[illegible] 004.89

[illegible]

[illegible]

Введение. Обеспечение информационной безопасности является первостепенной задачей каждого государства. В эпоху компьютеризации и автоматизации проблема компьютерной безопасности выходит на первый план. Одна из задач, которую приходится решать в контексте информационной безопасности, – защита информации, которая хранится, обрабатывается и передается в компьютерных системах и сетях. Одной из угроз компьютерной безопасности являются сетевые атаки. Под сетевой (или хакерской) атакой понимается информационное разрушающее воздействие, осуществляемое программным методом и направленное на распределенную вычислительную систему [1]. В зависимости от метода организации сетевой атаки и используемых средств выделяют несколько разновидностей сетевых атак – *DoS*, *U2R*, *R2L* и *Probe* (подробное описание каждой из разновидности атак представлены ниже).

Основным недостатком существующих систем защиты от сетевых атак, основанных на традиционных методах, является их неспособность обнаруживать новые или неизвестные атаки, которые характеризуются отсутствием записей в системе о них. Современные системы обнаружения вторжений также плохо приспособлены к работе в реальном режиме времени, что снижает их эффективность использования в системах защиты. Постоянно изменяющаяся природа сетевых атак требует гибкой защитной системы, которая способна анализировать грандиозное количество сетевого трафика [2].

В связи с несовершенством существующих методов защиты компьютерных систем от сетевых атак, разработка новых методов защиты информации, позволяющих повысить уровень защищенности компьютерных систем от несанкционированного воздействия, является актуальной и востребованной.

Обзор существующих систем обнаружения сетевых атак. Обнаружение сетевых атак на компьютерную систему происходит посредством анализа сетевого трафика – данные, которые поступают в систему или отправляются из нее. Для ясности процесса обнаружения рассмотрим параметры сетевого трафика, которые анализируются для обеспечения безопасности компьютерных систем, а также о типах сетевых атак.

Данные в компьютерных сетях передаются в виде сетевых пакетов. В структуре сетевого пакета выделяют три основных поля (рис. 1): заголовок пакета, поле данных пакета, заключение пакета [3].

Заголовок пакета содержит стартовую комбинацию, которая обеспечивает настройку сетевого оборудования на прием и обработку пакета, а также сетевые адреса приемника и передатчика пакета и некоторую общую служебную информацию.

Поле данных пакета содержит в себе собственно информацию, которая и передается от передатчика приемнику.

Заключение пакета содержит в себе контрольную сумму, которая позволяет судить об успешности передачи информации, стоповую комбинацию, которая служит для информирования об окончании пакета, а также некоторую служебную информацию.

Выделяют 41 параметр (или атрибут) сетевого соединения, которые в свою очередь объединены в 3 группы [4]:

а) *Встроенные атрибуты*. Эти атрибуты извлекаются из зоны заголовка сетевых пакетов. Выделяют 9 встроенных атрибутов, которые содержат информацию о времени работы соединения, типе протокола, количестве переданных байт и т.д.

б) *Атрибуты контента*, которые извлекаются из зоны контента и содержат такую информацию, как: количество неудачных попыток регистрации, количество неудачных попыток регистрации в системе, количество возникновений ошибок, количество операций создания файлов и т.д. Существует 13 атрибутов контента.

в) *Атрибуты трафика*. Вычисляются исходя из предыдущих соединений. В свою очередь выделяют атрибуты временного и машинного трафика. 19 атрибутов трафика содержат следующую информацию: количество соединений к этому же IP адресу, количество соединений к этому же номеру порта и т.д.

В зависимости от используемых техник при совершении несанкционированных воздействий на компьютерную систему выделяют 4 типа сетевых атак [4].

DoS (denial of service) атаки – это сетевые атаки, направленные на возникновение ситуации, когда на атакуемой системе происходит отказ в обслуживании. Данные атаки характеризуются генерацией большого объема трафика, что приводит к перегрузке и блокированию сервера. Выделяют шесть *DoS* атак: *back, land, neptune, pod, smurf, teardrop*.

U2R (user-to-root) атаки предполагают получение зарегистрированным пользователям привилегий локального суперпользователя (администратора). Выделяют четыре типа *U2R* атак: *buffer_overflow, loadmodule, perl, rootkit*.

R2L (remote-to-local) атаки характеризуются получением доступа незарегистрированного пользователя к компьютеру со стороны удаленной машины. Выделяют восемь типов *R2L* атак: *ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster.*

Probe атаки заключаются в сканировании сетевых портов с целью получения конфиденциальной информации. Выделяют четыре типа *Probe* атак: *ipsweep, nmap, portsweep, satan.*

В самом простом случае система защиты от сетевых атак может представлять собой межсетевой экран (firewall), он же брандмауэр [2, 5]. Сетевой экран представляет собой программное или аппаратное средство фильтрации сетевого трафика посредством анализа его параметров, таких как адреса источника и приемника, типов се-

Рис. 1. Структура сетевого пакета

Комар Мирослав Петрович, *аспирант кафедры информационно-вычислительных систем и управления Тернопольского национального экономического университета.*

тевых протоколов и служб и т.д. Главным отличием сетевого экрана от системы обнаружения вторжений (см. ниже) является то, что в нем отсутствует анализ содержимого передаваемых пакетов. Соответственно, сетевые экраны обладают высокой скоростью обработки входящих и исходящих сетевых пакетов, и работают, как правило, основываясь на наборе правил. Недостатком таких систем является низкий уровень предоставляемой защиты, поскольку отсутствует анализ содержимого пакетов.

Система обнаружения вторжений (Intrusion Detection System - IDS) [6] на сегодняшний день является неотъемлемой частью системы безопасности любой компьютерной системы, подключенной к локальной или глобальной компьютерной сети. IDS, как правило, это программное или аппаратное средство, которое является «фильтром», находится между компьютерной системой и компьютерной сетью и анализирует параметры входящего и исходящего трафика с целью выявления фактов неавторизованного доступа. IDS перехватывает весь сетевой трафик и анализирует содержимое каждого пакета на наличие вредоносных компонентов.

Анализ показал, что существующие системы обнаружения вторжений имеют ряд существенных недостатков. А именно, они: а) обладают высокой ресурсоемкостью, из-за этого не всегда имеется возможность обрабатывать и анализировать все сетевые пакеты, что приводит к пропуску атаки; б) не способны анализировать зашифрованную информацию; в) имеют слабые способности обнаружения новых типов атак; г) требуют определенный уровень знаний в области безопасности; д) имеют высокий уровень ошибок первого и второго родов, когда нормальное соединение принимается за атаку и наоборот.

Для устранения перечисленных недостатков автором предложено применить нейронные сети в средствах защиты компьютерных систем от воздействия атак, что описано ниже.

Применение метода нейронных сетей для обнаружения сетевых атак. Искусственная нейронная сеть (ИНС) является математической (а также программной или аппаратной) моделью, построенной по принципу организации и функционирования биологических нейронных сетей. Сегодня существует несколько архитектур искусственных нейронных сетей, которые с успехом применяются для решения сложных технических и экономических задач. Некоторыми из особенностей ИНС являются способность в процессе обучения выявлять сложные зависимости между входной и выходной информацией, которая отсутствовала в обучающей выборке, и, способность корректно классифицировать зашумленные образы. Нейронные сети обладают рядом достоинств, которые выгодно отличают их от традиционных решений. Некоторые из них: высокая степень параллелизма обработки информации; способность к обобщению, адаптация к изменениям окружающей среды; распознавание зашумленных образов; низкий уровень ресурсоемкости и т.д. Перечисленные особенности и преимущества послужили основой для выбора структуры детектора обнаружения сетевых атак.

В качестве нейросетевого детектора для обнаружения сетевых атак была выбрана многослойная нейронная сеть с одним скрытым слоем, состоящим из нейронов Кохонена [7] (рис. 2).

Первый слой нейронных элементов распределяет входные сигналы *X*-41 параметр сетевого соединения на нейронные элементы скрытого слоя. Количество нейронных элементов распределительного слоя равняется количеству атрибутов сетевого трафика *n = 41*.

Второй слой состоит из *m = 41* нейронов Кохонена, которые используют конкурентный принцип обучения и функционирования в соответствии с правилом «победитель берет все» (*winner-take-all*) [7,8,9]. Это означает, что выходное значение нейрона-победителя равняется «1», а выходные значения остальных нейронных элементов равняются «0». Для определения нейрона-победителя используется Евклидово расстояние между входным и весовыми векторами.

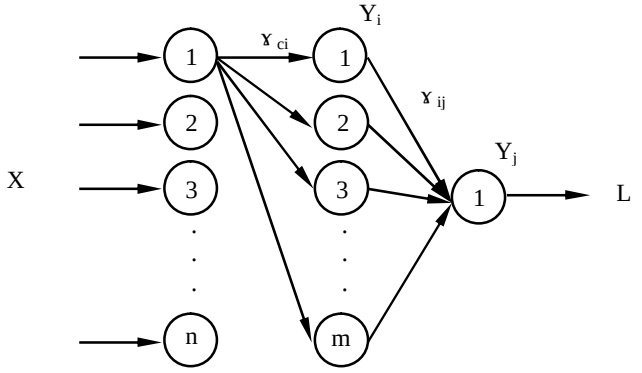

Рис. 2. Нейросетевой детектор

Так Евклидово расстояние между входным и весовым вектором *i*-го нейронного элемента определяется следующим образом:

$$D_i = \left| X - \omega_i \right| = \sqrt{(X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + ... + (X_c - \omega_{ci})^2}\,, \quad (1)$$

где ω_{ci} – весовой коэффициент между *i*-м нейроном распределительного слоя и *i*-м нейроном слоя Кохонена,

$X = [X_1, X_2, \ldots X_n]$ – входной образ.

Нейронный элемент-победитель с номером *k* определяется в соответствии с минимальным Евклидовым расстоянием.

Стоит отметить, что количество нейронов слоя Кохонена *m* не обязательно должно быть равным *41*. Проведенные эксперименты показали, что для разного класса атак при разной размерности обучающей выборки нейросетевой детектор быстрее обучается при разных значениях *m*. Однако влияние количества нейронов скрытого слоя не столь существенно и может варьироваться в пределах от *10* до *41*.

Третий слой состоит из одного линейного нейронного элемента, который осуществляет отображение кластеров, сформированных слоем Кохонена в два класса, которые характеризуют нормальное соединение или атаку. Активность выходного нейрона, когда значение его равно единице, характеризует атаку. Ноль на выходе характеризует нормальное соединение.

Для каждого типа сетевой атаки, а их насчитывается 22 типа, формируется отдельный нейросетевой детектор. Для обучения предложенного нейросетевого детектора используется обучающая выборка, состоящая из 80% соединений одного из типов атак и 20% нормального соединения. Результаты экспериментов показали, что наилучший процент обучаемости и обнаружения происходит, когда обучение производится на 32 соединений сетевой атаки и 8 соединений легитимного, нормального трафика.

В результате, предлагаемая система анализа сетевого трафика для обнаружения компьютерных атак состоит из 22 нейросетевых детекторов, каждый из которых характеризует определенный тип атаки. На нейросетевые детекторы поочередно подается 41 параметр сетевого соединения и происходит проверка на наличие запрещенных действий (рис. 3).

Результаты экспериментов. Для тестирования разработанной системы был проведен ряд экспериментов. В качестве входных данных для обучения и тестирования использовалась база данных *KDD Cup1999 Data* [4,10]. Данная база была сформирована в рамках про-

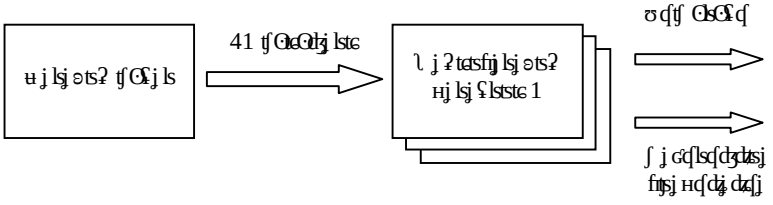

Рис. 3. Система анализа сетевого трафика для обнаружения компьютерных атак

ведения международной научной конференции KDD-99, целью которой было стимулирование исследований в области обработки данных и создания новых алгоритмов обнаружения сетевых атак. База содержит параметры как нормальных сетевых соединений, так и сетевых атак. *KDD Cup1999 Data* широко используется как один из немногих общедоступных наборов данных для сетевых систем обнаружения атак [11].

Таблица 1 содержит результаты обнаружения сетевых атак разных классов различными методами [12]. Как видно из представленных результатов, предлагаемый подход показывает лучшие результаты обнаружения сетевых атак. Следует отметить, что процент ложных обнаружений, когда легитимное соединение принимается за атаку, составляет менее 10%. Также стоит отметить, что в таблице представлены средние результаты по 4 классам сетевых атак.

Если брать отдельные типы атак, то тут явно можно выделить такие атаки, обнаружение которых происходит со 100% вероятностью (например, *neptune, teardrop*), и атаки, обнаружение которых не происходит (например, *guess_passwd, spy*) (таблица 2–5).

Таблица 1. Результаты обнаружения сетевых атак

	DoS, %	Probe, %	R2L, %	U2R, %
Нейросетевой детектор	**98,0**	**92,8**	**36,5**	**30,8**
Гауссовский классификатор	82,4	90,2	9,6	22,8
K-NN	97,3	87,6	6,4	29,8
Алгоритм ближайшего кластера	97,1	88,8	3,4	2,2
Лидер-алгоритм	97,2	83,8	1,0	6,6
Алгоритм гиперсферы	97,2	84,8	1,0	8,3
Fuzzy Art Map	97,0	77,2	3,7	6,1
Дерево решений C4.5	97,0	80,8	4,6	1,8
Победитель KDD-99	97,1	83,3	13,1	8,4

Таблица 2. Результаты обнаружения DoS-атак

Back, %	Land, %	Neptune, %	Pod, %	Smurf, %	Teardrop, %
99,5	90,5	100,0	98,1	100,0	100,0
Среднее = 98,0					

Таблица 3. Результаты обнаружения Probe-атак

Ipsweep, %	Nmap, %	Portsweep, %	Satan, %
98,0	74,5	99,6	99,3
Среднее = 92,8			

Таблица 5. Результаты обнаружения U2R-атак

Buffer_overflow, %	Loadmodule, %	Perl, %	Rootkit, %
73,3	0,0	0,0	50,0
Среднее = 30,8			

Заключение. Предлагаемый подход, основанный на применении метода нейронных сетей в качестве детекторов сетевых атак, позволяет повысить уровень обнаружения сетевых вторжений на компьютерные системы. Обнаружение некоторых типов атак происходит со 100% вероятностью при незначительном уровне ложных обнаружений. Кроме этого, предполагаемый подход не требователен к ресурсам системы и способен обнаруживать неизвестные типы атак (детекторы, обучаемые на одном типе атак, зачастую показывают хорошие результаты обнаружения других типов атак, т.е. на тех данных, на которых обучение не производилось, например, детектор, обучен на атаке DoS_neptune может обнаруживать атаку Probe_portsweep с вероятностью 99,61%, атаку Probe_satan с вероятностью 98,42%, атаку R2L_imap с вероятностью 50%).

Однако не все типы сетевых атак подвергаются обнаружению и могут быть пропущены. Для решения этой проблемной задачи в дальнейшем предлагается изменить структуру нейросетевого детектора и доработать алгоритм обучения нейронной сети.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Удаленные сетевые атаки. [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Удаленные_сетевые_атаки.
2. Лукацкий, А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ-Петербург, 2003. – 596 с.
3. Олифер, Н.А. Компьютерные сети. Принципы, технологии, протоколы / Н.А. Олифер, В.Г. Олифер. – СПб.: Питер, 2010. – 944с.
4. KDD Cup 1999 Data [Электронный ресурс]. – Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
5. Межсетевой экран. [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Межсетевой_экран.
6. Vacca, J.R. Computer and information security handbook / J.R. Vacca. – Morgan Kaufmann.: Computers, 2009. – 844c.
7. Kohonen, T. Sell-organised formation of topologically correct feature maps / T. Kohonen // Biological Cybernetics. – 1982. – N43. – P. 59-69.
8. Головко, В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение : учеб. пособие / В.А. Головко. – М., 2001 – 256 с.
9. Хайкин, С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1104 с.
10. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999.
11. Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali, A. Ghorbani, “ A Detailed Analysis of the KDD CUP 99 Data Set” / Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009). DOI: 10.1109/CISDA.2009 .5356528. Publication Year: 2009 , Page(s): 1 – 8.
12. KDD Cup 1999: Results [Электронный ресурс]. – Режим доступа: http://www.sigkdd.org/kddcup/index.php?section=1999&method=res.

Таблица 4. Результаты обнаружения R2L-атак

Ftp_write, %	Guess_passwd, %	Imap, %	Multihop, %	Phf, %	Spy, %	Warezclient, %	Warezmaster, %
25,0	0,0	50,0	28,5	100,0	0,0	29,0	80,0
Среднее = 36,5							

29.11.10

KOMAR M.P. System for analyzing network traffic to detect computer attacks

In this article are presented network traffic analysis system for detecting network attacks on computer systems based on application method of artificial intelligence – artificial neural networks. The Neural networks allow to create "intelligent" system in which the detectors can effectively detect not only known but also unknown cyber attacks. The structure, functioning and learning algorithms of neural detectors are presented. The results of studies that prove the effectiveness of the proposed approach are also presented.