УДК 004.056

# Об одном подходе к оценке уровня угроз информационной безопасности

Е. В. Зубков, В. М. Белов

В статье рассматривается вопрос автоматизации процесса исследования статистики событий информационной безопасности (СИБ). Предлагаемый подход направлен на использование ранее полученных результатов для оценки уровня текущих угроз ИБ.

*Ключевые слова:* системы обнаружения вторжений (СОВ), событие информационной безопасности, методы интеллектуального анализа данных (МИАД).

## 1. Введение

Системы обнаружения вторжений (СОВ) как ключевой технический компонент в парадигме обеспечения информационной безопасности (ИБ) все чаще находят свое применение при построении комплексной защиты инфотелекоммуникационных систем (ИТС). При этом вполне очевидно, что на современном этапе научного и технического развития, а также в обозримой перспективе создать СОВ, которая бы работала без помощи квалифицированного специалиста, вряд ли получится [1], поскольку выявление компьютерных атак из общей статистики событий ИБ, зафиксированных СОВ, в значительной степени процесс творческий, целиком зависящий от человека. Необходимость участия человека при исследовании полученной информации является объективным фактором, и сегодня может идти речь лишь о повышении уровня автоматизации этого процесса. В общем случае подходы к исследованию данных могут быть различными. Единой универсальной методики не существует.

Одна из основных проблем, связанных с эксплуатацией СОВ, заключается в большом количестве регистрируемых СИБ, в том числе ложных срабатываний, что создает очевидные трудности при их исследовании. События, которые представляют действительную угрозу ИТС, могут остаться незамеченными на фоне общей статистики. В этих условиях приобретает актуальность задача поиска решений, направленных на автоматизацию процесса исследования статистики СИБ. Их применение способно оказать существенное положительное влияние на общую эффективность СОВ.

## 2. Проблематика вопроса

При эксплуатации СОВ значительные усилия сосредоточены на работе со статистикой СИБ. Наиболее подозрительные из них требуют проведения дополнительного исследования: изучения трафика, лог-файлов и т.д. для принятия решения о наличии действительной угрозы ИБ.

Естественным результатом работы является либо подтверждение факта соответствия того или иного СИБ действительной угрозе, либо опровержение его, т.е. заключение о факте ложноположительной реакции СОВ на трафик легитимного характера. Кроме того, эксперт

может принять решение о неактуальности некоторого СИБ в контексте конкретной ИТС. Например, если в ИТС отсутствуют объекты, уязвимые к зафиксированной потенциально опасной сетевой активности. Проведенная работа служит основанием к выполнению мероприятий по настройке объектов сетевой инфраструктуры (сетевого оборудования, серверов и т.д.) в целях противодействия выявленным угрозам ИБ, а также более тонкой настройке СОВ для повышения точности ее работы.

Чаще всего результаты экспертных оценок СИБ носят частный характер. Специалист проводит исследование и на его основе принимает то или иное решение. Следующее исследование начинается с чистого листа. Учитывая весьма высокую трудоемкость работы, справедливо задаться вопросом: а могут ли полученные ранее результаты быть использованы в будущем и если да, то каким образом?

Единичное исследование дает ответ только по конкретной ситуации. Однако если накапливается некоторая статистика подобных решений, то она может рассматриваться в качестве объекта применения МИАД и служить источником новой информации для составления прогноза о степени угрозы текущих СИБ.

Имея в своем распоряжении ретроспективу соответствия (либо несоответствия) отдельных СИБ действительной угрозе (т.е. множества маркированных данных), становится возможным дать оценку степени опасности СИБ, зафиксированных позднее. Такая оценка будет носить вероятностный характер и представлять собой своего рода проекцию предыдущего опыта на текущий момент.

Основой идеи для решения этой задачи послужили методики, используемые для поиска ассоциативных правил. Их целью является нахождение закономерностей между связанными событиями в базах данных (БД) [2, 3]. В своем классическом исполнении эти методики опираются на две основные характеристики: поддержку (support) и достоверность (confidence).

Для правила $X \rightarrow Y$ (из события X следует событие Y) вероятность совместного наступления событий X и Y: $P(X \cup Y)$ определяет значение поддержки, а вероятность наступления Y при условии наступления события X: $P(Y|X)$ – значение достоверности. Обе величины в значительной мере характеризуют правило с количественной точки зрения. Поддержка позволяет оценить количество событий X относительно общего количества событий, а достоверность – вероятность того, что из события X следует событие Y. Такая форма оценочной системы, видимо, связана с тем фактом, что ассоциативные правила впервые были разработаны для поиска корреляций в транзакциях данных розничной торговли [3]. Полученные величины отвечали решаемой прикладной задаче и способствовали формированию более выгодной ценовой политики. В рассматриваемой задаче ассоциативное правило предопределено: с одной стороны, это текущие события, с другой – события, прошедшие экспертную оценку.

Для дифференциации СИБ статистика подвергается кластеризации, т.е. объединению похожих элементов в группы. Тем самым достигается несколько целей. Основная из них – формирование нового представления данных, когда в роли объекта исследований выступает не единичное СИБ, а их совокупность. Такое представление позволяет соотнести между собой группы однородных событий, ранее получивших соответствующую экспертную оценку с аналогичными группами событий, такой оценки не имеющих.

Необходим признак, позволяющий оценить степень соответствия СИБ кластера реальной угрозе ИБ. При этом необходимо учитывать два фактора. Во-первых, этот признак может быть как со знаком «плюс» (т.е. СИБ соответствует угрозе ИБ), так и со знаком «минус», когда СИБ соответствует легитимному трафику (т.е. ложному срабатыванию СОВ) либо неактуальной угрозе ИБ. Во-вторых, значительная часть СИБ не будет иметь служебной метки.

Основной акцент при выборе оценочных критериев, таким образом, смещается в сторону качественной оценки. Для решения подобного рода задач предлагается ввести:

– критерий, по которому можно оценить степень изученности СИБ, составляющих тот или иной кластер;

– критерий, характеризующий степень непротиворечивости (однозначности) результатов исследования СИБ.

Решение по первому пункту находится в результате проецирования кластера на область уже исследованных СИБ (маркированных данных) (рис. 2.1).

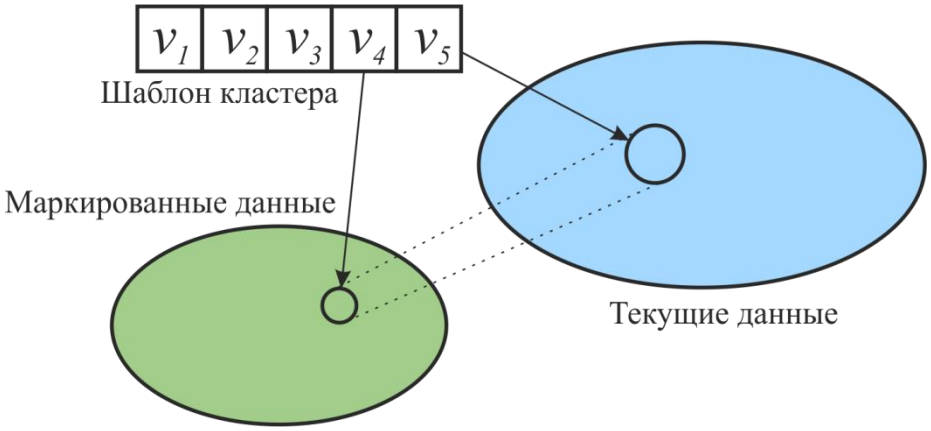


Рис. 2.1. Проекция кластера на множество маркированных данных

Отметим, что маркированные и текущие данные могут образовывать пересекающиеся множества, что приводит к многообразию возможных распределений. Основные случаи представлены на рис. 2.2, где синим цветом обозначена область текущих немаркированных данных, желтым – текущих маркированных, а зеленым – ретроспективных маркированных данных. Граничные ситуации соответствуют случаям 1 и 4, когда кластер либо вовсе не имеет соответствующих ему исследований, либо целиком состоит из СИБ, уже прошедших такое исследование. Случаи 2 и 3 соответствуют некоторому промежуточному варианту. Во втором случае существуют ретроспективные маркированные данные, соответствующие исследуемому кластеру, в третьем – помимо ретроспективных данных сам кластер содержит некоторое количество СИБ, прошедших экспертную оценку.

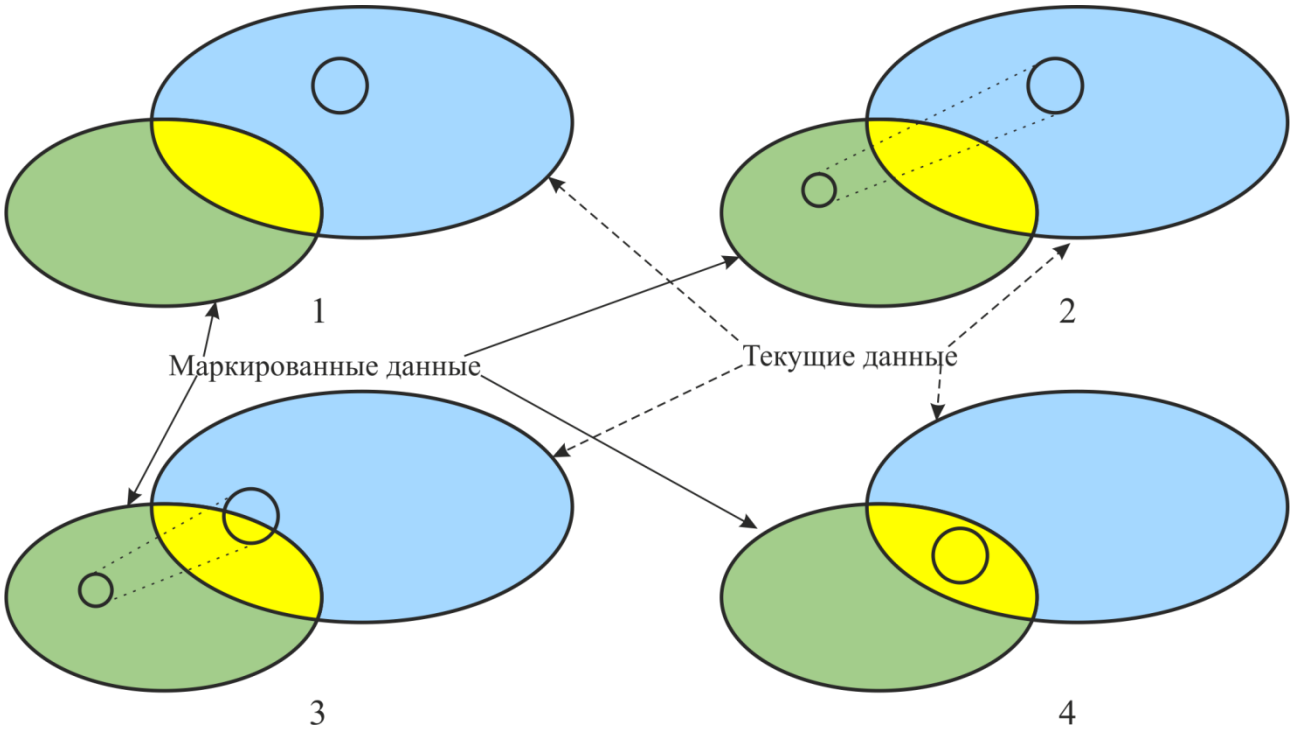


Рис. 2.2. Примеры случаев распределения данных

В конечном счете имеет смысл объединить элементы кластера с маркированными элементами ретроспективных данных, соответствующих шаблону кластера, и проводить дальнейшую работу с полученным множеством.

## 3. Построение оценочных критериев СИБ и общего алгоритма определения степени угроз ИБ

Для оценки степени изученности СИБ кластера R (от англ. research) предлагается использовать следующую формулу:

$$\begin{cases} R = 1, \text{при } N_m \neq 0, N_{\bar{m}} = 0; \\ R = \dfrac{N_m \cdot U_{\bar{m}}}{N_s \cdot (U_{\bar{m}} + U_m)}, \text{при } N_m \neq 0, N_{\bar{m}} \neq 0; \\ R = 0, \text{при } N_m = 0, N_{\bar{m}} \neq 0, \end{cases} \quad (3.1)$$

где $N_s = N_m + N_{\bar{m}}$ – общее количество маркированных и немаркированных элементов; $N_m$ – количество маркированных элементов; $N_{\bar{m}}$ – количество немаркированных элементов; $U_m$ – однородность множества маркированных элементов; $U_{\bar{m}}$ – однородность множества немаркированных элементов. Во всех случаях речь идет о данных, соответствующих шаблону исследуемого кластера.

**Докажем ряд утверждений.** Пусть $A_m$ и $A_{\bar{m}}$ – множества маркированных и немаркированных элементов соответственно. Обозначим через $k_N = \frac{N_m}{N_s}$ коэффициент, учитывающий размеры этих множеств, а через $k_U = \frac{U_{\bar{m}}}{(U_{\bar{m}} + U_m)}$ – коэффициент, учитывающий степень их однородности. Тогда $R = k_N \cdot k_U$.

**Утверждение 1.** Для непустых множеств $A_m$ и $A_{\bar{m}}$ будет выполняться условие $0 < R < 1$.

**Доказательство.** Действительно, поскольку $N_s > N_m$, то $k_N < 1$, а поскольку $U_{\bar{m}} + U_m > U_{\bar{m}}$, то $k_U < 1$, следовательно, $k_N \cdot k_U = R < 1$. Выражение $0 < R$ также выполняется, поскольку все параметры выражения (3.1) имеют положительные значения.

**Утверждение 2.** Для непустых множеств $A_m$ и $A_{\bar{m}}$ при $N_m = \text{const}$, $N_{\bar{m}} = \text{const}$, $U_m = \text{const}$ уменьшение $U_{\bar{m}}$ ведет к уменьшению R.

**Доказательство.** Пусть $\Delta U_{\bar{m}}$ – некоторая сколь угодно малая положительная величина, такая, что выполняется условие $U_{\bar{m}} > \Delta U_{\bar{m}}$. Докажем, что $R(U_{\bar{m}}) > R(U_{\bar{m}} - \Delta U_{\bar{m}})$.

Действительно,

$$R(U_{\bar{m}}) - R(U_{\bar{m}} - \Delta U_{\bar{m}}) = \frac{U_{\bar{m}}}{U_{\bar{m}} + U_m} - \frac{(U_{\bar{m}} - \Delta U_{\bar{m}})}{(U_{\bar{m}} - \Delta U_{\bar{m}} + U_m)} = \frac{U_{\bar{m}} \cdot (U_{\bar{m}} - \Delta U_{\bar{m}} + U_m) - (U_{\bar{m}} - \Delta U_{\bar{m}}) \cdot (U_{\bar{m}} + U_m)}{(U_{\bar{m}} + U_m) \cdot (U_{\bar{m}} - \Delta U_{\bar{m}} + U_m)}.$$

Поскольку знаменатель выражения положительный, рассмотрим числитель:

$$U_{\bar{m}} \cdot (U_{\bar{m}} - \Delta U_{\bar{m}} + U_m) - (U_{\bar{m}} - \Delta U_{\bar{m}}) \cdot (U_{\bar{m}} + U_m) = {U_{\bar{m}}}^2 - U_{\bar{m}} \Delta U_{\bar{m}} + U_{\bar{m}} U_m - {U_{\bar{m}}}^2 - U_{\bar{m}} U_m + \Delta U_{\bar{m}} U_{\bar{m}} + \Delta U_{\bar{m}} U_m = \Delta U_{\bar{m}} U_m > 0.$$

Таким образом, $R(U_{\bar{m}}) - R(U_{\bar{m}} - \Delta U_{\bar{m}}) > 0$, следовательно, $R(U_{\bar{m}}) > R(U_{\bar{m}} - \Delta U_{\bar{m}})$. Утверждение доказано.

Дополнительно отметим, что если $U_{\bar{m}} \to 0$, то $k_U \to 0$:

$$\lim_{U_{\bar{m}} \to 0} k_U = \lim_{U_{\bar{m}} \to 0} \frac{U_{\bar{m}}}{U_{\bar{m}} + U_m} = \frac{0}{0 + U_m} = 0.$$

**Утверждение 3.** Для непустых множеств $A_m$ и $A_{\bar{m}}$: при $N_m = \text{const}, N_{\bar{m}} = \text{const}, U_{\bar{m}} = \text{const}$ уменьшение $U_m$ ведет к увеличению R.

**Доказательство.** Пусть $\Delta U_m$ – некоторая сколь угодно малая положительная величина, такая, что выполняется условие $U_m > \Delta U_m$. Докажем, что $R(U_m) > R(U_m - \Delta U_m)$.

Действительно,

$$R(U_m - \Delta U_m) - R(U_m) = \frac{U_{\bar{m}}}{(U_{\bar{m}} + U_m - \Delta U_m)} - \frac{U_{\bar{m}}}{U_{\bar{m}} + U_m} = \frac{U_{\bar{m}} \cdot (U_{\bar{m}} + U_m) - U_{\bar{m}} \cdot (U_{\bar{m}} + U_m - \Delta U_m)}{(U_{\bar{m}} + U_m) \cdot (U_{\bar{m}} + U_m - \Delta U_m)}.$$

Поскольку знаменатель выражения положительный, рассмотрим числитель:

$$U_{\bar{m}} \cdot (U_{\bar{m}} + U_m) - U_{\bar{m}} \cdot (U_{\bar{m}} + U_m - \Delta U_m) = {U_{\bar{m}}}^2 + U_{\bar{m}} U_m - {U_{\bar{m}}}^2 - U_{\bar{m}} U_m + U_{\bar{m}} \Delta U_m = U_{\bar{m}} \Delta U_m > 0.$$

Таким образом, $R(U_m - \Delta U_m) - R(U_m) > 0$, следовательно, $R(U_m - \Delta U_m) > R(U_m)$. Утверждение доказано.

Дополнительно отметим, что если $U_m \to 0$, то $k_U \to 1$:

$$\lim_{U_m \to 0} k_U = \lim_{U_m \to 0} \frac{U_{\bar{m}}}{U_{\bar{m}} + U_m} = \frac{U_{\bar{m}}}{U_{\bar{m}} + 0} = 1.$$

Учитывая вышесказанное, а также тот очевидный факт, что увеличение количества маркированных элементов $N_m$ приводит к увеличению $k_N$ (а следовательно и R), а увеличение немаркированных $N_{\bar{m}}$ – к его уменьшению, подведем итог. Предлагаемая величина позволяет соотносить между собой различные комбинации изученных и неизученных данных. Важно, что R является нормированной величиной и изменяется на интервале от 0 до 1. Это обстоятельство позволяет рассматривать ее в качестве показателя вероятности текущей угрозы ИБ и будет в дальнейшем использовано при оценке уровня совокупной угрозы ИБ.

Для оценки непротиворечивости экспертной оценки C (от англ. consistency) используем энтропийный подход:

$$C = (1 + P_{m+} \cdot \log P_{m+} + P_{m-} \cdot \log P_{m-}) \cdot \text{sign},$$

где $P_{m+} = \frac{n_{m+}}{N}$ – вероятность положительного заключения, $P_{m-} = \frac{n_{m-}}{N}$ – вероятность отрицательного заключения, $n_{m+}$ – количество элементов с положительной оценкой, $n_{m-}$ – количество элементов с отрицательной оценкой, N – общее количество элементов, прошедших экспертную оценку, sign – определяет знак оценки и вычисляется следующим образом:

$$\text{sign} = \begin{cases} 1, & n_{m+} \geq n_{m-} \\ -1, & n_{m+} < n_{m-} \end{cases}.$$

Значение величины C изменяется на интервале от $-1$ до 1. Знак выражает преобладание положительных либо отрицательных заключений, а абсолютное значение – степень их однозначности. При исследовании кластеров СИБ, обладающих ненулевым значением R, следует учитывать соответствующее значение C. Низкое положительное значение непротиворечивости означает, что наряду с СИБ, представляющими опасность, ранее встречалось некоторое количество аналогичных СИБ, не соответствующих угрозе ИБ, что в той или иной мере ставит под сомнение действительную опасность текущих СИБ исследуемого кластера. Отрицательное же значение величины C прямо говорит о доминировании в кластере событий, не представляющих угрозы ИБ. Граничные значения 1 и $-1$ означают, что все маркированные СИБ представляют собой действительную угрозу ИБ либо такой угрозы ИБ не представляют, соответственно.

Для оценки уровня совокупной угрозы ИБ всех зафиксированных СИБ используем формулу вероятности суммы нескольких совместных событий:

$$P(A_1, A_2, \dots, A_n) = 1 - P(\overline{A_1}) \cdot P(\overline{A_2}) \cdot \dots \cdot P(\overline{A_n}),$$

где $A_1, A_2, \dots, A_n$ – список совместных событий, $P(\overline{A_i})$ – вероятность наступления события, противоположного $A_i$.

Для исследуемого случая эта формула примет вид:

$$R_s = 1 - \prod_{i=1}^{N}(1 - R_i),$$

где $R_i$ – степень изученности *i*-го кластера, N – количество исследуемых кластеров. При расчете данного показателя следует исключить кластеры с показателем непротиворечивости C ниже некоторого предопределенного порогового значения $C_{min}$, в том числе с отрицательными значениями. Общий алгоритм вычислений представлен на рис. 3.1.

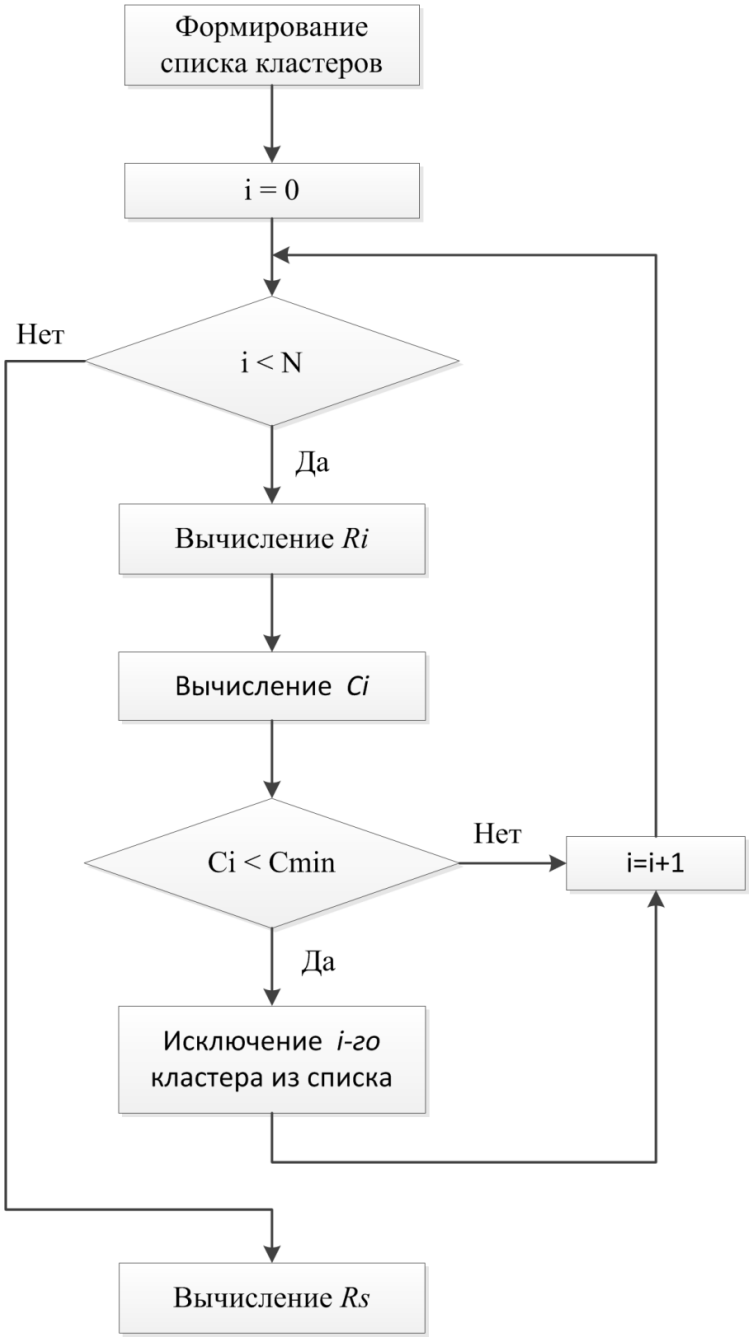


Рис. 3.1. Общий алгоритм определения степени угрозы ИБ

Таким образом, при наличии ретроспективных данных о соответствии тех или иных СИБ действительной угрозе ИБ становится возможным в автоматическом режиме дать оценку текущему состоянию как отдельно по каждому кластеру, так и в совокупности для всех СИБ. Точность и объективность полученной оценки зависит от объема и разнообразия множества маркированных данных.

## 4. Выводы

В статье рассмотрен вопрос исследования статистики СИБ как неотъемлемой составляющей при эксплуатации СОВ. Детальное изучение обстоятельств отдельных СИБ позволяет ответить на вопрос: несут ли они действительную угрозу ИТС или нет? Учитывая трудоемкость этого процесса, отмечается целесообразность сохранения результатов проделанной работы и использования их в будущем для расчета прогноза о степени угрозы текущих СИБ.

Введенные метрики дают нормированные числовые величины, характеризующие степень изученности СИБ того или иного кластера и непротиворечивость проведенных исследований.

Реализация предложенного подхода в виде общего алгоритма позволяет проецировать накопленный опыт экспертных оценок на текущую картину сетевой активности и акцентировать внимание специалистов на кластерах событий, имеющих аналитическую историю.

## Литература

1. *Норткат С., Новак Дж.* Обнаружение нарушений безопасности в сетях. 3-е издание: Пер. с англ. М. : Издательский дом «Вильямс», 2003. 448 с.
2. Интуит. Национальный открытый университет. Лекция 9: Методы классификации и прогнозирования. Деревья решений. [Электронный ресурс], http://www.intuit.ru/studies/ courses/6/6/lecture/174 (дата обращения: 10.12.2014).
3. *Harshna Navneet K.* Fuzzy Data Mining Based Intrusion Detection System Using Genetic Algorithm. January 2014 [Электронный ресурс]. URL: http://www.ijarcce.com/upload/2014/january/IJARCCE3I__a_harshna_fuzzy.pdf, (дата обращения: 16.02.2015).

*Статья поступила в редакцию 25.04.2016*

**Зубков Евгений Валерьевич**
аспирант кафедры безопасности и управления в телекоммуникациях СибГУТИ, тел.+7-913-798-01-48, e-mail: evz.nsk@gmail.com.

**Белов Виктор Матвеевич**
д.т.н., профессор, профессор кафедры безопасности и управления в телекоммуникациях СибГУТИ, тел.+7-963-906-84-83, e-mail: vmbelov@mail.ru.

**About an approach to assessing the level of information security threats**

**E. Zubkov, V. Belov**

This article focuses on the problem of the research process automation of information security event statistics. The proposed approach is aimed to use earlier results for assessing the level of current information security threats.

*Keywords*: intrusion detection system, information security event, data mining.