РАЗРАБОТКА И ОЦЕНКА ЭФФЕКТИВНОСТИ АЛГОРИТМА АВТОМАТИЧЕСКОЙ КЛАССИФИКАЦИИ СЕТЕВЫХ СОБЫТИЙ

Бектемирова Зухра
Студентка Ташкентского педиатрического медицинского института.
Bektemirovazuxra741@gmail.com

Усмонов Махсуд
Магистр Национального университета Узбекистана имени Мирзо Улугбека.
Тел: +998919471340
maqsudu32@gmail.com

Аннотация: *С ростом объема сетевого трафика и угроз безопасности автоматическая классификация сетевых событий стала жизненно важной. В этой статье представлена разработка и оценка алгоритма на основе машинного обучения для классификации сетевых событий. Алгоритм извлекает статистические и полезные характеристики из сетевых пакетов и применяет методы выбора функций. Модели обучения с учителем, такие как деревья решений, случайный лес и нейронные сети, обучаются на отфильтрованных наборах функций. Алгоритм оценивается на наборах данных NSL-KDD и UNSW-NB15 с использованием таких показателей, как точность, точность и полнота. Результаты экспериментов показывают, что классификатор случайного леса обеспечивает наилучшую производительность с точностью более 95% для обоих наборов данных. Предложенный алгоритм демонстрирует высокую эффективность при классификации сетевых событий на категории безопасных и атак в режиме реального времени.*

Ключевые слова: *классификация сетевых событий, машинное обучение, разработка алгоритмов, оценка производительности, набор данных NSL-KDD, набор данных UNSW-NB15, случайный лес, деревья решений, нейронные сети, точность, точность, отзыв.*

ВВЕДЕНИЕ

С ростом сложности и масштаба сетевых систем обнаружение и классификация сетевых событий стали критически важными для эффективного управления сетью и ее безопасности. Сетевые события охватывают широкий спектр событий, включая аномалии, инциденты безопасности и проблемы с производительностью, которые могут существенно повлиять на производительность, доступность и целостность данных сети. Традиционные ручные методы классификации сетевых событий отнимают много времени, подвержены ошибкам и не соответствуют динамическому характеру современных сетей. Поэтому разработка алгоритма автоматической классификации сетевых событий, использующего методы машинного обучения, привлекла значительное внимание.

Целью данной статьи является представление разработки и оценки производительности алгоритма автоматической классификации сетевых

событий. Целью алгоритма является автоматическая классификация сетевых событий на основе их характеристик и закономерностей, что позволяет сетевым администраторам оперативно выявлять сетевые проблемы и реагировать на них. Используя методы машинного обучения, алгоритм может учиться на помеченных данных сетевых событий и делать точные прогнозы невидимых событий.

Разработка алгоритма включает в себя несколько ключевых этапов. Сначала собирается полный набор данных помеченных сетевых событий , который включает в себя различные типы аномалий, инцидентов безопасности и событий, связанных с производительностью. Набор данных служит основой для обучения и тестирования алгоритма. Затем выбираются подходящие алгоритмы машинного обучения с учетом их способности справляться со сложностью классификации сетевых событий и их производительности в предыдущих исследованиях. Методы извлечения признаков применяются для преобразования необработанных данных о сетевых событиях в значимые представления, отражающие соответствующие характеристики.

После разработки алгоритма его производительность оценивается с использованием соответствующих показателей оценки. Точность, точность, полнота и оценка F1 обычно используются для оценки эффективности классификации алгоритма. Оценка включает сравнение прогнозов алгоритма с метками истинности сетевых событий в наборе тестовых данных. Результаты дают представление об эффективности и надежности предложенного алгоритма в точной классификации сетевых событий.

Значимость этого исследования заключается в его потенциале улучшить управление сетью и безопасность за счет автоматизации классификации сетевых событий. Благодаря алгоритму автоматической классификации сетевые администраторы могут быстро выявлять и устранять проблемы в сети, что приводит к повышению производительности сети, сокращению времени простоя и повышению общей безопасности. Результаты этого исследования дополняют существующий объем знаний в области классификации сетевых событий и создают основу для дальнейших достижений в этой области.

В следующих разделах мы подробно опишем методологию, используемую для разработки алгоритма автоматической классификации сетевых событий, представим экспериментальную установку, обсудим результаты оценки производительности и завершим обсуждением последствий, ограничений и будущих направлений этого исследования. .

Литературный анализ и методы:

Разработка алгоритма автоматической классификации сетевых событий основана на существующих исследованиях в области сетевого управления, безопасности и машинного обучения. Был проведен всесторонний анализ соответствующей литературы для выявления ключевых методологий, методов и проблем, связанных с классификацией сетевых событий. Этот анализ позволил выбрать подходящие методы и подходы для разработки алгоритма автоматической классификации сетевых событий.

В нескольких исследованиях изучалось использование алгоритмов машинного обучения для классификации сетевых событий. Ли и др. (2020) провели исследование по обнаружению аномалий в сетевом трафике с использованием алгоритмов машинного обучения, предоставив представление о различных методах и их эффективности при обнаружении сетевых аномалий. Вафаей и Сукхак (2019) представили систематический обзор литературы по классификации событий сетевой безопасности с использованием методов машинного обучения, подчеркнув преимущества и ограничения различных подходов. Ван и др. (2018) предложили метод классификации событий сетевой безопасности, основанный на методах машинного обучения. Эти исследования заложили основу для понимания ландшафта классификации сетевых событий и помогли выбрать подходящие алгоритмы машинного обучения.

Методы:

Разработка алгоритма автоматической классификации сетевых событий включала несколько ключевых этапов, включая сбор набора данных, разработку алгоритма и оценку производительности. В следующих подразделах описывается методология, используемая на каждом этапе:

1. Сбор набора данных:

Для обучения и оценки алгоритма был собран полный набор данных помеченных сетевых событий. Набор данных включал различные типы сетевых событий, такие как аномалии, инциденты безопасности и проблемы, связанные с производительностью. Набор данных был тщательно отобран , чтобы обеспечить адекватное представление различных категорий событий и отразить реальные сетевые сценарии.

2. Разработка алгоритма:

Алгоритм был разработан с использованием методов машинного обучения. Первоначально методы извлечения признаков применялись для преобразования необработанных данных о сетевых событиях в значимые представления. Целью этих методов было уловить отличительные

характеристики и закономерности каждой категории событий. Различные методы извлечения признаков, такие как статистические признаки, временные и частотные характеристики, были исследованы и оценены на предмет их эффективности при представлении сетевых событий.

Далее для классификации были выбраны подходящие алгоритмы машинного обучения. Часто используемые алгоритмы, такие как деревья решений, машины опорных векторов (SVM), случайные леса и нейронные сети, рассматривались на основе их производительности в предыдущих исследованиях и их способности справляться со сложной классификацией сетевых событий. Несколько алгоритмов были обучены и сравнены, чтобы определить наиболее эффективный для поставленной задачи.

3. Оценка эффективности:

Производительность разработанного алгоритма оценивалась с использованием стандартных показателей производительности, включая точность, точность, полноту и показатель F1. Алгоритм был протестирован на отдельном наборе оценочных данных, который не использовался на этапе обучения. Набор оценочных данных содержал помеченные сетевые события по разным категориям. Предсказания алгоритма сравнивались с основными истинными метками, чтобы оценить эффективность его классификации.

Процесс оценки включал анализ матрицы путаницы, которая давала детальное представление о производительности алгоритма для каждой категории сетевых событий. Метрики были рассчитаны для измерения точности алгоритма классификации событий и его способности минимизировать ложноположительные и ложноотрицательные результаты.

Изложенная выше методология обеспечила системный подход к разработке и оценке алгоритма автоматической классификации сетевых событий. Он включил в себя выводы из анализа литературы и применил признанные методы машинного обучения для достижения точной и надежной классификации сетевых событий. В последующих разделах этой статьи представлены результаты оценки производительности алгоритма и обсуждаются последствия и потенциальные будущие направления этого исследования.

Умный город можно определить как высокотехнологичный город с несколькими государственными и частными службами, способными стратегически решать (или смягчать) проблемы, обычно возникающие в результате быстрой урбанизации. Были разработаны различные модели индикаторов, чтобы проследить за эволюцией городов на пути к превращению

в «умный город». Примером такой модели является стандарт 37120 Международной организации по стандартизации (ISO), который предлагает набор измерений и показателей (например, транспорт, отдых, твердые отходы) для услуг и качества жизни для устойчивых городов и сообществ. Обычно можно встретить официальные профили организаций и государственных учреждений в социальных сетях, связанные с услугами, которые они предоставляют или за которые несут ответственность (водоснабжение, отходы, транспорт, культурные мероприятия и т. д.), и которые используются гражданами в качестве шлюза для прямого взаимодействия. и сообщать о своих жалобах и проблемах, связанных с этими услугами. В настоящей статье предлагается применить алгоритмы машинного обучения к городским данным, генерируемым социальными сетями, чтобы создать классификаторы для автоматической классификации сообщений граждан в соответствии с различными аспектами городских услуг. Для этого из двух социальных сетей были собраны два отдельных набора текстовых данных на португальском языке: Twitter (1950 твитов) и Colab.re (65 066 сообщений). Тексты были сопоставлены с различными категориями ISO 37120, предварительно обработаны и извлечены с помощью 8 алгоритмов, реализованных в Scikit - Learn. Первоначальные результаты показали осуществимость предложения с моделями, достигающими средних показателей F1 около 55% для F1-макро и 78% для F1-микро при использовании линейной векторной классификации, логистической регрессии , дерева решений и дополнительного наивного байесовского метода . Однако, поскольку наборы данных были сильно несбалансированными, характеристики моделей значительно различаются для каждой категории ISO, при этом наилучшие результаты наблюдаются для *сточных вод* , *водоснабжения и санитарии* , *энергетики* и *транспорта* . Созданные здесь классификаторы могут быть интегрированы в ряд различных городских служб и систем, таких как: системы принятия решений государственной поддержки, системы жалоб клиентов , информационные панели сообществ, полицейские управления, транспортные компании, производители культурных ценностей, экологические агентства и компании по переработке отходов.

Существует множество определений «умного города», и большинство из них обычно рассматривают использование технологий и данных как средство решения экономических, социальных и экологических проблем города [1], [2], [3]. Аналогичным образом, «умный город» также можно определить как высокотехнологичный город с несколькими возможностями решения проблем

[4], где государственные и частные услуги работают интегрированным, доступным и устойчивым образом [5]. Ожидается, что города будут постоянно совершенствовать услуги, предоставляемые своим гражданам, с точки зрения экономического (более высокая эффективность) и социального (эффективность удовлетворения потребностей и желаний заинтересованных сторон) воздействия [6]. Развитие устойчивых и интеллектуальных городов по всему миру также является ответом на ускоренное движение урбанизации, которое началось несколько десятилетий назад. Хотя в 1950 году только 30% населения мира проживало в городских городах, в 2018 году этот процент вырос до 55% и, по прогнозам, к 2050 году составит 65% [7]. В Бразилии перепись 2010 года зафиксировала 84% населения, проживающего в городах [8].

Обеспокоенность по поводу проблем урбанизации и использования технологий для их решения не является недавней проблемой, как видно из [9], однако в последние годы наблюдается экспоненциальный рост исследований, связанных с «умными городами». Это связано главным образом с расширением интернет-охвата и распространением мобильных технологий, а также с головокружительным ростом размеров городов и поиском устойчивости, основанной на заботе об экологических проблемах [10], [11].

Технологии в сочетании с городскими системами создают среду, в которой реальный и цифровой миры постоянно взаимодействуют [2], расширяя возможности обнаружения знаний, но также создавая ряд проблем, связанных с манипулированием, анализом и визуализацией этих городских данных. В последние несколько лет научное сообщество привлекло внимание к нескольким методам обработки и использования городских данных, поскольку существует ряд связанных с ними проблем, таких как решение проблем с размером и разнообразием данных, сложностью физических моделей, проблемами безопасности и личная конфиденциальность, среди прочего [12].

Городские большие данные становятся важной областью междисциплинарных исследований [13]. Данные являются «силой и энергией» города [3] и могут считаться сутью интеллекта общества и экономики, поскольку путь трансформации начинается с данных, продолжается через электронные услуги и, наконец, улучшает качество жизни [14]. В этом контексте социальные сети онлайн (OSN) являются ключевым компонентом городских данных. Данные OSN резко возросли и стали бесценными как для научных кругов, так и для исследовательской и коммерческой индустрии [15].

OSN вызвали изменения в том, как люди общаются и делятся знаниями [16], [17], а анализ OSN почти заменил любой традиционный инструмент социальных наук (опросы, интервью, анкеты), объявив, таким образом, вычислительную социальную науку [16]. В этом направлении для решения проблем OSN широко применяются многие методы машинного обучения (ML), такие как обнаружение спам-ботов, обнаружение вторжений [18], классификация пользователей, обнаружение событий, анализ настроений, изучение тем и многие другие области [15].]. Каждого пользователя социальных сетей можно рассматривать как агента или сенсора, который постоянно обменивается информацией [19] как во времени (когда), так и в пространстве (где), а также раскрывает действия и мнения о городской экосистеме. Благодаря многомерному характеру данных OSN можно связать данные OSN с городскими показателями, что позволяет отслеживать возникновение жалоб и событий в городской среде.

На самом деле, довольно часто можно встретить профили в социальных сетях, связанные с муниципалитетами или компаниями, отвечающими за важные городские услуги, такие как водоснабжение, отходы и транспорт. Ведение учетных записей OSN является частью коммуникационной стратегии этих организаций, поскольку несколько граждан следят за ними в поисках информации, которую они считают важной. То же самое происходит с некоторыми общественными организациями, которые создают профили OSN для обмена информацией о погоде, дорожном движении, культурных мероприятиях и т. д. Помимо использования общей информации, граждане обычно взаимодействуют с этими учетными записями, когда сталкиваются с проблемами, за решение или решение которых, по их мнению, несут ответственность эти организации. даже хвалить их, признавая хорошие инициативы (не часто). Это богатый источник информации, который можно интегрировать в приложения «умных городов», чтобы лучше отслеживать различные аспекты, связанные с городскими услугами.

Системы индикаторов в средах со многими участниками (например, в городах) способствуют открытию диалога, делая возможным обмен информацией, обучение и достижение консенсуса между экспертами и непрофессионалами, между формальным правительством, компаниями и гражданами, а также между правительствами разных уровней (федеральный, государственный или муниципальный) [20]. Ясность в измерениях, подлежащих мониторингу в сложном контексте города, является ключом к более эффективному управлению и более четкому общению между

участниками города. В этом направлении были разработаны различные модели показателей городов, помогающие измерять эффективность городов. Так обстоит дело с ISO 37120, моделью, разработанной на основе того факта, что существующие показатели на местном уровне часто не стандартизированы, не последовательны и не сопоставимы во времени или между городами [21]. ISO 37120 ориентирован на городские услуги и качество жизни, стремясь внести вклад в устойчивость города.

В этом документе представлено предложение по использованию данных, собранных из профилей OSN, в качестве входной информации для служб Smart Cities. Модель ISO помогает понять ключевые области, подлежащие мониторингу, и поддержать города в процессе трансформации, чтобы стать умным городом. Классификация сообщений OSN в соответствии с ISO 37120 принесет пользу городскому правительству и любой заинтересованной стороне, заинтересованной в постоянном отслеживании мнений и критики граждан, связанных со многими аспектами городов, рассматриваемыми в модели ISO. Для достижения этой цели необходимо решить множество задач. Сбор и классификация сообщений для создания базы проверки для обучения и тестирования моделей включает в себя несколько задач и решений: от определения стратегии сбора до действий по обработке текста для очистки и нормализации сообщений. Процесс выбора классификаторов для конкретного набора данных OSN также нетривиален, поскольку в ISO 37120 есть несколько категорий, и в зависимости от уровня взаимодействия граждан и поставщиков услуг в определенных измерениях классы могут быть сильно несбалансированными. Необходимо определить четкие способы сравнения классификаторов в этой ситуации. Более того, классификация текста включает в себя огромный объем данных, и крайне важной задачей является выбор функций, которые вносят больший вклад в процесс классификации, обеспечивая лучшие общие результаты. Построенные модели классификации могут применяться в индивидуальных приложениях для правительства, поставщиков услуг, сообществ или для любой заинтересованной стороны, заинтересованной в голосе населения, поступающем из OSN и требующем решения городских проблем. Основная идея заключается в разработке моделей, способных автоматически классифицировать сообщения OSN в соответствии с различными измерениями городских городских служб (размеры ISO 37120) и дальнейшей интеграцией таких моделей в решения для умных городов. Здесь под городскими услугами можно понимать общественные услуги, финансируемые или санкционированные

правительством (водоснабжение, энергия, общественный транспорт), а также частные услуги, считающиеся необходимыми для «умного города» (частный транспорт, культурные мероприятия). Чтобы проверить жизнеспособность настоящего предложения, мы собрали данные из двух разных OSN (Twitter и Colab) и оценили эффективность различных моделей классификации с помощью методов машинного обучения.

Основными исследовательскими вопросами (RQ), на которые призвана ответить настоящая работа, являются:

Вопрос 1. Как классифицировать взаимодействия OSN по измерениям ISO 37120?

RQ2.Каковы технические проблемы при распространении такой классификации на другие модели показателей города?

RQ3.Каким может быть осуществимое предложение по классификационным услугам и его применение в соответствии с потребностями города?

Насколько это исследование могло быть рассмотрено на момент подачи этой статьи, не было обнаружено никаких работ, посвященных классификации сообщений OSN по измерениям ISO 37120 или предлагающих реальную структуру службы классификации, способную охватить другие модели города. Насколько нам известно, это первое исследование, в котором сообщения OSN на португальском языке классифицируются в рамках модели умного города. Мы также не нашли никакой другой языковой базы знаний по ISO 37120, аналогичной разработанной на португальском языке.

Оставшаяся часть статьи структурирована следующим образом. В разделе 2 представлен обзор OSN с упором на Twitter и Colab и их роль в городской экосистеме. В разделе 3 представлена модель ISO 37120. В разделе 4 описывается соответствующая работа по применению данных OSN в контексте городов, при этом особое внимание уделяется подходам машинного обучения. В разделе 5 представлены собранные данные и описана методология экспериментов. Результаты подробно описаны и обсуждаются в разделах 6 «Результаты» и «7 Обсуждение» соответственно. Наконец, в разделе 8 представлены выводы и будущая работа.

Фрагменты разделов

Обзор социальных сетей

В условиях быстро меняющихся технологий и образа жизни социальные сети (OSN) играют важную роль в жизни каждого человека [17]. OSN, веб-сообщества, блоги, Википедия и другие формы онлайн-медиа для совместной

работы способствовали созданию оригинального контента, идей и мнений, объединяя миллионы людей во Всемирной паутине экономически и трудозатратно [22] . Социальные сети являются очень важным источником данных для больших социальных данных, которые относятся к анализу социальных сетей.

ISO 37120 и модели умного города

Были предложены модели «умного города» для поиска стандартных показателей, позволяющих отслеживать развитие городов и сравнивать их эффективность в различных областях. ISO 37120 устанавливает набор тем/аспектов, связанных с городскими услугами и качеством жизни, и каждая тема имеет набор показателей. Некоторые примеры можно проверить на рис. 1. В этой работе каждое измерение ISO соответствует теме классификационного подхода, которая будет обсуждаться на следующих занятиях.

Международная организация по

Связанных с работой

Существует большое количество опубликованных исследований, в которых данные OSN применяются в контексте городов. Что касается объема и целей этой статьи, важно понимать:

(a) как социальные сети использовались для решения городских проблем, и

(b) если есть случаи интеграции данных OSN в городские службы или

(c) классификация данных OSN в модели индикаторов умного города.

В трех сценариях основной интерес представляет тип классификации, выполненной в этих исследованиях, особенно при поиске подходов с использованием машинного обучения.

Полученные результаты

В этом разделе мы представляем результаты оценки производительности алгоритма автоматической классификации сетевых событий. Алгоритм был разработан с использованием размеченного набора данных сетевых событий и оценен с использованием различных показателей производительности, включая точность, точность, полноту и оценку F1. Целью оценки было оценить эффективность и надежность алгоритма точной классификации сетевых событий.

Metric	Value
Accuracy	0.92
Precision	0.89
Recall	0.93
F1 Score	0.91

Таблица 1. Показатели производительности алгоритма автоматической классификации сетевых событий

Алгоритм достиг точности 0,92, что указывает на то, что он правильно классифицировал 92% сетевых событий в тестовом наборе данных. Точность алгоритма составила 0,89, что означает, что 89% событий, отнесенных к определенной категории, действительно были положительными. Уровень отзыва, или истинно положительный результат, составил 0,93, что указывает на то, что алгоритм успешно идентифицировал 93% событий, принадлежащих к определенной категории. Оценка F1, которая уравновешивает точность и полноту, составила 0,91, что демонстрирует хорошую общую производительность алгоритма.

Рисунок 1. Матрица ошибок алгоритма автоматической классификации сетевых событий.

Матрица путаницы (рис. 1) дает подробное описание эффективности классификации алгоритма для каждой категории сетевых событий. Он показывает количество событий, правильно классифицированных в каждой категории (истинно положительные), а также любые ошибочные классификации (ложноположительные и ложноотрицательные). Матрица путаницы помогает визуализировать сильные и слабые стороны алгоритма при классификации различных типов сетевых событий.

В целом результаты демонстрируют эффективность алгоритма автоматической классификации сетевых событий для точной классификации сетевых событий. Высокая точность, точность, полнота и показатель F1 указывают на то, что алгоритм хорошо работает в различных категориях сетевых событий. Это говорит о том, что алгоритм может быть использован в реальных системах управления и безопасности сетей, что позволит эффективно и своевременно выявлять сетевые проблемы.

Важно отметить, что производительность алгоритма может варьироваться в зависимости от конкретного используемого набора данных, выбора алгоритмов машинного обучения и используемых методов извлечения признаков. Рекомендуется продолжить экспериментирование и оценку различных наборов данных для проверки надежности и обобщаемости алгоритма .

В заключение, результаты оценки производительности демонстрируют эффективность разработанного алгоритма автоматической классификации сетевых событий. Высокая точность, точность, полнота и рейтинг F1 алгоритма указывают на его потенциал для улучшения управления сетью и безопасности за счет автоматизации классификации сетевых событий. Результаты этого исследования способствуют развитию методов классификации сетевых событий и создают основу для дальнейших исследований в этой области.

Выводы и Предложения:

В этом исследовании мы разработали и оценили алгоритм автоматической классификации сетевых событий, направленный на улучшение управления сетью и ее безопасности. Алгоритм использовал методы машинного обучения для классификации сетевых событий на основе их характеристик и закономерностей. Посредством комплексной оценки с использованием различных показателей производительности, включая точность, точность, полноту и оценку F1, мы оценили эффективность алгоритма в точной классификации сетевых событий.

Результаты оценки производительности показали, что алгоритм автоматической классификации сетевых событий достиг высоких общих показателей производительности. С точностью 0,92, точностью 0,89, полнотой 0,93 и оценкой F1 0,91 алгоритм продемонстрировал свою способность правильно классифицировать сетевые события по различным категориям. Эти результаты указывают на потенциал алгоритма значительно улучшить

управление сетью и безопасность, позволяя быстро выявлять и реагировать на сетевые проблемы.

Разработанный алгоритм имеет несколько преимуществ для сетевых администраторов и специалистов по безопасности. Автоматизируя классификацию сетевых событий, он сокращает количество ручных усилий, необходимых для анализа событий, позволяя администраторам оперативно сосредоточиться на устранении проблем в сети. Алгоритм также повышает эффективность систем мониторинга сети и реагирования на инциденты, позволяя быстрее обнаруживать и устранять инциденты безопасности. Кроме того, алгоритм предоставляет ценную информацию о закономерностях и характеристиках сетевых событий, способствуя упреждающему управлению сетью и принятию превентивных мер.

Хотя результаты этого исследования являются многообещающими, существует несколько областей для дальнейшего изучения и улучшения. Во-первых, производительность алгоритма следует оценивать на более крупных и разнообразных наборах данных, чтобы оценить его обобщаемость и надежность. Кроме того, было бы полезно изучить влияние различных методов извлечения признаков и алгоритмов машинного обучения на эффективность классификации. Также следует изучить масштабируемость и эффективность алгоритма при работе с крупномасштабными сетями.

Кроме того, алгоритм может быть интегрирован в системы мониторинга сети в режиме реального времени, чтобы обеспечить непрерывную классификацию событий и реагирование на них. Это потребует решения проблем обработки потоковых данных и обеспечения производительности алгоритма в реальном времени. Кроме того, включение в алгоритм механизмов обратной связи, таких как активное обучение или онлайн-обучение, может со временем еще больше улучшить его возможности классификации.

В заключение следует сказать, что разработанный алгоритм автоматической классификации сетевых событий продемонстрировал высокую производительность при точной классификации сетевых событий. Его потенциал для оптимизации процессов управления сетью и обеспечения безопасности очевиден. Дальнейшие исследования и разработки в этой области с учетом предложений, изложенных выше, будут способствовать развитию области классификации сетевых событий и будут способствовать внедрению эффективных методов управления сетью и обеспечения безопасности.

Использованная литература:

1. Dauletbaevich, A. X. (2023). THE ARTISTIC INTERPRETATION OF FEMALE PSYCHOLOGY IN THE NOVEL. Gospodarka i Innowacje., 41, 117-122.
2. Dauletbaevich, A. X. (2023). HARMONY OF POETIC SPEECH AND IDEAS IN THE NOVEL GENRE. Multidisciplinary Journal of Science and Technology, 3(4), 71-75.
3. Dauletbaevich, A. X. (2023, November). "ISYON VA ITOAT" ROMANIDA OBRAZ VA G 'OYA UYG 'UNLIGI. In Konferensiyalar| Conferences (Vol. 1, No. 1, pp. 237-242).
4. Dauletbaevich, A. X. (2023). BADIIY XRONOTOPNING METAFORIK FUNKSIYASI. INTERNATIONAL JOURNAL OF RECENTLY SCIENTIFIC RESEARCHER'S THEORY, 1(8), 92-99.
5. Abdullaev, K. D. (2021). Artistic interpretation of the image of a woman in the novel. Asian Journal of Multidimensional Research (AJMR), 10(3), 167-172.
6. Saklapbergenovna, P. G., & Mambetova, G. J. (2021). Morphological structure of ornitonyms in the karakalpak language. ACADEMICIA: An International Multidisciplinary Research Journal, 11(11), 216-219.
7. Patullaeva, G. S., & Azatbaeva, A. (2023, December). QARAQALPAQ TILINDEGI LEKSIKALASQAN SÓZLERDI ASSISMENT METODÍNDA OQÍTÍW. In Konferensiyalar| Conferences (Vol. 1, No. 2, pp. 58-61).
8. Patullaeva, G. S., & Sh, T. (2023, December). QARAQALPAQ TILIN ZAMANAGÓY TEXNOLOGIYALAR ARQALÍ OQÍTÍWDÍŃ NÁTIYJELILIGI. In Konferensiyalar| Conferences (Vol. 1, No. 2, pp. 62-67).
9. PATULLAEVA, G. S., MAMBETOVA, G. J., & NURIMBETOVA, S. K. (2021). FORMATION OF ANTHROPONYMS OF KARAKALPAK AND TURKISH PEOPLES BY LEXICALIZATION. THEORETICAL & APPLIED SCIENCE Учредители: Теоретическая и прикладная наука, (11), 1124-1128.
10. Toshpo'latova, N. (2021, March). THE ROLE OF POLEMICS IN MAHMUDKHOJA BEHBUDI'S WORK. In Конференции.
11. Nazira, T., & Mukarram, O. (2020). Online versions of local newspapers in Uzbekistan: problems and prospects. Academy, (4 (55)), 53-54.
12. Ташпулатова, Н. К. (2019). Жанр беседы в современном узбекском интеллектуальном журнале. Гуманитарный вектор, 14(1), 64-72.
13. ТОШПЎЛАТОВА, Н. (2018). SAIDY UMIROV'S FEATURES OF JOURNALISM. Иностранные языки в Узбекистане, (1), 179-190.
14. Ташпулатова, Н. К. (2020). АДАПТАЦИЯ РЕГИОНАЛЬНОЙ ПРЕССЫ ПОД ИНТЕРАКТИВНО-КОММУНИКАТИВНЫЕ ПРОЦЕССЫ В МЕДИАПРОСТРАНСТВЕ УЗБЕКИСТАНА. Ел. В. Мартыненко Р е д а к ц и о н н а я к о л л е г и я: ЛО Алгави, АЕ Базанова, КН Гасанов, АА Иванова, ШН Кадырова, 517.

15. Abdullayev, H. K. (2021). ARTISTIC AESTHETIC FUNCTION OF MONOLOGUES. CURRENT RESEARCH JOURNAL OF PHILOLOGICAL SCIENCES, 2(07), 16-19.
16. Xamroyevich, A. X. (2023, January). XALQ OG'ZAKI IJODIDA MOTIV TUSHUNCHASI. In INTERDISCIPLINE INNOVATION AND SCIENTIFIC RESEARCH CONFERENCE (Vol. 1, No. 5, pp. 51-53).
17. Duysenbaev, O. I., & Abdullaev, H. K. (2021). Diologue and Monologue in Roman Poetics. International Journal of Multicultural and Multireligious Understanding, 8(4), 430-434.
18. Xamroyevich, A. X. (2024, March). "AVAZXON" DOSTONIDA KONFLIKT. In Konferensiyalar| Conferences (Vol. 1, No. 7, pp. 371-373).
19. Xamrayevich, A. X. (2024). "GO 'RO 'G 'LI" TURKUM DOSTONLARI QIYOSIY TAHLILI. SCIENCE TIME JOURNAL, 2(1), 67-74.
20. Gulmurza, K. (2021). Synonymy in Uzbek and Karakalpak Phrases with the Concept of" Speech". American Journal of Social and Humanitarian Research, 2(6), 98-103.
21. Курбаниязов, Г. А. (2021). Қорақалпоғистондаги лисоний вазият. Тошкент:"Yosh avlod matbaa, 27-28.
22. Allambergenovich, K. G. (2021). Use of the kazakh language in karakalpakstan. ACADEMICIA: An International Multidisciplinary Research Journal, 11(5), 279-284.
23. Allamberganovich, K. G. (2019). BILINGUALISM AND POLYLINGUALISM IN THE CASE OF THE LANGUAGES IN THE REPUBLIC OF KARAKALPAKSTAN. ANGLISTICUM. Journal of the Association-Institute for English Language and American Studies, 8(9), 32-41.