УДК 519.687

ИССЛЕДОВАНИЕ МОДЕЛИ НЕЙРОННОЙ СЕТИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КАЧЕСТВА ОБСЛУЖИВАНИЯ МУЛЬТИОБЛАЧНОЙ ПЛАТФОРМЫ

Болодурина Ирина Павловна
Д.т.н., профессор, заведующий кафедрой, e-mail: prmat@mail.osu.ru
Парфёнов Денис Игоревич
К.т.н., начальник отдела, e-mail: fdot_it@mail.osu.ru
Федеральное государственное бюджетное образовательное учреждение высшего образования "Оренбургский государственный университет",
460018 г. Оренбург, пр. Победы 13

Аннотация. В настоящей работе построен и исследован прототип автономной системы для обеспечения кибербезопасности и качества обслуживания мультиоблачных платформ. В основу разработанной системы положена математическая модель анализа трафика. Математическая модель построена на базе нейронной сети. Предложена гибридная архитектура нейронной сети на основе многослойного персептрона и самоорганизующейся сети Кохонена. Такой подход позволил более точно классифицировать и обнаруживать вредоносный трафик. Проведенные экспериментальные исследования показали, что использование предлагаемого решения позволяет повысить эффективность обнаружения таких атак как отказ в обслуживании, а также во время атаки обеспечить требуемое качество обслуживания.

Ключевые слова: облачные вычисления, виртуальные центры обработки данных, программно-управляемые архитектура, нейронная сеть, кибербезопасность, качество обслуживания/

Цитирование: Болодурина И.П., Парфёнов Д.И. Исследование модели нейронной сети для обеспечения безопасности и качества обслуживания мультиоблачной платформы // Информационные и математические технологии в науке и управлении. 2018. № 3 (11). С. 18–26. DOI:10.25729/2413-0133-2018-3-02

Введение. Сегодня проблема кибербезопасности является достаточно актуальной. Это в первую очередь связано с растущим влиянием локальных и глобальных сетей передачи данных на развитие современных услуг и технологий. Одной из проблем современных сетей является ежегодный рост конвергентного трафика. Согласно аналитическим данным ведущих поставщиков сетевого оборудования, таких, как Cisco и Huawei, объем трафика ежегодно увеличивается на 20-35%. Рост трафика связан в основном с кибер-атаками на корпоративные облачные сервисы и приложения [2]. Оценивая вектор атак на инфраструктуру, которая поддерживает работу информационных систем в крупных компаниях, можно сделать вывод, что основной целью атак является ограничение доступа легитимных пользователей к ключевым ресурсам (35%), нарушение работы технологического оборудования (35%), уничтожение или кража конфиденциальных данных

(23%). При этом основную массу составляют кибер-атаки типа отказ в обслуживании (DDoS) [7].

Корпоративные пользователи предпочитают брать в аренду средства, обеспечивающие кибербезопасность. Для этого корпоративные информационные ресурсы размещают в центрах обработки данных. Вычислительные мощности в одном центре обработки данных обычно арендуют сразу несколько компаний. Основная задача операторов центра обработки данных (ЦОД) - удовлетворить потребности корпоративных пользователей для обеспечения защиты арендованной инфраструктуры от внешних воздействий, а также обеспечить качество обслуживания (QoS) в соответствии с соглашением об уровне обслуживания (SLA). Однако, учитывая объем данных, поступающих в центр обработки данных и количество пользователей, работающих одновременно с одним и тем же оборудованием, существует риск ошибок в конфигурации сетевого оборудования. Это может привести к негативным последствиям как для центра обработки данных оператора, так и для корпоративных клиентов. Поэтому операторы центров обработки данных предпочитают изолировать инфраструктуру корпоративных пользователей с использованием мультиоблачных платформ. В рамках настоящего исследования нами подготовлен ряд решений, которые отвечают за фильтрацию и поиск вредоносных потоков трафика в корпоративной инфраструктуре, развернутой с использование программно-управляемой инфраструктуры.

Обзор существующих решений. Сегодня существует множество подходов к обеспечению безопасности приложений и сервисов, включая использование технологий для программных сетей (SDN) и мультиоблачных платформ.

Отечественными исследователями в области кибербезопасности разработан прототип системы обнаружения вторжений для сети SDN [4]. Прототип состоит из модуля сбора и обработки статистики, а также модуля принятия решений. Исследования проводились с использованием среды моделирования Mininet для оценки работы модулей. Предлагаемый алгоритм решения, основанный на нечеткой логике, показал лучшие результаты, чем алгоритмы безопасности, используемые отдельно.

Alshamrani и его коллеги из Аризонского государственного университета провели исследование ограничений существующих механизмов обнаружения атак. В рамках исследования ими предложена система безопасности, которая периодически собирает сетевую статистику из элементов распределения и применяет алгоритмы для классификации машинного обучения. Таким образом архитектура сети становится самоорганизующейся и интеллектуальной, реагируя на сетевые изменения, которые помогают обнаруживать различные типы атак [1].

Исследователи под руководством Jankowski D. предлагают свою концепцию применения программных сетей и методов машинного обучения для мониторинга и обнаружения вредоносных действий в сети. В исследовании представлена виртуальная среда, способная генерировать в программно-конфигурируеймой сети различные виды вредоносного трафика. Иерархическое изучение векторного квантования (HLVQ) показало лучшие результаты по сравнению с другими алгоритмами классификации [5].

Ученые из Италии предложили механизм обнаружения атак бот-сетей, основанный на искусственном классификаторе нейронных сетей, обученных доступным наборам данных в

обычных сетях. Экспериментальные результаты показывают точность обнаружения ботнета выше 99% по сравнению с существующими механизмами обнаружения таких атак [6].

Борисенко К. в своей диссертационной работе предложил новый метод обнаружения сетевых атак с учетом динамических изменений структуры и объема легитимного трафика, который позволяет обнаруживать вредоносные действия в виртуальной сети с меньшим количеством ошибок первого и второго рода [3].

Еще одним подходом для борьбы с DoS-атаками является распределенный брандмауэр с системой обнаружения вторжений для настраиваемых пользователем облаков. Предлагаемый механизм распределенной безопасности рассматривается для двух типов DoS-атак, ICMP-атак и SYN-атак в различных сетевых сценариях [8].

Wang S. и др. разработали алгоритм SECO (SDN sEcure COntroller) для улучшения функций безопасности сети SDN в случае DoS-атак. Результаты моделирования показывают, что атаки DoS могут ухудшить производительность контроллера, и предлагаемый алгоритм может значительно снизить влияние таких атак [9].

Существенным недостатком всех рассмотренных решений является экспоненциальный рост стоимости вычислительных ресурсов во время атаки на корпоративные сервисы. Кроме того, во время атак типа отказ в обслуживании существует значительное нарушение политики QoS. Это в первую очередь связано с механизмом защиты. Поставщики услуг, которые готовят защиту от этого типа атаки, направляют весь трафик в свою собственную сеть. Эта сеть используется в качестве фильтра для идентификации легитимного трафика, но это увеличивает время отклика приложений и сервисов.

Таким образом, обзор исследований по данной теме показывает, что в настоящее время используются различные подходы к обнаружению сетевых атак, но на практике эти подходы не всегда неэффективны. По этой причине мы предложили решение, которое устранит перечисленные недостатки и повысит эффективность защиты корпоративной сети, а так же позволит обеспечить требуемое качество обслуживания.

Реализационная часть. В рамках наших исследований предложен подход, основанный на использовании группы компонентов, которые являются основой для виртуального центра обработки данных. Разработанное решение построено с использованием гибридного синтеза двух прорывных технологий: программно-конфигурируемых сетей (SDN) и виртуализации сетевых функций (VNF). Первый компонент (SDN) позволяет изолировать и реализовать эффективное управление потоком трафика на основе методов и динамических алгоритмов маршрутизации [5, 9]. Второй компонент (VNF) позволяет осуществлять комплекс мероприятий, направленных на мониторинг и своевременное обновление протоколов и средств обеспечения кибербезопасности на всех устройствах (объектах), задействованных в работе мультиоблачной платформы.

Разработанный прототип представляет собой модульное и масштабируемое решение, которое позволяет интегрировать его в состав любой системы управления облачными вычислениями. Прототип включает в себя следующую серию программных компонентов:

1) модуль для глубокого анализа данных, который собирает информацию, необходимую для принятия решений о фильтрации трафика на сетевых и вычислительных узлах мультиоблачной платформы;

2) модуль контроллера сетевой безопасности, который на основе алгоритма брандмауэра управляет правилами доступа к ресурсам в сетевой среде с мультиоблачными платформами;

3) модуль обеспечения качества в своей работе использует алгоритм самоорганизации для управления адаптивной маршрутизацией сетевого трафика в программно настраиваемой сети для управления потоками данных приложений и сервисов на мультиоблачной платформе;

4) модуль управления мультиоблачной платформой осуществляет размещение приложения и службы в сетевой среде с мультиоблачными платформами.

Разработанные модули адаптированы для работы контейнеров на основе Docker, что позволяет им быстро развертываться в сетевой среде с несколькими облачными платформами. Архитектура предлагаемого решения показана на рисунке 1.

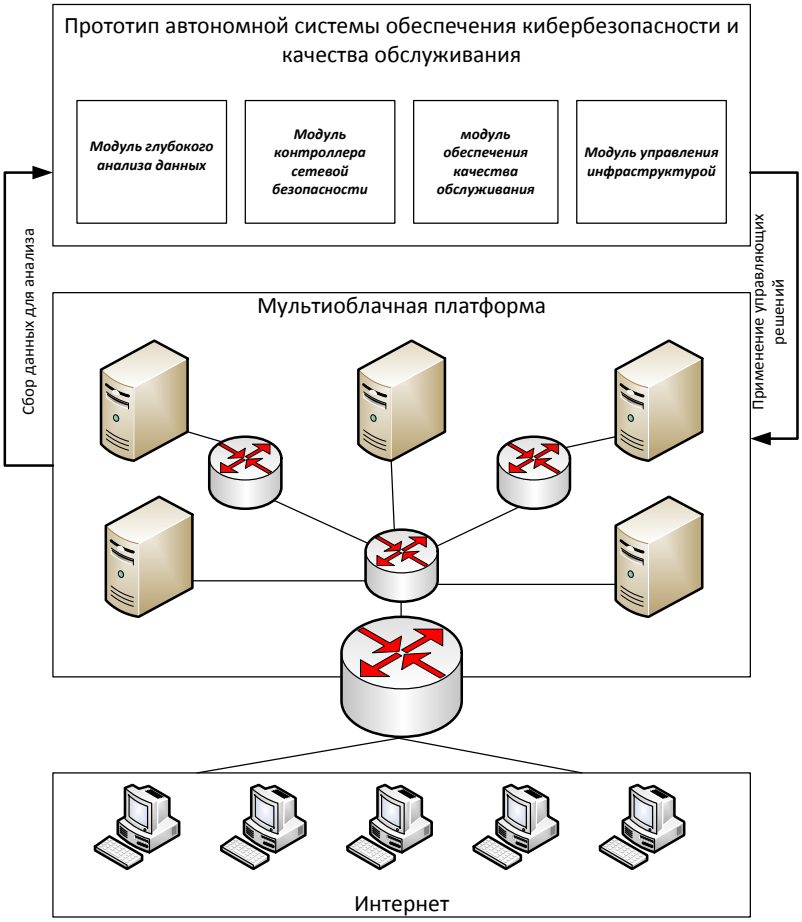

Рис. 1. Архитектура прототипа автономной системы обеспечения кибербезопасности и качества обслуживания программно-управляемой инфраструктуры мультиоблачной платформы

Чтобы повысить качество услуг и безопасность мультиоблачных платформ, подробно опишем основной объект, который должен дать представление об архитектуре сети виртуального центра обработки данных. Сеть виртуального центра обработки данных можно описать как граф

$$VDCnetwork = (V, e, u, FE), \quad (1)$$

где V – вершины графа (узлы сети), e – дуги графа (сетевые подключения), $FE : E(G) \to R^+$ - поток запросов в сети SDN; $u : E(G) \to R^+$ - стоимость реализации сетевого подключения в сети SDN.

Для поддержания требуемого качества обслуживания (QoS) и заданного уровня бесперебойной работы запишем уравнения баланса:

$$ex_f(u,v) := \sum_{e \in \delta^-(U,V)} FE(e) - \sum_{e \in \delta^+(U,V)} FE(e), \forall e = (u,v) \in E(G) \quad (2)$$

Представленное описание необходимо для перехода к моделированию на уровне потоков передаваемых и проанализированных данных. Каждая запись потока $FE_{kij} = FE_{ki}(t)$ является динамической и изменяется в моменты времени t. Каждый поток имеет набор характеристик, которые однозначно идентифицируют его. В системе управления трафиком поток может быть представлен в виде:

$$FE_{kij} = (Match_{kij}, Act_{kij}, TO_{kij}, FE_{kij}, CNT_{kij}(t)), \quad (3)$$

где $Match_{kij}$ - это набор полей для проверки совпадений с заголовками пакета; Act_{kij} - набор действий, выполняемых на пакете, если его заголовки соответствуют $Match_{kij}$; TO_{kij} - время фиксации потока в системе; FE_{kij} - поток, к которому применяется это правило OpenFlow; CNT - статистические счетчики OpenFlow.

В этом случае для более эффективного анализа трафика, как правило, в сетях используется алгоритм поиска профиля трафика. В рамках исследования разработанный подход дополняется методами интеллектуального анализа данных, которые позволяют снизить набор характеристик, что значительно ускоряет обработку информации. Это важно при анализе больших потоков данных, которые происходят в сетях виртуальных центров обработки данных из-за многочисленных пересечений каналов связи. Схема анализа потока в точке подключения к сети на узле центра обработки данных может быть формализована следующим образом:

$$Analyzer_{ki} = (Node_{ki}, CurFlows_{ki}(t), SuspFlows_{ki}(t)), \quad (4)$$

где $Node_{ki}$ - сетевой узел, на котором работает анализатор трафика, $CurFlows_{ki}$ (t) = {CurrentFlowskij} и $SuspFlows_{ki}$ (t) = {$SuspFlow_{kij}$} - соответственно, набор токов и набор подозрительных потоков, обнаруженных анализатором в момент времени t.

Для представленной модели правила брандмауэра были разработаны отдельно для уровней L2 и L3-L4 модели OSI. Все правила имеют две части - заголовки, которые идентифицируют пакеты, и действие. Заголовки для правил уровня L2 включают в себя исходный порт пакета, переключатель источника, MAC-адреса отправителя и получателя пакета, тип протокола и т.д. Заголовки правил уровня L3-L4 содержат IP-адрес адреса и порты источника и адресата пакета, тип инкапсулированного протокола и т. д. Возможные действия - удаление или разрешение пакета.

При необходимости такие правила могут быть объединены в цепочки. Каждая цепочка представляет собой упорядоченный список правил с идентификатором. Вся цепочка правил проверяется в порядке приоритета до тех пор, пока не будет правила, подходящего для проанализированного пакета. В этом случае выполняется действие, указанное в этом правиле, и последующее выполнение цепочки завершается. Чтобы передать правило в другую цепочку, можно указать соответствующее действие с его идентификатором.

Чтобы найти потоки аномального трафика, предлагается использовать гибридную нейронную сеть, состоящую из самоорганизующейся карты Кохонена (SOM) и многослойного персептрона.

Применяя карту Кохонена, кластеризация сетевых событий происходит в узлах матрицы, в которых будут группироваться события. Фактически, отдельные узлы будут представлять собой определенные сценарии атаки. Входной вектор для SOM содержит следующие компоненты: x1 - IP-адрес назначения, x2 - исходный IP-адрес, x3 - порт назначения TCP / UDP, x4 - исходный порт TCP / UDP, x5 - продолжительность, x6 - количество пакетов, x7 - количество байтов, x8 - однократная скорость, x9 - скорость для хоста, x10 - средняя скорость с одним и тем же исходным хостом, x11 - скорость соединений на одном и том же порту с хостом из других узлов.

После кластеризации данных, основанной на SOM, данные заголовка пакета и информация группировки подаются на вход многослойного персептрона, обученного распознавать аномальный трафик, но с учетом информации о событии, то есть содержимого пакета для определенной группы. Это позволяет не только обнаруживать аномалии в одиночных пакетах, но и выявлять принадлежность пакета к атаке, основанной на времени.

Формат входного вектора для многослойного персептрона выглядит следующим образом. Входной образец делится на непересекающиеся части длиной 150 пакетов. Все пакеты проходят через сеть Кохонена. Пакет связан с номером кластера (номер нейронов победителя). Кластеры консолидируются - 5 соседних объединяются. Получается 100 больших кластеров.

По увеличенным кластерам считается, что гистограмма представляет собой трафик, то есть первым компонентом вектора является количество пакетов, попавших в первый объединенный кластер (кластеры 1-5) и т.д. Гистограмма нормализована, компоненты уменьшены до диапазона 0-1. После этого вычисляется дельта между соседними векторами.

В предлагаемом методе учитываются два типа трафика. При анализе отдельных узлов кластера идентифицируются индивидуальные сценарии атаки. Кроме того, анализируются резкие изменения мощности сетевого потока для обнаружения всплесков нагрузки. Совместный анализ этих двух типов событий позволяет более точно реагировать на появление вредоносного трафика, уменьшая при этом количество ложных срабатываний, связанных с увеличением полосы пропускания.

Созданная нейронная сеть позволяет не только идентифицировать аномалии в сети, но и прогнозировать их появление, собирая данные с датчиков, расположенных на основе виртуальных сетевых функций в среде мультиоблачной платформы, расположенной в виртуальном центре обработки данных. Полученная информация необходима для обучения и тестирования нейронной сети. Следующим шагом будет определение оптимальной схемы правил идентификации атак. Это позволит настроить набор входных данных и улучшить качество результата на выходе нейронной сети. Последним шагом является тестирование системы с использованием примеров, не включенных в обучающую выборку.

Еще одним преимуществом сети Кохонена является способность идентифицировать новые кластеры. Обученная сеть распознает кластеры в данных обучения и назначает все данные тому или иному кластеру. Если сеть затем встречает набор данных, который отличается от любого из известных образцов, он будет независимо определять новый кластер элементов. Эта функция очень актуальна, поскольку она позволяет защитить архитектуру

виртуального центра обработки данных без фактического изменения алгоритмов обнаружения атак.

4. Экспериментальная часть. Для проведения тестирования сценариев экспериментальных атак мы использовали виртуальную сеть в облаке OpenStack. Она включает в себя 4 коммутатора OpenFlow (2 HP 3500yl, 2 Netgear GSM7200), 8 вычислительных узлов (32 ГБ оперативной памяти, 4 ядра), 1 сервер (32 ГБ ОЗУ, 8 ядер) с контроллером OpenFlow и 1 сервер для мониторинга. Маршрутизаторы со связанными соединениями со скоростью 1000 Мбит / с, а компьютеры подключены к маршрутизатору со скоростью 100 Мбит / с. В этой инфраструктуре были подготовлены 100 виртуальных машин (атакующих узлов), а также один узел, который контролирует атаку. В рамках эксперимента случайным образом выбирается пять атакованных виртуальных машин (хост службы). Эксперименты показали, что максимальная производительность датчика и модуля сбора при работе в парах ограничена двумя факторами: пропускной способностью канала между коллектором и датчиком и мощностью сервера, на котором расположен коллектор. Данные от датчика поступают в виде пакетов UDP, пакет содержит максимальную информацию о 30 потоках. Если датчик обработал 240000 потоков в секунду, он отправит 8000 UDP-пакетов по 1506 байтов каждый, что создаст нагрузку 92 Мбит / с. Модуль тестировался со значениями до 4 миллионов потоков в секунду. При среднем размере потока 1 Мбайт значение мощности потоков будет 3900 ГБ / с. Во всех экспериментах временная задержка, введенная модулем, не превышала 300 мс. Эта задержка достаточна для своевременного ответа на вредоносный трафик. Максимальная скорость атаки DDoS в нашем эксперименте составляла 0,5 Гбит / с.

Таблица 1. Результаты исследования

№ п/п	Скорость вредоносного трафика, Гбит / с	Время отклика Active / Passive	Нарушение QoS, % Active / Passive
1	0.10	45/90	0.01/0.10
2	0.20	48/120	0.20/0.20
3	0.30	50/150	0.50/30
4	0.40	60/180	1.80/25
5	0.50	65/220	2.50/30

Заключение. Экспериментальные исследования показали, что разработанный прототип системы позволяет не только значительно сократить время отклика приложений и услуг в сети с несколькими облачными платформами при проведении кибератак, но и поддерживать указанное качество обслуживания на требуемом уровне.

В будущем планируется исследовать работу прототипа ресурсоемкости, а также поведение различных типов кибератак.

Работа выполнена при поддержке РФФИ (научные проекты 16-37-60086 мол_а_дк и 16-07-01004, 16-29-09639, 18-07-01446, 18-47-560016), и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук (МК-1624.2017.9).

СПИСОК ЛИТЕРАТУРЫ

1. Alshamrani A., Chowdhary A., Pisharody S., Lu D., Huang D. A Defense System for Defeating DDoS Attacks in SDN based Networks // 15th ACM International Symposium on Mobility Management and Wireless Access. 2017. Pp. 83–92.
2. Bolodurina I.P., Parfenov D.I. Models and algorithm of optimization launch and deployment of virtual network functions in the virtual data center // Journal of Physics: Conference Series. vol. 913. no. 1. Pp. 012012. DOI: 10.1088/1742-6596/913/1/012012
3. Borisenko K. Methods and model for protecting virtualized computer networks of distributed cloud computing environments from network attacks // Thesis for Degree of Master Science in Computer Engineering. 2016. 173 p.
4. Dotcenko S., Vladyko A., Letenko I. A fuzzy logic-based information security management for software-defined networks // 16th International Conference Advanced Communication Technology (ICACT). 2014. Pp. 167−171.
5. Jankowski D., Amanowicz M. On efficiency of selected machine learning algorithms for intrusion detection in software defined networks // International Journal of Electronics and Telecommunications. 2016. vol. 62. no. 3. Pp. 247–252.
6. Letteri I., Del Rosso M., Caianiello P., Cassioli D. Performance of Botnet Detection by Neural Networks in Software-Defined Networks // Second Italian Conference on Cyber Security. 2018. Pp. 1–10.
7. Parfenov D., Bolodurina I. Methods and algorithms optimization of adaptive traffic control in the virtual data center // International Siberian Conference on Control and Communications (SIBCON-2017). 2017. Pp. 1–6. DOI: 10.1109/SIBCON.2017.7998475
8. Rengaraju P., Ramanan V.R., Lung, C.H. Detection and prevention of DoS attacks in Software-Defined Cloud networks // Dependable and Secure Computing Conference. 2017. Pp. 217–223.
9. Wang S., Chavez K.G., Kandeepan S. SECO: SDN sEcure COntroller algorithm for detecting and defending denial of service attacks // 5th International Conference Information and Communication Technology (ICoIC7). 2017. Pp. 1–6.

UDK 519.687

INVESTIGATION THE NEURAL NETWORK MODEL FOR SECURITY AND QUALITY OF SERVICE OF MULTI-CLOSE PLATFORM

Irina P. Bolodurina
Dr., Professor, Head. Department of Applied mathematics Orenburg State University
Pobedy avenue, 13, 460018, Orenburg, Russia, e-mail: prmat@mail.osu.ru
Denis I. Parfenov
Faculty of Distance Learning Technologies Orenburg State University
Pobedy avenue, 13, 460018, Orenburg, Russia, e-mail: prmat@mail.osu.ru

Abstract. In this study, a prototype of an autonomous system was developed and investigated to provide cyber security and quality of service for multi-cloud platforms. Based on the developed system is a mathematical model of traffic analysis. The

mathematical model is based on the neural network. A hybrid neural network based on a multi-layer perceptron and a self-organizing Kohonen network was designed. This approach allowed to more accurately classify and detect malicious traffic. The conducted experimental researches have shown that using the proposed approach allows to increase the effectiveness of detection of such attacks as denial of service. At the same time, during the attack, the required quality of service is maintained in the multi-cloud platform network.

Key words: cloud computing, virtual data centers, software-controlled architecture, neural network, cybersecurity, quality of service.

References

1. Alshamrani A., Chowdhary A., Pisharody S., Lu D., Huang D. A Defense System for Defeating DDoS Attacks in SDN based Networks // 15th ACM International Symposium on Mobility Management and Wireless Access. 2017. Pp. 83–92.
2. Bolodurina I.P., Parfenov D.I. Models and algorithm of optimization launch and deployment of virtual network functions in the virtual data center // Journal of Physics: Conference Series. vol. 913. no. 1. Pp. 012012. DOI: 10.1088/1742-6596/913/1/012012
3. Borisenko K. Methods and model for protecting virtualized computer networks of distributed cloud computing environments from network attacks // Thesis for Degree of Master Science in Computer Engineering. 2016. 173 p.
4. Dotcenko S., Vladyko A., Letenko I. A fuzzy logic-based information security management for software-defined networks // 16th International Conference Advanced Communication Technology (ICACT). 2014. Pp. 167–171.
5. Jankowski D., Amanowicz M. On efficiency of selected machine learning algorithms for intrusion detection in software defined networks // International Journal of Electronics and Telecommunications. 2016. vol. 62. no. 3. Pp. 247–252.
6. Letteri I., Del Rosso M., Caianiello P., Cassioli D. Performance of Botnet Detection by Neural Networks in Software-Defined Networks // Second Italian Conference on Cyber Security. 2018. Pp. 1–10.
7. Parfenov D., Bolodurina I. Methods and algorithms optimization of adaptive traffic control in the virtual data center // International Siberian Conference on Control and Communications (SIBCON-2017). 2017. Pp. 1–6. DOI: 10.1109/SIBCON.2017.7998475
8. Rengaraju P., Ramanan V.R., Lung, C.H. Detection and prevention of DoS attacks in Software-Defined Cloud networks // Dependable and Secure Computing Conference. 2017. Pp. 217–223.
9. Wang S., Chavez K.G., Kandeepan S. SECO: SDN sEcure COntroller algorithm for detecting and defending denial of service attacks // 5th International Conference Information and Communication Technology (ICoIC7). 2017. Pp. 1–6.