ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056

НЕЙРОСЕТЕВАЯ ТЕХНОЛОГИЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

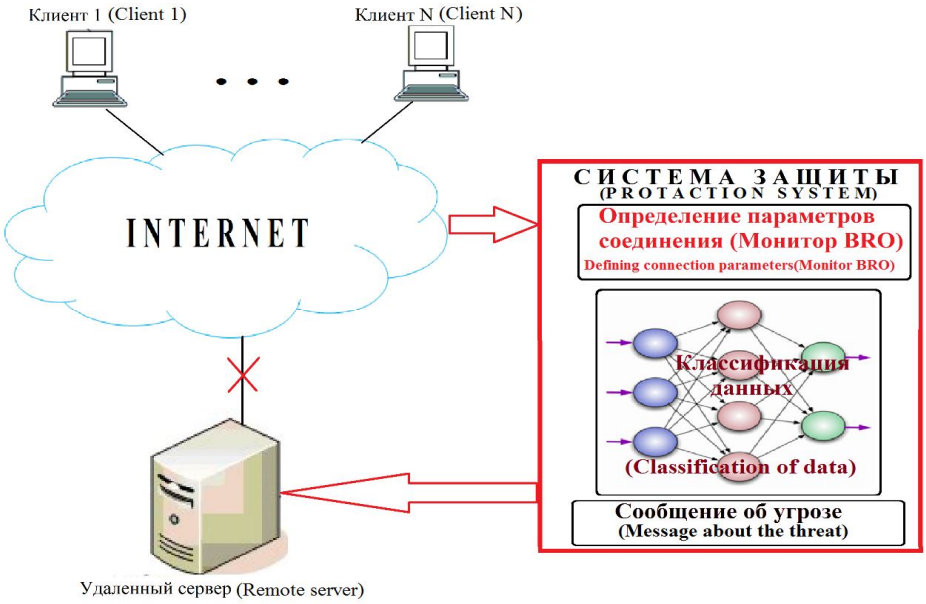
Статья поступила в редакцию 19.09.2018, в окончательном варианте – 22.10.2018.

Кочетов Дмитрий Алексеевич, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
магистрант, e-mail: aziris_nuna@list.ru
Лукащик Елена Павловна, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,
кандидат физико-математических наук, доцент, e-mail: lep_9091@mail.ru

Эффективность системы защиты информации в компьютерной сети во многом зависит от того, какая технология была выбрана для обнаружения сетевых вторжений. Наиболее перспективной для этих целей в настоящее время является нейросетевая технология. Искусственные нейронные сети после обучения способны адаптироваться под новые типы угроз; распознавать их, даже если они до этого с ними не сталкивались. Эта особенность позволяет системе защиты, построенной на основе искусственных нейронных сетей, быть более гибкой и независимой от типов угроз. В статье рассмотрены возможности нейросетевой технологии, предназначенные для создания системы обнаружения сетевых атак. Эта нейросетевая технология способна захватить поток данных из сети, проанализировать эти данные и, в случае обнаружения угрозы, сообщить об этом администратору. Был проведен ряд вычислительных экспериментов, включающих построение различных типов нейронных сетей, обучение их несколькими методами, тестирование для оценки эффективности защиты. В результате тестирования была выбрана архитектура нейронных сетей, наиболее полно и точно классифицирующая входные данные. Для проведения тестирования разработанного авторами программного обеспечения был развернут виртуальный комплекс у хостинг-провайдера Flops. На этот сервер был направлен трафик различных сетевых сервисов. Результаты проведенных компьютерных экспериментов показывают эффективность применения нейронных сетей при решении задач обеспечения безопасности информационной системы, использующей компьютерную сеть.

Ключевые слова: информационная безопасность, сетевая атака, обнаружение вторжений, нейронные сети, сети Кохонена, многослойный персептрон, Python, вычислительные эксперименты

Графическая аннотация (graphical annotation)



NEURAL NETWORK TECHNOLOGY FOR DETECTION OF NETWORK INTRUSIONS

The article was received by editorial board on 19.09.2018, in the final version – 22.10.2018.

Kochetov Dmitriy A., Kuban State University, 149, Stavropolskaya St., Krasnodar, 350040, Russian Federation,

undergraduate student, e-mail: aziris_nuna@list.ru

Lukashchik Elena P., Kuban State University, 149, Stavropolskaya St., Krasnodar, 350040, Russian Federation,

Cand. Sci. (Physics and Mathematics), Associate Professor, e-mail: lep_9091@mail.ru

The efficiency of an information protection system in a computer network depends on the type of technology chosen for the detection of network intrusions. At present, the neural network technology is the most promising for these purposes. Having been trained, synthetic neural networks are able to adapt to new types of threats and recognize them even if they did not detect them before. This feature allows a protection system based on synthetic neural networks to become more flexible and independent. This article demonstrates the application of the neural network technology for building a protection system. This technology can capture a data stream from the network, analyze these data and, in case of a threat, inform the administrator. A number of simulation experiments were carried out, including the creation of different types of neural networks, its training with the use of different methods and testing for security efficiency assessment. As a result, the neural network architecture that classifies input data most accurately and fully has been chosen. A virtual server was deployed at the hosting provider *Flops* to test the software of the developed detection system. The traffic from different services was directed to that server. The results of computer-aided experiments for different types of attacks prove the efficiency of neural network method to solve the problems of safety of the computer information system based on a computer network.

Keywords: information security, network attack, intrusion detection, neural networks, Kohonen networks, multilayer perceptron, Python, simulation experiments

Введение. В последние годы информационные ресурсы и сервисы все чаще сталкиваются с попытками вредоносных воздействий, осуществляемых с использованием протоколов межсетевого взаимодействия – удаленной сетевой атакой. Такие атаки при неблагоприятных условиях оказывают информационное разрушающее воздействие на распределённую вычислительную систему [2]. В настоящее время информационные и сетевые технологии интенсивно развиваются. В процессе развития они меняются настолько быстро, что статичные защитные механизмы, такие как разграничение доступа и системы аутентификации во многих случаях не могут обеспечить достаточно эффективную защиту. Поэтому требуются динамические методы, способные в короткий срок обнаружить попытки нарушения информационной безопасности и предотвратить их. Как следствие, в современные системы сетевой безопасности целесообразно (необходимо) включать интеллектуальные составляющие.

Искусственная нейронная сеть (НС) является одной из технологий создания интеллектуальных систем, основанных на имитации поведения человеческого мозга при анализе информации и обосновании (выборе) принимаемых решений. После обучения искусственные НС способны адаптироваться под новые типы угроз, распознавая их, даже если ранее до этого с ними не сталкивались. Данная особенность позволяет системе защиты, использующей искусственную НС, стать более гибкой и независимой [1]. Целью данной работы является представление методологии построения системы обнаружения сетевых атак на основе нейросетевой технологии; демонстрация эффективности такого подхода.

Архитектура системы защиты. Базовыми функциями разработанной системы обнаружения несанкционированных вторжений являются следующие: получение данных о соединении с «сетевой карты»; классификация вторжений по типам атак; отправка пользователю (администратору системы) уведомления при обнаружении угрозы. Структура комплекса включает три модуля:

1) модуль сбора информации о пакетах в сети;
2) модуль классификации сетевых данных;
3) модуль оповещения администратора.

С целью получения оптимальных значений параметров конфигурации системы производилось ее тестирование на наборе данных KDD Cup 1999 [11]. Он представляет собой совокупность смоделированных необработанных данных дампа TCP. Такой набор содержит около 5 миллионов классифицированных по 22 типам (классам) экземпляров атак записей. Каждая запись состоит из 41 параметра, характеризующего сетевое подключение, и метки о том, является подключение вредоносным или нет [8].

Типы атак сгруппированы в четыре группы (категории) [14]:

1) Denial of Service Attack (DoS) – отказ в доступе легальному пользователю;

2) User to Root Attack (U2R) – злоумышленник, получив доступ к системе в качестве рядового пользователя, пытается эксплуатировать уязвимость системы и стать «суперпользователем»;

3) Remote to Local Attack (R2L) – злоумышленник пытается получить удаленный доступ к системе с неавторизированной машины (компьтера);

4) Probe – сбор информации о вычислительной сети с целью обхода её системы управления безопасностью.

При разработке модуля сбора информации использовался монитор сетевой безопасности Bro. Архитектурно Bro (рис. 1) делится на два основных компонента. Первый компонент (механизм событий или ядро) переводит поток входящих пакетов в ряд событий. Эти события описывают параметры, характеризующие имеющую место сетевую активность. Например, HTTP-запрос превращается в соответствующее событие http_request. Оно характеризует задействованные IP-адреса и порты; запрашиваемый URI; используемую версию HTTP [3].

Осмысление полученной информации, т.е. получение ответа, соответствует ли этот URI известному сайту вредоносного ПО, производится вторым семантическим компонентом Bro (интерпретатором сценария) путем выполнения обработчиков событий, написанных на пользовательском языке сценариев Bro. Эти сценарии отражают политику безопасности сайта, т.е., какие действия следует предпринять, когда монитор обнаруживает различные виды деятельности, представляющие угрозу информационной безопасности. Эта компонента в системе защиты называется «модулем классификации».

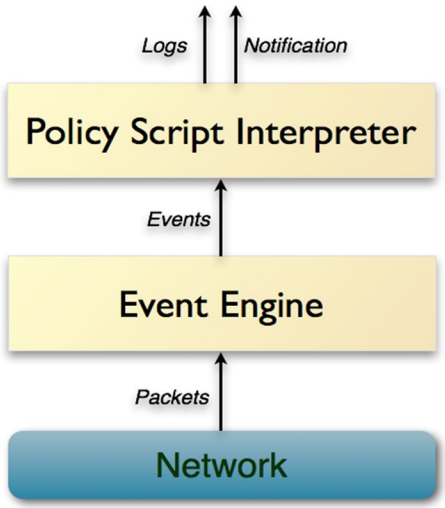


Рисунок 1 – Архитектура монитора BRO

Для определения наиболее подходящей архитектуры НС, используемой для классификации сетевых данных, был проведен ряд вычислительных экспериментов. В результате оптимальной для анализа трафика оказалась гибридная НС [7], состоящая из самоорганизующейся сети Кохонена и многослойного персептрона [5].

При применении сети Кохонена происходит кластеризация входных данных в узлы матрицы, в которых будут сгруппированы события по числовым символам. Фактически отдельные узлы представляют собой определённые сценарии атак. Входной вектор данной сети содержит 35 компонентов, соответствующих параметрам записи в базе данных KDD99. На выходе матрица содержит 22 узла, которые соответствуют типам атак [4].

После этого набор параметров трафика и информация о номере узла из сети Кохонена подается на вход многослойного персептрона, обученного распознавать аномальный трафик, но уже с учетом информации о событии, т.е. принадлежности пакетов к той или иной группе.

Для определения структуры НС, при использовании которой процент корректной классификации сетевых данных имел бы наибольшее значение, было проведено исследование с использованием многослойного персептрона, содержащего три типа слоев нейронов: входной, один скрытый и выходной слой. Входной слой нейронной сети имеет 41 нейрон, скрытый слой содержит 82 нейрона, выходной слой имеет 22 нейрона, соответствующих типам атак, взятым из базы данных KDD99. При проектировании сети с другим количеством нейронов в скрытом слое процент ошибок первого и второго рода увеличивался. В ходе выполнения экспериментов в качестве функции активации для нейронов скрытого слоя использовались следующие функции:

- линейная функция;
- сигмоид;
- гиперболический тангенс;
- функция Гаусса;
- LSTM.

В качестве метода для обучения многослойного персептрона использовались метод обратного распространения ошибки и пороговый алгоритм обратного распространения ошибки.

В результате проведенных исследований был подобран метод обучения НС, а также функция активации для нейронов скрытого слоя, при использовании которых процент корректной классификации данных имел наибольшее значение. Данным методом является пороговый алгоритм обратного распространения ошибки, а функцией активации – гиперболический тангенс.

Экспериментальное обучение НС осуществлялось на наборе данных KDD99 [9] сокращённого объема, содержащего 10 % записей от полного набора, включающего в себя информацию о нормальных подключениях и сетевых атаках.

Данные таблицы 1 показывают, что гибридная НС позволяет не только обнаружить сетевые вторжения в единичных пакетах, но и выявить принадлежность пакета к распределённой по времени атаке.

Таблица 1 – Точность и полнота определения сетевых атак

Группа	**Класс**	**Полнота**	**Точность**
probe	satan	0,9895	0,9795
u2r	rootkit	0,1429	0,1667
probe	portsweep	0,9842	0,9987
dos	back	0,6633	0,7224
u2r	buffer_overflow	0,7500	0,0325
r2l	ftp_write	0,25	0,9852
r2l	guess_passwd	0,9623	0,1683
r2l	imap	0,8333	0,3030
probe	ipsweep	0,9704	0,9920
dos	land	0,9566	0,9245
u2r	loadmodule	0,5	0,9536
r2l	multihop	0,5714	0,7265
dos	neptune	0,9996	0,991
probe	nmap	0,9253	0,6871
normal	normal	0,9966	0,9969
u2r	perl	0,5	0,6666
r2l	phf	0,3333	0,0240
dos	pod	0,7843	0,2492
dos	smurf	0,9992	0,9925
r2l	spy	0,5	0,444
dos	teardrop	0,9975	0,6552
r2l	warezclient	0,9612	0,8226
r2l	warezmaster	0,95	0,8913

В данной работе понятия «точности» и «полноты» определяются так:

- точность – доля правильно обнаруженных алгоритмом сетевых атак относительно всех обнаруженных атак в тестовом наборе данных;
- полнота – доля найденных алгоритмом сетевых атак относительно всех существующих атак в тестовом наборе данных.

При всем существующем разнообразии методов интеллектуального анализа и машинного обучения практически все они сталкиваются с общей трудностью – вопросом отбора значимых для модели входных данных (Feature Selection). Отбор признаков – это процесс выбора признаков, имеющих наиболее тесные взаимосвязи с целевой переменной. Отбор признаков перед моделированием обеспечивает три следующих преимущества.

1) уменьшение вероятности переобучения модели. Чем меньше избыточных данных, тем меньше возможностей у модели принимать решения на основе «шума»;
2) повышение точности. Чем меньше противоречивых данных, тем выше точность решения;
3) сокращение времени обучения. Чем меньше данных, тем быстрее обучается модель.

В данной работе для отбора признаков использовалось два метода. Первым является метод, реализованный в модуле *Feature Selection* в программе Statistica. Он специально разработан для обработки чрезвычайно больших наборов непрерывных и/или категориальных независимых переменных с целью определения значащих предикторов регрессии или проблем классификации. Признаки, имеющие наиболее выраженную взаимосвязь с зависимой переменной, могут быть отобраны с помощью статистических критериев. В модуле Feature Selection реализован одномерный отбор «К» лучших признаков на основе критерия *хи-квадрат*.

Второй метод для отбора значимых признаков использует ансамблевые алгоритмы на основе деревьев решений, такие как случайный лес (*random forest*). Данный метод оценивания предикторов был реализован на языке Python с применением библиотеки Scikit-learn.

Результаты, полученные в ходе эксперимента с применением многослойного персептрона, показали, что удаление незначащих предикторов уменьшило процент ошибок при обучении и классификации входных данных по типам атак. Рисунки 2–3 демонстрируют увеличение точности и полноты классификации данных по типам атак при удалении незначащих и наименее влияющих признаков (набор данных № 1 – полный набор данных KDD'99; набор данных № 2 – набор с удаленными незначимыми признаками; набор данных № 3 – набор с удаленными незначимыми и наименее влияющими признаками).

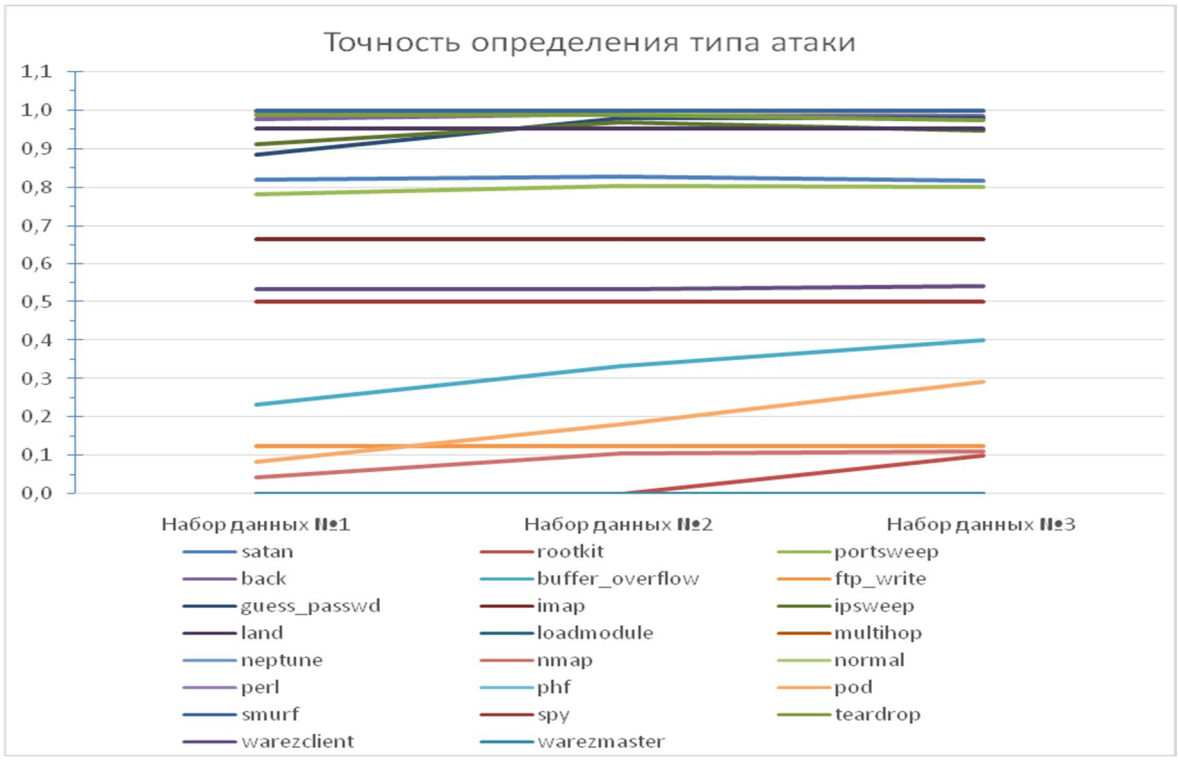


Рисунок 2 – Характеристики точности определения сетевых атак

Рисунок 3 – Характеристики полноты определения типа атаки

Таким образом, чем меньше будет ошибок первого и второго родов при обнаружении сетевых атак, тем более точным и полным будет алгоритм по их обнаружению.

В ходе исследования был проведен эксперимент, направленный на сравнение точности и полноты классификации наборов входных данных с определением самого факта атаки, без определения конкретной группы вторжения или его класса. Данное сравнение выполнялось с использованием массивов с полным перечнем параметров, а также с наиболее значимыми показателями. Результаты такой классификации приведены в таблице 2. Тестирование показывает достаточно высокие показатели качества распознавания сетевых атак.

Таблица 2 – Характеристика точности и полноты определения сетевых атак

Набор данных	Класс	Полнота	Точность
№ 1	Норма	0,9943	0,9714
	Атака	0,9939	0,9986
№ 2	Норма	0,9954	0,9725
	Атака	0,9932	0,9989
№ 3	Норма	0,9969	0,9731
	Атака	0,9933	0,9992

Если в результате анализа сетевых данных, представленных модулем сбора информации, обнаружен факт сетевой атаки, то реализуется отправка администратору e-mail сообщения «модулем оповещения». В таком сообщении указывается следующее: IP-адрес и порт источника соединения; IP-адрес и порт назначения; название сервиса подключения; тип сетевой атаки. Для блокирования IP-адреса подключения, распознанного как сетевая атака, рекомендуется использование утилиты командной строки Iptables, управляющей работой межсетевого экрана Netfilter для ядер Linux.

Апробация разработанной системы. Для апробации разработанного программного комплекса обнаружения вторжений на реальных сетевых данных был развернут виртуальный сервер у хостинг-провайдера Flops. На этом сервере было установлено и настроено следующее: монитор сетевой безопасности Bro; интерпретатор, написанный на языке Python; дополнительные библиотеки, необходимые для функционирования программного комплекса по обнаружению сетевых атак. Для генерации различного рода сетевого трафика на сервере были использованы почтовые и веб-сервисы. В фоновом режиме на сервере были запущены реализованные на языке Python скрипты для работы модулей сбора информации и классификации сетевых данных [15]. С помощью различных утилит и скриптов на данный сервер был сгенерирован трафик для разных сервисов.

Сбор и журналирование сетевого трафика осуществлялись монитором сетевой безопасности Bro. Каждая запись в журнале сетевого трафика характеризует одно сетевое соединение. Кроме стандартных параметров дампа сетевого соединения Bro вычисляет продолжительность соединения, размер переданных и принятых пакетов, определяет флаг, который определяет статус соединения (этот флаг формируется в зависимости от последовательности обмена управляющими битами отправителя и получателя). Для составления набора входных данных, имеющего параметры как у KDD'99, в наборе данных из журналов Bro не хватало таких параметров: наличие флага URG, количество пакетов с неверной хэш-суммой, параметров, получаемых из анализа TCP-соединения. Для получения нужных данных были расширены скрипты Bro по сбору параметров.

По завершении соединения с источником информации Bro выполняет запись вычисленных параметров сетевого соединения в журнал.

На языке Python был реализован класс, позволяющий выполнять чтение постоянно обновляющегося журнала, фиксирующего активность сетевого трафика. При появлении новой записи о подключении вызывается функция, выполняющая дальнейшую обработку данных. Параметром этой функции является список атрибутов сетевого трафика. По порту назначения для протоколов TCP, UDP определяется сервис, с которым выполняется соединение. Для протокола ICMP порт источника является типом ICMP-сообщения, а порт назначения – кодом ICMP-сообщения. Затем выполняется вычисление следующих двух групп параметров трафика:

- атрибуты временного трафика (для их подсчета учитываются подключения за последние 2 секунды);
- атрибуты машинного трафика (для их вычисления используется «окно» в 100 соединений).

Атрибуты временного трафика используются для обнаружения сетевых атак, выполняющих сканирование информационных систем с некоторым интервалом по времени. Если интервал превышает 2 секунды, то используются атрибуты машинного трафика, выполняется сбор статистики сетевого трафика на основе хоста.

Для определения данных параметров было реализовано два класса, в которых накапливается статистика по подключениям за указанное число соединений. Первый класс используется для получения статистики для одинаковых хостов, второй класс – для получения статистики для одинаковых сервисов.

Данные классы являются значениями словаря, ключи которого определяются парой IP-адресов источника и назначения или именем сервиса подключения.

При логировании нового соединения монитором Bro выполняется определение окон, равных 100 подключениям и 2 секундам. Сетевые соединения, не попадающие в данный промежуток, удаляются из массива, а новое соединение добавляется. При этом происходит обновление статистических данных активного окна соединений, а затем выполняется расчет значений атрибутов трафика.

Полный набор параметров трафика передается в модуль классификации для анализа и определения метки – является ли подключение сетевой атакой или нет?

В целях тестирования программного комплекса для обнаружения сетевых атак с помощью утилиты Tcpreplay был симулирован трафик на тестовый сервер для оценки точности классификации описанного в статье программного комплекса для обнаружения сетевых атак. Данный трафик был перехвачен снифферером и сохранён в формате pcap, затем с помощью данной утилиты перенаправлен на другой IP-адрес (рис. 4).

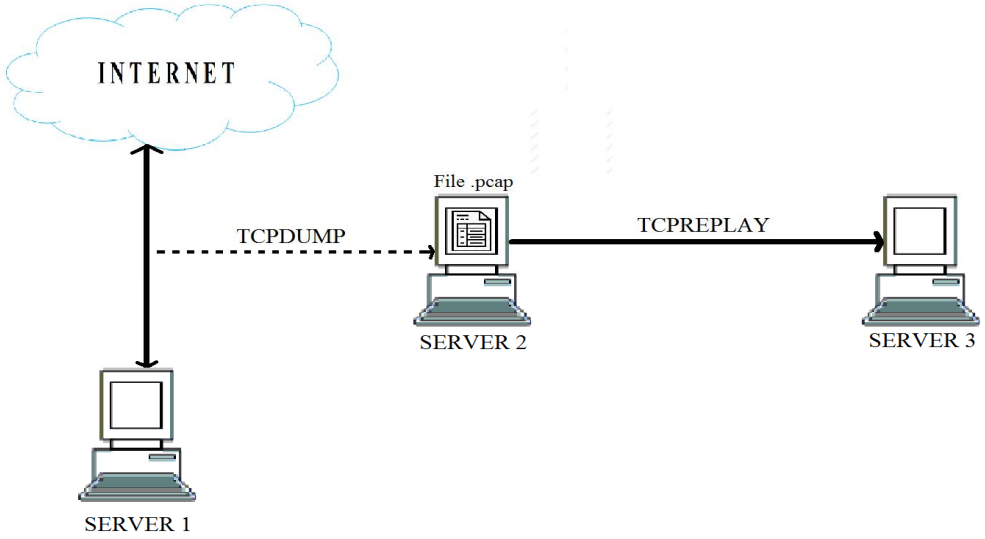


Рисунок 4 – Схема тестирования программного комплекса

В таблице 3 представлена информация о количестве подключений, распознанных как атака, и их процентные доли в общем количестве соединений (подключений).

Таблица 3 – Анализ количества подключений в разрезе «типов атак»

Группа	Класс	Количество подключений	Процентная доля в общем количестве подключений
probe	satan	15892	0,32443041
u2r	rootkit	10	0,00020415
probe	portsweep	10413	0,21257827
dos	back	2203	0,04497358
u2r	buffer_overflow	30	0,00061244
r2l	ftp_write	8	0,00016332
r2l	guess_passwd	53	0,00108198
r2l	imap	12	0,00024498
probe	ipsweep	12481	0,25479587
dos	land	21	0,00042871
u2r	loadmodule	9	0,00018373
r2l	multihop	7	0,00014290
dos	neptune	1072017	21,88490560
probe	nmap	2316	0,04728045
normal	normal	972781	19,85903241
u2r	perl	3	0,00006124
r2l	phf	4	0,00008166
dos	pod	264	0,00538948
dos	smurf	2807886	57,32215070
r2l	spy	2	0,00004083
dos	teardrop	979	0,01998599
r2l	warezclient	1020	0,02082299
r2l	warezmaster	20	0,00040829

Выборка эталонов в обучающем наборе сетевых данных очень неравномерна. Это существенно ухудшает обучение нейронной сети в данной системе обнаружения атак и приводит к различной точности определения классов атак.

Программный комплекс показал следующие результаты распознавания: 0,26 % записей были отнесены в неверную категорию, из них 14 % (0,18 % от общего количества нормальных соединений) являются ошибками первого рода, когда нормальные записи были отмечены (распознаны) как атака, и 23 %, т.е. 0,07 % от общего количества вредоносных соединений, составляют ошибки второго рода – пропущенные атаки.

Заключение. Результаты проведенного исследования на реальных сетевых потоках подтвердили эффективность использования разработанного программного комплекса при определении сетевых атак как интеллектуального компонента систем обеспечения сетевой безопасности.

Список литературы

1. Абрамов Е. С. Использование аппарата нейросетей при обнаружении сетевых атак / Е. С. Абрамов, М. В. Аникеев, О. Б. Макаревич // Известия ТРТУ. – 2004. – № 1 (36). – С. 130.

2. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук : мат-лы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). – Уфа : Лето, 2011. – С. 8–13.

3. Васильев В. И. Интеллектуальная система обнаружения атак в локальных беспроводных сетях / В. И. Васильев, И. В. Шарабыров // Вестник УГАТУ = Vestnik UGATU. – 2015. – № 4 (70). – Режим доступа: https://cyberleninka.ru/article/n/intellektualnaya-sistema-obnaruzheniya-atak-v-lokalnyh-besprovodnyh-setyah, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 13.05.2018).

4. Емельянова Ю. Г. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы / Ю. Г. Емельянова, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко // Программные системы, теория и приложения. – 2011. – № 3 (7). – С. 3–15. – Режим доступа: http://psta.psiras.ru/read/ psta2011_3_3-15.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 20.05.2017).

5. Круглов В. В. Искусственные нейронные сети. Теория и практика / В. В. Круглов, В. В. Борисов. – Москва : Горячая линия – Телеком, 2002. – 382 с.

6. Лукащик Е. П. Применение нейронных сетей для обнаружения сетевых атак / Е. П. Лукащик, Д. А. Кочетов // Традиционная и инновационная наука: история, современное состояние, перспективы : сб. ст. Междунар. науч.-практ. конф. (Уфа, 21.08.2017 г.). – Стерлитамак : АМИ, 2017. – С. 24–27.

7. Тарасов Я. В. Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети / Я. В. Тарасов // Известия ЮФУ. Технические науки. – 2014. – № 8. – Режим доступа: https://cyberleninka.ru/article/n/metod-obnaruzheniya-nizkointensivnyh-ddos-atak-na-osnove-gibridnoy-neyronnoy-seti, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 13.05.2018).

8. Anjali M. B. Padmavathi. DDOS Attack Detection based on Chaos Theory and Artificial Neural Network / Anjali M. B. Padmavathi // International Journal of Computer Science and Information Technologies. – 2014. – Vol. 5 (6). – P. 7276–7279.

9. Dubey S. A Survey Intrusion Detection with KDD99. Cup Dataset / S. Dubey, J. Dubey // International Journal of Computer Science and Information Technology Research. –2014. – July–September. – Vol. 2, iss. 3. – P. 146–157.

10. Huseynov K. Evaluation of Public Datasets for Intrusion Detection/Prevention System Benchmar / K. Huseynov, K. Kim, P. Yoo.

11. KDD Cup 1999 Data. – Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения 05.05.2017).

12. Mohammad Sazzadul Hoque. An Implementation of Intrusion Detection System Using Genetic Algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md. Abu Naser Bikas // International Journal of Network Security & Its Applications. – 2012. – March. – Vol. 4, № 2. – P. 109–120.

13. Olusola A. Analysis of KDD‘99 Intrusion Detection Dataset for Selection of Relevance Features / A. Olusola, A. Oladele, D. Abosede // Proceedings of the World Congress on Engineering and Computer Science. – San Francisco, 2010. – Vol. 1. – P. 162–168.

14. Tavallaee M. A detailed analysis of the KDD CUP 99 data set / M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani // IEEE Symposium on Computational Intelligence for Security and Defense Applications. – Ottawa, ON, 2009. – P. 1–6. – Режим доступа: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5356528&isnumber=5356514, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения 05.05.2018).

15. Tom Schaul. PyBrain / Tom Schaul, Justin Bayer, Daan Wierstra, Sun Yi, Martin Felder, Frank Sehnke, Thomas Rückstieb, Jürgen Schmidhuber // Journal of Machine Learning Research. – 2010. – № 11. – P. 743–746.

References

1. Abramov E. S., Anikeev M. B., Makarevich O. B. Ispolzovanie apparata neurosetey pri obnaruzhenii setevykh atak [Application of neural network mechanism to detect network attacks]. *Izvestiya TRTU* [TRTU News], 2004, no. 1 (36), P. 130.

2. Borshchevikov A. E. Setevye ataki. Vidy. Sposoby borby [Network attacks. Kinds. Countermeasures]. *Sovremenye tendentsii tekhnicheskikh nauk : trudy mezhdunarodnoy nauchnoy konferentsii [*Modern trends of technical sciences : Procedings of the International Scientific Conference]. Ufa, Leto Publ., 2011, pp. 8–13.

3. Vasiliev V. I., Sharabirov I. V. Intellektualnaya sistema obnaruzheniya atak v lokalnykh besprovodnykh setyakh [Intelligent system for detecting attacks in local wireless networks]. *Vestnik UGATU* [UGATU Herald], 2015, no. 4 (70). Available at: https://cyberleninka.ru/article/n/intellektualnaya-sistema-obnaruzheniya-atak-v-lokalnyh-besprovodnyh-setyah (accessed 13.05.2018).

4. Yemelyanova Y. G., Talalayev A. A., Tishchenko I. P., Fralenko V. P Neyrosetevaya tekhnologiya obnaruzheniya setevykh atak na informatsionnye resursy [Neural network technology to detect network attacks on information resources]. *Programmnye sistemy, teoriya i prilozheniya* [Software systems: theory and applications], 2011, no. 3 (7), pp. 3–15. Available at: http://psta.psiras.ru/read/psta2011_3_3-15.pdf (accessed 20.05.2017).

5. Kruglov V. V., Borisov V. V. *Iskusstvennye neyronnye seti. Teoriya i praktika* [Artificial neural networks. Theory and practice]. Moscow, Goryachaya liniya – Telecom publ., 2002.

6. Lukashik E. P., Kochetov D. A. Primenenie neyronnykh setey dlya obnaruzheniya setevykh atak [Application of Neural Networks to Detect Network Attacks]. *Traditsionnaya i innovatsionnaya nauka: istoriya, sovremennoe sostoyanie, perspektivy : Sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Traditional and innovative science: history, current state, prospects : Proceedings of the International Scientific and Practical Conference "] (Ufa, 21.08.2017). – Sterlitamak, AMI Publ., 2017, pp. 24–27.

7. Tarasov Y. V. Metod obnaruzheniya nizkointensivnykh DDoS-atak na osnove gibridnoy neyronnoy seti [Method for detection of low-intensive DDOS-attacks based on a hybrid neural network]. *Izvestiya YuFU. Tekhnicheskie nauki* [News of SFU. Technical Science], 2014, no. 8. Available at: https://cyberleninka.ru/article/n/metod-obnaruzheniya-nizkointensivnyh-ddos-atak-na-osnove-gibridnoy-neyronnoy-seti (accessed 13.05.2018).

8. Anjali M. B. Padmavathi. DDOS Attack Detection based on Chaos Theory and Artificial Neural Network. *International Journal of Computer Science and Information Technologies*, 2014, vol. 5 (6), pp. 7276–7279.

9. Dubey S., Dubey J. A Survey Intrusion Detection with KDD99. Cup Dataset. *International Journal of Computer Science and Information Technology Research*, 2014, July–September, vol. 2, iss. 3, pp. 146–157.

10. Huseynov K., Kim K., Yoo P. *Evaluation of Public Datasets for Intrusion Detection/Prevention System Benchmar.*

11. *Kdd cup 1999 data.* Available at: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed 05.05.2017).

12. Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md. Abu Naser Bikas. An Implementation of Intrusion Detection System Using Genetic Algorithm. *International Journal of Network Security & Its Applicationsm*, 2012, March, vol. 4, no. 2, pp. 109–120.

13. Olusola A., Oladele A., Abosede D. Analysis of KDD‘99 Intrusion Detection Dataset for Selection of Relevance Features. *Proceedings of the World Congress on engineering and Computer Science*, San Francisco, 2010, vol. 1, pp. 162–168.

14. Tavallaee M., Bagheri E., Lu W. and Ghorbani A. A. A detailed analysis of the KDD CUP 99 data set. *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, 2009, pp. 1–6. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5356528&isnumber=5356514 (accessed 05.05.2018).

15. Tom Schaul, Justin Bayer, Daan Wierstra, Sun Yi, Martin Felder, Frank Sehnke, Thomas Rückstieb, Jürgen Schmidhuber. PyBrain. *Journal of Machine Learning Research*, 2010, no. 11, pp. 743–746.