УДК 004.56

**А. А. Брюховецкий**, канд. техн. наук,
**А. В. Скатков**, д-р техн. наук

## АДАПТИВНАЯ МОДЕЛЬ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

***Аннотация.*** *Предлагается адаптивная модель и синтезированная на ее основе система обнаружения вторжений (СОВ), которые построены с использованием иммунологических принципов. Распознавание состояния сетевого трафика осуществляется в условиях дефицита априорной информации о свойствах источника вторжений и стохастической природы распознаваемых событий. Для повышения уровня достоверности обнаружения вторжений в системе производится адаптивная настройка правил принятия решений по классификации состояний сетевого трафика компьютерной сети. Настройка и тестирование модели выполнены на основе обнаружения аномалий в реальных наборах данных, полученных из реальных IP-трафиков компьютерных сетей и содержащихся в известной базе данных KDD'99.*

***Ключевые слова:*** *адаптивная модель, обнаружение вторжений, решающие правила, метрика правила, IP-трафик, признаки трафика, иммунные системы, качество правил, классификатор, популяция, обучение, тестирование, алгоритм оптимизации*

**A. A. Briukhovetskyi**, PhD.,
**A. V. Skatkov**, ScD.

## AN ADAPTIVE MODEL OF INTRUSION DETECTION IN COMPUTER NETWORKS BASED ON ARTIFICIAL IMMUNE SYSTEM

***Abstract.*** *It is proposed adaptive model and it is based the intrusion detection system (IDS), which is constructed on the basis of immunological principles. Recognition of the state of network traffic is in conditions of shortage priori information about the properties of the source intrusion and the stochastic nature of recognizable events. In order to improve the reliability of intrusion detection system is made adaptive setting decision rules for classifying the states of network traffic. The system is designed for the detection and classification of network attacks classes: DoS, R2L, U2R, Probe. Setting up and testing of the model is based on the search of anomalies in real data sets of IP-traffic computer networks and contained in known database KDD'99.*

***Keywords:*** *adaptive model, intrusion detection, decision rules, metric rule, IP-traffic, features traffic, immune system, quality rules, classifier, population, training, testing, the optimization algorithm*

**О. О. Брюховецький**, канд. техн. наук,
**О. В. Скатков**, д-р техн. наук

## АДАПТИВНА МОДЕЛЬ ВИЯВЛЕННЯ ВТОРГНЕНЬ В КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ ШТУЧНИХ ІМУННИХ СИСТЕМ

***Анотація*** *Пропонується адаптивна модель і на її основі система виявлення вторгнень (СВВ), які побудовані на основі імунологічних принципів. Розпізнавання стану мережевого трафіку здійснюється в умовах дефіциту апріорної інформації про властивості джерела вторгнень і стохастичної природи розпізнаваних подій. Для підвищення рівня достовірності виявлення вторгнень в системі проводиться адаптивна настройка правил прийняття рішень щодо класифікації станів мережевого трафіку комп'ютерної мережі. Налагодження та тестування моделі здійснюється на основі пошуку аномалій в реальних наборах даних, які одержані з реальних IP- трафіків комп'ютерних мереж і містяться у відомій базі даних KDD'99.*

***Ключові слова:*** *адаптивна модель, виявлення вторгнень, вирішальні правила, метрика правила, IP-трафік, ознаки трафіку, імунні системи, якість правил, класифікатор, популяція, навчання, тестування, алгоритм оптимізації.*

**Введение.** Пользователи современных сетей сталкиваются с беспрецедентным спектром атак и угроз, которые приводят к масштабным потерям. В связи с этим весьма актуальной является задача своевременного и достоверного обнаружения атак различных типов и видов [1, 2]. На сегодняшний день предложены различные решения по разработке систем обнаружения вторжений (СОВ), которые широко используются при поиске источников несанкционированных действий. Однако ощущается острая необходимость в постоянном совершенствовании СОВ, так как непрерывно развиваются виды атак на различные объекты сети.

В зависимости от источника обнаружения вторжений различают системы уровня Host–based (HBIDS) и сетевые СОВ (NIDS – Network Intrusion Detection) [3, 4]. Первые, как правило, проводят мониторинг трафика и отдельных ядер компьютера, в то время как вторые – исследуют сетевой трафик локальной сети и определяют его состояние. Этим самым текущее состояние (ТС) трафика классифицируется либо как нормальное (НС), либо как аномальное (АС) [5]. Основная проблема в обнаружении вторжений состоит в необходимости получения объективной оценки состояния трафика в сочетании с высокой их достоверностью, реактивностью в условиях экономного потребления вычислительных ресурсов [1–3].

Основные методы обнаружения вторжений принято подразделять на методы выявления нарушений прав доступа и методы обнаружения аномалий трафика [1,3–5]. Первое направление предполагает поиск нарушителей на основе известных сигнатур атак в сочетании с накоплением данных о них [6]. Второе направление методов обнаружения вторжений ориентировано на контроль отклонений заданных значений параметров трафика от установленных ограничений [7]. К недостаткам сигнатурных методов следует отнести: неспособность обнаруживать и блокировать ранее неизвестные вторжения, невозможность автоматического ввода новых контролируемых шаблонов, отсутствие возможностей прогнозирования действий нарушителя, отсутствие подсистемы мониторинга аппаратных ресурсов и др.

Задача классификации НС и АС сетевых компьютерных систем является на сегодняшний день до конца нерешенной и требует разработки новых комплексных подходов. В настоящее время для ее решения представляется перспективным использовать различные статистические модели для оценки вероятностей появления заданных значений (событий) [8], методы интеллектуальной обработки данных, такие как применение нейронных сетей [9], нечетких систем [10], решающих деревьев [11], генетических алгоритмов (ГА) [12], искусственных иммунных систем (ИИС) [1], кластеризации данных [13] и др.

Наиболее актуальными проблемами, требующими своего разрешения уже сегодня, по мнению авторов, являются: повышение уровня достоверности классификации состояний трафика, распознавание атак на ранних стадиях обнаружения, снижение числа ложных тревог, классификация событий при малых выборках, принятие решений в условиях нестационарного трафика.

Первоочередными научными задачами в разрешении указанных проблем являются следующие:

1. Совершенствование комбинированных методов обнаружения вторжений, включающих в себя адаптивные методы, интеллектуальную логику, методы ИИС, позволяющих повысить эффективность СОВ комплексно.

2. Повышение устойчивости адаптивных методов классификации событий в условиях дефицита априорной информации о свойствах источника вторжений. Применение таких методов позволит минимизировать число ложных тревог при изменениях сетевого трафика.

3. Повышение эффективности СОВ путем использования моделей, включающих в себя процедуры обучения как средство реализации адаптивного подхода. В основе такого подхода могут быть, например, использованы ГА [12]. Известно, что классические ГА и их разновидности не всегда применимы при решении задачи мультимодальной оптимизации. Поэтому в таких условиях целесообразно расширить методы ГА использованием подходов ИИС [14], которым присущи такие свойства как распознавание, использование принципа необходимого разнообразия, обучение, метадинамика и др.

4. Разработка систем, в структуре которых содержатся модули адаптации, модификации правил принятия решений, динамического формирования оценок качества правил классификации событий, позволяющих получить более эффективные в смысле Парето решения задач распознавания вторжений.

**Целью** настоящей работы является развитие и совершенствование методов обнаружения атак на основе использования адаптивной модели системы принятия решений в сочетании с методами ИИС. В связи с

этим предлагается модель и структура адаптивной СОВ, соответствующей иммунологическим принципам [1, 3, 14].

Настройка и тестирование модели выполнены на основе анализа информации, полученной при обработке реальных *IP*-трафиков, информация о которых представлена в общедоступной базе образцов сетевого трафика *KDD Cup* 1999 [15]. Используемые из этой базы входные данные структурно представляют собой *n*-мерные вектора, о которых априори известно, что они принадлежат к одному из следующих выделенных пяти классов $C_l$ (l=1..5) возможных состояний трафика: НС, *DoS* – отказ в обслуживании, *R2L* – несанкционированный доступ с удаленного компьютера, *U2R* – несанкционированный доступ к правам привилегированного пользователя (атаки на корневой каталог), *Probe* – сканирование портов с целью выявления уязвимостей в системе.

**Метод построения системы решающих правил адаптивной модели**. Особенностью рассматриваемого далее метода построения системы решающих правил лежит динамическое формирование оценок качества и состава таких правил для задачи *к*–мерной классификации отнесения векторов $\boldsymbol{x} = (x_1, ..., x_n)$ с *n* непрерывными атрибутами к одному из $C_l$ $(l=1,k)$ классов. В соответствии с известным механизмом организации функционирования ИИС [1] и использованием продукционных правил вида «ЕСЛИ “УСЛОВИЕ” – ТО “ДЕЙСТВИЕ”» предлагается каждое правило из множества всех правил *R* представлять так:

$$Rj: \text{ЕСЛИ } B_{j1} \text{ И } ... \text{ И } B_{jn} \text{ то } CLASS\ C_l \,|\, f_j, \qquad (1)$$

где *Rj* – метка *j*-го решающего правила, $j=1,2,...,N$; *N* – число решающих правил; $B_{ji}$ — логическая переменная, значение которой определяется бинарным отношением вида $x_i\ Q\ t_i$, построенном на входном интервале каждого числового признака, $t_i$ – пороговое значение для $x_i$; *Q* – отношение, построенное с использованием операции сравнения =, >, < и т.д.; $C_l$ — один из пяти классов возможных состояний сетевого трафика при условии, что $f_j$ — численное значение функции качества классификации правила *Rj*, которое определяет степень принадлежности вектора $\boldsymbol{x}$ к классу $C_l$. Оценивание функции $f_j$ качества правил *Rj* производится по результатам обучения с использованием данных базы образцов сетевого трафика *KDD Cup* 1999 и специальной предлагаемой авторами метрики:

$$fj = w1 \cdot a_j/|A| - w2 \cdot b_j/|B|, \qquad (2)$$

где $a_j$ — число случаев правильной классификации АС; $|A|$ – общее число АС, $b_j$ — число ошибочно классифицированных НС, $|B|$ — общее число НС; $w1, w2$ — неотрицательные весовые коэффициенты; $w1+w2=1$.

Значения $w1$ и $w2$ назначаются экспертом (ЛПР) на основе учета специфических особенностей решаемой задачи. Коэффициент $w1$ оценивает вклад числа правильно обнаруженных атак, $w2$ – вклад числа ложных тревог.

Областью изменений $f_j$ для каждого правила является отрезок [-1; 1] он определяется для каждого правила из множества *R*. Вид формулы (2) не является единственно возможным. Подобным образом можно конструировать и другие соотношения для коррекции оценок, которые учитывают особенности контролируемых событий.

Для обеспечения необходимого качества распознавания состояний трафика предлагается на основе множества всех правил *R* динамически формировать подмножества таких правил, каждое из которых имеет значение метрики $f_j$ выше заданного порогового значения $f_\alpha$, которое должно определяться ЛПР в зависимости от уровня критичности контролируемого трафика. Правила $R_j$, у которых $f_j > f_\alpha$ , образуют, подмножество эффективных правил – $R_\alpha$. Остальные правила включаются во множество $R_0$ ($R = \mathrm{R}_0 \cup \mathrm{R}_\alpha$). За счет использования при классификации состояний сети правил, входящих в $R_\alpha$ , обеспечивается высокое значение показателя правдоподобия обнаружения вторжений, а также минимальное число ложных тревог. Это утверждение справедливо в условиях стационарности процессов, протекающих в сети. При качественных изменениях трафика целесообразно корректировать множество правил $R_\alpha$ с учетом новых значений $f_j$.

Первоначально отсутствует априорная информация о значениях функции $f_j$. Качест-

во правил, входящих в $R_\alpha$ интегрально, оценивается метрикой *Fp*, которая построена как среднее значение $f_j$ метрик качества отдельных правил классификации. Построенное таким образом множество $R_\alpha$ соответствует группе условий $B_{ji}$, входящих в (1). При варьировании $B_{ji}$ формируется новое подмножество $R_\alpha$. Все такие подмножества $R_\alpha$ входят в качестве элементов во множество активных правил $R_{ac.}$ Тогда каждое такое подмножество $R_\alpha \in R_{ac}$ характеризуется интегральной оценкой $F\alpha p$, где $p=1,\ldots,|R_{ac}|$.

Наиболее эффективное подмножество $R_\alpha$ выбирается по условию:

$$Fmax = \max_{R_\alpha \subseteq R_{ac}} \{F\alpha p\}. \qquad (3)$$

Подмножество $R_\alpha$ ,удовлетворяющее условию (3), обозначим как $R_{\alpha m}$ . На основе описанного подхода предлагается адаптивная СОВ, структура которой представлена на рис. 1.

В ней выделены следующие основные функциональные модули: формирования компонент вектора *X*, анализа вектора *X*, обработки параметров трафика, формирования выходного сигнала, адаптации, принятия решений и др. Система может функционировать в одном из трёх функциональных режимов: рабочем (стационарном), обучения и оптимизации. Адаптивные свойства системы реализуются посредством использования двух последних режимов. В рабочем режиме адаптивной СОВ происходит также самотестирование системы. По его результатам в случае неудовлетворительной работы принимается решение о переходе СОВ в режим обучения и далее в режим оптимизации, после которых тестирование повторяется.

Функционирование системы состоит в следующем. По результатам текущего решения задачи классификации формируется текущий вектор $\boldsymbol{x} = (x_1, \ldots, x_n)$ состояния трафика, который поступает на вход модуля анализа. Первоначальные значения качества *fj* правил определяются на этапе обучения системы при использовании обучающих выборок с известными откликами из базы *KDD Cup*. Для правил $R_\alpha$, входящих в $R_{ac}$,

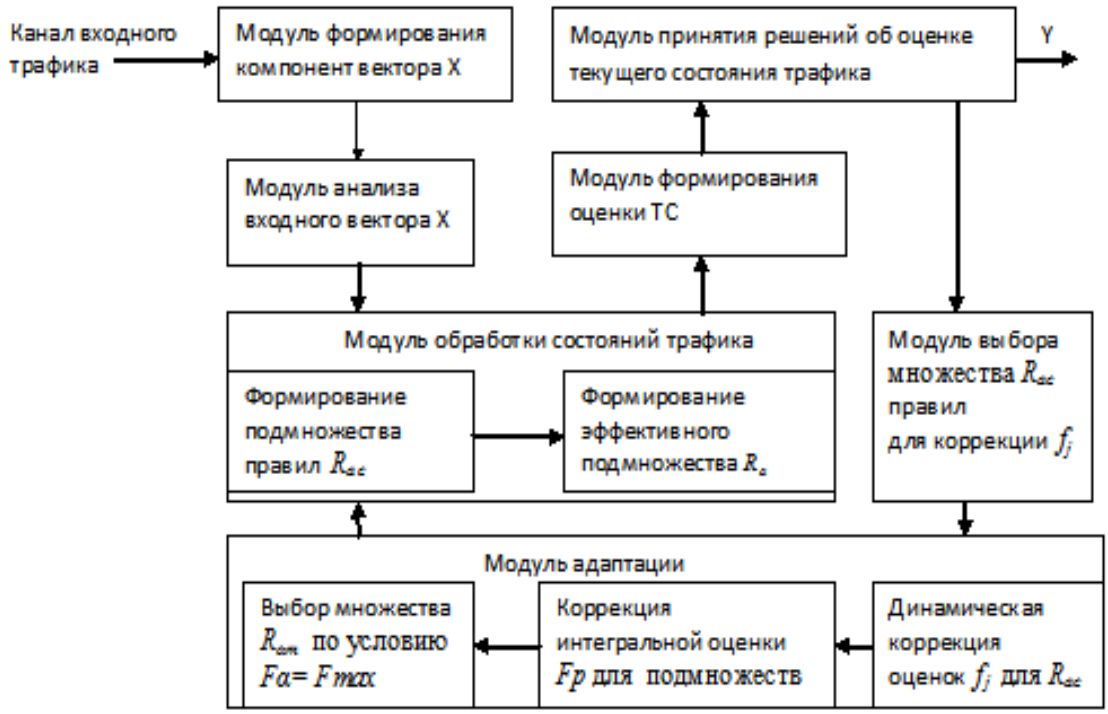



Рис. 1. Структура системы обнаружения вторжений на основе адаптивной модели

вырабатывается бинарный сигнал *Y* в случае, когда верно классифицируется ТС. Этот бинарный сигнал сравнивается с бинарным сигналом S, который для каждой выборки *X* априорно определяет ее принадлежность классу {НС, АС}. С использованием этих бинарных сигналов осуществляется коррекция значений функции качества в режиме обучения.

Классификатор предлагается реализовать в виде двухуровневой структуры, представленной на рис. 2. В нее входят модули: формирования оценок *fj* для каждого множества правил, формирования подмножества эффективных правил $R_{am}$ , определения максимальных значений *fj*.

На первом уровне происходит распознавание входного трафика *X* и делается заключение о его нормальности / аномальности: ТС={НС, АС}. На втором уровне применяются правила для обнаружения аномального трафика.

Таким образом, классификатор выполняет распознавание объектов, которые могут принадлежать одному из шести множеств правил: на первом уровне два множества описывают НС и АС трафика, на втором — четыре множества правил, каждое из которых описывает заданный класс одного из аномальных состояний.

С целью повышения качества классификации в системе предусмотрен режим адаптации правил к состоянию текущего трафика. Модуль адаптации производит коррекцию правил в зависимости от текущего состояния трафика. На основании информации об активированных правилах и текущего состояния трафика выполняется коррекция значений *fj* качества классификации. В модуле обратной связи анализируются значения сигналов Y активированных правил и сигнала *S*.

Коррекция правил осуществляется в результате пересчета значений функций качества активированных правил по формуле (2). Таким образом, значения функций качества правил корректируются в процессе функционирования системы обнаружения вторжений и адаптируются к анализируемому трафику.

Ниже описывается алгоритм формирования и оптимизации структуры решающих правил, который базируется на итерационной процедуре последовательной обработки примеров обучающей выборки на основе методов искусственных иммунных систем. При этом в качестве антигенов выступают *n*-мерные числовые вектора обучающей выборки, в качестве антител — решающие правила. В алгоритме предусмотрено два этапа: собственно обучение и тестирование результатов обучения. Алгоритм представлен в виде последовательности этапов и шагов.

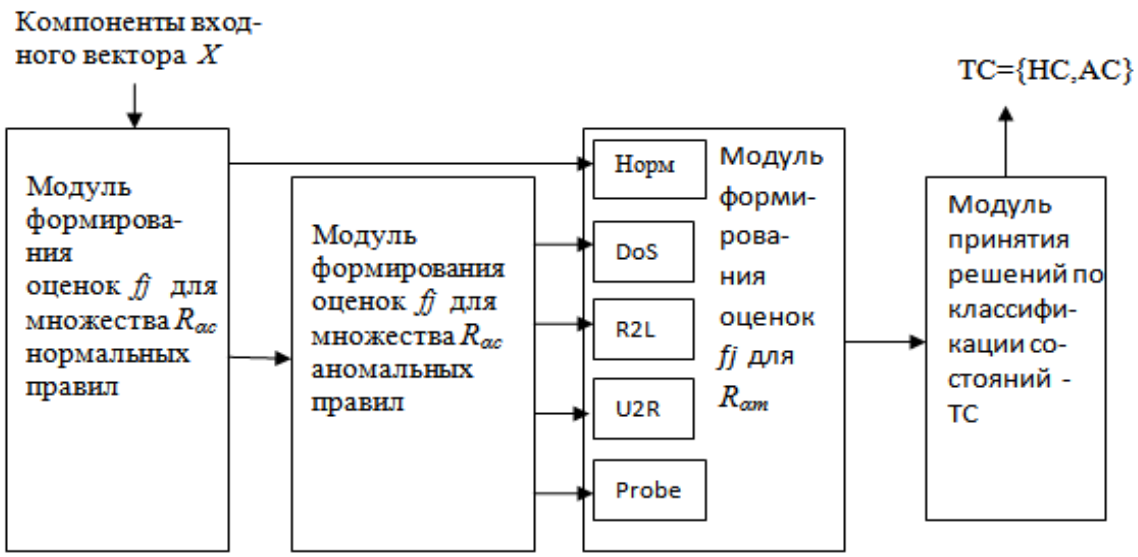



Рис. 2. Структура модуля обработки состояний трафика – классификатора

**Этап обучения**

1-й шаг. На основе метода построения решающих деревьев [11] сформировать решающие правила с использованием примеров обучающей выборки.

2-й шаг. Для каждого правила *Rj* заданного класса вычислить значение функции качества $f_j$.

3-й шаг. Пункты п1 и п2 повторить для правил каждого класса.

После окончания этапа обучения сформировано множество правил $R_\alpha$ вида (1), которое можно рассматривать в терминах ИИС, как популяцию антител.

**Этап оптимизации**

На этом этапе выполняется оптимизация множества правил для каждого из пяти классов. Для заданных критерия (3), соотношения (2) и значений весовых коэффициентов *w*1 и *w*2, установленных экспертом, выполнить:

Цикл для каждого антигена *Agi* :

1-й шаг. Все примеры предъявляются каждому правилу. Вычисляется оценка качества $f_j$ в соответствии с (2).

2-й шаг. Упорядочивается популяция $R_\alpha$ по убыванию значения $f_j$. Выбрать *m* первых антител, обладающих максимальным значением $f_j$, для клонирования *M* раз.

3-й шаг. Формируется популяция клонов $R_{\alpha c}$*. На основе популяции $R_\alpha$ для каждой случайно выбранной пары антител построить пару клонов. Клонирование выполняется с заданной вероятностью с помощью операции скрещивания [10].

4-й шаг. Выполняется мутация клонов популяции $R_{\alpha c}$* путем случайного изменения в одном из условий правила значения $t_j$ .

5-й шаг. Вычисляется оценка качества $f_j$ в соответствии с (2) , полученная при взаимодействии каждого антитела популяции $R_{\alpha c}$* с антигеном *Agi*. Добавить популяцию $R_{\alpha c}$* к популяции $R_\alpha$ .

6-й шаг. Упорядочивается популяция $R_\alpha$ по убыванию значений $f_j$.

7-й шаг. Внести изменения в состав множества $R_\alpha$ . В терминологии ИИС это соответствует супрессии антител внутри популяции $R_\alpha$ . Заменяются *d* худших антител случайными новыми антителами в популяции антител $R_\alpha$ .

8-й шаг. Повторяются пп.1–7 заданное число итераций.

9-й шаг. Повторяются пп.1–8 для формирования новых множеств $R_\alpha$ при различных значениях *w*1,*w*2 в зависимости от требований к системе и ситуаций, оценивающих уровень критичности объекта.

10-й шаг. Для каждого множества $R_\alpha$ вычисляется интегральная оценка *Fp*. В соответствии с критерием (3) выбрать наиболее эффективное подмножество $R_{\alpha m}$ для каждого класса.

По результатам исполнения алгоритма реализуется оптимизированная структура решающих правил.

Предлагаемый метод сочетает локальный и глобальный поиск на основе антител, имеющих максимальные оценки $f_j$. Алгоритм позволяет отыскать оптимальное решение при различной структуре правил, заданном критерии (3), соотношении (2) и ограничениях на значения весовых коэффициентов *w*1 и *w*2. С целью исследования влияния на уровень правдоподобия различных объемов тестирующих выборок, адаптивного изменения значения *fj* , а также различных значений весовых коэффициентов *w*1 и *w*2, которые задавались экспертом, были проведены специальные эксперименты.

В качестве оценки качества классификации использовалась оценка *DR* [5], которая наиболее чувствительна к состоянию сетевого трафика. В таблице представлены результаты четырех экспериментов при адаптивном изменении *fj*.

После последовательного многократного выполнения этапов обучения и оптимизации для всех классов проведены эксперименты на одной и той же смешанной выборке объемом 49198 векторов. В результате сформировано 79 правил, описывающих нормальный трафик, и 92 – аномальный. Ниже приведены примеры правил вида (1), используемые при классификации нормального и аномального состояний трафиков:

1) правило для распознавания нормального трафика:

*ЕСЛИ(x*5 < 1625 *& x*23 < 8 *& x*24 < 42 *& x*33 >= 96 *& x*34 >= 0,75 *& x*40 < 0,61*) то NORMAL;*

1. Результаты экспериментов при адаптивном изменении значения *fj*

| Класс $C_l$ | Номер и объемы тестовых выборок | | | | Уровень правдоподобия *DR* в экспериментах | | | |
|---|---|---|---|---|---|---|---|---|
| | 1-й | 2-й | 3-й | 4-й | 1-й | 2-й | 3-й | 4-й |
| | 29101 | 52389 | 279220 | 675128 | | | | |
| *Normal* | 17325 | 22891 | 68211 | 90592 | 0,9740 | 0,9802 | 0,9955 | 0,9958 |
| *DoS* | 9462 | 25988 | 204646 | 572594 | 0,9628 | 0,9798 | 0,9847 | 0,9919 |
| *U2R* | 7 | 16 | 48 | 70 | 0,6815 | 0,7823 | 0,7141 | 0,7363 |
| *R2L* | 831 | 1622 | 2843 | 7683 | 0,8316 | 0,9067 | 0,9135 | 0,9039 |
| *Probe* | 1476 | 1872 | 3472 | 4189 | 0,9112 | 0,9371 | 0,9140 | 0,9275 |

2) правило для распознавания общего вида аномального трафика:

*ЕСЛИ(*$x5$ >=1625 *&* $x23$ >= 205 *&* $x24$ >= 18 *&* $x33$ < 181 *&* $x34$ >= 0,95 *&* $x40$ >= 0,07*) то ATTACK;*

3) правила для классификации вида аномального трафика:

*ЕСЛИ(*$x5$ >= 1192 *&* $x6$ >= 329 *&* $x23$ < 21 $x24$ < 14 *&* $x29$ >= 6 *&* $x32$ < 256 *&* $x33$ >= 82 *&* $x34$ < 0,05 *&* $x35$ < 0.88 *&* $x38$ >= 0,31 *&* $x39$ >= 0,02 *&* $x40$ <= 0,01*) то U2R;*

*ЕСЛИ(*$x5$ >= 1192 *&* $x6$ >= 329 *&* $x23$ >= 21 $x24$ < 55 *&* $x29$ <12 *&* $x32$ >= 137 *&* $x33$ >= 204 *&* $x34$ < 1,00 *&* $x38$ < 0,21 *&* $x35$ >= 0,01 *&* $x39$ < 0,62 *&* $x40$ >= 0,81*) то DoS.*

На основании использования всего множества таких правил $R_{\alpha p}$ анализировались вектора из базы *KDD CUP'*99 . В таблице представлены результаты для четырех тестовых выборок, которые случайным образом извлечены из этой базы. Левая часть таблицы содержит значения объемов тестовых выборок, правая часть — результаты экспериментов по классам атак соответственно. В качестве тестовой выборки использовались данные [15]. Для каждого из четырех экспериментов использовалась индивидуальная выборка, номер которой совпадает с номером эксперимента.

Средний уровень правдоподобия *DR* ( в порядке убывания ) при интервале вариации Δ для классов в экспериментах №1–№4 составил: для класса *Normal* – 0,9864 и 0,0218 соответственно, для класса *DoS* – 0,9798 и 0,0291, для класса *Probe* – 0,9245 и 0,0259, для класса *R2L* – 0,8889 и 0,0819, для класса – 0, *U2R* 7286 и 0,1008. Кроме того, с целью оценки эффективности режима адаптации эксперимент № 4 проводился дважды: в отсутствии адаптации и при ее включении. При этом использовались полученные ранее результаты работы [11]. Оказалось, что для описанных условий использование режима адаптации позволило повысить уровень правдоподобия для атак типа *U2R* и *R2L* на примерно 5–11 %. В случае сравнения уровня правдоподобия для атак типа *DoS, Probe* и *Normal* с результатами [11] следует констатировать, что режим адаптации повысил качество классификации на примерно 1 – 6 %.

Представленные в таблице результаты имеют статистически устойчивый характер и в целом презентативно отображают особенности предложенного подхода.

По результатам проведенных экспериментов можно сделать следующие выводы.

1. Использование режима адаптации значительно увеличивает уровень правдоподобия классификации состояний сети.

2. При увеличении объемов выборок и использовании режима адаптации длина доверительного интервала для уровня правдоподобия уменьшается пропорционально корню квадратному из коэффициента кратности увеличения объема. Это обусловлено продуктивной коррекцией функции качества *fj* и возрастанием этой оценки. Для классов *Normal* и *DoS* такая

закономерность наблюдается во всех четырех экспериментах. Однако в некоторых случаях наблюдалось увеличение длины доверительного интервала, что можно интерпретировать влиянием неоднородности распределения примеров по классам из-за двух возможных причин: существенно неравномерного распределения векторов по классам и влияния ситуаций, в которых не было активировано ни одно из правил, а следовательно, коррекция *fj* не выполнялась.

3. Выбор весовых коэффициентов *w*1 и *w*2 , как и следовало ожидать, значительно влияет на результаты экспериментов. Например, эксперименты № 1–№ 4 проведены для *w*1 = *w*2. Проводился дополнительный эксперимент для значений весовых коэффициентов *w*1=0,4, *w*2=0,6 для объема тестовых выборок эксперимента № 4. Полученные оценки уровня правдоподобия в этом случае зависят от класса:

| класс | оценка |
|---|---|
| *Normal* | 0,9342 |
| *DoS* | 0,9217 |
| *Probe* | 0,8635 |
| *R2L* | 0,7940 |
| *U2R* | 0,6583 |

Изменение оценок вызвано увеличением относительного веса ошибок ложных тревог, которые привели к снижению уровня правдоподобия. Следует отметить, что необходимо компромиссное решение с привлечением дополнительной информации к выбору весовых коэффициентов *w*1 и *w*2 в зависимости от административных требований к системе и ситуаций, описывающих уровень критичности объекта.

Аналогичные эксперименты были спланированы и выполнены для различных классов атак с целью определения уровня ложных срабатываний, влияния периодичности модификации базы правил на основе адаптивной модели СОВ с использованием методов ИИС, значений коэффициентов *w*1 и *w*2 и др. Как оказалось, предложенная модель локально устойчива в пределах выделенных классов атак, а также чувствительна к настраиваемым параметрам бинарных отношений и порогу $f_\alpha$ формирования подмножества эффективных правил $R_\alpha$. Это позволяет эксперту учесть специфические особенности администрирования компьютерных сетей, в том числе в части раннего обнаружения фактов атак указанных классов.

Предлагаемая адаптивная модель обнаружения атак и возможных уязвимостей в компьютерных сетях на основе методов искусственных иммунных систем может являться основой для IT-технологий обеспечения компьютерной безопасности в условиях адаптации при быстром изменении состояния сетевого трафика. Использование адаптивной модели системы принятия решений в сочетании с ИИС позволяет повысить уровень правдоподобия распознавания событий, минимизировать число ложных тревог, а также обеспечить высокую реактивность системы, что особенно важно для этапов раннего обнаружения.

С целью дальнейшего совершенствования предлагаемого подхода представляется перспективным рассмотреть многомерную задачу классификации на множестве альтернативных признаков, Парето-подхода для задач многомерной оптимизации, а также целесообразность предварительной фильтрации трафика.

Список использованной литературы

1. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты: пер. с англ. – М. : Физматлит, 2006. – 344 с.

2. Информационные технологии для критических инфраструктур: монография / Под ред. А. В.Скаткова. – Севастополь : СевНТУ, 2012. – 306с.

3. Varghese S. M., and Jacob K. P Anomaly Detection Using System Call Sequence Sets, (2007), Journal of Software, No. 2(6), pp.14 – 21.

4. Yeung D.Y., and Ding Y. Host-Based Intrusion Detection Using Dynamic and Static Behavioral Models, (2003), Journal of Pattern Recognition, No. 36, pp. 229 – 243.

5. Ji Z., and Dasgupta D. Real-valued Negative Selection Algorithm with Variable-sized Detectors, (2004), Proceedings of the Genetic and Evolutionary Computation,

Springer–Verlag, Seattle, WA,USA, pp. 287 – 298.

6. Chen Y., Abraham A., and Yang B. Hybrid Flexible Neural–Tree–Based Intrusion Detection Systems, (2007), International Journal of Intelligent Systems, No. 22, pp. 337 – 352.

7. Shon T., and Moon J. A Hybrid Machine Learning Approach to Network Anomaly Detection, (2007), Journal of Information Sciences, No.177, pp. 3799 – 3821.

8. Kabiri P., and Ghorbani A. Research in Intrusion Detection and Response. – A Survey, (2005), International Journal of Network Security, No. 1, pp. 84 – 102.

9. Beghdad R. Critical Study of Neural Networks in Detecting Intrusions, (2008), Journal of Computers and Security, No. 27, pp.168 – 175.

10. Castro P. A., Coelho G. P., and Von Zuben F. J. Designing Ensembles of Fuzzy Classification Systems: An Immune-Inspired Approach, (2005), Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS), Lecture Notes in Computer Science, Springer–Verlag, Berlin, No. 3627, pp.469 – 482.

11. Брюховецкий А. А. Обнаружение уязвимостей в критических приложениях на основе решающих деревьев /А. А. Брюховецкий, А. В. Скатков, П. О. Березенко. – Радиоэлектронные и компьютерные системы. – 2013. – № 5(64). – Харьков : Изд-во ХАИ. – С. 18 – 23.

12. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская. – М. : Горячая линия, 2006. – 452 с.

13. Abraham A. Soft Computing Models for Network Intrusion Detection Systems. Classification and Clustering for Knowledge Discovery Studies / A. Abraham, R. Jain. – Computational Intelligence. – 2005. – P. 191 – 207.

14. Ройт А. Иммунология /А. Ройт, Дж. Бростофф, Д. Мейл / Пер. с англ. – М. : Мир, 2000. – 592 с.

15. KDD cup 99 Intrusion Detection Data Set [Электронный ресурс]. – Электрон.текстовые данные (752 Мб). – Darpa: Irvine, CA 92697–3425, 1999. – Режим доступа: /http:// kdd.ics.uci.edu/ databases/kddcup99 / Monday, 17 March 2013, 19:07:34.

Получено 04.11.2013

References

1. Dasgupta D. (ed.) Iskusstvennye immunnye sistemy i ikh primenenie [Artificial Immune Systems and Applications], (2006), Moscow, Russian Federation, *Pod red. D. Dasgupty, Fizmatlit Publ.*, 344 p. (In Russian).

2. Skatkov A.V. (ed.) Informatsionnye tekhnologii dlya kriticheskikh infrastruktur: monografiya [Information Technology for Critical Infrastructures: Monograph.], (2012), *Pod red. A.V. Skatkova,* Sevastopol, Ukraine, SevNTU, 306 p. (In Russian).

3. Varghese S.M., and Jacob K.P. Anomaly Detection Using System Call Sequence Sets, (2007), *Journal of Software Publ.,* pp.14 – 21.

4. Yeung D.Y., and Ding Y. Host-Based Intrusion Detection Using Dynamic and Static Behavioral Models, (2003), *Journal of Pattern Recognition Publ.*, pp.229 – 243.

5. Ji Z., and Dasgupta D. Real-Valued Negative Selection Algorithm with Variable-sized Detectors, (2004), *Proceedings of the Genetic and Evolutionary Computation, Seattle,* WA, USA, pp. 287 – 298.

6. Chen Y., Abraham A., and Yang B. Hybrid Flexible Neural-Tree-Based Intrusion Detection Systems, (2007), *International Journal of Intelligent Systems Publ.*, pp. 337 – 352.

7. Shon T., and Moon J.A. Hybrid Machine Learning Approach to Network Anomaly Detection, (2007), *Journal of Information Sciences Publ.*, pp. 3799 – 3821.

8. Kabiri P., and Ghorbani A. Research in Intrusion Detection and Response, (2005), *International Journal of Network Security Publ.*, pp. 84 – 102.

9. Beghdad R. Critical Study of Neural Networks in Detecting Intrusions, (2008), *Journal of Computers and Security Publ.*, pp.168 – 175.

10. Castro P.A., Coelho, G.P., and Von Zuben F.J. Designing Ensembles of Fuzzy

Classification Systems: An Immune-Inspired Approach, (2005), *Paper presented at the 4th International Conference on Artificial Immune Systems (ICARIS)*, Springer–Verlag, Berlin, pp. 469 – 482.

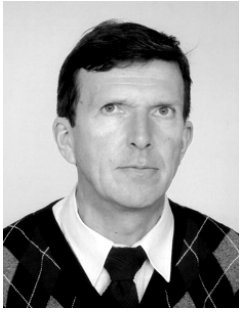
11. Bryukhovetskyi A.A. Skatkov A.V., and Berezenko P.O. Obnaruzhenie uyazvimostei v kriticheskikh prilozheniyakh na osnove reshayushchikh derev'ev [The Discovery of Vulnerabilities in Critical Applications Based on Decision Trees], (2013), *Journal Electronic and Computer Systems Publ.*, Kharkov, Ukraine, Vol. 5(64), pp. 18 – 23.

12. Rutkovska D. Neironnye seti, geneticheskie algoritmy i nechetkie siste-my [Neural Networks, the Genetic Algorithms and Fuzzy Systems], (2006), Moscow, Russian Federation, *Goryachaya* liniya Publ., 452 p.

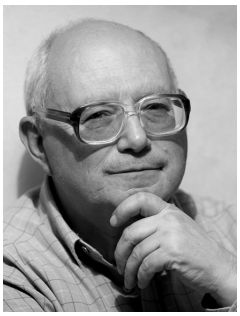
13. Abraham A., and Jain R. Soft Computing Models for Network Intrusion Detection Systems. Classification and Clustering for Knowledge Discovery Studies, (2005), *Journal Computational Intelligence Publ.*, pp. 191 – 207.

14. Roit I., Brostoff Dzh., and Meil D. Immunologya] [Immunology], (2000), *Per. s angl.*, Moscow, Russian Federation, *Mir Publ.*, 592 p. (In Russian).

15. KDD cup 99 Intrusion Detection Data Set [Elektronnyi Resurs], Electron. Texts data (752 Мб), Darpa: Irvine, CA 92697-3425, (1999), available at: /http: // kdd.ics.uci.edu /databases/kddcup99/ accessed: Monday, 17 March 2013, 19:07:34.



Брюховецкий
Алексей Алексеевич,
к.т.н., доцент каф. кибернетики и вычислительной техники Севастопольского нац. технич. ун-та,
ул. Университетская,33, Севастополь, Украина, 99053.
Тел.: +38(0)692-435-008,
E-mail: a.alexir@mail.ru



Скатков
Александр Владимирович,
д.т.н., профессор, зав. каф. кибернетики и вычислительной техники Севастопольского нац. технич. ун-та,
ул. Университетская,33,
Севастополь, Украина, 99053.
Тел. +38(0)692-435-008,
E-mail sevkvt.info@gmail.com