ОБЗОР СПОСОБОВ ПРИМЕНЕНИЯ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ К ПРОГРАММНО-КОНФИГУРИРУЕМЫМ СЕТЯМ

З. С. Канивец[1], А. И. Выборнова[1]*

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

*Адрес для переписки: a.vybornova@spbsut.ru

Аннотация—С появлением концепции программно-конфигурируемых сетей с централизованной плоскостью управления стало возможным собирать огромное количество информации о сети, например, информацию о топологии и загруженности сети, состоянии сетевых устройств. Эти данные можно использовать для тренировки алгоритмов машинного обучения, причём данные алгоритмы могут быть применены для широкого спектра задач, таких как классификация трафика, качество обслуживания, оптимизация маршрутов передачи трафика, управление ресурсами и обеспечение безопасности. **Предмет исследования:** ПКС и различные аспекты их функционирования. **Методы исследования:** анализ литературы, посвященной применению методов МО для работы с ПКС. **Основные результаты:** анализ областей для использования МО с точки зрения эффективности работы ПКС, анализ и классификация существующих решений по использованию МО в ПКС. Практическая значимость работы состоит в возможности использования полученных результатов для оптимизации различных аспектов работы ПКС.

Ключевые слова—программно-конфигурируемые сети, алгоритмы машинного обучения.

Информация о статье
УДК 004.722
Язык статьи – русский.
Поступила в редакцию 28.09.2021, принята к печати 10.12.2021.

Ссылка для цитирования: Канивец З. С., Выборнова А. И. Обзор способов применения методов машинного обучения к программно-конфигурируемым сетям // Информационные технологии и телекоммуникации. 2021. Том 9. № 3. С. 11–21. DOI 10.31854/2307-1303-2021-9-3-11-21.

A SURVEY ON MACHINE LEARNING ALGORITHMS FOR SOFTWARE-DEFINED NETWORKS

Z. Kanivets[1], A. Vybornova[1*]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

[*]Corresponding author: a.vybornova@spbsut.ru

Abstract—With the advent of the concept of Software-Defined Networks with a centralized control plane, it became possible to collect a huge amount of information about the network, for example, network topology, network congestion, the state of network devices. This data can be used to train machine learning algorithms. Moreover, these algorithms can be applied for completely different purposes, such as traffic classification, quality of service, optimization of traffic transmission routes, resource management, and security. **Research subject** of this article consist on the different aspects of SDN operating that can be optimized with ML. **Research method** is an analysis of the literature on the subject. **Core results are** analysis and classification of the areas and methods of the ML algorithms implementation for the SDN. **Practical relevance** of the work is that the results can be used for optimization of different SDN characteristics.

Keywords—software defined networks, machine learning algorithms.

Article info
Article in Russian.
Received 28.09.2021, accepted 10.12.2021.

For citation: Kanivets Z., Vybornova A.: A Survey on Machine Learning Algorithms for Software-Defined Networks // Telecom IT. 2021. Vol. 9. Iss. 3. pp. 11–21 (in Russian). DOI 10.31854/2307-1303-2021-9-3-11-21.

Введение

Идея применения технологий машинного обучения (МО) для оптимизации работы сетей связи уже возникала в научно-техническом сообществе ранее. Например, в 2003 году был предложен подход к проектированию сети, основанный на инструментах, использующих искусственный интеллект. Смысл заключался в том, что сеть пронизывала «knowledge plane», распределённая интеллектуальная система, собирающая информацию о сети и принимающая решения по конфигурации сети и разрешению возможных конфликтов и проблем при передаче данных [1]. Также она должна была обеспечивать безопасность и автоматизировать функции, которые выполняются людьми.

Однако в тот момент технические возможности были не столь развиты, а основной причиной отсутствия практической реализации стал тот факт, что традиционные сети имеют распределённую структуру. Изучение узлов сети, имеющих лишь частичное представление о системе в целом, для управления сетью за пределами ограниченной области являлось слишком сложной задачей.

С появлением концепции программно-конфигурируемых сетей (ПКС), а также с развитием технологий, связанных с машинным обучением, стало возможным приступить к разработке решений на их основе. Программно-конфигурируемые сети могут облегчить реализацию подобных решений, поскольку обеспечивают разделение между плоскостью передачи данных и программной плоскостью управления, а также обладают возможностью централизованного отслеживания состояния сети. Встроенные механизмы сбора информации о сети облегчают накопление необходимых данных для их дальнейшего использования в задачах машинного обучения без необходимости в дополнительном промежуточном программном обеспечении для этой цели и с возможностью изменения поведения сети на основе полученных результатов. Благодаря программируемости SDN максимально эффективные и оптимальные решения, полученные с помощью МО, могут применяться в режиме реального времени [2].

Существует большое количество задач, в которых могут быть применены алгоритмы машинного обучения, например, такие как обеспечение безопасности (контроль доступа, обнаружение DDOS- и DOS-атак) или прогнозирование перегрузок и тенденций в сети (например, объёмов трафика).

Цель данной статьи – описать возможные варианты применения алгоритмов машинного обучения для решения проблем, связанных с конфигурацией и эксплуатацией ПКС. В первой части будут более подробно рассмотрены разные виды подобных задач и различные алгоритмы МО, которые могут быть использованы для их решения. Во второй части статьи приведён обзор существующих применений инструментов МО для ПКС. В третьей части приведены выводы и возможные направления для дальнейших исследований.

Задачи программно-конфигурируемых сетей, решаемые с помощью алгоритмов МО

В данном разделе мы пристальнее рассмотрим существующие группы задач, которые встречаются при эксплуатации и конфигурации ПКС и которые могут

быть решены с использованием МО. В целом можно выделить следующие пять групп:

1. Классификация трафика – функция, предоставляющая детальное управление сетью путём определения различных типов трафика. Благодаря классификации трафика, операторы сети могут предоставлять услуги и распределять сетевые ресурсы более эффективно.

К широко используемым методам классификации трафика относятся глубокая проверка пакетов (DPI) и машинное обучение [3].

DPI сопоставляет полезную нагрузку потоков трафика с заранее определёнными шаблонами, чтобы понять, каким приложениям принадлежат потоки трафика. Шаблоны определяются регулярными выражениями. Подход, основанный на DPI, обычно имеет высокую точность, но также у него имеются и недостатки. Во-первых, DPI может распознавать трафик только в том случае, если имеется необходимый шаблон. Из-за стремительного роста количества приложений создавать новые шаблоны и поддерживать существующие в актуальном состоянии достаточно сложно. Во-вторых, DPI требует больших вычислительных затрат, так как проверять необходимо все транспортные потоки. В-третьих, DPI имеет ограниченные возможности при работе с зашифрованным трафиком.

Подходы на основе машинного обучения могут правильно распознавать зашифрованные данные и требуют гораздо меньших вычислительных затрат, чем подход на основе DPI. Для решения задачи классификации собирается огромное количество данных, а затем методы машинного обучения применяются для поиска в них закономерностей [4]. В SDN контроллер располагает информацией о состоянии сети, что облегчает сбор и анализ трафика. Таким образом, инструменты МО реализуются в контроллере.

2. Оптимизация маршрутизации – в SDN контроллер может управлять маршрутизацией потоков трафика, изменяя таблицы потоков в маршрутизаторах, чтобы отбросить поток трафика или перенаправить его по другому маршруту. Очень важно эффективно управлять маршрутизацией, иначе могут возникнуть перегрузка сетевых каналов, увеличение задержки при передаче данных и т. д. Таким образом, оптимизация маршрутизации трафика в SDN – одна из приоритетных задач.

Алгоритм кратчайшего пути и эвристические алгоритмы [5] – два широко используемых подхода. Алгоритм SPF (*Shortest Path First*) маршрутизирует пакеты, используя такие простые показатели, как количество переходов или задержка. К сожалению, алгоритм SPF не максимально эффективно использует сетевые ресурсы.

Следующий подход – эвристические алгоритмы (например, алгоритм оптимизации муравьиной колонии). Большая вычислительная сложность – главный недостаток эвристических алгоритмов [6]. Так как для каждого нового потока контроллер разрабатывает собственную политику маршрутизации, в случае с использованием эвристических алгоритмов нагрузка на контроллер значительно увеличивается.

По сравнению с эвристическими алгоритмами алгоритмы МО имеют ряд преимуществ. Во-первых, высокая скорость предоставления решений в том случае,

если используется уже обученная модель. Во-вторых, алгоритмы МО не нуждаются в точной математической модели базовой сети. Проблема оптимизации маршрутизации может быть рассмотрена как задача принятия решений. Таким образом, обучение с подкреплением в данном случае является оптимальным подходом.

3. QoS/прогнозирование QoE – параметры QoS, такие как коэффициент потерь, задержка, джиттер и пропускная способность, являются сетевыми метриками, которые обычно используются сетевыми операторами для оценки производительности сети. В процессе распространения и популяризации мультимедийных технологий для поставщиков сетевых услуг становится крайне важной удовлетворённость конечного пользователя. Именно QoE помогает оценить, насколько клиенты довольны предоставляемой услугой. На основе прогнозов QoS/QoE, провайдеры могут предпринять те или иные действия, чтобы предотвратить отток клиентов или увеличить их количество.

Параметры QoS тесно связаны с производительностью сети и показателями KPI (*Key Performance Indicators*). К ним относятся размер пакета, скорость передачи, длина очереди и т. д. Выявление количественных соотношений между KPI и параметрами QoS может улучшить управление QoS путём их прогнозирования в соответствии с KPI. Поскольку параметры QoS обычно представляют собой непрерывные данные, эту задачу можно рассматривать как задачу регрессии. В этом случае оптимально использовать обучение с учителем.

Обучение с учителем может быть использовано и в случае прогнозирования QoE. QoE – это субъективный показатель, чаще всего получаемый с помощью опросов пользователей, которые зачастую бывают затратными по времени и ресурсам. Значения QoE в большой степени зависят от параметров QoS, и есть возможность получать значения QoE в режиме реального времени, если понять, как именно параметры QoS влияют на значения QoE. Машинное обучение – это эффективный метод изучения взаимосвязи между параметрами QoS и значениями QoE. Поскольку значения QoE как правило, дискретные данные, проблема прогнозирования QoE может быть рассмотрена как задача классификации, для которой оптимально использовать метод обучения с учителем.

4. Управление ресурсами – эффективное управление сетевыми ресурсами является основным требованием сетевых операторов для повышения производительности сети. SDN упрощает использование сетевых ресурсов и управление ими для максимально полезного использования сетевых ресурсов. К задаче управления ресурсами относится огромный пласт задач, связанных и с плоскостью данных, и с плоскостью управления. Вот лишь некоторые из них: распределение ресурсов (как в случае использования одного контроллера, так и в случае с мультиконтроллерной SDN), контроль возможности подключения новых устройств (для того, чтобы уже имеющиеся устройства в сети не пострадали от нехватки ресурсов), проблема размещения контроллеров и многие другие. Для каждой из этих задач имеется не одно решение, однако найти оптимальное только предстоит. И в этом также могут помочь методы МО. Несколько примеров будут рассмотрены в следующем разделе.

5. Безопасность – аспект, который обязательно рассматривается провайдерами. Обнаружение вторжений является важным элементом сетевой безопасности. Система обнаружения вторжений (IDS) – это устройство или программное обеспечение, цель которого – отслеживать события в сетевой системе и определять возможные атаки [6], что помогает предотвратить атаку и минимизировать ущерб. По методам анализа выделяются два типа IDS: IDS на основе сигнатур и IDS на основе аномалий.

Анализ сигнатур основан на простом поиске совпадений между последовательностью и образцом, т. е. просматривается входящий пакет и сравнивается с сигнатурой (подписью) – характерной строкой программы, которая может содержать особенный набор слов или команду, прежде связанную с атаками. При обнаружении совпадений объявляется тревога. Этот метод достаточно точен, однако его главными недостатками являются необходимость постоянного и своевременного пополнения базы сигнатур, что оставляет брешь в безопасности сети, и долговременная процедура сравнения подписей с последовательностью.

В случае использования второго метода рассматриваются протоколы сети. Каждый пакет сопровождается различными протоколами. Инструменты IDS разворачивают и осматривают эти протоколы (TCP, UDP, IP) в соответствии со стандартами. Если что-нибудь нарушает эти стандарты (например, неправильные значения в полях протокола), то существует вероятность атаки и объявляется тревога.

Методы машинного обучения широко используются в IDS на основе аномалий путём обучения модели для определения нормальных и аномальных действий. Проблема обнаружения вторжений является задачей классификации. Таким образом, алгоритмы обучения с учителем часто применяются для обнаружения вторжений.

Теперь, когда мы рассмотрели ключевые задачи, которые необходимо решить в рамках эксплуатации и конфигурации SDN и которые могут быть решены с использованием МО, следует изучить конкретные примеры.

Существующие решения, использующие методы машинного обучения

Решение, представленное в [8], используется для классификации трафика. В этой статье применены такие методы машинного обучения, как SVM (*Support Vector Machine* – метод опорных векторов), который является набором схожих алгоритмов для обучения с учителем, использующихся для задач классификации и регрессионного анализа, а также метод K-средних, являющийся методом кластеризации для обучения без учителя. С их помощью производится разделение трафика на классы приложений на основе данных, полученных непосредственно из заголовков пакетов (размер сегмента, время между прибытиями пакетов). Результаты указывают на то, что метод опорных векторов обеспечивает высокую точность классификации, равную 98 %, причём среди всех классов трафика.

В статье [9] для определения трафика, принадлежащего к различным мобильным приложениям, используется глубокая нейронная сеть. В качестве данных для обучения 8-слойной модели выбраны пять параметров потока трафика,

такие как адрес и порт назначения, тип протокола, размер и время жизни пакета). Результаты моделирования демонстрируют, что обученная модель для идентификации 200 мобильных приложений может достичь точности 93,5 %.

Для оптимизации маршрутизации может быть применён метод, описанный в статье [10]. В этой статье предложен фреймоворк на основе метода машинного обучения, который использует новую технологию глубокого обучения с подкреплением под названием DDPG (*Deep Deterministic Policy Gradient*) для оптимизации процесса маршрутизации. Данная структура позволяет управлять сетью в реальном времени и по сравнению с существующими решениями для оптимизации может улучшить производительность сети. Авторы статьи [11] предлагают фреймворк для динамической маршрутизации, называемую NeuRoute. В NeuRoute используется архитектура рекуррентной нейронной сети LSTM (*Long short-term memory*) для оценки будущего сетевого трафика. Информация о состоянии сети и предполагаемый сетевой трафик подаются на вход нейронной сети, также имеются соответствующие решения для маршрутизации, всё это используется для обучения нейронной сети. После тренировки обученная модель может быть применена для получения эвристических результатов в реальном времени.

В работах [12, 13] приведены способы прогнозирования задержки и объема трафика в перспективных сетях связи при помощи методов машинного обучения, в частности, нейронных сетей с кратковременной памятью. Авторы работ сосредотачиваются на приложениях Интернета вещей, однако те же методы можно применять и для других перспективных телекоммуникационных приложений.

В статье [14] методы машинного обучения используются для демонстрации возможности оценки и предсказания ключевых факторов QoE по показателям QoS. Авторы обнаружили важные закономерности в переменных QoE и построили модель байесовской сети, что обеспечило высокую точность предсказаний. Также было показано, что для всех рассмотренных решающих факторов QoE промежуточные прогнозы для скрытых переменных могут повысить эффективность подхода.

Авторы статьи [15] используют четыре алгоритма машинного обучения (*Decision Tree*, нейронная сеть, метод *k*-ближайших соседей и *Random Forest*) для прогнозирования значений QoE на основе параметров для оценки качества видео (индекса структурного сходства (SSIM) и индекс качества видео (VQM)). Коэффициент корреляции Пирсона и среднеквадратичная ошибка применяются для оценки производительности этих алгоритмов.

Статья [16] описывает алгоритм балансировки нагрузки для контроля и координации распределения рабочей нагрузки по для эффективного использования сетевых ресурсов. Авторами предложен алгоритм MRBS (*Multiple Regression Based Searching*), который на основе различных показателей нагрузки, таких как количество трафика и его характеристики (всплески активности и разная частота сообщений) оценивает необходимость переадресации запросов на серверы, у которых мало подключений и меньший поток трафика, по пути с наименьшими затратами. Данный алгоритм повышает эффективность использования полосы пропускания, уменьшает задержку и уравновешивает нагрузку на сервера в кластере.

В работе [17] предлагается прогнозировать интенсивность потока служебных сообщений на контроллере Open Flow. Для прогнозирования используется обычная нейронная сеть. Полученные результаты позволяют не только прогнозировать нагрузку на контроллеры, но и интеллектуально управлять потоками в мультиконтроллерных ПКС.

В статье [18] описаны три различные регрессионные модели, которые предназначены для поиска соответствия между потреблением ресурсов центрального процессора (ЦП) и частотой управляющих сообщений. Собранные данные о загрузке ЦП сетевых гипервизоров и о частоте управляющих сообщений используются для обучения моделей. Далее модели могут быть использованы в режиме реального времени для оценки того, насколько сетевые гипервизоры перегружаются в соответствии с измеренной частотой управляющих сообщений, что важно, поскольку перегрузка сетевых гипервизоров оказывает значительное влияние на обработку управляющих сообщений каждого клиента.

Авторы статьи [19] предлагают решение для защиты от DDoS-атак, особенно от TCP-SYN flood атак и ICMP flood атак с использованием машинного обучения в сетях ISP на основе ПКС. Алгоритм машинного обучения, основанный на методе k-ближайших соседей, упрощает операции в реальном времени, используется для обнаружения и устранения вредоносного трафика, отслеживая источники атаки, в то время как нормальный трафик практически не затрагивается. Также ими предложен метод машинного обучения для автоматической адаптации времени работы окна мониторинга в зависимости от входящего трафика для повышения эффективности смягчения последствий атаки. Экспериментальные результаты трассировки трафика CAIDA, а также трафика с тестового стенда показывают, что при работе в режиме реального времени более 98% вредоносного трафика обнаруживаются и отбрасываются, а обычный трафик почти не затрагивается.

В работе [20] алгоритмы МО (MLP, SVM, дерево принятия решений и *Random Forest*) были предложены для обнаружения DDoS-атак трех различных категорий (атака на полосы пропускания, атака на контроллер и атака на таблицу потоков). В результате эксперимента Дерево решений было признано лучшим алгоритмом в целом, поскольку обладает наименьшее время обработки, однако Random Forest имеет наибольшую точность. Можно увидеть, что источник порта является наиболее важной характеристикой при классификации аномалий, за которой следует время жизни соединения. Полученные результаты могут помочь в построении системы для нейтрализации последствий DDoS-атак.

Заключение

В данной статье рассмотрены способы применения алгоритмов МО для решения задач, связанных с ПКС. В рассмотренных работах использованы различные алгоритмы машинного обучения, такие как метод опорных векторов, метод k-ближайших соседей, Random Forest и многие другие, а некоторые статьи предлагают собственные алгоритмы, построенные на их основе. Однако в подобном многообразии решений только предстоит найти лучшие, которые смогут быть использованы в дальнейшем при построении ПКС. Стоит более подробно рассмотреть методы глубокого обучения, поскольку они могут обеспечить более высокую

точность предсказаний и более эффективно использовать те огромные объёмы данных, которые собираются при работе сети.

Исследование выполнено в рамках исполнения ПНИ по государственному заданию СПбГУТ на 2021 год.

Литература

1. D. Clark, C. Partridge, J. Ramming, J. Wroclawski, "A Knowledge Plane for the Internet," Proc SIGCOMM'03. 3–10, 2003.
2. G. Xu, Y. Mu, and J. Liu, "Inclusion of artifificial intelligence in communication networks and services," ITU Journal: ICT Discoveries, no. 1, pp. 1–6, Oct. 2017.
3. P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares, and H. S. Mamede, "Machine learning in software defifined networks: Data collection and traffific classifification," in Proc. IEEE ICNP'16, Singapore, Nov. 2016, pp. 1–5.
4. Кучерявый А. Е., Бородин А. С., Мутханна А. С. А., Абделлах А. Р., Волков А. Н. Искусственный интеллект в сетях связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021) : сб. науч. ст. в 4 т., Санкт-Петербург, 24–25 февраля 2021 года; СПбГУТ. Санкт-Петербург, 2021. Т. 1. С. 8–18.
5. R. Hajlaoui, H. Guyennet, and T. Moulahi, "A survey on heuristic-based routing methods in vehicular ad-hoc network: Technical challenges and future trends," IEEE Sensors Journal, vol. 16, no. 17, pp. 6782–6792, Sept. 2016.
6. L. Yanjun, L. Xiaobo, and Y. Osamu, "Traffific engineering framework with machine learning based meta-layer in software-defifined networks," in Proc. IEEE ICNIDC'14, Beijing, China, Sept. 2014, pp. 121–125.
7. Бобров А. Системы обнаружения вторжений. URL: http://www2.icmm.ru/~masich/win/lexion/ids/ids.html
8. Fan, Z., & Liu, R., "Investigation of machine learning based network traffic classification". 2017 International Symposium on Wireless Communication Systems (ISWCS). doi:10.1109/iswcs.2017.8108090.
9. A. Nakao and P. Du, "Toward in-network deep machine learning for identifying mobile applications and enabling application specific network slicing," IEICE Trans. Communications, p. 2017CQI0002, 2014.
10. Yu, C., Lan, J., Guo, Z., & Hu, Y. (2018). "DROM: Optimizing the Routing in Software-Defined Networks with Deep Reinforcement Learning". IEEE Access, 1–1. doi:10.1109/access.2018.2877686
11. A. Azzouni, R. Boutaba, and G. Pujolle, "NeuRoute: Predictive dynamic routing for software-defifined networks," arXiv:1709.06002, 2017.
12. Абделлах А. Р., Махмуд О. А., Парамонов А. И., Кучерявый А. Е. Прогнозирование задержки в сетях интернета вещей и тактильного интернета с использованием машинного обучения // Электросвязь. 2021. № 1. С. 23–27. DOI 10.34832/ELSV.2021.14.1.002.
13. Бородин А. С., Абделлах А. Р., Кучерявый А. Е. Глубокое обучение с долговременной краткосрочной памятью для прогнозирования трафика интернета вещей // Электросвязь. 2021. № 2. С. 26–30. DOI 10.34832/ELSV.2021.15.2.003.
14. Vasilev, V., Leguay, J., Paris, S., Maggi, L., & Debbah, M., "Predicting QoE Factors with Machine Learning". 2018 IEEE International Conference on Communications (ICC).
15. T. Abar, A. B. Letaifa, and S. E. Asmi, "Machine learning based QoE prediction in SDN networks," in Proc. IEEE IWCMC'17, Valencia, Spain, 2017.
16. G. Sulthana Begam, M. Sangeetha and N.R Shanker, "Load Balancing in DCN Servers through SDN Machine Learning Algorithm", 2021.
17. Волков А. Н., Кучерявый А. Е. Метод прогнозирования нагрузки на контроллеры SDN с помощью технологий искусственного интеллекта // Электросвязь. 2021. № 2. С. 31–38. DOI 10.34832/ELSV.2021.15.2.004.
18. C. Sieber, A. Basta, A. Blenk, and W. Kellerer, "Online resource mapping for SDN network hypervisors using machine learning," in Proc. IEEE NETSOFT'16, Seoul, South Korea, June. 2016, pp. 78–82.

19. Tuan, N. N., Hung, P. H., Nghia, N. D., Tho, N., Phan, T., & Thanh, N. (2020). A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN. Electronics, 9(3), 413.
20. Santos, R., Souza, D., Santo, W., Ribeiro, A., & Moreno, E. (2019). Machine learning algorithms to detect DDoS attacks in SDN. Concurrency and Computation: Practice and Experience, e5402.

References

1. D. Clark, C. Partridge, J. Ramming, J. Wroclawski, "A Knowledge Plane for the In-ternet," Proc SIGCOMM'03. 3-10, 2003.
2. G. Xu, Y. Mu, and J. Liu, "Inclusion of artifificial intelligence in communication net-works and services," ITU Journal: ICT Discoveries, no. 1, pp. 1–6, Oct. 2017.
3. P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares, and H. S. Mamede, "Machine learning in software defifined networks: Data collection and traffific classifification," in Proc. IEEE ICNP'16, Singapore, Nov. 2016, pp. 1–5.
4. Koucheryavy A., Borodin A., Muthanna A., Abdellah A. R., Volkov A. Artificial Intelligence for Telecommunication Networks // 10TH International conference on advanced infotelecommunications, ICAIT 2021. PP. 8–18(in Russia).
5. R. Hajlaoui, H. Guyennet, and T. Moulahi, "A survey on heuristic-based routing methods in vehicular ad-hoc network: Technical challenges and future trends," IEEE Sensors Journal, vol. 16, no. 17, pp. 6782–6792, Sept. 2016.
6. L. Yanjun, L. Xiaobo, and Y. Osamu, "Traffific engineering framework with machine learning based meta-layer in software-defifined networks," in Proc. IEEE ICNIDC'14, Beijing, China, Sept. 2014, pp. 121–125.
7. Bobrov A. Sistemy obnaruzheniya vtorzhenij. URL: http://www2.icmm.ru/~masich/win/lexion/ids/ids.html (in Russia).
8. Fan, Z., & Liu, R., "Investigation of machine learning based network traffic classifi-cation". 2017 International Symposium on Wireless Communication Systems (ISWCS). doi:10.1109/iswcs.2017.8108090.
9. A. Nakao and P. Du, "Toward in-network deep machine learning for identifying mobile applications and enabling application specific network slicing," IEICE Trans. Communications, p. 2017CQI0002, 2014.
10. Yu, C., Lan, J., Guo, Z., & Hu, Y. (2018). "DROM: Optimizing the Routing in Software-Defined Networks with Deep Reinforcement Learning". IEEE Access, 1–1. doi:10.1109/access.2018.2877686
11. A. Azzouni, R. Boutaba, and G. Pujolle, "NeuRoute: Predictive dynamic routing for software-defifined networks," arXiv:1709.06002, 2017.
12. Abdellach A.R., Mahmood O.A., Paramonov A.I., Koucheryavy A.E. Delay prediction in IoT and tactile internet using machine learning approach // Electrosvyaz. 2021. No 1. PP. 23–27. DOI 10.34832/ELSV.2021.14.1.002 (in Russia).
13. Borodin A. S., Abdellah A. R., Koucheryavy A. E. Deep learning with long-term short-term memory for IoT traffic prediction // Electrosvyaz. 2021. No 2. PP. 26–30. DOI 10.34832/ELSV.2021.15.2.003 (in Russia).
14. Vasilev, V., Leguay, J., Paris, S., Maggi, L., & Debbah, M., "Predicting QoE Fac-tors with Machine Learning". 2018 IEEE International Conference on Communica-tions (ICC).
15. T. Abar, A. B. Letaifa, and S. E. Asmi, "Machine learning based QoE prediction in SDN networks," in Proc. IEEE IWCMC'17, Valencia, Spain, 2017.
16. G. Sulthana Begam, M. Sangeetha and N.R Shanker, "Load Balancing in DCN Servers through SDN Machine Learning Algorithm", 2021.
17. Volkov A. N., Koucheryavy A. E. Prediction method of SDN controllers loading based on the artificial intelligence technologies // Electrosvyaz. 2021. No 2. PP. 31–38. DOI 10.34832/ELSV.2021.15.2.004 (in Russia).
18. C. Sieber, A. Basta, A. Blenk, and W. Kellerer, "Online resource mapping for SDN network hypervisors using machine learning," in Proc. IEEE NETSOFT'16, Seoul, South Korea, June. 2016, pp. 78–82.
19. Tuan, N. N., Hung, P. H., Nghia, N. D., Tho, N., Phan, T., & Thanh, N. (2020). A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN. Electronics, 9(3), 413.

20. Santos, R., Souza, D., Santo, W., Ribeiro, A., & Moreno, E. (2019). Machine learning algorithms to detect DDoS attacks in SDN. Concurrency and Computation: Practice and Experience, e5402.

Канивец Злата Сергеевна
магистрант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича zkanivec@gmail.com

Выборнова Анастасия Игоревна
кандидат технических наук, доцент кафедры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.vybornova@spbsut.ru

Kanivec Zlata S.
Undergraduate, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, zkanivec@gmail.com

Vybornova Anastasia I.
Candidate of Engineering Sciences, Associate Professor, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, a.vybornova@spbsut.ru