Для цитирования: *М.В. Тумбинская, В.В. Волков, Б.Г. Загидуллин. Применение статистических методов для прогнозирования UDP-FLOOD атак. Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47(2): 108-122. DOI:10.21822/2073-6185-2020-47-2-108-122*
For citation: *M.V. Tumbinskaya, V.V. Volkov, B.G. Zagidullin. Application of statistical methods for predicting udp-flood attacks. Herald of Daghestan State Technical University. Technical Sciences. 2020; 47 (2): 108-122. (In Russ.) DOI:10.21822/2073-6185-2020-47-2-108-122*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 519.71
DOI: 10.21822/2073-6185-2020-47-2-108-122

ПРИМЕНЕНИЕ СТАТИСТИЧЕСКИХ МЕТОДОВ ДЛЯ ПРОГНОЗИРОВАНИЯ UDP-FLOOD АТАК

М.В. Тумбинская, В.В. Волков, Б.Г. Загидуллин
Казанский национальный исследовательский технический университет им. А.Н. Туполева, 420111, г. Казань, ул. Карла Маркса, 10, Россия

Резюме. Цель. *Web-ресурсы являются неотъемлемой частью жизни современного человека, которые в настоящее время все чаще подвергаются хакерским атакам, такими как внедрение операторов SQL, межсайтовое выполнение сценариев и др. DDoS-атаки продолжают входить в топ-10 сетевых атак и приводить к серьезным сбоям и отказам работы web-ресурсов, наиболее распространенным типом DDoS-атак является UDP-flood атаки, основанные на бесконечной посылке UDP-пакетов на порты различных UDP-сервисов. Основанием для проведения эмпирического исследования являются факторы: отсутствие эффективных средств защиты от DDoS-атак, специфика UDP-flood атак, отсутствие моделей прогнозирования, адекватно описывающих исследуемый процесс. Целью исследования является повышение уровня защищённости web-ресурсов, за счет своевременного обнаружения аномалий в их работе, обнаружении информационных угроз безопасности на основе методов анализа и прогнозирования. В качестве объекта исследования был выбран тип атак UDP-flood из семейства DDoS атак.* ***Метод.*** *Методами корреляционного анализа и моделирования были рассчитаны индекс сезонности UDP-flood атак, автокорреляция временного ряда данного типа атак, на основе моделей простого экспоненциального сглаживания и нейросетевого прогнозирования построен прогноз UDP-flood атак.* ***Результат.*** *В работе предложена классификация DDoS-атак, описаны способы защиты. На основе корреляционного анализа рассчитаны прогнозные значения воздействия UDP-flood атак на web-ресурсы, выявлен фактор – сезонность. Анализ результатов прогнозирования показал, что разброс прогнозных значений не значительный, наибольшее количество атак ожидается в IV квартале 2020 года. Для DDoS-атак длительностью до 20 минут также выявлена сезонность в I квартале календарного года, а значит, в I квартале 2020 года следует ожидать наибольшее количество атак данной длительности.* ***Вывод.*** *Перспективы дальнейшего исследования проблемы защиты от DDoS атак представляются в дальнейшей проработке методики противодействия UDP-flood атакам, алгоритмов информационной безопасности web-ресурсов, что позволит сократить количество инцидентов UDP-flood атак, планировать мероприятия по повышению уровня защищенности web-ресурсов, повысить уровень их защищенности.*

Ключевые слова: *DDoS-атака, UDP-flood, корреляционный анализ, прогнозирование, метод простого экспоненциального сглаживания, коэффициент сглаживания, моделирование, аддитивная модель временных рядов, автокорреляционная функция, защита информации*

APPLICATION OF STATISTICAL METHODS FOR PREDICTING UDP-FLOOD ATTACKS

M.V. Tumbinskaya, V.V. Volkov, B.G. Zagidullin
Kazan National Research Technical University named after A. N. Tupolev,
10 Karl Marx St., Kazan 420111, Russia

Abstract. Aim. *Web resources are an integral part of modern human life. Today, these resources are increasingly exposed to hacker attacks, such as the introduction of SQL operators, cross-site scripting, etc. DDoS attacks continue to be included in the top 10 network attacks that lead to serious failures of web resources. The most common type of DDoS attack is UDP-flood attacks based on the endless sending of UDP packets to the ports of various UDP services. Our empirical study was based on the following factors: the lack of effective means of protection against DDoS attacks, the specificity of UDP-flood attacks, and the lack of prediction models that adequately describe the process under study. The aim of this study was to increase the level of security of web resources by means of timely detection of anomalies in their work, detection of information security threats based on analysis and forecasting methods. The research object was UDP-flood attacks.* ***Methods.*** *Correlation analysis and modelling methods were used to calculate the seasonal index of UDP-flood attacks and the autocorrelation of the time series of this type of attack. The forecast of UDP-flood attacks was built based on simple exponential smoothing and neural network forecasting models.* ***Results.*** *A classification of DDoS attacks was proposed, along with possible protection approaches. Using a correlation analysis, the forecast values of the impact of UDP-flood attacks against web resources were calculated, and the seasonal factor was identified. The analysis of the forecast results showed that the spread of forecast values was not significant; the largest number of attacks is expected in the fourth quarter of 2020. For DDoS attacks lasting up to 20 minutes, seasonality was also detected in the first quarter of the calendar year, which means that the largest number of attacks of this duration should be expected in the first quarter of 2020.* ***Conclusion.*** *In order to improve the level of protection against DDoS attacks, further research should be aimed at developing methods for combating UDP-flood attacks and algorithms increasing the information security of web resources, as well as implementing measures to improve the security of web-based resources.*

Keywords: *DDoS attack, UDP-flood, correlation analysis, forecasting, simple exponential smoothing method, smoothing coefficient, modeling, additive time series model, autocorrelation function, information protection*

Введение. DDoS (Distributed Denial of Service) − это распределенная атака типа «отказ в обслуживании», которая представляет собой одновременную, массовую отправку информационных запросов на веб-сервер, при которых пользователи не смогут получить доступ к веб-серверу из-за его перегрузки [1].

На практике скорость поступления новых запросов на web-сервер превышает скорость обработки, очередь запросов становится длинной, и новые запросы не обрабатываются. Это главный принцип DDoS-атаки. Подобного рода атаки выполняются одновременно с большого количества устройств. Злоумышленники для этих целей используют персональные компьютеры, различные IoT устройства, к которым они смогли получить доступ, например, видеокамеры и роутеры с устаревшей версией программного обеспечения, устройства контроля, компьютеры пользователей с вредоносным программным обеспечением. Одним из видов [2] DDoS-атак является UDP-flood, сценарий которой заключается в одновременной отправке веб-серверу большого количества UDP-пакетов с широкого диапазона IP-адресов. Вследствие атаки, сетевые интерфейсы перегружены поддельными UDP-пакетами на всей полосе пропускания трафика.

Для проведения эффективной защиты от угроз UDP-flood атак методы анализа и прогнозирования должны быть эффективными. Решению общих проблем прогнозирования и выявления UDP-flood атак посвящены работы зарубежных авторов Cabrera J. B. D. и др. [3], Raza M. A. и др. [4], K. S. Sahoo и др. [5], российских авторов В.И. Городецкого, И.В. Котенко, А.В. Лу-

кацкого, С.М. Климова, С.С. Корта и др. [6 – 11]. Однако проанализированные работы не могут полностью решить задачу своевременного обнаружения угроз информационной безопасности из-за отсутствия точных и адекватных прогнозов неблагоприятного сетевого трафика.

Постановка задачи. Для повышения качества средств защиты web-ресурсов, методами корреляционного анализа, на основе анализа результатов прогнозирования методами простого экспоненциального сглаживания, на основе аддитивной модели временных рядов и нейросетевого прогнозирования предлагается построить среднесрочный прогноз кибератак типа UDP-flood с учетом факторов сезонности и длительности по времени, который позволит обеспечить необходимый уровень безопасности web-ресурсов, предотвратить инциденты UDP-flood атак на web-ресурсы.

Целью исследования является повышение уровня защищённости web-ресурсов, за счет своевременного обнаружения аномалий в их работе, обнаружении информационных угроз безопасности на основе методов анализа и прогнозирования.

В результате анализа научной литературы и интернет ресурсов [12 – 17] было выявлено, что сценариев исполнения UDP-flood атак много, но суть атаки заключается в насыщении полосы пропускания UDP-пакетами.

Цели данной атаки заключаются в следующем: сгенерировать такое количество bps (бит в секунду), чтобы исчерпать канал связи атакуемого; сгенерировать такое количество pps (пакетов в секунду), которое оборудование не сможет обработать; нагрузить оборудование атакуемого, отправляя UDP-пакеты на разные порты, тем самым заставляя сервер обрабатывать данные пакеты.

Классификация DDoS – атак

На рис. 1 представлена схема классификации DDoS-атак. Рассмотрим подробнее предложенную классификацию.

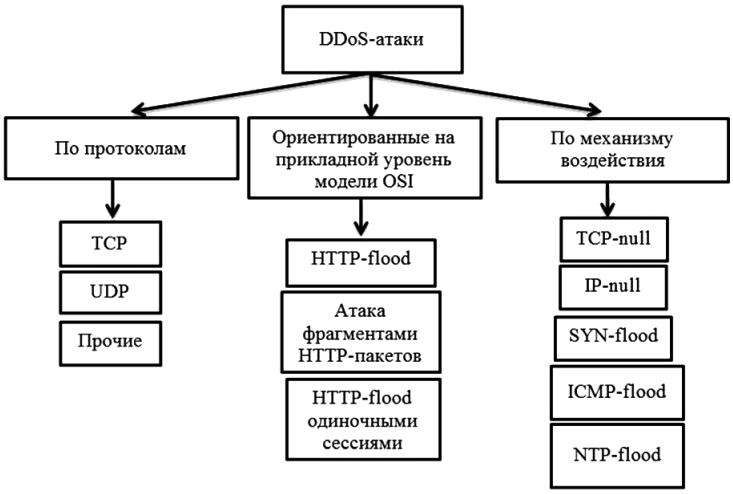

Рис. 1. Схема классификации DDoS-атак
Fig. 1. Classification of DDoS attacks

1. Классификация DDoS-атак по протоколам [9, 10]:

- UDP (User Datagram Protocol),
- TCP (Transmission Control Protocol)
- прочие атаки (атаки на протоколы ICMP, GRE, IPIP, ESP, AH, SCTP, OSPF, SWIPE, TLSP, Compaq_PEE и т.д.).

2. Классификация DDoS-атак по механизму воздействия [9, 10, 14]:

- атаки, направленные на переполнение канала связи, к данной категории относятся типы атак flood, которые эксплуатируются путем создания большого количества запросов (например, DNS-амплификация, фрагментированный UDP-flood, ICMP-flood, NTP-амплификация, NTP-flood);

- атаки, воздействующие на сетевой и транспортный уровни модели OSI, подобные атаки фальсифицируют пакеты, которыми «засоряют» ресурсы оборудования, в следствие чего возникает перегрузка ресурсов системы и отсутствие возможности обработки полезного трафика (например, SYN-flood, IP-null атака, атака с поддельными TCP-сессиями, TCP-null атака, атаки с модификациями поля TOS и др.);

3. Классификация DDoS-атак, ориентированных на прикладной уровень модели OSI [9, 10]:

- атаки, воздействующие на прикладной уровень модели OSI, к данной категории относятся типы атак, которые эксплуатируют уязвимости программного обеспечения и приводят к сбою в системе (например, HTTP-flood атака с целью отказа приложения, HTTP-flood атака одиночными запросами, атака фрагментированными HTTP-пакетами, HTTP-flood одиночными сессиями и др.);

Методы защиты от DDoS-атак

1. DDoS-защищенный хостинг

Одним из методов защиты от DDoS-атак является DDoS-защищенный хостинг. Основной недостаток этого метода заключается в том, что он неэффективно отражает DDoS-атаки, использующие недостаток ресурсов и атаки на уровне приложения. Более эффективными в борьбе с такого рода атаками является усиленная идентификация пользователей web-ресурса.

2. Защита от DDoS с помощью IPTables

Суть метода заключается в определении и блокировании атакующих IP-адресов, например, всех адресов с превышением лимита UDP-запросов в секунду. Лимит может варьироваться и быть, при необходимости, изменен. Как правило, все блокируемые IP-адреса добавляются в «черный список», на основании которого строится цепочка правил IPTables.

Однако, данный метод имеет существенный недостаток: в конечном итоге блокирование подозрительных IP-адресов также заблокирует и весь входящий трафик от них, включая клиентов и других легитимных посетителей. Поскольку в настоящее время существует проблема исчерпания адресного пространства IP, тысячи людей могут использовать любой конкретный IP-адрес в текущий момент времени, и среди них могут быть как легитимные пользователи, так и нелегитимные.

3. Защита от DDoS с помощью Интернет-провайдера

Как правило, Интернет-провайдеры обеспечивают защиту только на сетевом уровне, поэтому такую защиту нельзя назвать полноценной.

По данным компании Imperva Incapsula [18], с начала 2015 года до начала 2016 года количество DDoS атак на клиентов сервиса выросло на 94% на прикладном уровне и на 141% на сетевом. Стоит отметить, что любая on-premise система защиты становится бесполезна, когда огромный объем входящего трафика превышает производительность активного оборудования Интернет-провайдера или полностью заполняет полосу пропускания канала связи.

Несомненно, можно запросить увеличение пропускной способности, но часто ресурсы провайдера ограничены, либо это вовсе невозможно из-за ограничений, накладываемых физическим каналом связи. Более того, когда один клиент Интернет-провайдера находится под DDoS атакой из-за перегрузки канала и сбоев оборудования могут пострадать и другие клиенты.

4. Защита от DDoS с помощью конфигурирования web-сервера

Метод защиты путем предварительной настройки параметров или плагинов web - сервера. Метод эффективен в борьбе с некоторыми атаками прикладного уровня, но против распределенных атак или атак на сетевом уровне он малоэффективен.

UDP-flood атака: характеристика и реализация

UDP-flood – сетевая атака типа «отказ в обслуживании», в которой используется безсессионный режим протокола UDP. Заключается в отправке большого числа UDP-пакетов на определённые или случайные номера портов удаленного хоста, который для каждого получен-

ного пакета должен определить соответствующее приложение, убедиться в отсутствии его активности и отправить ответное ICMP-сообщение «адресат недоступен».

Механизм UDP-flood атак заключается в следующем. Атакующий хост запускает DDoS-атаку, выполняя команду атаки, имеющую адрес «жертвы», продолжительность атаки, методы атаки и другие параметры для управляющих программ (программы для реализации DDoS-атак), которые служат обработчиками атак.

Управляющие программы передают команду шпионам, которые являются скомпрометированными системами (могут быть «взломанными системами»). Шпионы – это «зомби», используемые для атаки на «жертву». Получив команду атаки от управляющих программ, скомпрометированные системы начинают рассылку UDP-пакетов «жертве» с поддельным IP-адресом в качестве источника. «Жертва» при получении данных пакетов отправляет подтверждение на IP-адрес источника, но не получает никакого ответа и продолжает его ждать. После использования всех ресурсов системы «жертвы» происходит сбой или отключение системы. Шпионов может быть несколько и все они управляемы программами для реализации DDoS-атак, что приводит к отправке большого количества UDP пакетов в систему «жертвы». Система заполняется запросами вследствие использования всей полосы пропускания.

Защита от подобного рода атак осуществляется следующим образом: закрытием неиспользуемых портов; блокированием UDP-трафика на TCP-порты; использованием систем защиты от DDoS атак; настройкой фильтров на оборудовании оператора связи на случай атаки. Для организации атак используются такие программы, как LOIC и UDP Unicorn [19]. Обобщённая схема реализации UDP-flood атаки представлена на рис. 2.

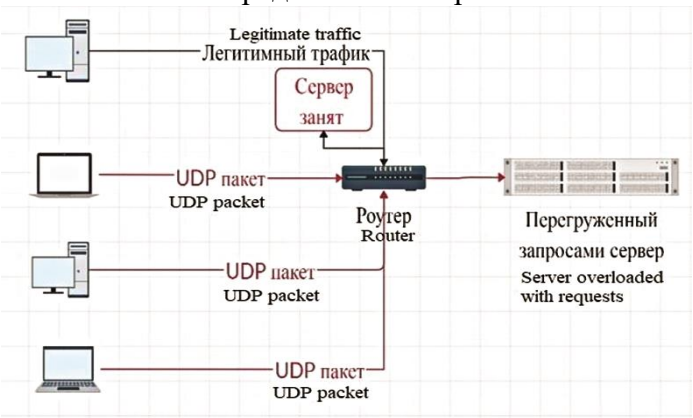

Рис. 2. Схема реализации UDP-flood атак
Fig. 2. Implementing of UDP-flood attacks

В настоящее время существует множество моделей прогнозирования временных рядов: регрессионные и авторегрессионные, нейросетевые, модели экспоненциального сглаживания, модели на базе цепей Маркова, нечеткие и др., условно которые делятся на группы:

- первая группа моделей предполагает зависимость между прогнозными и реальными значениями временного ряда, которая задана аналитически (регрессионные, авто регрессионные модели, а также модели экспоненциального сглаживания);

- вторая группа моделей предполагает зависимость между прогнозными и реальными значениями временного ряда, которая задана структурно (нейронные сети, цепи Маркова, деревья решений и др.) [34].

Достоинствами 1 группы моделей являются: простая, гибкая для пользователя в процессе моделирования, формализованная при анализе и проектировании, обладает широким применением. Недостатками 1 группы моделей являются: наличие трудностей при выявлении зависимостей в анализируемых данных, сложность при анализе и моделировании нелинейных зависимостей, высокая трудоёмкость построения модели, не высокая адаптивность к анализируемым данным, прикладной характер.

Достоинствами 2 группы моделей являются: нелинейность, масштабируемость, адаптивность, четко формализованная при анализе и проектировании, обладает большим количеством

применений, простота при моделировании, позволяют учитывать качественные признаки. Недостатками 2 группы моделей являются: неоднозначность использования алгоритма при построении дерева решений, требуют большого количества ресурсов при обучении, неоднозначность использования алгоритма обучения, высокие требования к качеству данных для обучения, трудности при выборе архитектуры нейронной сети [35, 36].

Анализ показал, что ни одна из указанных групп моделей не обладает существенными достоинствами относительно других моделей. Поэтому для решения задач анализа и прогнозирования выбраны модели 1 и 2 группы – модель экспоненциального сглаживания и нейросетевая модель.

Методы исследования. 1. Корреляционный анализ UDP-flood атак

1.1 Анализ временных рядов UDP-flood атак и DDoS-атак длительностью до 4 часов. Для повышения уровня защищенности web-ресурсов, методами корреляционного анализа спрогнозируем воздействия кибератак типа UDP-flood на web-ресурсы учетом факторов сезонности и длительности по времени, который позволит обеспечить необходимый уровень безопасности web-ресурсов. В качестве объекта исследования был выбран тип атак UDP-flood из семейства DDoS атак. Статистические данные [20−31] о количестве UDP-flood атак и DDoS-атак длительностью до 20 минут представлены в табл. 1.

Таблица 1. Данные о количестве UDP-flood атак и DDoS-атак длительностью до 4 часов
Table 1. The number of UDP-flood attacks and DDoS attacks lasting up to 4 hours

Год Year	Квартал Quarter	UDP-flood атаки, % UDP-flood attacks,%	DDoS-атаки длительностью до 4 часов, % DDOS attacks lasting up to 4 hours,%
2017	I	8,71	82,21
	II	11,91	85,93
	III	10,15	76,09
	IV	15,24	76,76
2018	I	13,2	80,73
	II	10,6	69,49
	III	11,9	86,94
	IV	31,1	83,34
2019	I	8,9	78,66
	II	10,94	82,69
	III	9,4	84,69
	IV	8,73	81,86

Выполним анализ временного ряда DDoS-атак типа UDP-flood [9, 10], где в качестве исходных параметров выберем данные таблицы 1, $n = 12$ – общее число периодов в исследовании. Динамика автокорреляции для временного ряда UDP-flood атак представлена на гистограмме (рис. 3).

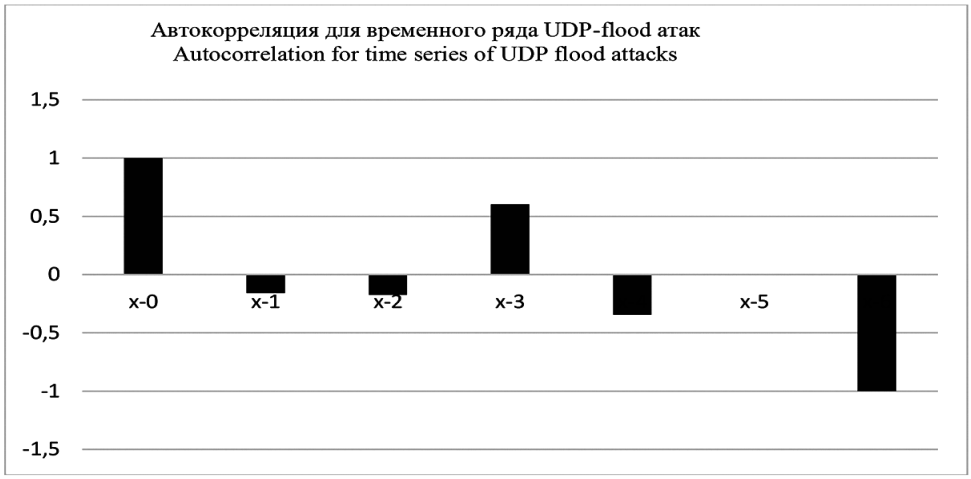

Рис. 3. Динамика автокорреляции для временного ряда UDP-flood атак с учетом лага
Fig. 3. Autocorrelation dynamics for the time series of UDP-flood attacks taking into account the lag

Гистограмма демонстрирует, что тренд отсутствует, корреляция между исходным рядом и сдвинутым на 4 позиций заметная – 0,829, что говорит о сезонности, период которой равен 5 кварталам. Данные расчетов по определению индекса сезонности (I_n) для DDoS-атак типа UDP представлен в табл. 2.

Таблица 2. Индексы сезонности для UDP-flood атак
Table 2. Seasonal indices for UDP-flood attacks

Год наблюдений Year / Квартал Quarter	**2017**	**2018**	**2019**	I_n
I	8,71	13,2	8,90	0,922
II	11,91	10,6	10,94	1,056
III	10,15	11,90	9,40	0,96
IV	15,24	31,10	8,73	1,062

На основе работ [9, 10] проанализируем временной ряд DDoS-атак длительностью до 4 часов, результаты автокорреляции приведены в таблице 3.

Таблица 3. Автокорреляция для временного ряда DDoS-атак длительностью до 4 часов
Table 3. Autocorrelation for a time series of DDoS attacks lasting up to 4 hours

Лаг Lag	Автокорреляция Autocorrelation
x-0	1
x-1	-0,158
x-2	-0,1736
x-3	0,6019
x-4	-0,3448
x-5	-0,00287
x-6	-1

1.2. Прогнозирование UDP-flood атак по методу простого экспоненциального сглаживания. Определив оптимальный коэффициент сглаживания α, значения коэффициента α разобьем в сетку с шагом 0,1 и проведем расчет средней абсолютной ошибки (M) между сглаженными прогнозными значениями (S_t) и реальными наблюдениями (Y_{t+1}) при $\alpha = \overline{0.1, \quad 0.9}$, при этом выбрав значение коэффициента, при котором ошибка минимальная. Результаты расчета ошибок представлены в табл. 4, 5.

Таблица 4. Расчет ошибок при коэффициенте сглаживания α = 0,1
Table 4. Calculation of errors with a smoothing coefficient α = 0,1

Период, t Period, t	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Количество атак, %, Y_{t+1} Number of attacks,%, Yt + 1	8,71	11,71	10,15	15,24	13,2	10,6	11,90	31,10	8,9	10,94	9,4	8,73
Прогноз,%,S_t Forecast,%, St	8,71	9,01	9,12	9,73	10,08	10,13	10,31	12,38	12,04	11,93	11,67	11,82
$\lvert Y_{t+1} - S_t \rvert$	0	2,7	1,03	6	3,12	0,47	1,59	18,72	3,14	0,99	2,27	3,09
$\lvert Y_{t+1} - S_t \rvert / Y_{t+1}$	0	0,23	0,1	0,39	0,23	0,04	0,13	0,6	0,35	0,09	0,24	0,35

Таблица 5. Динамика средней абсолютной ошибки (M) при выборе разных значений коэффициента сглаживания *α*
Table 5. Dynamics of the average absolute error (M) with different values of the smoothing coefficient *α*

Значение *α* Value *α*	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
M *(%)*	9,23	1,27	2,89	4,78	5,28	4,94	4,07	2,88	1,5

Результаты расчетов показали, что наименьшая ошибка получается при α = 0,2, таким образом, данное значение коэффициента позволит прогнозировать эффективнее по сравнению с другими значениями диапазона [0,1;0,9] с шагом 0.1.

На основе результатов работ [9, 10] рассчитаны сглаженные значения количества DDoS-атак на I, II, III, IV кварталы 2020 года и I квартал 2021 года, при α = 0,2.

$S_{13} = \alpha Y_{13} + (1-\alpha)S_{12} \approx 0{,}2 * 8{,}9 + 0{,}8 * 12{,}2241 \approx 11{,}5593$ (2020 год, I квартал) (1)

$S_{14} = \alpha Y_{14} + (1-\alpha)S_{13} \approx 0{,}2 * 12{,}06 + 0{,}8 * 11{,}5593 \approx 11{,}6593$ (2020 год, II квартал) (2)

$S_{15} = \alpha Y_{15} + (1-\alpha)S_{14} \approx 0{,}2 * 13{,}76 + 0{,}8 * 11{,}6593 \approx 12{,}0794$ (2020 год, III квартал) (3)

$S_{16} = \alpha Y_{16} + (1-\alpha)S_{15} \approx 0{,}2 * 15{,}2 + 0{,}8 * 12{,}0794 \approx 12{,}7035$ (2020 год, IV квартал) (4)

$S_{17} = \alpha Y_{17} + (1-\alpha)S_{16} \approx 0{,}2 * 7{,}3 + 0{,}8 * 12{,}7035 \approx 11{,}6228$ (2021 год, I квартал) (5)

2. Нейросетевое прогнозирование временных рядов на основе аналитической платформы Deductor. В настоящее время используются различные пакеты прикладных программ, позволяющие анализировать временные ряды (например, MS Excel, Matlab, Statistica, Deductor и др.). Для решения задачи анализа и прогнозирования в работе выбран пакет Deductor Studio Academic, так как обладает широким набором функционала для конкретной задачи (анализ данных, прогнозирование, поиск закономерностей, формирование аналитической отчетности). Для анализа временных рядов и построения прогноза были выбраны квартальные статистические данные о количестве UDP-flood атак длительностью до 4 часов за период 2017 - 2019 гг. Исходные данные были импортированы в Deductor Studio Academic (рис. 4).

Количество атак, %	Квартал
8,71	1 (2017)
11,91	2 (2017)
10,15	3 (2017)
15,24	4 (2017)
13,2	1 (2018)
10,6	2 (2018)
11,9	3 (2018)
31,1	4 (2018)
8,9	1 (2019)
10,94	2 (2019)
9,4	3 (2019)
8,73	4 (2019)

Рис. 4. Импортированные в Deductor Studio Academic статистические данные о количестве UDP-flood атак за 2017-2019 гг.
Fig. 4. Statistics on the number of UDP-flood attacks for 2017-2019 imported into the Deductor Studio Academic

Следующим этапом было устранение содержащихся в данных аномальных отклонений и шумов путем применения спектрального Фурье-преобразования [32].

Далее следовал этап трансформации, на котором решалась задача представления данных в таком виде, чтобы они могли быть обработаны наиболее эффективно. На данном этапе использовался метод скользящего окна [33], трансформированные данные представлены на (рис.5).

Количество атак, %-4	Количество атак, %-3	Количество атак, %-2	Количество атак, %-1	Количество атак, %	Квартал
8,71	11,91	10,15	15,24	13,2	1 (2018)
11,91	10,15	15,24	13,2	10,6	2 (2018)
10,15	15,24	13,2	10,6	11,9	3 (2018)
15,24	13,2	10,6	11,9	31,1	4 (2018)
13,2	10,6	11,9	31,1	8,9	1 (2019)
10,6	11,9	31,1	8,9	10,94	2 (2019)
11,9	31,1	8,9	10,94	9,4	3 (2019)
31,1	8,9	10,94	9,4	8,73	4 (2019)

Рис.5. Трансформированные данные по методу скользящего окна
Fig. 5. Transformed data using the sliding window method

Процесс создания нейронной сети в пакете Deductor Studio Academic:

1. Вызов меню «Мастера обработки» и выбор метода «Нейросеть»;
2. В мастере «Нейросеть» выбор входных и выходных переменных и указание типов данных;
3. Разбиение исходного множества данных: обучающее и тестовое;
4. Структуризация нейронной сети: указание количества слоев, числа нейронов в скрытых слоях и крутизны функции активации;
5. Настройка параметров обучения нейронной сети: выбор алгоритмов обучения и параметры;
6. Обучение нейронной сети с заданными параметрами.

Визуализация проекта в Deductor Studio Academic для построения нейросетевых моделей представлена на рис. 6.

После преобразования данных по методу скользящего окна, экспериментальным путем выбраны следующие параметры трансформации: глубина погружения – 4, горизонт прогнозирования – 5. Глубина погружения – количество кварталов в прошлом, горизонт прогнозирования в данном случае представляет количество кварталов для прогнозирования. В результате трансформации данных получены обучающие нейросетевые модели. Для оценки построенных моделей представим данные в виде диаграммы рассеяния, которая более наглядно отображает качество обучения нейронной сети.

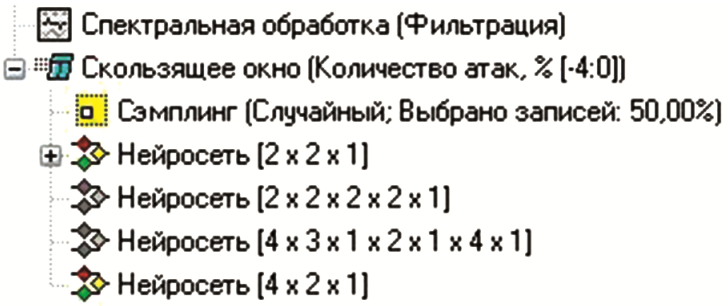

Рис.6. Визуализация проекта в Deductor Studio для построения нейросетевых моделей
Fig. 6. Visualization of the project in Deductor Studio for building neural network models

Она отображает отклонение прогнозной величины от истинного значения: большое отклонение говорит о необходимости увеличения обучающей выборки, точное совпадение прогнозных значений с эталонными, говорит о переобучении модели, т.е. модель использовала все примеры при обучении. Пример диаграммы рассеяния для оценки аппроксимирующей способности построенной нейросетевой модели представлен на (рис.7).

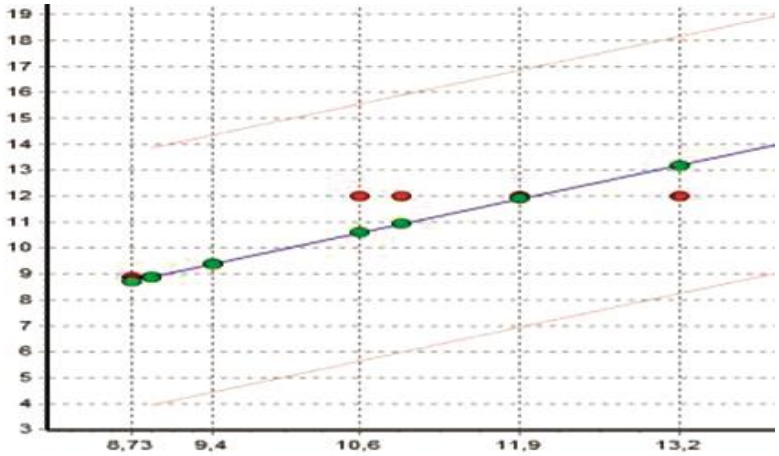

Рис.7. Диаграмма рассеяния для оценки аппроксимирующей способности построенной нейросетевой модели
Fig. 7. Scatter chart for evaluation approximating ability of the constructed neural network model

Анализ показал, что модель хорошо аппроксимирует тестовые данные. Приведенным способом проведена оценка аппроксимирующей способности всех построенных нейросетевых моделей на одних и тех же тестовых данных. Среди всех моделей наибольшая точность наблюдалась у модели с 2 нейронами в скрытом слое. В связи с этим имеется возможность эффективного практического использования данной модели для анализа и прогнозирования временного ряда.

Обсуждение результатов. Используя методы корреляционного анализа рассчитаны индекс сезонности UDP-flood атак, автокорреляцию временных рядов атак этого типа. Используя простой метод экспоненциального сглаживания построен прогноз UDP-flood атак. Результаты исследования показали, что UDP-flood атакам свойственна сезонность, количество UDP-flood атак составит 11,66%, 12,08%, 12,7% на II, III, IV кварталы 2020 года и 11,62% на I квартал 2021 года соответственно.

Рассчитанные прогнозные значения DP-flood атак на 2020 – начало 2021 года представлены на рис. 8.

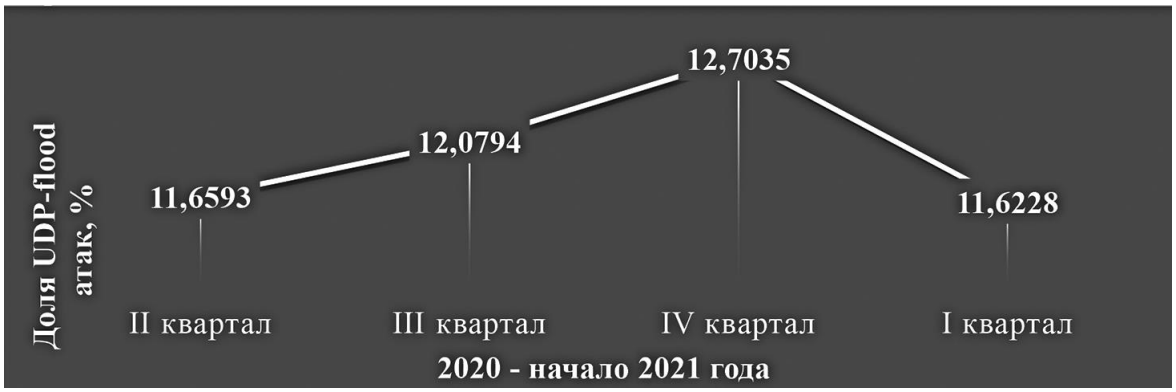

Рис. 8. Прогноз величины UDP-flood атак в 2020 – начале 2021 года
Fig. 8. The forecast of UDP-floud attacks in 2020 - early 2021

На базе аналитической платформы Deductor Studio построен прогноз на основе модели с 2 нейронами в скрытом слое (рис.9).

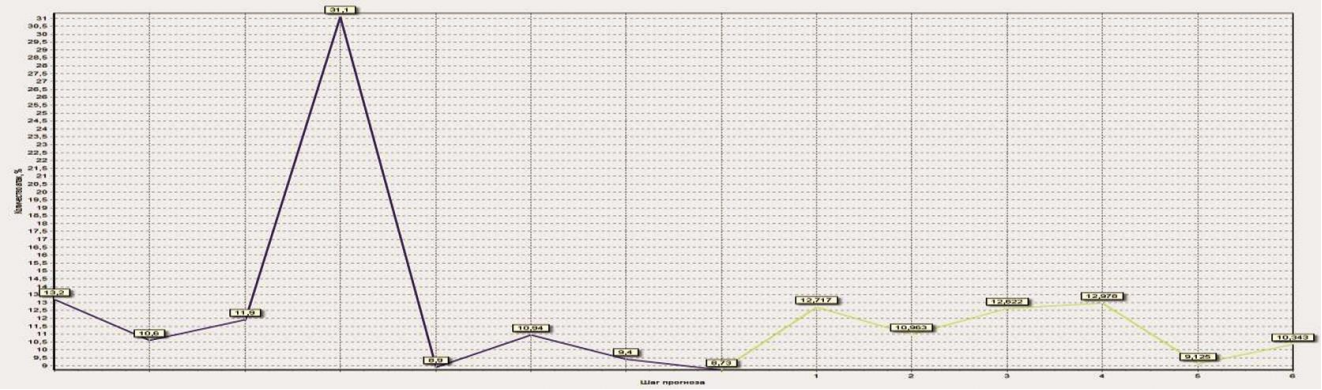

Рис. 9. Прогноз на основе модели с 2 нейронами в скрытом слое
Fig. 9. Prediction based on a model with 2 neurons in a hidden layer

Далее, сравним рассчитанные прогнозные значения, представленные в табл. 6.

Таблица 6. Сравнение прогнозных значений рассмотренных методов
Table 6. Comparison of the predicted values of the considered methods

Прогнозные значения UDP-flood атак Predicted UDP flood attacks		
Квартал / год Quarter / year	Метод корреляционного анализа временных рядов Time series correlation analysis method	Метод нейросети Neural network method
II / 2020	11,659	10,963
III / 2020	12,079	12,622
IV / 2020	12,704	12,978
I / 2021	11,623	9,125

Сравнительная характеристика рассчитанных прогнозных значений методами корреляционного анализа и нейронных сетей представлена на графике (рис. 10).

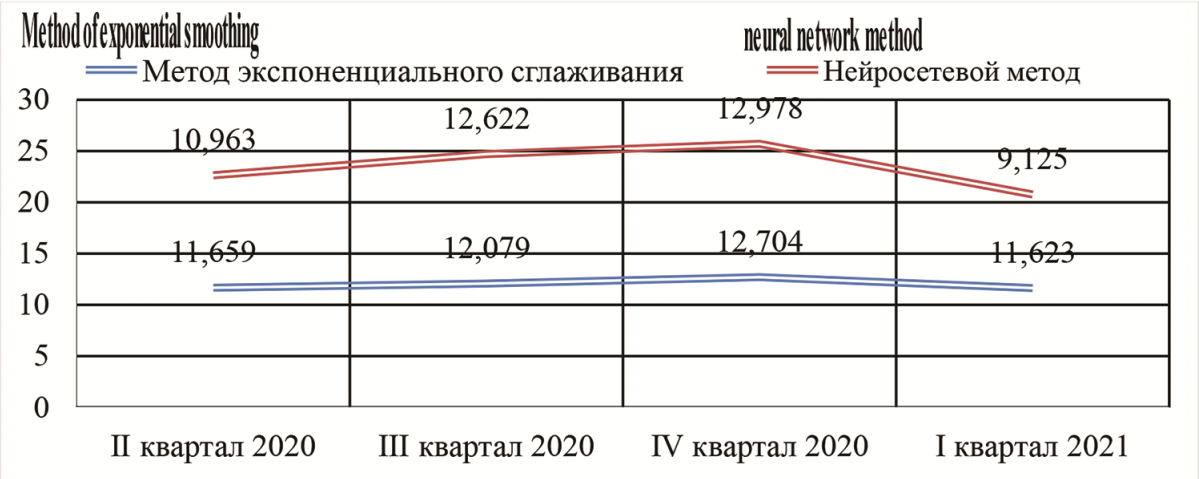

Рис. 10. График сравнения прогнозных значений, полученных методом экспоненциального сглаживания и нейросетевым методом
Fig. 10. Graph for comparing the predicted values obtained by the exponential smoothing method and the neural network method

Анализ показал, что полученные прогнозные значения методом экспоненциального сглаживания и нейросетевым методом существенно не отличаются. В среднем отклонение значений не превышает 1%, следовательно, можно считать оба метода эффективными для анализа и прогнозирования UDP-flood атак, однако для долгосрочного и более точного прогноза необходим большой объем исходной выборки.

В среднем, количество UDP-flood атак составит 11%, 12%, 13% на II, III, IV кварталы 2020 года и 10 на I квартал 2021 года соответственно.

Вывод. В работе предложена классификация DDoS-атак, описаны способы защиты. Представлен сравнительный анализ моделей прогнозирования, выявлены преимущества и недостатки. Корреляционный анализ UDP-flood атак позволил выявить фактор – сезонность. Для DDoS-атак длительностью до 20 минут выявлена сезонность в I квартале календарного года, а значит, в I квартале 2021 года следует ожидать наибольшее количество атак данной длительности. Построен прогноз на основе модели простого экспоненциального сглаживания и нейросетевой модели. Наибольшее количество UDP-flood атак следует ожидать в IV квартала 2020 года.

В среднем отклонение значений прогнозов, на основе данных моделей, не превышает 1%, следовательно, можно считать оба метода эффективными для анализа и прогнозирования UDP-flood атак, однако для долгосрочного и более точного прогноза необходим большой объем исходной выборки. В среднем, количество UDP-flood атак составит 11%, 12%, 13% на II, III, IV кварталы 2020 года и 10% на I квартал 2021 года соответственно.

Стоит отметить, что в работе имеются ограничения - недостаточно длительный период исследования и трудность получения статистических данных в связи с тем, что IT-компании неохотно раскрывают сведения о реализации на информационные ресурсы различного рода атак. Результаты работы могут быть использованы как самостоятельно при анализе атак, так и для формирования адаптивной системы защиты информации web-ресурсов, для построения системы обеспечения информационной безопасности.

Библиографический список:

1. Харитонов В. С., Черяпкин Д. П. DDoS-атака: классификация и особенности // Постулат, 2016. № 12 (14). С. 45.
2. Фролов С. Г., Демин А. Ю. Типы DDoS-атак, методы профилактики и защиты от них // III Международная научная конференция «Информационные технологии в науке, управлении, социальной сфере и медицине». Издательство: Национальный исследовательский Томский политехнический университет (Томск), 2016. С. 76−78.
3. Cabrera J., Lewis L., Qin X., Lee W., Mehra R. Proactive intrusion detection and distributed denial of service attacks-a case study in security management // Journal of network and systems management. 2002. vol. 2. P. 225−254.
4. Raza M. A., Khan A., Raza M. A restrictive model (RM) for detection and prevention of INVITE flooding attack // 3rd IEEE International Conference on Computer, Control and Communication (IC4). September 2013, Pakistan, DOI: 10.1109/IC4.2013.6653766.
5. K. S. Sahoo, Iqbal A., Maiti P., Sahoo B. A Machine Learning Approach for Predicting DDoS Traffic in Software Defined Networks // 2018 International Conference on Information Technology (ICIT). December 2018, India, DOI: 10.1109/ICIT.2018.00049.
6. Фаткиева Р.Р. Разработка метрик для обнаружения атак на основе анализа сетевого трафика // Вестник Бурятского государственного университета, 2013. № 9. С. 81–86.
7. Лаптев В.Н., Сидельников О.В., Шарай В.А. Применение метода индуктивного прогнозирования состояний для обнаружения компьютерных атак в информационно-телекоммуникационных системах // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2011. № 72. С. 76–85.
8. Мухаматханов Р.М., Михайлов А.А., Баянов Б.И., Тумбинская М.В. Классификация DDOS-атак на основе нейросетевой модели // Прикладная информатика, 2019. Т. 14. № 1 (79). С. 96–103.
9. Бармина С.С., Таджибаева Ф.М., Тумбинская М.В. Корреляционный анализ и прогнозирование SYN-флуд атак // Прикладная информатика, 2018. Т. 13. № 4 (76). С. 93–102.
10. Тумбинская М.В. Анализ и прогнозирование сетевых атак типа SYN-flood на web-ресурсы // Информатизация образования и науки, 2018. № 4 (40). С. 61–68.
11. Тумбинская М.В., Баянов Б.И., Рахимов Р.Ж., Кормильцев Н.В., Уваров А.Д. Анализ и прогнозирование вредоносного сетевого трафика в облачных сервисах // Бизнес-информатика, 2019. Т. 13. № 1. С. 71-81.
12. Бизнес без опасности. [Электронный ресурс]. – URL: https://lukatsky.blogspot.com/ (дата обращения 06.11.2019).
13. Xu Z., Li X. Protecting hosts against attacks in IMAGO system Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513), May 2004, Canada, DOI: 10.1109/CCECE.2004.1345030.
14. Краснов К. Ф., Коринов И.П., Хороший А.А., Беленькая М. Н. Анализ атак типа «Отказ в обслуживании» при использовании протоколов ICMP, UDP, TCP // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, 2018. №2 (65). С. 116–118.
15. Netwild. UDP-flood атаки. [Электронный ресурс]. – URL:http://netwild.ru/udp-flood/ (дата обращения: 17.09.2019).
16. Ежегодный отчет Cisco по кибербезопасности за 2018 г. [Электронный ресурс]. – URL:https://www.cisco.com/c/ru_ru/about/press/press-releases/2018/03-12.html (дата обращения 05.11.2019).
17. Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization’s information security // Business Informatics, 2017. No. 1 (39). pp. 68–77.

18. Imperva раскрыла технические подробности взлома Cloud WAF [Электронный ресурс]. – URL:https://habr.com/ru/company/itsumma/blog/472708/ (дата обращения: 26.11.2019).
19. Защита от DDoS. Обзор методов. [Электронный ресурс]. – URL: https://protosecurity.ru/novosti/zaschita-ot-ddos/ (дата обращения: 17.09.2019)
20. Лаборатория Касперского. DDoS-атаки в первом квартале 2017 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-attacks-in-q1-2017/30631/ (дата обращения: 26.03.2019).
21. Лаборатория Касперского. DDoS-атаки во втором квартале 2017 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-in-q2-2018/90436/ (дата обращения: 26.03.2019).
22. Лаборатория Касперского. DDoS-атаки в третьем квартале 2017 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-in-q3-2018/92512/ (дата обращения: 26.03.2019).
23. Лаборатория Касперского. DDoS-атаки в четвертом квартале 2017 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-attacks-in-q4-2017/88505/ (дата обращения: 26.03.2019).
24. Лаборатория Касперского. DDoS-атаки в первом квартале 2018 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-in-q1-2018/89700/ (дата обращения: 26.03.2019).
25. Лаборатория Касперского. DDoS-атаки во втором квартале 2018 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-in-q2-2018/90436/ (дата обращения: 26.03.2019).
26. Лаборатория Касперского. DDoS-атаки в третьем квартале 2018 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-in-q3-2018/92512/ (дата обращения: 26.03.2019).
27. Лаборатория Касперского. DDoS-атаки в четвертом квартале 2018 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-in-q3-2018/92512/ (дата обращения: 26.03.2019).
28. Лаборатория Касперского. DDoS-атаки в первом квартале 2019 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-q1-2019/93890/ (дата обращения: 19.10.2019).
29. Лаборатория Касперского. DDoS-атаки во втором квартале 2019 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-q2-2019/94452/ (дата обращения: 04.11.2019).
30. Лаборатория Касперского. DDoS-атаки в третьем квартале 2019 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-q3-2019/94981/ (дата обращения: 05.11.2019).
31. Лаборатория Касперского. DDoS-атаки в четвертом квартале 2019 года. [Электронный ресурс]. – URL:https://securelist.ru/ddos-report-q4-2019/95568/ (дата обращения: 14.02.2020).
32. Муцалова С.Ш., Магомедбеков У.Г., Убаева Р.Ш. Фурье – преобразование временного ряда при жидкофазном окислении 1,4нафтодиола // Качество науки - качество жизни, 2010. №2. С. 66–67.
33. Клачек П.М., Полупан К.Л., Либерман И.В. Цифровизация экономики на основе системно-целевой технологии управления знаниями // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки, 2019. Т. 12. №3. С. 9–19.
34. Панченко А.Д. Обзор методов и моделей прогнозирования развития социально-экономических систем // В сборнике: Бизнес-инжиниринг сложных систем: модели, технологии, инновации сборник материалов IV международной научно-практической конференции, 2019. С. 86–89.
35. Селиверстова А.В. Сравнительный анализ моделей и методов прогнозирования // Современные научные исследования и инновации, 2016. №11(67). С. 241–248.
36. Катасёва Д.В., Катасев А.С., Кирпичников А.П., Абянов Б.Э. Нейронечеткая модель анализа и прогнозирования временных рядов // Вестник технологического университета, 2016. Т. 19. №13. С. 127-131.

References:

1. Kharitonov V. S., Cheryapkin D. P. DDoS-ataka: klassifikatsiya i osobennosti // Postulat, 2016. № 12 (14). S. 45. [Kharitonov V.S., Cheryapkin D.P. DDoS attack: classification and features. Postulat. 2016. No. 12 (14), p. 45. (In Russ.)]
2. Frolov S. G., Demin A. YU. Tipy DDoS-atak, metody profilaktiki i zashchity ot nikh // III Mezhdunarodnaya nauchnaya konferentsiya «Informatsionnyye tekhnologii v nauke, upravlenii, sotsial'noy sfere i meditsine». Izdatel'stvo: Natsional'nyy issledovatel'skiy Tomskiy politekhnicheskiy universi-tet (Tomsk), 2016. S. 76-78. [Frolov S.G., Demin A.Yu. Types of DDoS-attacks, methods of prevention and protection from them. Proc. 3rd Sci. Conf. “Information Technologies in Science, Management, Social Sphere and Medicine”, Tomsk. 2016. pp. 76−78. (In Russ.)]
3. Cabrera J., Lewis L., Qin X., Lee W., Mehra R. Proactive intrusion detection and distributed denial of service attacks-a case study in security management. Journal of network and systems management. 2002. no. 2, pp. 225−254.
4. Raza M. A., Khan A., Raza M. A restrictive model (RM) for detection and prevention of INVITE flooding attack. Proceedings of the 3rd IEEE International Conference on Computer, Control and Communication (IC4). Pakistan, September 2013. DOI: 10.1109/IC4.2013.6653766.
5. K. S. Sahoo, Iqbal A., Maiti P., Sahoo B. A Machine Learning Approach for Predicting DDoS Traffic in Software Defined Networks. Proceedings of the International Conference on Information Technology (ICIT). India, December 2018. DOI: 10.1109/ICIT.2018.00049.
6. Fatkiyeva R.R. Razrabotka metrik dlya obnaruzheniya atak na osnove analiza setevogo trafika // Vestnik Buryatskogo gosudarstvennogo universiteta, 2013. № 9. S. 81–86. [Fatkieva R.R. Development of metrics for detecting attacks based on network traffic analysis. Bulletin of the Buryat State University. 2013. no 9, pp. 81–86 (In Russ.)]
7. Laptev V.N., Sidel'nikov O.V., Sharay V.A. Primeneniye metoda induktivnogo prognozirovaniya sostoyaniy dlya obnaruzheniya komp'yuternykh atak v informatsionno-telekommunikatsionnykh sistemakh // Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta, 2011. № 72. S. 76–85. [Laptev V.N., Sidelnikov O.V., Sharay V.A. The use of the method of inductive state prediction for the detection of computer attacks in

information and telecommunication systems. Political Mathematical Network Electronic Scientific Journal of the Kuban State Agrarian University. 2011. No 72, pp. 76–85 (In Russ.)]

8. Mukhamatkhanov R.M., Mikhaylov A.A., Bayanov B.I., Tumbinskaya M.V. Klassifikatsiya DDOS-atak na osnove ney-rosetevoy modeli // Prikladnaya informatika, 2019. T. 14. № 1 (79). S. 96–103. [Mukhamathanov R.M., Mikhailov A.A., Bayanov B.I., Tumbinskaya M.V. Classification of DDOS attacks based on a neural network model. Applied Informatics. 2019. Vol. 14, No 1(79), pp. 96–103 (In Russ.)]
9. Barmina S.S., Tadzhibayeva F.M., Tumbinskaya M.V. Korrelyatsionnyy analiz i prognozirovaniye SYN-flud atak // Prikladnaya informatika, 2018. T. 13. № 4 (76). S. 93–102. [Barmina S.S., Tadjibaeva F.M., Tumbinskaya M.V. Correlation analysis and forecasting of SYN flood attacks. Applied Informatics. 2018. Vol. 1, No 4(76), pp. 93–102 (In Russ.)]
10. Tumbinskaya M.V. Analiz i prognozirovaniye setevykh atak tipa SYN-flood na web-resursy // Informatizatsiya obrazovaniya i nauki, 2018. № 4 (40). S. 61–68. [Tumbinskaya M.V. Analysis and forecasting of network attacks like SYN-flood on web-resources. Informatization of Education and Science. 2018. No. 4(40), pp. 61–68 (In Russ.)]
11. Tumbinskaya M.V., Bayanov B.I., Rakhimov R.ZH., Kormil'tsev N.V., Uvarov A.D. Analiz i prognozirovaniye vredonosnogo setevogo trafika v oblachnykh servisakh // Biznes-informatika, 2019. T. 13. № 1. S. 71-81. [Tumbinskaya M.V., Bayanov B.I., Rakhimov R.Zh., Kormiltsev N.V., Uvarov A.D. Analysis and forecasting of malicious network traffic in cloud services. Business Informatics. 2019. vol. 13, no 1, pp. 71–81 (In Russ.)]
12. Biznes bez opasnosti. [Elektronnyy resurs]. – URL: https://lukatsky.blogspot.com/ (data obrashcheniya 06.11.2019). [Business without danger. [Electronic resource]. – URL: https://lukatsky.blogspot.com/ (accessed: 06.11.2019) (In Russ.)]
13. Xu Z., Li X. Protecting hosts against attacks in IMAGO system. Proceedings of the Canadian Conference on Electrical and Computer Engineering. Canada, May 2004, DOI: 10.1109/CCECE.2004.1345030.
14. Krasnov K. F., Korinov I.P., Khoroshiy A.A., Belen'kaya M. N. Analiz atak tipa «Otkaz v obsluzhivanii» pri ispol'zovanii protokolov ICMP, UDP, TCP // Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki, 2018. №2 (65). S. 116-118. [Krasnov K. F, Korinov I. P., Khoroshiy A. A., Belenkaya M. N. Analysis of denial of service attacks using ICMP, UDP, TCP protocols. Transactions of the North Caucasian branch of the Moscow Technical University of Communications and Informatics. 2018. no 2(65), pp. 116–118 (in Russ.)]
15. Netwild. UDP-flood attack. [Electronic resource]. – URL : http://netwild.ru/udp-flood/ (accessed: 17.09.2019)
16. Cisco Annual Cybersecurity Report 2018. [Electronic resource]. – URL: https://www.cisco.com/c/ru_ru/about/press/press-releases/2018/03-12.html (accessed: 05.11.2019).
17. Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organiza-tion's information security // Business Informatics, 2017. No. 1 (39). pp. 68–77. [Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization's information security. Business Informatics. 2017. no 1(39), pp. 68–77. (In Russ.)]
18. Imperva raskryla tekhnicheskiye podrobnosti vzloma Cloud WAF [Elektronnyy resurs]. – URL:https://habr.com/ru/company/itsumma/blog/472708/ (data obrashcheniya: 26.11.2019). [Imperva revealed the technical details of hacking Cloud WAF. [Electronic resource]. – URL: https://habr.com/ru/company/itsumma/blog/472708/ (accessed: 26.11.2019) (In Russ.)]
19. Zashchita ot DDoS. Obzor metodov. [Elektronnyy resurs]. – URL: https://protosecurity.ru/novosti/zaschita-ot-ddos/ (data obrashcheniya: 17.09.2019) [DDoS protection. Method Overview. [Electronic resource]. – URL: https://protosecurity.ru/novosti/zaschita-ot-ddos/ (accessed: 17.09.2019) (in Russ.)]
20. Laboratoriya Kasperskogo. DDoS-ataki v pervom kvartale 2017 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-attacks-in-q1-2017/30631/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the first quarter of 2017. [Electronic resource]. – URL: https://securelist.ru/ddos-attacks-in-q1-2017/30631/ (accessed 26.03.2019) (in Russ.)]
21. Laboratoriya Kasperskogo. DDoS-ataki vo vtorom kvartale 2017 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-in-q2-2018/90436/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the second quarter of 2017. [Electronic resource]. – URL: https://securelist.ru/ddos-report-in-q2-2018/90436/ (accessed 26.03.2019) (in Russ.)]
22. Laboratoriya Kasperskogo. DDoS-ataki v tret'yem kvartale 2017 goda. [Elektronnyy resurs]. –URL:https://securelist.ru/ddos-report-in-q3-2018/92512/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the third quarter of 2017. [Electronic resource]. – URL: https://securelist.ru/ddos-report-in-q3-2018/92512/ (accessed 26.03.2019) (in Russ.)]
23. Laboratoriya Kasperskogo. DDoS-ataki v chetvertom kvartale 2017 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-attacks-in-q4-2017/88505/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the fourth quarter of 2017. [Electronic resource]. – URL: https://securelist.ru/ddos-attacks-in-q4-2017/88505/ (accessed 26.03.2019) (in Russ.)]
24. Laboratoriya Kasperskogo. DDoS-ataki v pervom kvartale 2018 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-in-q1-2018/89700/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the first quarter of 2018. [Electronic resource]. – URL: https://securelist.ru/ddos-report-in-q1-2018/89700/ (accessed 26.03.2019) (in Russ.)]
25. Laboratoriya Kasperskogo. DDoS-ataki vo vtorom kvartale 2018 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-in-q2-2018/90436/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the second quarter of 2018. [Electronic resource]. – URL: https://securelist.ru/ddos-report-in-q2-2018/90436/ (accessed 26.03.2019) (in Russ.)]
26. Laboratoriya Kasperskogo. DDoS-ataki v tret'yem kvartale 2018 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-in-q3-2018/92512/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the third quarter of 2018. [Electronic resource]. – URL: https://securelist.ru/ddos-report-in-q3-2018/92512/ (accessed 26.03.2019) (in Russ.)]
27. Laboratoriya Kasperskogo. DDoS-ataki v chetvertom kvartale 2018 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-in-q3-2018/92512/ (data obrashcheniya: 26.03.2019). [Kaspersky Lab. DDoS-attacks in the fourth quarter of 2018. [Electronic resource]. – URL: https://securelist.ru/ddos-attacks-in-q4-2018/93384/ (accessed 26.03.2019) (in Russ.)]

28. Laboratoriya Kasperskogo. DDoS-ataki v pervom kvartale 2019 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-q1-2019/93890/ (data obrashcheniya: 19.10.2019). [Kaspersky Lab. DDoS-attacks in the first quarter of 2019. [Electronic resource]. – URL: https://securelist.ru/ddos-report-q1-2019/93890/ (accessed 19.10.2019) (in Russ.)]
29. Laboratoriya Kasperskogo. DDoS-ataki vo vtorom kvartale 2019 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-q2-2019/94452/ (data obrashcheniya: 04.11.2019). [Kaspersky Lab. DDoS-attacks in the second quarter of 2019. [Electronic resource]. – URL: https://securelist.ru/ddos-report-q2-2019/94452/ (accessed 04.11.2019) (in Russ.)]
30. Laboratoriya Kasperskogo. DDoS-ataki v tret'yem kvartale 2019 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-q3-2019/94981/ (data obrashcheniya: 05.11.2019). [Kaspersky Lab. DDoS-attacks in the third quarter of 2019. [Electronic resource]. – URL: https://securelist.ru/ddos-report-q3-2019/94981/ (accessed 05.11.2019) (in Russ.)]
31. Laboratoriya Kasperskogo. DDoS-ataki v chetvertom kvartale 2019 goda. [Elektronnyy resurs]. – URL:https://securelist.ru/ddos-report-q4-2019/95568/ (data obrashcheniya: 14.02.2020). [Kaspersky Lab. DDoS-attacks in the fourth quarter of 2019. [Electronic resource]. – URL: https://securelist.ru/ddos-report-q4-2019/95568/ (accessed 14.02.2020) (in Russ.)]
32. Mutsalova S.SH., Magomedbekov U.G., Ubayeva R.SH. Fur'ye – preobrazovaniye vremennogo ryada pri zhidkofaznom okislenii 1,4naftodiola // Kachestvo nauki - kachestvo zhizni, 2010. №2. S. 66−67. [Mutsalova S.Sh., Magomedbekov U.G., Ubaeva R.Sh. Fourier - time series conversion during liquid phase oxidation of 1,4 naphthodiol. The quality of science is the quality of Life. 2010. No 2, pp. 66−67 (in Russ.)]
33. Klachek P.M., Polupan K.L., Liberman I.V. Tsifrovizatsiya ekonomiki na osnove sistemno-tselevoy tekhnologii upravleniya znaniyami // Nauchno-tekhnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Ekonomicheskiye nauki, 2019. T. 12. №3. S. 9−19. [Klachek P.M., Polupan K.L., Liberman I.V. Digitaliztaion of economy based on systemic target technology of knowledge management. St. Petersburg State Polytechnical University Journal. Economics. 2019. vol. 12, No. 3, pp. 9-19 (in Russ.)]
34. Panchenko A.D. Obzor metodov i modeley prognozirovaniya razvitiya sotsial'no-ekonomicheskikh sistem // V sbornike: Biznes-inzhiniring slozhnykh sistem: modeli, tekhnologii, innovatsii sbornik materialov IV mezhdunarodnoy nauchno-prakticheskoy konferentsii, 2019. S. 86−89. [Panchenko A.D. Review of methods and models for forecasting the development of socio-economic systems. In the collection: Business engineering of complex systems: models, technologies, innovations, collection of materials of the IV international scientific and practical conference. 2019. pp. 86−89 (in Russ.)]
35. Seliverstova A.V. Sravnitel'nyy analiz modeley i metodov prognozirovaniya // Sovremennyye nauchnyye issledovaniya i innovatsii, 2016. №11(67). S. 241−248. [Seliverstova A.V. Comparative analysis of models and forecasting methods. Modern scientific research and innovation. 2016. vol. 11, no 67, pp.241−248 (in Russ.)]
36. Katasova D.V., Katasev A.S., Kirpichnikov A.P., Abyanov B.E. Neyronechetkaya model' analiza i prognozirovaniya vremennykh ryadov // Vestnik tekhnologicheskogo universiteta, 2016. T. 19. №13. S. 127-131. [Kataseva D.V., Katasev A.S., Kirpichnikov A.P., Abyanov B.E. Neuro-fuzzy model of analysis and forecasting of time series. Bulletin of the Technological University. 2016. Vol. 19, No 13. pp. 127-131 (in Russ.)]

Сведения об авторах:

Тумбинская Марина Владимировна, кандидат технических наук, доцент, кафедра систем информационно-безопасности; e-mail: tumbinskaya@inbox.ru

Волков Василий Витальевич, студент, кафедра систем информационной безопасности; e-mail: waskis298@gmail.com

Загидуллин Булат Гаптельнурович, студент, кафедра систем информационной безопасности; e-mail: zagidullinbg@gmail.com

Information about the authors:

Marina V. Tumbinskaya, Cand. Sci. (Technical.), Assoc. Prof., Department of Information Protection Systems; e-mail: tumbinskaya@inbox.ru

Vasily V. Volkov, Student, Department of Information Protection Systems; e-mail: waskis298@gmail.com

Bulat G. Zagidullin**,** Student, Department of Information Protection Systems; e-mail: zagidullinbg@gmail.com

Конфликт интересов.
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 19.05.2020.
Принята в печать 22.06.2020.

Conflict of interest.
The authors declare no conflict of interest.
Received 19.05.2020.
Accepted for publication 22. 06.2020.