А. А. Тимаков
Московский институт новых информационных технологий ФСБ России

О ВЫБОРЕ ТОЧЕК ВСТАВКИ ПОДСИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В МОДЕЛЬ ПРОТОКОЛА

Предлагаются рекомендации по выбору точек введения функциональной избыточности в автоматную модель протокола сетевого взаимодействия, направленные на повышение эффективности разработки защищенных автоматизированных информационных систем (АИС) путем реализации некоторых дополнительных доверенных алгоритмов защиты информации (ЗИ) на уровне сетевого протокола прикладного уровня.

Ввиду отсутствия в нашей стране некоторых современных СУБД (Oracle) и, соответственно, невозможности проверки их исходных кодов, поставляемых иностранными компаниями-разработчиками, возникает недоверие к встроенным в такое программное обеспечение механизмам ЗИ. Таким образом, в настоящее время является достаточно актуальной проблема адаптации зарубежных СУБД к использованию в защищенных АИС, функционирующих на территории Российской Федерации.

Одним из возможных подходов к решению обозначенной проблемы для систем, в которых предполагается наличие лишь внешнего нарушителя, является замена штатного серверного компонента прикладного протокола СУБД вновь разработанным компонентом, включающим наиболее важные функции исходного программного продукта и функции безопасности, реализуемые доверенными и сертифицированными алгоритмами защиты.

Положим, в рамках реализации указанного подхода удалось получить автоматную модель прикладного протокола, который используется СУБД (1, 4, 5). Далее ставится задача выбора точек (состояний) абстрактной модели протокола для вставки подсистем ЗИ, которые могут рассматриваться как надежные.

Для определения точек вставки экземпляров подсистемы ЗИ в модель протокола предлагается использовать методический аппарат, основанный на таблице покрытий в сочетании с двухпараметрическим алгоритмом нечеткого вывода.

На рис. 1 представлен фрагмент графа переходов неинициального автомата, описывающего работу некоторого протокола сетевого взаимодействия, где $S = [s_1, s_2 \ldots s_i]$ — множество состояний автомата; $T = [t_1, t_2, \ldots t_j]$ — множество входных символов автомата.

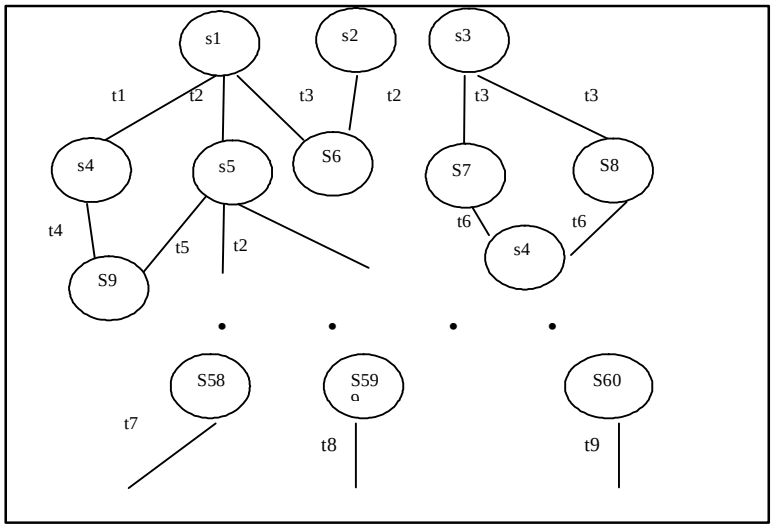

Рис. 1. Граф переходов неинициального автомата некоторого протокола

Обозначим через $K = [к_1, k_2. \ldots k_n]$ множество возможных путей прохождения сетевых пакетов в протокольной модели. Будем называть путь «благоприятным», если он описывает удачный

исход протокольной операции, и «тупиковым», если он соответствует некоторому событию, приведшему к неудачному завершению протокольной операции, например, обращение к несуществующему объекту базы данных, выявление недопустимого значения параметра и т. д.

Первоначально рекомендуется строить таблицу покрытия «благоприятных» путей состояниями конечного автомата (рис. 2), где символом g отмечены «благоприятные» пути, символом X помечены пути, которые перекрываются состоянием, указанным в заголовке столбца.

	Состояния								
Возможные пути прохождения сетевых пакетов			s_1	s_2	s_3	s_4	s_5	...	s_i
	7	k_1	X			X			
	7	k_2		X		X	X		
	7	k_3	X		X				X
		k_4					X		X
	7	k_5	X		X	X			
	7	k_6	X		X				
		...							
	7	k_n			X				

Рис. 2. Таблица покрытия «благоприятных» путей состояниями конечного автомата

Очевидно, допустимые для вставки некоторой подсистемы ЗИ сочетания состояний протокольного автомата должны покрывать все множество «благоприятных» путей автоматной модели протокола.

Пусть множество $X = \{X_1, X_2, ...X_n\}$ — множество всех сочетаний состояний протокольного автомата, которые обеспечивают покрытие всех «благоприятных» путей. Очевидно, $X_i \subset S$. Далее ставится задача определения такого элемента X_i множества X, который является наиболее подходящим с точки зрения внедрения в модель протокола подсистемы ЗИ.

Если для оценки эффективности использовать только один параметр — сложность внедрения подсистемы ЗИ, то задача становится тривиальной: из множества X выбирается подмножество X_i, включающее минимальное число состояний автомата. Однако такой подход отвергается в силу того, что большое значение имеет также и быстродействие конечной системы.

Оценку эффективности применения элементов множества X предлагается осуществлять на базе нечеткой логики с использованием двухпараметрического алгоритма (рис. 3).

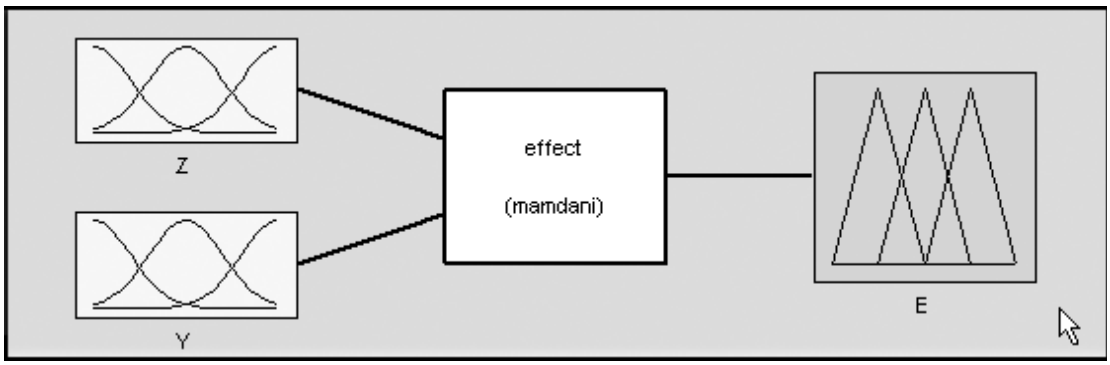

Рис. 3. Нечеткий вывод на основе двухпараметрического алгоритма

Основными этапами нечеткого вывода являются следующие [1].

1. *Ввод решающих правил в базу знаний* заключается в программировании базы знаний, т. е. в представлении ее в форме продукционных правил вида «ЕСЛИ… ТО», отражающих логические взаимосвязи входных лингвистических переменных с величиной риска. Эти правила формируются на основе общих закономерностей поведения исследуемой системы и позволяют «вложить» в механизм вывода логическую модель прикладного уровня.

2. *Задание функций принадлежности входных переменных* предполагает определение вида функций принадлежности для каждой из входных лингвистических переменных на оси возможных значений риска. Кроме этого, на данном этапе необходимо задать параметры выбранных функций принадлежности. Для выполнения этих процедур разработаны специализированные программы типа «Fuzzy logic», графический интерфейс которых существенно облегчает работу на этом этапе.

3. *Получение оценок входных переменных* является той процедурой, которая обеспечивает механизм вывода текущей информации, отражающей фактическое состояние защищенности исследуемой системы на данный момент времени. Для этого могут быть использованы оценки экспертов фактического состояния защищенности исследуемой системы. Оценки могут быть получены на основе заранее разработанных диагностических тестов, охватывающих различные аспекты проявления оцениваемых величин.

4. *Фазификация оценок входных переменных* представляет собой процедуру нахождения конкретных значений функций принадлежности, соответствующих полученным значениям оценок входных переменных.

5. *Агрегирование* является процедурой определения степени истинности условий по каждому из правил системы нечеткого вывода. Здесь значения функции принадлежности подвергаются преобразованиям типа нечеткая конъюнкция или нечеткая дизъюнкция в соответствии с продукционными правилами.

6. *Активизация заключений* представляет собой процедуру нахождения степени истинности каждого из заключений, входящих в продукционные правила. Активизация заключается в нахождении произведений весовых коэффициентов по каждому из правил и функций истинности условий, найденных на предыдущем этапе.

7. *Аккумулирование заключений* представляет собой процедуру нахождения функции принадлежности для каждой из выходных лингвистических переменных заданной совокупности правил нечеткого вывода. Результат аккумуляции для каждой лингвистической переменной определяется как объединение нечетких множеств одним из известных способов.

8. *Дефазификация* является процедурой нахождения четких значений выходных переменных, в наибольшей степени отвечающих входным данным и базе продукционных правил. Полученные значения выходных переменных могут быть использованы внешними по отношению к системе нечеткого вывода устройствами.

Введем следующие обозначения:

Z — входной параметр, значением которого является отношение числа «тупиковых» путей, охватываемых альтернативой X_i, к общему числу возможных путей $z \in U^{/}$, где $U^{/} = [0,1]$. Данный параметр характеризует степень охвата «тупиковых» путей.

Y — входной параметр, значение которого определяется как $\frac{m_i}{s}$, где m_i — длина множества X_i, а s — длина множества S. Положим $y \in U^{//}$, где $U^{//} = [0,1]$. Данный параметр характеризует сложность внедрения подсистемы ЗИ в модель протокола.

E — выходной параметр, характеризующий эффективность выбора альтернативы. Положим, $e \in U^{///}$, где $U^{///} = [0,1]$.

Для входных величин и эффективности выбора альтернативы зададим трехуровневые шкалы или нечеткие подмножества, соответствующие «низкому», «среднему» и «большому» значениям параметров:

$\tilde{A}^{/} = \{u^{/}, \mu_{A^{/}}(u^{/})\}$, $\tilde{B}^{/} = \{u^{/}, \mu_{B^{/}}(u^{/})\}$, $\tilde{C}^{/} = \{u^{/}, \mu_{C^{/}}(u^{/})\}$ — нечеткие подмножества множества $U^{/}$,

$\mu_{A^{/}}(u^{/}), \mu_{B^{/}}(u^{/}), \mu_{C^{/}}(u^{/})$ — функции принадлежности нечетких подмножеств $\tilde{A}^{/}, \tilde{B}^{/}, \tilde{C}^{/}$;

$\tilde{A}^{//} = \{u^{//}, \mu_{A^{//}}(u^{//})\}$, $\tilde{B}^{//} = \{u^{//}, \mu_{B^{//}}(u^{//})\}$, $\tilde{C}^{//} = \{u^{//}, \mu_{C^{//}}(u^{//})\}$ — нечеткие подмножества множества $U^{//}$,

$\mu_{A^{//}}(u^{//}), \mu_{B^{//}}(u^{//}), \mu_{C^{//}}(u^{//})$— функции принадлежности нечетких подмножеств $\tilde{A}^{//}, \tilde{B}^{//}, \tilde{C}^{//}$;

$\tilde{A}^{///} = \{u^{///}, \mu_{A^{///}}(u^{///})\}$, $\tilde{B}^{///} = \{u^{///}, \mu_{B^{///}}(u^{///})\}$, $\tilde{C}^{///} = \{u^{///}, \mu_{C^{///}}(u^{///})\}$— нечеткие подмножества множества $U^{///}$,

$\mu_{A^{///}}(u^{///}), \mu_{B^{///}}(u^{///}), \mu_{C^{///}}(u^{///})$— функции принадлежности нечетких подмножеств $\tilde{A}^{///}$, $\tilde{B}^{///}$, $\tilde{C}^{///}$.

Логические связи входных величин и эффективности выбора альтернатив представлены в таблице 1.

Таблица 1. Оценка эффективности выбора альтернативы по трехуровневым шкалам

	Степень охвата «тупиковых» путей		
Сложность внедрения подсистемы ЗИ	«Большая»	«Средняя»	«Низкая»
«Большая»	Н	Н	Н
«Средняя»	Н	С	С
«Низкая»	Н	С	Б

Положим, значимость всех логических правил вывода одинакова (все весовые коэффициенты продукционных правил равны единице).

Рассмотрим механизм получения оценок эффективности выбора альтернатив в представленном выше порядке.

1. Зададим продукционные правила, соответствующие таблице 1, следующим образом:

- ЕСЛИ степень охвата тупиковых путей «Большая» и сложность внедрения подсистемы ЗИ «Большая», ТО эффективность = «Низкая» (Н);
- ЕСЛИ степень охвата тупиковых путей «Большая» и сложность внедрения подсистемы ЗИ «Средняя», ТО эффективность = «Низкая» (Н);
- ЕСЛИ степень охвата тупиковых путей «Большая» и сложность внедрения подсистемы ЗИ «Низкая», ТО эффективность = «Низкая» (Н);
- ЕСЛИ степень охвата тупиковых путей «Средняя» и сложность внедрения подсистемы ЗИ «Большая», ТО эффективность = «Низкая» (Н);
- ЕСЛИ степень охвата тупиковых путей «Средняя» и сложность внедрения подсистемы ЗИ «Средняя», ТО эффективность = «Средняя» (С);
- ЕСЛИ степень охвата тупиковых путей «Средняя» и сложность внедрения подсистемы ЗИ «Низкая», ТО эффективность = «Средняя» (С);
- ЕСЛИ степень охвата тупиковых путей «Низкая» и сложность внедрения подсистемы ЗИ «Большая», ТО эффективность = «Низкая» (Н);
- ЕСЛИ степень охвата тупиковых путей «Низкая» и сложность внедрения подсистемы ЗИ «Средняя», ТО эффективность = «Средняя» (С);
- ЕСЛИ степень охвата тупиковых путей «Низкая» и сложность внедрения подсистемы ЗИ «Низкая», ТО эффективность = «Большая» (Б).

2. Для задания функций принадлежности воспользуемся пакетом Fuzzy Logic Toolbox системы MATLAB. Функции принадлежности для всех шкал зададим с помощью трапециевидных функций trampf (рис. 4). Параметры трапециевидных функций были определены опытным путем:

А. Параметры $\mu_{A'}(u')$: [-0.4, 0.1, 0.05, 0,35];

Параметры $\mu_{B'}(u')$: [0.15, 0.4, 0.5, 0.75];

Параметры $\mu_{C'}(u')$: [0.65, 0.85, 1, 1.35].

В. Параметры $\mu_{A''}(u'')$: [-0.5, -0.04, 0.04, 0.3];

Параметры $\mu_{B''}(u'')$: [0.15, 0.3, 0.4, 0.6];

Параметры $\mu_{C''}(u'')$: [0.5, 0.8, 1, 1.3].

С. Параметры $\mu_{A'''}(u''')$: [-0.36, -0.04, 0.04, 0.36];

Параметры $\mu_{B'''}(u''')$: [0.14, 0.46, 0.54, 0.86];

Параметры $\mu_{C'''}(u''')$: [0.69, 0.96, 1.04, 1.36].

На рис. 4 представлены функции принадлежности, определенные для подмножеств $\widetilde{A}'$,$\widetilde{B}'$,$\widetilde{C}'$,$\widetilde{A}''$,$\widetilde{B}''$,$\widetilde{C}''$.

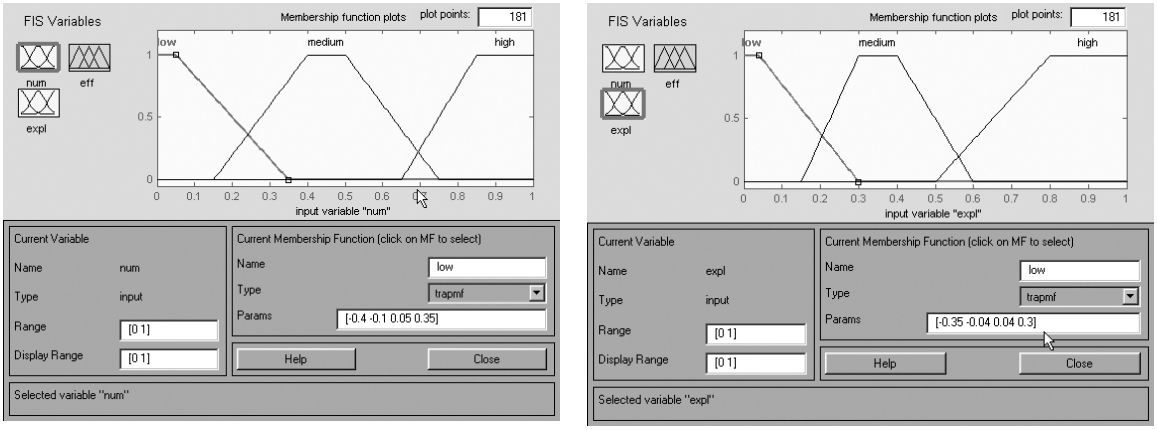

Рис. 4. Функции принадлежности на шкалах степени охвата «тупиковых» путей и сложности реализации подсистемы ЗИ

$\mu_{A'}(u^{I})$ — *трапециевидная функция* ***low*** *слева;*
$\mu_{B'}(u^{I})$ — *трапециевидная функция* ***medium*** *слева;*
$\mu_{C'}(u^{I})$ — *трапециевидная функция* ***high*** *слева;*
$\mu_{A''}(u^{II})$ — *трапециевидная функция* ***low*** *справа;*
$\mu_{B''}(u^{II})$ — *трапециевидная функция* ***medium*** *справа;*
$\mu_{C''}(u^{II})$ — *трапециевидная функция* ***high*** *справа.*

3. Предположим, для исследуемой альтернативы входной параметр Z принимает значение 0.3, а входной параметр Y — значение 0.2. Данные значения вводятся в окно Input графического интерфейса, представленного на рис. 5.

4. Далее определяются значения функций принадлежности для введенных оценок сложности внедрения подсистемы ЗИ и степени охвата «тупиковых» путей (левый и средний столбцы диаграмм на рис. 5 — этап фазификации).

5. На этом этапе ищется степень истинности условий по каждому из девяти правил, определенных в п. 1 (этап агрегирования):

$$d(\tilde{H}_1),\ d(\tilde{H}_2),\ d(\tilde{H}_3),\ d(\tilde{H}_4),\ d(\tilde{H}_5),\ d(\tilde{H}_6),\ d(\tilde{H}_7),\ d(\tilde{H}_8),\ d(\tilde{H}_9).$$

Учитывая, что в качестве связки между условиями используется функция «И», процедура агрегирования сводится к выбору минимального значения функций истинности, определенных на предыдущем этапе (результат агрегирования отражается в виде горизонтальных проекций на правый столбец диаграмм на рис. 5):

$$d(\tilde{H}_1)=\min\ \mu_{C'}(u^{I}),\ \mu_{B''}(u^{II})$$
$$d(\tilde{H}_2)=\min\ \mu_{C'}(u^{I}),\ \mu_{C''}(u^{II})$$
$$d(\tilde{H}_3)=\min\ \mu_{C'}(u^{I}),\ \mu_{A''}(u^{II})$$
$$d(\tilde{H}_4)=\min\ \mu_{B'}(u^{I}),\ \mu_{C''}(u^{II})$$
$$d(\tilde{H}_5)=\min\ \mu_{B'}(u^{I}),\ \mu_{B''}(u^{II})$$
$$d(\tilde{H}_6)=\min\ \mu_{B'}(u^{I}),\ \mu_{A''}(u^{II})$$
$$d(\tilde{H}_7)=\min\ \mu_{A'}(u^{I}),\ \mu_{C''}(u^{II})$$
$$d(\tilde{H}_8)=\min\ \mu_{A'}(u^{I}),\ \mu_{B''}(u^{II})$$
$$d(\tilde{H}_9)=\min\ \mu_{A'}(u^{I}),\ \mu_{A''}(u^{II})$$

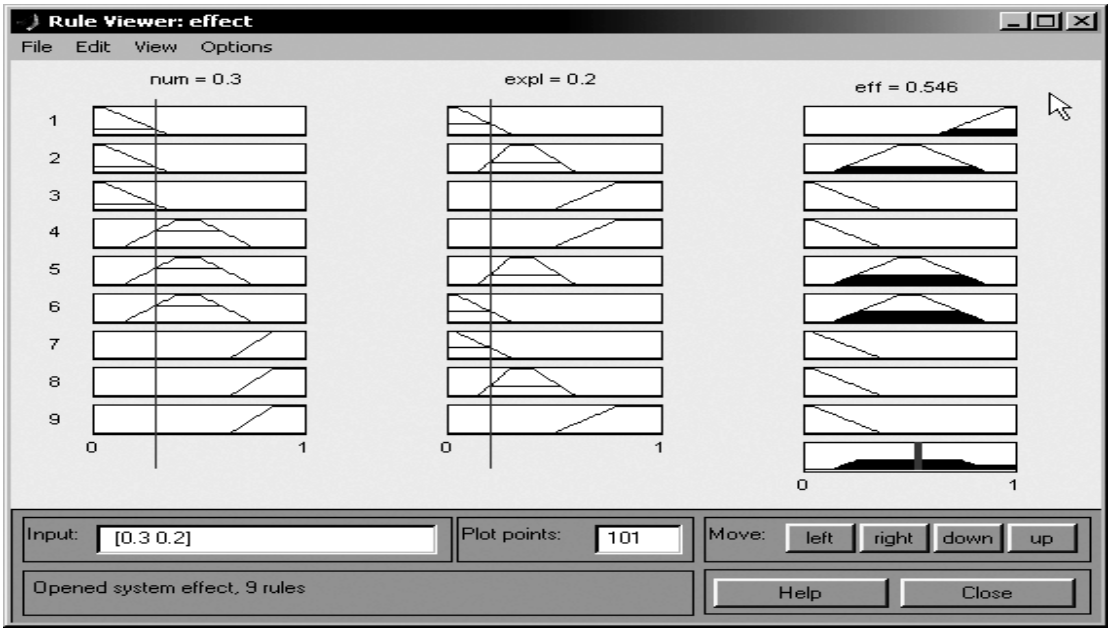

Рис. 5. Значения истинности для введенных оценок входных переменных

Входной параметр Z (num) обладает значением 0.3.

Входной параметр Y (expl) обладает значением 0.2.

Значения функций принадлежности нечетких множеств, соответствующие полученным оценкам входных переменных, представлены горизонтальными проекциями на левый и центральный столбцы диаграмм.

Значения степени истинности условий по каждому из продукционных правил системы нечеткого вывода представлены горизонтальными проекциями на правый столбец диаграмм.

Результирующее значение выходной величины — «центр тяжести» ступенчатой функции, представленной нижней диаграммой в правом столбце.

6. Поскольку было принято, что все продукционные правила имеют вес, равный единице, степень истинности для термов выходной переменной равна степени истинности условий, определенных на предыдущем этапе.

7. Аккумулирование заключений представляет собой процедуру нахождения результирующей функции принадлежности для всех термов функции эффективности выбора альтернативы. Результат аккумулирования определяется как объединение нечетких множеств и представляется в виде ступенчатой функции (нижний график в правом столбце на рис. 5).

8. Дефазификация определяет результирующее значение выходной величины как «центр тяжести» ступенчатой функции, полученной на предыдущем этапе, который в данном примере равен 0.546. Результат дефазификации равен искомому значению эффективности.

На рис. 6 представлена поверхность нечеткого вывода для заданных шкал. Из указанного рисунка видно, что значение эффективности убывает по каждой из входных переменных.

Таким образом, перебором всех элементов множества X, вычисляются оценочные значения эффективности выбора каждой из возможных альтернатив. Альтернативы, обладающие равными оценками, считаются равнозначными, в этом случае выбор конкретной альтернативы может осуществляться на основе субъективных предпочтений.

Повышение точности алгоритма вычисления оценки эффективности выбора альтернативы видится в переходе от трехуровневых шкал к пятиуровневым шкалам или к шкалам, обладающим большим числом уровней.

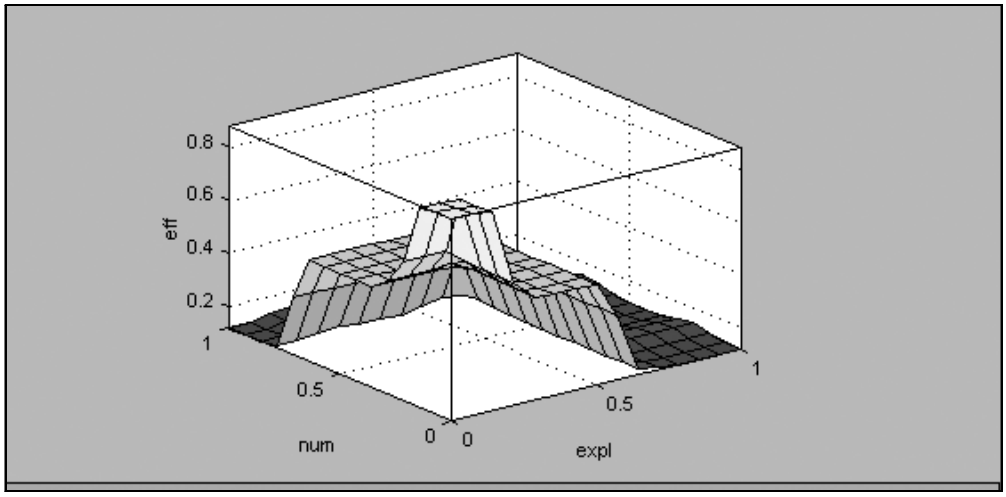

Рис. 6. Поверхность нечеткого вывода для заданных шкал

СПИСОК ЛИТЕРАТУРЫ

1. *Тимаков А. А., Кузнецов М. В.* Построение автоматов сетевых протоколов. Автомат ORACLE LISTENER — компонента протокола сетевого взаимодействия Net8. М., 2005. С. 125–132.
2. *Балашов П. А., Безгузиков В. П., Кислов Р. И.* Оценка рисков информационной безопасности на основе нечеткой логики // http://www.nwaktiv.ru/teztstat2/index.html.
3. *Блюмин С. Л., Шуйкова И. А.* Математические методы принятия решений. Липецк, 1999.
4. *Saleh K., Boujarwab A.* Communications software reverse engineering. A semi-automatic approach // Journal of Information and Software Technology. 1996. № 38. P. 379–390.
5. *Choi T. Y.* A sequence method for protocol construction Proc: Sixth IFIP International Workshop on Protocol Specification, Testing and Verification (June 1986). P. 9/1–9/18.