Таблица 1. Результаты детекции эпилептических событий

№ п/п	Эпилептичес-кие события (интервал t, с)	Расчет λ на всей обучающей выборке (интервал t', с)	Расчет λ на первые M = 10 точек (интервал t'', с)	Погреш-ность Δt', с	Погреш-ность Δt'', с
1.	0,20 – 0,30	0,25 – 0,45	0,20 – 0,35	0,15	0,05
2.	0,50 – 0,60	0,45 – 0,55	0,50 – 0,60	0,05	0
3.	0,80 – 0,90	0,70 – 0,85	0,85 – 0,90	0,1	0,05
4.	1,10 – 1,20	0,90 – 1,20	1,05 – 1,20	0,2	0,05
5.	1,35 – 1,45	1,30 – 1,55	1,30 – 1,50	0,1	0,05
6.	1,60 – 1,70	1,65 – 1,85	1,65 – 1,75	0,15	0,05
7.	1,95 – 2,05	1,90 – 2,10	1,95 – 2,05	0,05	0
8.	-	2,15 – 2,25	-	-	-
9.	2,20 – 2,30	2,30 – 2,45	2,25 – 2,35	0,15	0,05
10.	2,55 – 2,65	2,55 – 2,70	2,55 – 2,65	0,05	0
Итоговая максимальная погрешность:				0,2	0,05

3. Исследовано применение старшего показателя Ляпунова в качестве критерия детекции аномалий, возникающих в сигналах ЭЭГ. Определение наличия эпилепсии в сигнале производится согласно условию (4).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Verdes P.F, Deco G, Obradovic D, Dubé L.J, Hopfengaertner R, Stefan H. Detection and prediction of epileptic seizures: a patient's case study.- www.tecn.upf.es/~gdeco/pubeng.html, 2000
2. Litt B, Echauz J. Prediction of epileptic seizures: review. - http://www.ncbi.nlm.nih.gov/entrez/, 2002
3. Карлов В.А Эпилепсия. – М.: Медицина, 1990. - 336с.
4. Babloyantz A., Destexhe A. Low dimensional chaos in an instance of epilepsy. Proc. Nat. Acad. Sci. USA, 1986.
5. Toward a Neurodinamical Understanding of Ictogenesis // Epilepsia, v.uu, №1, 2003, - P. 30-43.
6. Moser H., Weber B., Wieser H. Electroencephalograms in epilepsy: analysis and seizure prediction within the framework of Lyapunov theory. Physiol. D, 1999, - P. 130, 291-305.
7. Sackellares J.Ch, Iasemidis L.D, Shiau D. Epilepsy when chaos fail. Singapore: Word Scientific, 1990.
8. Hyvaerinen A., Oja E. Independent component analysis: algorithms and applications // Neural Networks, №13, 2000, - P. 411-430.
9. Головко В.А., Чумерин Н.Ю. Нейросетевые методы определения спектра Ляпунова хаотических процессов // Нейрокомпьютеры: разработка и применение, 2004. – №1.
10. Vladimir Golovko, Nikolay Maniakov, Alexander Doudkin. Application of Neural Networks Techniques to Chaotic Signal Processing//Optical Memory and Neural Networks, vol.13, Number 4, 2004, - P. 195-215.
11. Головко В.А. Нейросетевые методы обработки хаотических процессов// В книге «Лекции по Нейроинформатике». – М.: МИФИ, 2005. – С. 43-88.
12. Данные электроэнцефалограмм - http://republica.pl, 2002.

УДК 004.8

Кочурко П.А.

СОВОКУПНОСТЬ ДЕТЕКТОРОВ НА ОСНОВЕ РЕЦИРКУЛЯЦИОННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РАСПОЗНАВАНИЯ КЛАССА СЕТЕВЫХ АТАК

1. ВВЕДЕНИЕ

Непрекращающееся распространение применения информационных технологий во всех сферах человеческой деятельности постоянно ставит новые требования к уровню защищённости информационных систем. Стандартным компонентом инфраструктуры сетевой безопасности уже стали системы обнаружения атак (СОА) – аппаратно-программные комплексы, реализующие совокупность мер по обнаружению, определению и распознаванию вредоносных сетевых воздействий и реакции на эти воздействия – прерывание сетевой активности, оповещение персонала, ответственного за информационную безопасность. Несмотря на то, что существуют и постоянно появляются новые методы анализа сетевой активности с помощью различных технологий добычи данных («data mining») [1], основной технологией обнаружения атак по-прежнему является сигнатурный поиск. Его основной недостаток – недостаточная гибкость при обнаружении модифицированных атак [2]. Значительно лучшие результаты при определении модифицированных и новых атак способны показать системы, использующие искусственные нейронные сети [3-11]. Искусственные нейронные сети (ИНС) имеют потенциал для решения большого количества проблем, охватываемых другими современными подходами к обнаружению атак. ИНС были заявлены в качестве альтернативы компонентам статистического анализа систем выявления аномалий. Нейросети были специально предложены для того, чтобы идентифицировать типичные характеристики пользователей системы и статистически значимые отклонения от установленного режима работы пользователя [2].

В данной работе рассматривается метод распознавания класса атак на основе анализа сетевого трафика. Обучение и тестирование ИНС производилось на выборке KDD'99, содержащей записи о TCP-соединениях, включающих 41 параметр, полученные из обработанной базы данных DARPA 1998 Intrusion detection evaluation [12]. Данная выборка включает нормальные соединения, а также атаки 23 типов, принадлежащие к четырём классам: DOS – «denial-of-service» - отказ в обслуживании, например, Syn-лавина; U2R – неавторизованное получение привилегий root на данной системе, например, различные атаки «переполнения буфера»; R2L – неавторизованный доступ с удалённой системы, например, подбор пароля; Probe – наблюдение и другое зондирование, разведка, например, сканирование портов.

Кочурко Павел Анатольевич, *аспирант каф. интеллектуальных информационных технологий Брестского государственного технического университета.*

Беларусь, БрГТУ, 224017, Беларусь, г. Брест, ул. Московская, 267.

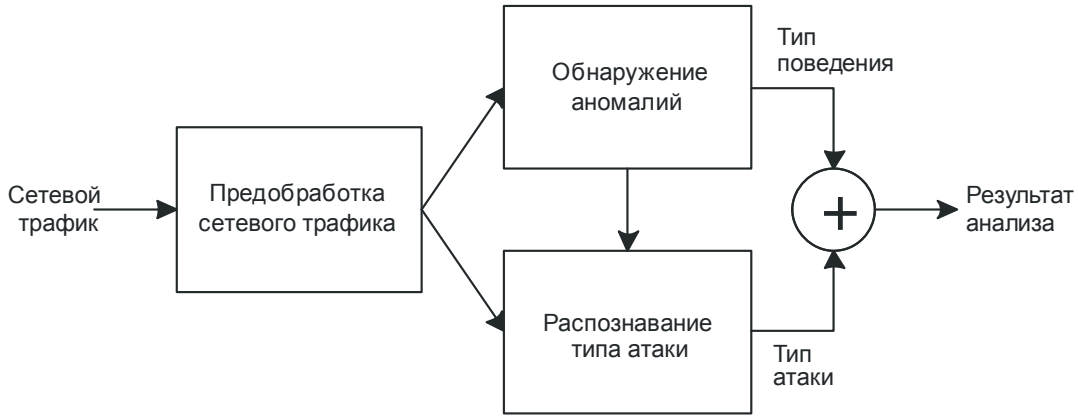

Рис. 1. Упрощенная структура СОА с детектором аномалий и блоком распознавания атаки.

Статья организована следующим образом. В разделе 2 описываются варианты организации системы обнаружения атак. В разделе 3 рассматриваются принципы применения нелинейных РНС для определения принадлежности входного образа к данному классу. Раздел 4 посвящен применению совокупности классификаторов на основе рециркуляционных нейронных сетей РНС и методике анализа и оптимизации их совместной работы. Выводы даны в 5 разделе.

2. СТРУКТУРНАЯ ОРГАНИЗАЦИЯ СОА

Существует две основных технологии обнаружения атак: обнаружение аномальной деятельности и обнаружение злоупотреблений. Основное их отличие заключается в том, что при использовании первой известно нормальное поведение субъекта и ищутся отклонения от этого поведения, в то время как при использовании второй известны именно атаки, которые ищутся и распознаются среди нормального поведения. Обе технологии нивелируют недостатки друг друга, вследствие чего наилучших результатов обнаружения можно достичь только применяя их одновременно (Рисунок 1), в рамках разных подсистем СОА [9] или с использованием комбинированных методов обнаружения [10].

Поступающий на вход системы сетевой трафик проходит предварительную обработку, после чего данные о сетевых соединениях поступают на вход детектора аномалий и блока распознавания атаки. При этом от качества работы первого зависит – будет ли она обнаружена, ведь если детектор аномалий характеризует соединение как нормальное, значит результат распознавания уже не важен. Для улучшения обнаруживающей способности детектора аномалий применяется метод обучения его на комбинированном наборе данных – нормальных соединениях и атаках [10], что приводит к комбинированию в нём обеих технологий.

Доказано [13, 14], что лучшие результаты при классификации (даже вопрос – «атака или нет?» - есть ни что иное, как определение принадлежности к классу атак или классу нормальных соединений; не говоря уже об определении класса атаки) дают независимые друг от друга классификаторы.

Основной проблемой в разработке систем из нескольких независимых детекторов или классификаторов становится вопрос выбора наиболее правдоподобного значения среди результатов, выдаваемых разными классификаторами (динамический выбор классификатора). В случае применения «слишком независимых» детекторов есть опасность, что построение общей оценки будет затруднено из-за несоизмеримости или несравнимости выходов детекторов. Так, в случае применения РНС в качестве детектора аномалий и многослойного персептрона (MLP) в качестве детектора злоупотреблений [9], можно оперировать лишь ответами детекторов – атака или нет – и никакими другими более-менее сравнимыми характеристиками (ошибка реконструкции на детекторе аномалий и значения выходов MLP не сравнимы).

Значительно больше возможностей для построения совокупной оценки общего классификатора при использовании независимых детекторов одинаковой природы. В этом случае выходы каждого отдельного детектора сравнимы между собой, и могут применяться различные методы динамического выбора классификатора: средняя оценка, максимальный голос, метод выбора “a posteriori” и др. [13], или описанные в разделе 4.

3. ДЕТЕКТОРЫ НА ОСНОВЕ РНС

3.1. Детектор аномалий

Рециркуляционные нейронные сети (рис. 2) отличаются от других ИНС тем, что на информация, подающаяся на вход в том же виде восстанавливается на выходе. Применяются они для сжатия и восстановления информации (прямое и обратное распространение информации в сетях «с узким горлом») [15], для определения резко выделяющихся векторов на фоне общего массива входных данных [16].

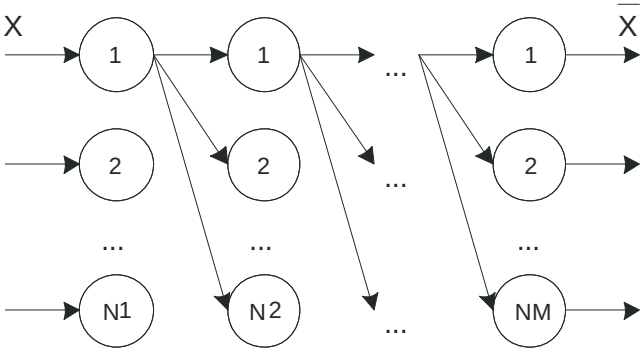

Рис. 2. Структура РНС из *M* слоёв

N_i – количество нейронных элементов в i-м слое, $NM=N1$ – количества нейронных элементов во входном и выходном слоях равны

Хорошие результаты показали нелинейные РНС в качестве детектора аномалий [9, 10]: обучение РНС производится на нормальных соединениях таким образом, чтобы входные векторы на выходе восстанавливались в себя, при этом чем соединение более похоже на нормальное, тем меньше ошибка реконструкции:

$$E^k = \sum_j (\bar{X}_j^k - X_j^k)^2, \qquad (1)$$

где X_j^k – j-й элемент k-го входного вектора, $\overline{X}_j^k$ – j-й элемент k-го выходного вектора. Если $E^k > T$, где T – некий заданный для данной РНС порог, то соединение признаётся аномалией, или атакой, иначе – нормальным соединением. При этом возникает проблема определения порога T, обеспечивающего наиболее качественное обнаружение аномальных соединений. Определить его можно исходя из минимизации суммы ошибок ложного срабатывания (FP – false positive) и неопределения атак (FN – false negative), либо основываясь на стоимостных характеристиках данных ошибок – ошибка FN обходится дороже, чем ошибка FP, соответственно стоимость у неё должна быть больше [10].

3.2. Частные классификаторы

Описанную выше методику определения принадлежности входного вектора к одному из двух классов – «нормальные» или «атаки», то есть «не-нормальные» – можно применить и прямо противоположным образом. Если при обучении детектора аномалий использовались нормальные векторы, которые восстанавливались в себя, и на основании этого делался вывод о их принадлежности к классу «нормальных», то обучая детектор на соединениях-атаках, которые должны восстановиться в себя, можно делать вывод о их принадлежности к классу «атаки». Таким образом, если в процессе функционирования данного детектора ошибка реконструкции (1) превышает определённый порог, то данное соединение можно отнести к классу «не-атак», то есть нормальных соединений. Так как обучение ведётся на векторах-атаках, то данный подход реализует именно технологию обнаружения злоупотреблений, и оправданно его употребление совместно с предыдущим подходом.

Таким образом, одна РНС может применяться для определения принадлежности входного вектора к одному из двух классов – тому, на котором обучалась (класс A), или ко второму (класс $\overline{A}$), которому соответствуют далеко отстающие вектора (outliers):

$$\begin{cases} X^k \in A, \quad если \quad E^k \le T, \\ X^k \in \overline{A}, \quad если \quad E^k > T. \end{cases} \qquad (2)$$

Стоит отметить, что можно специальным образом [10] обучать РНС на соединениях обоих классов так, чтобы повысить качество обнаружения по условиям (2).

Как уже упоминалось выше, база данных KDD включает соединения нормальные, а также атаки четырёх классов, которые радикально отличаются друг от друга. Поэтому целесообразно обучить детекторы для каждого из пяти классов отдельно, не объединяя все классы атак в единое целое.

И здесь вновь встаёт проблема выбора порога T для каждого конкретного детектора. Если для детектора аномалий можно было говорить сразу, что стоимость ошибки FN выше, чем стоимость ошибки FP, то в случае, например, детектора для класса атак R2L тяжело сказать, что будет хуже – ложное срабатывание FP (то есть назвать атакой R2L соединение, к этому классу не относящееся – атаку другого класса или нормальное соединение) или неопределение FN данной атаки (наоборот).

Многие исследователи [17] используют для определения стоимости ошибок матрицу стоимостей F (таблица 1).

Таблица 1. Матрица стоимости F ошибок неверной классификации атак

Реальный класс	Предполагаемый класс				
	normal	dos	probe	r2l	u2r
1 normal	0	2	1	2	2
2 dos	2	0	1	2	2
3 probe	1	2	0	2	2
4 r2l	4	2	2	0	2
5 u2r	3	2	2	2	0

Средние значения ошибок FP и FN каждого класса можно вычислить следующим образом:

$$F_i^{FP} = \frac{\sum_{j,\ j\neq i} F_{ji}}{N-1}, \quad F_i^{FN} = \frac{\sum_{j,\ i\neq j} F_{ij}}{N-1}, \qquad (3)$$

где N – количество классов (N=5). Исходя из данной матрицы можно сделать вывод, что ошибка FP для детектора класса normal в среднем имеет стоимость 2,5 (сумма элементов столбца normal, деленная на 4), а средняя ошибка FN будет стоить 1,75 (сумма элементов строки normal, деленная на 4). Так как ошибка FP детектора класса normal – это по сути необнаружение атаки, то есть ошибка FN всей системы, а ошибка FN детектора класса normal – ложное срабатывание (ошибка FP) всей системы, то данное соотношение повторяет сказанное выше, что ошибки FN системы обходятся дороже, чем FP.

Аналогично можно рассчитать средние стоимости ошибок F_i^{FP} и F_i^{FN} для $\forall i \in [1..5]$, то есть для детекторов всех классов (таблица 2).

Таблица 2. Средние стоимости ошибок детекторов каждого класса

Класс	Стоимость	
	F_i^{FP}	F_i^{FN}
1 normal	2,5	1,75
2 dos	2	1,75
3 probe	1,5	1,75
4 r2l	2	2,5
5 u2r	2	2,25

На основании данных стоимостей можно выбирать значение порога таким, которое минимизирует суммарную среднюю ошибку на тренировочной или валидационной выборке.

3.3. Результаты экспериментов

Для оценки эффективности предложенного подхода проведен ряд экспериментов. Обучены частные детекторы для каждого класса, причём сначала тренировочный набор выбирался из всей базы KDD, потом из выборок соединений по конкретным службам – HTTP, FTP_DATA, TELNET. Использовались нелинейные РНС с одним скрытым слоем с функцией активации гиперболический тангенс и сигмоидной функцией активации в выходном слое. Количество нейронных элементов во входном и выходном слоях согласно количеству параметров входных данных – 41, в скрытом слое – 50.

После обучения каждого детектора проводилось тестирование на тренировочной выборке с целью нахождения значения порога T, при котором средняя стоимость ошибки минимальна. В дальнейшем проводилось тестирование обученных детекторов на тестовой выборке с применением полученного ранее значения порога (таблица 3).

Таблица 3. Результаты тестирования детекторов

Служба	Порог	FP, %	FN, %	Средняя стоимость
ALL				
normal	0,00070	12,56	6,68	0,1844
dos	0,00214	4,33	1,09	0,0542
probe	0,00120	7,79	14,21	0,1675
r2l	0,00116	2,87	5,38	0,0947
u2r	0,00112	7,07	5,54	0,1323
HTTP				
normal	0,00620	2,4	0,17	0,0214
dos	0,00290	1,5	0	0,0098
probe	0,00114	0	0	0
r2l	0,00110	0	0	0
FTP_DATA				
normal	0,00123	6,8	2,72	0,0841
dos	0,00340	0	0	0
probe	0,00132	0	0	0
r2l	0,00114	5,17	0,25	0,0463
u2r	0,00126	0	0,07	0,0009
TELNET				
normal	0,00036	44,4	1,31	0,2394
dos	0,00650	0	0	0
probe	0,00162	0	0	0
r2l	0,00136	3,33	0	0,0294
u2r	0,00076	5,91	2	0,0907

4. СОВОКУПНОСТЬ ЧАСТНЫХ КЛАССИФИКАТОРОВ

4.1. Совместное функционирование

Как было сказано выше, наиболее эффективен процесс классификации при использовании нескольких независимых классификаторов одинаковой природы, поскольку построение общей оценки из частных может производиться большим числом методов. Объединим обученные в предыдущем разделе частные детекторы в один общий (рис. 3).

Основной проблемой в построении такого классификатора становится определение совокупной оценки исходя из оценок частных детекторов. В работах различных исследователей (например [13]) рассматривается множество методов, такие как нахождение среднего значения для каждого класса на основании показаний всех классификаторов, сумма голосов за каждый класс, методы оценки «a priori» и «a posteriori». Все эти методы подразумевают, что каждый классификатор даёт частную оценку относительно возможности принадлежности входного образа к сразу нескольким классам, и эти классы одинаковы для всех классификаторов. Однако в нашем случае классы, о принадлежности к которым судит каждый классификатор, во-первых, различны, во-вторых, пересекаются. Поэтому все перечисленные выше методы не применимы.

4.2. Динамический выбор классификатора

Общий классификатор состоит из $N=5$ частных детекторов, каждый из которых имеет порог T_i. Так как значения порогов на этапе обучения каждого из детекторов выбирались исходя из минимизации средней стоимости ошибки, то для приведения оценок детекторов к сравнимым значениям достаточно отмасштабировать ошибку реконструкции по порогу. Тогда (2) запишется как:

$$\begin{cases} X^k \in A_i, \quad если \quad \delta_i^k \le 1, \\ X^k \in \overline{A}_i, \quad если \quad \delta_i^k > 1, \end{cases} \tag{4}$$

где $\delta_i^k = \dfrac{E_i^k}{T_i}$ - относительная ошибка реконструкции. При этом, чем меньше δ_i^k, тем более вероятна принадлежность входного образа X^k к классу A_i. Поэтому можно выделить первый метод определения совокупной оценки – по *минимальной относительной ошибке реконструкции*:

$$\begin{cases} X^k \in A_m, \\ \delta_m^k = \min\limits_i \delta_i^k. \end{cases} \tag{5}$$

Так как целью улучшения эффективности классификации является минимизация ошибочной классификации, выражающаяся в минимизации средней стоимости классификации, то в построении совокупной оценки можно поступить так же, как и при выборе порога в частных детекторах – учесть стоимость ошибочной классификации. Если δ_i^k - показатель вероятности ошибки классификации на i-м детекторе, то оценка возможной средней стоимости ошибки на каждом из детекторов будет равна:

$$\Omega_i^k = \frac{\sum\limits_{j,j\neq i} \delta_i^k F_{ji}}{N-1}. \tag{6}$$

Оценка (6) показывает, какова возможность проигрыша в стоимости, если мы назовём вектор, принадлежащий j-му классу вектором i-го класса, т. е. будет победителем будет выбран i-й классификатор вместо j-го. На основании данной оценки выделим второй метод определения совокупной оценки – по *минимальной возможной стоимости ложной классификации*:

$$\begin{cases} X^k \in A_m, \\ \Omega_m^k = \min\limits_i \Omega_i^k. \end{cases} \tag{7}$$

Кроме того, можно учесть и взаимное влияние возможных ошибок – к оценке Ω_i^k добавить оценку того, какова возможность выигрыша в стоимости, если будет выбран i-й классификатор вместо неправильного j-го:

$$\Psi_i^k = -\frac{\sum\limits_{j,j\neq i} (\delta_j^k - \delta_i^k) F_{ij}}{N-1}. \tag{8}$$

Тогда на основании оценок (6) и (8) можно выделить третье правило определения детектора-победителя – по *минимальной возможной взаимной стоимости ложной классификации*:

$$\begin{cases} X^k \in A_m, \\ \Omega_m^k + \Psi_m^k = \min\limits_i (\Omega_i^k + \Psi_i^k). \end{cases} \tag{9}$$

4.3. Результаты экспериментов

Эффективность функционирования описанного выше общего классификатора проверим экспериментально. В качестве частных детекторов выступят детекторы из раздела 3. Результаты представлены в таблице 4.

Как видно из результатов, однозначного ответа на вопрос – какой метод лучше выбора лучше нет. Метод выбора итогового класса с использованием взаимной стоимости (9) может минимизировать ошибку, но со значительным увеличением количества ложных срабатываний (FP), методы (5) и (7) дают в основном сравнимые результаты, на какой-то службе лучше один, на какой-то – другой.

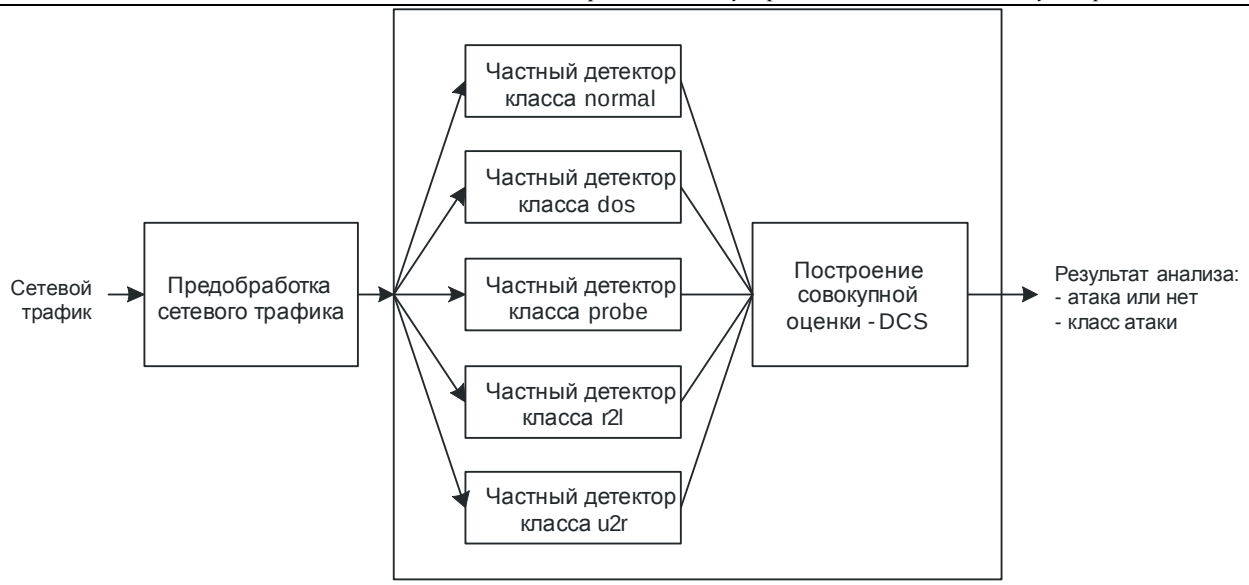

Рис. 3. Объединение независимых частных классификаторов в один общий.

Таблица 4. Результаты обнаружения и распознавания атак совокупным классификатором

Метод DCS	FP, %	FN, %	Качество распознавания				Средняя стоимость
			dos, %	probe, %	r2l, %	u2r, %	
ALL							
(5)	10,80	2,34	98,17	96,55	91,88	100	0,0617
(7)	30,80	0,87	97,83	99,28	92,50	100	0,0760
(9)	18,80	0,70	98,33	97,97	93,13	98,18	0,0745
HTTP							
(5)	0	0,08	99,75	100	100	–	0,0014
(7)	0	0,08	99,75	100	0	–	0,2871
(9)	0	0,08	99,75	100	100	–	0,0014
FTP_DATA							
(5)	0,66	1,09	100	100	96,66	100	0,0433
(7)	0,66	1,09	100	100	96,66	100	0,0433
(9)	27,33	0,36	100	77,55	98,66	100	0,1733
TELNET							
(5)	0	5,26	98,75	100	97,33	85,50	0,1507
(7)	0	5,03	97,75	100	98,00	85,50	0,1457
(9)	15,00	1,57	98,50	100	98,00	96,88	0,0689

5. ВЫВОДЫ

Сравним результаты, которые показали эксперименты с использованием описанной методики и результаты, полученные в рамках других исследований (таблицы 5 и 6).

Таблица 5. Результаты обнаружения при помощи различных технологий [8]:

Технология	FN, %	FP, %
Data mining [18]	10-30	2
Кластеризация [19]	7	10
K-NN [19]	9	8
SVM [19]	2	10

Таблица 6. Результаты распознавания классов атак в некоторых исследованиях

	dos, %	probe, %	r2l, %	u2r, %
Победитель KDD-99 [20]	97,12	83,32	13,16	8,40
SOM [8]	96,70	79,70	18,40	30,00
PHC+MLP [11]	99,98	98,78	45,20	3,84

Сравнивая значения в таблицах 4-6, можно отметить, что качество обнаружения атак по описанной методике не уступает (при применении одного классификатора для всех служб) и значительно превосходит (при применении отдельных классификаторов для каждой службы) аналоги. Уровень распознавания классов атак значительно улучшил ранее показанные результаты (PHC+MLP), особенно для атак классов r2l и u2r.

К недостаткам данной методики, над которыми необходимо работать в дальнейшем, можно отнести сильную зависимость качества обнаружения от пороговых значений частных детекторов. Значения порогов определяются, исходя из стоимостных соотношений, которые в корне своём имеют экспертную оценку, поэтому построение техники определения наилучших значений порогов только улучшит качество и стабильность работы системы.

Таким образом, можно сделать вывод, что метод совокупного классификатора на основе нелинейных рециркуляционных нейронных сетей в качестве частных детекторов может с успехом применяться для решения задач распознавания сетевых атак и других задач распознавания образов.

Исследования проводятся при поддержке БРФФИ при НАН Беларуси.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Brugger S. T. Data Mining Methods for Network Intrusion Detection. http://www.bruggerink.com/ ~zow/Projects.html

2. Лукацкий А. В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003.
3. J. Cannady. Applying Neural Networks to Misuse Detection. In *Proceedings of the 21st National Information Systems Security Conference.*
4. J. M. Bonifacio et al. Neural Networks applied in intrusion detection systems, In *Proc. of the IEEE World congress on Comp. Intell.* (WCCI'98), 1998.
5. C. Jirapummin and N. Wattanapongsakorn. Visual Intrusion Detection using Self-Organizing Maps. In *Proc. of Electrical and Electronic Conference (EECON-24)*, Thailand, Vol. 2, pp. 1343-1349, 2001.
6. D. Joo, T. Hong and I. Han. The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors. *Expert Systems with Applications, 25 (2003)*, pp. 69-75
7. C. Zhang, J, Juang, M. Kamel. Intrusion detection using hierarchical neural networks. *Pattern Recognition Letters (2004).*
8. H. G. Kayacik. Hierarchical self organizing map based IDS on KDD benchmark. M. Sc. work, Dalhousie university, Halifax, Nova Scotia, 2003.
9. Головко В. А., Каменда Д. В., Кочурко П. А. Некоторые аспекты применения нейронных сетей для обнаружения сетевых атак *Вестник БГТУ. Физика, математика, информатика*. – 2004. - №5(29). – С. 35-39
10. П. Кочурко. Нейросетевой детектор аномалий. Известия Белорусской инженерной академии, № 1(19)/2'2005 – с. 78-81.
11. V. Golovko, P. Kochurko. Intrusion recognition using neural networks. *International Scientific Journal of Computing*, vol.4, issue 3, 2005, p.37-42
12. KDD Cup'99 Competition, 1999, http://kdd.ics.uci.edu/ databases/kddcup99/ kddcup99.html
13. Giacinto G., Roli F., Fumera G. Selection of image classifier. *Electron*, 26(5), 2000, pp. 420-422.
14. Xu L., Krzyzak A., Suen C. Y. Methods for combining multiple classifiers and their applications to handwriting recognition. *IEEE Trans. Syst. Man Cybernitics*, 22, 1992, pp. 418-435
15. Головко В. А. Нейронные сети: обучение, организация и применение. М.: ИПРЖР, 2001.
16. S. Hawkins, H. He, G. Williams, R. Baxter. Outlier Detection Using Replicator Neural Networks. In *Proc. of the 4th International Conference on Data Warehousing and Knowledge Discovery (DaWaK02) Lecture Notes in computer Science*, Vol. 2454, Springer, Pages 170-180, ISBN 3-540-44123-9, 2002
17. Giacinto G., Roli F., Didaci L. Fusion of multiple classifiers for intrusion detection in computer networks. *Pattern Recognition Letters*, 24, 2003, pp. 1795-1803
18. Lee W., Stolfo S. A Framework for Constructing Features and Models for Intrusion Detection Systems. *Information and System Security*, 3(4), 2000, pp. 227-261
19. Eskin E., Arnold A., Prerau M., Portnoy L., and Stolfo S. A Geometric Framework for Unsupervised Anomaly Detection: Detecting intrusiond in unlabeled data. In D. Barbara and S. Jajodia editors, *Applications of Data Mining in Computer Security.* Kluwer, 2002.
20. Pfahringer B. Winnings the KDD99 Classification Cup: Bagged Boosting. *SIGKDD Explorations*, 1(2), 2000, pp. 65-66.

УДК 004.8.032.26

Безобразов С.В.

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ ВИРУСОВ

ВВЕДЕНИЕ

Развитие новых информационных технологий предоставило не только уникальные возможности для более активного и эффективного развития экономики, политики, государства и общества, но и стимулировали возникновение и развитие компьютерной преступности. Ярким и наиболее опасным примером компьютерной преступности является написание и распространение компьютерных вирусов – автономно функционирующих программ, способных к самостоятельному внедрению в тела других программ, к последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ, и выполняющих нежелательные для пользователя ЭВМ действий [1].

Число компьютерных преступлений растет и, ущерб от них увеличивается (рис. 1).

Современные антивирусные программы не обеспечивают должный уровень защиты компьютерной системы от заражения вирусом. Традиционные антивирусные программы имеют ряд существенных недостатков. Рассмотрим наиболее серьезные из них:

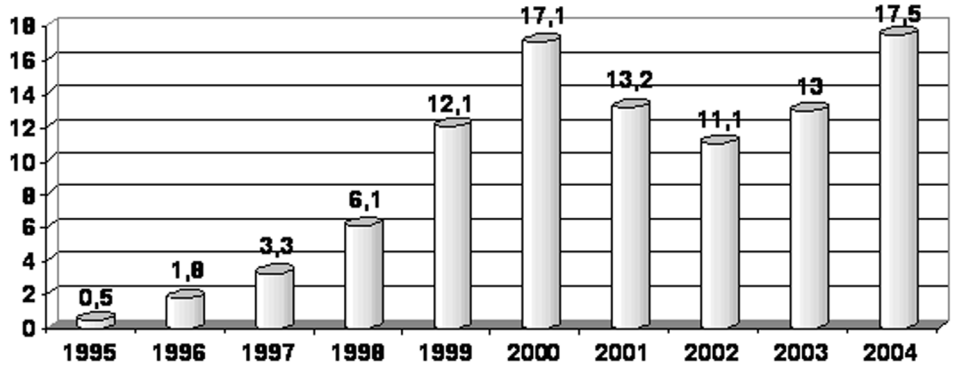

Рис. 1. Ущерб от компьютерных преступлений.

Безобразов С.В., *аспирант каф. интеллектуальных информационных технологий Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, Беларусь, г. Брест, ул. Московская, 267.