УДК 621.396.06 Обзорная статья

https://doi.org/10.32603/2071-8985-2024-17-9-35-45

Обоснование требований к системе мониторинга социальных сетей (на основе опыта их обслуживания)

В. М. Тайц✉, Н. А. Жукова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, СПИИРАН, Санкт-Петербург, Россия

✉ taizvadim@gmail.com

Аннотация. Анализируется специфика социальных сетей как объектов мониторинга. Представлен анализ возможностей программных средств, используемых для мониторинга этих сетей, а также проводимых исследований по их совершенствованию. Отмечается, что известные подходы к мониторингу социальных сетей не в полной мере учитывают их особенности. Формулируются требования к перспективным системам мониторинга этих сетей на основе анализа структуры социальных сетей и возможностей программных средств. Выделяются основные элементы, подлежащие мониторингу. Предъявляются требования к частоте сбора данных, а также к прогнозированию событий в социальных сетях.

Ключевые слова: социальные сети, угрозы, анализ, требования, система мониторинга

Для цитирования: Тайц В. М., Жукова Н. А. Обоснование требований к системе мониторинга социальных сетей (на основе опыта их обслуживания) // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 9. С. 35–45. doi: 10.32603/2071-8985-2024-17-9-35-45.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Review article

Justification of Requirements for a Social Network Monitoring System (Based on Experience in their Maintenance)

V. M. Taits✉, N. A. Zhukova

SPIIRAS of Saint Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, Russia

✉ taizvadim@gmail.com

Abstract. Analyzes the specifics of social networks as monitoring objects. An analysis of software tools used to monitor such networks is carried out, along with a review of research attempts to improve them. It is noted that the existing approaches to monitoring social networks fail to take their specific features into account. Requirements for prospective monitoring systems for such networks are formulated based on an analysis of the structure of social networks and the capabilities of software tools. The main elements to be monitored are identified. Requirements for the frequency of data collection, as well as for forecasting events in social networks, are formulated.

Keywords: social networks, threats, analysis, requirements, monitoring system

For citation: Taits V. M., Zhukova N. A. Justification of Requirements for a Social Network Monitoring System (Based on Experience in their Maintenance) // LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 9. P. 35–45. doi: 10.32603/2071-8985-2024-17-9-35-45.

Conflict of interest. The authors declare no conflicts of interest.

Введение. Социальные сети за последние десятилетия стали неотъемлемой частью повседневной жизни миллиардов людей по всему миру. Они преобразовали способы общения, позволяют делиться информацией, устанавливать бизнес-контакты и даже участвовать в социальных и политических процессах. Сегодня сложно представить себе общество без влияния ВКонтакте, ТикТок, Телеграм, Яндекс.Дзен и им подобных платформ. Эти цифровые пространства открыли новые горизонты для межличностного взаимодействия, предоставляя пользователям мощные инструменты для самовыражения и самореализации. Они стимулируют не только личные, но и коллективные действия, позволяя объединяться ради общих интересов и целей. Социальные сети играют ключевую роль в формировании общественного мнения, распространении новостей и поддержании культурных связей, что делает их важным объектом исследования и понимания современных социальных динамик.

Однако со стороны социальных сетей пользователи могут подвергаться различным угрозам, начиная от негативного психологического воздействия и заканчивая мошенничеством и распространением фейковых новостей. Для минимизации этих рисков и создания безопасной среды необходимо своевременное выявление и предотвращение таких угроз.

Не менее важно анализировать внутренние составляющие социальных сетей. В частности, программные сбои, отказ серверной инфраструктуры могут приводить к прямым экономическим убыткам (снижению дохода от рекламы и от других мероприятий). Такие сбои могут доставлять неудобство пользователям, рассчитывающим на оперативный доступ к определенной информации в профессиональных и других целях.

Обеспечение устойчивого функционирования социальных сетей гарантирует быструю и бесперебойную работу сервисов. В интересах этого могут применяться различные системы их мониторинга [1] и мероприятия по предотвращению потерь хранимых информационных ресурсов.

На текущий момент при мониторинге социальных сетей применяется ряд известных методов сбора и обработки данных [2]–[4]. Несмотря на их достоинства, они не в полной мере учитывают уникальные особенности функционирования социальных сетей, в том числе влияние деятельности пользователей на сами сети. Нет четких рекомендаций по периодичности мониторинга состояния социальных сетей в различных условиях и по целесообразным подходам к прогнозированию их состояний.

Цель данной статьи заключается в формулировании требований к перспективным системам мониторинга социальных сетей.

Постановка задачи. Для достижения поставленной цели эти сети сначала анализируются как объекты мониторинга. Затем критически рассматриваются известные системы мониторинга социальных сетей, после чего формулируются требования к перспективным системам мониторинга таких сетей.

Социальные сети как объекты мониторинга. Социальные сети с точки зрения мониторинга сочетают в себе особенности как высоконагруженного сервиса – мониторинг жестких дисков и загрузки сети и т. п., так и реальной среды, в которой взаимодействуют пользователи. Угрозы могут касаться непосредственно пользователей в случае предоставления оскорбительного или провокационного содержимого, а также серверной инфраструктуры. Атаки на серверную инфраструктуру могут быть как умышленными (ddos-атаки, попытки неправомерного получения доступа и/или распространения вирусов и др.), так и естественными (устаревание и выход из строя жестких дисков, большая нагрузка на инфраструктуру, связанная с каким-то событием, проблемы на линии связи и др.).

Когда речь заходит о системе, насчитывающей свыше 20 тыс. серверов и более 100 тыс. жестких дисков, а также свыше 50 млн активных пользователей в день, мониторинг превращается в сложнейший процесс, требующий высочайшего уровня организации и использования передовых технологий. Такой масштаб влечет за собой огромную сложность сетевой инфраструктуры, вариативность аппаратного и программного обеспечения, а также необходимость учета многих параметров работы системы в реальном времени.

Сеть состоит из различных кластеров серверов, географически удаленных друг от друга. Каждый сервер включает в себя несколько носителей данных (hdd и ssd), их функционирование обеспечивается системным ПО и драйверами. Такие серверы обеспечивают хранение данных и доступ к ним.

Отрицательные воздействия на отдельные серверы в кластере могут распространяться и вызывать цепную реакцию, поражая другие серверы, что в свою очередь приводит к ухудшению работы всей сети. Это может проявляться в виде увеличенной нагрузки на соседние узлы при выходе одного из них из строя, замедлении обработ-

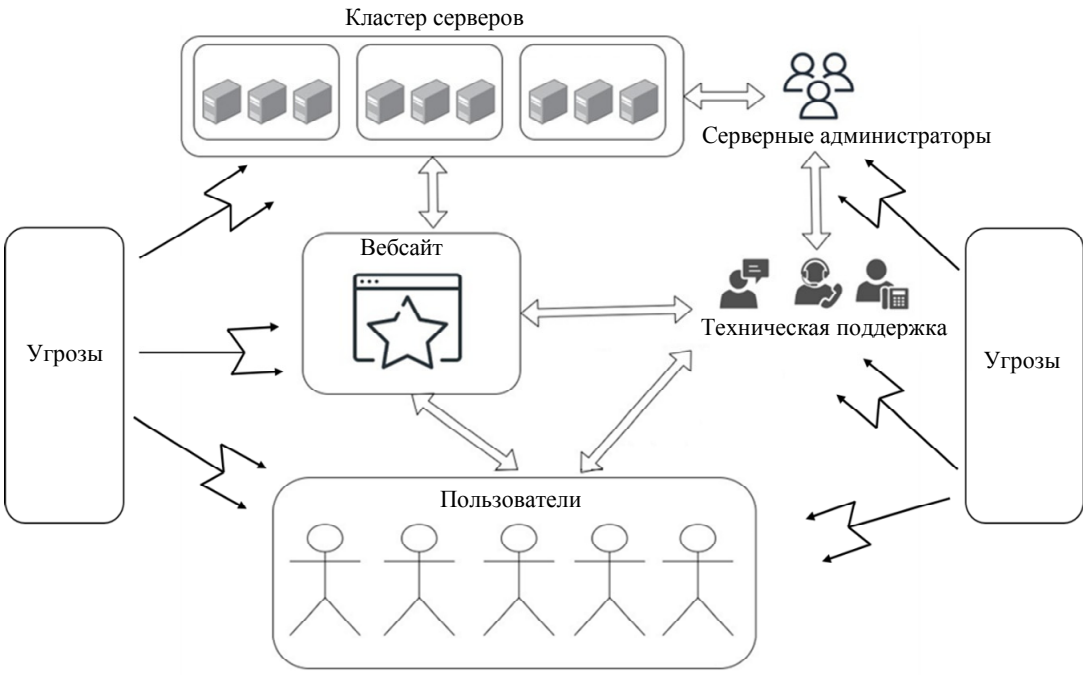
ки данных, увеличении времени отклика и, в крайних случаях, к полному отказу услуг. Такие ситуации негативно сказываются на общей доступности и надежности сетевых сервисов, подчеркивая необходимость реализации продуманной стратегии отказоустойчивости и восстановления после сбоев. Данные о состоянии серверов, кластеров и сети важны для прогнозирования сбоев и расследования инцидентов при их возникновении.

В процессе работы сети в связи с расширением бизнеса, природными явлениями или другими факторами возможна переконфигурация сети. Этот процесс может включать в себя добавление нового сервера в кластер при высокой нагрузке на него, замену одного из жестких дисков при его выходе из строя, переезд в другой дата-центр по экономическим причинам, обновление ПО с целью модернизации или устранения неполадок. Возможные ошибки конфигурации, попадание вирусов в процессе обновления или попытки неправомерного доступа к конфиденциальной информации со стороны серверных администраторов также оказывают существенное негативное воздействие на социальную сеть в целом, поэтому данные об управляющих воздействиях также представляют неотъемлемую часть данных мониторинга.

К особенностям социальной сети относится то, что источником негативного воздействия на сеть могут стать не только ее внутренние сотрудники, но и конечные пользователи. Причем воздействия не обязательно могут быть злонамеренными. Например, нагрузка на сеть может вызываться намеренной отправкой большого числа запросов со стороны пользователя, но может быть и стихийной – если пользователь, имеющий более 200 тыс. подписчиков, размещает новый пост, это может вызвать массовый поток запросов к серверу, поскольку большое количество людей захотят просмотреть опубликованный контент. Аналогичная ситуация также касается сообществ пользователей. Поэтому такие данные, как имя пользователя или сообщества, количество друзей и подписчиков, язык, активность, тематика и количество реакций на постах также важны для мониторинга социальной сети.

Однако негативные воздействия могут касаться не только серверной инфраструктуры, но и самих конечных пользователей, например прямые оскорбления и угрозы могут оказывать негативный эффект на их эмоциональное состояние. Возникают также ситуации, которые отследить не так легко, как обращения к пользователям напрямую. Например, посты, содержащие псевдомедицину, инструкции по некорректному обращению с электроприборами или финансовыми вложениями, могут побуждать пользователей к действиям, ведущим к негативным последствиям, даже если автор поста позиционировал его как шутку. Поэтому помимо вышеперечисленных параметров важны также содержимое постов и жалобы на пользователя/сообщество/пост/комментарий.

В обобщенном виде на уровне элементов структуру социальной сети можно представить в виде рисунка.



Обобщенная структура социальной сети
Generalized structure of a social network

Важно также понимать, что система мониторинга сама по себе – достаточно сложная подсистема, требующая своих вычислительных ресурсов и баз для хранения данных, а также создающая нагрузку на основную систему при сборе данных. Данные, собранные системой мониторинга, занимают огромные дисковые пространства. Очевидно, что есть разница в том, насколько часто нужно собирать параметры сервера, хранящего новую информацию, в которой заинтересована значительная часть пользователей, и сервера, хранящего фотографии 10-летней давности. Также пользователи, имеющие огромную аудиторию, намного интереснее с точки зрения мониторинга, чем пользователи, изредка контактирующие со своими родственниками. Поэтому экономическая целесообразность использования систем мониторинга неразрывно связана с их оптимизацией и возможностью легкой интеграции.

Существуют неявные закономерности в работе серверов и кластеров, действиях серверных администраторов и активности пользователей, которые могут оставаться невидимыми для человека из-за огромного количества параметров и сложности их взаимодействий. Грамотно настроенная система мониторинга способна собирать обширные и многогранные данные о состоянии инфраструктуры, которые, в свою очередь, могут служить входными данными для нейронной сети. Использование искусственного интеллекта и машинного обучения позволяет анализировать эти данные, выявлять скрытые взаимосвязи и тенденции, предсказывать возможные сбои и негативные воздействия на пользователей и оптимизировать работу системы в целом, что значительно повышает эффективность управления ИТ-инфраструктурой.

Анализ программных решений для мониторинга социальных сетей. Популярные программные решения, релевантные мониторингу социальных сетей, можно разделить на следующие категории:

• Инструменты мониторинга работы сетевых устройств и серверов, которые могут отслеживать доступность сервисов, использование пропускной способности, нагрузку на серверы и многое другое (системы Zabbix, PRTG Network Monitor, SolarWinds, OpenNMS, The Dude и др.).

• Инструменты мониторинга производительности и метрик приложений, которые фокусируются на отслеживании и анализе производительности приложений и серверов (Prometheus, Munin, Nagios, Icinga, ManageEngine и др.).

• Инструменты централизованного сбора и анализа логов из различных источников (IBM QRadar, RSYSLOG и др.).

• Инструменты обработки событий и оповещения о событиях в реальном времени (Sensu, Riemann, Alerta и др.).

• Инструменты отслеживания и анализа упоминаний брендов, продуктов, услуг или конкретных ключевых слов в социальных медиа- и других онлайн-платформах, которые предоставляют аналитику по тональности упоминаний, вовлеченности аудитории, демографическим характеристикам и географическому распределению (IQBuzz, Hootsuite, Popsters, Socialbakers, Semanticforce, Mediatoolkit и др.).

• Инструменты для анализа текста и выявления в нем потенциально нежелательного контента – оскорблений, призывов к ненависти, мошенничества и дезинформации, фальсификации новостей (DeepText, Perspective API, Community Sift, Crisp Thinking, IBM Watson Natural Language Understanding, Symanto Insights Platform, Logically, Cortical.io Contract Intelligence, SAS Text Analytics и др.).

Минус известных решений состоит в отсутствии комплексного анализа инцидентов и обнаружения аномалий с учетом управляющих воздействий, не связанных непосредственно с предметной областью (социальная сеть). Также не учитываются управляющие воздействия, не связанные с серверной инфраструктурой – такие, как публикации постов и комментариев.

Анализ теоретических исследований мониторинга социальных сетей. В интересах систематизации известные исследования можно разделить на несколько групп. Исследования [5]–[10] описывают подходы и программные средства (ПС) мониторинга компьютерных сетей и серверов, кластеров серверов в контексте сбора данных, а также простых способов определения аномалий на основе пороговых значений. Исследования [11]–[22] также предлагают механизмы определения аномалий и реакцию на них на основе простых механизмов – сравнение текущих значений параметров с пороговыми и т. п. Исследования [23]–[28] также используют компьютерные сети и кластеры серверов, но предлагают методы определения аномалий, основываясь на анализе временных рядов данных мониторинга. В ис-

следованиях [29]–[31] также анализируются управляющие воздействия на кластеры серверов. Исследования [32]–[37] описывают модели мониторинга различных областей с динамичными часто обновляющимися данными. Также в [33] проводится анализ естественного языка, трендов, а также поведения пользователей социальной сети для прогнозирования возможности знакомства пользователей друг с другом. В [2]–[4] анализируется поведение пользователей социальной сети для выявления аномалий в их активности. В [38]–[40] проводятся нейропрогнозирование нагрузки на сеть и сравнительный анализ различных методов нейропрогнозирования.

Из анализа видно, что такие локальные задачи, как мониторинг состояния серверов, анализ поведения пользователей и отслеживание трендов, хорошо проработаны, однако недостатком служит отсутствие комплексного анализа, учитывающего все составляющие социальной сети, позволяющего выявлять неявные закономерности между поведением пользователей, трендами и серверной инфраструктурой.

В связи со всем вышеуказанным требуется разработка методов, учитывающих особенности социальной сети и влияния действий пользователей на состояние серверов и на самих пользователей с учетом отслеживания трендов и обнаружения аномалий по временным рядам.

Требования к элементам социальных сетей, подлежащим мониторингу. Исходя из анализа структуры работы социальной сети на основе опыта работы с системами их мониторинга, можно выделить следующие элементы, подлежащие мониторингу:

• Жесткие диски: важно отслеживать их состояние, используя метрики SMART [41] и другие индикаторы, чтобы предотвратить потерю данных из-за отказа оборудования.

• Серверы: мониторинг серверов включает проверку их доступности, загрузки CPU, использования оперативной памяти и других системных параметров.

• Кластеры серверов: отслеживание статуса и производительности кластеров серверов помогает обеспечить высокую доступность и масштабируемость сервисов социальной сети.

• Сеть: мониторинг сетевых параметров – пропускной способности, задержек, ошибок и потерь пакетов, необходим для поддержания качественной связи между компонентами инфраструктуры.

• Пользователи/сообщества: анализ активности пользователей и сообществ позволяет оценить воздействия на других пользователей социальной сети.

• Посты пользователей/сообществ: мониторинг публикаций помогает анализировать контент и оперативно предотвращать возможные инциденты.

• Комментарии пользователей: аналогично публичным постам, комментарии также являются публичными высказываниями, которые могут оказывать воздействие на других пользователей.

Должен также осуществляться мониторинг следующих действий в социальных сетях:

• Добавление/извлечение жесткого диска: требует немедленного мониторинга, чтобы убедиться в корректности расширения или уменьшения хранилища данных.

• Добавление/отключение кластера серверов: напрямую влияет на производительность и доступность сервисов, должно сопровождаться анализом их воздействия на нагрузку и балансировку системы.

• Обновление ПО: может иметь как положительный эффект с точки зрения устранения проблем старых версий, так и отрицательный в случае попадания нежелательного ПО на какие-то элементы сети.

• Отправка публичного поста пользователем/сообществом: мониторинг публикаций важен для управления контентом и предотвращения распространения нежелательной информации.

• Отправка комментария пользователем/сообществом: аналогично отправке публичного поста.

Требования по частоте сбора данных. Каждый элемент мониторинга можно отнести к одной трех из категорий:

1. *Критические элементы*: для элементов этой категории требуется наивысший уровень внимания, поскольку любой сбой или проблема в их функционировании может иметь серьезные последствия. К примеру, серверы, предоставляющие данные о последних событиях, или пользователи с широкой аудиторией могут требовать непрерывного активного мониторинга, включая частые опросы для проверки доступности и производительности. Издержки, связанные с мониторингом таких важных ресурсов, считаются оправданными, учитывая их значение для обеспечения стабильности системы и удовлетворенности пользователей. Для таких элементов оптимальным интервалом сбора данных является 1–5 мин.

2. *Элементы среднего уровня критичности*: для элементов этой категории требования к мониторингу менее строгие, и его можно выполнять с меньшей частотой. Возможно использование пассивного мониторинга – например, анализа системных журналов, что позволяет выявлять потенциальные проблемы на основе анализа естественно генерируемых данных. Это может касаться пользователей со средней степенью активности и серверов, содержащих данные, которые используются не так часто, но важны для определенной части аудитории – например, личные фотографии пользователей. Для таких элементов оптимальный интервал сбора данных – 1–3 ч.

3. *Некритические элементы*: компоненты, попадающие в эту категорию, имеют наименьшую значимость для непрерывности бизнес-процессов и пользовательского опыта. Мониторинг таких элементов может осуществляться с минимальной частотой, поскольку их отказ оказывает незначительное влияние на общую работоспособность системы. Это могут быть устаревшие данные, редко запрашиваемые пользователем, или аккаунты с низкой социальной активностью. Пониженный приоритет позволяет сократить затраты на мониторинг и оптимизировать ресурсы, выделяемые под эти задачи. Для таких элементов оптимальный интервал сбора данных – 1 сутки.

Требования к прогнозированию состояний социальных сетей. Исходя из анализа структуры работы социальной сети, а также связанных исследований, можно выделить следующие требования к методам нейропрогнозирования социальных сетей:

• Обработка временных рядов, так как при анализе социальных сетей важно учитывать динамику взаимодействия пользователей с течением времени.

• Работа с большими объемами данных.

• Анализ в реальном времени для оперативного реагирования на изменения в поведении пользователей и серверной инфраструктуры.

• Автоматическое обнаружение аномалий, которые могут указывать на мошенничество, спам, вирусы, износ оборудования и другие виды нежелательной активности.

• Проактивное обслуживание аномалий для предотвращения или устранения проблем, возникающих из-за аномалий, например автоматическая блокировка подозрительных аккаунтов или добавление серверов в высоконагруженный кластер.

• Обработка естественного языка для анализа семантики и эмоциональной окраски сообщений.

• Работа с неструктурированными данными, так как в социальных сетях большая часть информации представлена в неструктурированном виде – тексты, изображения, видео.

• Понимание динамики распространения информации.

• Прогнозирование поведения пользователей для анализа вредоносности того или иного информационного ресурса.

• Учет социальных связей, так как в анализе необходимо учитывать сетевые структуры и связи между пользователями, поскольку они влияют на распространение информации и формирование мнений.

• Непрерывная адаптируемость и обучаемость для более точного прогнозирования с учетом трендов и текущих тенденций.

По глубине прогнозирования информационные ресурсы социальных сетей можно разделить на 3 категории:

1. *Краткосрочное прогнозирование* применимо для решения таких задач, как управление нагрузкой на серверы, распределение сетевого трафика, планирование краткосрочных окон в моменты, когда ожидается минимальная нагрузка на систему. Также оно применимо для модерации содержимого на выявление мошенничества, спама или оскорблений. Оптимальное время прогнозирования для таких ресурсов – от 1 до 3 ч.

2. *Среднесрочное прогнозирование* применимо для планирования обновлений, замены оборудования, анализа трендов для прогнозирования нагрузки на систему, анализа влияния публикаций на пользователей. Оптимальное время прогнозирования для таких ресурсов – от недели до месяца.

3. *Долгосрочное прогнозирование* применимо для таких задач, как планирование добавления новых серверов и кластеров, планирование нагрузки на систему, связанной с повышением числа активных пользователей, прогнозирование потребности в специалистах для поддержания и развития инфраструктуры. Оптимальное время прогнозирования для таких ресурсов – от месяца до года.

Требования к механизмам сбора и агрегации данных. Неотъемлемый этап успешного применения нейронных сетей – это качественный сбор данных мониторинга и их организация в виде временных рядов. Для формирования временных рядов с учетом вышеперечисленных тре-

Результаты сравнения систем мониторинга
Comparison of monitoring systems

Системы мониторинга	Критерии для сравнения							
	1	2	3	4	5	6	7	8
Zabbix, PRTG Network Monitor, SolarWinds, OpenNMS, The Dude	+	+	+	–	+	+	+	+
Prometheus, Munin, Nagios, Icinga, ManageEngine	+	+	+	–	+	+	+	–
IBM QRadar	+	+	+	–	+	+	+	+
RSYSLOG	–	+	+	–	–	+	–	–
Sensu, Riemann, Alerta	–	–	+	–	–	–	+	+
IQBuzz, Hootsuite, Popsters, Socialbakers, Semanticforce и Mediatoolkit	–	+	–	+	+	–	+	–
DeepText, Perspective API, Community Sift, Crisp Thinking, IBM Watson Natural Language Understanding, Symanto Insights Platform, Logically, Cortical.io Contract Intelligence, SAS Text Analytics	–	+	–	+	+	–	+	+

бований система мониторинга должна также иметь следующие возможности:

• Активный сбор данных – процесс, при котором система мониторинга инициирует сбор информации. Такой способ сбора данных подходит для критических элементов и элементов средней критичности по частоте сбора данных.

• Пассивный сбор данных – процесс, при котором система мониторинга оперирует данными, сгенерированными в процессе работы системы. Примерами пассивного мониторинга могут быть прослушивание сетевых портов или сбор лог-файлов. Такой подход позволяет минимизировать нагрузку на систему, что делает его более подходящим для некритичных элементов по частоте сбора данных.

• Агрегация данных из базовых детализированных данных – метрик производительности, статусов системных процессов и др., из разных источников в более обобщенные блоки данных для упрощения анализа данных и сокращении объема хранимых данных.

• Формирование временных рядов для возможности отслеживания динамики изменений и предсказания будущего поведения систем.

Анализ возможностей программных средств. Исходя из анализа, можно выделить следующие критерии для сравнения существующих систем мониторинга:

1. Возможность активного сбора данных.
2. Возможность пассивного сбора данных.
3. Возможность мониторинга серверной инфраструктуры.
4. Возможность обработки естественного языка.
5. Возможность агрегации данных.
6. Возможность формирования временных рядов.
7. Анализ в реальном времени.
8. Автоматическое обнаружение аномалий.

Для удобства анализа систем мониторинга эти критерии сведены в таблицу.

Выводы. Из анализа существующих систем мониторинга видно, что они способны решать множество разнообразных задач. Их комплексное применение позволяет обеспечить формирование временных рядов серверной инфраструктуры, а также отслеживание трендов и части активности пользователей.

Однако также стоит отметить отсутствие интегрированных решений, направленных на анализ влияния активности пользователей на серверную инфраструктуру, что необходимо для прогнозирования угроз и принятия мероприятий по преждевременному их устранению. Поэтому требуется разработка программного решения, учитывающего особенности социальной сети и влияния действий пользователей на состояние серверов и на самих пользователей.

Заключение. В данной статье была представлена структура взаимодействий крупной социальной сети, позволяющая понять динамику и механизмы взаимодействия между пользователями и информационными ресурсами. Выделены ключевые ресурсы, требующие непрерывного мониторинга, включая активность пользователей, нагрузку на серверную инфраструктуру и распространение контента. Были предложены требования к реализации систем мониторинга социальных сетей, включая оптимальное время мониторинга различных элементов, оптимальную глубину и точность прогнозирования различных событий, в процессе эксплуатации социальной сети.

Список литературы

1. Что такое мониторинг и его уровни / Журн. VK Cloud об IT-бизнесе, технологиях и цифровой трансформации. URL: https://cloud.vk.com/blog/chto-takoe-monitoring-i-ego-urovni (дата обращения: 25.09.2024).

2. A statistical approach to social network monitoring / E. M. Farahani, R. Baradaran Kazemzadeh, R. Noorossana, G. Rahimian // Com. in Statistics – Theory and Methods. 2017. Vol. 46, iss. 22. P. 11272−11288. doi: 10.1080/03610926.2016.1263741.

3. An overview and perspective on social network monitoring / W. H. Woodall, M. J. Zhao, K. Paynabar, R. Sparks, J. D. Wilson // IISE Transactions. 2016. Т. 49, № 3. P. 354–365. doi: 10.1080/0740817X.2016.1213468.

4. The effect of temporal aggregation level in social network monitoring / M. J. Zhao, A. R. Driscoll, S. Sengupta, N. T. Stevens, R. D. Fricker Jr., W. H. Woodall // Plos one. 2018. Vol. 13, iss. 12. Art. 0209075. doi: 10.1371/journal.pone.0209075.

5. Xiao B., Wang W. Intelligent network operation and maintenance system based on big data // J. of Phys. Conf. Series. 2021. Vol. 1744. P. 1−5. doi: 10.1088/1742-6596/1744/3/032033.

6. Gajica S. Monitoring of 6TiSCH infrastructure with MQTT and Zabbix NMS software // 2020 Intern. Symp. on Industrial Electronics and Appl. (INDEL). Banja Luka, Bosnia and Herzegovina: IEEE, 2020. doi: 10.1109/INDEL50386.2020.9266161.

7. Recio H. A. Automation for incorporating assets into monitoring tools // Telecommunications Technol. and Services Engin. Universitat Politècnica de Catalunya. Barcelona. 2022. 52 p. URL: https://upcommons.upc.edu/bitstream/handle/2117/379630/Degree_Thesis_43564685V.pdf?sequence=5&isAllowed=y (дата обращения: 25.09.2024).

8. Holopainen M. Monitoring container environment with prometheus and grafana. 2021. 54 p. URL: https://www.theseus.fi/bitstream/handle/10024/497467/Holopainen_Matti.pdf (дата обращения: 25.09.2024).

9. Rawoof F. M., Tajammul M., Jamal F. On-premise server monitoring with prometheus and telegram bot // Intern. J. of Sci. Res. Engin. and Man. (IJSREM). 2022. Vol. 06, iss. 04. P. 1−5. doi: 10.55041/IJSREM12276.

10. Absa S., Shajulin B., Kumar R. P. A. Monitoring IaaS using various cloud monitors // Cluster Comp. 2019. Vol. 22(5). P. 12459–12471. doi: 10.1007/s10586-017-1657-y.

11. Network monitoring in software-defined networking: A review / P.-W. Tsai, Ch.-W. Tsai, Ch.-W. Hsu, Ch.-S. Yang // IEEE Systems J. 2018. Vol. 12, iss. 4. P. 3958−3969. doi: 10.1109/JSYST.2018.2798060.

12. Svoboda Ja., Ghafir I., Prenosil V. Network monitoring approaches: An overview // Intern. J. of Advances in Comp. Networks and Its Security – IJCNS. 2015. Vol. 5, iss. 2. P. 88−93.

13. Shardakov K., Bubnov V., Kornienko S. Modeling the operation of a distributed high-load monitoring system for a data transmission network in a non-stationary mode // Models and Methods for Researching Information Systems in Transport (MMRIST). St. Petersburg, Russia: изд-во CEUR-WS, 2020. P. 107−116.

14. Proposal for server integrated management system using Zabbix for blockchain-based NTMobile / K. Suzuki, M. Matsuoka, H. Suzuki, K. Naito // IEEE 9th Gl. Conf. on Consumer Electronics (GCCE). Kobe, Japan: IEEE, 2020. doi: 10.1109/GCCE50665.2020.9291802.

15. Developing a monitoring system for Cloud-based distributed data-centers / D. Elia, G. Vino, G. Donvito, M. Antonacci // EPJ Web of Conf. 2019. Vol. 214. Art. 08012. doi: 10.1051/epjconf/201921408012.

16. Reconfigurable monitoring for telecommunication networks / M. Tianxing, V. Yu. Osipov, A. I. Vodyaho, A. Kalmatskiy, N. A. Zhukova, S. V. Lebedev, Yu. A. Shichkina // PeerJ Comp. Sci. 2020. Vol. 6. P. 1−21. doi: 10.7717/peerj-cs.288.

17. Samaneh S. G. Innovative monitoring systems and new protocols for wireless networks and wireless sensor networks. Master's Degree in ICT for smart societies: Politecnico di Torino, 2022. 64 p. URL: https://webthesis.biblio.polito.it/secure/23000/1/tesi.pdf (дата обращения: 25.09.2024).

18. Ayarza V. C., Bayona-Oré S. Cluster monitoring and integration in technology company // Intern. Conf. on Soft. Proc. Imp. Advances in Intelligent Systems and Computing (AISC). Springer, Cham. 2019. Vol. 1071. P. 253−265. doi: 10.1007/978-3-030-33547-2_19.

19. Obetko S. Monitoring distributed systems with Riemann. Bachelor's Thesis. Brno, Spring, 2016. 63 p. URL: https://is.muni.cz/th/fia5e/fi-pdflatex_Archive.pdf (дата обращения: 25.09.2024).

20. A modern IoT monitoring architecture using Sensu. URL: https://sensu.io/resources/whitepaper/sensu-iot-mo-nitoring (дата обращения: 25.09.2024).

21. A Big Data Platform for heterogeneous data collection and analysis in large-scale data centres / S. R. Tisbeni, D. Cesini, B. Martelli, A. Carbone, C. Cavallaro, D. C. Duma, A. Falabella, M. Galletti, Ja. Gasparetto, E. Furlan, D. Michelotto, F. Minarini, L. Morganti, E. Ronchieri, G. Sergi // Intern. Symp. on Grids & Clouds (ISGC2021). Taipei, Taiwan: Academia Sinica, 2021. P. 1−14. doi: 10.22323/1.378.0008.

22. Ahola J. Cloud monitoring: Cloud monitoring with dynatrace: Thesis. Oulu University of Applied Sciences, Information Technology, Oulu, Finland, 2022. 49 p. URL: https://www.theseus.fi/bitstream/handle/10024/786044/Ahola_Johannes.pdf?sequence=2&isAllowed=y (дата обращения: 25.09.2024).

23. Darwesh Gh., Vorobeva A. A. Kubernetes monitoring with Prometheus for security purposes // Вестн. науки. Сб. тр. по мат. IX Межд. конкурса науч.-исслед. раб. Уфа: изд-во «НИЦ Вестник науки», 2022. P. 44−50.

24. Security policy monitoring of BPMN-based service compositions / M. Asim, A. Yautsiukhin, A. D. Brucker, Th. Baker, Qi Shi, B. Lempereur // J. of Software: Evolution and Process. 2018. Vol. 30, iss. 9. P. 2–13 doi: 10.1002/smr.1944.

25. Research on cluster monitoring and prediction platform based on Zabbix technology / C. Peixian, B. Shenghua, Zh. Hongliang, T. Baoyu // IOP Conf. Series: Earth and Environmental Sci. (AESEE). Hangzhou, China, 2020. Vol. 512(1). Art. 012155. doi: 10.1088/1755-1315/512/1/012155.

26. Correction to: An explainable model for fault detection in HPC systems / M. Molan, A. Borghesi, F. Beneventi, M. Guarrasi, A. Bartolini // Lect. Notes in Comp. Sci. (LNTCS). Cham: ISC High Performance, Springer. 2021. Vol. 12761. P. 378–391. doi: 10.1007/978-3-030-90539-2_36.

27. Kunz P. HPC Job-Monitoring with SLURM, Prometheus and Grafana: Bachelor Thesis. 2022. URL: https://hpc.dmi.unibas.ch/wp-content/uploads/sites/87/2022/07/bsc-thesis-p-kunz.pdf (дата обращения: 25.09.2024).

28. Observability in Kubernetes Cluster: Automatic anomalies detection using Prometheus / O. Mart, C. Negru, F. Pop, A. Castiglione // 2020 IEEE 22nd Intern. Conf. on High Perf. Comp. and Commun.; IEEE 18th Int. Conf. on Smart City; IEEE 6th Int. Conf. on Data Science and Systems (HPCC/SmartCity/DSS). Yanuca Island, Cuvu, Fiji: IEEE, 2020. doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00071.

29. The secured clouds watch web service resources based on prescheduled changes to resources in big data management / M. Ramkumar, R. Karthick, N. Aravinth, A. Jayashree // ICTACT J. on Data Sci. and Machine Learning. 2021. Vol. 04, iss. 01. P. 396−399. URL: https://ictactjournals.in/paper/IJDSML_Vol_3_Issue_4_Paper_8_396_399.pdf (дата обращения: 25.09.2024).

30. Рукавицын А. Н. Кластеризация данных в распределенных системах мониторинга // Информационно-управляющие системы. 2019. № 2. С. 35–43. doi: 10.31799/1684-8853-2019-2-35-43.

31. Аллакин В. В., Будко Н. П., Васильев Н. В. Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Системы управления, связи и безопасности. 2021. № 4. С. 125−227. doi: 10.24412/2410-9916-2021-4-125-227.

32. Traffic accident detection and condition analysis based on social networking data / F. Ali, A. Ali, M. Imran, R. A. Naqvi, M. H. Siddiqi, K.-S. Kwak // Accident Analysis & Prevention. 2021. Vol. 151. P. 105973. doi: 10.1016/j.aap.2021.105973.

33. Social network analysis for precise friend suggestion for Twitter by Associating Multiple Networks using ML / D. K. Singh Singh, N. Nithya, L. Rahunathan, P. Sanghavi, R. S. Vaghela, P. Manoharan, M. Hamdi, G. B. Tunze // Intern. J. of Inform. Technol. and Web Engin. 2022. Vol. 17, iss. 1. P. 1−11. doi: 10.4018/IJITWE.304050.

34. Shmelkin I. Monitoring for control in role-oriented Self-Adaptive Systems // ACM 15th Int. Symp. on Software Eng. for Adaptive and Self-Managing Systems (SEAMS'20). New York, NY, United States: IEEE CS, 2020. P. 115−119. doi: 10.1145/3387939.3391598.

35. Рождественская К. Н. Количественный анализ программы для управления бортовой вычислительной сетью // Информационно-управляющие системы. 2020. № 4. С. 42–49. doi: 10.31799/1684-8853-2020-4-42-49.

36. Колесникова С. И., Фоменкова А. А. Динамические стратегии управления качеством мониторинга сложного биоинженерного объекта // Информационно-управляющие системы. 2023. № 2. С. 51−61. doi: 10.31799/1684-8853-2023-2-51-61.

37. Вейвлет-преобразование и одноклассовая классификация для мониторинга состояния дамб / А. П. Козионов, А. Л. Пяйт, И. И. Мохов, Ю. П. Иванов // Информационно-управляющие системы. 2014. № 4. С. 24−32.

38. A network traffic forecasting method based on SA optimized ARIMA–BP neural network / H. Yang, X. Li, W. Qiang, Yu. Zhao, W. Zhang, Ch. Tang // Comp. Networks. 2021. Vol. 193. Art. 108102. doi: 10.1016/j.comnet.2021.108102.

39. Prajam S., Wechtaisong C., Khan A. A. Applying machine learning approaches for network traffic forecasting // Indian J. of Comp. Sci. and Eng. (IJCSE). Vol. 13, iss. 2. P. 324−335. doi: 10.21817/indjcse/2022/v13i2/221302188.

40. A study of deep learning for Network Traffic Data Forecasting / B. Pfülb, Ch. Hardegen, A. Gepperth, S. Rieger // Int. Conf. on Artificial Neural Networks (ICANN 2019). Lect. Notes in Comp. Sci. (LNTCS). Vol. 11730. P. 497−512. doi: 10.1007/978-3-030-30490-4_40.

41. Predictive analysis and screening diagnosis of HDD Storage Deterioration using Smart MI Strategies / V. S. Prakash, U. Udayakumar, G. Rohini, Vishal Ratansing Patil, Sudhir Shenai, R. Thiagarajan // Math. Statistician and Engin. Appl. (MSEA). 2021. Vol. 70, № 2. P. 890−898. doi: 10.17762/msea.v70i2.2087.

Информация об авторах

Тайц Вадим Максимович – аспирант СПИИРАН СПб ФИЦ РАН, 14-я линия В. О., д. 39, Санкт-Петербург, 199178, Россия.
E-mail: taizvadim@gmail.com

Жукова Наталия Александровна – д-р техн. наук, доцент, вед. научный сотрудник СПИИРАН СПб ФИЦ РАН, 14-я линия В. О., д. 39, Санкт-Петербург, 199178, Россия.
E-mail: nazhukova@mail.ru
https://orcid.org/0000-0001-5877-4461

References

1. Chto takoe monitoring i ego urovni / Zhurn. VK Cloud ob IT-biznese, tehnologijah i cifrovoj transformacii. URL: https://cloud.vk.com/blog/chto-takoe-monitoring-i-ego-urovni (data obrashhenija: 25.09.2024). (In Russ.).

2. A statistical approach to social network monitoring / E. M. Farahani, R. B. Kazemzadeh, R. Noorossana, G. Rahimian // Com. in Statistics – Theory and Methods. 2017. Vol. 46, iss. 22. P. 11272–11288. doi: 10.1080/03610926.2016.1263741.

3. An overview and perspective on social network monitoring / W. H. Woodall, M. J. Zhao, K. Paynabar, R. Sparks, J. D. Wilson // IISE Transactions. 2016. T. 49, № 3. P. 354–365. doi: 10.1080/0740817X.2016.1213468.

4. The effect of temporal aggregation level in social network monitoring / M. J. Zhao, A. R. Driscoll, S. Sengupta, N. T. Stevens, R. D. Fricker Jr., W. H. Woodall // Plos one. 2018. Vol. 13, iss. 12. Art. 0209075. doi: 10.1371/journal.pone.0209075.

5. Xiao B., Wang W. Intelligent network operation and maintenance system based on big data // J. of Phys. Conf. Series. 2021. Vol. 1744. P. 1–5. doi: 10.1088/1742-6596/1744/3/032033.

6. Gajica S. Monitoring of 6TiSCH infrastructure with MQTT and Zabbix NMS software // 2020 Intern. Symp. on Industrial Electronics and Appl. (INDEL). Banja Luka, Bosnia and Herzegovina: IEEE, 2020. doi: 10.1109/INDEL50386.2020.9266161.

7. Recio H. A. Automation for incorporating assets into monitoring tools // Telecommunications Technol. and Services Engin. Universitat Politècnica de Catalunya. Barcelona. 2022. 52 p. URL: https://upcommons.upc.edu/bitstream/handle/2117/379630/Degree_Thesis_43564685V.pdf?sequence=5&isAllowed=y (data obrashhenija: 25.09.2024).

8. Holopainen M. Monitoring container environment with prometheus and grafana. 2021. 54 p. URL: https://www.theseus.fi/bitstream/handle/10024/497467/Holopainen_Matti.pdf (data obrashhenija: 25.09.2024).

9. Rawoof F. M., Tajammul M., Jamal F. On-premise server monitoring with prometheus and telegram bot // Intern. J. of Sci. Res. Eng. and Man. (IJSREM). 2022. Vol. 06, iss. 04. P. 1–5. doi: 10.55041/IJSREM12276.

10. Absa S., Shajulin B., Kumar R. P. A. Monitoring IaaS using various cloud monitors // Cluster Comp. 2019. Vol. 22(5). P. 12459–12471. doi: 10.1007/s10586-017-1657-y.

11. Network monitoring in software-defined networking: A review / P.-W. Tsai, Ch.-W. Tsai, Ch.-W. Hsu, Ch.-S. Yang // IEEE Systems J. 2018. Vol. 12, iss. 4. P. 3958–3969. doi: 10.1109/JSYST.2018.2798060.

12. Svoboda Ja., Ghafir I., Prenosil V. Network monitoring approaches: An overview // Intern. J. of Advances in Comp. Networks and Its Security – IJCNS. 2015. Vol. 5, iss. 2. P. 88–93.

13. Shardakov K., Bubnov V., Kornienko S. Modeling the operation of a distributed high-load monitoring system for a data transmission network in a non-stationary mode // Models and Methods for Researching Information Systems in Transport (MMRIST). St. Petersburg, Russia: izd-vo CEUR-WS, 2020. P. 107–116.

14. Proposal for Server integrated management system using Zabbix for blockchain-based NTMobile / K. Suzuki, M. Matsuoka, H. Suzuki, K. Naito // IEEE 9th Gl. Conf. on Consumer Electronics (GCCE). Kobe, Japan: IEEE, 2020. doi: 10.1109/GCCE50665.2020.9291802.

15. Developing a monitoring system for Cloud-based distributed data-centers / D. Elia, G. Vino, G. Donvito, M. Antonacci // EPJ Web of Conf. 2019. Vol. 214. Art. 08012. doi: 10.1051/epjconf/201921408012.

16. Reconfigurable monitoring for telecommunication networks / M. Tianxing, V. Yu. Osipov, A. I. Vodyaho, A. Kalmatskiy, N. A. Zhukova, S. V. Lebedev, Yu. A. Shichkina // PeerJ Comput. Sci. 2020. Vol. 6. P. 1–21. doi: 10.7717/peerj-cs.288.

17. Samaneh S. G. Innovative monitoring systems and new protocols for wireless networks and wireless sensor networks. Master's Degree in ICT for Smart Societies: Politecnico di Torino, 2022. 64 p. URL: https://webthesis.biblio.polito.it/secure/23000/1/tesi.pdf (data obrashhenija: 25.09.2024).

18. Ayarza V. C., Bayona-Oré S. Cluster monitoring and integration in technology company // Intern. Conf. on Soft. Proc. Imp. Advances in Intelligent Systems and Computing (AISC). Springer, Cham. 2019. Vol. 1071. P. 253–265. doi: 10.1007/978-3-030-33547-2_19.

19. Obetko S. Monitoring distributed systems with Riemann. Bachelor's Thesis. Brno, Spring, 2016. 63 p. https://is.muni.cz/th/fia5e/fi-pdflatex_Archive.pdf (data obrashhenija: 25.09.2024).

20. A Modern IoT monitoring architecture using Sensu. URL: https://sensu.io/resources/whitepaper/sensu-iot-monito-ring (data obrashhenija: 25.09.2024).

21. A Big Data Platform for heterogeneous data collection and analysis in large-scale data centres / S. R. Tisbeni, D. Cesini, B. Martelli, A. Carbone, C. Cavallaro, D. C. Duma, A. Falabella, M. Galletti, Ja. Gasparetto, E. Furlan, D. Michelotto, F. Minarini, L. Morganti, E. Ronchieri, G. Sergi // Intern. Symp. on Grids & Clouds (ISGC2021). Taipei, Taiwan: Academia Sinica, 2021. P. 1–14. doi: 10.22323/1.378.0008.

22. Ahola J. Cloud monitoring: Cloud monitoring with dynatrace: Thesis. Oulu University of Applied Sciences, Information Technology, Oulu, Finland, 2022. 49 p. URL: https://www.theseus.fi/bitstream/handle/10024/786044/Ahola_Johannes.pdf?sequence=2&isAllowed=y (data obrashhenija: 25.09.2024).

23. Darwesh Gh., Vorobeva A. A. Kubernetes monitoring with Prometheus for security purposes // Vestn. nauki. Sb. tr. po mat. IX Mezhd. konkursa nauch.-issled. rab. Ufa: izd-vo «NIC Vestnik nauki », 2022. P. 44–50.

24. Security policy monitoring of BPMN-based service compositions / M. Asim, A. Yautsiukhin, A. D. Brucker, Th. Baker, Qi Shi, B. Lempereur // J. of Software: Evolution and Process. 2018. Vol. 30, iss. 9. P. 2–13 doi: 10.1002/smr.1944.

25. Research on cluster monitoring and prediction platform based on Zabbix technology / C. Peixian, B. Shen-ghua, Zh. Hongliang, T. Baoyu // IOP Conf. Series: Earth and Environmental Sci. (AESEE). Hangzhou, China, 2020. Vol. 512(1). Art. 012155. doi: 10.1088/1755-1315/512/1/012155.

26. Correction to: An explainable model for fault detection in HPC systems / M. Molan, A. Borghesi, F. Beneventi, M. Guarrasi, A. Bartolini // Lect. Notes in Comp. Sci. (LNTCS). Cham: ISC High Performance, Springer. 2021. Vol. 12761. P. 378–391. doi: 10.1007/978-3-030-90539-2_36.

27. Kunz P. HPC Job-Monitoring with SLURM, Prometheus and Grafana: Bachelor Thesis. 2022. URL: https://hpc.dmi.unibas.ch/wp-content/uploads/sites/87/2022/07/bsc-thesis-p-kunz.pdf (data obrashhenija: 25.09.2024).

28. Observability in Kubernetes Cluster: Automatic anomalies detection using Prometheus / O. Mart, C. Negru, F. Pop, A. Castiglione // 2020 IEEE 22nd Intern. Conf. on High Perf. Comp. and Commun.; IEEE 18th Int. Conf. on Smart City; IEEE 6th Int. Conf. on Data Sci. and Systems (HPCC/SmartCity/DSS). Yanuca Island, Cuvu, Fiji: IEEE, 2020. doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00071.

29. The secured clouds watch web service resources based on prescheduled changes to resources in big data management / M. Ramkumar, R. Karthick, N. Aravinth, A. Jayashree // ICTACT J. on Data Sci. and Machine Learning. 2021. Vol. 04, iss. 01. P. 396−399. URL: https://ictactjournals.in/paper/IJDSML_Vol_3_Issue_4_Paper_8_396_399.pdf (data obrashhenija: 25.09.2024).

30. Rukavicyn A. N. Klasterizacija dannyh v raspredelennyh sistemah monitoringa // Informacionno-upravljajushhie sistemy. 2019. № 2. S. 35–43. doi: 10.31799/1684-8853-2019-2-35-43. (In Russ.).

31. Allakin V. V., Budko N. P., Vasil'ev N. V. Obshhij podhod k postroeniju perspektivnyh sistem monitoringa raspredelennyh informacionno-telekommunikacionnyh setej // Sistemy upravlenija, svjazi i bezopasnosti. 2021. № 4. S. 125−227. doi: 10.24412/2410-9916-2021-4-125-227. (In Russ.).

32. Traffic accident detection and condition analysis based on social networking data / F. Ali, A. Ali, M. Imran, R. A. Naqvi, M. H. Siddiqi, K.-S. Kwak // Accident Analysis & Prevention. 2021. Vol. 151. P. 105973. doi: 10.1016/j.aap.2021.105973.

33. Social network analysis for precise friend suggestion for twitter by associating multiple networks using ML / Dharmendra Kumar Singh Singh, N. Nithya, L. Rahunathan, P. Sanghavi, R. S. Vaghela, P. Manoharan, M. Hamdi, G. B. Tunze // Intern. J. of Information Technol. and Web Engin. 2022. Vol. 17, iss. 1. P. 1−11. doi: 10.4018/IJITWE.304050.

34. Shmelkin I. Monitoring for control in role-oriented self-adaptive systems // ACM 15th Int. Symp. on Software Eng. for Adaptive and Self-Managing Systems (SEAMS'20). New York, NY, United States: IEEE CS, 2020. P. 115−119. doi: 10.1145/3387939.3391598.

35. Rozhdestvenskaja K. N. Kolichestvennyj analiz programmy dlja upravlenija bortovoj vychislitel'noj set'ju // Informacionno-upravljajushhie sistemy. 2020. № 4. S. 42–49. doi: 10.31799/1684-8853-2020-4-42-49. (In Russ.).

36. Kolesnikova S. I., Fomenkova A. A. Dinamicheskie strategii upravlenija kachestvom monitoringa slozhnogo bioinzhenernogo ob#ekta // Informacionno-upravljajushhie sistemy. 2023. № 2. S. 51−61. doi: 10.31799/1684-8853-2023-2-51-61. (In Russ.).

37. Vejvlet-preobrazovanie i odnoklassovaja klassifikacija dlja monitoringa sostojanija damb / A. P. Kozionov, A. L. Pjajt, I. I. Mohov, Ju. P. Ivanov // Informacionno-upravljajushhie sistemy. 2014. № 4. C. 24−32. (In Russ.).

38. A network traffic forecasting method based on SA optimized ARIMA–BP neural network / H. Yang, X. Li, W. Qiang, Yu. Zhao, W. Zhang, Ch. Tang // Comp. Networks. 2021. Vol. 193. Art. 108102. doi: 10.1016/j.comnet.2021.108102.

39. Prajam S., Wechtaisong C., Khan A. A. Applying machine learning approaches for network traffic forecasting // Indian J. of Comp. Sci. and Eng. (IJCSE). Vol. 13, iss. 2. P. 324−335. doi: 10.21817/indjcse/2022/v13i2/221302188.

40. A study of deep learning for Network Traffic Data Forecasting / B. Pfülb, Ch. Hardegen, A. Gepperth, S. Rieger // Int. Conf. on Artificial Neural Networks (ICANN 2019). Lect. Notes in Comp. Sci. (LNTCS). Vol. 11730. P. 497−512. doi: 10.1007/978-3-030-30490-4_40.

41. Predictive analysis and screening diagnosis of HDD Storage Deterioration using Smart MI strategies / V. S. Prakash, U. Udayakumar, G. Rohini, V. R. Patil, S. Shenai, R. Thiagarajan // Math. Statistician and Engin. Appl. (MSEA). 2021. Vol. 70, №2. P. 890−898. doi: 10.17762/msea.v70i2.2087.

Information about the authors

Vadim M. Taits – postgraduate student, SPIIRAS of St. Petersburg Federal Research Center of the Russian Academy of Sciences, 14st line, 39, Vasilievsky Island, Saint Petersburg, 199178, Russia.
E-mail: taizvadim@gmail.com

Natalia A. Zhukova – Dr Sci. (Eng.), Associate Professor, Leading researcher, SPIIRAS of St. Petersburg Federal Research Center of the Russian Academy of Sciences, 14st line, 39, Vasilievsky Island, Saint Petersburg, 199178, Russia.
E-mail: nazhukova@mail.ru
https://orcid.org/0000-0001-5877-4461

Статья поступила в редакцию 14.05.2024; принята к публикации после рецензирования 26.09.2024; опубликована онлайн 25.11.2024.

Submitted 14.05.2024; accepted 26.09.2024; published online 25.11.2024.