфиденциальной информации в автоматизированной системе.

А. Выполнение требований к обеспечению защищенности доступа к конфиденциальной информации представлено в виде 9 групп (n=9), которые представляют базовые переменные: x_1 - выполнение правил контроля доступа; x_2 - контроль в отношении доступа пользователей; x_3 – выполнение своих обязанностей пользователями; x_4 - контроль сетевого доступа; x_5 - контроль доступа к операционной системе; x_6 – технические требования; x_7 - контроль доступа к приложениям; x_8 - мониторинг доступа

и использования системы; x_9 - контроль работы с мобильными устройствами и работы в дистанционном режиме.

Б. Фаззификация предпосылок осуществлена с помощью функций принадлежности

$$\mu_{Aij}(x_i),\ j=1,2,...9;\quad A_i=OH,H,C,B,$$

Фаззификация заключений осуществлена с помощью функций принадлежности $\mu_{b_i}(y),\ i=0,1,2,...,15$ выходных лингвистических переменных (Рисунок 2).

В. База правил представлена в виде (16×(9+1)) – матрицы.

Г. Заключение *y* о защищенности ресурса с помощью полученной базы правил определено по следующему алгоритму.

Алгоритм оценивания защищенности

1-й шаг. Выполнение требований каждой из указанных групп предлагается оценивать степенью выполнения соответствующих мероприятий (организационных и технических). Для этого каждой группе x_i ставится в соответствии определенная (конечная) совокупность мероприятий. Перечень мероприятий определяется исходя из конкретных условий функционирования защищаемой системы.

Определенный авторами в процессе проведения эксперимента перечень, насчитывающей около 100 мероприятий, для сокращения изложения, в данной статье не приводится.

2-й шаг. Строится база правил $\bigcup_{i=1}^{n} R_i$, предварительно упорядочив требования по степени возрастания важности их выполнения с точки зрения защищенности информационных ресурсов конкретной автоматизированной системы следующим образом (для примера): $x_1 \to x_9$.

Каждое правило R_i принимает вид (3) при n=9. А базу правил $\bigcup_{i=1}^{m} R_i$ можно представить, учитывая, что m=16, в виде 16×10 - матрицы (Рисунок 3), в которой первый столбец содержит номера правил, со второго по десятый столбцы содержат имена нечетких множеств A_{ij}, а в одиннадцатом столбце – обозначения нечетких множеств b_i).

Для примера рассмотрена одна из групп требований - пятая «контроль доступа к операционной системе», содержащую шесть подгрупп.

1. На множестве сформированных входных переменных X определено множество лингвистических термов A_5' с функциями принадлежности $\mu_{A_{5k}}(x_j)$ (Рисунок 1), считая что полностью выполненными оказались

только следующее подмножество требований (номера приведены их сформированного авторами перечня):

$$\left\{ \begin{array}{l} x_{51.3}, x_{52.1}, x_{52.3}, x_{52.4}, x_{52.8}, x_{53.1}, x_{53.2}, x_{54.1}, x_{54.2}, x_{54.3}, x_{54.6}, x_{54.7}, \\ x_{54.8}, x_{54.9}, x_{54.10}, x_{55.5}, x_{55.6}, x_{55.7}, x_{55.8}, x_{56.1}, x_{56.2}, x_{56.4} \end{array} \right\}$$

№	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	B
1	ОН	ОН	ОН	ОН	ОН	Н	Н	Н	Н	b_0
2	ОН	ОН	ОН	ОН	Н	Н	Н	Н	Н	b_1
3	ОН	ОН	ОН	Н	Н	Н	Н	Н	Н	b_2
4	ОН	ОН	Н	Н	Н	Н	Н	Н	С	b_3
5	ОН	Н	Н	Н	Н	Н	Н	С	С	b_4
6	Н	Н	Н	Н	Н	Н	С	С	С	b_5
7	Н	Н	Н	Н	Н	С	С	С	С	b_6
8	Н	Н	Н	Н	С	С	С	С	В	b_7
9	Н	Н	С	С	С	С	С	В	В	b_8
10	С	С	С	С	С	С	В	В	В	b_9
11	С	С	С	С	С	В	В	В	В	b_{10}
12	С	С	С	С	В	В	В	В	В	b_{11}
13	С	С	С	В	В	В	В	В	В	b_{12}
14	С	С	В	В	В	В	В	В	В	b_{13}
15	С	В	В	В	В	В	В	В	В	b_{14}
16	В	В	В	В	В	В	В	В	В	b_{15}

Рисунок 3 – База правил $\tilde{R}$

Получены значения переменных x_{5k} «доля выполненных требований»:

$$x_{51} = \frac{1}{3} = 0,33;\ x_{52} = \frac{4}{7} = 0,57;\ x_{53} = \frac{2}{4} = 0,5;\ x_{54} = \frac{8}{10} = 0,8;\ x_{55} = \frac{4}{8} = 0,5;\ x_{56} = \frac{3}{7} = 0,42.$$

Среднее значение: $x_5 = \frac{1}{6}\sum_i^6 x_{5i} = 0,52$, соответствует значению A'_5 = «Среднее» со значением μ=1,0 и «Низкое» со значением μ=0,18 (Рисунок 1).

Аналогично определены значения A_i и $\mu_{A_i}(x_i)$ для остальных восьми групп (Таблица 1).

Таблица 1 – Результаты фаззификации

x_i	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
Значение A_i	Н	Н	С	С	С	С	С	В	В
$\mu_{A_i}(x_i)$	1,0	0,80	0,95	1,0	1,0	1,0	0,95	0,73	1,0
Значение A_i	Н	Н	Н	Н	Н	С	С	С	В
$\mu_{A_i}(x_i)$	0,56	0,73	0,44	0,42	0,18	1,0	0,36	0,42	1,0

2. Агрегирование степеней истинности предпосылок выполнено по формуле (9) по каждому правилу (Таблица 2).

Таблица 2 - Результаты агрегирования предпосылок

№ правила	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
αj	0	0	0	0	0	0	0	0,36	0,73	0,14	0	0	0	0	0	0

3. Активизация заключений выполнена по формуле (10). Результаты приведены в Таблице 3.

Таблица 3 – Результаты активизации заключений

№	1	2	3	4	5	6	7	8	9	B
8	H/0,56	H/0,73	H/0,44	H/0,42	C/0,56	C/1,0	C/0,36	C/0,42	B/1,0	b7/0,36
9	H/1,0	H/0,80	C/0,95	C/1,0	C/1,0	C/1,0	C/0,95	B/0,73	B/1,0	b8/0,73
10	C/0,45	C/0,56	C/0,42	C/0,24	C/0,33	C/0,25	B/0,14	B/0,66	B/0,85	b9/0,14

В результате получено на множестве значений выходной переменной y функцию принадлежности $\mu_{\tilde{B}'}(y) = \sup_{x \in X} \left\{ \min \left[\mu_{A'}(x), \mu_R(x,y) \right] \right\}$. Графически функция $\mu_{\tilde{B}'}(y)$ приведена на Рисунке 4.

Д. Дефаззификация проведена по формуле (12), определяя центр площади, ограниченной ломаной линией $\mu_{\tilde{B}'}(y)$. В результате получено искомое значение y = 0,53 (Рисунок 4).

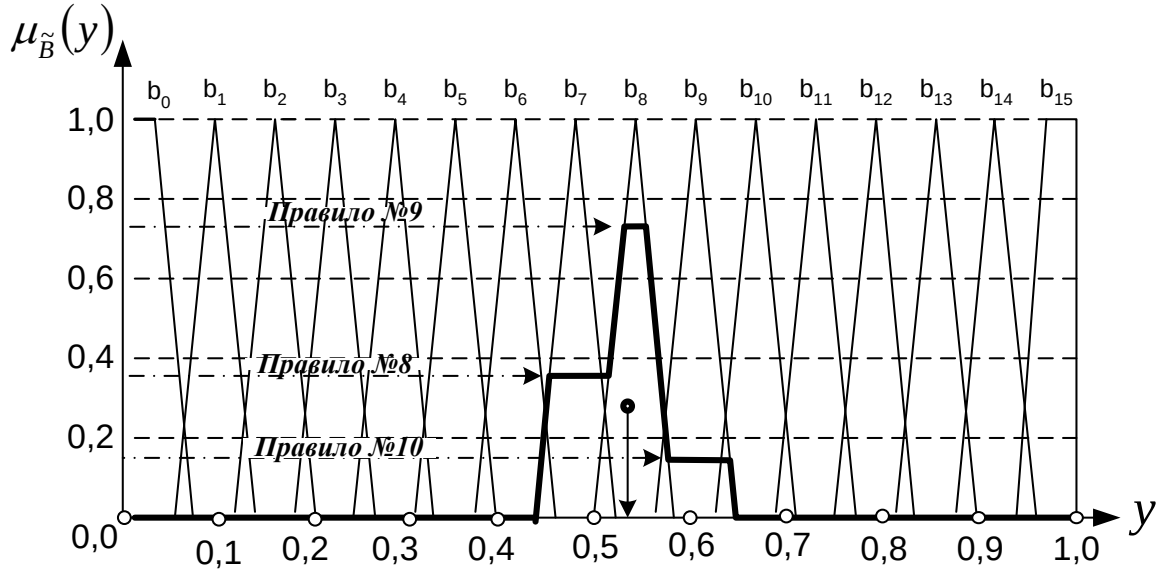

Рисунок 4 – Полученная функция принадлежности $\mu_{\tilde{B}'}(y)$

Полученное значение характеризует защищенность информации в рассмотренной для примера информационной системе.

Заключение. В целях информационной безопасности всегда требуется анализировать защищенность информационных ресурсов и принимать эффективные решения по определению методов и выбору технологий защиты. Предлагаемый подход позволит эффективно использовать полученные оценки для решения задачи обеспечения безопасности информации в автоматизированных системах. Его преимущества: не требует проведения сложных процедур тестирования, расчета вероятностей, привлечения и подбора экспертов и др. Предлагаемый подход может быть использован для оценивания большинства различных аспектов информационной безопасности.

ЛИТЕРАТУРА

1. Астахов, А. Анализ защищенности корпоративных систем / А. Астахов // Открытые системы, 2002. – № 7 – 8.
2. International standard ISO/IEC 15408:1999, “Information technology – Security techniques –Evaluation criteria for IT security – Part 1- Part 3”.
3. International standard ISO/IEC 17799:1999, “Information technology – Code of practice for information security management”.
4. С. Лыдин. Тестирование на проникновение при помощи Rapid7 Metasploit: - https://www.anti-malware.ru/practice/methods/penetration-testing-using-rapid7-metasploit
5. Захаров, А. П. Методология оценки информационной безопасности профиля защиты / А. П. Захаров. – http://beda.stup.ac.ru/rv-conf/.
6. Димов Э.М. Управление информационной безопасностью корпорации с применением критериев риска и ожидаемой полезности, Маслов О.Н., Раков А.С.; Информационные технологии. 2016. Т. 22. № 8. С. 620-627.
7. Разработка методов и алгоритмов проверки работы предприятия с точки зрения информационной безопасности его функционирования. Остроух Е.Н., Чернышев Ю.О., Мухтаров С.А., Богданова Н.Ю.; Инженерный вестник Дона. 2016. Т. 41. № 2 (41). С. 31.
8. Борисов В.В. Нечеткие модели и сети. / В.В. Борисов, В.В. Круглов, А.С. Федулов. – М: Горячая линия – Телеком, 2007. – 284 с.

V.L. Tokarev, A.A. Sychugov

METHOD OF AUDITING THE PROTECTION OF AUTOMATED SYSTEMS

Tula State University, Tula, Russia

The analysis of the currently existing regulatory framework and methods for analyzing the protection of information resources was carried out. It is noted that the basis of the methods is the use of technical methods of analysis, which involve the use of both active and passive testing of the information protection system. Another existing solution to this problem is the use of expert assessments. However, both approaches are laborious and often subjective. On the basis of the theory of fuzzy sets, a mathematical model is proposed for auditing the security of automated systems on the basis of which an appropriate method has been proposed. Fuzzy models are considered as a tool for auditing automated systems that process confidential information. As an example of the use of the proposed method, an assessment of one of the information security aspects is considered - the security of access to confidential information in an automated system. The proposed method will make it possible to effectively use the obtained estimates for solving the problem of ensuring the security of information in automated systems. The main advantage of the method is that it does not require complex testing procedures, calculating probabilities, attracting and selecting experts, etc., and can be used to evaluate most various aspects of information security.

Keywords: information security, access security, evaluation.

REFERENCES

1. Astakhov, A. Analysis of corporate systems security / A. Astakhov // Open systems, 2002. - № 7 - 8.
2. International standard ISO/IEC 15408:1999, “Information technology – Security techniques –Evaluation criteria for IT security – Part 1- Part 3”.
3. International standard ISO/IEC 17799:1999, “Information technology – Code of practice for information security management”.
4. S. Lydyn. Penetration testing with Rapid7 Metasploit:- https://www.anti-malware.ru/practice/methods/penetration-testing-using-rapid7-metasploit
5. Zakharov, A. P. Methodology for assessing information security of a protection profile / A. P. Zakharov. – http://beda.stup.ac.ru/rv-conf/.
6. Dimov E.M. Information security management of a corporation using risk and expected utility criteria, Maslov ON, Rakov A.S .; Information Technology. 2016. Vol. 22. No. 8. P. 620-627.
7. Development of methods and algorithms for testing the operation of an enterprise from the point of view of information security of its operation. Ostroukh E.N., Chernyshev Yu.O., Mukhtarov S.A., Bogdanova N.Y .; Engineering herald Don. 2016. V. 41. No. 2 (41). S. 31.
8. Borisov V.V. Fuzzy models and networks. / V.V. Borisov, V.V. Kruglov, A.S. Fedulov. - M: Hotline - Telecom, 2007. - 284 p