# ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ НИЗКОИНТЕНСИВНЫХ DDoS-АТАК ПРИКЛАДНОГО УРОВНЯ

***Тарасов Я.В.***[1]

*В статье рассматривается опыт применения искусственных нейронных сетей для обнаружения низкоинтенсивных (малой мощности) распределённых компьютерных атак на отказ в обслуживании, реализуемых на прикладном уровне. Рассмотрены особенности популярных компьютерных атак на отказ в обслуживании, в частности RUDY, SlowLoris и вариации HTTP–flood. Отмечен актуальность атак, имитирующих действий легитимных пользователей на веб–порталах. Показано, что применение традиционных средств обнаружения и противодействия крупномасштабным кибератак на отказ в обслуживании неэффективно либо экономически невыгодно. Даны рекомендации по снижению уровня ложных срабатываний. Рассмотрены различные сценарии низкоинтенсивных распределённых компьютерных атак. Предложена гибридная нейронная сеть для выявления распределенных компьютерных атак на отказ обслуживании. Разработаны концептуальные модели компонента источника событий и компонента формирования задержек. Разработан способ и общая методика выявления низкоинтенсивных компьютерных атак на отказ в обслуживании. Приведено экспериментальное исследования по применению нейросетевых подходов.*

***Ключевые слова****: обнаружение атак; низкоинтенсивная атака; DDoS–атака; персептрон, самоорганизующаяся карта; сетевая безопасность; распознавание образов; атака малой мощности.*

**DOI**: 10.21681/2311-3456-2017-5-23-29

**Введение**

В настоящее время защита веб-ресурсов информационных сетей от распределённых атак на отказ в обслуживании (DDoS-атак) является наиболее проблемной среди большинства задач по обеспечению безопасности киберпространства [1, 2]. По материалам ряда источников, касающихся безопасности Internet-ресурсов, в последние годы наблюдается постоянное увеличение и количества DDoS-атак, и убытков от них [3-7]. Новым в этой статистике являются сразу два аспекта:

- целями DDoS-атак стали чаще становится Internet-ресурсы малого и среднего размера;

- инструментами воздействия становятся DDoS-атаки малой мощности, иначе называемые низкоинтенсивными.

Следствием первого пункта является экономическая нецелесообразность для жертвы атаки в использовании средств провайдеров для обнаружения и предотвращения атак, т.к. эти средства изначально предназначены для борьбы с атаками большой мощности, заполняющими полосы канала связи и использующими бот-сети большого размера.

С другой стороны, для проведения низкоинтенсивных атак не используют бот-сетей большой мощности, и их проведение не сопровождается появлением заметных аномалий в использовании полосы пропускания канала связи [6]. Трафик, возникающий при такой атаке может вообще не отличаться от нормального сеанса работы с ресурсом-жертвой, так как клиенты бот-сети используют техники имитации поведения легитимных пользователей.

**Сценарии DDOS-атак малой мощности**

Характерными представителями рассматриваемого класса DoS-атак являются атаки RUDY, SlowLoris и вариации HTTP-flood.

Атака типа RUDY заключается в бесконечной отправке WEB-формы приложению (рис. 1). Для этого атакующий отправляет POST-запрос на определенный URI с содержимым небольшого размера – в пределе 1 байт. Далее следует задержка передачи на время меньшее чем, время ожидания окончания соединения (time-out) в протоколе TCP. В результате потоки приложения, занятые обработкой данных POST-запросов зависают на время необходимое атакующему.

Атака типа SlowLoris заключается в отправке незавершенных HTTP-запросов, чтобы занять стек приложения и держать соединения открытыми (рис. 2). WEB-сервер быстро достигает максимальной емкости стека и становится недоступным для новых подключений легитимных пользователей.

1 Тарасов Ярослав Викторович, ЗАО «Инфосистемы Джет», Москва, Россия. E-mail: info@jet.msk.su


***Рис. 1*** *- Сценарий атаки RUDY*

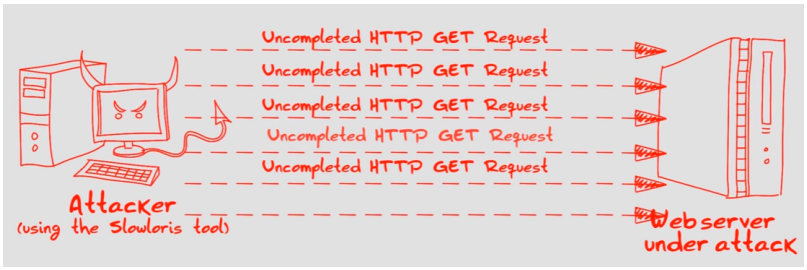


***Рис. 2*** *- Сценарий атаки SlowLoris*

Различают два типа основных типа HTTP-flood - GET и POST. GET HTTP-flood заключается в посылке большого числа GET-запросов, инициирующих скачивание больших объёмов данных с атакуемого web-сервера (рис. 3). Это приводит к истощению аппаратных ресурсов сервера.

При проведении POST HTTP-flood атакующий отправляет большое число данных в формы web-сайта, маскируясь под легитимную отправку данных пользователями (рис. 4). Использование разных параметров запросов позволяет избежать обнаружения и блокирования сценария при помощи средств защиты на основе статических сигнатур трафика.

Для рассмотренных сценариев атак характерны следующие признаки:

– генерация периодического трафика малого объёма;

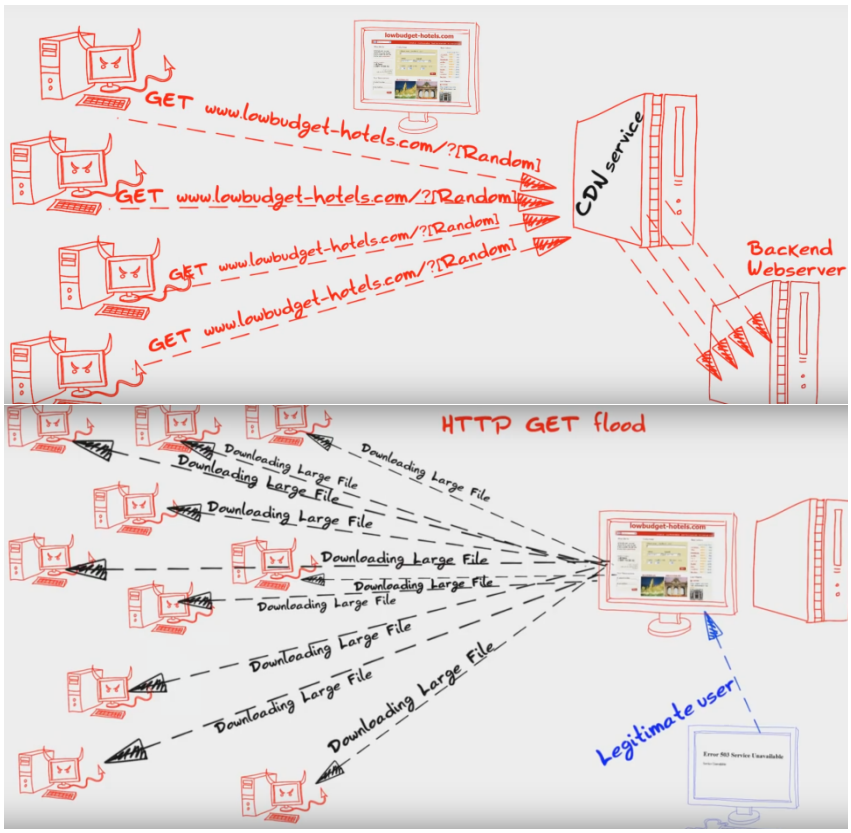


***Рис. 3*** *- Сценарий атаки GET HTTP-flood*


***Рис. 4** - Сценарий атаки POST HTTP-flood*

– атакующее воздействие составляют однотипные элементы трафика;

– отдельный запрос или сетевой пакет нельзя определить как аномалию.

Во всех сценариях временной интервал между отдельными пакетами значительно меньше таймаута окончания соединения (connection time out). Но так как значение connection time out практически для всех приложений является реконфигурируемым параметром, нельзя заранее установить точное значение временного интервала между отправкой пакетов.

Самым популярным сценарием продолжает оставаться HTTP-flood, однако, как сказано выше, отмечается эволюция данного типа атак в сторону имитации действий легитимных пользователей на сайте.

**Метод обнаружения низкоинтенсивных DDoS-атак**

Предлагаемая модель представляет собой упорядоченную по времени последовательность событий, т.е. временной ряд [11].

В число наблюдаемых свойств атаки включено:

1) Порядок поступления пакетов на атакуемую ЭВМ;
2) Поля заголовка уровня IP;
3) Поля заголовка уровня TCP;
4) Поля заголовка протокола HTTP;
5) Полезная нагрузка протокола HTTP;
6) Порядок следования пакетов, поступающих на сетевой узел;
7) Число пакетов в единицу времени, поступающее на целевой узел;
8) Количество бит информации в единицу времени, поступающее на целевой узел;
9) Промежутки времени между поступлением пакетов.

На рисунке 5 приведена логическая схема источника событий атаки, где *S,D,E* – соответственно временные ряды событий атаки, событий не относящихся к атаке и результирующий ряд событий на целевой машине, линии задержки выполняют задержку на заданное количество событий, переключатель *F* допускает передачу на выход (E) только события из одного ряда.

Рассмотрим схему канала связи от атакующей (или атакующих) до целевой ЭВМ с точки зрения относительных задержек (для элементов *S* по сравнению с элементами *D*). Такая схема представлена на рисунке 6.

Представим низкоинтенсивную атаку в виде наложения нормальных сетевых событий и аномального трафика. Тогда метод обнаружения заключается в последовательном выделении однородных групп временного ряда (поступающих сетевых пакетов) при помощи моделей распознавания образов и построения для каждой выделенной группы модели прогнозирования для обнаружения сценария атаки.

Необходимо отметить, что длительность ряда D значительно больше, чем длительность ряда S, поскольку выбранный класс атак по определению является низкоинтенсивным и вносит незначительный вклад в объем трафика. Переходя к понятиям цифровой обработки сигнала можно сформулировать следующее положение: если рассматривать вредоносное воздействие S как искомый сигнал, а временной ряд, представляющий легитимный трафик D как шум, затрудняющий обнаружение искомого сигнала, то рассматриваемый временной ряд E имеет высокий уровень шума (или низкое соотношение сигнал/шум). Указать точное соотношение сигнал/шум возможным не представляется возможным, поскольку существу-

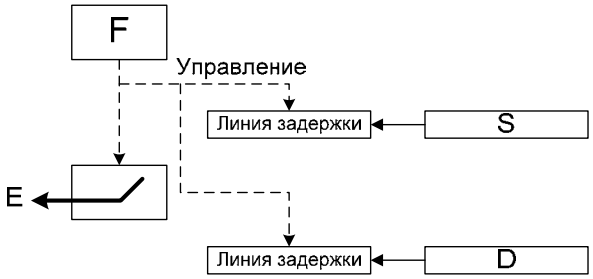


***Рис. 5** - Схема источника событий*

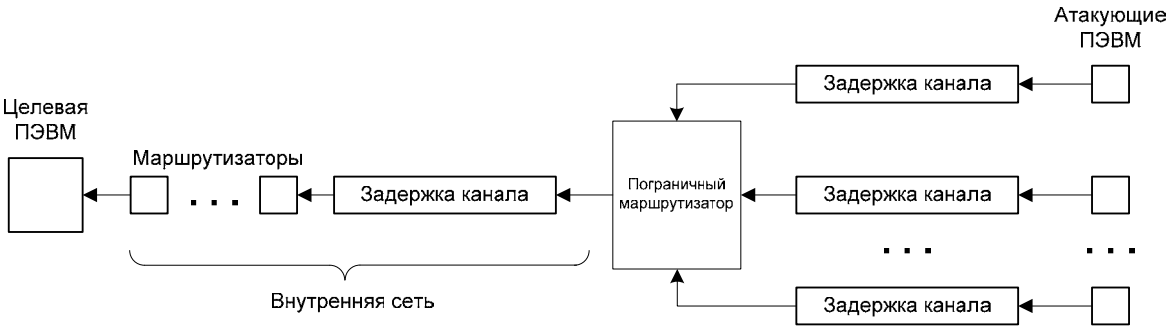


***Рис. 6** - Схема формирования задержек*

ющие модели шума не вполне подходят для оценки данного типа ряда (уровень шума в десятки раз превосходит уровень сигнала).

Это приводит нас к модели атаки в виде аддитивного наложения двух сигналов – атакующего воздействия и легального воздействия.

Подробно разработка модели низкоинтенсивной сетевой атаки рассматривается в [12].

Как и любой метод машинного обучения, описываемый метод обнаружения низкоинтенсивных атак может быть представлен в виде двух последовательных фаз - фазы обучения и фазы классификации.

Фаза обучения подчиняется общим принципам построения моделей данных, и конкретизируется только используемым методом обучения [13].

В фазе обучения строится классификатор. Это происходит путём итерационной настройки параметров классификатора на обучающем множестве. Далее в этой фазе происходит оценка (верификация) полученной модели прогнозирования временных рядов на тестовом множестве, состоящем из проверочных примеров. Как множество обучающих примеров, так и множество проверочных примеров должны быть предварительно, хотя бы частично, классифицированы экспертом.

В случае совпадения результата проверки обученного классификатора на тестовом множестве с ожидаемым результатом, и если, при этом, результат достаточен для классификации, переходят к следующей фазе. В результате фазы обучения мы получаем классификатор с настроенными параметрами, достаточными для успешной классификации.

Целью этапа классификации является вычисление меток классов для ранее неизвестных наборов данных с применением обученного классификатора. Результат этапа классификации - набор меток классов для ранее неизвестных наборов данных.

Можно сформулировать шаги метода.

1. Построить отдельную искусственную нейронную сеть для каждого контролируемого сервиса (порта). Сети функционируют аналогично друг другу. Далее будет рассматриваться выявление атак на один сервис.
2. Для выбранного сервиса принять от источника данных некоторое множество сетевых пакетов, число которых определяется выбранным значением величины окна.
3. На шаге снижения размерности формируются вектора для самоорганизующейся карты.
4. Снизить размерность входных данных. Для разработанного метода - кластеризация векторов самоорганизующейся картой.
5. Сформировать вектора для многослойного персептрона (MLP), где каждый компонент вектора будет соответствовать номеру кластера, в который распределился пакет. Таким образом, входной вектор представляет собой набор кластеризованных сетевых пакетов, который сохраняет информацию

о последовательности (порядке) поступления внутри окна. Для этих пакетов уже будет установлена их принадлежность к определённому типу.

6. Вектора анализируются на MLP, выявленные в трафике на шаге 4 наборы классифицируются. В результате осуществляется разделение на два класса - атака или норма.

Шаги метода подробно описаны в [13].

**Экспериментальное исследование разработанного метода**

Самоорганизующаяся сеть имеет размеры 25 на 20 и использует гексагональную структуру связей нейронов. Обучение сети Кохонена происходит на отдельных пакетах, последовательно выбираемых из окна.

Используется многослойный персептрон со следующей структурой – два скрытых слоя с числом нейронов 21 и 7 (подобрано в ходе экспериментов), выходной слой. Активационная функция в скрытый слоях – гиперболический тангенс, в выходном слое – линейная. Метод обучения – trainlm.

При проведении экспериментального исследования использовались следующие значения:

- размер окна 1500 пакетов – для утилизации канала передачи в 1% при скорости сети 100 Мбит/с [14, 15];

- размер окна 30 пакетов - минимальное значение числа пакетов в сценарии, применяемое в правилах системы обнаружения атак Snort для низкоинтенсивных атак.

- размер окна 180 - соответствует скорости поступления 1 пакет в секунду.

Для обучения искусственной нейронной сети моделировались два типа сетевого трафика – нормальный и атакующий, с имитацией распределённой низконтенсивной атаки с 10 адресов. В качестве цели атак использовался web-сайт с одноуровневой структурой.

При генерации нормального трафика генератор производит случайное количество запросов с случайным тайм-аутом без генерации случайных путей (только к корню).

При генерации трафика Slowloris и Rudy сценарий производит множество запросов к веб серверу с случайными URI и в дальнейшем поддерживает их, передавая запросы с заголовком поддержания соединения (keep-alive). Генерируется минимальное количество трафика. При моделировании GET HTTP-flood генерировалось около 10000 запросов в минуту размером 20 Кбайт.

Время обучения при выборке из 20000 векторов составляет 300 секунд (Intel Core i7, 16 Gb, SSD).

При тестировании результативности распознавания на нейронную сеть подавались оба типа трафика (атака-норма). В ходе экспериментов исследовалось влияние различных значений длины вектора, размера обучающей выборки и величины окна на точность распознавания. Ошибка первого рода (ложное срабатывание) в худшем случае не превышает 0,12%. Ошибка второго рода в наихудшем случае составляет 0,84%.

Более подробно процесс проведения экспериментального исследования рассматривается в [16].

**Заключение**

Результаты сравнительного анализа применяемых методов обнаружения показывают, что методы защиты, основанные на изменении конфигурации сервера или применении правил межсетевых экранов и СОВ на основе статических сигнатур не позволяют эффективно защищаться от низкоинтенсивных DDoS-атак. Для всех этих методов характерен высокий уровень ложных срабатываний (ошибок первого рода).

Для снижения указанного недостатка (как показал эксперимент) целесообразно использовать гибридные искусственные нейронные сети.

*Рецензент: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

**Литература**

1. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С. 28-35.
2. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении./Под общей редакцией С.Ф.Боева; вводные слова А.И.Смирнова и А.Г.Тормасова; вводная статья И.А.Каляева. -Инополис: Издательский Дом «Афина», 2017. 440 с.
3. Гнеушев В.А., Кравец А.Г., Козунова С.С., Бабенко А.А. Моделирование сетевых атак злоумышленников в корпоративной информационной системе // Промышленные АСУ и контроллеры. 2017. № 6. С. 51-60.
4. Гречишников Е.В., Добрышин М.М., Закалкин П.В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак // Вопросы кибербезопасности. 2016. № 3 (16). С. 4-12.
5. Ковалева И.В., Баженов Р.И. Исследование мультиагентной модели в системе Netlogo (модель DDoS атаки) // Постулат. 2017. № 5-1 (19). С. 104.

6. Косенко М.Ю., Мельников А.В. Вопросы обеспечения защиты информационных систем от ботнет атак // Вопросы кибербезопасности. 2016. № 4 (17). С. 20-28.
7. Оладько В.С. Программный комплекс для определения закона распределения атак злоумышленников // Вопросы кибербезопасности. 2015. № 1 (9). С. 55-59.
8. Пальчевский Е.В., Халиков А.Р. Применение нейронной сети в защите от DDOS-атак // В сборнике: Инновации в науке и практике. Сборник статей по материалам I международной научно-практической конференции. 2017. С. 37-42.
9. Петренко А.С., Петренко С.А. Первые межгосударственные киберучения стран СНГ: «Кибер-антитеррор-2016» // Защита информации. Инсайд. 2016. № 5 (71). С. 57-63.
10. Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDoS-угроз // Вопросы кибербезопасности. 2017. № 3 (21). С. 16-23.
11. Барсегян А.А., Куприянов М.С., Холод И.И., Тесс М.Д., Елизаров С.И. Анализ данных и процессов 3-е изд. СПб.: БХВ-Петербург, 2009. — 512 с. — ISBN: 978-5-9775-0368-6.
12. Тарасов Я.В. Опыт использования технологий нейронных сетей для обнаружения низкоинтенсивных DDoS-атак // В сборнике: Безопасные информационные технологии (БИТ-2016) Сборник трудов Седьмой Всероссийской научно-технической конференции. Под редакцией В.А. Матвеева. 2016. МГТУ им. Н.Э.Баумана, С. 270-274.
13. Абрамов Е.С., Тарасов Я.В., Тумоян Е.П., Нейросетевой метод обнаружения низкоинтенсивных атак типа «отказ в обслуживании» // Известия ЮФУ. Технические науки, № 9 (182), 2016.
14. Robert Graham, «What's the max speed on Ethernet?» // URL: blog.erratasec.com/2013/10/whats-max-speed-on-ethernet.html#.UIbwuNK8Dp8
15. Stephen Northcutt, Judy Novak (2002) "Network Intrusion Detection An Analyst's Handbook". Sams Publishing, 346 pp.
16. Абрамов Е.С., Тарасов Я.В. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы // Инженерный вестник Дона. 2017. № 3.

# INVESTIGATION OF THE USE OF NEURAL NETWORKS FOR DETECTING LOW-INTENSIVE DDoS-ATAK OF APPLIED LEVEL

***Tarasov Ya.V.*[2]**

*The article deals with the experience of using artificial neural networks to detect low–intensity (low power) distributed computer attacks on denial of service, implemented at the application level. Features of popular computer attacks on denial of service, in particular RUDY, SlowLoris and variations of HTTP–flood are considered. The relevance of attacks simulating the actions of legitimate users on web portals was noted. It is shown that the use of traditional means of detection and counteraction of large–scale cyberattacks on denial of service is inefficient or economically unprofitable. Recommendations are given to reduce the level of false positives. Various scenarios of low–level distributed computer attacks are considered. A hybrid neural network is proposed for detecting distributed computer attacks on failure of maintenance. Conceptual models of the source component of events and the component of delay formation are developed. A method and a general method for identifying low–intensity computer attacks on denial of service are developed. Experimental research on the application of neural network approaches is presented.*

***Keywords**: detection of attacks; low–intensity attack; DDoS; perceptron, self–organizing map; network security; pattern recognition; low power attack.*

**References**

1. Markov A.S., Tsirlov V.L. Rukovodyashchie ukazaniya po kiberbezopasnosti v kontekste ISO 27032, Voprosy kiberbezopasnosti. 2014, No 1 (2), pp. 28-35.
2. Petrenko S.A., Stupin D.D. Nacional'naya sistema rannego preduprezhdeniya o komp'yuternom napadenii./Pod obshchej redakciej S.F.Boeva; vvodnye slova A.I.Smirnova i A.G.Tormasova; vvodnaya stat'ya I.A.Kalyaeva. -Innopolis: Izdatel'skij Dom «Afina», 2017. 440 p.
3. Gneushev V.A., Kravec A.G., Kozunova S.S., Babenko A.A. Modelirovanie setevyh atak zloumyshlennikov v korporativnoj informacionnoj sisteme, Promyshlennye ASU i kontrollery. 2017, No 6, pp. 51-60.

2 Tarasov Yaroslav, CJSC Jet Infosystems, Moscow, Russia. E-mail: info@jet.msk.su

4. Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. Model' uzla dostupa VPN kak ob»ekta setevoj i potokovoj komp'yuternyh razvedok i DDoS-atak, Voprosy kiberbezopasnosti. 2016, No 3 (16), pp. 4-12.
5. Kovaleva I.V., Bazhenov R.I. Issledovanie mul'tiagentnoj modeli v sisteme Netlogo (model' DDoS ataki), Postulat. 2017, No 5-1 (19), pp. 104.
6. Kosenko M.YU., Mel'nikov A.V. Voprosy obespecheniya zashchity informacionnyh sistem ot botnet atak, Voprosy kiberbezopasnosti. 2016, No 4 (17), pp. 20-28.
7. Olad'ko V.S. Programmnyj kompleks dlya opredeleniya zakona raspredeleniya atak zloumyshlennikov, Voprosy kiberbezopasnosti. 2015, No 1 (9), pp. 55-59.
8. Pal'chevskij E.V., Halikov A.R. Primenenie nejronnoj seti v zashchite ot DDOS-atak, V sbornike: Innovacii v nauke i praktike. Sbornik statej po materialam I mezhdunarodnoj nauchno-prakticheskoj konferencii. 2017, pp. 37-42.
9. Petrenko A.S., Petrenko S.A. Pervye mezhgosudarstvennye kiberucheniya stran SNG: «Kiber-antiterror-2016», Zashchita informacii. Insajd. 2016, No 5 (71), pp. 57-63.
10. Revenkov P.V., Berdyugin A.A. Rasshirenie profilya operacionnogo riska v bankah pri vozrastanii DDoS-ugroz, Voprosy kiberbezopasnosti. 2017, No 3 (21), pp. 16-23.
11. Barsegyan A.A., Kupriyanov M.S., Holod I.I., Tess M.D., Elizarov S.I. Analiz dannyh i processov 3-e izd. SPb.: BHV-Peterburg, 2009. — 512 s. — ISBN: 978-5-9775-0368-6.
12. Tarasov YA.V. Opyt ispol'zovaniya tekhnologij nejronnyh setej dlya obnaruzheniya nizkointensivnyh DDoS-atak, V sbornike: Bezopasnye informacionnye tekhnologii (BIT-2016) Sbornik trudov Sed'moj Vserossijskoj nauchno-tekhnicheskoj konferencii. Pod redakciej V.A. Matveeva. 2016. MGTU im. N.EH.Baumana, S. 270-274.
13. Abramov E.S., Tarasov YA.V., Tumoyan E.P., Nejrosetevoj metod obnaruzheniya nizkointensivnyh atak tipa «otkaz v obsluzhivanii», Izvestiya YUFU. Tekhnicheskie nauki, № 9 (182), 2016.
14. Robert Graham, «What's the max speed on Ethernet?», URL: blog.erratasec.com/2013/10/whats-max-speed-on-ethernet.html#.UIbwuNK8Dp8
15. Stephen Northcutt, Judy Novak (2002) "Network Intrusion Detection An Analyst's Handbook", Sams Publishing, 346 pp.
16. Abramov E.S., Tarasov YA.V. Primenenie kombinirovannogo nejrosetevogo metoda dlya obnaruzheniya nizkointensivnyh DDoS-atak na web-servisy, Inzhenernyj vestnik Dona. 2017, No 3.