вателей в электронных технических средствах и системах общего применения. М.: Гелиос АРВ, 2010. – 224 с.
6. Алышев Ю.В., Маслов О.Н., Рябушкин А.В. Исследование интермодуляционных характеристик случайных антенн // Труды МТУСИ. Том II. М.: ИД Медиа Паблишер, 2008. – С. 68-74.
7. Маслов О.Н., Рябушкин А.В. Сотовые терминалы: утечка информации по интермодуляционным каналам // Мобильные телекоммуникации. №6, 2008. – С. 11-14.
8. Маслов О.Н., Рябушкин А.В. Интермодуляци-онные характеристики сложных случайных антенн // Телекоммуникации. №6, 2009. – С. 36-41.
9. Алышев Ю.В., Маслов О.Н., Рябушкин А.В. Оценка эффективности распределенных случайных антенн // Антенны. №10 (149), 2009. – С. 62-69.
10. Способ определения затухания сигнала в распределенной случайной антенне // Маслов О.Н., Раков А.С., Рябушкин А.В. Патент RU 2 393 493 от 06.04.2009, опубл. 27.06.2009, бюлл. №18.

FEATURES OF MODELING OF MODES EXCITATION OF MULTI-CHANNEL RANDOM ANTENNAS

Zasedateleva P.S., Maslov O.N., Ryabushkin A.V., Scherbakova T.A.

The modes of excitation of lumped and distributed random antenna (RA and DRA) are examined. The initial data necessary for the investigation of multi-channel RA and DRA by statistic imitation method (SIM) and designing of protection system confidential information security (CIS) are introduced.

Keywords: *confidential information security, multi-channel random antennas, modes of excitation of antennas, statistic imitation method, initial data.*

Заседателева Полина Сергеевна, аспирант Кафедры «Экономические и информационные системы (ЭИС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 228-00-36; 8-927-717-11-71.

Маслов Олег Николаевич, д.т.н., профессор, заведующий Кафедрой ЭИС ПГУТИ. Тел. (8-846) 271-06-24. E-mail: maslov@psati.ru

Рябушкин Аркадий Викторович, инженер Кафедры «Мультисервисные сети и информационная безопасность» ПГУТИ. Тел. (8-846) 339-11-99; 8-937-981-70-16.

Щербакова Татьяна Андреевна, аспирант Кафедры ЭИС ПГУТИ. Тел. (8-846) 228-00-36; 8-917-164-94-84.

УДК 004.043

ОБРАБОТКА РЕЗУЛЬТАТОВ ЭКСПЕРТНОЙ ОЦЕНКИ УЩЕРБА ИНФОРМАЦИОННОЙ СИСТЕМЕ ДЛЯ ВЫВОДА ИНТЕГРАЛЬНОЙ ФУНКЦИИ ПРИНАДЛЕЖНОСТИ

Дубинин Е.А., Копытов В.В., Тебуева Ф.Б.

Предложена методика вывода интегральной функции принадлежности нечеткого множества ущерба информационной системе. Методика базируется на экспертной оценке уровня воздействия классов угроз и использует методы нечеткой логики. Для обработки экспертных оценок разработан авторский способ.

Ключевые слова: угроза безопасности, ущерб информационной системе, способ распространения угрозы, нечеткое множество, экспертные оценки.

Введение

В современной динамической обстановке при управлении предприятием или организацией без достаточного информационного обеспечения невозможно принимать правильные решения. Это определяет необходимость внедрения сложных систем сбора, обработки и анализа различной информации. Объектом исследования в настоящей работе является информационная система предприятия, представляющая собой организационно-техническую систему, реализующую информационные технологии и предусматривающая аппаратное, программное и другие виды обеспечения, а также соответствующий персонал [1-2]. Ущерб информационной системе представляет собой численную величину урона в денежном выражении, нанесенного деятельности предпри-

ятия в результате реализации угроз безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации [1; 3].

Применение компьютеров и различных компьютерных систем для сбора, обработки и хранения информации [4] позволяет увеличить объемы обрабатываемых данных и их концентрацию в вычислительных системах. На современном этапе развития информационных технологий все чаще для решения разных прикладных задач используют математический аппарат нечетких множеств [5-6]. Эта тенденция также повлияла на создание моделей и систем с нечеткой логикой [6], направленной на решение задач в сфере информационной безопасности. Прежде всего это связано с тем, что процессы, которые происходят в исследуемом объекте, характеризуются большой степенью неопределенности, случайности, нестабильности, влиянием разнообразных возмущений во времени и т.п. Указанные факторы становятся существенным препятствием для построения точных моделей, основанных на классических теориях и моделях.

Основным понятием теории нечетких множеств является функция принадлежности. Поэтому определение степеней принадлежности элементов множеству и построение функции принадлежности является основным вопросом практических реализаций независимо от того, к какой предметной области они принадлежат. При решении задач защиты информации, моделирования процессов принятия решений в нечетких условиях и других прикладных задач можно использовать различных методы формирования функции принадлежности. В работах [7-8] приведены методы построения функции принадлежности, основной целью которых является формализация и интеграция исходных данных, сформированных экспертом (группой экспертов) в процессе оценивания параметров реальных объектов. Для эффективного решения указанных задач необходимо сделать правильный выбор нужного метода формирования функции принадлежности (с учетом ее класса) с целью использования возможных методов дальнейшей ее обработки.

Методика получения интегральной оценки ущерба информационной системе

Предлагаемая методика построения нечеткого множества уровня ущерба информационной системе использует мнение экспертов в области информационной безопасности. Суть методики состоит в следующем. Каждым экспертом формируются начальные нечеткие множества уровня воздействия определенной угрозы на информационную систему, которые обобщаются в нечеткие множества суммарного воздействия всего класса угроз. Оценка ущерба информационной системе получается путем нечеткого вывода функции принадлежности из обобщенных по всем экспертам функций принадлежности суммарного воздействия всего класса угроз.

Вычислительный процесс методики получения численной оценки ущерба информационной системе состоит из четырех этапов.

Этап 1. Формирование модели угроз, определение взаимосвязи между угрозами и ущербом информационной системе. Формирование модели угроз информационной безопасности состоит в выборе адекватной решаемой задаче классификации угроз и выделении наиболее распространенных классов из них. В настоящей методике предлагается классифицировать угрозы информационной безопасности по признаку «способ распространения». В таблице 1 для такой классификации приведены названия классов угроз и соответствующие им способы распространения угрозы

Ущерб информационной системе предприятия определяется, как сказано ранее, величиной урона, наносимого предприятию при реализации возможных видов угроз. Уровень ущерба компании, представляющий собой качественную характеристику, чаще всего представляется в виде следующей шкалы.

1. Малый ущерб, приводящий к незначительным потерям материальных активов (которые быстро восстанавливаются) или к незначительному влиянию на репутацию компании.

2. Умеренный ущерб, вызывающий заметные потери материальных активов или умеренное влияние на репутацию компании.

3. Ущерб средней тяжести, приводящий к существенным потерям материальных активов или значительному урону репутации компании.

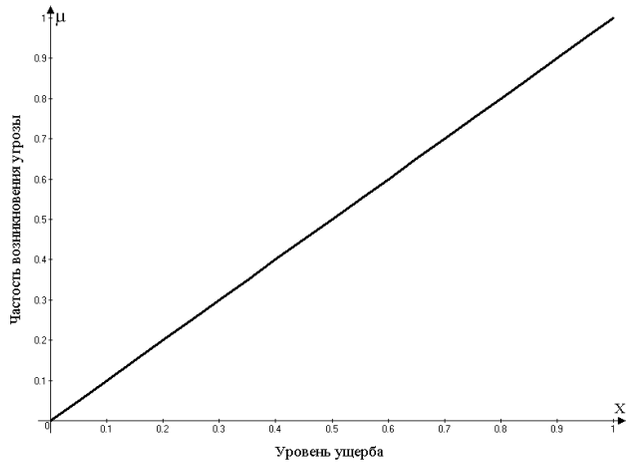
4. Большой ущерб, вызывающий большие потери материальных активов и наносящий большой урон репутации компании.

5. Критический ущерб, приводящий к критическим потерям материальных активов или к полной потере репутации компании на рынке, что делает невозможным дальнейшую деятельность организации.

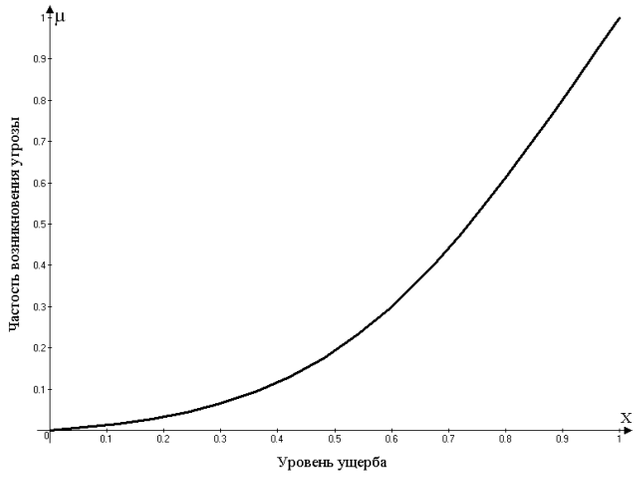
В настоящей методике предлагается оценивать уровень ущерба информационной системе в зависимости от частости проявления той или

Таблица 1. Классификация по признаку «способ распространения угрозы»

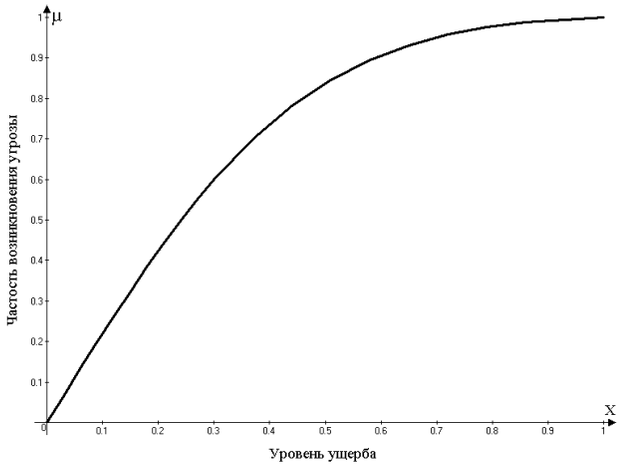
№ п/п	Класс угроз	Способ распространения
1	Атаки с использованием вредоносного кода	Через файл электронной почты
		Через дискеты и CD диски
		Через скачанный из Internet файл
		С пиратскими программами
		Со СПАМом
2	Сетевые атаки	На переполнение буфера
		IP-spoofing
		На систему НСД
		Cracking Web-серверов
3	Атаки на получение несанкционированного доступа	Установка и использование посторонних программ
		Сканирование IP адресов и портов сети
		Загрузка с дискеты
		Подбор паролей
		Атаки на переполнение буфера
		Подключение модемов и других аппаратных устройств
4	Злоупотребление полномочиями	Использование компьютера в личных целях
		Ошибки персонала
		Продажа корпоративных данных
		Раскрытие конфиденциальных данных
		Использование компьютеров для непроизводственной деятельности
5	Сбои в работе аппаратуры	Отказ связи
		Аппаратный сбой
		Потеря питания
		Зависание компьютера
6	Кражи и чрезвычайные ситуации	Воровство активов
		Похищение персонала
		Пожар
		Землетрясение
		Наводнение
7	Чрезмерное использование систем защиты, ухудшающее работу автоматизированной системы	Антивирусная защита
		Криптографическая защита
		Защита точек доступа, сетевых служб и сетевых коммуникаций (МЭ, DNS, DHCP и др.)
		Защита от НСД (встроенные средства и внешние устройства)
		Разграничение прав доступа, групповая политика и мониторинг



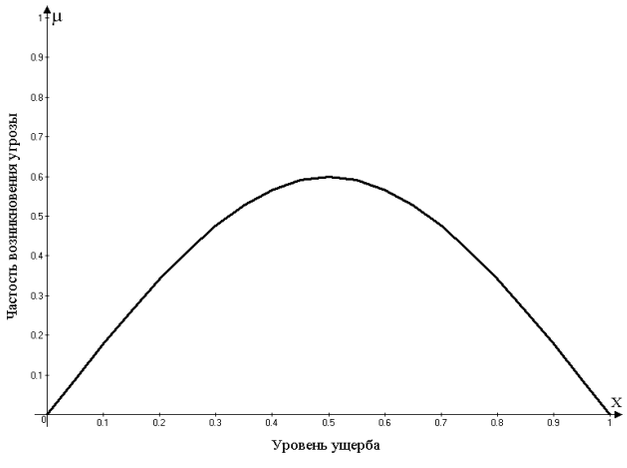
а) линейно возрастающий тренд



б) нелинейный тренд с монотонным возрастанием



в) нелинейный тренд с монотонным возрастанием



г) нелинейный тренд с периодом возрастания и убывания

Рис. 1. Виды функции принадлежности типовых нечетких множеств уровня ущерба информационной системе

иной угрозы. Такое оценивание имеет вид нечеткого множества, у которого носитель – уровень ущерба (в рублях), функция принадлежности – степень проявления угрозы (частость).

Этап 2. Построение начальных нечетких множеств уровня ущерба информационной системе. Построение функций принадлежности начальных нечетких множеств уровня ущерба информационной системе производится экспертным путем. Группе экспертов предлагается оценить зависимость частости появления выделенных видов угроз и соответствующего уровня ущерба предприятию. Такая зависимость представляет собой аналитическую функцию с одним из четырех основных видов трендов: линейный (Л), экспоненциальный (Э), логарифмический (Лог), полиномиальный (П). Причем линейный тренд является возрастающим, экспоненциальный и логарифмический – нелинейно монотонно возрастающими, полиномиальный – с периодом возрастания и убывания. Более точно экспертам необходимо для каждой угрозы выбрать типовую для нее функцию принадлежности уровня ущерба информационной системе. На рис. 1 приведены четыре типовые функции принадлежности.

Результаты своего оценивания каждый эксперт вносит в так называемый опросник, который представляет собой таблицу 1 с добавлением столбцов для выбора вида тренда поведения каждой угрозы. Таблица 2 является частью такого опросника для внесения результатов оценивания в рамках одного класса угроз. В ней для выбора вида тренда используется символ «+». В случае затруднения с ответом эксперт может выбрать вариант «не знаю». Такой вариант при дальнейшей обработке результатов учитываться не будет.

Заполнение всего опросника позволяет формировать нечеткие множества уровня ущерба информационной системе от реализации каждой конкретной угрозы заданным способом распро-

странения. Эти нечеткие множества будем называть экспертными, или начальными, и обозначим через

$$W^{q,l} = \left\{\left(x_i, \mu_i^{q,l}\right)\right\}, \quad (1)$$

где q – класс угроз; $l = 1;2 \ldots m$ – способ распространения угрозы; x_i – уровень ущерба информационной системе от реализации рассматриваемой угрозы; $\mu_i^{q,l}$ – частость появления угрозы класса q способом l.

Таблица 2. Результат экспертного оценивания поведения угроз в классе «Атаки с использованием вредоносного кода»

№ п/п	Способ распространения	Вид тренда				Не знаю
		Л	Э	Лог	П	
1	Через файл электронной почты	+				
2	Через дискеты и CD диски			+		
3	Через скачанный из Интернета файл	+				
4	С пиратскими программами	+				
5	Со СПАМом					+

Если задана стоимость S защищаемой информации, то по формуле умножения нечеткого множества на число можно получить величину ущерба информационной системы от реализации рассматриваемой угрозы

$$C^{q,l} = S \cdot W^{q,l} . \quad (2)$$

Этап 3. Построение обобщенных и итогового нечетких множеств уровня ущерба информационной системе (по данным одного эксперта). Для получения обобщенных нечетких множеств уровня ущерба от реализации всего класса угроз на информационную систему необходимо сложить полученные на этапе 2 начальные нечеткие множества. Сложение предлагается выполнять по алгебраическому методу [8]: функция принадлежности суммы двух нечетких множеств $\widetilde{A} = \left\{\left(x_i, \mu_{\widetilde{A}}\left(x_i\right)\right)\right\}$ и $\widetilde{B} = \left\{\left(x_i, \mu_{\widetilde{B}}\left(x_i\right)\right)\right\}$ при соответствующих носителях X равна величине

$$\mu_{\widetilde{A}+\widetilde{B}}(x_i) = \mu_{\widetilde{A}}(x_i) + \mu_{\widetilde{B}}(x_i) - \mu_{\widetilde{A}}(x_i) \cdot \mu_{\widetilde{B}}(x_i) . \quad (3)$$

Обобщенное нечеткое множество уровня ущерба от реализации класса угроз на информационную систему определяется суммой

$$\widetilde{W}^q = \left\{\left(x_i, \mu_{\widetilde{W}^q}\left(x_i\right)\right)\right\} = \sum_{l=1}^{m} W^{q,l} . \quad (4)$$

Итоговое нечеткое множество ущерба информационной системе представляет собой нечеткий вывод по всем полученным ранее обобщенным нечетким множествам

$$\hat{W} = \left\{\left(x_i, \hat{\mu}\left(x_i\right)\right)\right\},$$
$$\hat{\mu}\left(x_i\right) = \max_{i=1,..,n}\left(\mu_{\widetilde{W}^q}\left(x_i\right)\right). \quad (5)$$

Схема вывода итогового нечеткого множества ущерба информационной системе от реализации всех возможных угроз, полученная по данным одного эксперта, приведена на рис. 2.

Интегральной оценкой является результат обработки итоговых нечетких множеств ущерба информационной системе, полученных всеми экспертами.

Этап 4. Вывод интегральной оценки ущерба информационной системе предприятия (по данным группы экспертов). Обозначим количество экспертов, участвующих в оценивании ущерба информационной системе, переменной k. Предварительно каждый из этих экспертов определяет степень своей компетентности в вопросах информационной безопасности. В рамках предлагаемой методики следует упорядочить экспертов по убыванию степени их компетентности и перенумеровать индексом $j = 1;2 \ldots k$. Аналогичным образом необходимо перенумеровать итоговые нечеткие множества, полученные на этапе 3:

$$\hat{W}^j = \left\{\left(x_i^j, \hat{\mu}\left(x_i^j\right)\right)\right\}; \quad i = 1;2 \ldots r; \quad j = 1;2 \ldots k . \quad (6)$$

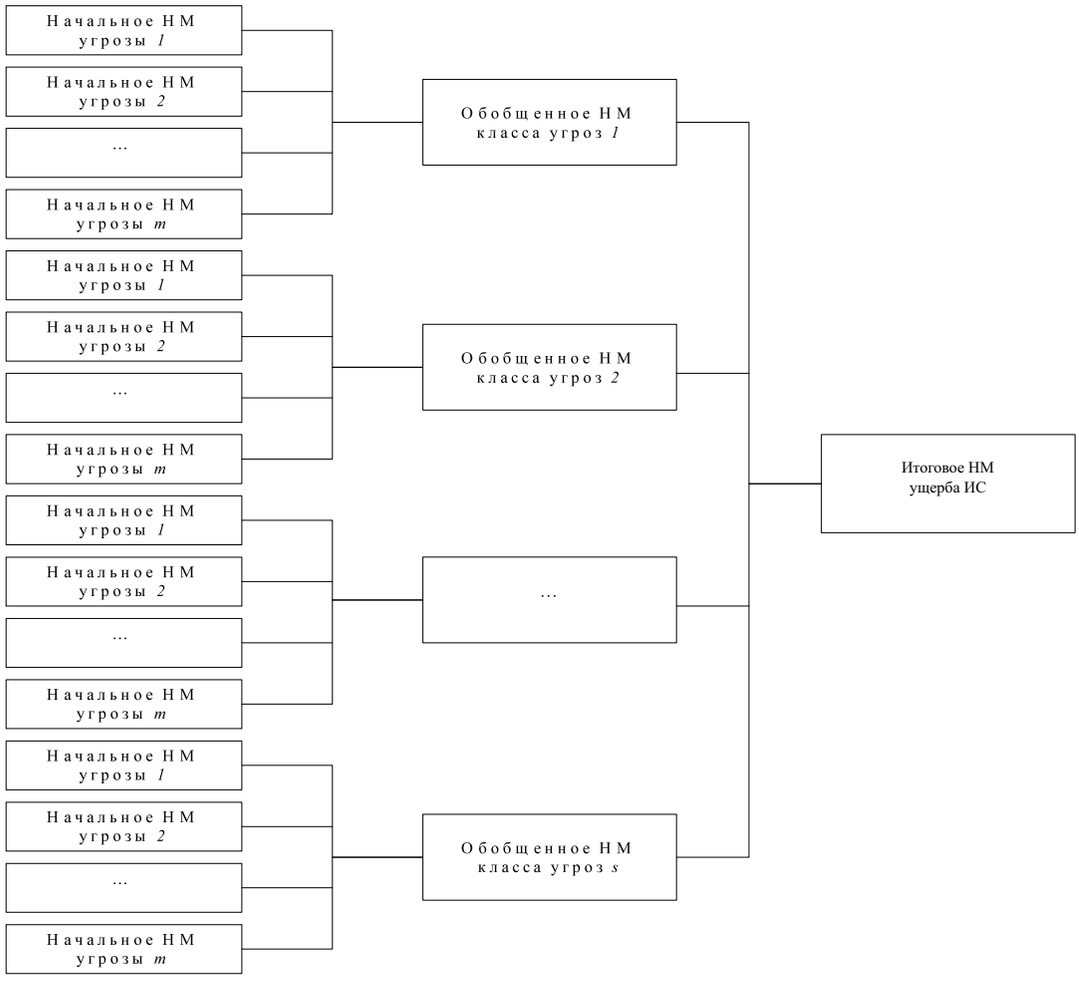


Рис. 2. Схема нечеткого вывода итогового нечеткого множества ущерба информационной системе (по данным одного эксперта)

Упорядоченные итоговые нечеткие множества (6) вносим в таблицу 3.

Далее предлагается составить матрицу соответствия мнения экспертов, являющуюся булевой матрицей. Обозначим эту матрицу через

$$Y = \left\| y_{ij} \right\|;\ i = 1,2,...,r;\ j = 1,2,...,k\ . \quad (7)$$

Ее элементы будут формироваться следующим образом. Присвоим эксперту $j = 1$ степень «наиболее компетентен». Тогда элементы первого столбца y_{i1} матрицы Y будут равны 1. Теперь необходимо сравнить степени принадлежности $\hat{\mu}\left(x_i^2\right)$, $\hat{\mu}\left(x_i^3\right)$, …, $\hat{\mu}\left(x_i^k\right)$ попарно с $\hat{\mu}\left(x_i^1\right)$. Если их относительное отклонение от $\hat{\mu}\left(x_i^1\right)$ колеблется в пределах 5%, то соответствующему элементу y_{ij} приписывается значение 1, в противном случае 0.

Таблица 3. Упорядоченные по убыванию степени компетентности экспертов и итоговые нечеткие множества

Эксперты → / Степени принадлежности ↓	$j=1$	$j=2$	…	$j=k$
$\hat{\mu}\left(x_1^j\right)$	$\hat{\mu}\left(x_1^1\right)$	$\hat{\mu}\left(x_1^2\right)$	…	$\hat{\mu}\left(x_1^k\right)$
$\hat{\mu}\left(x_2^j\right)$	$\hat{\mu}\left(x_2^1\right)$	$\hat{\mu}\left(x_2^2\right)$	…	$\hat{\mu}\left(x_2^k\right)$
…	…	…	…	…
$\hat{\mu}\left(x_r^j\right)$	$\hat{\mu}\left(x_r^1\right)$	$\hat{\mu}\left(x_r^2\right)$	…	$\hat{\mu}\left(x_r^k\right)$

Интегральную оценку ущерба информационной системе обозначим через $W = \left\{\left(x_i, \mu\left(x_i\right)\right)\right\}$. Ее вывод является итеративным процессом. Приведем описание итераций.

Итерация 1. Обозначим матрицу соответствия мнений экспертов через $Y^{(1)}$. В этой матрице следует выполнить $i=\overline{1,r}$ проверок. Каждая проверка включает в себя построчное сложение элементов $\sum_{j=1}^{k} y_{ij}$ и сравнение этой суммы с величиной $2/3\cdot k$. Если $\sum_{j=1}^{k} y_{ij} \geq 2/3\cdot k$, то элементу нечеткого множества интегральной оценки ущерба информационной системе присваивается соответствующее значение степени принадлежности первого эксперта $\mu(x_i)=\hat{\mu}(x_i^1)$. В противном случае считается, что данная степень принадлежности не определена. Интегральная оценка ущерба информационной системе считается построенной, если определены все степени принадлежности $\mu(x_i)$, $i=1;2\ ...\ r$. В противном случае следует выполнять итерацию 2.

Итерация 2. Для получения не определенных на предыдущей итерации степеней принадлежности необходимо сформировать новую матрицу соответствия мнений экспертов, которую обозначим через $Y^{(2)}$. В ней степень «наиболее компетентен» следует присвоить второму эксперту $j=2$. Тогда элементы второй строки матрицы $Y^{(2)}$ равны 1, а для получения остальных необходимо сравнивать относительные отклонения их от $\hat{\mu}(x_i^2)$. Как и ранее, допустимым является отклонение в пределах 5%. Ячейкам с допустимым отклонением присвоить значение 1, с недопустимым – 0.

Проверку согласованности мнений экспертов следует производить для не определенных на предыдущей итерации степеней принадлежности. Как и прежде, если сумма элементов строки матрицы $\sum_{j=1}^{k} y_{ij}^{(2)} \geq 2/3\cdot k$, то неопределенному элементу $\mu(x_i)$ присвоить соответствующее значение $\hat{\mu}(x_i^2)$. Если по завершении итерации 2 остались неопределенными некоторые степени принадлежности $\mu(x_i)$, то следует перейти к итерации 3, где наиболее компетентным будем считать мнение третьего эксперта $j=3$ и т.д. Процесс следует продолжать до тех пор, пока не будут определены все степени принадлежности нечеткого множества $W=\{(x_i,\mu(x_i))\}$.

Валидация интегральной оценки ущерба информационной системе

Для получения качественных оценок состояния уровня информационной безопасности необходимо провести соотношение между значениями функции принадлежности и результатом логического вывода. При этом пороговое значение результатов логического вывода в зависимости от решаемой задачи может изменяться. Если функция принадлежности не имеет монотонный характер, то даже плавное изменение порога принятия решения может привести к резкому изменению качественной оценки. Аналогичная ситуация может возникнуть и при наличии разрывов в функции принадлежности.

Следовательно, для оценки качества интегральной оценки ущерба информационной системе предлагается использовать векторную целевую функцию [9-10]

$$F=(F_1,F_2). \tag{8}$$

Критерий F_1 является критерием монотонности функции принадлежности по возрастанию и определяется как

$$F_1=\mu_{i+1}(x)-\mu_i(x)\geq 0. \tag{9}$$

Критерий F_2 является критерием сглаженности и оценивается с помощью среднего квадратичного отклонения

$$F_2=\sqrt{\frac{\sum_{i=1}^{r}\left(\mu(x_i)-\mu^*(x_i)\right)^2}{r}}\to 0, \tag{10}$$

где $\mu(x_i)$ – степени принадлежности нечеткого множества интегральной оценки ущерба информационной системе, $\mu^*(x_i)$ – степени принадлежности соответствующего типового тренда. Оптимальной интегральной оценкой ущерба информационной системе будем считать такое нечеткое множество $W=\{(x_i,\mu(x_i))\}$, в котором наиболее полно выполняются критерии (9)-(10).

Заключение

Предложенная методика получения интегральной оценки ущерба информационной системе базируется на экспертном подходе построения функций принадлежности начальных нечетких множеств. Для формирования обобщенных нечетких множеств ущерба информационной системе от реализации класса угроз предложено использовать алгебраическое сложение начальных нечетких множеств.

Для вывода итогового нечеткого множества предлагается использовать правило максимального риска. Формирование интегральной оценки производится посредством авторского подхода,

называемым процедурой проверки согласованности мнений экспертов. Для возможности проведения валидации интегральной оценки ущерба информационной системе и выбора наиболее оптимальной интегральной оценки из имеющихся альтернатив предложено использовать многокритериальный подход. Векторная целевая функция при таком подходе состоит из критериев монотонности и сглаженности.

Предложенная методика формирования нечеткого множества ущерба информационной системе от реализации всех возможных угроз обладает следующими двумя основными достоинствами:

- не использует аппарат теории вероятностей в силу отсутствия реальной статистики воздействия угроз;

- не применяет процедуру оценки степени соответствия информационной системы определенному набору требований по обеспечению информационной безопасности, что может являться весьма дорогой процедурой для предприятия.

Работа выполнена в рамках федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009-2013 годы

Литература

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД ДС», 2001. – 688 с.
2. Емельянников М. Информационные системы персональных данных: http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=22489.
3. Малюк А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации. М.: Горячая Линия – Телеком, 2004. – 280 с.
4. Шураков В.В. Обеспечение сохранности информации в системах обработки данных (по данным зарубежной печати). М.: Финансы и статистика, 1985. – 224 с.
5. Zadeh L.A. Fuzzy sets // Information and Control. Vol.8, N3, 1965. – P. 338-353.
6. Кофман А. Введение в теорию нечетких множеств. М.: Радио и связь, 1982. – 432 с.
7. Корченко А.Г., Рындюк В.А. Исследование статистических методов формирования функций принадлежности // Защита информации. Сб. научных трудов. Вып.2(9). К.: НАУ, 2002. – С. 54-60.
8. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей: Примеры использования. Рига: Зинатне, 1990. – 184 с.
9. Подиновский В.В., Ногин В.Д. Парето-оптимальные решения многокритериальных задач. М.: Наука, 1982. – 256 с.
10. Емеличев В.А., Перепелица В.А. Сложность дискретных многокритериальных задач // Дискретная математика. Т.6, Вып.1, 1994. – С. 3-33.

PROCESSING OF RESULTS OF THE EXPERT ASSESSMENT OF DAMAGE TO INFORMATION SYSTEM FOR THE CONCLUSION OF INTEGRATED FUNCTION OF THE ACCESSORY

Dubinin E.A., Kopytov V.V., Tebueva F.B.

The offered procedure of a conclusion of integrated function of an accessory of fuzzy set of damage information system. The procedure is based on an expert assessment of a level of influence of classes of threats and uses methods of fuzzy logic. The author's way is developed for processing expert assessments.

Keywords: *threat of a security, damage to information system, a way of propagation of threat, fuzzy set, expert assessments.*

Дубинин Евгений Александрович, соискатель Кафедры «Прикладная математика» Ставропольского государственного университета (СтГУ). Тел. (8-865) 235-62-66; 8-928-006-39-40. E-mail: mobls@mail.ru

Копытов Владимир Вячеславович, д.т.н., профессор, начальник Управления информатизации СтГУ. Тел. (8-865) 235-62-66; 8-918-751-33-43. E-mail: mobls@mail.ru

Тебуева Фариза Биляловна, к.ф-м.н., доцент Кафедры «Организация и технологии защиты информации» Ст.ГУ. Тел. 8-928-308-03-07. E-mail: tebueva@stavsu.ru