УДК 622.276.001

М.Е. Бурлаков, А.Н. Ивкин

Самарский национальный исследовательский университет
им. академика С.П. Королёва, Самара, Россия

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ НА ОСНОВЕ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ

На сегодняшний день интерес к искусственным иммунным системам многократно возрос, так как иммунные системы позволяют решать большое количество проблем в сфере компьютерной безопасности. Система обнаружения вторжений обеспечивает защиту от атак при работе в сети. Система сканирует сетевой трафик на наличие сигнатур атак, использующих уязвимости операционной системы и установленных программ. В статье рассмотрена статистическая модель системы обнаружения вторжения, основанная на искусственной иммунной системе. Для корректной работы систем обнаружений вторжений требуется детерминированный набор параметров работы. Наборы детекторов выбраны на основе заголовков пакетов. Используются только значения в заголовках для изучения аномального поведения пакетов во время передачи в любом сетевом трафике стека TCP/IP. На основе результатов тестирования предложены и реализованы методы улучшения системы обнаружения вторжения. В статье для повышения эффективности работы системы обнаружения вторжений объединены теория негативной селекции и правила машинного обучения. В модуле негативной селекции вместо использования только нормального профиля для разделения и классификации пакетов на два разных класса выполняется дополнительная проверка каждого пакета с использованием экспертных правил, созданных ранее на основе таблицы нормального профиля. Таким образом, пакет проходит больше этапов с целью конкретизации, является ли пакет аномальным. В результате частота ложных срабатываний значительно снижается, а частота обнаружения увеличивается. Для генерации детекторов разработан набор базовых правил с использованием программного обеспечения для анализа данных и машинного обучения. Сгенерированы и детализированы детекторы внутри модуля негативной селекции. В статье проводится тестирование предложенной модели на наборе данных DARPA1999.

Ключевые слова: искусственная иммунная система, система обнаружения вторжения, негативная селекция, машинное обучение.

M.E. Burlakov, A.N. Ivkin

Samara National Research University named after S.P. Korolev,
Samara, Russian Federation

INTRUSION DETECTION SYSTEM BASED ON THE ARTIFICIAL IMMUNE SYSTEM

Today, the interest in artificial immune systems has increased many times, because immune system solves a large number of problems in the field of computer security. Intrusion detection system provides protection against network attacks. The system scans network traffic for signatures of attacks that exploit operating system vulnerabilities and installed programs. The article describes a

statistical model of an intrusion detection system, based on artificial immune system, with the detector sets chosen based on packet headers. For correct operation of intrusion detection systems, a deterministic set of operating parameters is required. Only header values are used to study the anomalous behavior of packets during transmission in any TCP/IP network traffic. Based on the test results, methods for improving the intrusion detection system have been proposed and implemented. The article combines the theory of negative selection, one of the most important theories of artificial immune systems, and the rules of machine learning, and offering a new intrusion detection system. In the negative selection module, instead of using only the normal profile, to separate and classify the packages into two different classes, an additional check of each package is performed using expert rules created earlier on the basis of the normal profile table. Thus, the package goes through more stages, in order to specify whether the package is anomalous. As a result, the frequency of false positives is significantly reduced, and the frequency of detection increases. Generate detectors, a set of basic rules has been developed, using data analysis and machine learning software, and then new detectors were generated and detailed, inside the negative selection module. After testing the proposed model, using the DARPA1999 data set, the model showed good performance compared to previous models.

Keywords: artificial immune system, intrusion detection system, negative selection, machine learning.

Введение. На сегодняшний день в сфере информационных систем существуют задачи по обнаружению и предотвращению вторжений, поиску аномальных запросов и т.д. Для решения подобных задач используются искусственные иммунные системы (ИИС) [1]. ИИС – это адаптивная вычислительная система, основанная на принципах иммунной системы позвоночных. Проблемы в области компьютерной безопасности и иммунных систем имеют сходство в части организации работы в недетерминированных средах. ИИС используют аналог биологической иммунной теории для поиска и разработки моделей и алгоритмов с целью решения различных проблем в области компьютерной безопасности [2].

1. Система обнаружения вторжения *PbPHAD*. Для корректной работы систем обнаружений вторжений (СОВ) требуется детерминированный набор параметров работы (мониторинга). В [3] предлагается статистическая модель СОВ *PbPHAD* (*protocol based packet header anomaly detection*), основанная на ИИС.

В статье [3] наборы детекторов являются значениями в заголовках пакетов, передаваемых в информационном трафике стека *TCP/IP*. В качестве примера предлагается взять отчет [4]. В отчете выбираются 33 поля передаваемых пакетов из протоколов *Ethernet, IP, TCP, UDP* и *ICMP* (табл. 1). Работа СОВ *PbPHAD* связана с тремя протоколами: *TCP, UDP, ICMP*.

Таблица 1

Статистическая модель *PbPHAD*

i	Название	*R*	*N*	Найденные аномалии		
				TCP	UDP	ICMP
1	Etherdesthi	9	12,814,738	0.045	0.057	0.060
2	Etherdestlo	12	12,814,738	0.045	0.056	0.059
3	Etherprotocol	4	12,814,738	0.048	0.060	0.063
4	Ethersize	1456	12,814,738	0.031	0.040	0.041
5	Ethersrchi	6	12,814,738	0.047	0.059	0.061
6	Ethersrclo	9	12,814,738	0.045	0.057	0.060
7	Icmpchecksum	2	7,169	0.000	0.000	0.038
8	Icmpcode	3	7,169	0.000	0.000	0.037
9	Icmptype	3	7,169	0.000	0.000	0.037
10	Ipchecksum	1	12,715,589	0.052	0.065	0.068
11	Ipdest	1934	12,715,589	0.031	0.039	0.040
12	Ipfragid	12489	12,715,589	0.025	0.032	0.034
13	Ipfragptr	2	12,715,589	0.050	0.062	0.065
14	Ipheaderlength	1	12,715,589	0.052	0.065	0.068
15	Iplength	1463	12,715,589	0.031	0.040	0.041
16	Ipprotocol	3	12,715,589	0.049	0.061	0.064
17	Ipsrc	1918	12,715,589	0.031	0.039	0.040
18	Iptos	4	12,715,589	0.008	0.060	0.063
19	Ipttl	11	12,715,589	0.045	0.057	0.059
20	Tcpack	6,015,527	10,617,293	0.008	0.000	0.000
21	Tcpchecksum	2	10,617,293	0.049	0.000	0.000
22	Tcpdestport	22,293	10,617,293	0.023	0.000	0.000
23	Tcpflag	10	10,617,293	0.045	0.000	0.000
24	Tcpheaderlength	3	10,617,293	0.048	0.000	0.000
25	Tcpoption	3	10,617,293	0.048	0.000	0.000
26	Tcpseq	7,357,319	10,617,293	0.007	0.000	0.000
27	Tcpsrcport	22,293	10,617,293	0.023	0.000	0.000
28	Tcpurgptr	2	10,617,293	0.049	0.000	0.000
29	Tcpwindowsize	10,705	10,617,293	0.025	0.000	0.000
30	Udpchecksum	2	2,091,127	0.000	0.056	0.000
31	Udpdestport	8,050	2,091,127	0.000	0.027	0.000
32	Udplength	129	2,091,127	0.000	0.042	0.000
33	Udpsrcport	8,051	2,091,127	0.000	0.027	0.000
n	Итого	13,463,719		1.000	1.000	1.000

Значения столбцов *TCP, UDP, ICMP* в табл. 1 рассчитываются из соотношения:

$$\text{Result} = \left(1 - \log \frac{R_i}{N_i}\right) \cdot 100\ \%, \qquad (1)$$

где i – порядковый номер заголовка, R – число аномальных запросов, N – общее число пакетов, связанных с конкретным протоколом.

Из табл. 1 следует, что в модели СОВ *PbPHAD* чем больше число аномальных полей (R), тем меньше значение аномалии. Значение аномалии, равное 0,000, показывает отсутствие связи поля с конкретным протоколом. Отдельного внимания в табл. 1 заслуживают значения полей *IP*-адресов назначения (*ipdest*) и *IP*-адресов источников (*ipsrc*), показывающие количество хостов, используемых в проведенных испытаниях (рис. 1).

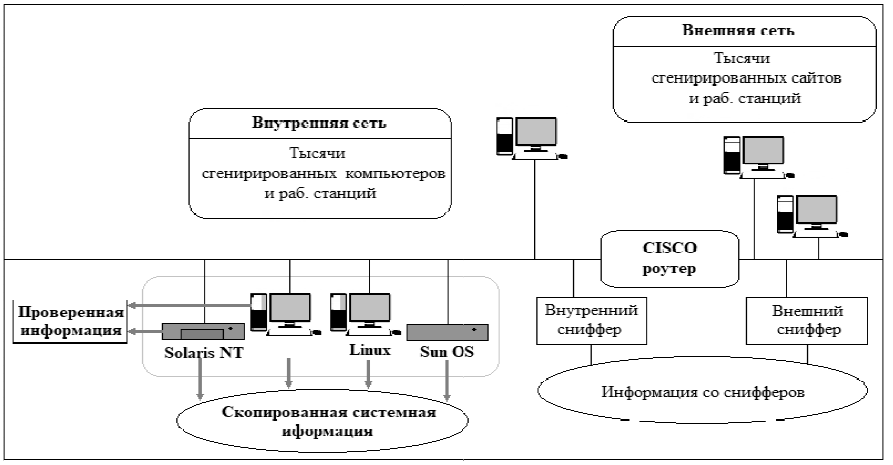

Рис. 1. Модель испытания

На рис. 1 показана модель генерации насыщенного трафика. Автоматические атаки начаты на компьютер жертвы *UNIX* и маршрутизатор со стороны внешних хостов. Машины, обозначенные как сниффер, запускают ПО *tcpdump* для перехвата пакетов, переданных через подключенный сегмент сети. Полученные данные разбиваются повременно, исходя из 5-недельного сбора в формате *pcap*, с собранными данными за 3 недели, используемыми для обучения ИИС, и за 2 недели с данными тестирования [5]. Процесс построения модели СОВ *PbPHAD* представлен на рис. 2.

Построение делится на 3 этапа:

1. Подготовка данных. Парсинг и конвертирование в формат *csv* собранных ПО *tcpdump* данных. Оценка производительности основывается на 189 обнаруженных аномалиях, зафиксированных в данных тестирования (табл. 2). В табл. 2 показано распределение атак относительно их типа и протоколов реализации. Отдельно отметим, при подготовке данных дублирование протоколов не учитывается.

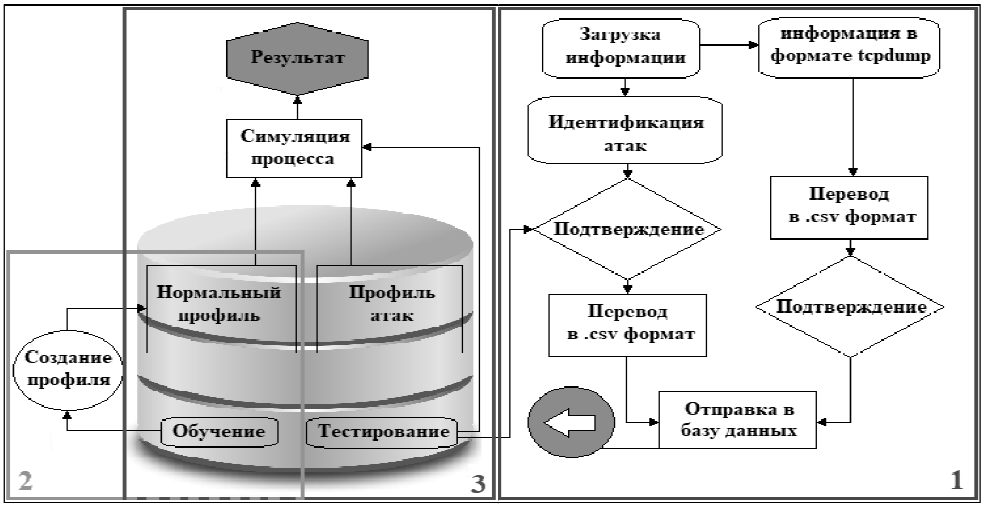

Рис. 2. Модель обнаружения вторжения *PbPHAD*

Таблица 2

Распределение всех атак во внутренних данных тестирования

Категория	TCP	UDP	ICMP	Всего
Probe	30	7	8	45
Dos	37	10	7	54
U2R	27	0	0	27
R2L	54	3	0	57
Data	4	2	0	6
Всего	152	22	15	189

2. Построение нормализованного профиля. Исходя из п.1, данные обучения заносятся в таблицу базы данных согласно их значениям, указанным в табл. 1 (33 поля).

3. Тестирование. Моделируется сетевой трафик за 2 недели данных тестирования и используется предложенная модель СОВ. 33 поля в пакете (в зависимости от протокола) сравниваются с нормализованным полем по тождественному значению. Если значение поля не найдено в нормализованном профиле, то пакет помечается как аномальный с расчетом статистических характеристик (как в табл. 1). Если сумма значений аномальных обнаруженных полей превышает определенный заданный порог, то происходит фиксация пакета в таблице обнаруженных аномалий.

2. Результаты тестирования СОВ на наборе данных *DARPA1999.* Протестированная модель содержит 22 095 072 пакетов и 121 зарегистрированную аномалию, превышающие определенные предварительно установленные пороги (*TCP* = 0,041, *UDP* = 0,128, *ICMP* = 0,034) показателей аномалий. Обнаруженные аномальные пакеты составляют около 10 % тестовых данных, включая ложные срабатывания. Выявлены 18 полей заголовков пакетов, внесших вклад в оценку аномалии обнаруженных атак. Распределение частоты аномальных полей показано в табл. 3. Остальные 15 полей заголовков пакетов отмечены как не вносящие вклад в оценку. Таким образом, табл. 3 используется для разработки модели СОВ, принимая во внимание нужные поля заголовков пакетов. Следовательно, время обработки данных будет уменьшено.

Таблица 3

Распределение частот аномальных полей

№ п/п	Поле заголовка пакета	Частота
1	Tcpseq	83
2	Ipsrc	60
3	Ipfragid	53
4	Tcpack	50
5	Ipdest	34
6	Tcpsrcport	16
7	Tcpdestport	11
8	Tcpwindowsize	8
9	Udpsrcport	8
10	Ipfragptr	7
11	Udpdestport	6
12	Udplen	6
13	Iplength	5
14	Tcpflag	4
15	Tcpurgptr	3
16	Tcpchecksum	2
17	Etherdesthi	1
18	Etherdestlo	1

На примере полученных выводов, используя работу [5], проведено тестирование хостовой СОВ *PbPHAD*, и для каждого отдельно исследованного хоста создавался нормализованный профиль. Для анализа взяты значения полей заголовка пакета только из протоколов модели

OSI уровня 3 и 4 (*IP, TCP, UPD, ICMP*). Общее количество проверяемых полей – 27 (см табл. 1) за исключением первых 6. Время тестирования СОВ *PbPHAD* – 2 недели. В ходе сбора данных собрано 22 095 072 пакетов. Количество обнаруженных аномалий – 154 случая. Таким образом, прирост эффективности работы СОВ по сравнению с предыдущим вариантом составляет 27 %. Хостовая СОВ *PbPHAD* обнаружила 25 аномальных полей по сравнению с 18 обнаруженными в сетевом варианте. В табл. 4 показаны 9 дополнительных полей заголовка пакета (17–25), обнаруженных хостовым вариантом.

Таблица 4

Распределение частот аномальных полей

№ п/п	Поля заголовка пакета	Частота сетевой PbPHAD	Частота хостовой PbPHAD
1	Tcpseq	83	125
2	Ipsrc	60	96
3	Ipfragid	53	15
4	Tcpack	50	55
5	Ipdest	34	13
6	Tcpsrcport	16	64
7	Tcpdestport	11	49
8	Tcpwindowsize	8	22
9	Udpsrcport	8	6
10	Ipfragptr	7	9
11	Udpdestport	6	7
12	Udplen	6	7
13	Iplength	5	38
14	Tcpflag	4	5
15	Tcpurgptr	3	0
16	Tcpchecksum	2	0
17	Ipheaderlen	–	1
18	Iptos	–	1
19	Ipttl	–	1
20	Ipprotocol	–	3
21	Ipchecksum	–	1
22	Tcpheaderlength	–	3
23	Udpchecksum	–	2
24	Icmptype	–	6
25	Icmpcode	–	1

Проведено сравнение между СОВ *PbPHAD* и комбинированными оценочными системами *DARPA1999* на основе атак, классифицированных как «плохо обнаруживаемых» согласно статье [6]. Сетевой СОВ

PbPHAD удалось обнаружить 48 аномалий по сравнению с 15 аномалиями, обнаруженными композитными системами (табл. 5). Полученный результат показывает увеличение на 39,76 % уровня детектирования плохо обнаруживаемых атак. Хостовая СОВ обнаружила 61 аномалию (улучшение на 55,41 %).

Анализируя результаты обнаружения в сетевых и хост-моделях, сетевая СОВ *PbPHAD* лучше с точки зрения определения атак вида *Probe* по сравнению с хостовой СОВ *PbPHAD*. Сетевая версия видит больший горизонт атаки, а хостовая не может обнаружить часть сканирования (например, анализируются пакеты с сигнатурами атак собственного *IP* адреса). Таким образом, развертывание сетевых и хост-моделей СОВ в рамках сетевой инфраструктуры обеспечит более широкую защиту от злонамеренных атак.

Таблица 5

Общие результаты сравнения СОВ

№ п/п	Название	Категория	Всего	Обнаружено		
				Комб. сист. DARPA1999	Сетевая PbPHAD	Хостовая PbPHAD
1	Ipsweep	Probe	7	0	7	7
2	Lsdomain	Probe	2	1	2	2
3	Portsweep	Probe	13	3	13	13
4	Queso	Probe	4	0	2	3
5	Resetscan	Probe	1	0	1	1
6	Arpoison	DoS	5	1	0	0
7	Dosnuke	DoS	4	2	4	4
8	Selfping	DoS	3	0	1	1
9	Tcpresert	DoS	3	1	2	2
10	Warezcient	DoS	3	0	3	3
11	Ncftp	R2L	5	0	4	5
12	Netbus	R2L	3	1	2	2
13	Netcat	R2L	4	2	0	4
14	Snmpget *	R2L	4	0	0	0
15	Sshtrojan	R2L	3	0	1	1
16	Loadmodule	U2R	3	1	0	2
17	Ntfsdos *	U2R	3	1	0	0
18	Perl	U2R	4	0	3	3
19	Sechole	U2R	3	1	1	2
20	Sqlattack	U2R	3	0	1	2
21	Xterm	U2R	3	1	1	3
Всего			83	15	48	61
Процент обнаруженных				18,07 %	57,83 %	73,49 %
Процент улучшения					39,76 %	55,41 %

3. Улучшение СОВ *PbPHAD.* Взяв во внимания результаты [7–8], предложена гибридная модель СОВ (рис. 3).

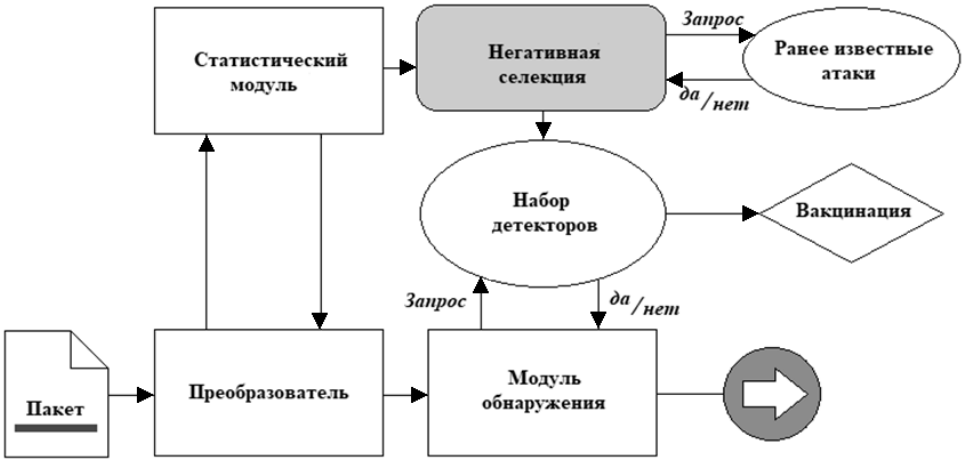

Рис. 3. Гибридная модель СОВ

Отдельное внимание стоит уделить модулю отрицательной селекции [9], отвечающему за:

– создание различных наборов детекторов;

– отправку новых наборов детекторов в другой модуль.

Работа модуля отрицательной селекции показана на рис. 4.

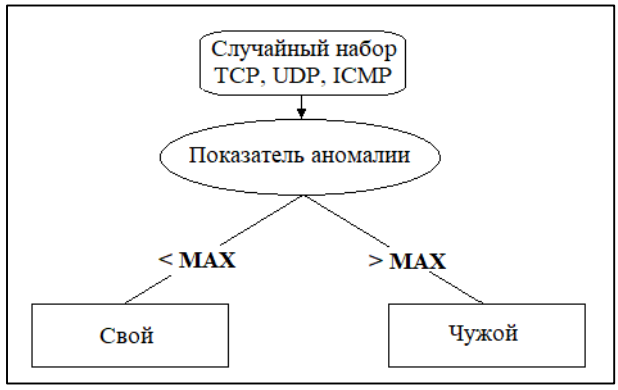

Рис. 4. Работа модуля отрицательной селекции

На рис. 4 создается случайный бинарный набор на основе полей заголовка пакета из табл. 6, для одного из протоколов (*TCP*, *UDP*, *ICMP*), затем рассчитывается показатель аномалии и сравнивается с некоторым пороговым значением (*MAX*). Если показатель аномалии

ниже порогового значения, то набор отбрасывается или считается «своим». Если порог будет превышен, то набор считается «чужим» и отправляется в набор новых детекторов.

Таблица 6

Используемые поля заголовка пакета

TCP	UDP	ICMP
Source IP Dest. Port IPFragID IPFragOff TCPSeq. TCPAck. Source Port Dest. Port	Source IP Dest. Port IPFragID IPFragOff Source Port Dest. Port UDP Length	Source IP Dest. Port IPFragID IPFragOff

В статье [7] часть атак некорректно детектируются, следовательно, требуется максимальное уменьшение уровня ложных срабатываний. В финальной версии СОВ, основанной на ИИС, интегрируется модуль отрицательной селекции (см. рис. 3). В модуле отрицательной селекции вместо использования только нормального профиля для разделения и классификации пакетов на два разных класса «нормальный» и «аномалия» выполняется дополнительная проверка каждого пакета с использованием экспертных правил, созданных ранее на основе таблицы нормального профиля. Таким образом, пакет проходит больше этапов с целью конкретизации, является ли пакет аномальным. В результате частота ложных срабатываний значительно снижается, а частота обнаружения увеличивается. Для создания экспертных правил используется инструмент *WEKA* [10], содержащий более 80 алгоритмов классификации [11]. В качестве базового алгоритма классификации выбрано дерево *J48*.

Лист дерева рассматривается как новое экспертное правило. Блок-схема построения дерева с помощью WEKA показана на рис. 5.

На рис. 5 выбирается один из хостов в наборе данных с наибольшим количеством атак, и после генерации имеющихся правил происходит обобщение. Цель обобщения – возможность применения к остальным хостам модели. Для имеющихся хостов создается нормирующий профиль. Профиль фильтруется по определенным протоколам. В результате получаются 3 таблицы заголовка пакета протоколов *TCP*, *UDP*, *ICMP* для

конкретного хоста. Далее определяется, является ли пакет атакой или нет, используя *DARPA IDS Dataset*. Выбор подобного набора данных обусловлен ориентацией на решение вопросов, связанных с обучением адаптивных алгоритмов [12–20]. Далее происходит обработка полученных таблиц из протоколов *TCP*, *UDP*, *ICMP* с помощью *WEKA*.

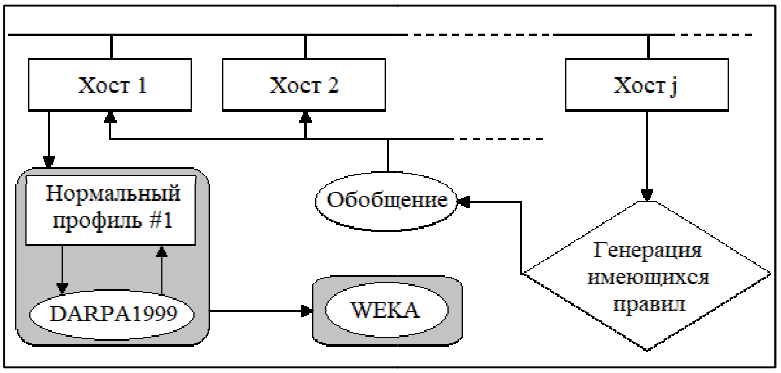

Рис. 5. Построение дерева *WEKA* для конкретного хоста

На рис. 6 показано одно из правил для протокола *UDP*, извлеченное из набора данных. Если *IP*-адрес источника находится в списке аномалий, *UDP*-порт назначения и *UDP*-порт источника меньше 1024, следовательно, пакет является *DOS*-атакой.

```
Time taken to build model: 0.33 seconds

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances       35021               100      %
Incorrectly Classified Instances         0                 0      %
Kappa statistic                          1
Mean absolute error                      0
Root mean squared error                  0
Relative absolute error                  0      %
Root relative squared error              0      %
Total Number of Instances            35021

=== Detailed Accuracy By Class ===

               TP Rate   FP Rate   Precision   Recall  F-Measure   ROC Area  Class
                 1         0          1         1         1          1        Normal
                 1         0          1         1         1          1        probe
                 1         0          1         1         1          1        dos
Weighted Avg.    1         0          1         1         1          1

=== Confusion Matrix ===

     a     b     c   <-- classified as
 32895     0     0 |     a = Normal
     0  1990     0 |     b = probe
     0     0   136 |     c = dos
```

Рис. 6. Вывод из *WEKA* для конкретного хоста

После создания дерева и использования *WEKA* процесс извлечения экспертных правил не ресурсоемок. Дерево на рис. 7 является результатом классификации, выполненной *WEKA*. Дерево преобразуется в экспертные правила (ветвь – правило).

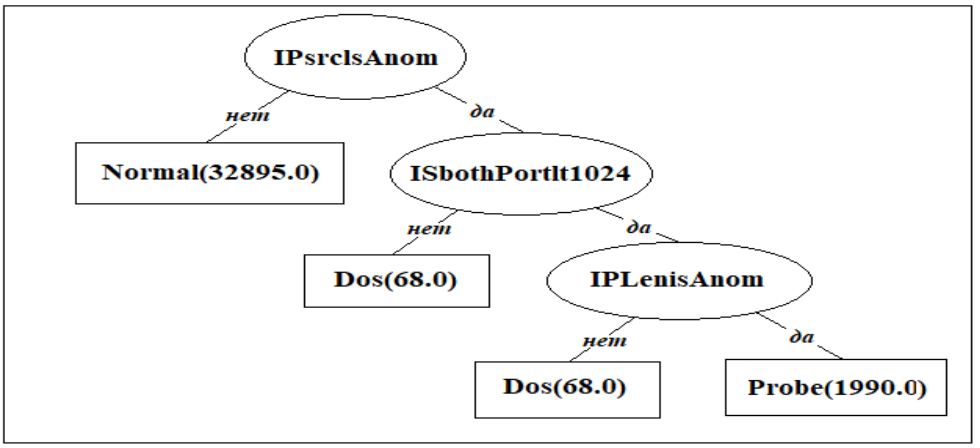

Рис. 7. Дерево *WEKA*

В табл. 7 показана производительность модели с точки зрения частоты обнаружения для различных категорий атак.

Таблица 7

Сравнение с моделью в статье [7]

Категория атаки	Работа из статьи [7]	Финальная модель
Probe	91,32 %	92,59 %
DOS	73,98 %	75,02 %
U2R	62,63 %	66,87 %
R2L	58,45 %	63,39 %

Замена модуля отрицательной селекции на модуль, работающий по экспертным правилам, увеличивает эффективность ИИС в рамках СОВ [7] в части уменьшения ложных срабатываний. Можно сделать вывод: использование отрицательной селекции значительно улучшает производительность СОВ. Конечной оценкой при выборе алгоритма стоит определить количество ложных срабатываний и возможность предельной загрузки системы.

Выводы. В работе рассмотрена СОВ, основанная на ИИС *PbPHAD*, демонстрирующая себя как очень эффективная, основанная

на аномалиях модель СОВ. В работе показана разница между развертыванием сетевых и хостовых СОВ в конкретной сетевой установке в части обеспечения более эффективной защиты сетевой инфраструктуры от умышленных атак. Путем тестирования на наборе данных *DARPA1999* показана возможность улучшения алгоритма ИИС. Произведена эффективная замена модуля отрицательной селекции на модуль из *WEKA*, построенный на основе экспертных правил с использованием ПО для машинного обучения. Проведены сравнения между *PbPHAD* и комбинированными оценочными системами *DARPA1999* на основе атак, классифицированных как «плохо обнаруживаемые» по методике из [4]. Показана общая производительность модели *PbPHAD* с точки зрения ложных срабатываний и частоты обнаружений лучше, чем в комбинированных оценочных системах *DARPA1999*. Получены и подтверждены улучшения с более ранней моделью из [7].

Библиографический список

1. Levitt K.N., Mykejee B. Network intrusion detection // IEEE Network. – 1995. – Vol. 2. – P. 25–40.

2. McLeod J., Aickelin U. Danger theory: the link between AIS and IDS // Proc. ICARIS-2003: 4nd International Conf. on Artificial Immune Systems. – 2003. – P. 130–160.

3. Solahuddin Michael E. Woodward. Modeling Protocol Based Packet Header Anomaly Detector for Network and Host Intrusion Detection Systems / Dep. of Computing, School of Inf. Un. of Bradford, U.K. – January 2008.

4. Mahoney M.V. PbPHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic. Tech. rep. Florida CS-2002-4 (April 2002).

5. MIT Lincoln Lab. 1999 DARPA Data Sets. – 1999. – URL: http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html.

6. Haines J.W., Fried D.J. The 1999 DARPA Off-Line Intr. Det. Evaluation. MIT Lincoln Lab. – 2002.

7. Mahboubian M., A naturally inspired statistical intrusion detection model // Proc. of ICINC. – Malaysia, 2010.

8. Mahboubian M. A novel intrusion detection model based on combination of artificial immune system and data mining approaches // Proc. WEC-2010. – Malaysia, 2010.

9. Li X., Duan S.R. The anomaly intrusion detection based on immune negative selection algorithm // Proc. IEEE International Conference on Granular Computing. – 2009.

10. WEKA. Soft. Machine Learn. The Un. of Waikato, New Zealand. – URL: http://www.cs.waikato.ac.nz/ml/weka

11. Shamsuddin S.B. Applying knowledge discovery in database techniques in modeling packet header anomaly intrusion detection systems // Journal of Software. – 2008. – Vol. 2, № 9.

12. Stolfo S.J. Anomalous Payload-based Network Intrusion Detection // Heidelberg. – 2004. – Vol. 3. – P. 190–240.

13. Chan P.K. Learning Rules for Anomaly Detection of Hostile Network Traffic // Proc. of the 3rd IEEE Int. Conf. on Data Mining. – 2003.

14. Marin G.A. Modeling Networking Protocols to Test Intrusion Detection Systems // LCN 2005. IEEE Intern. Conf. on Local Comp. Net. – 2005.

15. Detection of Novel Network Attacks Using Data Mining / L. Ertoz, E. Eilertson, A. Lazarevic, P.N. Tan, P. Dokas, V. Kumar, J. Srivastava // Proc. of SIAM Conf. Data Mining. – 2003.

16. Etalle D., Zambon P. POSEIDON: A 2-Tier Anomaly Based IDS // IWIA 2006. Proc. 4th IEEE Intern. Workshop on Inform. Assurance. – 2006. – P. 140–160.

17. Vliet F.V. Turnover Poseidon: Incremental Learning in Clustering Methods for Anomaly based Intrusion Detection // Proc. 20th Stud. Conf. on IT, University of Twente. – 2006.

18. Couto D., Popyack S. ADAM: Detecting intrusions by data mining // Proc. of the IEEE Workshop on Inform. Assurance and Security. – 2001.

19. Tian C., Huang S. Applying Genetic Programming to Evolve Learned Rules for Network Anomaly Detection // ICNC 2005. LNCS. – Heidelberg, 2005. – Vol. 3. – P. 290–350.

20. Mohammad Mahboubian. An alert fusion model inspired by artificial immune system // Conf.: Cyber Security, Cyber Warfare and Digital Forensic, IEEE, Malaysia. – July 2012. DOI: 10.1109/CyberSec.2012.6246083

References

1. Levitt K.N., Mykejee B. Network intrusion detection. *IEEE Network*, 1995, vol. 2, pp. 25-40.

2. McLeod J., Aickelin U. Danger theory: the link between AIS and IDS. *Proc. ICARIS-2003: 4nd International Conf. on Artificial Immune Systems*, 2003, pp. 130-160.

3. Solahuddin Michael E. Woodward. Modeling Protocol Based Packet Header Anomaly Detector for Network and Host Intrusion Detection Systems. Dep. of Computing, School of Inf. Un. of Bradford, U.K. January 2008.

4. Mahoney M.V. PbPHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic. Tech. rep. Florida CS-2002-4 (April 2002).

5. MIT Lincoln Lab. 1999 DARPA Data Sets, 1999, available at: http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html.

6. Haines J.W., Fried D.J. The 1999 DARPA Off-Line Intr. Det. Evaluation. MIT Lincoln Lab. 2002.

7. Mahboubian M., A naturally inspired statistical intrusion detection model. *Proc. of ICINC*. Malaysia, 2010.

8. Mahboubian M. A novel intrusion detection model based on combination of artificial immune system and data mining approaches. *Proc. WEC-2010*. Malaysia, 2010.

9. Li X., Duan S.R. The anomaly intrusion detection based on immune negative selection algorithm. *Proc. IEEE International Conference on Granular Computing*, 2009.

10. WEKA. Soft. Machine Learn. The Un. of Waikato, New Zealand, available at: http://www.cs.waikato.ac.nz/ml/weka

11. Shamsuddin S.B. Applying knowledge discovery in database techniques in modeling packet header anomaly intrusion detection systems. *Journal of Software*, 2008, vol. 2, no. 9.

12. Stolfo S.J. Anomalous Payload-based Network Intrusion Detection. *Heidelberg*, 2004, vol. 3, pp. 190-240.

13. Chan P.K. Learning Rules for Anomaly Detection of Hostile Network Traffic. *Proc. of the 3rd IEEE Int. Conf. on Data Mining*, 2003.

14. Marin G.A. Modeling Networking Protocols to Test Intrusion Detection Systems. *LCN 2005. IEEE Intern. Conf. on Local Comp. Net*, 2005.

15. Ertoz L., Eilertson E., Lazarevic A., Tan P.N., Dokas P., Kumar V., Srivastava J. Detection of Novel Network Attacks Using Data Mining. *Proc. of SIAM Conf. Data Mining*, 2003.

16. Etalle D., Zambon P. POSEIDON: A 2-Tier Anomaly Based IDS. *IWIA 2006. Proc. 4th IEEE Intern. Workshop on Inform. Assurance*, 2006, pp. 140-160.

17. Vliet F.V. Turnover Poseidon: Incremental Learning in Clustering Methods for Anomaly based Intrusion Detection. *Proc. 20th Stud. Conf. on IT, University of Twente*, 2006.

18. Couto D., Popyack S. ADAM: Detecting intrusions by data mining. *Proc. of the IEEE Workshop on Inform. Assurance and Securit*y, 2001.

19. Tian C., Huang S. Applying Genetic Programming to Evolve Learned Rules for Network Anomaly Detection. *ICNC 2005. LNCS*. Heidelberg, 2005, vol. 3, pp. 290-350.

20. Mohammad Mahboubian. An alert fusion model inspired by artificial immune system. *Conf.: Cyber Security, Cyber Warfare and Digital Forensic, IEEE*, Malaysia. July 2012. DOI: 10.1109/CyberSec.2012.6246083

Сведения об авторах

Бурлаков Михаил Евгеньевич (Самара, Россия) – старший преподаватель кафедры «Безопасность информационных систем» Самарского национального исследовательского университета имени академика С.П. Королева (443086, Самара, Московское шоссе, 34, e-mail: knownwhat@gmail.com).

Ивкин Андрей Николаевич (Самара, Россия) – аспирант Самарского национального исследовательского университета имени академика С.П. Королева (443086, Самара, Московское шоссе, 34, e-mail: ivkin.92@bk.ru).

About the authors

Burlakov Mikhail Evgenyevich (Samara, Russian Federation) is a Senior Lecturer in Department of information security systems Samara National Research University (443086, Samara, 34, Moskovskoye highway, e-mail: knownwhat@gmail.com).

Ivkin Andrey Nikolaevich (Samara, Russian Federation) is a Graduate Student Samara National Research University (443086, Samara, 34, Moscow highway, e-mail: ivkin.92@bk.ru).

Получено: 17.01.2019