Компьютерные инструменты в образовании, 2023
№ 3: 35–50
УДК: 004.67
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-3-35-50

ПРОГРАММНЫЙ УРОВЕНЬ СИСТЕМЫ МОНИТОРИНГА КОМПЬЮТЕРНОЙ СЕТИ С МОДУЛЕМ ДОПОЛНИТЕЛЬНОЙ ДИАГНОСТИКИ АНОМАЛИЙ

Авилов М. И.[1], инженер, ✉ avilovmaxim@gmail.com

[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), ул. Профессора Попова, 5, корп. 3, 197022, Санкт-Петербург, Россия

Аннотация

В статье описывается программный уровень архитектуры системы мониторинга функционирования компьютерной сети с модулем диагностики аномалий. Предлагается программное решение для данного уровня архитектуры системы мониторинга сети. Также в статье отражены результаты проверки архитектуры системы мониторинга функционирования компьютерной сети с модулем диагностики аномалий на соответствие требованиям: возможность кластеризации аномалий в работе сети, ручное и автоматическое управление формированием сценариев воздействия на узлы, возможность масштабирования системы мониторинга сети, наличие раздельного хранения данных для статистики и сценариев воздействия на узлы и др. Кроме этого, в статье представлены результаты тестирования разработанного программного решения. Тесты проводились по кластеризации аномалий компьютерной сети и формированию сценариев воздействия на наблюдаемые нестабильные сетевые узлы. Полученные результаты показывают, что разработанное программное обеспечение позволяет проводить кластеризацию аномалий в работе компьютерной сети, а также осуществлять формирование сценариев воздействия на такие узлы при проведении дополнительной диагностики нестабильных узлов.

Ключевые слова: *система мониторинга компьютерной сети, компьютерная сеть, модуль диагностики аномалий, архитектура информационной системы.*

Цитирование: Авилов М. И. Программный уровень системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий // Компьютерные инструменты в образовании. 2023. № 3. С. 35-50. doi: 10.32603/2071-2340-2023-3-35-50

1. ВВЕДЕНИЕ

В последние годы активно развиваются различные информационные технологии, которые используют компьютерные сети (КС) для обмена данными. Для обеспечения стабильной связи необходимо непрерывно отслеживать состояние функционирования таких сетей. При этом необходимо учесть, что с увеличением размеров и сложности сетей, где проводные и беспроводные сети могут представлять логически одну или несколько сетей, возникает сложность управления ими и контроля. Для обеспечения штатного режима работы КС и избегания негативных последствий из-за возникновения проблемных

и аномальных ситуаций применяются системы мониторинга КС [1–3]. Такие системы позволяют выявлять различные проблемы, сбои в работе конкретных хостов или определять узкие места, где происходит снижение производительности сети [4]. Кроме этого, системы мониторинга КС могут предоставлять информацию об имеющемся оборудовании и его загруженности, что, в свою очередь, может помочь в планировании изменений конфигурации сети и установке нового оборудования, а также в анализе рисков и возможностей для совершенствования критически значимых участков сетевой инфраструктуры [5].

В случае проактивного наблюдения за состоянием элементов сети системы проактивного мониторинга КС позволяют предупреждать и устранять проблемы до того, как они оказывают негативное влияние на производительность отдельных узлов и работоспособность сети в целом. Прогнозы строятся на основе собранных статистических данных с наблюдаемых сетевых узлов. Для этого анализируется динамика изменений значений метрик временного ряда, и в случае выявления, например, предотказного состояния сетевого элемента, система мониторинга сети обрабатывает значения метрик и формирует сигналы о ситуации для дальнейшего автоматического или ручного действия с целью нормализации ситуации [6]. Реактивный мониторинг КС, в свою очередь, работает на основе анализа возникшей ситуации. В этом случае система реактивного мониторинга КС анализирует возникшую ситуацию, а затем принимает меры для устранения причин возникновения ситуации и восстановления работоспособности сети [7]. Однако системы мониторинга КС, которые в случае выявления аномалий в функционировании сети проводили бы дополнительную диагностику конкретных узлов и формировали сценарии воздействия на такие узлы, применяются нечасто.

В данной статье описывается программный уровень архитектуры системы мониторинга КС с модулем дополнительной диагностики аномалий и предлагается программное решение на основе такой архитектуры. Программное решение основывается на предыдущих исследованиях [8–10] и позволяет выявлять аномалии в наблюдаемой статистической или динамической КС. В случае динамической КС учитывается изменение количества наблюдаемых узлов. В статической же сети количество наблюдаемых узлов не изменяется. Также программное решение позволяет формировать сценарии воздействия на выявленные нестабильные сетевые узлы.

2. ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ

В настоящее время существует множество различных решений по вопросам мониторинга КС. Для поддержания штатной работы КС такие решения могут производить опрос наблюдаемых узлов, сбор, представление данных, проводить оценку состояния сети по определенным заранее критериям, осуществлять воздействие по определенным сценариям или прогнозировать возможное развитие событий.

В [11] автор предлагает архитектуру системы мониторинга КС на основе мобильных мультиагентов. В таком решении применяется многоуровневый подход, где происходит разделение КС на компоненты по оборудованию, сервисам, пользователям. Автор отмечает, что многие решения неэффективны в условиях частой изменяемости состояния сети, и требуются новые решения с учетом возможностей масштабирования системы мониторинга КС. Предложенное решение позволяет масштабировать систему мониторинга за счет введения новых агентов.

Отслеживание состояния бесперебойных источников питания (ИБП) при помощи SNMP (Simple Network Management Protocol — простой протокол сетевого управления)

рассматривается в работе [12]. Авторы отмечают, что у современных моделей ИБП есть специальный интерфейс, по которому возможно осуществлять сбор данных о состоянии источников питания. Опрос происходит по КС при помощи сервера мониторинга сети, где наблюдаемый сетевой объект отмечается как источник бесперебойного питания. Далее статические данные с ИБП собираются на сервере, где оператор может с ними ознакомиться.

В работе [13] авторы предлагают программное и алгоритмическое решение, которое может быть использовано для мониторинга аномалий в работе КС. Для выявления аномалий сети извлекается необходимая информация из собранных исторических данных, на основе которой формируются симптомы возможных будущих аномалий сети. Отмечается, что такое обучение позволяет прогнозировать аномалии в функционировании КС и своевременно реагировать, если симптомы подтверждаются. Также авторы предлагают функциональную схему системы «здоровья» сети, где происходит анализ характеристик состояния КС. По этим характеристикам и происходит диагностика возникшей ситуации в функционировании сети.

Автоматизированная система мониторинга и обработки статистики корпоративной сети с применением криптомаршрутизаторов предлагается в работе [14]. Для сбора и обработки статистики используются комбинация MRTG (The Multi Router Traffic Grapher) и Nagios. Авторы отмечают, что такое решение позволяет контролировать работу корпоративной сети и проводить эксперименты по имитационному моделированию нагрузки на различные участки сети.

Распределенную систему мониторинга состояния КС в [15] предлагается создать на основе архитектуры REST (Representational State Transfer — передача репрезентативного состояния). Отмечается, что такое решение позволяет разделять клиентов и сервера, что, в свою очередь, позволяет хранить данные отдельно и осуществлять вычисления на специальных узлах. Такое разделение создает возможность разрабатывать клиентскую и серверную части раздельно. В качестве пользовательского интерфейса мониторинга КС предлагается одностраничное приложение, которое использует AngularJS. Предложенное решение позволяет создавать собственное API (Application Programming Interface) для различных дополнительных программных разработок и улучшений системы мониторинга КС.

В [16] рассматриваются вопросы касательно обработки и представления данных состояния информационно-телекоммуникационных сетей и систем при помощи Hadoop с учетом анализа объемов Big Data. Авторы предлагают структуру узла мониторинга, который позволяет упорядочивать связанные данные и формировать «витринные данные» в виде «таблицы фактов». Применяется хранилище «ключ-значение», где находятся первичные данные с нескольких узлов мониторинга, создавая, таким образом, витрину первичных данных. Авторы отмечают, что современные технологии работы с большими данными формируют предпосылки для создания основы «интеллектуального» мониторинга, где используются подходы машинного обучения как для долговременных трендов, так и для оперативного анализа возникающих ситуаций по наблюдаемым устройствам. Отмечается, что вариант реализации создания витринных данных при помощи Hadoop создает возможность в будущем формировать порядок функционирования подсистемы мониторинга для выявления аномалий в работе информационно-телекоммуникационных сетей и систем.

Архитектурное решение автоматизированной системы мониторинга серверов и сервисов в КС, представленное в [17], дает возможность наблюдать за производительностью

серверов и сервисов, строить графики и оповещать системного инженера о проблемных ситуациях. Система состоит из четырех частей: сервер мониторинга, сервис мониторинга, установленный на наблюдаемом узле, сервер web-приложений и сервер уведомлений. Такое разделение создает разграничение вычислительных функций системы мониторинга. Автор отмечает, что применение предложенной архитектуры позволяет создать гибкую систему мониторинга статусов серверов в КС с различной сложностью сетевой инфраструктуры, а также не требует подключения дополнительных сервисов.

Система мониторинга трафика технологических сетей передачи данных на основе Zabbix и Net-Flow Analyzer предлагается в [18]. Предложенная система мониторинга сети производит сбор данных по пропускной способности каналов связи для анализа загруженности сети и оптимизации топологии сети с целью улучшения качества связи. Сам сбор данных может осуществляться как по SNMP, так и по протоколу Net-Flow. В случае возникновения нештатной ситуации в КС информация от комплексной системы мониторинга КС поступает в виде СМС-уведомлений или при помощи e-mail главному оператору.

Модель системы мониторинга сетевой распределенной информационной инфраструктуры и её функции в рамках медицинского учреждения предлагается в [19]. Модель делится на три уровня: уровень приложений, промежуточный уровень, нижний уровень. На нижнем уровне собираются данные с наблюдаемых узлов, обрабатываются и передаются на уровень выше. Промежуточный уровень осуществляет обработку данных, полученных от разных источников, и передает на уровень приложений. Уровень приложений необходим для представления обработанных данных пользователям системы. Авторы отмечают, что такая модель позволяет создавать динамическую структуру данных, где источником могут выступать различные программно-аппаратные элементы. Также в работе предложен алгоритм диагностики состояния рассматриваемой КС, в котором осуществляется опрос наблюдаемых устройств, проверка доступности, проверка состояния интерфейсов, проверка ошибок конфигурации узла и информирование о выявленных проблемных ситуациях.

Системы мониторинга КС развиваются с каждым годом, о чем говорят работы [20–22], которые посвящены сравнительному анализу таких систем. На основе сравнительного анализа можно выявлять как преимущества, так и недостатки различных систем мониторинга сетей. Например, в [22] отражено, что Zabbix может работать с различными системами управления баз данных (СУБД), в то время как Nagios и Cacti могут работать преимущественно с RRDTool, а с MySQL только через специальный плагин. Однако потребление вычислительных ресурсов у Zabbix и Nagios выше, чем у Cacti. В то же время, если компоненты Zabbix будут разнесены на несколько вычислительных узлов, то нагрузку системы можно распределить между этими узлами. В [20] приведен сравнительный анализ 12 систем по 9 параметрам: формирование отчетов SLA (Service Level Agreement), формирование трендов, прогнозирование трендов, анализ топологии сети, использование агентной модели, поддержка SNMP, протоколирование событий, датчики внештатных ситуаций, распределенный мониторинг. Авторы отмечают, что для эффективного управления в телекоммуникационной сети системы мониторинга должны поддерживать функции не только формирования трендов по полученным статистическим данным, но и осуществлять прогнозирование возможных ситуаций в работе таких сетей. В работе [21] отмечается, что в качестве пассивного мониторинга событий могут быть использованы такие системы как MRTG, Cacti, Nagios, Zabbix. Если необходим активный мониторинг сети, то в качестве решения могут подойти системы HP Open View, IBM Tivoli. Также отмечается, что при выборе системы мониторинга сети необходимо учитывать такие факторы, как

отказ отдельных элементов или всей системы мониторинга, умышленного вредоносного воздействия на систему, возможности распределения нагрузки системы на нескольких узлах.

Проведенный анализ исследований систем мониторинга функционирования КС показал, что, несмотря на существование множества различных систем мониторинга, для решения всех необходимых задач по обеспечению качественной работы КС требуется комбинировать разные системы мониторинга сети или дорабатывать имеющиеся. Также в случае выявления нештатных аномальных ситуаций в работе сети требуется оперативная дополнительная диагностика состояний нестабильных наблюдаемых узлов для корректного реагирования на выявленные состояния. Многие системы такую диагностику в автоматическом режиме не проводят или выполняют действия по шаблонам, которые не подходят для выявленной ситуации.

Целью проводимых исследований являлась разработка программного решения по выявлению аномалий в функционировании КС, а также формирование в автоматическом режиме сценариев воздействия на выявленную аномалию сети. Для этого был создан программный уровень архитектуры системы мониторинга КС с модулем дополнительной диагностики аномалий. Кроме того, было разработано программное обеспечение по автоматической дополнительной диагностике аномалий нестабильных наблюдаемых узлов и формированию сценариев воздействия на выявленную аномалию. Также было спроектировано программное решение по корректировке параметров формирования сценариев и диагностике аномалий в ручном режиме без приостановки работы системы мониторинга КС

3. ПРОГРАММНЫЙ УРОВЕНЬ АРХИТЕКТУРЫ

Система мониторинга КС с модулем дополнительной диагностики аномалий основывается на требованиях и архитектуре системы мониторинга сети, предложенной в [9]. При проектировании системы мониторинга сети применялся модульный подход. Такой подход позволяет разбить систему на отдельные модули, каждый из которых решает свои задачи. Кроме того, модули могут быть усовершенствованы как независимые компоненты и легко подключаться к основной части системы мониторинга ее без приостановки работы. Взаимодействие компонентов системы мониторинга функционирования КС с модулем дополнительной диагностики аномалий и наблюдаемого объекта представлен на рисунке 1.

Описание работы системы мониторинга сети с модулем дополнительной диагностики аномалий на программном уровне архитектуры

Первоначально наблюдаемый объект добавляется в систему мониторинга сети. Наблюдаемый объект может быть добавлен вручную или при помощи автоматического обнаружения по определенным параметрам (проверки по ICMP, SNMP, HTTPS и другим). В качестве основы для сбора данных применяется Zabbix, потому что он позволяет собирать данные разными способами (SNMP, IPMI, zabbix-агенты, JMX) и есть API. Далее системный инженер определяет параметры, которые система мониторинга сети должна отслеживать, и пороговые значения для этих параметров, которые отражают состояние работы КС. Определение наблюдаемых параметров и пороговых значений основывается на требованиях к работе конкретной КС, с которой системный инженер работает. Вся статистика по собранным данным сохраняется в базу данных MySQL, потому что одним из критериев работы Zabbix является взаимодействие с такой СУБД.

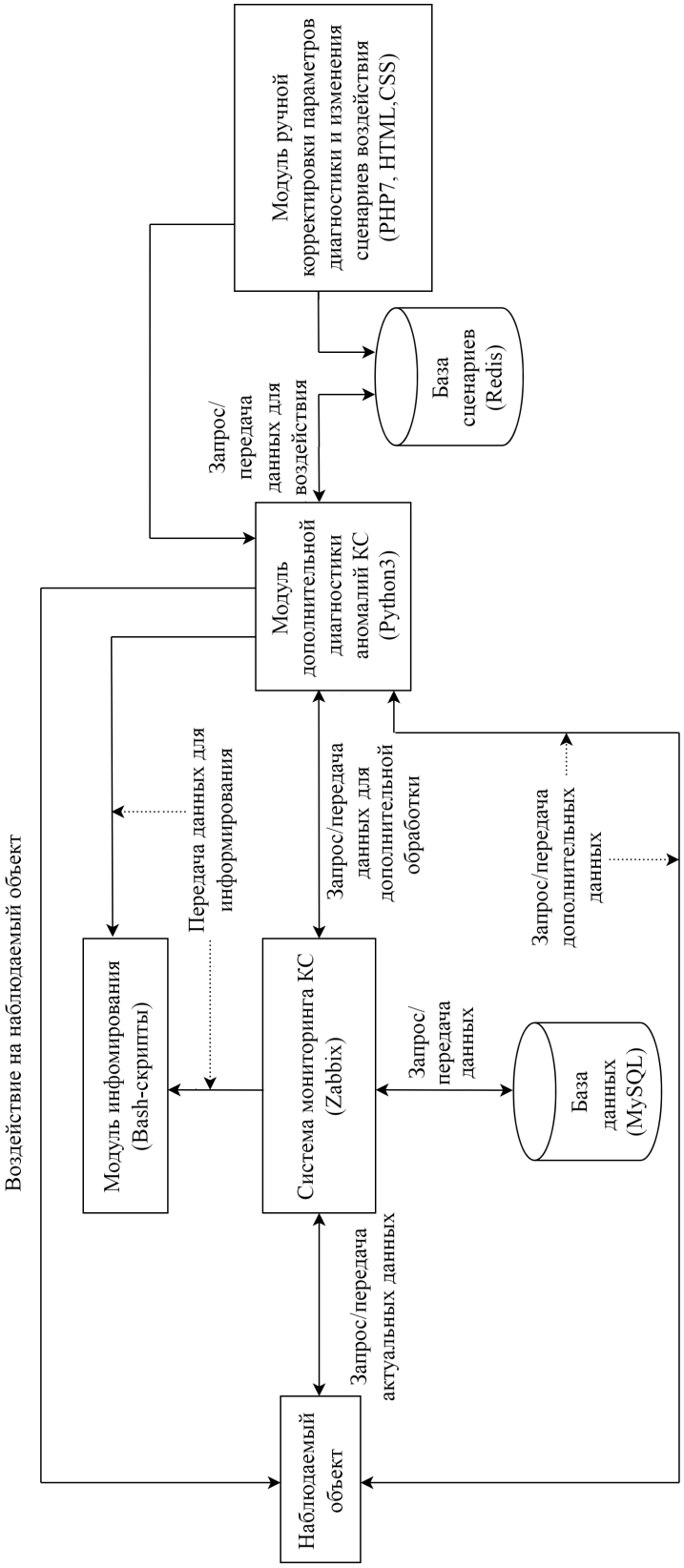

Рис. 1. Программный уровень системы мониторинга сети модулем дополнительной диагностики аномалий

Модуль дополнительной диагностики аномалий КС написан на языке программирования Python3 и обрабатывает информацию при помощи API Zabbix. Прежде чем запустить модуль, необходимо провести первоначальную конфигурацию. Такая конфигурация осуществляется при помощи дополнительного модуля ручной корректировки параметров диагностики и изменения сценариев воздействия, который написан на языке программирования PHP7 с применением HTML (Hyper Text Markup Language — язык гипертекстовой разметки) и CSS (Cascading Style Sheets — каскадные таблицы стилей). Некоторые web-окна этого модуля представлены на рисунке 2.

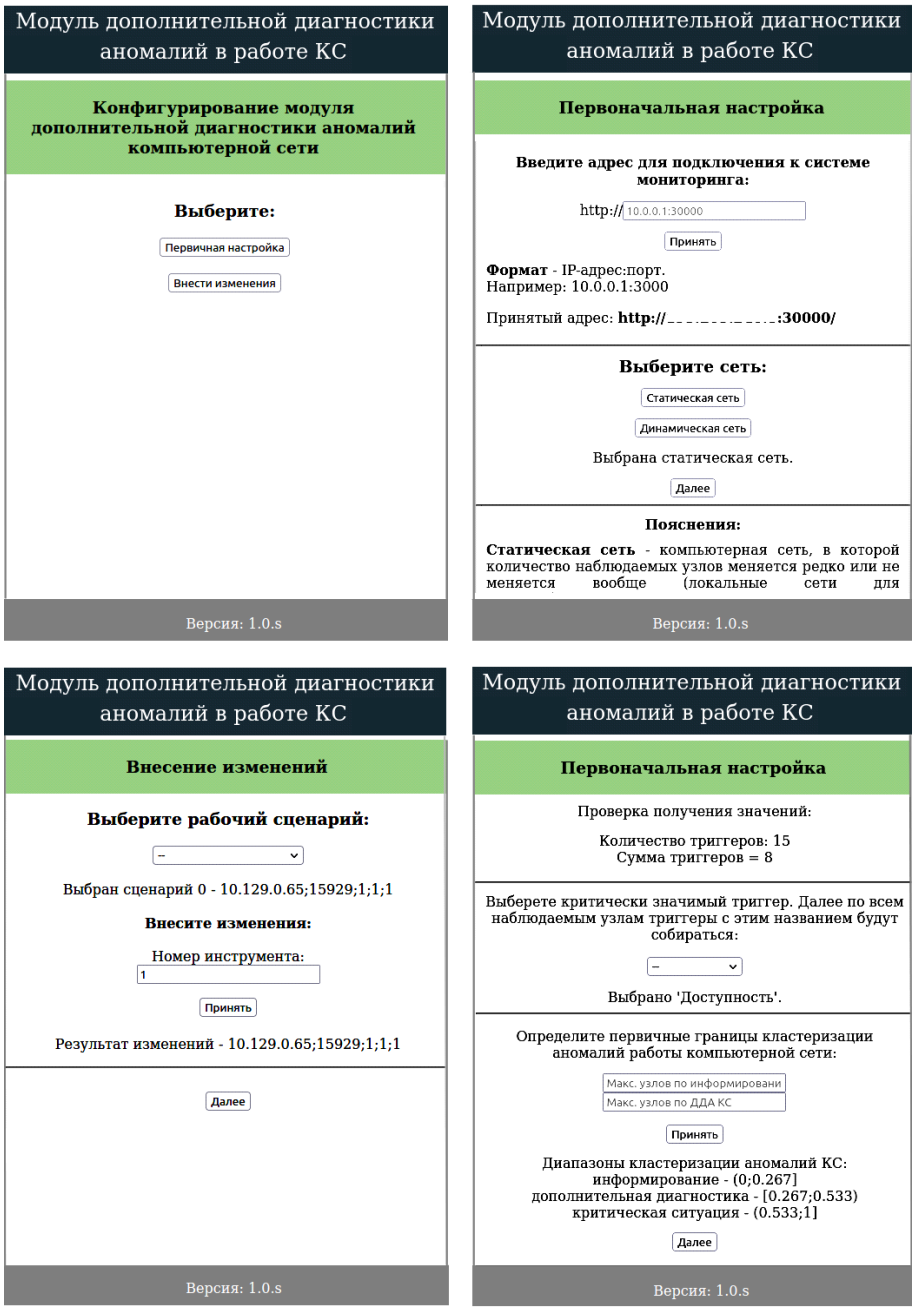

Рис. 2. Web-окна модуля ручной корректировки параметров диагностики и изменения сценариев воздействия на наблюдаемые узлы

При первоначальной конфигурации модуля дополнительной диагностики аномалий сети системный инженер отмечает критически значимые наблюдаемые узлы, определяет первоначальные границы кластеризации аномалий сети и загружает вспомогательные инструменты из перечня своего инструментария. Инструменты запускаются как скрипты. Также при первоначальной конфигурации системный инженер отмечает, какая именно сеть находится под наблюдением: статическая или динамическая. Под статической КС понимается сеть, где количество наблюдаемых узлов не изменяется или крайне редко изменяется. Под динамической КС понимается сеть, где количество наблюдаемых узлов периодически изменяется. После первоначальной настройки модуль дополнительный диагностики аномалий КС запускается в виде фонового процесса в операционной системе и отслеживает пороговые значения параметров критически значимых наблюдаемых сетевых узлов.

В случае выявления аномалий в работе сети запускается сбор дополнительных данных (признаков) по каждому нестабильному узлу сети и происходит проверка вспомогательных инструментов. Если по результатам этих проверок вспомогательный инструмент помог, то есть значение наблюдаемых параметров вернулось в состояние нормы, то фиксируются условия ситуации, номер инструмента и формируется рабочий сценарий. Рабочий сценарий представляет собой набор значений в виде текстовой строки и записывается в базу сценариев Redis, потому что такая резидентная система управления базами данных NoSQL класса позволяет хранить данные в структуре вида «ключ — значение». Если какие-то сценарии уже есть в базе данных, то сначала происходит проверка существующих сценариев по зафиксированным признакам, а после уже запускается формирование нового сценария.

По результатам проведенных действий системы мониторинга сети с модулем дополнительной диагностики аномалий осуществляется информирование системного инженера о ситуации и проведенных действиях. Информирование может осуществляться по разным каналам связи: e-mail, Telegram, СМС и другим. Запуск информирования по соответствующему каналу связи осуществляется в виде скриптов.

Предложенное программное решение было проверено на соответствие требованиям, предъявляемым к архитектуре системы мониторинга функционирования КС с модулем диагностики аномалий в работе [9]. Результаты сверки на соответствие (см. таблицу 1) показали, что реализованное программное решение удовлетворяет всем требованиям, которые были предъявлены.

4. ТЕСТИРОВАНИЕ

Прежде чем запускать диагностику возникшей аномалии в работе сети, ситуацию необходимо выявить. Выявление аномальных ситуаций основывается на результатах, полученных в исследованиях [8, 10].

При кластеризации аномалий сети диапазоны разделяют ситуации для следующих действий:

— 0 — когда ничего не надо делать;
— (0; граница 1) — когда достаточно только информирования;
— [граница 1; граница 2) — когда необходимо запускать формирование сценария воздействия на наблюдаемый узел со вспомогательным инструментом;
— [граница 2; 1) — когда необходимо запускать сценарий для предкритической ситуации;
— 1 — когда все узлы недоступны.

Таблица 1. Соответствие требованиям системы мониторинга с модулем дополнительной диагностики аномалий

Требования	Как реализовано
Наличие средств мониторинга состояния наблюдаемого сетевого объекта	В качестве средства мониторинга наблюдаемых сетевых объектов используется Zabbix
Возможность реализации методов кластеризации аномалий КС и формирования рабочих сценариев при дополнительной диагностике аномалий работы КС	Возможности на основе методов кластеризации аномалий КС и формирования рабочих сценариев при дополнительной диагностике аномалий работы КС реализованы в модуле дополнительной диагностики аномалий КС
Наличие ручного и автоматического управления формированием рабочих сценариев при дополнительной диагностике КС	Возможности управления формированием рабочих сценариев реализованы в модуле дополнительной диагностики аномалий КС и модуле корректировки параметров диагностики и изменения сценариев воздействия
Наличие модульности для возможности масштабирования системы	При разработке применялся модульный подход, который позволяет масштабировать систему мониторинга сети
Наличие раздельного хранения собираемых данных о состоянии наблюдаемого узла и рабочих сценариев для воздействия на наблюдаемый сетевой узел	Данное требование достигается путем разделения хранения статических данных в MySQL, а сценариев воздействия в Redis
Наличие блока информирования о состоянии наблюдаемого узла при проведении дополнительной диагностики аномалий работы КС	Информирование вынесено как отдельный модуль, который реализован в виде BASH-скриптов

После разработки программного обеспечения было проведено тестирование кластеризации аномалий при мониторинге функционирования КС, результаты которого отражены на рисунке 3.

В процессе тестирования было проведено 50 проверок кластеризации выявленных ситуаций в работе КС. Система мониторинга наблюдала за 53 сетевыми объектами по протоколу ICMP. Критически значимым параметром была доступность наблюдаемого объекта по сети. Для формирования первой границы кластеризации было определено, что 11 из 53 устройств может быть недоступно, для того чтобы сеть продолжала корректно функционировать. Для проведения дополнительной диагностики нестабильных узлов и формирования сценариев воздействия было определено, что максимальное количество недоступных устройств может быть 31 из 53 устройств. Соответственно, в случае выявления ситуации, когда устройств недоступно от 31 до 53, необходимо запускать сценарий для критической ситуации. В данном случае значение первой границы кластеризации получилось 0,226, а значение второй границы кластеризации — 0,585. В случаях, если происходит мониторинг динамической КС, границы кластеризации аномалий этой сети изменяются на количество добавленных или удаленных сетевых узлов. При добавлении узла под наблюдение отмечается, к какому диапазону кластеризации относится данный сетевой узел. Пример изменения границ кластеризации аномалий представлен на рисунке 4.

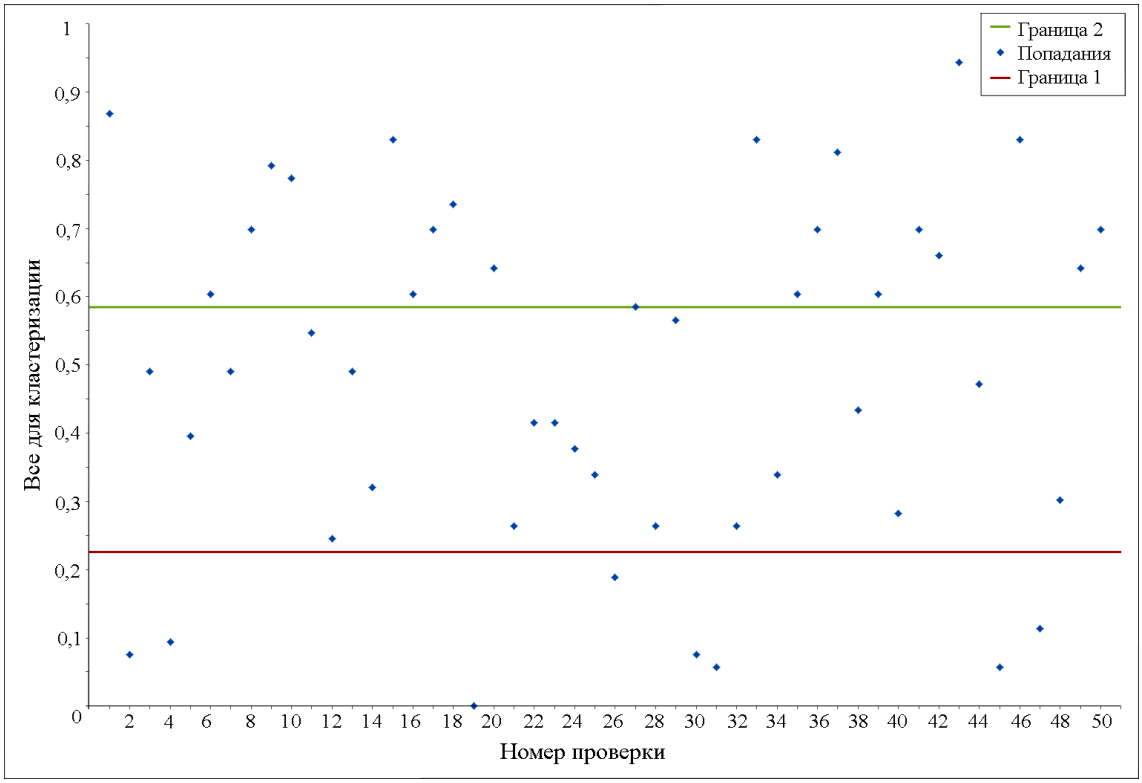

Рис. 3. Кластеризация аномалий в КС

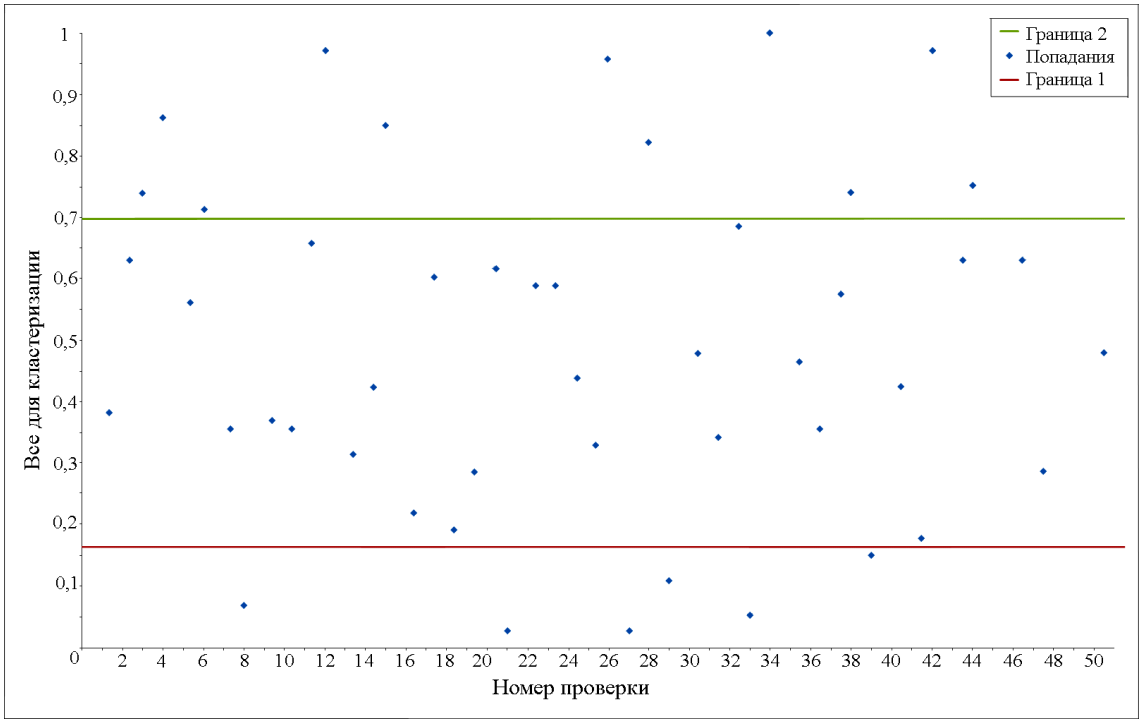

Рис. 4. Изменение границ кластеризации аномалий в работе КС

Для проверки изменения границ кластеризации было добавлено дополнительно 20 сетевых узлов с отметкой для диапазона с дополнительной диагностикой аномалии сети и запуском вспомогательных инструментов. Границы диапазонов кластеризации изменились с учетом добавленных сетевых узлов. В данном случае значение первой границы кластеризации изменилось с 0,226 на 0,164, а значение второй границы кластеризации изменилось с 0,585 на 0,699. Изменения границ диапазонов кластеризации произошли с учетом имеющихся ранее значений, то есть количественно по узлам диапазоны (0; граница 1) и [граница 2; 1) не изменились, но значения самих границ изменились с учетом добавленных узлов.

Для тестирования работы с формированием сценариев проводилось наблюдение за нагрузкой на центральный процессор (ЦП) коммутатора. Вместо критерия доступности, как при тестировании кластеризации аномалий работы сети, проводилось отслеживание нагрузки ЦП на нескольких коммутаторах. Результаты применения рабочего сценария показаны на рисунке 5.

После выявления аномалии в работе коммутаторов, нагрузка на ЦП выше 15 %, запускался сбор дополнительных данных по объемам трафика на сетевых интерфейсах нестабильного коммутатора. Было определено, что на десятом интерфейсе коммутатора начала активно передаваться multicast трафика: свыше тысячи сетевых пакетов в моменты сбора информации. В результате чего запустился вспомогательный инструмент в виде удаленного выполнения команд. В автоматическом режиме сетевой интерфейс был выключен, и было установлено соответствующее ограничение на объем передачи такого типа трафика. После этого интерфейс был автоматически включен тогда, когда значение ЦП опустилось ниже 15 %.

По результатам разработки программного обеспечения были проведены тесты кластеризации аномалий как в работе статической КС, когда границы кластеризации не изменяются, так и для динамической сети, когда границы кластеризации корректируются при изменении количества наблюдаемых узлов. Также были проведены тесты по формированию рабочих сценариев воздействия на узел при выявлении аномалии в КС на примере нагрузки ЦП коммутатора и всплесков сетевого трафика на интерфейсах. Тесты показали, что разработанное программное обеспечение дало положительные результаты при кластеризации аномалий КС и формировании рабочих сценариев воздействия на нестабильные наблюдаемые сетевые узлы.

5. ЗАКЛЮЧЕНИЕ

В данной работе представлен программный уровень системы мониторинга КС с модулем дополнительной диагностики аномалий, который не был описан в исследовании [9]. Для реализации программного решения использовался модульный подход. Сам модуль дополнительной диагностики аномалий КС разработан на языке Python3. Модуль ручной корректировки параметров диагностики и сценариев воздействия на наблюдаемые объекты разработан на языке PHP с применением HTML и CSS. Для хранения сценариев воздействия была выбрана резидентная система управления базами данных Redis. В качестве основной системы мониторинга сети для сбора данных использовался Zabbix с СУБД MySQL, для хранения статистических данных по состоянию наблюдаемых объектов. Взаимодействие с Zabbix происходит по API. Представленный программный уровень удовлетворяет требованиям к архитектуре системы мониторинга функционирования КС с модулем диагностики аномалий, которые были предъявлены в работе [9].

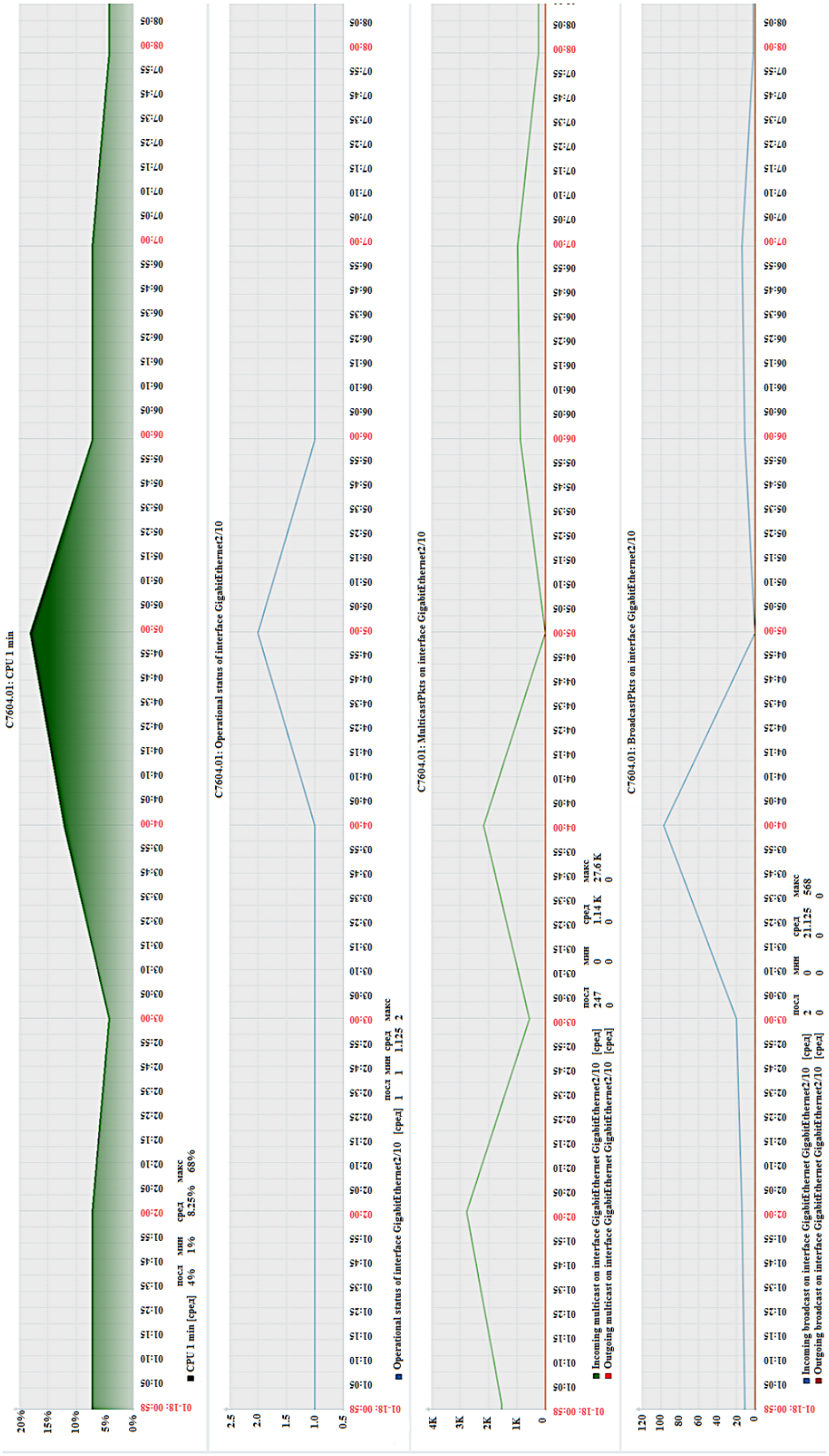

Рис. 5. Применение сценария воздействия на интерфейс коммутатора

Список литературы

1. *Mistry D., Modi P., Deokule K., Patel A., Patki H., Abuzaghleh O.* Network traffic measurement and analysis // 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2016, P. 1–7, doi:10.1109/LISAT.2016.7494141
2. Siswanto A., Syukur A., Kadir E. A. and Suratin Network Traffic Monitoring and Analysis Using Packet Sniffer // 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, 2019, P. 1–4, doi:10.1109/COMMNET.2019.8742369
3. *Kurt B., Zeydan E., Yabas U., Karatepe I. A., Kurt G. K., Cemgil A. T.* A Network Monitoring System for High Speed Network Traffic // 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK, 2016, P. 1–3, doi:10.1109/SAHCN.2016.7732965
4. *Канаев А. К., Камынина М. А., Опарин Е. В.* Способы обнаружения отклонений в функционировании элементов сети передач и данных в интересах системы управления // Бюллетень результатов научных исследований. 2012. №4 (3). С. 137–148.
5. *Дородников Н. А., Дородникова И. М., Арустамов С. А.* Пути решения проблем локальных сетей на этапах планирования и эксплуатации // Сборник научных трудов Sworld. Украина. Одесса. 2013. Т. 12. № 4. С. 66–70.
6. *Аллакин В. В.* Анализ методов оценки временных рядов сервером мониторинга информационно-телекоммуникационной сети общего пользования // Техника средств связи. 2021. № 2 (154). С. 60–80.
7. *Моисеев А. Л., Моисеева Р. Р., Шаров В. В., Зацаринная Ю. Н.* Методы тестирования и диагностирования компьютерных сетей // Вестн. Казан. тех-нол. ун-та. 2014. Т. 17, № 1. С. 315–316.
8. *Авилов М. И., Шичкина Ю. А.* Дополнительная диагностика аномалий при мониторинге динамической компьютерной сети с применением рабочих сценариев // Известия СПбГЭТУ «ЛЭТИ». 2021. № 10. С. 94–102.
9. *Авилов М. И., Шичкина Ю. А.* Многоуровневая архитектура системы мониторинга функционирования компьютерной сети с модулем диагностики аномалий // Компьютерные инструменты в образовании. 2023. № 1. С. 55–73. doi:10.32603/2071-2340-2023-1-55-73
10. *Авилов М. И., Шичкина Ю. А., Куприянов М. С.* Мониторинг информационно-коммуникационной компьютерной сети с применением модуля дополнительной диагностики // Известия СПбГЭТУ «ЛЭТИ». 2020. № 5. С. 34–45.
11. *Shykhaliev R. G.* A mobile multi-agent-based conceptual architecture for theintelligent monitoring of computer networks // Problems of information technology. 2015. № 2. P. 68-75. doi:10.25045/jpit.v06.i2.07
12. *Моисеев А. Л., Шаров В. В., Моисеева Р. Р., Зацаринная Ю. Н.* Автоматизированная система контроля электрических параметров питания узлов компьютерных сетей / Вестник Казанского технол. ун-та. 2013. Т. 16, № 11. С. 237–238
13. *Шелухин О. И., Осин А. В., Костин Д. В.* Мониторинг и диагностика аномальных состояний компьютерной сети на основе изучения "исторических данных"// T-Comm: Телекоммуникации и транспорт. 2020. Т. 14, № 4. С. 23–30.
14. *Богомолов В. А., Первухин И. Д.* Создание автоматизированной системы для мониторинга, сбора и обработки статистики для защищенной корпоративной сети КНИТУ // Современная наука: актуальные проблемы теории и практики. Серия: естественные и технические науки. 2019 №8 С. 35–42.
15. *Безрук П. А.* Разработка системы распределенного мониторинга компьютерной сети на основе Rest API // Актуальные проблемы авиации и космонавтики. 2017. № 13. С. 94–95.
16. *Будко Н. П., Васильев Н. В., Груздев А. А.* Сбор и обработка больших данных в системах мониторинга информационно-телекоммуникационных сетей средствами технологии Hadoop // Техника средств связи.СПб. 2023. № 1 (161). С. 78–88. doi: 10.24412/2782-2141-2023-1-78-88.
17. *Опрышко А. В.* Архитектура автоматизированной системы мониторинга серверов и сервисов компьютерной сети // Молодежный научно-технический вестник. 2015. № 8. http://ainsnt.ru/doc/799398.html (дата обращения 10.05.2023).

18. *Костенко Е. Ю., Дуйсенгалиев Р. Р., Барабанова Е. А.* Система мониторинга для контроля трафика технологических сетей передачи данных // Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ.Астрахань. 2015. № 4. С. 101–109.
19. *Синицын Ю.И., Кунавин Д. А.* Система мониторинга сетевой информационной инфраструктуры медицинского учреждения // Norwegian Journal of development of the International Scienc. Норвегия. Осло. 2018. №1(1). С. 45–51.
20. *Высочина О. С., Шматков С. И., Мухсин С. А.* // Анализ систем мониторинга телекоммуникационных сетей // Радиоэлектроника, информатика, управление. Украина. Запорожье. 2010. № 2. С. 139–142.
21. *Гайфулин Т. А., Костомаров Д. С.* Анализ современных систем мониторинга // Известия ТулГУ. Технические науки. 2013. Вып. 9. Ч. 2. С. 51–55.
22. *Шардаков К. С.* Сравнительный анализ популярных систем мониторинга сетевого оборудования, распространяемых по лицензии GPL // Интеллектуальные технологии на транспорте. 2018. № 1(13). С. 44–48.

Поступила в редакцию 22.06.2023, окончательный вариант — 31.08.2023.

Авилов Максим Игоревич, инженер отдела сетевых технологий СПбГЭТУ «ЛЭТИ», ✉ **avilovmaxim@gmail.com**

Computer tools in education, 2023
№ 3: 35–50
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-3-35-50

Software Level of the Computer Network Monitoring System with Additional Anomaly Diagnostics Module

Avilov M. I.[1], Systems Engineer, ✉ avilovmaxim@gmail.com

[1]Saint Petersburg Electrotechnical University,
5, building 3, st. Professora Popova, 197022, Saint Petersburg, Russia

Abstract

This article describes the software architecture level of the computer network operation monitoring system with an anomaly diagnostics module. A software solution for this level of network monitoring system architecture is proposed. Also, the article reflects the results of tests of compliance with the requirements to the architecture of the monitoring system of computer network operation with an anomaly diagnostics module: the ability to cluster anomalies in the network, manual and automatic control of forming scenarios of impact on nodes, the ability to scale the network monitoring system, the availability of separate data storage for statistics and scenarios impact on nodes and other requirements. In addition, this article presents the results of testing the developed software solution. The tests were conducted to cluster computer network anomalies and forming scenarios of impact on the observed unstable network nodes. The results show that the developed software allows you to cluster anomalies in the computer network, as well as during additional diagnostics of unstable nodes to form scenarios of impact on such nodes.

Keywords: *network monitoring system, computer network, anomaly diagnostics module, information system architecture.*

Citation: M. I. Avilov, "Software Level of the Computer Network Monitoring System with Additional Anomaly Diagnostics Module," Computer tools in education, no. 3, pp. 35-50, 2023 (in Russian); doi:10.32603/2071-2340-2023-3-35-50

References

1. D. Mistry, P. Modi, K. Deokule, A. Patel, H. Patki, and O. Abuzaghleh, "Network traffic measurement and analysis," in *Proc. of 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY, USA, pp. 1–7, 2016; doi:10.1109/LISAT.2016.7494141
2. A. Siswanto, A. Syukur, E. A. Kadir, and Suratin, "Network Traffic Monitoring and Analysis Using Packet Sniffer," in *Proc. 2019 Int. Conf. on Advanced Communication Technologies and Networking (CommNet)*, pp. 1–4, 2019; doi:10.1109/commnet.2019.8742369
3. B. Kurt, E. Zeydan, U. Yabas, I. A. Karatepe, G. K. Kurt, and A. T. Cemgil, "A Network Monitoring System for High Speed Network Traffic," in *Proc. of 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–3, 2016; doi:10.1109/sahcn.2016.7732965
4. A. K. Kanaev, M. A. Kamynina, and E. V. Oparin, "Methods of detecting of anomalies in functioning of elements of data transmission network for management system," *Bulletin of scientific research results*, vol. 3, no.4, pp. 137–148, 2012 (in Russian).
5. N. A. Dorodnikov, I. M. Dorodnikova, and S. A. Arustamo, "Puti resheniya problem lokal'nyhsetej na etapah planirovaniya i ekspluatacii" [Ways to solve local network problems in the planning and operation phases], *Collection of scientific papers SWorld*, vol. 12, no. 4, pp. 66–70, 2013 (in Russian).
6. V. V. Allakin, "Analysis of methods for estimating time series by the monitoring server of a public information and telecommunications network," *Means of Communication Equipment*, no. 2, pp. 60–80, 2021 (in Russian).
7. A. L. Moiseev, R. R. Moiseeva, V. V. Sharov, and Yu. H. Zatsarinnaya, "Metody testirovaniya i diagnostirovaniya komp'yuternyh setej" [Methods for testing and diagnosing computer networks], *Herald of Technological University*, no. 1 (17), pp. 315–316, 2014 (in Russian).
8. M. I. Avilov and Yu. A. Shichkina, "Additional diagnostics of anomalies when monitoring a dynamic computer network using working scenarios," *Proceedings of Saint Petersburg Electrotechnical University*, no. 10, pp. 94–102, 2021 (in Russian).
9. M. I Avilov and Yu. A. Shichkina, "Multilevel Architecture of a Computer Network Operation Monitoring System With an Anomaly Diagnostics Module," *Computer tools ineducation*, no. 1, pp. 55–73, 2023 (in Russian); doi:10.32603/2071-2340-2023-1-55-73
10. M. I. Avilov, Yu. A. Shichkina, and M. S. Kupriyanov, "Monitoring of an information and communication computernetwork using a neural network module," *Proceedings of Saint Petersburg Electrotechnical University*, no. 5, pp. 34–45, 2020 (in Russian).
11. R.G. Shykhaliev, "A mobile multi-agent-based conceptual architecture for theintelligent monitoring of computer networks," *Problems of information technology*, no. 2, pp. 68–75, 2015; doi:10.25045/jpit.v06.i2.07
12. A. L. Moiseev, V. V. Sharov, R. R. Moiseeva, and Yu. H. Zatsarinnaya, "Avtomatizirovannaya sistema kontrolya elektricheskih parametrov pitaniya uzlov komp'yuternyh setej" [Automated system for controlling electrical parameters of computer network nodes power supply], *Herald of Technological University*, vol. 16, no. 11, pp. 237–238, 2013 (in Russian).
13. O. I. Sheluhin, A. V. Osin, and D. V. Kostin, "Monitoring and diagnostics of anomalous states in a computer network based on the study of "historical data" *T-Comm*, vol. 14, no.4, pp. 23–30, 2020 (in Russian).
14. V. A. Bogomolov and I. D. Pervukhin, "Creating an automated system for monitoring, collection and processing statistics for a protected corporate network KNITU," *Modern Science: actual problems of theory and practice. Ser. Natural and Technical Sciences*, no. 8, pp. 35–42, 2019 (in Russian).
15. P. A. Bezruk, "Developing distributed monitoring system of the computer Network based on rest api," *Proc. of Current problems of aviation and cosmonautics*, no. 13, pp. 94–95, 2017 (in Russian).
16. N. P. Budko, N. V. Vasiliev, and A. A Gruzdev, "Collection and processing of big data in monitoring systems of information and telecommunication networks by means of Hadoop technology," *Means of*

Communication Equipment, no. 1 (161), pp. 78–88, 2023 (in Russian); doi:10.24412/2782-2141-2023-1-78-88
17. A. V. Opryshko, “Arhitektura avtomatizirovannoj sistemy monitoringa serverov i servisov komp’yuternoj seti” [Architecture of an automated system for monitoring servers and services of a computer network], in *Youth Scientific and Technical Bulletin*, no. 8, pp. 1–8, 2015 (in Russian). [Online]. Available: http://ainsnt.ru/doc/799398.html
18. E. Yu. Kostenko, R. R. Duysengaliev, and E. A. Barabanova, “Monitoring systems for traffic control of technological networks of data transmission,” *Vestn. Astrakhan State Technical Univ. Ser. Management, Computer Sciences and Informatics*, no. 4, pp. 101–109, 2015 (in Russian).
19. Yu. Sinitsyn and D. Kunavin, “Monitoring system of the network infrastructure of the medical institution,” *Norwegian Journal of development of the International Science*, no. 1(1), pp. 45–51, 2018.
20. O. S. Vysochina, S. I. Shmatkov, and S. A. Muchsin, ”Analysis of telecommunications networks monitoring systems,” *Radio Electronics, Computer Science, Control*, no. 2, pp. 139–142, 2010.
21. T. A. Gayfulin and D. S. Kostomarov, “Analysis of modern monitoring systems,” *Proceedings of Tula State University*, no. 9, pp. 51–55, 2013 (in Russian).
22. K. S. Shardakov, “Sravnitelnyi analiz populiarnykh sistem monitoringa setevogo oborudovaniia, rasprostraniaemykh po litsenzii GPL” [Comparative Analysis of the Popular Monitoring Systems for Network Equipment DistributedUnder the GPL License], *Intellectual Technologies on Transport*, no. 1(13), pp. 44–48, 2018 (in Russian).

Received 22-06-2023, the final version — 31-08-2023.

Maxim Avilov, Systems Engineer, Network Technologies Department, Saint Petersburg Electrotechnical University, ✉ **avilovmaxim@gmail.com**