УДК 004.043

МЕТОДИКА ПОЛУЧЕНИЯ НЕЧЕТКОГО МНОЖЕСТВА УРОВНЯ ВОЗДЕЙСТВИЯ КЛАССА УГРОЗ НА ИНФОРМАЦИОННУЮ СИСТЕМУ

Е. А. Дубинин[1]*,*
соискатель
Ставропольский государственный университет

Предложенная методика построения нечеткого множества уровня воздействия класса угроз на информационную систему использует мнение экспертов в области информационной безопасности. Каждым экспертом формируются начальные нечеткие множества уровня воздействия определенной угрозы на информационную систему, которые обобщаются в нечеткие множества суммарного воздействия всего класса угроз.

Ключевые слова *— угроза, информационная безопасность, информационная система, нечеткое множество, ущерб.*

Введение

Настоящая работа посвящена проблеме математического оценивания воздействия различных видов угроз на информационную систему в контексте управления информационными рисками. Известно, что управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача состоит в объективной идентификации и оценке наиболее значимых для бизнеса информационных рисков компании, а также адекватности используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Информационный риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам [1]. Под термином «управление информационными рисками» обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативно-правовой базы в области защиты информации и собственной корпоративной политики безопасности. Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании [2].

Этап 1: формирование модели угроз, определение взаимосвязи между угрозами и рисками информационной безопасности

Формирование модели угроз информационной безопасности состоит в выборе адекватной решаемой задаче классификации угроз и выделении наиболее распространенных классов из них.

В публикациях [3–5] классификацию угроз выполняют по двум базовым признакам: по действию на характеристики безопасности информации и по природе источника.

По признаку «действие на характеристики безопасности информации» классификация имеет вид:

1) угроза конфиденциальности;
2) угроза целостности;
3) угроза доступности;
4) угроза конфиденциальности и целостности;
5) угроза конфиденциальности и доступности;
6) угроза целостности и доступности;
7) угроза конфиденциальности, целостности и доступности.

[1] Научный руководитель — доктор технических наук, профессор, начальник Управления информатизации Ставропольского государственного университета *В. В. Копытов.*

По признаку «природа источника» классификация угроз имеет вид:

1) объективная (угроза, возникновение которой не зависит от прямой деятельности человека и которая связана с разными стихийными природными явлениями);

2) субъективная (угроза, возникновение которой зависит от деятельности человека).

Основным недостатком этих двух классификаций является зависимость угрозы от ресурса, на который она воздействует, при этом не отражаются возможные альтернативные сценарии развития угрозы.

В настоящей работе предлагается классифицировать угрозы информационной безопасности по признаку «способ распространения»:

1) атаки с использованием вредоносного кода;

2) сетевые атаки;

3) атаки на получение несанкционированного доступа;

4) злоупотребления полномочиями;

5) сбои в работе аппаратуры;

6) кражи и чрезвычайные ситуации;

7) чрезмерное использование систем защиты, ухудшающих работу автоматизированной системы.

Уровень риска информационной безопасности предприятия определяется, как сказано ранее, уровнем ущерба, наносимого предприятию при реализации возможных видов угроз. Уровень ущерба представляет собой качественную характеристику. В табл. 1 приведена качественная шкала уровня ущерба компании.

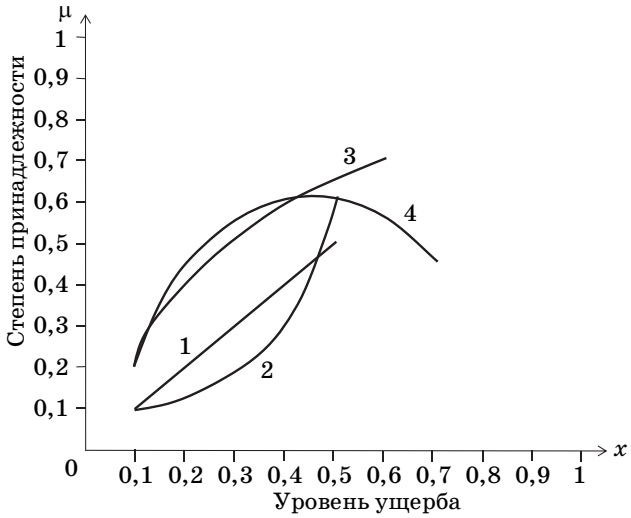
■ ***Таблица 1***. *Качественная шкала оценки уровня ущерба*

Уровень ущерба	Описание
Малый	Приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании
Умеренный	Вызывает заметные потери материальных активов или умеренно влияет на репутацию компании
Средней тяжести	Приводит к существенным потерям материальных активов или значительному урону репутации компании
Большой	Вызывает большие потери материальных активов и наносит большой урон репутации компании
Критический	Приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке, что делает невозможным дальнейшую деятельность организации

В настоящей работе предлагается определять оценки уровня ущерба информационной системе в зависимости от частости проявления той или иной угрозы. Такая оценка представляется в виде нечеткого множества, у которого носитель — уровень ущерба, функция принадлежности — степень проявления угрозы (частость).

Этап 2: построение функций принадлежности начальных нечетких множеств уровня ущерба информационной системе

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 задачах можно использовать различные методы формирования функции принадлежности. В работах [6, 7] 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 вы-



■ ***Рис. 1***. *Виды функции принадлежности типовых нечетких множеств уровня ущерба информационной системе*: *1 — линейно возрастающий тренд* (*линейный*); *2, 3 — нелинейный тренд с монотонным возрастанием* (*экспоненциальный и логарифмический соответственно*); *4 — нелинейный тренд с периодом возрастания и убывания* (*полиномиальный*)

■ ***Таблица 2.*** *Выбор вида тренда и задание ключевых точек (для одного эксперта)*

Класс угрозы	Способ распространения	Вид тренда				Уровень ущерба
		Л	Э	Лог	П	
Атаки с использованием вредоносного кода	Через файл, прикрепленный к сообщению электронной почты	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Через посторонние дискеты и CD-диски			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Через скачанный из Интернета файл	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	С пиратскими программами	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Со СПАМом			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
Сетевые атаки	На переполнение буфера	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	На отказ в обслуживании		•			$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	IP-spoofing		•			$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Cracking Web-серверов		•			$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
Атаки на получение несанкционированного доступа	Установка и использование посторонних программ			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Сканирование IP-адресов и портов сети			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Загрузка с дискеты			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Подбор паролей			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Атаки на переполнение буфера	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Подключение модемов и других аппаратных устройств			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
Злоупотребления полномочиями	Использование компьютера в личных целях	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Ошибки персонала	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Продажа корпоративных данных	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Раскрытие конфиденциальных данных	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Использование компьютеров для непроизводственной деятельности			•		$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
Сбои в работе аппаратуры	Отказ связи	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Аппаратный сбой	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Потеря питания	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Зависание компьютера	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
Кражи и чрезвычайные ситуации	Воровство активов	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Похищение персонала	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Пожар	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Землетрясение	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Наводнение	•				$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
Чрезмерное использование систем защиты, ухудшающих работу автоматизированной системы	Антивирусная защита				•	$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Криптографическая защита				•	$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Защита точек доступа, сетевых служб и сетевых коммуникаций (межсетевой экран, DHCP-сервер и др.)				•	$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Защита от несанкционированного доступа (встроенные средства и внешние устройства)				•	$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$
	Разграничение прав доступа, групповая политика и мониторинг				•	$(x_{нач}, \mu_{нач}), (x_{пр}, \mu_{пр}), (x_{кон}, \mu_{кон})$

бор нужного метода формирования функции принадлежности (с учетом ее класса) с целью использовать возможные методы дальнейшей ее обработки.

Метод экспертного построения функций принадлежности оценки уровня ущерба информационной системе состоит в следующем. Группе экспертов предлагается оценить зависимость частоты появления выделенных видов угроз и соответствующего уровня ущерба предприятия. Такая зависимость представляет собой аналитическую функцию. Существуют 4 основных вида трендов (линейный (Л), экспоненциальный (Э), логарифмический (Лог), полиномиальный (П)) функций

такой зависимости, которые в общем случае можно представить в виде трех видов линий:

1) линейно возрастающая;

2) нелинейная с монотонным возрастанием;

3) нелинейная с периодом возрастания и убывания.

В качестве иллюстрации на рис. 1 показаны эти виды линий.

Уточнение выбранного тренда функции поведения информационной системы состоит в задании ключевых точек: начальной ($x_{нач}$, $\mu_{нач}$), промежуточной ($x_{пр}$, $\mu_{пр}$) и конечной ($x_{кон}$, $\mu_{кон}$). Пример заполненной анкеты эксперта приведен в табл. 2.

Построенные с использованием заданных экспертами ключевых точек и выбранный ими тип тренда позволяют строить нечеткое множество уровня ущерба конкретной угрозы заданным способом распространения на защищаемую информационную систему. Эти нечеткие множества будем называть экспертными, или начальными, и обозначим через

$$W^{l,q} = \{(x_i, \mu_i)\},$$

где индекс $l = 1, 2, ..., m$ — способы распространения угроз; индекс q — класс угроз; x_i — носители нечеткого множества, полученные в результате дискретизации значений уровня ущерба информационной системы в результате реализации рассматриваемой угрозы; μ_i — степени принадлежности носителей нечеткому множеству. Ущерб при такой угрозе составляет величину

$$C^{l,q} = SW^{l,q},$$

где S представляет собой стоимость защищаемой информации.

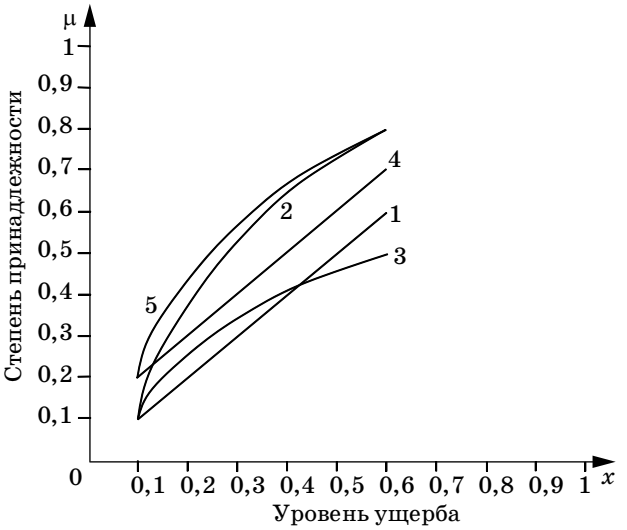
Этап 3: построение обобщенного нечеткого множества уровня воздействия класса угроз на информационную систему

Для получения обобщенного нечеткого множества уровня ущерба всего класса угроз на информационную систему необходимо сложить полученные на этапе 2 начальные нечеткие множества. Сложение двух нечетких множеств $\tilde{A}$ и $\tilde{B}$ предлагается выполнять по алгебраическому методу [8]:

$$\mu_{\tilde{A}+\tilde{B}}(x) = \mu_{\tilde{A}}(x) + \mu_{\tilde{B}}(x) - \mu_{\tilde{A}}(x) \cdot \mu_{\tilde{B}}(x).$$

Искомое обобщенное нечеткое множество уровня ущерба класса угроз на информационную систему

$$\tilde{W}^q = \sum_{l=1}^{m} W^{l,q}. \qquad (*)$$



■ ***Рис. 2.*** *Начальные нечеткие множества для способов распространения угроз $l = 1, 2, 3, 4, 5$ класса $q = 1$: 1 — через файл, прикрепленный к сообщению электронной почты; 2 — через посторонние дискеты и CD-диски; 3 — через скачанный из Интернета файл; 4 — с пиратскими программами; 5 — со СПАМом*

Приведем пример получения обобщенного нечеткого множества $\tilde{W}_k^q$ (*). Будем рассматривать конкретный класс угроз. Пусть $q = 1$, что соответствует первому классу угроз из табл. 2, а именно «Атаки с использованием вредоносного кода». Для этого класса обозначим способы распространения угроз $l = 1, 2, 3, 4, 5$.

В результате экспертного опроса для способов распространения l получены начальные нечеткие множества (рис. 2).

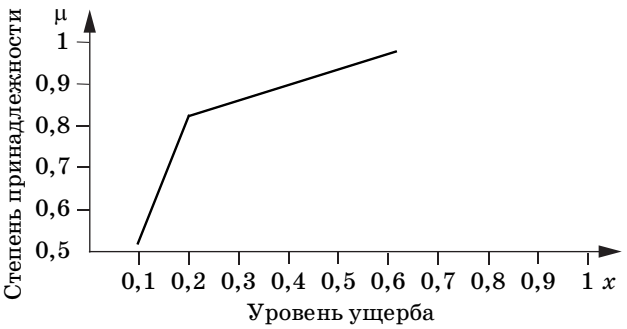
Нечеткие множества из рис. 2 имеют следующие числовые соответствия:

$$W^{1,1} = \{(0,1; 0,1), (0,2; 0,2), (0,6; 0,6)\};$$

$$W^{2,1} = \{(0,1; 0,1), (0,2; 0,4), (0,6; 0,8)\};$$

$$W^{3,1} = \{(0,1; 0,1), (0,2; 0,2), (0,6; 0,5)\};$$

$$W^{4,1} = \{(0,1; 0,2), (0,2; 0,3), (0,6; 0,7)\};$$



■ ***Рис. 3.*** *Обобщенное нечеткое множество $\tilde{W}^1$*

$$W^{5,1} = \{(0,1; 0,2), (0,2; 0,4), (0,6; 0,8)\}.$$

Вычислим обобщенное нечеткое множество $\tilde{W}^1$ уровня ущерба первого класса угроз на информационную систему по формуле (*):

$$\tilde{W}^1 = \sum_{l=1}^{5} W^{l,1} = \{(0,1; 0,53), (0,2; 0,83), (0,6; 0,99)\}.$$

Функция принадлежности для этого класса угроз является монотонно возрастающей (рис. 3). Это означает, что уровень ущерба прямо пропорционален степени принадлежности.

Заключение

Предложенная методика построения нечеткого множества уровня воздействия класса угроз на информационную систему 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 быть весьма дорогой процедурой для предприятия.

В области информационной безопасности недостаточно теоретической базы для решения задач качественной оценки. Это особенно важно, когда нет полных данных о воздействии угроз на информационную систему или эти данные заданы нечетко (размыто). Математический аппарат нечеткой логики является адекватным инструментарием для решения таких задач.

Литература

1. **Корченко А. Г.** Построение систем защиты информации на нечетких множествах. Теория и практические решения. — Киев: МК-Пресс, 2006. — 200 с.
2. **Петренко С. А., Симонов С. В.** Управление информационными рисками. — М.: ДМК Пресс, 2004. — 300 с.
3. **Вихорев С. В.** Классификация угроз информационной безопасности // Сетевые атаки и системы информационной безопасности. 2001. № 2. С. 23–30.
4. **Пархоменко Н., Яковлев С., Пархоменко П., Мисник Н.** Угрозы информационной безопасности. Новые реалии и адекватность классификации// Защита информации. Конфидент. 2003. № 6. С. 34–41.
5. **Халов Е. А.** Теоретические основы построения многопараметрических функций принадлежности нечетких систем// Информационные процессы. 2009. № 1. С. 15–21.
6. **Емельянников М.** Информационные системы персональных данных: http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=22489 (дата обращения: 25.03.2011).
7. **Алтунин А. Е., Семухин М. В.** Модели и алгоритмы принятия решений в нечетких условиях / ТюмГУ. — Тюмень, 2000. — 87 с.
8. **Борисов А. Н., Крумберг О. А., Федоров И. П.** Принятие решений на основе нечетких моделей: Примеры использования. — Рига: Зинатне, 1990. — 150 с.