электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056

Модель оценки риска информационной безопасности сети VANET на основе теории нечетких множеств

Моёров А.С., студент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Бельфер Р.А., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

Введение.

Одной из перспективных технологий беспроводных самоорганизующихся сетей связи являются автомобильные сети связи VANET (Vehicular Ad-hoc Networks). Автомобильные беспроводные самоорганизующиеся сети VANET предназначены для повышения эффективности и безопасности дорожного движения. В настоящее время при поддержке индустрии, государственных и академических институтов в мире выполняются несколько научно-исследовательских проектов, направленных на разработку и принятие стандартов таких автомобильных сетей. Основные цели использования VANET можно разделить на три группы [1]:

1. помощь водителю (навигация, предотвращение столкновений и смена полос);
2. информирование (об ограничении скорости или зоне ремонтных работ);
3. предупреждение (послеаварийные, о препятствиях или состоянии дорог).

Для всех беспроводных самоорганизующихся сетей связи одной из важных является задача обеспечения информационной безопасности. Хотя VANET является одной из технологий самоорганизующихся сетей, однако вопросы обеспечения информационной безопасности для неё специфичны. Причиной является характерная для VANET высокая динамическая природа сети, частая смена топологии сети, непостоянные пользователи сетью и кратковременные связи [1]. Другая особенность VANET заключается в большом числе взаимодействующих объектов в течение короткого времени. Настоящая работа посвящена анализу особенностей обеспечения информационной безопасности сети VANET.

1. Особенности угроз информационной безопасности.

Приведём характерные типы нарушителей, которые могут быть причиной угроз информационной безопасности в сети VANET [1].

- *Недобросовестные водители.* Хотя мы полагаем, что большинство водителей-участников сети VANET будут добропорядочными и будут соблюдать правила безопасного взаимодействия с другими участниками сети, некоторые водители могут пытаться извлечь максимальную личную выгоду. Например, возможны такие ситуации, когда водитель может послать ложную информацию, чтобы направить трафик по другому маршруту и освободить себе путь.
- *Мошенники, использующие прослушивание.* Цель этих злоумышленников – сбор информации о водителях и использование этой информации для анализа поведения водителей и потоков трафика.
- *Инсайдеры.* Этот тип злоумышленников включает работников автомобильных компаний, производящих установку и настройку модулей, используемых для построения сети VANET.
- *Преступники.* Эти злоумышленники обладают большими финансовыми возможностями по созданию инструментов для реализации угроз информационной безопасности в сетях VANET.

Ниже приводятся особенности угроз информационной безопасности сети VANET на основе анализа зарубежных работ.

1. Для защиты от угроз информационной безопасности в VANET характерна необходимость учёта противоречивости требовании к гарантии подлинности источника сообщений и приватности. Чтобы гарантировать, что определённые узлы именно те, за кого себя выдают, необходимо, чтобы все сообщения отправлялись после уверенности в подлинности источника сообщения. Однако это может привести к возможности определения местоположения автомобиля. Приватность — важное требование безопасности, потому что автомобиль — сугубо персональное средство передвижения. Итак, система обеспечения безопасности должна быть спроектирована таким образом, чтобы позволять анонимный обмен сообщениями, но при этом допускать возможность идентификации узлов в некоторых случаях, например, при расследовании инцидентов.

2. Высокая мобильность и частая смена пользователей может быть причиной угрозы отказа в обслуживании. В автомобильных сетях VANET узлы движутся со скоростью в десятки километров в час. Число соседних узлов меняется с высокой скоростью, преобладают разовые и кратковременные взаимодействия между

пользователями. В результате может создаваться большой поток сообщений между пользователями, что может вызвать перегрузки и угрозу отказа в обслуживании.

3. Высокая вероятность всплеска нагрузки при аварии и других причинах (пробки) может вызвать перегрузки, следствием которых является угроза отказа в обслуживании.

4. Условия возникновения ситуаций в сети VANET, указанные в пунктах 2 и 3, могут быть причиной возникновения не только угрозы отказа в обслуживании, но и угрозы нарушения качества обслуживания.

5. Для сети VANET характерна угроза получения недостоверных данных, необходимых в аварийных ситуациях. Это вызвано зависимостью сети VANET от GPS. Любые ошибки в этих системах находят отражение в функционировании VANET сети.

2. Методология оценки риска на основе теории нечетких множеств

Перечисленные выше особенности угроз транспортных сетей связи VANET и в связи с невозможностью точной количественной оценки последствий реализаций угроз требуют применения метода оценки рисков на основе теории нечётких множеств. Этот математический аппарат позволяет определить количественные характеристики субъективным методом. Цель данной работы – предложение модели анализа угроз на основе теории нечетких множеств для транспортных сетей связи стандарта VANET.

Основные этапы схемы нечеткого вывода представлены на рисунке 1 [3].

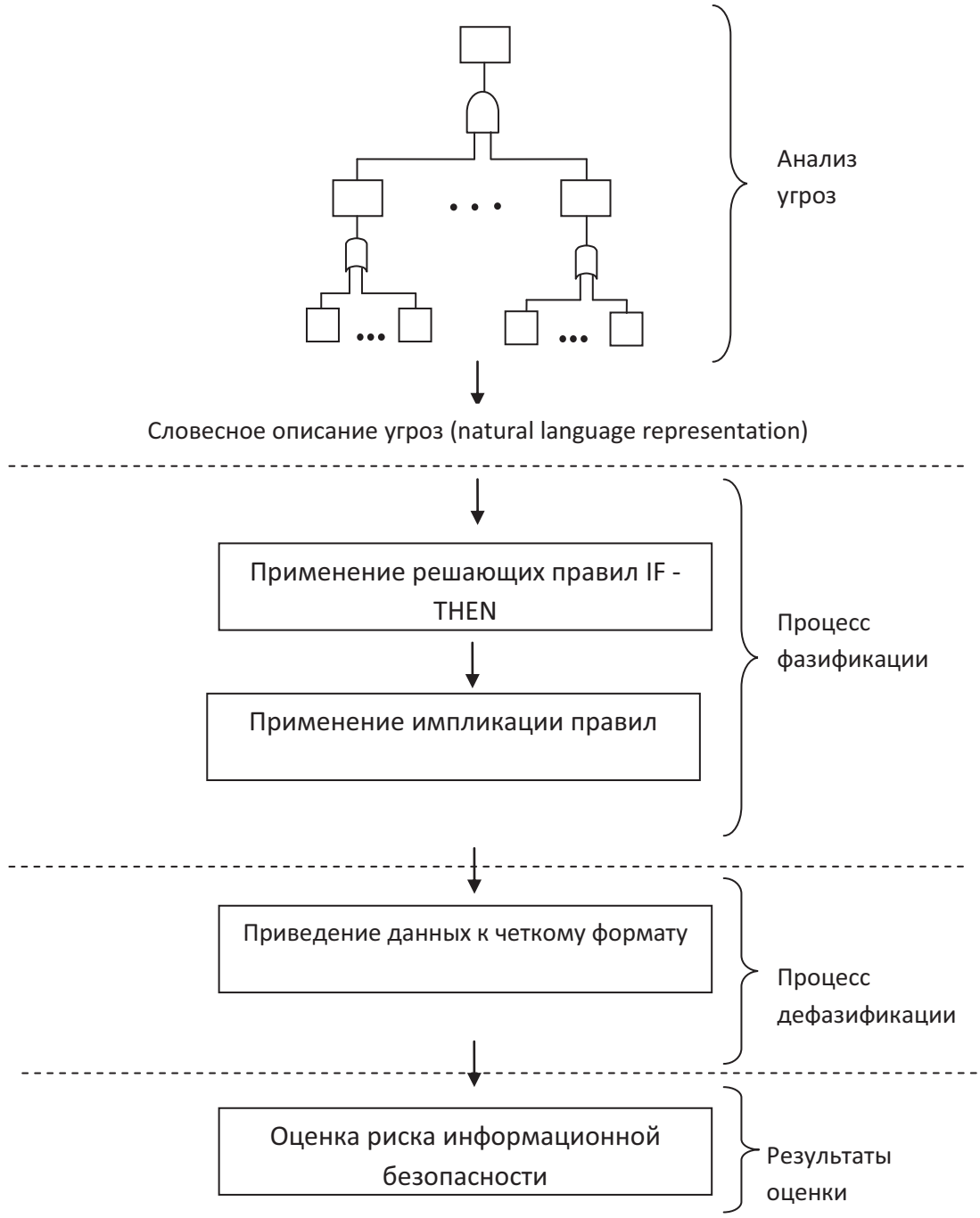


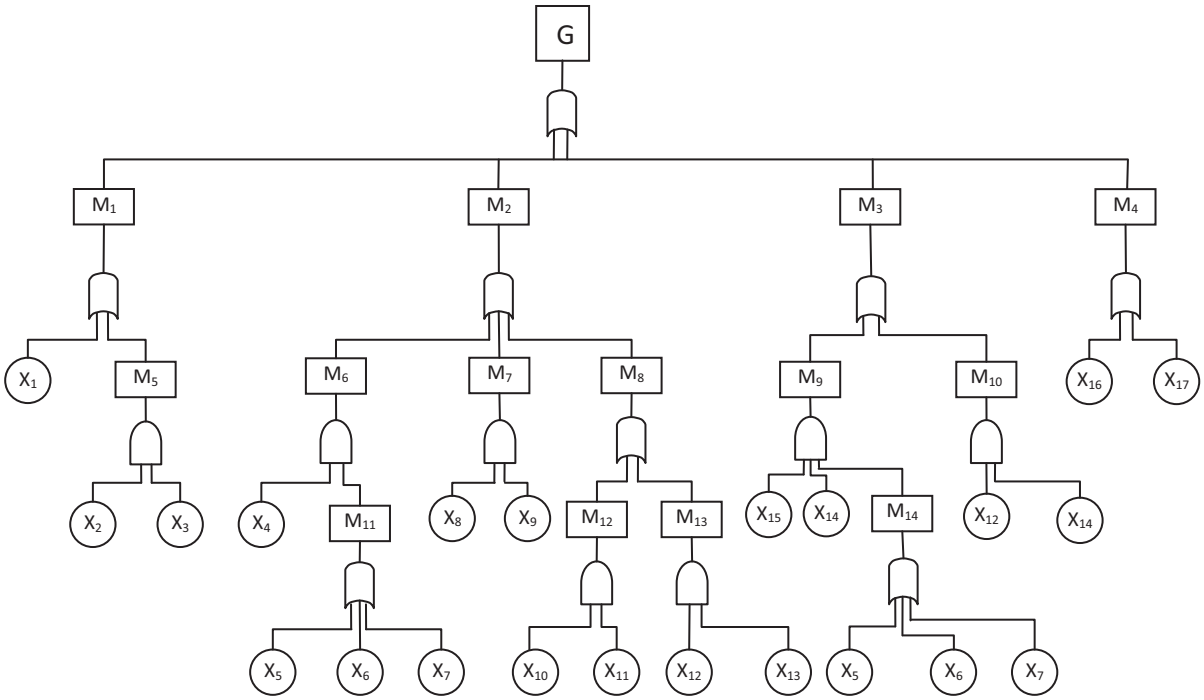
Рис. 1. Модель системы оценки риска на основе теории нечетких множеств

2.1. Описание угроз информационной безопасности

Важным этапом оценки риска информационной безопасности является анализ возможных угроз. В данной работе предлагается построение дерева угроз (attack tree). Вершина этого дерева – конечная цель нарушителя. После определения цели следует анализ сети и выявление условий и событий, ведущих к реализации атаки. В соответствии с логическими связями между событиями, они могут быть соединены либо конъюнкцией либо дизъюнкцией. Дизъюнкция используется в случае, если вышележащее событие

реализуется, когда выполняется хотя бы одно из нижележащих условий. Соответственно конъюнкция используется, если для реализации вышележащего необходимо выполнение всех нижележащих событий.

Дерево атак для угрозы «Утечка приватной информации» [2] приведено на рисунке 2.



G – утечка приватной информации
M_1 – прямое воздействие
M_2 – прослушивание
M_3 – кража
M_4 – незаконное разглашение
M_5 – мошенничество
M_6 – прослушивание на физическом уровне
M_7 – прослушивание на MAC-уровне
M_8 – прослушивание на прикладном уровне
M_9 – физическая кража
M_{10} – кража с использованием вредоносного ПО
M_{11} – установка прослушивающего беспроводного устройства
M_{12} – подслушивание псевдонима
M_{13} – запуск прослушивающего ПО
M_{14} – кража автомобиля
X_1 – допрос
X_2 – поиск уязвимостей в механизме аутентификации
X_3 – подделка ID

X_4 – демонтаж устройства защиты от прослушивания
X_5 – сервис-провайдер автомобилей
X_6 – разрушение противоугонной системы автомобиля
X_7 – использование ошибок владельца
X_8 – анализ протокола взаимодействия на уязвимости
X_9 – сброс конфигурации
X_{10} – доступ к передатчику
X_{11} – анализ слабостей механизма присвоения псевдонимов
X_{12} – преодоления межсетевого экрана сети
X_{13} – знание слабостей механизмов защиты беспроводных сетей
X_{14} – дешифрование зашифрованных файлов
X_{15} – нарушение работы функции очищения памяти
X_{16} – получение данных от третьих лиц
X_{17} – утечка от официальных источников

Рис. 2. Дерево атак для реализации угрозы “Утечка приватной информации”

Сценарий атаки – это набор действий злоумышленника, которые привел к реализации его угрозы «Утечка приватной информации». Другими словами, $S_i = (X_{i1}, X_{i2}, \ldots, X_{in})$. В этом случае вероятность реализации конкретного сценария равна произведению входящих в него событий:

$$P(S_i) = P(X_1)*P(X_2)*...*P(X_n) \quad (1)$$

Применим правила булевой алгебры для получения всех возможных сценариев реализации рассмотренной атаки [2]:

$M_1 = X_1 \vee M_5 = X_1 \vee (X_2 \wedge X_3)$

$M_2 = M_6 \vee M_7 \vee M_8 = (X_4 \wedge M_{11}) \vee (X_8 \wedge X_9) \vee (M_{12} \vee M_{13}) = X_4 \wedge (X_5 \vee X_6 \vee X_7) \vee (X_8 \wedge X_9) \vee (X_{10} \wedge X_{11} \vee X_{12} \wedge X_{13})$

$M_3 = M_9 \vee M_{10} = (X_{15} \wedge X_{14} \wedge M_{14}) \vee (X_{12} \vee X_{14}) = (X_{15} \wedge X_{14} \wedge (X_5 \vee X_6 \vee X_7)) \vee (X_{12} \wedge X_{14})$

$M_4 = X_{16} \vee X_{17}$

$G = M_1 \vee M_2 \vee M_3 \vee M_4 = X_1 \vee (X_2 \wedge X_3) \vee X_4 \wedge (X_5 \vee X_6 \vee X_7) \vee (X_8 \wedge X_9) \vee (X_{10} \wedge X_{11} \vee X_{12} \wedge X_{13}) \vee (X_{15} \wedge X_{14} \wedge (X_5 \vee X_6 \vee X_7)) \vee (X_{12} \wedge X_{14}) \vee X_{16} \vee X_{17} = X_1 \vee X_2 \wedge X_3 \vee X_4 \wedge X_5 \vee X_4 \wedge X_6 \vee X_4 \wedge X_7 \vee X_8 \wedge X_9 \vee X_{10} \wedge X_{11} \vee X_{12} \wedge X_{13} \vee X_{15} \wedge X_{14} \wedge X_5 \vee X_{15} \wedge X_{14} \wedge X_6 \vee X_{15} \wedge X_{14} \wedge X_7 \vee X_{12} \vee X_{14} \vee X_{16} \vee X_{17}.$

Таким образом, были получены 14 различных сценариев реализации угрозы «Утечка приватной информации». Сценарии перечислены в таблице 1.

Таблица 1

Сценарии реализации атаки «Утечка приватной информации»

S_1	X_1	**S_8**	X_{12}, X_{13}
S_2	X_2, X_3	**S_9**	X_5, X_{14}, X_{15}
S_3	X_4, X_5	**S_{10}**	X_6, X_{14}, X_{15}
S_4	X_4, X_6	**S_{11}**	X_7, X_{14}, X_{15}
S_5	X_4, X_7	**S_{12}**	X_{12}, X_{14}
S_6	X_8, X_9	**S_{13}**	X_{16}
S_7	X_{10}, X_{11}	**S_{14}**	X_{17}

2.2. Введение функций принадлежности

В теории нечетких множеств основным понятием является понятие нечеткого множества, которое характеризуется своей функцией принадлежности. Наиболее часто используют 2 типа функций принадлежности – треугольная и трапециевидная (рисунок 3) [4].

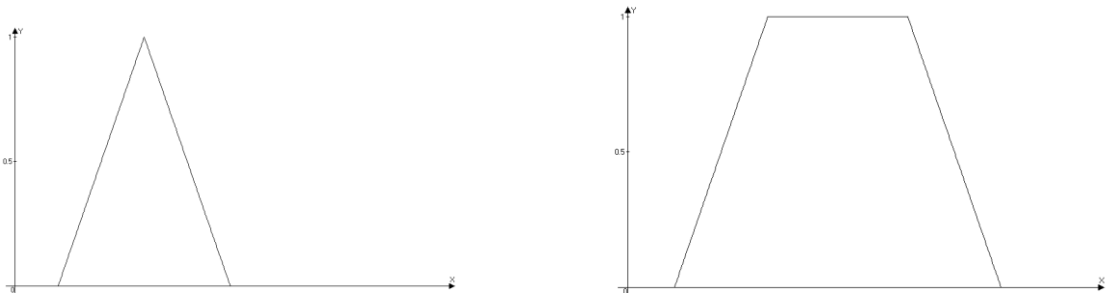
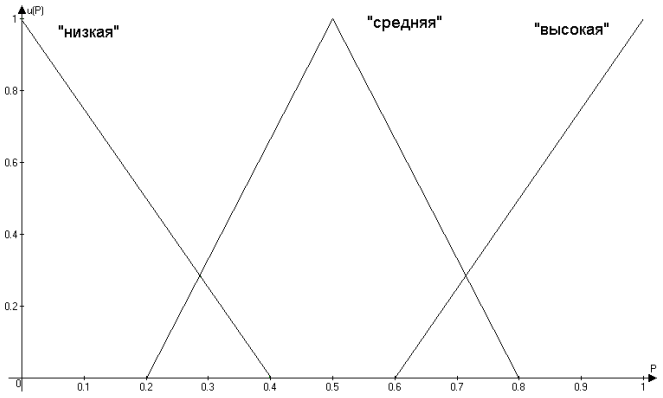
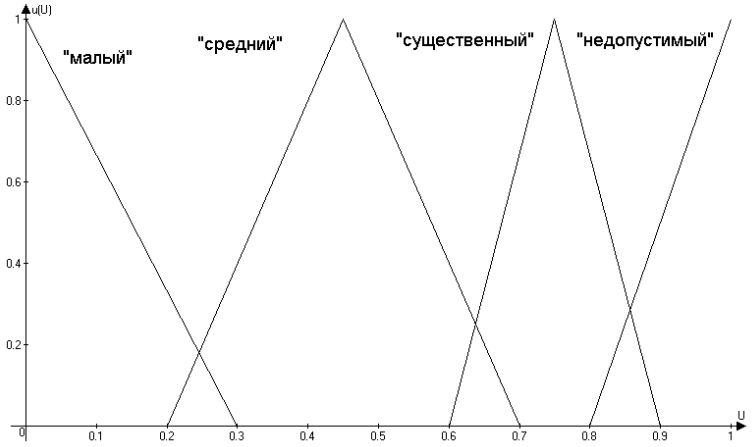


Рис. 3. Функции принадлежности

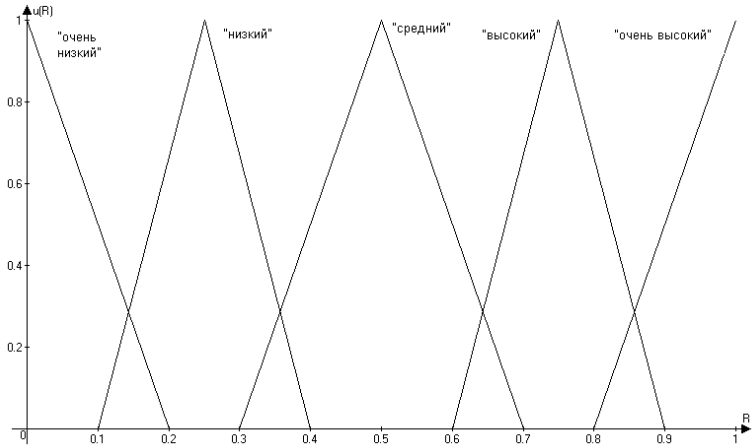
Предлагается ввести три нечетких множества: вероятность реализации атаки, ущерб от реализации атаки и риск информационной безопасности. Функции принадлежности данных трех нечетких множеств приведены на рисунке 4.



а)



б)



в)

Рис. 4. Функции принадлежности введенных нечетких множеств

а) «вероятность реализации угрозы»

б) «ущерб от реализации угрозы»

в) «риск»

Далее необходимо получить экспертные оценки вероятностей и ущерба от реализации атак X_i и затем по формуле (1) вычислить вероятности реализации сценариев S_i.

2.3. Фазификация

Этап фазификации заключается в применении решающих правил к входным данным (оценкам экспертов) и служит для конвертации четких входных данных к нечеткому формату. Связь входных и выходных величин представлена в таблице 2.

Таблица 2

Связь входных и выходных величин

Вероятность реализации угрозы	Ущерб от реализации угрозы				
	Незначит.	Малый	Средний	Существенный	Недопустимый
Низкая	1	1	2	3	4
Средняя	1	2	3	4	5
Высокая	2	3	4	5	5

Продукционные правила целиком соответствуют данной таблице: например, первое правило звучит следующим образом: *«Если В «низкая» и У «незначительный», то Р «очень низкий»».* Остальные правила составлены аналогичным образом. Далее для каждого значения вероятности реализации атаки x_i и ущерба от реализации атаки y_i находятся так называемые уровни отсечения:

$$\alpha_1 = B_1(x_i) \wedge У_1(y_i)$$

...

$$\alpha_{15} = B_3(x_i) \wedge У_5(y_i)$$

Затем необходимо определить усеченные функции принадлежности для переменной выхода – в нашем случае это лингвистическая переменная «риск информационной безопасности»:

$$P^*_1 = \alpha_1 \wedge P_1(z)$$

...

$$P^*_{15} = \alpha_{15} \wedge P_{15}(z)$$

Производится композиция полученных усеченных функций и получается итоговая функция принадлежности:

$$\mu_и(z) = P(z) = P^*_1 \vee \ldots \vee P^*_{15}.$$

2.4. Дефазификация

На данном этапе определяется чёткое значение выходной переменной – значение риска информационной безопасности (например, с использованием центроидного метода – определение центра тяжести полученной кривой)[5]:

$$R = \frac{\int_0^1 R \cdot \mu_z(R) \cdot dR}{\int_0^1 \mu_z(R) \cdot dR}$$

3. Пример расчета риска информационной безопасности

Проведем расчет четкого значения выходной переменной «риск информационной безопасности», используя описанный выше алгоритм. По результатам проведённого ранее опроса вероятность реализации сценария 1 **P = 0.4,** а ущерб от реализации угрозы **U = 0.3.**

Этап фазификации.

На этом этапе необходимо определить значения функций принадлежности входных лингвистически переменных в точках P = 0.4 и U = 0.3:

$$\mu_{в1}(0.4) = 0,\ \mu_{в2}(0.4) = 0.66,\ \mu_{в3}(0.4) = 0$$

$$\mu_{у1}(0.3) = 0,\ \mu_{у2}(0.3) = 0.67,\ \mu_{у3}(0.3) = 0.4,\ \mu_{у4}(0.3) = 0,\ \mu_{у5}(0.3) = 0$$

Таблица 3

Уровни отсечения для каждого правила

№ Правила	$B_i(P)$	$У_i(U)$	α_i	**№ Правила**	$B_i(P)$	$У_i(U)$	α_i
1	0	0	0	**9**	0.66	0.4	0.4
2	0	0	0	**10**	0.66	0	0
3	0	0	0	**11**	0	0	0

4	0	0.67	0	**12**	0	0	0
5	0	0.67	0	**13**	0	0	0
6	0.66	0.67	0.66	**14**	0	0	0
7	0.66	0.4	0.4	**15**	0	0	0
8	0.66	0.4	0.4				

Далее применяя операцию максимума, получаем итоговую функцию принадлежности:

$\mu_{и}(R) = \{0.66 \wedge P_1(R)\} \vee \{0.4 \wedge P_2(R)\} \vee \{0.4 \wedge P_3(R)\} \vee \{0.4 \wedge P_4(R)\}$.

Результат объединения приведен на рисунке 5.

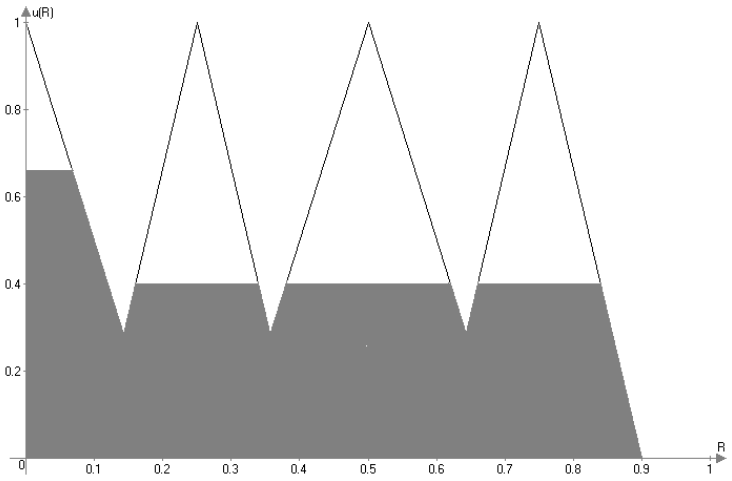


Рис. 5. Итоговая функция принадлежности для выходной переменной «риск информационной безопасности»

Этап дефазификации.

Определяем чёткое значение выходной переменной – значение риска информационной безопасности с использованием центроидного метода – определение центра тяжести полученной кривой:

$$R = \frac{\int_0^1 R \cdot \mu_{и}(R) \cdot dR}{\int_0^1 \mu_{и}(R) \cdot dR} = 0.45$$

4. Выводы

Применение теории нечетких множеств даёт возможность очень гибкой оценки рисков и ущерба от реализации различных угроз ИБ. Учитывая актуальность и новизну данного подхода для транспортных сетей связи VANET, планируется продолжить исследования в области анализа риска ИБ в этой сети связи. Данная модель оценки риска информационной безопасности может быть использована также для других сетей связи.

Список литературы

1. А.С.Моёров, Р.А. Бельфер. Безопасность самоорганизующихся автомобильных сетей VANET, журнал «Электросвязь», номер 3, 2012 г., стр. 28-29. УДК: 621.391 + 004.58
2. Dandan.Ren, Suguo.Du, Haojin Zhu. A Novel Attack Tree Based Assessment Aproach for Location Privacy Preservation in the VANETs, IEEE ICC, no. 8, 2011.
3. Fakariah Hani Mohd Ali, Wan Mohd Nadzir Hadzril Wan Ismail. Network Security Threat Assessment Model Based on Fuzzy Algorithm, IEEE, no. 11, 2011.
4. Maxwell Dondo, A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System, Defence R&D Canada – Ottawa, Technical Memorandum DRDC Ottawa TM 2007-090, May 2007.
5. В.Б.Щербаков, С.А. Ермаков. Безопасность беспроводных сетей: стандарт IEEE 802.11, сс.117-140, –М: РадиоСофт, 2010.