М. Б. Гузаиров, И. В. Машкина, Е. С. Степанова

МЕТОД ОПРЕДЕЛЕНИЯ ЦЕННОСТИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ АППАРАТА НЕЧЕТКОЙ ЛОГИКИ

В связи с повсеместным использованием информационных технологий в различных сферах деятельности организаций риски нарушения информационной безопасности (ИБ) являются достаточно серьезной сопутствующей проблемой для любой компании.

Основными задачами управления рисками нарушения ИБ являются их идентификация и оценка. Оценка риска может заключаться в качественном или количественном определении его уровня. Уровень риска нарушения безопасности информационного объекта (ИО) определяется как функция двух величин: вероятности реализации актуальных угроз данному ИО и цены потери с точки зрения последствий для бизнеса [1]. Таким образом, оценка риска включает идентификацию информационных объектов и определение ценности каждого ИО, идентификацию и оценку уязвимостей и осуществляемых с их использованием угроз, а также выявление функциональной зависимости уровня риска нарушения ИБ информационной системы (ИС) от указанных характеристик.

Численная оценка уровня риска, в отличие от качественной, должна позволить судить об эффективности планируемых или используемых средств защиты и адекватности инвестиций в информационную безопасность в количественном выражении.

На сегодняшний день разработано несколько программных продуктов, автоматизирующих оценку риска нарушения информационной безопасности, ориентированных на *оценку уровня угроз*. При этом вопросу определения значений второго параметра — цены потери в результате нарушения ИБ — не уделяется должного внимания, пользователю не предлагается какой бы то ни было методики ее оценивания. В международном стандарте [2] такие методики также не приведены, в нем содержатся лишь *критерии для оценивания* возможных *последствий нарушения ИБ*.

При решении проблемы оценивания рисков нарушения информационной безопасности в [3] предложено производить детализацию структуры ИС до уровня сегментов сети. В качестве объекта атаки рассматривается сегмент сети, в котором обрабатывается множество ИО. Пользователи рабочих станций другого сегмента сети рассматриваются, как внутренние источники атаки рассматриваются. Внешними источниками атаки являются удаленные пользователи, обладающие правами доступа к ИС, и злоумышленники. В рассмотрение принимаются преднамеренные угрозы несанкционированного доступа и утечки информации. Использование метода предполагает идентификацию и количественное оценивание уровней угроз для каждого из сегментов сети. Значение уровня риска ИС определяется суммированием уровней рисков нарушения ИБ каждого из сегментов. В [4] предложен метод построения модели актуальных угроз с помощью нечеткой когнитивной карты, построенной в проекции на топологию сети. В работе [4] дополнено и формализовано предложенное в [3] решение проблемы оценки вероятности угрозы через эксплуатируемые уязвимости. Однако вопрос получения количественной оценки параметра «Цена потери» в [4, 5] остается нерешенным.

В [6] предлагается при оценке риска использовать термин «ценность информации» в рамках аддитивной модели ее оценивания. Как отмечается в [7], *ценность* информации оценивается *степенью полезности* ее для собственника ввиду того, что владение ею обеспечивает определенные *преимущества*, *цена* же — характеристика *информации как товара*, который производится, покупается и продается, и складывается из себестоимости и прибыли. Таким образом, при оценке рисков нарушения ИБ предлагается оперировать понятием «ценность информации», позволяющим судить о степени ее важности для осуществления бизнес-процессов.

Сущность предложенного в [6] подхода может быть сведена к следующему: информация, обрабатываемая на объекте защиты, представляется в виде конечного множества элементов,

упорядоченных в соответствии с иерархической относительной шкалой, что позволяет их сравнивать по значению ценности относительно друг друга. В случае, если известна ценность одного из элементов множества, вычисляется оценка одного балла и с учетом этой величины определяются значения ценностей остальных элементов множества. Возможна вариация метода, когда априорно известна ценность всех элементов множества, значения ценностей отдельных элементов могут быть вычислены через оценку одного балла иерархической относительной шкалы. Недостатками методики являются: необходимость наличия *экспертов* — представителей бизнеса с их знанием бизнес-процессов и способностью *выносить суждения* относительно *ценности активов*, а также то, что полученные результаты достаточно субъективны и зависят от адекватности оценки одного балла иерархической шкалы.

Таким образом, в настоящее время проблема получения параметра «Ценность информационного объекта» является актуальной.

Для информационных систем, инфраструктура которых построена с учетом требований безопасности к архитектуре самой сети, приведенных в [4], предлагается метод определения относительных ценностей информационных объектов, обрабатываемых в каждом из сегментов сети.

При решении задачи защиты информации в целом, и в особенности оценки рисков, первым шагом является идентификация информационных активов организации и их категорирование по уровням конфиденциальности (критичности, секретности, важности). Введем уровни критичности информации У = {«Н», «С», «В»} («Н» – низкий, «С» – средний, «В» – высокий).

Особенностью предлагаемого метода является то, что для оценивания параметра «Ценность информационных объектов» заданного уровня критичности, обрабатываемых в соответствующем локальном сетевом сегменте, в качестве исходной информации используются сведения о *количестве ИО* в сегменте и *числе критериев*, описывающих возможные негативные последствия нарушения их защищенности.

Введем обозначение общего количества сегментов сети организации X, где $X = N + M + L$. N, M, L определены в [4].

В сегментах сети могут обрабатываться информационные объекты, категории критичности которых соответствуют или ниже уровней доступа пользователей данного сегмента, т. е. множества O_n^H, O_m^C, O_l^B могут быть представлены в виде конечных множеств информационных объектов:

$$\begin{aligned} O_n^H &= \left\{ o_{n(1)}^H, o_{n(2)}^H .. o_{n(f_n)}^H .. o_{n(F_n)}^H \right\}, \\ O_m^C &= \left\{ o_{m(1)}^C, o_{m(2)}^C .. o_{m(g_m)}^C .. o_{m(G_m)}^C .. o_{m(1)}^H .. o_{m(F_m)}^H \right\}, \\ O_l^B &= \left\{ o_{l(1)}^B, o_{l(2)}^B .. o_{l(h_l)}^B .. o_{l(H_l)}^B .. o_{l(1)}^C .. o_{l(G_l)}^C .. o_{l(1)}^H .. o_{l(F_l)}^H \right\}, \end{aligned} \quad (1)$$

где F_n, F_m, F_l – количество информационных объектов категории критичности «Н», обрабатываемых в сегментах C_n, C_m, C_l соответственно,

G_m, G_l – количество информационных объектов категории критичности «С», обрабатываемых в сегментах C_m, C_l соответственно,

H_l – количество информационных объектов категории критичности «В», обрабатываемых в сегменте C_l.

Анализ ГОСТ 27005-2010 [2] позволяет задать множество критериев K, которые могут использоваться в качестве основы для получения численного значения параметра «Ценность информационных объектов уровня критичности У», обрабатываемых в заданном сегменте сети:

$$K = \bigcup_{e \in E} k, \quad (2)$$

где E – общее количество используемых критериев для определения ценности информационных объектов.

Перечень выбранных из [2] критериев приведен в таблице 1.

Таблица 1. Условные обозначения и наименования возможных видов последствий нарушения ИБ (из ГОСТ 27005-2010)

Условное обозначение	**Возможное последствие нарушения свойств ИБ**
ВП1	невозможность обеспечения сервиса
ВП2	утрата доверия клиента
ВП3	помехи для самой организации
ВП4	дополнительные внутренние расходы
ВП5	помехи для третьих сторон, ведущих дела с организацией
ВП6	нарушение законов/предписаний
ВП7	неспособность выполнения договорных обязательств
ВП8	финансовые потери, связанные с непредвиденными случаями или ремонтом оборудования
ВП9	потеря клиентов, потеря поставщиков
ВП10	потеря конкурентного преимущества

В работе предлагается для определения ценности информационных объектов использовать механизм нечеткого логического вывода, который позволяет использовать качественные оценки естественного языка для получения количественных характеристик выходных переменных.

Нечетким множеством A в некотором непустом пространстве Y называется совокупность пар [8]:

$$A = \{(y, \mu_A(y))\}; y \in Y, \quad (3)$$

где μ_A: $Y \to [0, 1]$ – функция принадлежности (ФП), приписывающая каждому элементу степень его принадлежности к нечеткому множеству A. Функция принадлежности выражает субъективную возможность наличия свойств, позволяющих отнести элемент y к множеству A.

Каждому значению лингвистической переменной (ЛП) – переменной, значениями которой могут быть выраженные на естественном языке слова или словосочетания, – соответствует нечеткое множество с определенной ФП. Множество всех возможных значений ЛП называется терм-множеством.

В работе предложено определять ценность информационных объектов в соответствии с входными лингвистическими переменными: «Количество информационных объектов уровня критичности У», обрабатываемых в заданном сегменте сети организации, и «Количество возможных видов последствий нарушения ИБ» для данной совокупности объектов.

Предложено использовать систему нечеткого вывода для преобразования значений входных переменных в выходную переменную $Ц^{У}_{C_x}$ – ценность информационных объектов уровня критичности У, обрабатываемых в заданном сегменте сети C_x, – на основе использования нечетких правил продукции. Для этого система нечеткого вывода должна содержать базу продукционных правил, представленных в форме нечетких логических высказываний – посылок, в соответствии с которыми осуществляется нечеткий вывод заключений.

На рис. 1 приведена схема нечеткого вывода применительно к решению проблемы оценивания $Ц^{У}_{C_x}$.

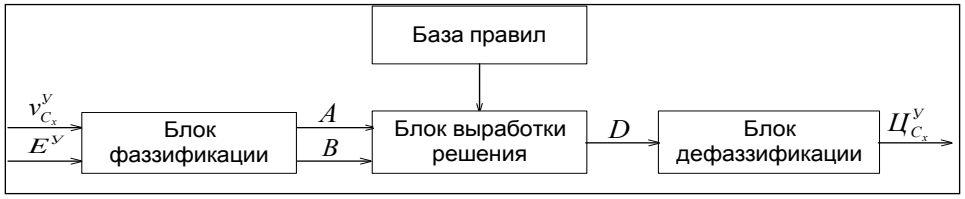

Рис. 1. Система нечеткого логического вывода параметра «Ценность информационных объектов уровня критичности У»

На рис. 1 $v^{У}_{C_x}$ – количество информационных объектов уровня критичности У, обрабатываемых в сегменте сети C_x, $x \in X$; $E^{У}$ – количество возможных видов последствий нарушения свойств ИБ для информационных объектов с уровнем критичности У, обрабатываемых в сегменте сети C_x (2); A – нечеткая ЛП, соответствующая входной переменной $v^{У}_{C_x}$; B – нечеткая ЛП, соответствующая входной переменной $E^{У}$; D – результат логического вывода нечеткого множества «Ценность информационных объектов уровня критичности У», обрабатываемых в сегменте сети C_x; $Ц^{У}_{C_x}$ – четкое значение параметра «*Ценность информационных объектов* уровня критичности У», обрабатываемых в сегменте сети C_x.

ФП входных и выходной ЛП строятся экспертом на основе сведений об особенностях обработки информации на конкретном объекте защиты.

На рис. 2 приведена функция принадлежности входной лингвистической переменной «Количество информационных объектов уровня критичности У», обрабатываемых в сегменте сети C_x. Областью определения ЛП является диапазон $\lfloor 0, V^{У} \rfloor$, где $V^{У} = max\ v^{У}_{C_x}$ для заданного уровня критичности информации У. Терм-множество, функции принадлежности определяются экспертом на основании анализа количества информационных объектов заданного уровня критичности, обрабатываемых во всех сегментах сети организации.

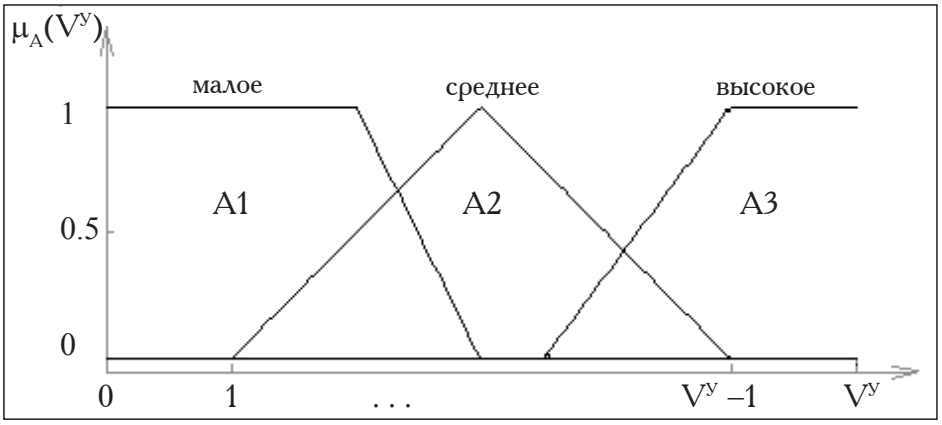

Рис. 2. ФП входной ЛП «Количество информационных объектов уровня критичности У», обрабатываемых в сегменте сети

На основе анализа критериев, приведенных в таблице 1, выбирается набор критериев, которые с точки зрения последствий для бизнеса целесообразно использовать в процессе получения оценки $Ц^{У}_{C_x}$. В качестве области определения второй входной переменной принимается диапазон $\lfloor 0,\ E^{У} \rfloor$, где $E^{У}$ – число критериев, приемлемых для определения ценности информационных объектов заданного уровня критичности У. Терм-множество и ФП лингвистической переменной «Количество возможных видов последствий нарушения ИБ» ИО уровня критичности У определяются в зависимости от $E^{У}$ и величины набора критериев для информации, обрабатываемой в сегменте C_x. На рис. 3 приведены функции принадлежности ЛП «Количество возможных видов последствий нарушения ИБ» для информационных объектов с уровнем критичности У.

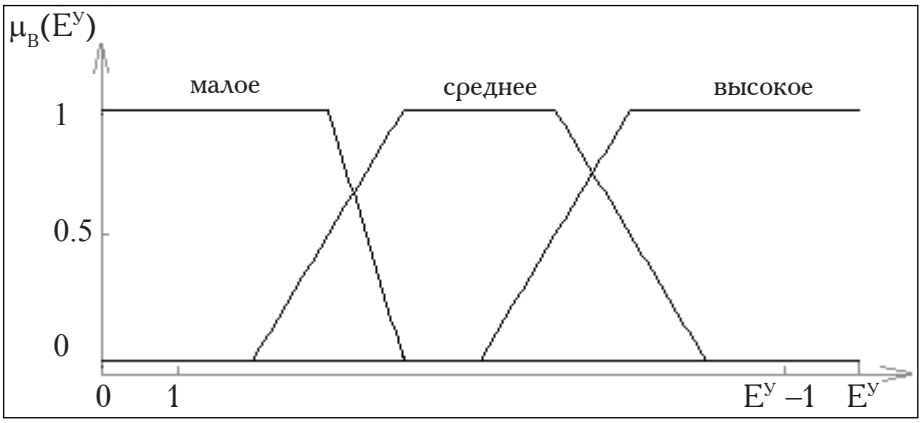

Рис. 3. ФП входной ЛП «Количество возможных видов последствий в результате нарушения ИБ» для информационных объектов с уровнем критичности У

Для выходной лингвистической переменной «Ценность информационных объектов уровней критичности *У*» (рис. 4) предлагается следующее терм-множество, определенное на основе анализа ГОСТ 27005-2010 [2]:

$$D = \left\{ \begin{array}{l} \text{«}\textit{пренебрежительно малая}\text{»}, \text{«}\textit{малая}\text{»}, \text{«}\textit{ниже средней}\text{»}, \text{«}\textit{средняя}\text{»}, \\ \text{«}\textit{выше средней}\text{»}, \text{«}\textit{высокая}\text{»}, \text{«}\textit{чрезвычайно высокая}\text{»} \end{array} \right\}.$$

При определении ценности информационных объектов разных уровней критичности очевидно должны использоваться различные наборы нечетких множеств, что отражается в продукционных правилах. Так, для ИО с уровнем критичности «Н» приемлемым набором является: «пренебрежительно малая», «малая», «ниже средней»; ценность ИО со средним уровнем критичности описывается неточными формулировками «ниже средней», «средняя», «выше средней»; лингвистические значения ценностей ИО с уровнем критичности «В» – «выше средней», «высокая», «чрезвычайно высокая». Область определения выходной переменной $Ц^{У}_{C_x} = [0, 1]$.

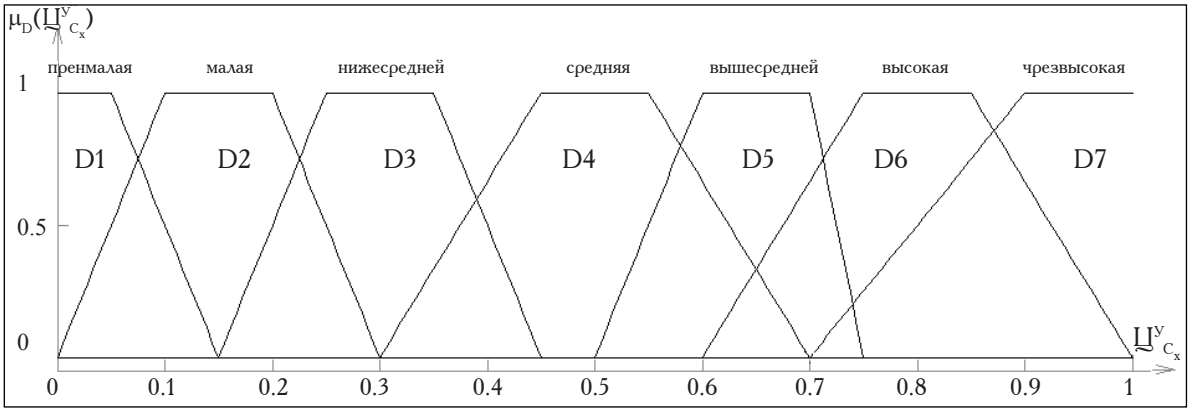

Рис. 4. Объединенные функции принадлежности выходной ЛП «Ценность информационных объектов уровней критичности У»

Лингвистическая модель – база правил – представляет множество нечетких правил, согласно которым нечеткие входные данные преобразуются в блоке принятия решений в нечеткое выходное значение переменной.

Разработанная база продукционных правил приводится в таблице 2.

Таблица 2. База продукционных правил для численной оценки ценности информационных объектов с высоким уровнем критичности

№	Атрибуты и их значения	Результат
П1	если $A = A1$ и $B = B1$, или $A = A1$ и $B = B2$, или $A = A2$ и $B = B1$, то	$D = D5$
П2	если $A = A1$ и $B = B3$, или $A = A2$ и $B = B2$, или $A = A3$ и $B = B1$, то	$D = D6$
П3	если $A = A2$ и $B = B3$, или $A = A3$ и $B = B2$, или $A = A3$ и $B = B3$, то	$D = D7$

В качестве алгоритма нечеткого вывода предлагается использовать алгоритм Мамдани, а дефаззификацию производить методом центров тяжести [8].

Идентификация информационных объектов позволяет определить, ИО каких категорий критичности обрабатываются в каждом сегменте сети организации, а также определить их количество. Перед экспертом ставится задача формирования терм-множеств и функций принадлежности на основе анализа *объективной* априорной информации об объекте защиты.

После того как в блоке дефаззификации были получены значения ценностей информационных объектов $Ц^{Н}_{C_x}$, $Ц^{С}_{C_x}$, $Ц^{В}_{C_x}$ уровней критичности «Н», «С», «В» соответственно, обрабатываемых в X сегментах сети, необходимо вычислить их сумму:

$$Ц_{\Sigma} = \sum_{n \in N} Ц^{H}_{C_n} + \sum_{m \in M} (Ц^{H}_{C_m} + Ц^{C}_{C_m}) + \sum_{l \in L} (Ц^{H}_{C_l} + Ц^{C}_{C_l} + Ц^{B}_{C_l}). \quad (4)$$

Затем производится нормирование полученных ранее значений $Ц^{У}_{C_x}$. Полученные значения могут быть далее использованы в расчетах рисков нарушения ИБ информационных объектов, обрабатываемых в сегментах $C_n{}^{H}$, $C_m{}^{C}$ и $C_l{}^{B}$ соответственно и ИС в целом, согласно методу, приведенному в [4]:

$$\overline{R_{C^H}} = \sum_{n=1}^{N} P^{U}_{C^{Н}_n} \cdot \frac{Ц_{C^{Н}_n}}{Ц_{\Sigma}},$$

$$\overline{R_{C^C}} = \sum_{m=1}^{M} P^{U}_{C^{С}_m} \cdot \frac{Ц_{C^{С}_m}}{Ц_{\Sigma}}, \quad (5)$$

$$\overline{R_{C^B}} = \sum_{l=1}^{L} P^{U}_{C^{В}_l} \cdot \frac{Ц_{C^{В}_l}}{Ц_{\Sigma}},$$

где $\frac{Ц_{C^{Н}_n}}{Ц_{\Sigma}}, \frac{Ц_{C^{С}_m}}{Ц_{\Sigma}}, \frac{Ц_{C^{В}_l}}{Ц_{\Sigma}}$ – относительные ценности информационных объектов, обрабатываемых в сегментах сети с наивысшими уровнями критичности информации «Н», «С», «В» соответственно.

Приводится вычислительный пример для топологии сети объекта защиты, приведенной в [4].

В процессе оценки ценности информационных объектов предлагается заполнение таблицы 3, в которой необходимо указать, в каком сегменте сети они обрабатываются. Варианты возможных последствий в результате нарушения ИБ информационных объектов, полученные в результате анализа [2], приведены ранее в таблице 1.

Таблица 3. Идентификация информационных объектов и возможных последствий нарушения информационной безопасности

Наименование объекта	Категория критичности	Месторасположение (сегмент)	Виды последствий нарушения ИБ
1. Сведения об обеспечении производства основным и вспомогательным оборудованием			
1.1. перечень основного и вспомогательного оборудования	С	C^{B}_{2}	ВП4; ВП8
1.2. план капитального и текущего ремонта оборудования	С	C^{B}_{2}	ВП4; ВП8
1.3. перспективный план обновления и переоснащения основного и вспомогательного оборудования	В	C^{B}_{2}	ВП4; ВП10
2. Сведения об обеспечении производства сырьем и вспомогательными материалами			
2.1. номенклатурный перечень поставщиков сырья (с указанием цен на сырье)	С	C^{C}_{5}	ВП3; ВП4; ВП9; ВП10
2.2. перечень поставщиков сырья, плохо зарекомендовавших себя	С	C^{C}_{5}	ВП3; ВП4; ВП10
2.3. перечень организаций, оказывающих транспортные услуги предприятию	Н	C^{C}_{5}	ВП3; ВП5
2.4. план организации входного контроля качества сырья и вспомогательных материалов	С	C^{B}_{3}	ВП3; ВП8
2.5. план утилизации технических отходов производства	Н	C^{B}_{2}	ВП3; ВП4
3. Сведения о производственном процессе			
3.1. сведения о производственных мощностях и объемах производства	С	C^{B}_{2}	ВП4; ВП10
3.2. технологический регламент об аналитическом контроле качества продукции по стадиям производства	С	C^{B}_{3}	ВП1; ВП3; ВП5; ВП9
3.3. технологический регламент об аналитическом контроле качества готовой продукции	С	C^{B}_{3}	ВП1; ВП2; ВП3; ВП5; ВП9
3.4. программа лабораторных исследовательских работ по выбору оптимальных химических добавок во вторсырье для улучшения качества готовой продукции	В	C^{B}_{3}	ВП3; ВП4; ВП5; ВП7; ВП9

3.5. план выпуска продукции	В	C^{B}_{2}	ВП1; ВП2; ВП3; ВП5; ВП7; ВП9
3.6. программа повышения эффективности производства по стадиям	С	C^{B}_{2}	ВП3; ВП4
3.7. технологический регламент участка декорирования и этикетирования тары	С	C^{C}_{6}	ВП1; ВП2; ВП4
3.8. сменный отчет	Н	C^{H}_{9}	ВП1; ВП3; ВП4
4. Сведения об особенностях хранения произведенной продукции			
4.1. технологический регламент о хранении произведенной готовой продукции	С	C^{C}_{7}	ВП2; ВП4; ВП5; ВП9
4.2. перспективный план расширения складского хозяйства	С	C^{C}_{7}	ВП3; ВП4; ВП7; ВП10
5. Сведения о потребителях произведенной продукции			
5.1. клиентская база	В	C^{B}_{1}	ВП1; ВП3; ВП4; ВП9; ВП10
5.2. прайс-лист произведенной продукции	В	C^{B}_{1}	ВП4; ВП10
5.3. перспективный план развития производства (расширение ассортимента выпускаемой продукции, освоение новых видов продукции)	В	C^{B}_{2}	ВП3; ВП4; ВП10
5.4. договора с потребителями продукции	В	C^{B}_{4}	ВП4; ВП6; ВП9; ВП10
6. Сведения, связанные с аудиторской проверкой предприятиями-клиентами			
6.1. план аудиторской проверки предприятиями-клиентами	С	C^{C}_{10}	ВП2; ВП3; ВП4
6.2. план подготовки к аудиторской проверке	С	C^{B}_{3}	ВП1; ВП2; ВП3; ВП4
7. Сведения о персонале и графике трудовой деятельности			
7.1. сведения о персонале и его квалификации	Н	C^{H}_{8}	ВП3; ВП6
7.2. сведения о графике трудовой деятельности	Н	C^{H}_{8}	ВП1; ВП4
7.3. программа повышения эффективности работы персонала	Н	C^{H}_{8}	ВП3; ВП4

На рис. 5, 6 представлены функции принадлежности входных лингвистических переменных для информационных объектов низкого уровня критичности.

Областью определения ЛП «Количество информационных объектов уровня критичности “Н”» является диапазон $\lfloor 0, V^{H} \rfloor$, где в соответствии с таблицей 3 $V^{H} = max\ (F_{n}, F_{m}, F_{l}) = 3$, для

$n \in N, m \in M, l \in L$. Анализ распределения ИО по сегментам сети показал, что в одном сегменте не обрабатывается более трех информационных объектов с низким уровнем критичности.

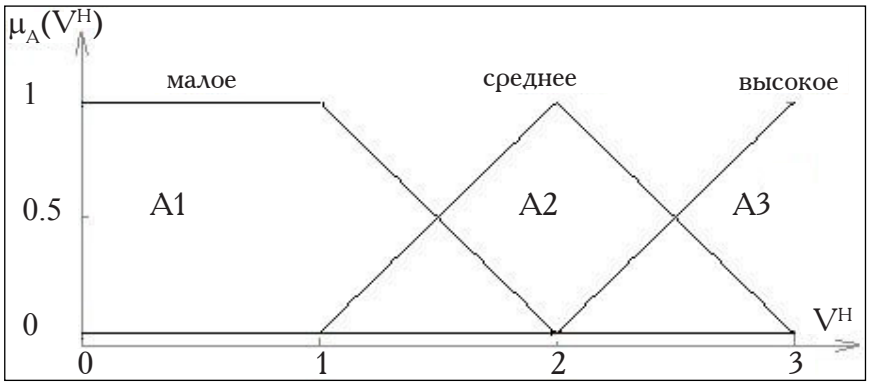

Рис. 5. ФП входной ЛП «Количество информационных объектов низкого уровня критичности», обрабатываемых в сегментах сети организации

Областью определения входной ЛП «Количество возможных видов последствий» является интервал, соответствующий действительной оси от 0 до 6, так как исходя из анализа таблицы 3 для информационных объектов с уровнем критичности «Н» число критериев, которые могут использоваться в качестве основы для получения численного значения $Ц^{H}_{C_x}$, составляет 6.

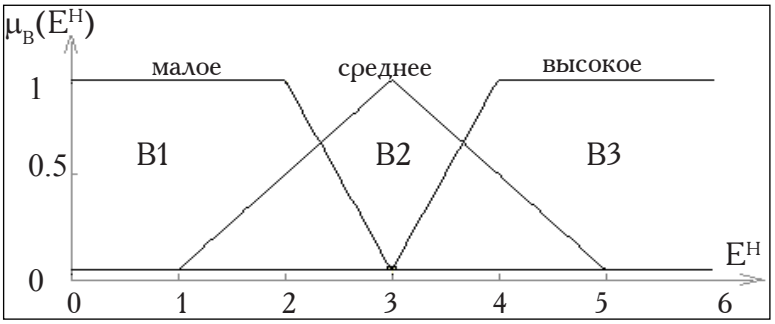

Рис. 6. ФП входной ЛП «Количество возможных видов последствий нарушения ИБ» для информационных объектов с низким уровнем критичности

Для информационных объектов с уровнем критичности «С» экспертом строятся функции принадлежности входных лингвистических переменных, приведенные на рис. 7, 8.

Анализ таблицы 3 показал, что максимальное «Количество информационных объектов среднего уровня критичности» составляет $V^{C} = max\ (G_m,\ G_l) = 4$, для $m \in M, l \in L$, таким образом, областью определения данной входной ЛП является диапазон $[0,4]$.

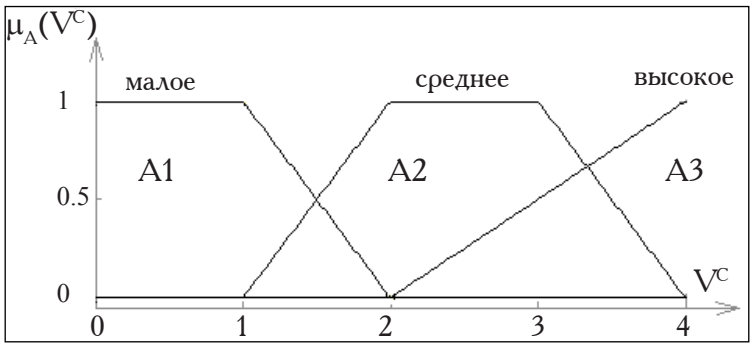

Рис. 7. ФП входной ЛП «Количество информационных объектов среднего уровня критичности», обрабатываемых в сегменте сети

Областью, на которой определена ЛП «Количество возможных видов последствий нарушения ИБ» для информационных объектов с уровнем критичности «С», является диапазон $[0, E^C]$, где $E^C = 8$.

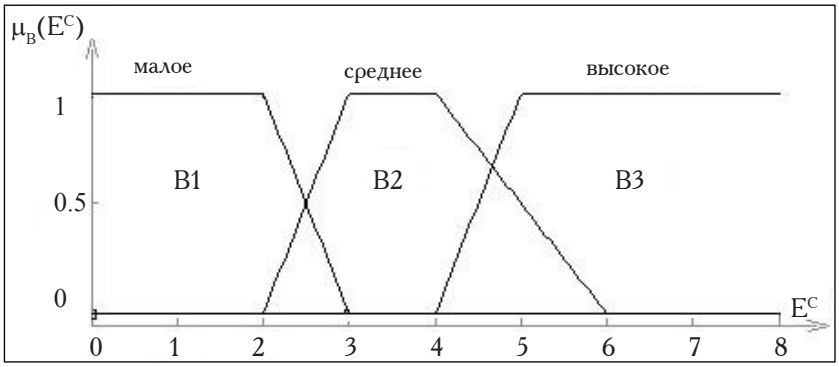

Рис. 8. ФП входной ЛП «Количество возможных видов последствий нарушения ИБ» для информационных объектов со средним уровнем критичности

На рис. 9, 10 приведены функции принадлежности входных ЛП, используемых для определения ценности информационных объектов категории критичности «В».

Областью определения входной ЛП «Количество информационных объектов уровня критичности "В"» является диапазон $[0, V^B]$, где $V^B = \max H_l = 3$, для $l \in L$.

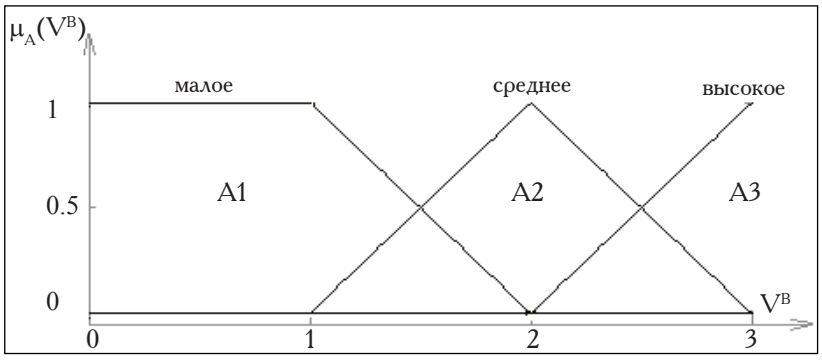

Рис. 9. ФП входной ЛП «Количество информационных объектов высокого уровня критичности», обрабатываемых в сегменте сети

В результате анализа таблицы 3 выявлено, что число критериев, которые могут использоваться в качестве основы для получения численного значения $\tilde{Ц}^B_{C_x}$, составляет 10, таким образом, областью определения соответствующей входной ЛП является интервал [0,10].

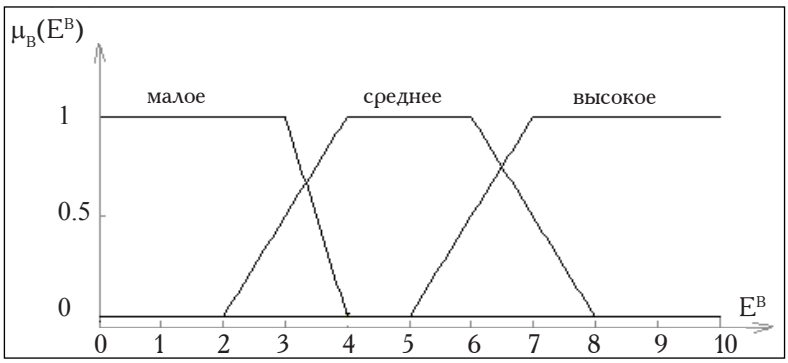

Рис. 10. ФП входной ЛП «Количество возможных видов последствий нарушения ИБ» для информационных объектов с высоким уровнем критичности

Сформируем базы правил системы нечеткого вывода для информационных объектов категорий критичности «Н», «С» с учетом определенных ранее допустимых термов выходной ЛП «Ценность информационных объектов» (таблицы 4, 5).

Таблица 4. База продукционных правил для численной оценки ценности информационных объектов с низким уровнем критичности

№	Атрибуты и их значения	Результат
П1	если $A = A1$ и $B = B1$, или $A = A1$ и $B = B2$, или $A = A2$ и $B = B1$, то	$D = D1$
П2	если $A = A1$ и $B = B3$, или $A = A2$ и $B = B2$, или $A = A3$ и $B = B1$, то	$D = D2$
П3	если $A = A2$ и $B = B3$, или $A = A3$ и $B = B2$, или $A = A3$ и $B = B3$, то	$D = D3$

Таблица 5. База продукционных правил для численной оценки ценности информационных объектов со средним уровнем критичности

№	Атрибуты и их значения	Результат
П1	если $A = A1$ и $B = B1$ или $A = A1$ и $B = B2$ или $A = A2$ и $B = B1$, то	$D = D3$
П2	если $A = A1$ и $B = B3$ или $A = A2$ и $B = B2$ или $A = A3$ и $B = B1$, то	$D = D4$
П3	если $A = A2$ и $B = B3$ или $A = A3$ и $B = B2$ или $A = A3$ и $B = B3$, то	$D = D5$

База продукционных правил для численной оценки ценности информационных объектов с уровнем критичности «В» приведена в таблице 2.

С учетом продукционных правил и согласно алгоритму нечеткого вывода Мамдани были получены (четкие) значения ценностей информационных объектов категорий критичности «Н», «С», «В». Значения, полученные в результате вычислительного эксперимента, были нормированы. В таблице 6 приведены значения относительных ценностей информационных объектов, обрабатываемых в сегментах сети.

Таблица 6. Относительные ценности информационных объектов с указанием сегментов сети

Номер сегмента сети	Ценность ИО категории критичности			Относительная ценность ИО
	«Н»	«С»	«В»	
1	-	-	0,8	0,1146
2	0,113	0,636	0,894	0,2354

3	0,245	0,636	0,72	0,2294
4	-	-	0,636	0,0911
5	0,113	0,5	-	0,0878
6	-	0,3	-	0,043
7	-	0,636	-	0,0911
8	0,3	-	-	0,0443
9	0,15	-	-	0,0215
10	-	0,3	-	0,043
	Итого: 6,979			1

Преимущества предложенного метода заключаются в том, что, во-первых, метод позволяет получить *численные оценки* параметра «*Ценность информационных объектов*», обрабатываемых в каждом из сегментов сети организации, с учетом *объективной* информации: *количество информационных объектов* заданного уровня критичности и *число* возможных *видов последствий* для бизнеса в случае нарушения свойств ИБ; во-вторых, эксперт в процессе определения ценности информационных объектов опирается на *сформированные в ГОСТ 27005-2010* [2] критерии оценивания информационных объектов; в-третьих, метод может быть использован в сети любой сложности, состоящей из множества локальных сетевых сегментов, в которых обрабатывается информация *разных уровней критичности*; в-четвертых, метод целесообразно использовать при численной оценке риска нарушения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004. — 392 с.
2. ГОСТ Р ИСО/МЭК 27005-2010 «Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
3. *Машкина И. В.* Идентификация угроз на основе построения семантической модели информационной системы // Вестник УГАТУ. Серия «Управление, вычислительная техника и информатика». Т. 11. № 1 (28). С. 208—214.
4. *Гузаиров М. Б., Машкина И. В., Степанова Е. С.* Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. 2011. № 2. С. 37—49.
5. *Stepanova E. S., Mashkina I. V., Guzairov M. B.* The numerical evaluation method of the infosecurity violation risk based on the creating of a threat model with the help of fuzzy cognitive maps // Proceedings of the 13th International Workshop on Computer Science and Information Technologies CSIT'2011. Vol. 1. Ufa State Aviation Technical University. 2011. P. 98—103
6. *Грушо А. А., Применко, Э. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности: учеб. пособие для для студентов высш. учеб. заведений. М.: Издательский центр «Академия», 2009. — 272 с.
7. *Торокин А. А.* Основы инженерно-технической защиты информации. М.: Ось-89, 1998. — 336 с.
8. *Рутковский Л.* Методы и технологии искусственного интеллекта: пер. с польск. М.: Горячая линия — Телеком, 2010. — 520 с.