

АНАЛИЗ ЗАВИСИМОСТИ УРОВНЯ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ СВЯЗИ ОТ ЭКСПЕРТНЫХ ДАННЫХ ПРИ РАСЧЕТАХ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ НЕЧЕТКИХ МНОЖЕСТВ

*Бельфер Рувим Абрамович, кандидат технических наук, доцент
Калюжный Денис Александрович
Тарасова Дарья Владимировна*

В работе анализируется влияние экспертных данных на оценку уровня риска угроз информационной безопасности (ИБ) в сетях связи при расчете значений риска этих угроз с помощью модели нечетких множеств. В качестве таких данных рассматривались функции принадлежности, терм-множество, продукционные правила. Расчет производился на примерах нескольких угроз фрода в сети VoIP стандарта сигнализации SIP.

Ключевые слова: информационная безопасность, фрод, угроза, нечеткое множество, оценка риска, уровень риска угрозы, протокол установления сеанса связи (сигнализации), вероятность реализации угрозы, ущерб, функция принадлежности, терм-множество, экспертная оценка; лингвистическая переменная

ANALYSIS OF DEPENDENCE OF RISK LEVEL OF SAFETY OF COMMUNICATION NETWORKS ON EXPERT DATA DURING CALCULATIONS WITH THE USE OF A MODEL OF THE ILLEGIBLE SETS

*Ruvim Belfer, Ph.D, Associate Professor
Denis Kalyuzhnyy
Daria Tarasova*

This paper analyzes the impact of expert data on the risk assessment of information security (IS) threats in communication networks when calculating the risk of information security threats with a model of fuzzy sets. As these data were considered membership function, term set, production rules. The calculation is made on the examples of several threats of fraud in the VoIP network signaling standard SIP.

Keywords: information security; fraud; threat; fuzzy set; risk; risk level of threat; protocol SIP (Session Initialization Protocol likelihood of occurrence; impact; membership function; term set; linguistic variable.

Введение

Согласно стандарту международного союза электросвязи (ITU-T) E.408 [ITU-T. Recommendation E.408. Telecommunication Network Security Requirement, 2004] количественная оценка риска угрозы ИБ в сети связи, определяется двумя характеристиками – вероятностью угрозы и последствием при реализации этой угрозы (т.е. ущербом). На основании значений риска угроз ИБ производится их ранжирование по уровню риска угрозы ИБ. Это позволяет при проектировании, испытаниях и эксплуатации сети наибольшее вни-

мание уделять обеспечению защиты от угроз ИБ с наиболее высокими уровнями риска.

В основу некоторых работ по вычислению риска угрозы ИБ в сети связи положена модель с использованием теории нечетких множеств и нечеткой логики [1]. К ним относится работа [2] безотносительно конкретной сети связи, а также работы относительно следующих сетей связи:

- беспроводной сети стандарта IEEE 802.11 [3];
- транспортная сеть VANET [4].

Для этой модели расчета характерно использование многих данных нечетких множеств, по-

лученных с помощью субъективных оценок экспертным методом.

В настоящей работе на основе модели с использованием теории нечетких множеств и нечеткой логики приводится определение количественной характеристики риска угрозы ИБ в сети связи. Практическим результатом использования полученных значений риска угроз ИБ является их ранжирование [3,5]. Это дает возможность принять первоочередные меры по усилению защиты от угроз ИБ с наиболее высокими уровнями риска.

Задача настоящей работы показать возможную погрешность определения риска нескольких угроз ИБ и соответственно результатов ранжирования уровней риска этих угроз, вызванную субъективностью некоторых экспертных данных в модели с использованием теории нечетких множеств и нечеткой логики. Анализ подлежат влияние только тех экспертных данных, которые используются этим математическим аппаратом при определении риска угрозы ИБ. Этому посвящен раздел 2 статьи.

В разделе 1 настоящей статьи приводится пример расчета риска одной из угроз ИБ, в основу которого положена методика в работе [3], используемая для беспроводных сетей стандарта IEEE 802.11.

1. Расчет риска угрозы ИБ сети связи

Определение риска угрозы ИБ на основе теории нечетких множеств состоит из следующих последовательных этапов: описание угроз ИБ сети, формализация лингвистической переменной вероятности реализации угрозы, формализация лингвистической переменной ущерба реализации угрозы ИБ, фазификация, дефазификация, оценка риска угрозы ИБ.

На первом этапе необходимо определить угрозы ИБ сети, для которых производится оценка риска. В настоящей работе примем угрозы фрода в сигнализации по протоколу SIP сети передачи речи и данных поверх IP (Voice over IP, VoIP) [6]. Примером могут быть некоторые угрозы фрода, приведенные в работах [7,8]: мошенничество с подпиской, перехват и кража подписки, мошеннический обход, манипуляция сигнальными сообщениями, использование уязвимостей в учрежденческих станциях и в системе голосовой почты, распределение дохода между операторами и др.

На основе модели с использованием теории нечетких множеств и нечеткой логики для примера определим значение риска одной из угроз фрода в сети сигнализации SIP.

1.1. Формализация лингвистических переменных вероятности реализации угрозы ИБ и ущерба угрозы ИБ

Как было отмечено выше, в настоящей работе при определении риска угрозы ИБ и соответствующего уровня риска угрозы ИБ анализу подлежат влияние на возможную погрешность только тех экспертных данных, которые используются аппаратом теории нечетких множеств и нечеткой логики. По этой причине влияние экспертных данных при определении вероятностей при реализации угроз и ущерба при реализации угроз не рассматривается. Для приведенного ниже примера расчета риска рассмотрим угрозу фрода с соответствующими параметрами: вероятность реализации $P=0.83$ и ущерб при реализации $U=0.4$.

Для анализа риска угрозы фрода на основе модели с использованием теории нечетких множеств и нечеткой логики необходимо формализовать лингвистические переменные вероятности реализации угрозы или ущерба. Нечетким множеством (fuzzy set) \tilde{A} на универсальном множестве U называется совокупность пар $(\mu_A(u), u)$, где $\mu_A(u)$ - степень принадлежности элемента $u \in U$ к нечеткому множеству. Степень принадлежности - это число из диапазона $[0, 1]$. Чем выше степень принадлежности, тем в большей мере элемент универсального множества соответствует свойствам нечеткого множества. Лингвистической переменной (linguistic variable) называется переменная, значениями которой могут быть слова или словосочетания некоторого естественного или искусственного языка. Терм-множеством (term set) называется множество всех возможных значений лингвистической переменной. Для лингвистической переменной вероятности реализации угрозы фрода для настоящего примера определим следующие терм-множества: низкая, средняя и высокая. Для лингвистической переменной ущерба при реализации угрозы фрода для настоящего примера определим следующее терм-множество: незначительный, малый, средний, существенный, недопустимый.

Термом (term) называется любой элемент терм-множества. В теории нечетких множеств терм формализуется нечетким множеством с помощью функции принадлежности. Нечеткое множество характеризуется функцией принадлежности, которая позволяет вычислить степень принадлежности произвольного терм-множества (в данном примере – вероятности реализации угрозы фрода, ущерба фрода) универсальному множеству.

Таблица 1. Связь вероятности и ущерба угроз с риском ИБ

Вероятность 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

Для каждого термина множества лингвистических переменных вероятности реализации угрозы фрода и лингвистических переменных ущерба при реализации угрозы фрода производится построение функций принадлежности термина. В основу может быть положен широко используемый метод последовательных интервалов, использующий опрос экспертов. Пример использования такого метода приведен в работе [3]. Для построения функции принадлежности определенного термина по результатам опроса экспертов составляется два графика размытости смежных с ним термов. Используя эти графики, формируется искомая функция принадлежности.

В работе [3] приведен также метод построения функций принадлежности термина для риска безопасности угрозы. Для получения значения выходной переменной риск угрозы ИБ используем алгоритм нечеткого вывода Мамдани. Определим в настоящем примере для лингвистической переменной риска безопасности угрозы фрода следующие терм-множества: низкий, умеренный, средний, высокий, экстремальный.

1.2. Фазификация

Этап фазификации заключается в применении решающих правил к входным данным (оценки экспертов вероятности и ущерба угрозы) и служит для конвертации четких входных данных к нечеткому формату. Связь входных и выходных (риск угрозы) величин представлена в таблице 1.

Из приведенного примера следует, что использование экспертного метода при выборе числа множеств в терм-множестве и формировании функций принадлежности термина является субъективным. Использование этих данных может быть причиной недостоверной оценки риска угрозы фрода, их ранжирования и как следствия принятие первоочередных мер по усилению защиты от угроз не с самым высоким уровнем риска ИБ.

Зададим продукционные правила с единичными весовыми коэффициентами, соответствующие таблице 1, следующим образом.

Функции принадлежности трех нечетких множеств (вероятности угрозы, ущерба от реализации угрозы и риска угрозы ИБ) приведены соответственно на рис.2, рис.3, рис.4 соответственно.

1. If (Вероятность is Низкая) and (Ущерб is Малый) then (Риск is Низкий) (1)
2. If (Вероятность is Низкая) and (Ущерб is Средний) then (Риск is Умеренный) (1)
3. If (Вероятность is Низкая) and (Ущерб is Существенный) then (Риск is Средний) (1)
4. If (Вероятность is Низкая) and (Ущерб is Недопустимый) then (Риск is Высокий) (1)
5. If (Вероятность is Низкая) and (Ущерб is Незначительный) then (Риск is Низкий) (1)
6. If (Вероятность is Средняя) and (Ущерб is Незначительный) then (Риск is Низкий) (1)
7. If (Вероятность is Средняя) and (Ущерб is Малый) then (Риск is Умеренный) (1)
8. If (Вероятность is Средняя) and (Ущерб is Средний) then (Риск is Средний) (1)
9. If (Вероятность is Средняя) and (Ущерб is Существенный) then (Риск is Высокий) (1)
10. If (Вероятность is Средняя) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)
11. If (Вероятность is Высокая) and (Ущерб is Незначительный) then (Риск is Умеренный) (1)
12. If (Вероятность is Высокая) and (Ущерб is Малый) then (Риск is Средний) (1)
13. If (Вероятность is Высокая) and (Ущерб is Средний) then (Риск is Высокий) (1)
14. If (Вероятность is Высокая) and (Ущерб is Существенный) then (Риск is Экстремальный) (1)
15. If (Вероятность is Высокая) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)

Рис. 1. Заданные продукционные правила

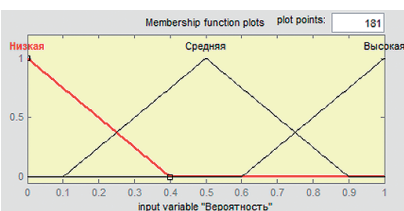


Рис. 2. Вероятность угрозы

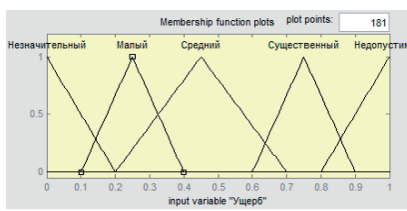


Рис. 3. Ущерб от реализации угрозы

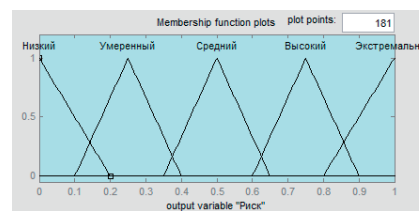


Рис. 4. Риск угрозы

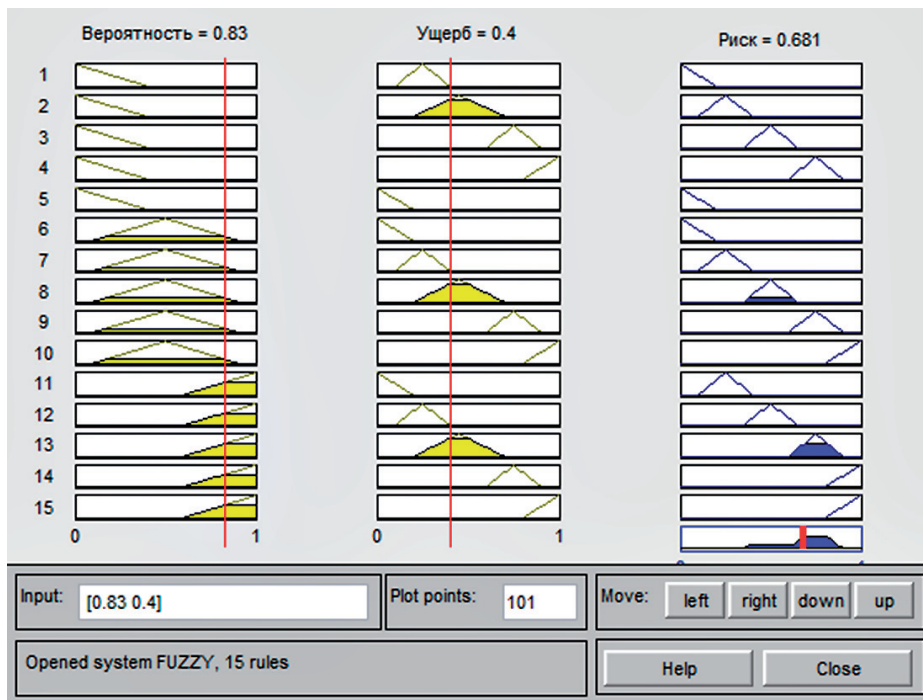


Рис. 5. Графическая интерпретация алгоритма нечеткого вывода Мамдани

1.3. Дефазификация

Определяется четкое значение выходного значения параметра риска анализируемой угрозы фрода (например, центридным методом, как центр тяжести для кривой $H_i(z)$):

$$R_0 = \frac{\int_0^1 R \mu_{\Sigma}(R) dR}{\int_0^1 \mu_{\Sigma}(R) dR} = 0.68$$

Для автоматизации процесса получения четких значений «риска информационной безопасности» по алгоритму нечеткого вывода Мамдани можно воспользоваться пакетом Fuzzy Logic Toolbox системы разработки MATLAB.

На рисунке 5 представлена графическая интерпретация алгоритма нечеткого вывода Мамдани для рассматриваемого примера угрозы ($P=0,83$ и $U=0,4$) и полученный результат риска, равный 0.681.

2. Уровни риска угроз фрода при различных экспертных данных

В настоящем разделе производится определение уровней риска шести угроз фрода со следующими характеристиками вероятности реализации угроз P и ущерба U :

- 1. $P= 0,83, U=0,4$; 2. $P= 0,6, U=0,7$; 3. $P= 0,41, U=0,5$;
- 4. $P= 0,2, U=0,61$; 5. $P= 0,6, U=0,35$; 6. $P= 0,72, U=0,8$.

Для этого рассчитываются значения риска этих угроз ИБ при разных составах экспертных данных теории множественных чисел - функции принадлежности, терм-множества и продукционных правил. Расчет производится для четырех вариантов состава этих экспертных данных.

Вариант 1. Функции принадлежности, терм-множества и продукционные правила те же, при которых производился расчет для приведенного примера ($P= 0,83, U=0,4$).

Вариант 2. Состав аналогичен варианту 1, кроме измененных функций принадлежности. На рис. 6-8 приведены эти функции принадлежности.



Рис. 6. Вероятность реализации угрозы

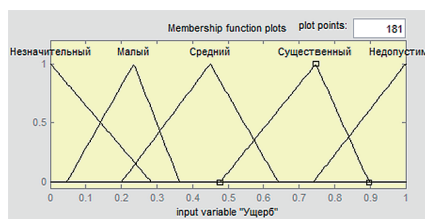


Рис. 7. Ущерб от реализации угрозы

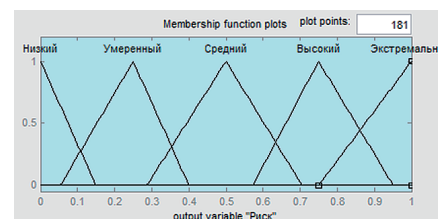


Рис. 8. Риск угрозы ИБ

Таблица 2. Связь вероятности и ущерба угроз с риском ИБ

Вероятность угрозы	Ущерб от реализации угрозы, У			
	Малый	Средний	Существенный	Недопустимый
Низкая	1	1	3	4
Средняя	1	2	3	4
Выше среднего	2	3	3	4
Высокая	2	3	4	4



Рис. 9. Вероятность реализации угрозы

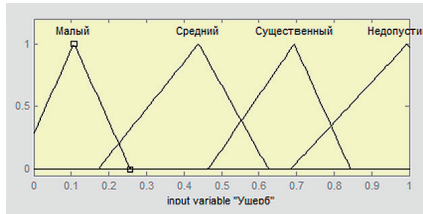


Рис. 10. Ущерб от реализации угрозы

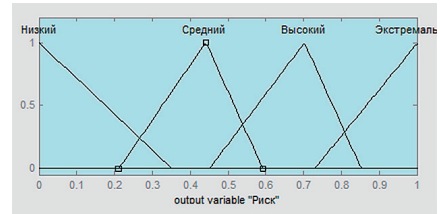


Рис. 11. Риск угрозы ИБ

Вариант 3. Состав аналогичен варианту 1, кроме измененных терм-множеств.

Новые терм - множества

Вероятность – Низкая, Средняя, Выше среднего, Высокая.

Ущерб- Малый, Средний, Существенный, Недопустимый.

Риск - Низкий, Средний, Высокий, Экстремальный.

Связь входных (Вероятность угрозы, Ущерб от реализации угрозы) и выходных (Риск угрозы) величин представлена в таблице 2.

На рис. 9-11 представлены новые функции принадлежности.

Вариант 4. Состав аналогичен варианту 1, кроме измененных продукционных правил.

В таблице 3 приведены измененные по сравнению с табл.1 экспертные данные связи вероятности и ущерба угроз с риском ИБ

В таблице 4 приведены для каждого варианта состава экспертных данных теории множеств чисел (функции принадлежности, термножества и продукционных правил) результаты ранжирования всех шести анализируемых угроз

Таблица 3. Связь вероятности и ущерба угроз ИБ с риском

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

1. If (Вероятность is Низкая) and (Ущерб is Малый) then (Риск is Низкий) (1)
2. If (Вероятность is Низкая) and (Ущерб is Средний) then (Риск is Средний) (1)
3. If (Вероятность is Низкая) and (Ущерб is Существенный) then (Риск is Средний) (1)
4. If (Вероятность is Низкая) and (Ущерб is Недопустимый) then (Риск is Высокий) (1)
5. If (Вероятность is Низкая) and (Ущерб is Незначительный) then (Риск is Низкий) (1)
6. If (Вероятность is Средняя) and (Ущерб is Незначительный) then (Риск is Умеренный) (1)
7. If (Вероятность is Средняя) and (Ущерб is Малый) then (Риск is Умеренный) (1)
8. If (Вероятность is Средняя) and (Ущерб is Средний) then (Риск is Высокий) (1)
9. If (Вероятность is Средняя) and (Ущерб is Существенный) then (Риск is Экстремальный) (1)
10. If (Вероятность is Средняя) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)
11. If (Вероятность is Высокая) and (Ущерб is Незначительный) then (Риск is Умеренный) (1)
12. If (Вероятность is Высокая) and (Ущерб is Малый) then (Риск is Средний) (1)
13. If (Вероятность is Высокая) and (Ущерб is Средний) then (Риск is Высокий) (1)
14. If (Вероятность is Высокая) and (Ущерб is Существенный) then (Риск is Экстремальный) (1)
15. If (Вероятность is Высокая) and (Ущерб is Недопустимый) then (Риск is Экстремальный) (1)

Рис. 12. Заданные продукционные правила

Таблица 4. Ранги риска угроз ИБ для каждого варианта

Ранг риска угроз ИБ	Вариант 1	Вариант 2	Вариант 3	Вариант 4
1	$R_6(0,72;0,8) = 0,801$	$R_6(0,72;0,8) = 0,796$	$R_6(0,72;0,8) = 0,761$	$R_2(0,6;0,7) = 0,931$
2	$R_2(0,6;0,7) = 0,75$	$R_1(0,83;0,4) = 0,76$	$R_2(0,6;0,7) = 0,678$	$R_6(0,72;0,8) = 0,923$
3	$R_1(0,83;0,4) = 0,681$	$R_2(0,6;0,7) = 0,759$	$R_1(0,83;0,4) = 0,6$	$R_3(0,41;0,5) = 0,751$
4	$R_3(0,41;0,5) = 0,5$	$R_3(0,41;0,5) = 0,529$	$R_4(0,2;0,61) = 0,573$	$R_1(0,83;0,4) = 0,75$
5	$R_5(0,6;0,35) = 0,401$	$R_5(0,6;0,35) = 0,458$	$R_5(0,6;0,35) = 0,529$	$R_4(0,2;0,61) = 0,622$
6	$R_4(0,2;0,61) = 0,397$	$R_4(0,2;0,61) = 0,42$	$R_3(0,41;0,5) = 0,47$	$R_5(0,6;0,35) = 0,551$

фрода в порядке от наибольшего к наименьшему риску угрозы ИБ. Обозначим через $R_i(P;U)$ риск i -й угрозы фрода с вероятностью реализации P и ущербом U . Тогда для угрозы, при которой производился расчет в разделе 1 статьи, $R_1(0,83;0,4) = 0,681$. Уровень риска угроз ИБ определяется диапазоном значений риска ИБ. Для представленных вариантов они будут разные. Поэтому ограничимся таблицей 4 рангов риска.

Из приведенных в таблице результатов для рассмотренных примеров можно отметить следующие зависимости уровня риска угроз ИБ от экспертных данных.

1. В основном, ранг риска угрозы ИБ зависит от количественных значений экспертных показателей вероятности реализации P и ущерба U . Например, к наиболее высокой по сравнению с другими угрозе 6 ($P=0,72; U=0,8$) относится наиболее высокий ранг риска в трех вариантах состава экспертных данных функции принадлежности, термножества и продукционных правил. В четвертом варианте риск этой угрозы незначительно меньше по сравнению с угрозой 2.
2. В некоторых вариантах состава экспертных данных функции принадлежности, термножества и продукционных правил уровни риска одних и тех же угроз могут существенно различаться. Например, в варианте 2 угрозе 2 соответствует третий ранг риска, а угрозе 3 – второй ранг риска. В

варианте 1 – наоборот. Исключение составляет в варианте 3, при котором угрозе 4 соответствует ранг риска 3, а угрозе 3 – ранг риска 6, а в варианте 1 – наоборот. В этом случае ранги риска ИБ угроз 3 и 4 в вариантах 1 и 3 состава экспертных данных функции принадлежности, термножества и продукционных правил отличаются на два. При этом в варианте 3 ранг риска угрозы 3 наименьший (шесть), а в варианте 1 – ранг риска этой угрозы четвертый. Если сравнивать варианты 4 и 3, то ранги риска угроз 3 и 4 отличаются еще более – на три. При этом в варианте 3 ранг риска угрозы 3 наименьший (шесть), а в варианте 4 – ранг риска этой угрозы третий.

Выводы

Показано, что при расчете риска угрозы ИБ с помощью модели нечетких множеств с разными возможными вариантами состава экспертных данных для одних и тех же угроз уровни риска ИБ могут существенно различаться. В качестве таких данных рассматривались: функции принадлежности, термножества, продукционные правила. Это приводит к тому, что первоочередные меры по защите могут относиться к угрозам не с более высоким уровнем риска ИБ.

Расчет производился на примерах нескольких угроз фрода в сигнализации по протоколу SIP сети VoIP (сеть передача речи и данных поверх IP).

Литература

1. Д. Рутковская, М. Пилиньский, Л. Рутковский. Нейронные сети, генетические алгоритмы и нечеткие системы. М: Горячая линия-Телеком, 2006. 388 с.
2. Maxwell Dondo. A Fuzzy Risk Calculations Approach for a Network Valnurability Ranking System. Defence R@D Canada-Ottawa, Technical Memorandum [Электронный ресурс]. 2007.

References

1. D. Rutkovskaya, M. Pilin'skij, L. Rutkovskij. Nejrornyie seti, geneticheskie algoritmy i nechetkie sistemy. M: Goryachaya liniya-Telekom, 2006. 388 s.
2. Maxwell Dondo. A Fuzzy Risk Calculations Approach for a Network Valnurability Ranking System. Defence R@D Canada-Ottawa, Technical Memorandum [EHlektronnyj resurs]. 2007.

3. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. М: РадиоСофт, 2010. 256 с.
4. Моёров А.С., Бельфер Р.А. Общие положения и математический аппарат для определения характеристики вероятности угроз в транспортной сети VANET, Сборник трудов всероссийской научно-технической конференции «Безопасные информационные технологии» НИИ РЛ МГТУ им. Н.Э.Баумана, 2012. С. 132-134.
5. Бельфер Р.А. Сравнительный анализ моделей оценки уровня риска угроз ИБ сети связи (по материалам ETSI). Сборник трудов всероссийской научно-технической конференции «Безопасные информационные технологии» НИИ РЛ МГТУ им. Н.Э.Баумана, 2013. С. 12-15.
6. Sisalem D. [and others]. SIP security. N.Y. Wiley, 2009. 355 p.
7. Матвеев В.А., Морозов А.М., Р.А. Бельфер. Фрод и угрозы в сети IP-телефонии по протоколу SIP. Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение», Специальный выпуск №5, «Информатика и системы управления», 2012. С. 236-248.
8. А.М.Морозов. Анализ уязвимостей сети SIP к угрозам фрода // Электросвязь. 2013. №7. С. 10-13.
3. SHHerbakov V.B., Ermakov S.A. Bezopasnost' besprovodnykh setej: standart IEEE 802.11. M: RadioSoft, 2010. 256 s.
4. Moyorov A.S., Bel'fer R.A. Obshhie polozheniya i matematicheskij apparat dlya opredeleniya kharakteristiki veroyatnosti ugroz v transportnoj seti VANET, Sbornik trudov vserossijskoj nauchno-tekhnicheskoj konferentsii «Bezopasnye informatsionnye tekhnologii» NII RL MGTU im. N.EH.Baumana, 2012. S. 132-134.
5. Bel'fer R.A. Sravnitel'nyj analiz modelej otsenki urovnya riska ugroz IB seti svyazi (po materialam ETSI). Sbornik trudov vserossijskoj nauchno-tekhnicheskoj konferentsii «Bezopasnye informatsionnye tekhnologii» NII RL MGTU im. N.EH.Baumana, 2013. S. 12-15.
6. Sisalem D. [and others]. SIP security. N.Y. Wiley, 2009. 355 p.
7. Matveev V.A., Morozov A.M., R.A. Bel'fer. Frod i ugrozy v seti IP-telefonii po protokolu SIP. Vestnik MGTU im. N.EH. Baumana, ser. «Priborostroenie», Spetsial'nyj vypusk №5, «Informatika i sistemy upravleniya», 2012. C. 236-248.
8. A.M.Morozov. Analiz uyazvimostej seti SIP k ugrozam froda // EHlektrosvyaz'. 2013. №7. S. 10-13.

*Рецензент: Горшков Юрий Георгиевич,
кан дидат технических наук, доцент*

