# МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 621.391

## АНАЛИЗ ЗАВИСИМОСТИ УРОВНЯ РИСКА УГРОЗ БЕЗОПАСНОСТИ ФРОДА СЕТИ NGN ОТ ЭКСПЕРТНЫХ ДАННЫХ ПРИ РАСЧЕТАХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ АНАЛИЗА ИЕРАРХИЙ И АНАЛИЗА ПАР

**В.А. Матвеев**, **Р.А. Бельфер**, **Д.А. Калюжный**, **А.М. Морозов**

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: v.a.matveev@bmstu.ru; a.belfer@yandex.ru; denis.kaluzhnyy@gmail.com; a.m.morozov@gmal.com

*Выполнен анализ зависимости от экспертных данных уровня угрозы безопасности фрода находящейся в эксплуатации системы сигнализации SIP оператора связи сети нового поколения NGN. В основу ранжирования угроз безопасности положены методы анализа иерархий AHP и анализа пар SPA, предложенные в работе Головной лаборатории по сетям, информационным атакам и технологии защиты Пекинского университета связи для ранжирования угроз DoS в сетях программного коммутатора (сетях Softswitch). С помощью методов AHP и SPA рассчитана максимальная мощность каждой угрозы, на основе значений которой проводится ранжирование анализируемых угроз безопасности. Приведен расчет на примерах шести угроз фрода системы сигнализации SIP. При использовании методов анализа учтена особенность угроз фрода в части принятия другой иерархической модели последствий угроз и принятия показателей последствий угроз одинаковой размерности при формировании матрицы парных сравнений. Показано существенное различие результатов ранжирования угроз безопасности фрода при разных вариантах состава экспертных данных. В качестве таких данных рассмотрены значения матрицы парных сравнений и значения характеристик уровня потерь по результатам опроса экспертов. Показано, что первоочередные меры по защите могут быть неэффективны и не относиться к угрозам с более высоким уровнем риска ИБ.*

***Ключевые слова*:** информационная безопасность; программный коммутатор; гибкий коммутатор; метод анализа иерархий МАИ; метод анализа пар; фрод; протокол установления сеансов; сети связи нового поколения NGN; угроза; передача голоса по IP сетям.

## DEPENDENCE ANALYSIS OF THEAT RISK LEVEL OF FRAUD SECURITY WITHIN NGN USING EXPERIMANTAL DATA DURING CALCULATION BY ANALYTIC HIERARCHY PROCESS AND SET PAIRS ANALYSIS

**V.A. Matveev**, **R.A. Bel'fer**, **D.A. Kalyuzhnyy**, **A.M. Morozov**

Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: v.a.matveev@bmstu.ru; a.belfer@yandex.ru; denis.kaluzhnyy@gmail.com; a.m.morozov@gmal.com

*The article analyzes the dependence of expert data versus threat level of fraud security being used by Session Initiation Protocol (SIP) signaling of service provider of New Generation Network (NGN). Analytic Hierarchy Process (AHP) and Set Pairs Analysis (SPA) are the base of ranking security threats. They are proposed by Head Laboratory specialized in networks, information attacks and protection technology located in Beijing University of Posts and Telecommunications for ranking threats*

*DoS within softswitch networks (networks Softswitch). Using the methods of AHP and SPA the authors calculated maximum capacity of each threat, based on the values which made the ranking analyzed security threats. The calculation is provided by six examples of fraud threats of alarm system SIP. Fraud threat feature is taken into account during using AHP and SPA for making another hierarchical model of threat consequences and making threat consequences indicators of the same dimension while forming the matrix of pairwise comparisons. A significant difference between the results of ranking fraud security threats at various variants of expert data contents is presented. Matrix value of pairwise comparisons and value characteristics of loss level are considered as the above data in expert survey. The calculation results in showing that the priority measures for the protection can appear ineffective and would not relate to threats of a higher risk level of Information Security.*

***Keywords*:** information security, softswitch, Analytic Hierarchy Process (AHP), Set Pairs Analysis (SPA), fraud, Session Initiation Protocol (SIP), New Generation Networks (NGN), threat, voice over IP (VoIP).

В работе [1] предлагается методика оценки уровня риска угроз безопасности фрода находящейся в эксплуатации системе SIP. Для ранжирования угроз используется теория нечетких множеств и нечеткой логики. В работе [2] показано, что при расчете риска угрозы информационной безопасности (ИБ) при разных возможных вариантах состава экспертных данных используемого математического аппарата для одних и тех же угроз уровни риска ИБ могут существенно различаться. Это приводит к тому, что первоочередные меры по защите могут относиться к угрозам не с более высоким уровнем риска ИБ, что приводит к неэффективным мерам по повышению безопасности сети связи. Расчет проводился на примерах нескольких угроз фрода в находящейся в эксплуатации системе сигнализации по протоколу SIP сети нового поколения NGN. Настоящая работа посвящена аналогичной задаче определения зависимости ранжирования угроз безопасности фрода находящейся в эксплуатации системы сигнализации SIP. В данном случае для ранжирования угроз используется другая методика, основанная не на теории нечетких множеств, а на методах анализа иерархий AHP (Set Pairs Analysis) и анализа пар SPA (Set Pairs Analysis). Этот математический аппарат предлагается в работе [3] Головной лаборатории по сетям, информационным атакам и технологии защиты Пекинского университета связи для ранжирования угроз DoS в сетях нового поколения NGN технологии передачи данных и речи VoIP (Voice over IP). Система сигнализации SIP этой технологии является наиболее перспективной. В то же время, согласно данным за 2013 г. Ассоциации по контролю за мошенничеством (фродом) CFCA (Communication Fraud Control Association), ежегодная доля потерь дохода 8,8 % операторов сетей составляет более 10 % [4]. Существенную долю составляют потери от фрода в системе сигнализации SIP. При этом следует отметить, что потери с каждым годом растут, а по данным CFCA за 2011 г. [5] 25,9 % операторов связи Западной Европы принимали участие в сборе

данных, а в России — всего 1,7 %. В 2013 г. — 31,9 % операторов связи Западной Европы принимали участие, данные по России отсутствуют.

**Алгоритм ранжирования угроз безопасности фрода в системе SIP с использованием метода анализа иерархий AHP и метода анализа пар SPA** включает в себя три этапа, из которых только первый этап отличается от приведенного алгоритма в работе [3].

- Структуризация задачи в виде иерархической модели AHP с несколькими уровнями.
- Определение степени связи двух множеств с помощью метода SPA.
- Определение уровня угроз фрода на основании SPA и нечетких комплексных решений.

**Структуризация задачи в виде иерархической модели AHP с несколькими уровнями.** Указанная работа [3] по ранжированию угроз в сетях нового поколения NGN технологии передачи данных и речи VoIP (Voice over IP) относится к отказам DoS. Настоящая работа посвящена анализу зависимости ранжирования угроз безопасности фрода находящейся в эксплуатации системы сигнализации SIP. Для решения поставленной задачи на рис. 1 представлена одна из возможных иерархических моделей соответствующих последствий угроз фрода [6, 7].

На верхнем уровне приводится глобальная характеристика последствий угроз фрода, на промежуточном уровне — разделение последствий угроз фрода на потери оператора и потери клиента. Нижний уровень характеризует следующие потери:

- финансовые потери оператора без учета потерь из-за оттока клиентов ($C_1$);
- финансовые потери оператора из-за оттока клиентов к другому оператору ($C_2$). Такое решение клиент принимает при низком показателе качества обслуживания QoE, который показывает удовлетворен ли пользователь различными характеристиками обслуживания сети ОП при ее эксплуатации. К числу таких характеристик относится

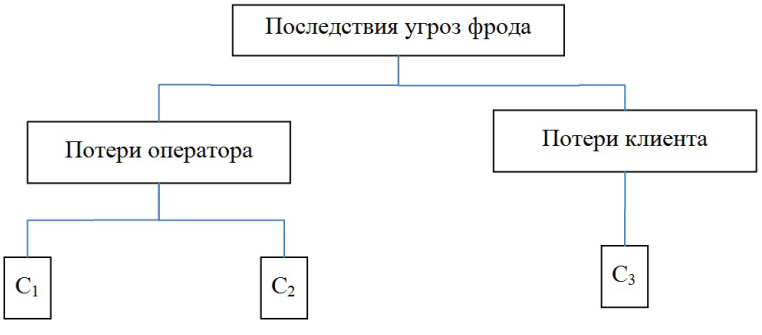


**Рис. 1. Иерархическая модель последствий угроз фрода**

интегральная характеристика качества обслуживания (integrity of the service). Эта характеристика является обобщенным восприятием пользователем качества обслуживания сетью и состоит из многих показателей (задержки, джиттер и др.) К этим характеристикам относится и обеспечение информационной безопасности. В данном случае к ним относятся характеристики угроз фрода;

• финансовые потери клиентов ($C_3$).

**Определение степени связи двух множеств с помощью метода SPA.** Метод SPA рассматривает пару взаимосвязанных множеств. Основная идея заключается в анализе параметров этой пары и вывода формулы, выражающей степень связи двух множеств, включая такие параметры, как степени идентичности, различия и несовпадения двух множеств.

Введем определение степени связи двух множеств следующим образом:

$$\mu(W) = S/N + F/Ni + P/Nj, \tag{1}$$

где $\mu$ — степень связи двух множеств; $S$ — представляет собой число идентичных характеристик; $N$ — общее число характеристик; $F = N - S - P$ — число характеристик, которые не являются ни идентичными, ни различными; $P$ — число различных характеристик; $S/N$, $F/N$ и $P/N$ — степени идентичности, несовпадения и различия двух множеств соответственно; значение коэффициента $i$ лежит в отрезке от $-1$ до 1; $j$ — коэффициент степени различия и определен как $-1$. Примем $a = S/N$, $b = F/N$, $c = P/N$ и перепишем выражение (1) в виде

$$\mu = a + bi + cj. \tag{2}$$

Коэффициенты $a$, $b$ и $c$ удовлетворяют соотношению $a + b + c = 1$.

**Определение уровня угроз фрода на основании SPA и нечетких комплексных решений.** Для ранжирования анализируемых угроз фрода по уровню их безопасности выполняется следующая последовательность.

• Формируются оценочные количественные показатели принятых характеристик финансовых потерь от реализации угрозы фрода. Как было отмечено, в настоящей работе принято множество характеристик, состоящие из трех элементов — $C = (C_1, C_2, C_3)$. Эти значения могут быть выражены либо в денежном выражении, либо в процентном отношении к доходу для оператора связи, а для клиента — по отношению к затратам при легитимных соединениях.

• Определяется количественная оценка веса каждой характеристики потерь $C_i$ от реализации определенной угрозы фрода $\mathrm{W} = (W_1, W_2, W_3)$. Для определения этих характеристик используется составленная экспертами матрица парных сравнений [8, 9].

• Принимается множество уровней потерь $m$. Определяется экспертная оценка уровня потерь. Примем множество уровней, состоящее из $m$ элементов $L = (L_1, L_2 \dots L_m)$. В приведенном далее примере для наглядности расчета примем $m = 3$, что соответствует — "большие", "средние" и "незначительные". В поставленной задаче для большей достоверности результатов ранжирования таких уровней должно быть больше.

• Экспертами оценивается каждая характеристика уровня потерь по каждому критерию $L$.

• Составляются матрицы степеней связи каждой характеристики потерь $C_i$ от реализации определенной угрозы фрода

$$\mathrm{B} = \begin{bmatrix} \mu_{11} & \dots & \mu_{16} \\ \vdots & \ddots & \vdots \\ \mu_{31} & \dots & \mu_{36} \end{bmatrix}, \tag{3}$$

где $\mu_{ij}$ — анализируемые с помощью множества пар SPA степени связи элемента $C_i$ с уровнем $l_i$.

• Выполняется расчет для каждого элемента $C_i$ матрицы связи A с помощью нечеткой операции умножения "$\circ$" матриц W и B:

$$\mathrm{A} = \mathrm{W} \circ \mathrm{B}. \tag{4}$$

• Проводится вычисление мощности связи shi (set pair power) [3] для каждой угрозы фрода на основе параметров матрицы связи A, входящих в степень связи множеств (формула (2)):

$$\mathrm{shi} = \frac{a}{c}, \tag{5}$$

где $c \neq 0$.

• Выполняется количественная оценка угрозы безопасности фрод методом выбора максимальной мощности связи shi.

• Проводится ранжирование анализируемых угроз фрода по уровню их безопасности на основании сравнения их максимальной мощности shi.

**Пример использования предложенной методики ранжирования угроз фрода с использованием метода AHP и SPA.** Приведем пример ранжирования шести угроз фрода $Y_1$, $Y_2$, $Y_3$, $Y_4$, $Y_5$, $Y_6$ системы сигнализации по протоколу SIP в сети речи и передачи данных VoIP.

Составляется матрица (табл. 1) парных сравнений $3 \times 3$ характеристик ($C_1$, $C_2$, $C_3$) угроз фрода на основе метода усреднения значений оценок экспертов, предложенного в работе [3]. Данная матрица показывает взаимную важность показателя, который приведен в строке, по сравнению с показателем в столбце. Приняты следующие значения степеней важности:

1 — параметры одинаково важны по отношению друг к другу; 2 — параметр $C_i$ в небольшой степени важнее параметра $C_j$ ; 3 — параметр $C_i$ более или менее важен по отношению к параметру $C_j$; 4 — параметр $C_i$ важнее параметра $C_j$; 5 — параметр $C_i$ в значительной степени важнее параметра $C_j$.

Если указанный в строке показатель не является более важным, используется обратное значение [8]. Например, значение 5 в первом столбце и третьей строке соответствует тому, что финансовые потери оператора без учета потерь из-за оттока клиентов ($C_1$) более важные, чем финансовые потери клиентов ($C_3$). Обратная величина 1/5 автоматически записывается на пересечении третьего столбца и первой строки.

Таблица 1

**Матрица парных сравнений**

| Параметр | $C_1$ | $C_2$ | $C_3$ |
|---|---|---|---|
| $C_1$ | 1 | 1/2 | 1/5 |
| $C_2$ | 2 | 1 | 1/3 |
| $C_3$ | 5 | 3 | 1 |

Рассчитаем уровни шести анализируемых угроз безопасности фрода в соответствии с приведенным алгоритмом и по данным матрицы (см. табл. 1):

$$w'_1 = \sqrt[6]{\Pi c_1 i} = 0{,}681; \quad w_{C1} = \frac{w'_1}{\sum\limits_{i=1}^{6} W'_i} = 0{,}214;$$

$$w'_2 = \sqrt[6]{\Pi c_2 i} = 0{,}935; \quad w_{C2} = \frac{w'_2}{\sum\limits_{i=1}^{6} W'_i} = 0{,}293;$$

$$w'_3 = \sqrt[6]{\Pi c_3 i} = 1{,}57; \quad w_{C3} = \frac{w'_3}{\sum\limits_{i=1}^{6} W'_i} = 0{,}492;$$

$$W = (w_{C1}, \ldots w_{C3}) = [0{,}214 \;\; 0{,}293 \;\; 0{,}492].$$

Затем 10 экспертов оценили каждую характеристику уровня потерь по трем критериям $L_1$, $L_2$, $L_3$ — соответственно “большие”, “средние” и “незначительные”. Результаты опросов приведены в табл. 2.

Таблица 2

**Оценка результатов опроса экспертов характеристик уровня потерь**

| Параметры | | $C_1$ | $C_2$ | $C_3$ |
|---|---|---|---|---|
| $Y_1$ | $l_1$ | 2 | 9 | 7 |
| | $l_2$ | 4 | 0 | 0 |
| | $l_3$ | 4 | 1 | 3 |
| $Y_2$ | $l_1$ | 0 | 7 | 9 |
| | $l_2$ | 0 | 2 | 0 |
| | $l_3$ | 10 | 1 | 1 |
| $Y_3$ | $l_1$ | 9 | 5 | 2 |
| | $l_2$ | 0 | 4 | 1 |
| | $l_3$ | 1 | 1 | 7 |
| $Y_4$ | $l_1$ | 2 | 4 | 3 |
| | $l_2$ | 1 | 0 | 6 |
| | $l_3$ | 7 | 6 | 1 |
| $Y_5$ | $l_1$ | 5 | 6 | 3 |
| | $l_2$ | 4 | 3 | 5 |
| | $l_3$ | 1 | 1 | 2 |
| $Y_6$ | $l_1$ | 0 | 1 | 1 |
| | $l_2$ | 9 | 0 | 0 |
| | $l_3$ | 1 | 9 | 9 |

Составление по формуле (3) матрицы степеней связи B ($B_1$, $B_2$, $B_3$, $B_4$, $B_5$, $B_6$) каждой характеристики потерь $C_i$ от реализации рассматриваемых шести угроз фрода.

Рассчитанные для каждой угрозы фрода матрицы степеней связей SPA приведены на рис. 2. В матрице первый столбец соответствует уровню потерь “большие”, второй столбец — “средние” и третий — “незначительные”.

Затем вычисляем оценочные матрицы по A1–A6 по формуле (4):

$$\begin{aligned}
&\mathrm{A1} = \mathrm{W} * \mathrm{B1} = [0,652 + 0,086i + 0,263j\; 0,086 + 0,652i + 0,263j\; 0,263 + 0i + 0,738j];\\
&\mathrm{A2} = \mathrm{W} * \mathrm{B2} = [0,649 + 0,059i + 0,292j\; 0,059 + 0,649j + 0,292j\; 0,292 + 0i + 0,708j];\\
&\mathrm{A3} = \mathrm{W} * \mathrm{B3} = [0,438 + 0,166i + 0,395j\; 0,166 + 0,438i + 0,395j\; 0,395 + 0i + 0,604j];\\
&\mathrm{A4} = \mathrm{W} * \mathrm{B4} = [0,308 + 0,317i + 0,375j\; 0,317 + 0,308i + 0,375j\; 0,375 + 0i + 0,625j];\\
&\mathrm{A5} = \mathrm{W} * \mathrm{B5} = [0,431 + 0,42i\;\; + 0,149j\; 0,42\;\; + 0,431i + 0,149j\; 0,149 + 0i + 0,851j];\\
&\mathrm{A6} = \mathrm{W} * \mathrm{B6} = [0,078 + 0,192i + 0,729j\; 0,192 + 0,078i + 0,729j\;\; 0,729 + 0i + 0,27j].
\end{aligned}$$

Вычисляем мощность связи shi по формуле (5) и выбираем максимум, применяя метод максимальной мощности:

$$\begin{aligned}
\mathrm{shi}_{Y_1} &= \max(2{,}48, 0{,}33, 0{,}36) = 2{,}48;\\
\mathrm{shi}_{Y_2} &= \max(2{,}22, 0{,}2, 0{,}41) = 2{,}22;\\
\mathrm{shi}_{Y_3} &= \max(1{,}11, 0{,}42, 0{,}65) = 1{,}11;\\
\mathrm{shi}_{Y_4} &= \max(0{,}82, 0{,}85, 0{,}6) = 0{,}85;\\
\mathrm{shi}_{Y_5} &= \max(2{,}89, 2{,}82, 0{,}18) = 2{,}89;\\
\mathrm{shi}_{Y_6} &= \max(0{,}11, 0{,}26, 2{,}7) = 2{,}7.
\end{aligned}$$

$$B_1 = \begin{matrix} 0.2+0.4i+0.4j & 0.4+0.2i+0.4j & 0.4+0i+0.6j \\ 0.9+0.0i+0.1j & 0.0+0.9i+0.1j & 0.1+0i+0.9j \\ 0.7+0.0i+0.3j & 0.0+0.7i+0.3j & 0.3+0i+0.7j \end{matrix}$$

$$B_2 = \begin{matrix} 0.0+0.0i+1.0j & 0.0+0.0i+1.0j & 1.0+0i+0.0j \\ 0.7+0.2i+0.1j & 0.2+0.7i+0.1j & 0.1+0i+0.9j \\ 0.9+0.0i+0.1j & 0.0+0.9i+0.1j & 0.1+0i+0.9j \end{matrix}$$

$$B_3 = \begin{matrix} 0.9+0.0i+0.1j & 0.0+0.9i+0.1j & 0.1+0i+0.9j \\ 0.5+0.4i+0.1j & 0.4+0.5i+0.1j & 0.1+0i+0.9j \\ 0.2+0.1i+0.7j & 0.1+0.2i+0.7j & 0.7+0i+0.3j \end{matrix}$$

$$B_4 = \begin{matrix} 0.2+0.1i+0.7j & 0.1+0.2i+0.7j & 0.7+0i+0.3j \\ 0.4+0.0i+0.6j & 0.0+0.4i+0.6j & 0.6+0i+0.4j \\ 0.3+0.6i+0.1j & 0.6+0.3i+0.1j & 0.1+0i+0.9j \end{matrix}$$

$$B_5 = \begin{matrix} 0.5+0.4i+0.1j & 0.4+0.5i+0.1j & 0.1+0i+0.9j \\ 0.6+0.3i+0.1j & 0.3+0.6i+0.1j & 0.1+0i+0.9j \\ 0.3+0.5i+0.2j & 0.5+0.3i+0.2j & 0.2+0i+0.8j \end{matrix}$$

$$B_6 = \begin{matrix} 0.0+0.9i+0.1j & 0.9+0.0i+0.1j & 0.1+0i+0.9j \\ 0.1+0.0i+0.9j & 0.0+0.1i+0.9j & 0.9+0i+0.1j \\ 0.1+0.0i+0.9j & 0.0+0.1i+0.9j & 0.9+0i+0.1j \end{matrix}$$

**Рис. 2. Матрицы степеней связи для каждой угрозы**

Используя полученные значения, ранжируем угрозы фрода по известным ранее характеристикам. Большему значению характеристики мощности связи shi соответствуют более высокий уровень угрозы безопасности фрода. Таким образом, если ранжировать угрозы от более опасной к менее опасной, то получаем $Y_5 > Y_6 > Y_1 > Y_2 > Y_3 > Y_4$.

**Ранжирование угроз фрода при различных экспертных данных.** В работе [2] показано, при расчете риска угрозы ИБ с помощью теории нечетких множеств в разных составах экспертных данных этого математического аппарата для одних и тех же угроз уровни риска ИБ могут существенно различаться. Это приводит к тому, что первоочередные меры по защите могут относиться к угрозам не с более высоким уровнем риска ИБ. В настоящем разделе покажем зависимость результатов ранжирования от различных вариантов экспертных данных в методике, использующей AHP и SPA. Расчет проводится на примерах угроз фрода в сигнализации по протоколу SIP, используемых в настоящей работе. Варианты экспертных данных определяются составом матрицы парных сравнений и значениями характеристик уровня потерь по результатам опроса экспертов. Состав табл. 1 и 2 определяют вариант 1, табл. 3 и 2 — вариант 2, табл. 1 и 4 — вариант 3.

Таблица 3

**Матрица парных сравнений (вариант 2)**

| Параметры | $C_1$ | $C_2$ | $C_3$ |
|---|---|---|---|
| $C_1$ | 1 | 3 | 1/2 |
| $C_2$ | 1/3 | 1 | 1/5 |
| $C_3$ | 2 | 5 | 1 |

Таблица 4

**Оценка результатов опроса экспертов (вариант 3)**

| Параметры | | $C_1$ | $C_2$ | $C_3$ |
|---|---|---|---|---|
| $Y_1$ | $l_1$ | 9 | 6 | 6 |
| | $l_2$ | 0 | 0 | 3 |
| | $l_3$ | 1 | 4 | 1 |
| $Y_2$ | $l_1$ | 8 | 7 | 9 |
| | $l_2$ | 1 | 0 | 0 |
| | $l_3$ | 1 | 3 | 1 |
| $Y_3$ | $l_1$ | 1 | 5 | 8 |
| | $l_2$ | 0 | 4 | 1 |
| | $l_3$ | 9 | 1 | 1 |
| $Y_4$ | $l_1$ | 8 | 5 | 6 |
| | $l_2$ | 1 | 3 | 3 |
| | $l_3$ | 1 | 2 | 1 |
| $Y_5$ | $l_1$ | 7 | 6 | 9 |
| | $l_2$ | 2 | 1 | 0 |
| | $l_3$ | 1 | 3 | 1 |
| $Y_6$ | $l_1$ | 3 | 5 | 3 |
| | $l_2$ | 4 | 2 | 5 |
| | $l_3$ | 3 | 3 | 2 |

В табл. 5 приведены значения максимальной мощности (shi) для трех рассмотренных вариантов экспертных данных, в табл. 6 — результаты расчета ранга шести угроз фрода при всех трех вариантах экспертных данных.

Таблица 5

**Значения максимальной мощности (shi)**

| Угроза фрода | Вариант 1 | Вариант 2 | Вариант 3 |
|---|---|---|---|
| $Y_1$ | 2,48 | 1,95 | 3,55 |
| $Y_2$ | 2,22 | 1,38 | 5,19 |
| $Y_3$ | 1,11 | 1,31 | 2,08 |
| $Y_4$ | 0,85 | 0,77 | 4,76 |
| $Y_5$ | 2,89 | 2,93 | 4,87 |
| $Y_6$ | 2,7 | 1,71 | 1,56 |

Из табл. 5 следует, что диапазоны значений максимальной мощности shi в первом и третьем варианте сильно отличаются. Поэтому сравнение результатов ранжирования угроз фрода в табл. 6 приводится не по уровню безопасности, как это показано в табл. 4, а по рангу риска угрозы фрод (т.е. по значению shi).

Таблица 6

**Ранг угроз фрода трех вариантов экспертных данных**

| Ранг риска угрозы фрода | Вариант 1 | Вариант 2 | Вариант 3 |
|---|---|---|---|
| $Y_1$ | Y5 | Y5 | Y2 |
| $Y_2$ | Y6 | Y1 | Y5 |
| $Y3$ | Y1 | Y6 | Y4 |
| $Y_4$ | Y2 | Y2 | Y1 |
| $Y_5$ | Y3 | Y3 | Y3 |
| $Y_6$ | Y4 | Y4 | Y6 |

Из табл. 6 следует: 1) при экспертных данных варианта 3 угроза $Y_2$ имеет наибольший ранг риска ИБ, а при экспертных данных варианта 1 — четвертый; 2) при экспертных данных варианта 3 угроза $Y_6$ имеет наименьший ранг риска ИБ, а при экспертных данных варианта 1 — второй; 3) при экспертных данных варианта 2 угроза $Y_4$ имеет наименьший ранг, а при экспертных данных варианта 3 — третий.

**Выводы.** Результаты ранжирования угроз безопасности фрода с помощью методов анализа иерархий AHP и анализа пар SPA (по принятым этим математическим аппаратом значениям максимальной мощности shi) при разных вариантах состава экспертных данных могут существенно различаться. В качестве таких данных рассматривались значения матрицы парных сравнений и значения характеристик уровня потерь по результатам опроса экспертов. Это привело к тому, что первоочередные меры по защите могут относиться к угрозам не с более высоким уровнем риска ИБ. Расчет проводился на примерах нескольких угроз фрода в сигнализации по протоколу SIP сети VoIP (сеть передачи речи и данных поверх IP). Для повышения достоверности субъективных экспертных данных, используемых в математических аппаратах для ранжирования угроз безопасности фрода, проводятся работы по тестированию с имитацией угроз находящихся в эксплуатации системах SIP операторов связи России [10].

## ЛИТЕРАТУРА


1. *Матвеев В.А.*, *Морозов А.М.*, *Бельфер Р.А.* Оценка уровня риска угрозы безопасности фрода в сети VoIP по протоколу SIP // Электросвязь. 2014. № 6. С. 35–38.
2. *Бельфер Р.А.*, *Калюжный Д.А.*, *Тарасова Д.В.* Анализ зависимости уровня риска угроз безопасности сетей связи от экспертных данных при расчетах с использованием теории нечетких множеств // Вопросы кибербезопасности. 2014. № 1 (2). С. 61–67.
3. *Yao Jiang*, *Kang Feng Zheng*. Evaluation Model for DoS Attack Effect in Softswitch Network. International Conference on Communications and Intelligence Information Security, 2010. P. 88–91.

4. *Communications* Fraud Control Association (CFCA). 2013 Global Fraud Loss Survey, www.cfca.org
5. *Communications* Fraud Control Association (CFCA). 2011 Global Fraud Loss Survey, www.cfca.org
6. *Sisalem D.* [and others]. SIP security. N.Y. Wiley, 2009. 355 p.
7. *Матвеев В.А.*, *Морозов А.М.*, *Бельфер Р.А.* Фрод и угрозы в сети IP-телефонии по протоколу SIP // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. Спец. вып. № 5 “Информатика и системы управления”. 2012. С. 236–248.
8. *Саати Т.П.* Принятие решений при зависимостях и обратных связях. М.: ЛКИ, 2008. 357 с.
9. *Денисова О.К.* Применение метода анализа иерархий для ранжирования бизнес-процессов (на примере вуза) // Научно-технические ведомости СПбГПУ. Сер. Экономические науки. 2013. 173 с.
10. *Морозов А.М.* Анализ уязвимостей сети SIP к угрозам фрода // Электросвязь. 2013. № 7. С. 10–13.

## REFERENCES

[1] Matveev V.A., Morozov A.M., Bel’fer R.A. The assessment of the risk level for threat of security fraud in the VoIP network under the SIP. *Elektrosvyaz’* [Telecommunications], 2014, no. 6, pp. 35–38 (in Russ.).
[2] Bel’fer R.A., Kalyuzhnyy D.A., Tarasova D.V. 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. *Voprosy kiberbezopasnosti* [Questions of cybersecurity], 2014, no. 1(2), pp. 61–67 (in Russ.).
[3] Jiang Y., Zheng K., Luo S., Zhao J. Evaluation Model for DoS Attack Effect in Softswitch Network. *Proc. Int. Conf. on Communications and Intelligence Inform. Security (ICCIIS)*, 2010, pp. 88–91. DOI: 10.1109/ICCIIS.2010.30
[4] Global Fraud Loss Survey, 2013. *Proc. Communications Fraud Control Association (CFCA).* Available at: www.cfca.org (accessed 01.09.2014).
[5] Global Fraud Loss Survey, 2011. *Proc.Communications Fraud Control Association (CFCA)*. Available at: www.cfca.org (accessed 01.09.2014).
[6] Sisalem D., Floroiu J., Kuthan J., Abend U. SIP security. New York, Wiley, 2009. 352 p.
[7] Matveev V.A., Morozov A.M., Bel’fer R.A. Fraud and threats in IP-telephony network under the SIP. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr. Spetsvyp. “Informatika i sistemy upravleniya”* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng. Spec. Iss. “Informatics and control systems”], 2012, iss. 5, pp. 236–248.
[8] Saaty T.L. Decision making with dependence and feedback: the analytic network process. Rws Publications, 2001. 370 p. (Russ. ed.: Saati T.L Prinyatie resheniy pri zavisimostyakh i obratnykh svyazyakh. Per. s angl. Moscow, LKI Publ, 2008, 360 p.).
[9] Denisova O.K. Application of a method of the analysis of hierarchies for ranging of business processes (on the example of higher education institution). *Nauchno-tehnicheskie vedomosti SPbGPU. Ser. “Ekonomicheskie nauki”* [Scientific and technical sheets. Economic sciences], 2013, 173 p. (in Russ.).
[10] Morozov A.M. The analysis of vulnerabilities of the SIP network to threats of a frod. *Elektrosvjaz’* [Telecommunications], 2013, no. 7, pp. 10–13 (in Russ.).

Статья поступила в редакцию 18.06.2014

Матвеев Валерий Александрович — д-р техн. наук, профессор, зав. кафедрой “Информационная безопасность”, руководитель НУК ИУ МГТУ им. Н.Э. Баумана. Автор более 200 научных работ и 25 патентов в области приборостроения и высокотемпературной сверхпроводимости.
МГТУ им. Н.Э. Баумана, Россия, 105005, Москва, 2-я Бауманская ул., д. 5.

Matveev V.A. — Dr. Sci. (Eng.), professor, head of “Information Security” department of the Bauman Moscow State Technical University, head of the Scientific and Educational Complex for Information and Control of the Bauman Moscow State Technical University. Author of more than 200 publications and 25 patents in the field of instrument engineering and high-temperature superconductivity.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federationa.

Бельфер Рувим Абрамович — доцент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор 97 научных работ в области информационных технологий.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Bel’fer R.A. — assoc. professor of “Information Security” department of the Bauman Moscow State Technical University. Author of 97 publications in the field of information technologies.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Калюжный Денис Александрович — студент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана Автор двух научных работ в области информационной безопасности.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Kalyuzhnyy D.A. — student of “Information Security” department of the Bauman Moscow State Technical University. Author of two publications in the field of information security systems and networks.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Морозов Алексей Михайлович — ведущий инженер отдела управления сетями Регионального центра управления сетями связи Московского филиала ОАО “Ростелеком”. Автор шести научных работ в области информационной безопасности.
Региональный центр управления сетями связи Московского филиала ОАО “Ростелеком”. Российская Федерация, 140000, Московская область, г. Люберцы, Московская ул., д. 17.

Morozov A.M. — leading engineer of department for network management of Regional Center for Management of Communication Networks of Moscow Branch of OAO “Rostelekom”. Author of six publications in the field of information Security.
Regional Center for Management of Communication Networks of Moscow Branch of OAO “Rostelekom”, Moskovskaya ul. 17, Lyubertsy, Moscow region, 140000 Russian Federation.