Интеллектуальный анализ сетевого трафика для идентификации компьютерных вторжений*

А. О. Суворов[I,II], В. А. Суворова[III]

[I] Пермский национальный исследовательский политехнический университет, г. Пермь, Россия
[II] Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия
[III] Акционерное общество «Инфосистемы Джет», г. Москва, Россия

Аннотация. В статье рассматривается процесс построения системы обнаружения вторжений с использованием интеллектуального анализа сетевого трафика. Сформулированы требования к разрабатываемой системе обнаружения вторжений, а также предложена ее архитектура. В качестве механизма принятия решений о наличии атак предложено использовать методы индуктивного машинного обучения, а именно – искусственные нейронные сети. Предлагается построение нейросетевой модели на основе многослойного персептрона, для которой определены наиболее значимые входные параметры. Рассмотрена методика построения модуля интеллектуального анализа сетевого трафика, логика его работы. Приведены результаты тестирования разработанного клиент-серверного приложения для анализа сетевого трафика по сформированным параметрам.

Ключевые слова: система обнаружения вторжений, искусственные нейронные сети, сетевые атаки, интеллектуальный анализ трафика.

DOI 10.14357/20718594190106

Введение

Стремительный рост числа компьютерных сетей, пользователей и услуг, подключенных к Интернету объемов обрабатываемых и передаваемых данных, приводит к увеличению вероятности хищения или разрушения информации, к возникновению угроз информационной безопасности. Поэтому защита данных в компьютерных сетях становится одной из самых острых проблем в области компьютерной безопасности.

На сегодняшний день, по данным Лаборатории Касперского [1], по всему миру ежедневно сетевым атакам подвергаются около 7 млн пользователей, а в Российской Федерации фиксируется более 500 тыс. сетевых вторжений в сутки.

Построение систем обнаружения вторжений (Intrusion Detection System, IDS) [2] является одним из методов обеспечения защиты информационных ресурсов в вычислительных сетях. Системы анализа защищенности и системы обнаружения компьютерных атак являются важными элементами системы безопасности сетей любого современного предприятия [3].

Обнаружение вторжений можно определить как процесс идентификации событий, происходящих в вычислительной сети или системе, их анализ на наличие признаков нарушения политики безопасности и попытки поставить под угрозу конфиденциальность, целостность, доступность, или обойти механизмы безопасности хоста или сети [4].

Эффективность работы IDS во многом зависит от методов анализа информации. В настоящее время подавляющее большинство существующих систем использует сигнатурные методы анализа сетевого трафика. В таких системах содержится описания атак («сигнатуры»), которые сопоставляются с данными в проверяемом потоке, с це-

*Работа выполнена при поддержке «Фонда содействия развитию малых форм предприятий в научно-технической сфере» по программе УМНИК.

✉ *Суворов Александр Олегович. E-mail: aosuvorov@pstu.ru*

лью обнаружения известной атаки [5, 6]. К недостаткам систем подобного рода относятся: невозможность выявлять новые, ранее неизвестные атаки, необходимость регулярного обновления баз сигнатур, ручной анализ новых аномалий.

Учитывая факт, что ни один из существующих методов не обеспечивает 100% защиту от сетевых вторжений, разработка новых методик обнаружения, основанных на применении методов машинного обучения, а именно, искусственных нейронных сетей (ИНС), позволяющих повысить уровень защищенности компьютерных систем от несанкционированного воздействия, является востребованной и актуальной.

В статье описывается процесс разработки программного модуля интеллектуального анализа сетевого трафика для обнаружения и классификации сетевых вторжений с использованием механизмов искусственных нейронных сетей.

Авторами были поставлены следующие задачи:

- описание принципиальной архитектуры будущей системы, формирование требований;
- построение различных нейросетевых моделей с использованием общедоступных наборов данных, их оптимизация;
- выбор оптимальной модели искусственной нейронной сети и ее сравнение с аналогами;
- разработка модуля интеллектуального анализа данных на основе полученной модели.

В данной работе предлагается построение нейросетевой модели на основе многослойного персептрона (Multilayer Perceptron – MLP), так как она показала свою эффективность для решения задач классификации [7].

В дальнейшем разработанный модуль будет применен в качестве одной из компонент интеллектуальной системы обнаружения вторжений.

Изложение материала в статье организовано следующим образом: в Разделе 1 рассматривается архитектура разрабатываемой системы в целом, определяется место модуля интеллектуального анализа. Раздел 2 содержит описание нейросетевых моделей, которые были построены при проведении экспериментов, полученные результаты сравниваются с аналогичными моделями. Процесс разработки и результаты тестирования модуля изложены в Разделе 3. В Заключении описаны полученные результаты и дальнейшие планы по разработке интеллектуальной системы защиты от компьютерных вторжений.

1. Архитектура разрабатываемой системы

Предполагается, что программный комплекс для автоматизированной идентификации и классификации сетевых вторжений будет состоять из совокупности нескольких взаимосвязанных программных модулей и хранилища данных. На Рис. 1 изображена предполагаемая архитектура будущей системы обнаружения вторжений.

Система состоит из следующих компонент:

1. Модуль сбора сетевого трафика необходим для сбора всей информации с сетевых устройств, находящихся на периметре сети, преобразования исходного сетевого трафика в требуемый вид (определение и вычисление не-

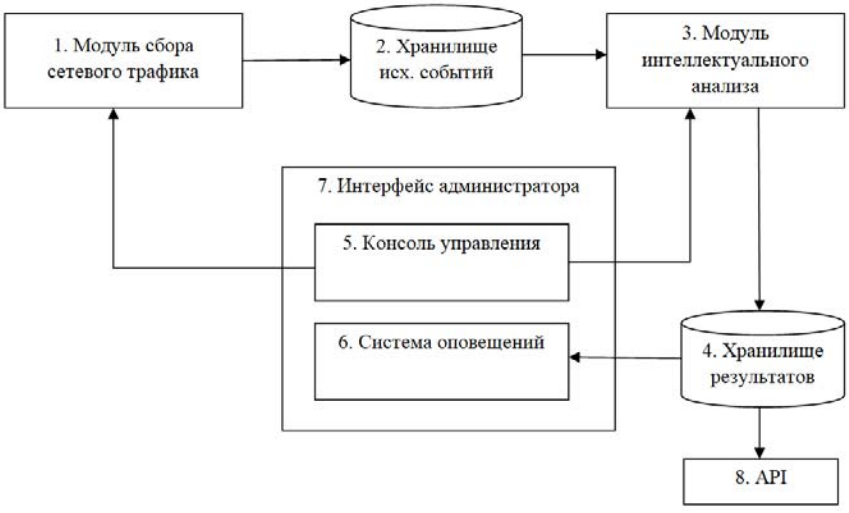


Рис. 1. Архитектура разрабатываемой системы обнаружения вторжений

обходимых параметров) и записи данных в хранилище исходных событий.

2. Хранилище исходных событий предназначено для хранения информации, которую необходимо проанализировать на наличие сетевых атак. Каждая запись будет хранить информацию о потоке, по параметрам, которые требуются для обработки модулем интеллектуального анализа данных.

3. Модуль интеллектуального анализа сетевого трафика выполняет анализ каждой записи о потоке, хранящейся в базе данных исходных событий, с помощью алгоритмов, использующих методы машинного обучения. В результате для каждой записи определяется вид соединения: нормальное или атака, а также вид атаки в случае ее обнаружения. Результаты анализа будут записаны в базу данных результатов.

4. Хранилище результатов представляет собой базу данных, где будут храниться обнаруженные аномалии. Данная база будет использоваться системой оповещений, а также модулем совместимости для извлечения результатов анализа. Хранение результатов позволит в дальнейшем производить временной анализ состояния безопасности системы.

5. Консоль управления системой предназначена для общей настройки всех компонент программного комплекса.

6. Система оповещения о выявленных инцидентах будет мгновенно уведомлять администратора безопасности об обнаруженных инцидентах, отображать в удобном для пользователя виде обнаруженные аномалии, указывать на тип обнаруженных аномалий, а также предоставлять возможности для построения отчетов.

7. Графический интерфейс администратора системы будет объединять консоль управления и систему оповещений. Он предназначен для взаимодействия пользователя с системой.

8. Модуль интеграции представляет собой API для возможности интеграции с системами реагирования, интерфейс для взаимодействия с системой посредством http-запросов.

В рамках статьи будет рассмотрена методика построения одного из модулей системы – модуля интеллектуального анализа сетевого трафика. Ключевую роль в создании интеллектуальной системы обнаружения вторжений играет разработка модуля интеллектуального анализа сетевого трафика, так как именно он будет содержать методы обнаружения, интеллектуальные алгоритмы. Именно от работы данного модуля зависит эффективность обнаружения вторжений.

2. Нейросетевые модели для анализа сетевого трафика

Разрабатываемый модуль интеллектуального анализа сетевого трафика в качестве механизма принятия решений о наличии атак будет использовать методы индуктивного машинного обучения, а именно – искусственные нейронные сети (ИНС).

При создании нейронных сетей важно сформировать множество примеров, которые в дальнейшем будут использоваться для обучения, тестирования и проверки нейронной сети. Задача обнаружения сетевых атак связана с выделением большого числа признаков, по которым можно будет проводить классификацию атак. В ранних работах для проведения исследований применялись данные из набора Knowledge Discovery in Database (KDD) Cup 1999 Data [8]. По результатам проведенных исследований [9, 10] была доказана эффективность применяемого подхода по сравнению с результатами аналогичных работ [11-14].

Однако база данных KDD CUP 1999 Data была создана еще в 1999 г. На данный момент сведения об атаках, содержащиеся в ней, во многом не актуальны [15, 16]. В 2015 г. была создана новая база данных атак UNSW-NB15, в которой учитывались недостатки созданных ранее баз данных атак. Разработанная исследователями база данных UNSW-NB15 содержит более 2,5 млн записей.

При построении модуля интеллектуального анализа для обучения интеллектуальных моделей было принято решение использовать более новую выборку, содержащую сведения о сетевых атаках UNSW-NB-15 [17, 18].

В базе UNSW-NB15 каждая запись содержит 47 признаков сетевого трафика пяти типов: номинальные, целочисленные, числовые, временные, бинарные. Полный перечень признаков соединений, используемых в UNSW-NB1, представлен в [17]. Для каждой записи содержится информация о том, к какому из десяти классов относится соединение: нормальные соединение (Normal) или один из девяти различных видов атак. В Табл. 1 перечислены виды

Табл. 1. Виды атак, представленные в базе UNSW-NB15

№	Вид соединения	Количество	Описание
1	Normal	2 218 761	Естественные данные транзакций
2	Fuzzers	24 246	Попытка вызвать приостановление программы или сети путем ее подачи случайно сгенерированные данные
3	Analysis	2 677	Содержит различные атаки сканирования порта, спама и проникновения html-файлов
4	Backdoors	2 329	Техника, в которой механизм безопасности системы обходится незаметно для доступа к компьютеру или его данным
5	DoS	16 353	Вредоносная попытка сделать сервер или сетевой ресурс недоступным для пользователей, обычно это временное прерывание или приостановка услуг хоста, подключенного к Интернету
6	Exploits	44 525	Злоумышленник знает о проблемах безопасности в системе и использует данные уязвимости в своих целях
7	Generic	215 481	Техника работает против всех блочных шифров (с заданным блоком и размером ключа), независимо от структуры блочного шифра
8	Reconnaissance	13 987	Содержит все типы атак, которые собирают информацию о сети (с целью разведки)
9	Shellcode	1 511	Небольшой фрагмент кода, используемый как полезная нагрузка при эксплуатации уязвимостей программного обеспечения
10	Worms	174	Атакующий реплицирует себя, чтобы распространиться на другие компьютеры. Часто он использует компьютерную сеть для распространения, полагаясь на сбои в безопасности на целевом компьютере для доступа к нему

соединений, хранящиеся в базе UNSW-NB1, количество представленных записей о них, а также краткое описание.

Как видно из Табл. 1, выборка эталонов в базе UNSW-NB15 неравномерна по видам соединений: для типа атаки Worms представлено достаточно малое количество примеров для обучения.

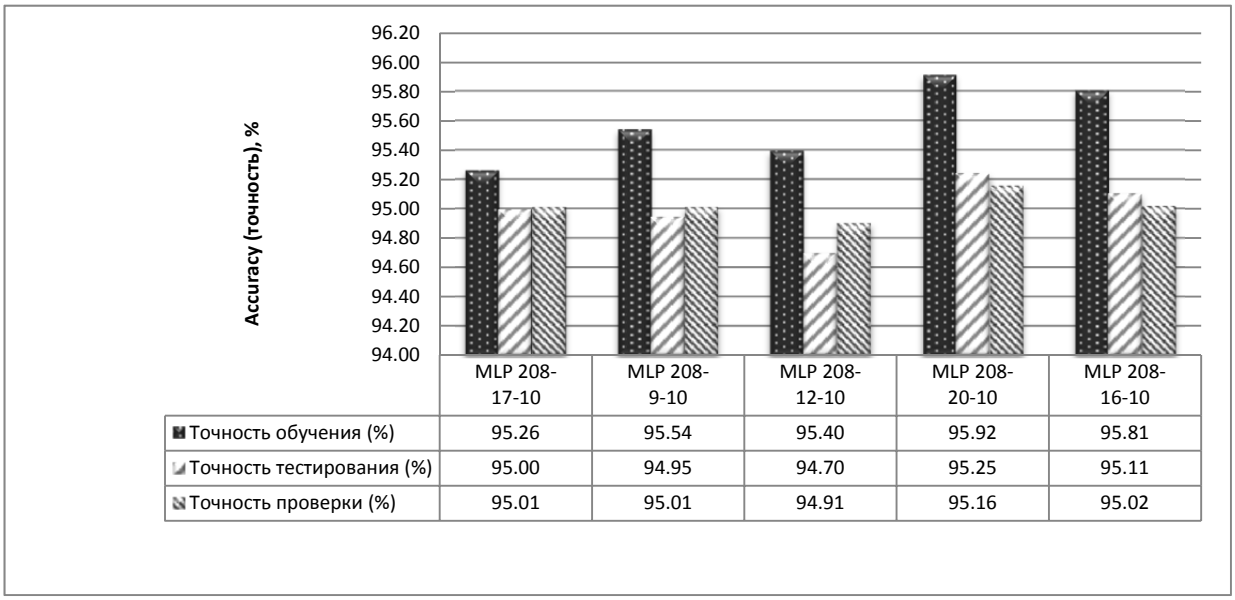
2.1. Проектирование нейронных сетей с полным набором параметров

Проектирование нейронных сетей, использующих набор данных UNSW-NB1, осуществлялось в пакете Statistica с использованием инструментов Automated Nerual Networks.

Количество нейронов на входном и выходном слоях определяется набором данных UNSW-NB1, на скрытом слое – случайным образом, путем перебора различных вариантов, исходя из минимальной ошибки обучения, тестирования и проверки. Диапазон количества нейронов на скрытом слое определяется по формуле, являющейся следствием теорем Арнольда-Колмогорова-Хехт-Нильсена [7].

На первом этапе исследований, было выполнено построение нейронных сетей с полным набором параметров [17]: на вход нейронной сети подаются 45 признаков сетевого трафика (за исключением *ip*-адреса отправителя и получателя).

Были проведены исследования на входных множествах различной мощности (от 100 000 до 700 000 записей). Входное множество автоматически разбивается на обучающее, тестовое и проверочное. Для обучения используется 70% от входного множества, а для тестирования и проверки – по 15%. На Рис. 2 представлены 5 наилучших вариантов построения нейронных сетей, смоделированных на входном множестве мощностью 100 000 записей. В качестве метрики оценки качества модели используется Accuracy (аккуратность, точность) – доля от обучающей, тестовой, проверочной выборки в отно-отношении которой классификатор принял верное решение.



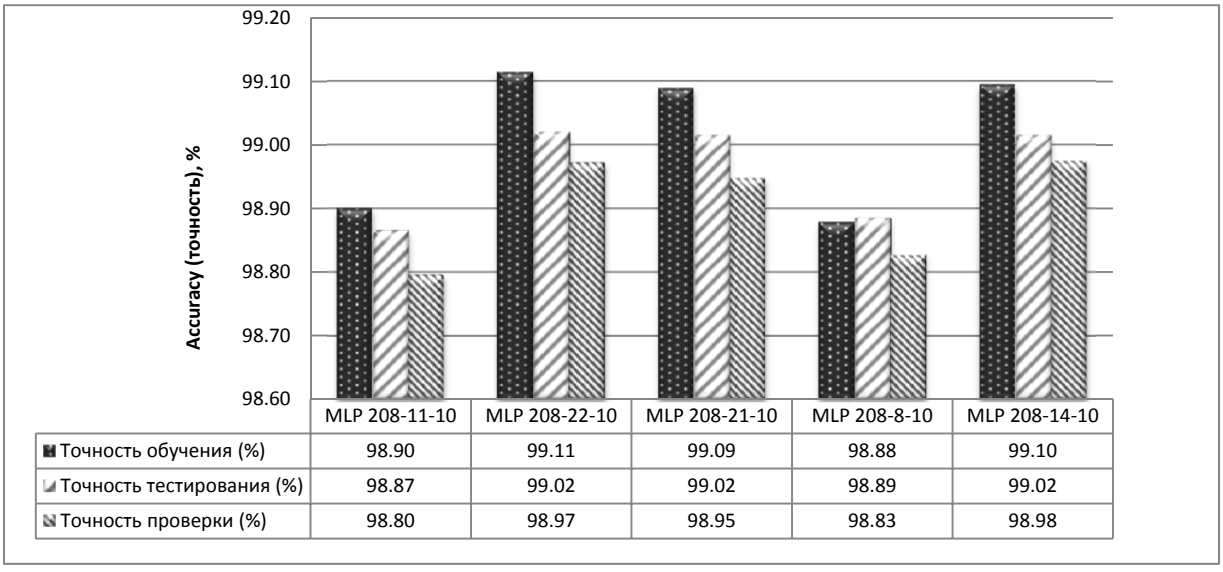
	MLP 208-17-10	MLP 208-9-10	MLP 208-12-10	MLP 208-20-10	MLP 208-16-10
Точность обучения (%)	95.26	95.54	95.40	95.92	95.81
Точность тестирования (%)	95.00	94.95	94.70	95.25	95.11
Точность проверки (%)	95.01	95.01	94.91	95.16	95.02

Рис. 2. Характеристики нейронных сетей с полным набором параметров с использованием обучающего множества UNSW-NB1 мощностью 100 000 записей

При увеличении входного множества данных в 7 раз точность обучения, тестирования и проверки в среднем увеличилась и теперь для каждой из пяти наилучших нейронных сетей, представленных на Рис. 3, превышает 98,5%.

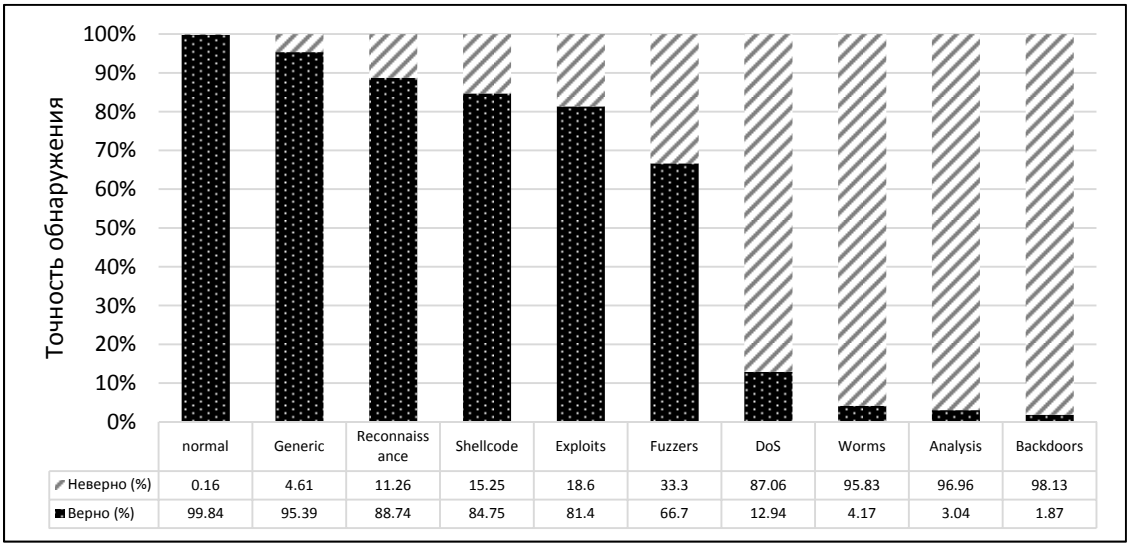
Наилучшие результаты (наименьшая ошибка проверки) показала нейронная сеть MLP 208-14-10 (208, 14 и 10 – количество нейронов на входном, скрытом и выходном слое соответственно), для которой на Рис. 4 представлены результаты классификации по видам атак.

Полученные результаты показывают что, несмотря на высокую точность проверки для MLP 208-14-10, определение отдельных видов атак происходит затруднительно. Лишь 6 из 10 видов соединений удается определить с точностью более 66%. При этом наблюдается следующая ситуация: распознавание нормального трафика происходит верно в подавляющем большинстве случаев (99,08%), однако правильно классифицировать атаку по виду удается в среднем лишь с точностью 75,96%.



	MLP 208-11-10	MLP 208-22-10	MLP 208-21-10	MLP 208-8-10	MLP 208-14-10
Точность обучения (%)	98.90	99.11	99.09	98.88	99.10
Точность тестирования (%)	98.87	99.02	99.02	98.89	99.02
Точность проверки (%)	98.80	98.97	98.95	98.83	98.98

Рис. 3. Характеристики нейронных сетей с полным набором параметров с использованием обучающего множества UNSW-NB1 мощностью 700 000 записей



	normal	Generic	Reconnaissance	Shellcode	Exploits	Fuzzers	DoS	Worms	Analysis	Backdoors
Неверно (%)	0.16	4.61	11.26	15.25	18.6	33.3	87.06	95.83	96.96	98.13
Верно (%)	99.84	95.39	88.74	84.75	81.4	66.7	12.94	4.17	3.04	1.87

Рис. 4. Результаты проверки сети MLP 208-14-10, сгруппированные по видам атак

2.2. Определение значимости параметров

Далее необходимо предпринять попытку сокращения числа входных параметров нейронной сети, что требует дополнительных исследований входного множества записей из набора UNSW-NB15.

Определение значимости входных признаков набора UNSW-NB15 было произведено аналогично процессу определения значимости параметров для базы KDD Cup [9].

Сначала были получены значения информативности параметров для каждой из пяти нейронных сетей, построенных на расширенном (700 000 записей) и сокращенном (100 000 записей) входном множестве. И затем вычислено среднее значение значимости для каждого признака по пяти нейронным сетям.

Для определения наименее значимых параметров были вычислены средние коэффициенты значимости для всех признаков по двум группам нейронных сетей, построенных на сокращенном и расширенном входном множестве.

Затем с помощью вычисления коэффициентов линейной корреляции для всех числовых признаков были выявлены группы линейно-зависимых параметров. Из полученной матрицы линейной корреляции было выявлено, что имеется 5 групп линейно-зависимых параметров (прямая линейная зависимость). В дальнейшем при построении нейросетей с сокращенным числом параметров из каждой группы линейно-зависимых признаков будет оставлен только один, значимость которого максимальна.

2.3. Построение нейронных сетей с сокращенным набором параметров

Исследования, описанные выше, позволяют составить список параметров, которые могут быть исключены из входного множества признаков для построения нейронных сетей.

В отличие от нейронных сетей с полным набором параметров, сети с сокращенным числом параметров не будут использовать признаки, указанные в Табл. 2.

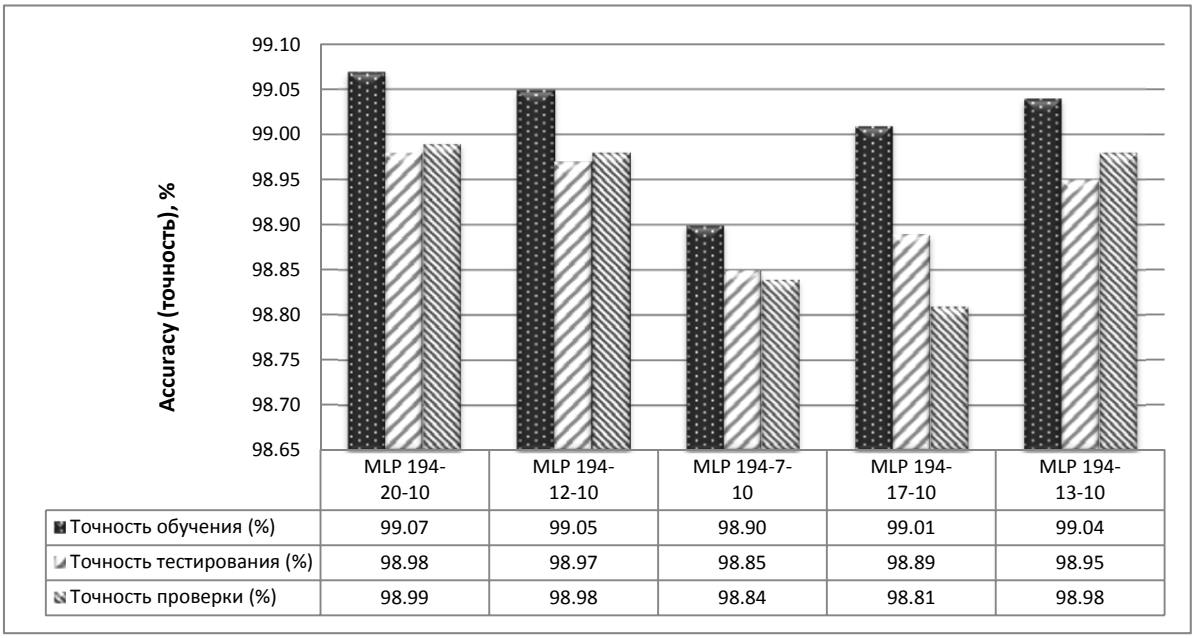
Далее было выполнено построение нейронных сетей, использующих сокращенное количество входных нейронов. Удалось сократить входное множество признаков до 32, что значительно ускоряет процесс обучения и тестирования нейронной сети, а также упрощает ее дальнейшее использование. Результаты построения представлены на Рис. 5.

Полученные результаты указывают на то, что наименее значимые параметры были определены верно, так как точность обучения, тестирования и проверки для каждой из 5 ИНС не меньше 98,8%.

Нейросетевая модель MLP 194-20-10 (194, 20 и 10 – количество нейронов на входном, скрытом и выходном слое соответственно) показала наименьшую ошибку проверки. Данная модель является оптимизированной по количеству параметров и в дальнейшем будет использована при создании программного модуля интеллектуального анализа сетевого трафика.

Табл. 2. Наименее значимые параметры множества UNSW-NB15

Признак	Описание признака
ackdat	Время между пакетами SYN_ACK и ACK в TCP сессии
dbytes	Число переданных байт от получателя к источнику
tcprtt	Время установления TCP сессии (от первого syn до первого пакета с данными)
sintpkt	Время прибытия промежуточного пакета источника (мс)
res_bdy_len	Фактический размер несжатого размера данных, передаваемых с http-службы сервера
ct_ftp_cmd	Количество потоков, которые используют команды в ftp-сессии
dur	Общая продолжительность соединения
sloss	Исходящие пакеты повторно переданы или удалены
dloss	Пакеты получателя повторно переданы или удалены
djit	Джиттер назначения (мс)
sbytes	Число переданных байт от источника до получателя
spkts	Количество пакетов от источника к получателю
dwin	Размер объявленного TCP-окна получателя
ltime	Время окончания записи



	MLP 194-20-10	MLP 194-12-10	MLP 194-7-10	MLP 194-17-10	MLP 194-13-10
Точность обучения (%)	99.07	99.05	98.90	99.01	99.04
Точность тестирования (%)	98.98	98.97	98.85	98.89	98.95
Точность проверки (%)	98.99	98.98	98.84	98.81	98.98

Рис. 5. Характеристики нейронных сетей с сокращенным набором параметров с использованием обучающего множества UNSW-NB1

2.4. Сравнение с аналогичными нейросетевыми моделями

Набор данных о сетевых атаках UNSW-NB15 был создан в 2015 г., поэтому исследования данного набора активно ведутся в мире и только начинают проводиться в России. В связи с этим открытых публикаций по созданию нейронных сетей с использованием UNSW-NB15 немного, так как большое количество исследований являются не завершенными (их результаты еще не опубликованы).

В статье [19] авторы построили многослойный персептрон в среде Matlab Neural Network Toolbox с двумя скрытыми слоями. Полученная нейросеть использует 42 входных параметра и способна определить лишь наличие атаки (без определения вида) с точностью 91,16%.

Разработчики компании Oracle в своей презентации [20] на BIWA Summit 2017 описали многослойный персептрон с одним скрытым слоем, построенный на UNSW-NB15 и показавший точность 98,11%.

Авторы работы [21] также работают над созданием интеллектуальной системы обнаружения вторжений с использованием набора UNSW-NB15, однако используют не ИНС, а иные методы машинного обучения: наивный байесовский классификатор и логистическую регрессию. С использованием данных методов исследователям удалось достичь высокой точности обнаружения: 99,82 и 99,93% соответственно.

Полученная в ходе выполнения работы модель MLP 194-20-10 показывает точность определения атаки равную 98,99%, что выше, чем у описанных в работах [19, 20] многослойных персептронов. При этом разработанная модель использует всего 32 входных параметра, что меньше, чем у аналогов. Следовательно, полученная нейросетевая модель обладает рядом преимуществ по сравнению с аналогичными моделями: происходит не только определение наличия атаки, но и их классификация с использованием сокращенного числа входных параметров.

Однако результаты, полученные в работе [21], говорят о том, что использование классификаторов машинного обучения позволит приблизить точность обнаружения к 100%. Поэтому, в дальнейшем планируется продолжить исследования и создать алгоритм, дополняющий разработанную нейросеть иными методами машинного обучения, в частности, машинными классификаторами.

3. Реализация и тестирование модуля интеллектуального анализа

На предыдущем этапе исследований с помощью инструмента Statistica Automated Neural Network (SANN) была получена оптимизированная нейросетевая модель MLP 194-20-10, способная отличать 10 видов атак с точностью в среднем 98,99%. Используемый инструмент нейросетевого моделирования после обучения нейронной сети позволяет выгрузить ее параметры в файл формата *.xml, что дает возможность использовать полученную нейросеть в дальнейшем при разработке приложений. Данная модель MLP 194-20-10 стала основой для разработки модуля интеллектуального анализа.

В Разделе 1 статьи описаны в общем виде взаимосвязи модуля интеллектуального анализа с другими компонентами будущей системы. Для того чтобы обеспечить взаимодействие модуля интеллектуального анализа сетевого трафика с хранилищем данных была создана специальная программа-заглушка, выполняющая функции прослойки между хранилищем данных и разрабатываемым модулем анализа (Рис. 6).

Программа-заглушка играет роль клиента и отправляет данные модулю анализа, который в свою очередь играет роль сервера, обрабатывая поступающие запросы и отвечая на них. Взаимодействие осуществляется посредством сокетов. Сообщения пересылаются в формате http-запросов. На данном этапе исследования не стояла задача реализации хранилища данных, именно поэтому создание программы-заглушки необходимо для того, чтобы написать модуль анализа, который не будет зависеть от способа организации хранилища событий.

Логику работы модуля интеллектуального анализа сетевого трафика удобно отобразить в виде блок-схемы, изображенной на Рис. 7.

В соответствии с предложенным алгоритмом работы было разработано клиент-серверное приложение, которое предназначено для анализа сетевого трафика по сформированным параметрам. В основе серверной части – искусственная нейронная сеть, которая отвечает за выработку результата анализа.

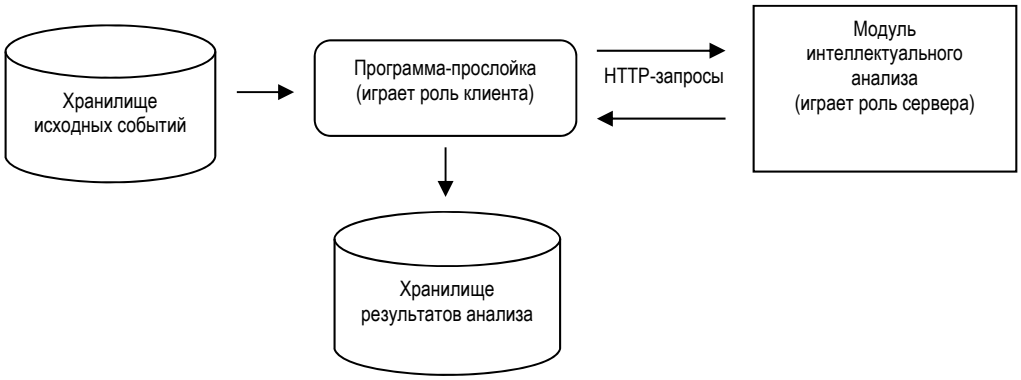


Рис. 6. Схема взаимодействия модуля анализа с хранилищами данных системы

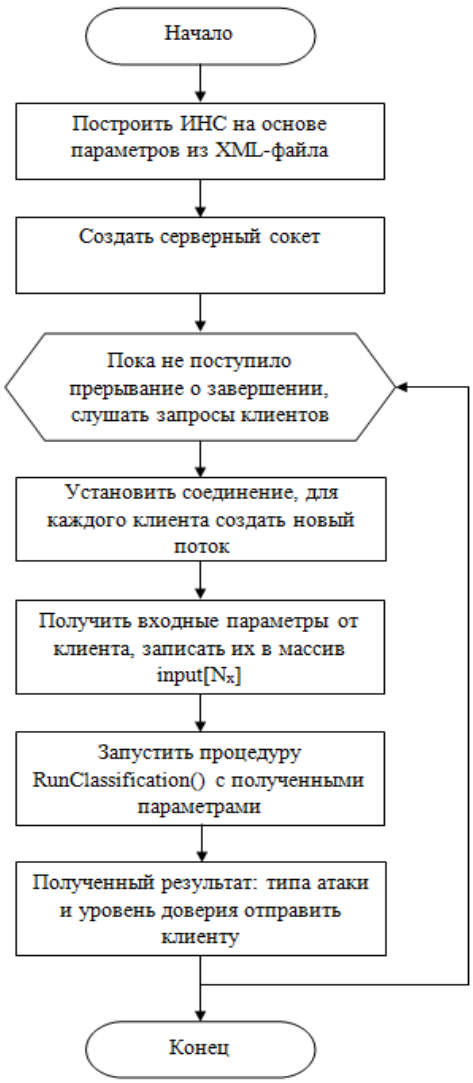


Рис. 7. Логика работы модуля интеллектуального анализа

Созданное приложение было протестировано на множестве записей из набора данных UNSW-NB15, которое не входило в обучающее и тестовое множество при создании нейросетевой модели. Таким образом, используя данные из UNSW-NB15, результат анализа при тестировании известен для каждой записи, однако нейронная сеть, лежащая в основе модуля анализа, не обучалась на данных записях, т.е. для нее они являются «неизвестными».

Приложение было протестировано на множестве мощностью 10 000 записей. Результаты тестирования представлены в Табл. 3. Первая строка – название вида атаки, которая была подана на вход. Первый столбец – вид атаки, к которому приложение отнесло данную запись по результатам вычислений. Таким образом, на пересечении *i*-ой строки и *j*-го столбца – количество записей, которые относятся к виду *j*, но по результатам вычислений были отнесены к виду *i*. На главной диагонали квадратной матрицы – количество записей, для которых вид атаки определен верно. Исходя из полученных значений были вычислены показатели полноты (Recall) и точности (Precision) по видам атак.

Как видно из Табл. 3, нейронная сеть и созданный на ее основе модуль интеллектуального анализа способен с высокой точностью определять легальные соединения, не содержащие атаку (тип normal). Однако с классификацией некоторых видов атак возникают проблемы: удается с точностью не менее 69 % определить 6 видов атак из 9, и с полнотой не менее 70 % – 5 из 9 видов атак. Наблюдаются ошибки в классификации следующих видов атак: Analysis, Backdoors, DoS, Worms. Данные виды атак в большинстве случаев классифицируются неверно по причине того, что нейронная сеть относит их к классу Exploits. Данную особенность можно объяснить тем, что эти виды атак, так или иначе, используют для своей реализации какие-либо известные уязвимости, т. е. Exploit'ы системы.

Следовательно, по результатам тестирования можно сделать следующие выводы: созданный модуль интеллектуального анализа сетевого трафика показывает высокое качество классификации при отсутствии атаки. Ошибка первого рода (выводится результат об атаке, когда атаки нет) равна 0,16%, второго рода (выводится результат об отсутствии атаки, но атака имеется) – 4,48%. Однако при классификации сетевых вторжений не все виды атак удается классифицировать верно. Созданное на основе MLP 194-20-10 приложение способно классифицировать с высокой полнотой следующие виды сетевых соединений: Fuzzers, Exploits, Generic, Reconnaissance, Shellcode, normal.

Заключение

Авторами была разработана архитектура программного комплекса системы обнаружения вторжений, в рамках которой был реализован прототип модуля интеллектуального анализа сетевого трафика.

Табл. 3. Результаты тестирования на множестве мощностью 10 000 записей

Показатели	**Вид атаки**										
	Fuzzers	Analysis	Backdoors	DoS	Exploits	Generic	Reconnaissance	Shellcode	Worms	Normal	
Общее кол-во записей	504	437	263	531	542	752	165	209	14	6583	**Precision (точность),%**
Fuzzers	354	208	114	126	53	4	2	2	0	7	**40,69**
Analysis	0	18	0	0	2	0	0	0	0	2	**81,82**
Backdoors	1	7	7	1	1	0	0	2	0	0	**36,84**
DoS	3	4	6	68	8	3	1	0	1	4	**69,39**
Exploits	51	158	129	323	440	23	12	18	7	3	**37,80**
Generic	0	0	1	11	11	717	0	6	3	0	**95,73**
Reconnaissance	2	0	1	1	13	2	146	0	0	1	**87,95**
Shellcode	1	0	5	0	4	1	0	179	0	0	**94,21**
Worms	0	0	0	0	0	0	0	0	1	0	**100,00**
Normal	92	42	0	1	10	2	4	2	2	6566	**97,69**
Recall (полнота), %	**70,24**	**4,12**	**2,66**	**12,81**	**81,18**	**95,35**	**88,48**	**85,65**	**7,14**	**99,74**	

Обученный на сокращенном наборе данных из базы UNSW NB-15 двухслойный персептрон MLP 194-20-10 использует 32 входных параметра и способен классифицировать следующие виды сетевых соединений: Fuzzers, Exploits, Generic, Reconnaissance, Shellcode, normal. При этом ошибка первого рода (выводится результат об атаке, когда атаки нет) составила 0,16%; ошибка второго рода (выводится результат об отсутствии атаки, но атака имеется) – 4,48%.

В дальнейших исследованиях для увеличения точности классификации сетевых соединений планируется дополнить модуль интеллектуального анализа сетевого трафика другими методами машинного обучения, в частности, машинным классификатором. Также будут решаться задачи по обновлению созданной начальной версии модуля интеллектуального анализа с целью добавления возможностей переобучения нейронной сети в процессе работы модуля.

Кроме того, планируется разработка остальных модулей системы обнаружения вторжений согласно предложенной архитектуре и создание единого программного комплекса для интеллектуального анализа сетевого трафика.

Литература

1. Лаборатория Касперского. Статистика сетевых атак. [Электронный ресурс] URL: https://securelist.ru/statistics/ (дата обращения: 30.07.2018).
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2016. 996 с.
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей; учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. 416 с.
4. Тимофеев А.В., Броницкий А.А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевых атак // International Journal «Information Technologies & Knowledge» Vol.6, Number 3, 2012. С.257-265.
5. Ilgun K., Kemmerer R.A., Porras P.A. «State Transition Analysis: A Rule-Based Intrusion Detection System», IEEE Trans. Software Eng. vol. 21, no. 3, Mar. 1995. pp. 181-199.
6. Lindqvist U., Porras P.A. «Detecting Computer and Network Misuse with the Production-Based Expert System Toolset», IEEE Symp. Security and Privacy, IEEE CS Press, Los Alamitos, Calif., 1999. pp. 146-161.
7. Ясницкий Л.Н. Интеллектуальные системы. М.: Лаборатория знаний, 2016. 221 с.
8. KDD Cup 1999 Data [Электронный ресурс] http://kdd.ics.uci.edu/databases/kddcup99 (дата обращения: 3.06.2018)
9. Суворова В.А. Суворов А.О. Разработка модели обнаружения сетевых атак на основе искусственной нейронной сети. Искусственный интеллект в решении актуальных социальных и экономических проблем

XXI века: сб. ст. по материалам Второй всеросс. науч.-практ. конф. Перм. гос. нац. исслед. ун-т. Пермь, 2017. С. 129-135.
10. Суворова В.А. Разработка приложения для обнаружения и классификации атак на основе нейросетевой модели. Ломоносов – 2017: XXIV Международная научная конференция студентов, аспирантов, молодых ученых: сб. тезисов. М.: Издательский отдел факультета ВМиК МГУ, 2017. С. 117-119.
11. Мустафаев А.Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика // Вопросы безопасности. 2016. № 2. С.1-7. [Электронный ресурс] URL: http://e-notabene.ru/nb/article_ 18834.html (дата обращения: 3.01.2017).
12. Жигулин П.В., Мальцев А.В., Мельников М.А., Подворчан Д.Э. Анализ сетевого трафика на основе нейронных сетей // Электронные средства и системы управления. 2013. №2. С.44-48.
13. Емельянова Ю.Г., Талалаев А.А., Тищенко И.П., Фраленко В.П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: Теория и приложения. 2011. № 3(7). С.3–15.
14. L´ıdio Mauro, Roberto C´elio Lim˜ ao de Oliveira, Mauro Roisenberg. Network Intrusion Detection System Using Data Mining // Communications in Computer and Information Science. 2012. Chapter: Engineering Applications of Neural Networks, Publisher: Springer Berlin Heidelberg, pp 104-113.
15. Зубков Е.В. Алгоритмы и методики интеллектуального анализа событий информационной безопасности в сетях и системах телекоммуникаций: диссертация кандидата технических наук. Сибирский государственный университет телекоммуникаций и информатики, Новосибирск, 2016. 179 с.
16. Ireland E. Intrusion Detection with Genetic Algorithms and Fuzzy Logic / E. Ireland // UMM CSci Senior Seminar Conference. – Morris, 2013. pp. 1-6.
17. Moustafa Nour, Jill Slay. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015. pp. 1-6.
18. Moustafa Nour, Jill Slay. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. // Information Security Journal: A Global Perspective (2016): 1-14.
19. Ле Тхи Чанг Линь. Многослойная нейронная сеть в задаче обнаружения атак, представленных в современной базе данных UNSW-NB15. Сб. Тезисов Международной конференции «Инжиниринг & Телекоммуникации – En&T 2016». М.: МФТИ, 2016. С. 163-164.
20. Zhe Wu, Chris Nicholson, Charlie Berger. Build Recommender Systems, Detect Network Intrusion, and Integrate Deep Learning with Graph Technologies. BIWA 2017. [Электронный ресурс] URL: https://download.oracle.com/otndocs/products/spatial/pdf/biwa2017/Biwa2017_Build_Recommenders_DeepLearning_Graph_Wu_Berger_Nicholson_842439.pdf. (дата обращения: 03.06.2018).
21. Dipali Gangadhar Mogal, Sheshnarayan R. Ghungrad, Bapusaheb B. Bhusare. NIDS using Machine Learning Classifiers on UNSW-NB15 and KDDCUP99 Datasets. // International Journal of Advanced Research in Computer and Communication Engineering.Vol. 6, Issue 4, April 2017. pp. 533-537.

Intelligent network traffic analysis for computer intrusion detection

A. O. Suvorov[I,II], V. A. Suvorova[III]

[I] Perm National Research Polytechnic University, Perm, Russia
[II] National Research University Higher School of Economics, Moscow, Russia
[III] JSC "Jet Infosystems", Moscow, Russia

Abstract. The article considers the process of building an intrusion detection system using intelligent network traffic analysis. The requirements for the developed system of intrusion detection are formulated, as well as its architecture is proposed. As a mechanism for making decisions about the presence of attacks, it is suggested to use methods of inductive machine learning, namely, artificial neural networks. The paper proposes the construction of a neural network model based on a multilayer perceptron, for which the most significant input parameters are determined. The technique of constructing the intelligent network traffic analysis module, its logic of work are considered. The client-server application for network traffic analysis on the generated parameters was developed ang the results of testing are given in the paper. The created module of intelligent network traffic analysis shows high accuracy of attacks identification. To increase the accuracy of network attack classification, in future studies, it is planned to supplement the intelligent network traffic analysis module with other methods of machine learning, in particular, the machine classifier.
Keywords: intrusion detection system, artificial neural networks, network attacks, intelligent traffic analysis.

DOI 10.14357/20718594190106

References

1. Laboratoriya Kasperskogo. Statistika setevykh atak [Kaspersky Lab. Statistics of network attacks]. Available at: https://securelist.ru/statistics/ (accessed July 30, 2018).
2. Olifer V.G., Olifer N.A. 2016. Komp'yuternye seti. Printsipy, tekhnologii, protokoly [Computer networks. Principles, technologies, protocols]. St. Petersburg: Peter. 996 p.
3. Shangin V.F. 2011. Informatsionnaya bezopasnost' komp'yuternykh sistem i setej [Information security of computer systems and networks]. Moscow: ID FORUM: INFRA-M. 416 p.
4. Timofeev A.V., Bronitsky A.A. 2012. Issledovanie i modelirovanie nejrosetevogo metoda obnaruzheniya i klassifikatsii setevykh atak [Investigation and simulation of the neural network method for detecting and classifying network attacks]. International Journal "Information Technologies & Knowledge". 6 (3): 257-265.
5. Ilgun K., Kemmerer R.A, Porras P.A. 1995. State Transition Analysis: A Rule-Based Intrusion Detection System. IEEE Trans. Software Eng. 21 (3): 181-199.
6. Lindqvist U., Porras P.A. 1999. Detecting Computer and Network Misuse with the Production-Based Expert System Tools. IEEE Symp. Security and Privacy, IEEE CS Press, Los Alamitos, Calif. 146-161.
7. Yasnitsky L.N. 2016. Intellektual'nye sistemy [Intelligent Systems]. Moscow: Laboratoriya znanij. 221 p.
8. KDD Cup 1999 Data. Available at: http://kdd.ics.uci.edu/databases/kddcup99 (accessed June 3, 2018).
9. Suvorova V.A. Suvorov A.O. 2017. Razrabotka modeli obnaruzheniya setevykh atak na osnove iskusstvennoj nejronnoj seti [Development of a model for detecting network attacks based on an artificial neural network]. Iskusstvennyj intellekt v reshenii aktual'nykh sotsial'nykh i ehkonomicheskikh problem XXI veka: sb. st. po materialam Vtoroj vseross. nauch.-prakt. konf. Perm. gos. nats. issled. un-t. [Artificial intelligence in solving urgent social and economic problems of the XXI century: Sat. Art. based on the Second All-Russian. scientific-practical. Conf. Perm. state. nat. Issled. un-t]. Perm. 129-135.
10. Suvorova V.A. 2017. Razrabotka prilozheniya dlya obnaruzheniya i klassifikatsii atak na osnove nejrosetevoj modeli [Development of an application for detecting and classifying attacks based on a neural network model]. Lomonosov – 2017: XXIV Mezhdunarodnaya nauchnaya konferentsiya studentov, aspirantov, molodykh uchenykh: sb. tezisov. Izdatel'skij otdel fakul'teta VMiK MGU [Lomonosov – 2017: XXIV International Scientific Conference of Students, Postgraduates, Young Scientists: Sat. theses. Publishing Department of the Faculty of Computer Science and Computer Science of Moscow State University]. Moscow. 117-119.
11. Mustafayev A.G. 2016. Nejrosetevaya sistema obnaruzheniya komp'yuternykh atak na osnove analiza setevogo trafika [Neural network system for detecting computer attacks based on network traffic analysis] Voprosy bezopasnosti [Security issues]. 2: 1-7. Available at: http://e-notabene.ru/nb/article_18834.html (accessed January 3, 2017).
12. Zhigulin PV, Maltsev AV, Melnikov MA, Podvorchan D.E. 2013. Analiz setevogo trafika na osnove nejronnykh setej [Analysis of network traffic based on neural networks]. Elektronnye sredstva i sistemy upravleniya [Electronic means and control systems]. 2: 44-48.
13. Yemelyanova Yu.G., Talalayev A.A., Tischenko I.P., Fralenko V.P. 2011. Nejrosetevaya tekhnologiya obnaruzheniya setevykh atak na informatsionnye resursy [Neural network technology for detecting network attacks on information resources]. Programmnye sistemy: Teoriya i prilozheniya [Software Systems: Theory and Applications]. 3 (7): 3-15.
14. L'ıdio Mauro, Roberto C'elio Lima ao de Oliveira, Mauro Roisenberg. 2012. Network Intrusion Detection System Using Data Mining. Communications in Computer and Information Science. Chapter: Engineering Applications of Neural Networks, Publisher: Springer Berlin Heidelberg. 104-113.
15. Zubkov E.V. 2016. Algoritmy i metodiki intellektual'nogo analiza sobytij informatsionnoj bezopasnosti v setyakh i sistemakh telekommunikatsij [Algorithms and techniques of the intellectual analysis of events of information safety in networks and systems of telecommunications]. PhD Diss. Novosibirsk. 179 p.
16. Ireland E. 2013. Intrusion Detection with Genetic Algorithms and Fuzzy Logic. UMM CSci Senior Seminar Conference. Morris. 1-6.
17. Moustafa Nour, Jill Slay. 2015. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Military Communications and Information Systems Conference (MilCIS). IEEE. 1-6.
18. Moustafa Nour, Jill Slay. 2016. The evaluation of the Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective. 1-14.
19. Le Thi Chang Lin. 2016. Mnogoslojnaya nejronnaya set' v zadache obnaruzheniya atak, predstavlennykh v sovremennoj baze dannykh UNSW-NB15 [Multilayer neural network in the task of detecting attacks presented in the modern database UNSW-NB15]. Sb. Tezisov Mezhdunarodnoj konferentsii «Inzhiniring & Telekommunikatsii – En&T 2016». [Sat. Theses of the International Conference "Engineering & Telecommunications – En&T 2016"]. Moscow. Dolgoprudny. MIPT. 163-164.
20. Zhe Wu, Chris Nicholson, Charlie Berger. Build Recommender Systems, Detect Network Intrusion, and Integrate Deep Learning with Graph Technologies. BIWA 2017. Available at: https://download.oracle.com/otndocs/products/spatial/pdf/biwa2017/Biwa2017_Build_Recommenders_DeepLearning_Graph_Wu_Berger_Nicholson_842439.pdf (accessed June 3, 2018).
21. Dipali Gangadhar Mogal, Sheshnarayan R. Ghungrad, Bapusaheb B. Bhusare. 2017. NIDS using Machine Learning Classifiers on UNSW-NB15 and KDDCUP99 Datasets. International Journal of Advanced Research in Computer and Communication Engineering. 6 (4): 533-537.