Компьютерные инструменты в образовании, 2023
№ 1: 55–73
УДК: 004.67
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-1-55-73

инженерия программного обеспечения

МНОГОУРОВНЕВАЯ АРХИТЕКТУРА СИСТЕМЫ МОНИТОРИНГА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНОЙ СЕТИ С МОДУЛЕМ ДИАГНОСТИКИ АНОМАЛИЙ

Авилов М. И.[1], инженер, ✉ avilovmaxim@gmail.com
Шичкина Ю. А.[1], доктор техн. наук, профессор, shichkina@etu.ai

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

Аннотация

Данная статья является продолжением исследований, которые посвящены своевременному выявлению и оперативному реагированию на аномалии в работе компьютерной сети при помощи системы мониторинга сети с модулем дополнительной диагностики аномалий. Приведена многоуровневая архитектура системы мониторинга сети с модулем дополнительной диагностики аномалий, в которой учитывается модульный способ организации работы такой информационной системы. Описаны ситуации, в которых предлагаемая архитектура может применяться, приведены ее преимущества и недостатки. Также описывается процесс формирования рабочих сценариев при обработке аномалии в функционировании компьютерной сети с учетом приведенной архитектуры системы мониторинга с модулем дополнительной диагностики аномалий такой сети. Рассмотрены подходы к формированию входных и выходных данных при создании рабочего сценария.

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

Цитирование: 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

1. ВВЕДЕНИЕ

Мониторинг компьютерных сетей (КС) — одна из важнейших задач для любой организации, функционирование которой зависит от ее компьютерных систем. Мониторинг сети помогает обеспечить бесперебойную работу систем, которые в качестве транспортной составляющей по передаче данных между хостами используют компьютерную сеть. Системы мониторинга сети позволяют отслеживать, своевременно выявлять, информировать о возникших состояниях компьютерной сети. Такие информационные системы значительно упрощают решения задач по определению причин возникших проблемных ситуаций и оперативному их устранению.

Несмотря на то, что в настоящее время применяются различные системы мониторинга компьютерной сети, построенные на различных архитектурах информационных систем [1–6], в организациях задействуются команды системных инженеров для поддержания работы компьютерных сетей и систем в штатном режиме. Также применяются ITIL (Information Technology Infrastructure Library — библиотека инфраструктуры информационных технологий) [7], ITSM (IT Service Management, управление ИТ-услугами) [8] для формирования взаимодействия команд ИТ-специалистов по разработке и поддержанию инфраструктуры различных организаций. Однако существующие системы мониторинга функционирования компьютерной сети, которые учитывали бы различные архитектурные уровни информационной системы, применяются нечасто.

В данной статье предлагается архитектура системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий, основанная на предыдущих исследованиях [9–11]. Архитектура является многоуровневой, учитывая модульный подход к организации работы такой информационной системы. Система мониторинга компьютерной сети позволяет в режиме реального времени выявлять аномалии в работе компьютерной сети, реагировать, формировать рабочие сценарии и информировать системного инженера о возникшей ситуации.

2. ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ

На сегодняшний день много работ посвящено системам мониторинга работы компьютерной сети. Развитие как самих компьютерных сетей, так и систем мониторинга КС привели к тому, что требуется учитывать разнородность элементов сети (различные модели коммутаторов, маршрутизаторов, файерволов, прокси-серверов, беспроводных точек доступа и др.), чтобы обеспечивать корректность функционирования всей организации. Для такого обеспечения могут применяться решения по созданию систем мониторинга компьютерной сети, основанные на различных архитектурах информационных систем.

Так, в [12] предлагается решение, основанное на концептуальной архитектуре интеллектуального мониторинга компьютерных сетей. В основе архитектуры используются интеллектуальные мобильные мульти-агенты, которые осуществляют наблюдение за отдельными составляющими компьютерной сети. Например, наблюдение за состоянием сетевого оборудования, сетевыми соединениями, загруженностью каналов трафиков, состоянием сервисов на хостах. Такая концептуальная архитектура расширяет охват системы мониторинга и легко масштабируется, в случае необходимости.

Модель, способная осуществлять мониторинг работы между мобильными устройствами и персональным компьютером по Wi-Fi с помощью портативных устройств, приводится в [13]. Мониторинг узла в сети возможен путем получения текущего состояния сетевого узла на телефоне с операционной системой Android. Благодаря этому можно производить наблюдения за состоянием сети мобильно, то есть без привязки к конкретному компьютеру системного инженера.

Модель, основанная на машинном обучении, рассматривается в [14]. Авторами предлагается модель для анализа трафика при мониторинге КС с целью выявления аномалий и дальнейшего формирования шаблонов для проактивного мониторинга работы сети. Применение таких шаблонов позволяет управлять потоками трафика, что позволяет предотвращать снижение производительности сети в случаях её загруженности большими объемами передаваемых данных.

Работы [15, 16] описывают современные проблемы в области мониторинга беспроводных сетей как для Интернета вещей, так и для различных физических киберсистем. Авторы предлагают архитектурные решения для беспроводных сетей, которые позволяют выявлять определенные сигналы в виде отклонений от нормы по аномалиям при мониторинге КС путем захвата и анализа сетевых пакетов.

В [17] представлена реализация системы сетевого мониторинга данных авиационных радаров на основе PRTG (Paessler Router Traffic Grapher). Архитектура такой системы основана на PRTG, а сбор данных осуществляется при помощи SNMP (Simple Network Management Protocol).

SNMP, NetFlow, RMON (Remote Network MONitoring) [18–21] часто применяются при мониторинге КС и разработке архитектуры системы мониторинга компьютерной сети. В [22] в архитектуре системы Zabbix может применяться как SNMP, IPMI (Intelligent Platform Management Interface), проверки по ICMP(Internet Control Message Protocol), так и собственные zabbix-агенты на серверах, компьютерах конечных пользователей. В системе мониторинга компьютерной сети Nagios [23], которая основана на клиент-серверной архитектуре, проверки осуществляются при помощи SNMP, ICMP и других способов с возможностью создания карт сетей. Авторы сообщают, что за счет возможности применения плагинов можно разрабатывать свои способы проверок хостов и различных сетевых служб.

В работе [24] авторы предлагают архитектуру системы мониторинга компьютерной сети, основанную на Hadoop MapReduce и Spark для ускорения обработки данных путем разделения и одновременной обработки потоков данных с целью выявления аномалий в функционировании компьютерной сети. Архитектура системы состоит из агентов мониторинга, облачной инфраструктуры и операционного центра. Агенты собирают информацию и передают через облачную инфраструктуру в операционный центр, где дальше уже применяется решение по дальнейшим действиям, связанным с выявленной аномалией в функционировании компьютерной сети.

В работе [25] проводится анализ современных технологий и систем мониторинга информационно-телекоммуникационных сетей общего пользования, а также предлагается обобщенная архитектура построения перспективных систем сетевого мониторинга и общая субъектно-объектная ее модель в виде «сущность-связь». Прогнозирование аномальных ситуаций осуществляется на основе собираемых метрик, отражающих состояние сетевых элементов, с применением метода символического представления временных рядов. Как практическая значимость отмечено, что выработан общий подход к построению алгоритма функционирования перспективных систем сетевого мониторинга.

Проведенный анализ исследований в области мониторинга работы компьютерной сети показывает, что в настоящее время существует много различных архитектур систем мониторинга функционирования компьютерной сети. Однако архитектур систем мониторинга состояния компьютерной сети, которые сочетали бы в себе возможности проактивного и реактивного мониторинга работы сети, значительно меньше. Несмотря на то что такие архитектуры комбинируют способы проактивного и реактивного мониторинга сети, они не учитывают возможности проведения дополнительной диагностики возникшей ситуации, когда невозможно осуществить прогноз из-за нехватки данных или среагировать по заранее написанному сценарию, в автоматическом режиме с целью формирования рабочих сценариев для устранения причин аномалий в работе компьютерной сети.

Целью проводимых исследований являлась разработка архитектуры системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий, позволяющая учитывать возможность в автоматическом режиме формировать сценарии по устранению аномалий в работе компьютерной сети при помощи вспомогательных инструментов диагностики сети. Для это была разработана многоуровневая архитектура системы мониторинга функционирования компьютерной сети. В данной статье описаны основные уровни системы и их связность между собой. Представлен подход к модульной организации работы такой информационной системы.

3. ТРЕБОВАНИЯ К АРХИТЕКТУРЕ СИСТЕМЫ МОНИТОРИНГА КОМПЬЮТЕРНОЙ СЕТИ С МОДУЛЕМ ДОПОЛНИТЕЛЬНОЙ ДИАГНОСТИКИ АНОМАЛИЙ

Проектирование любой информационной системы опирается на требования, которым эта система должна удовлетворять. Без таких требований процесс создания информационной системы может стать хаотичным и неэффективным, что приведет к дорогостоящим издержкам в реализации или к некорректно функционирующей информационной системе (ИС).

Система мониторинга компьютерной сети с модулем дополнительной диагностики аномалий является информационной системой с определенной архитектурой, отвечающей задачам поддержания компьютерной сети в нормальном рабочем состоянии и задачам управления компьютерной сетевой инфраструктурой. В данном случае система мониторинга компьютерной сети с модулем дополнительной диагностики решает задачи адаптивного управления относительно возникающих аномальных ситуаций в работе компьютерной сети. Благодаря такому решению, сформированное операционное управление сетью остается, а ситуативное управление при возникновении аномальных ситуаций в сети осуществляется через формирование рабочих сценариев, которые фиксируются в соответствующей базе данных.

Несмотря на то, что такая система должна обеспечивать автоматическое проведение дополнительной диагностики КС, необходимость в ручном управлении формированием рабочих сценариев по устранению аномалий работы компьютерной сети остается. Кроме того, должна быть возможность конфигурирования составляющей дополнительную диагностику аномалий системы мониторинга компьютерной сети.

На основе вышеизложенного к архитектуре системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий предъявляются следующие требования:

- наличие средств мониторинга состояния наблюдаемого сетевого объекта;
- возможность реализации методов кластеризации аномалий КС и формирования рабочих сценариев при дополнительной диагностике аномалий работы компьютерной сети;
- наличие ручного и автоматического управления формированием рабочих сценариев при дополнительной диагностике КС;
- наличие модульности для возможности масштабирования системы;
- наличие раздельного хранения собираемых данных о состоянии наблюдаемого узла и рабочих сценариев для воздействия на наблюдаемый сетевой узел;
- наличие блока информирования о состоянии наблюдаемого узла при проведении дополнительной диагностики аномалий работы компьютерной сети;
- наличие ручного конфигурирования составляющей дополнительную диагностику аномалий системы мониторинга компьютерной сети.

4. УРОВНИ АРХИТЕКТУРЫ СИСТЕМЫ МОНИТОРИНГА КОМПЬЮТЕРНОЙ СЕТИ С МОДУЛЕМ ДОПОЛНИТЕЛЬНОЙ ДИАГНОСТИКИ АНОМАЛИЙ

При проектировании архитектуры системы мониторинга КС с модулем дополнительной диагностики аномалий применяется многоуровневый подход. Такой подход позволяет снизить сложность разрабатываемой системы путем разбиения ИС на части, которые легче анализировать, а значит, и заменять, усложнять или упрощать отдельно взятые компоненты, масштабировать, повышать надежность системы мониторинга КС с модулем дополнительной диагностики аномалий. Также многоуровневый подход позволяет делать изменения на определенном уровне, не затрагивая или минимально изменяя другие уровни архитектуры системы мониторинга КС с модулем дополнительной диагностики аномалий, что повышает гибкость такой системы.

Архитектура системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий в работе компьютерной сети состоит из следующих логически связанных между собой уровней:

1. Информационный уровень.
2. Функциональный уровень.
3. Системный уровень.
4. Программный уровень.
5. Уровень структуры входных и выходных данных.

Программный уровень в данной статье не рассматривается. Это отдельная проблема с множеством различных вариантов решений.

4.1. Информационный уровень

Информационный уровень архитектуры системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий необходим для того, чтобы сформировать направления движения потоков информации в процессе работы информационной системы.

Информационный уровень, который представлен на рисунке 1, описывает потоки информации для сбора, обработки, хранения и представления результатов работы системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий.

Информационный уровень сложно отделить от функционального уровня, потому что на стыках информационных потоков связывающие по смыслу узловые соединения в основе своей представляют функции сбора, хранения, обработки, передачи и представления информации. В качестве информационного объекта здесь понимаются блоки данных, в которых может быть отражена информация по состоянию наблюдаемого сетевого узла, информация по воздействию на наблюдаемый объект. Потоки информации, которые представлены на рисунке 1, показывают, по каким путям передается информация между информационными объектами.

Описание движения потоков информации

Актуальные данные с наблюдаемого объекта могут быть получены активным и пассивным способом. В случае пассивного способа данные передаются через определённые промежутки времени с наблюдаемого объекта без ожидания каких-либо запросов на передачу актуальных данных. В случае активного способа данные передаются только после получения запроса на предоставление актуальной информации о состоянии наблюдаемого объекта.

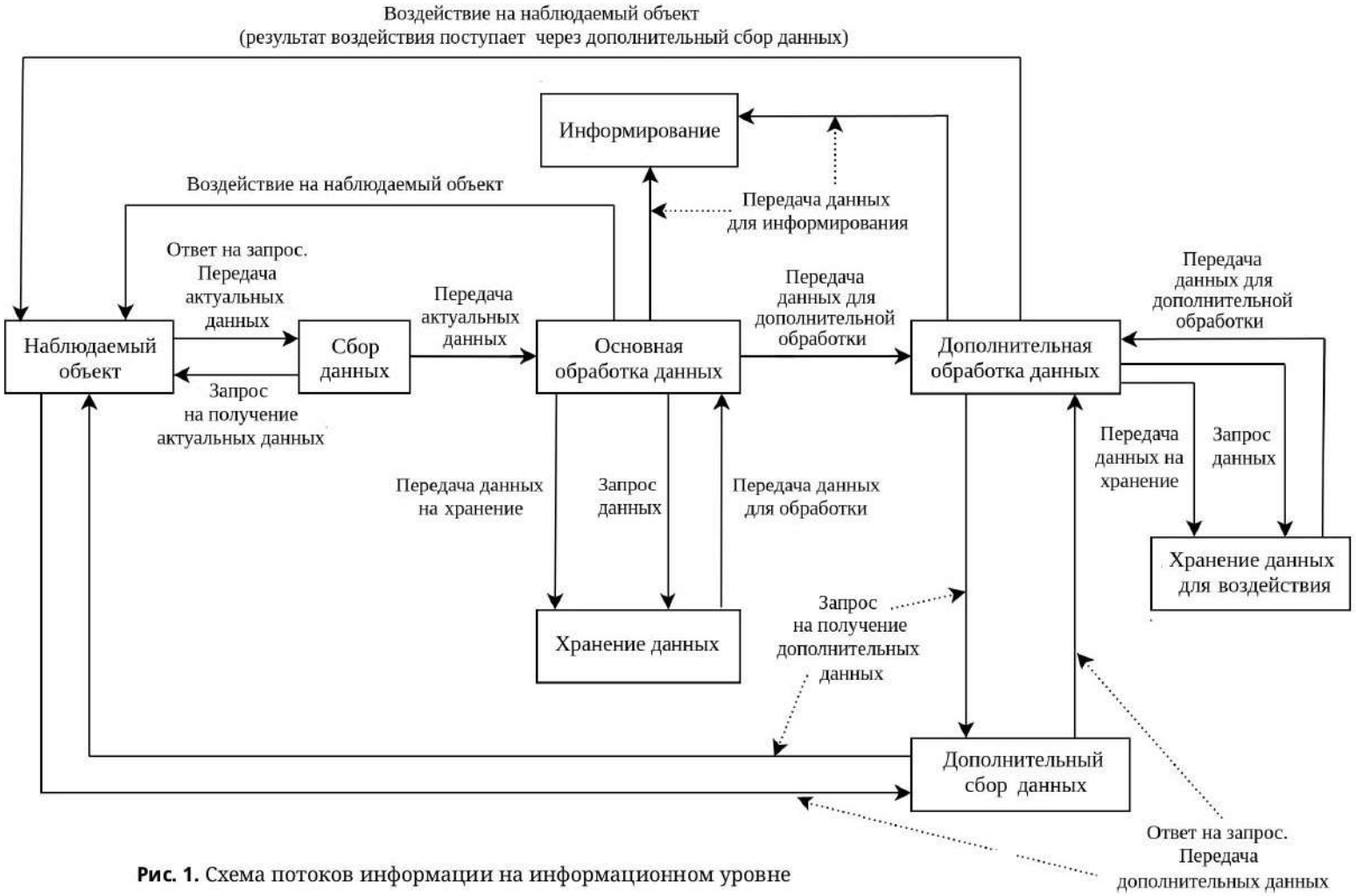

Рис. 1. Схема потоков информации на информационном уровне

После того как данные собраны с наблюдаемого объекта, они передаются в блок основной обработки данных. Под основной обработкой данных понимается обработка данных по заранее установленным сценариям реагирования на возникающее событие, то есть происходит реакция на событие, которое известно как обрабатывать.

В блоке основной обработки данных о состоянии наблюдаемого объекта происходит передача данных на хранение и, в случае необходимости, передача сведений о состоянии наблюдаемого узла блоку информирования. Если происходит воздействие на узел, то сведения о результатах воздействия также передаются блоку информирования. В случае необходимости проведения дополнительной обработки данных они передаются соответствующему блоку.

Дополнительная обработка данных происходит в случаях, если неизвестно, как реагировать на возникшую ситуацию по заранее определенному сценарию. В процессе дополнительной обработки данных осуществляется дополнительный сбор информации для корректного проведения воздействия на наблюдаемый объект. Воздействие на наблюдаемый объект выполняется с целью возвращения объекта в состояние, определённое для этого объекта как норма. Информация о результате воздействия передается через блок дополнительного сбора данных. В случае успешного воздействия на наблюдаемый объект формируется рабочий сценарий, который передаётся в блок хранения данных для воздействия на наблюдаемый объект. Такие сценарии могут со временем изменяться. В случае исчерпания всех возможностей воздействия на наблюдаемый объект системой производится формирование соответствующей информации о ситуации.

По результатам проведения дополнительной обработки данных происходит информирование системного инженера о состоянии наблюдаемого объекта и о результатах поведения воздействия на наблюдаемый объект.

4.2. Функциональный уровень

Функциональный уровень архитектуры системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий необходим для того, чтобы автоматизировать процессы работы с потоками информации, которые описаны на информационном уровне.

Функциональный уровень, который представлен на рисунке 2, показывает, как потоки информации обрабатываются и передаются от одной функции к другой.

В качестве компонентов функционального уровня понимаются связующие блоки, которые обрабатывают потоки информации. Такие компоненты позволяют учитывать следующие характеристики:

— возможность повторного использования — компоненты могут быть использованы несколько раз при проведении дополнительной диагностики аномалий КС;
— заменимость — компоненты, которые могут быть заменены аналогичными другими компонентами;
— расширяемость — возможность расширения существующих компонент для создания нового функционала или масштабирования системы;
— инкапсулированность — возможность по-разному реализовывать сам компонент в силу того, что функциональные возможности компонента не раскрывают детали внутренних процессов пользователю;
— независимость — компоненты минимально связаны между собой.

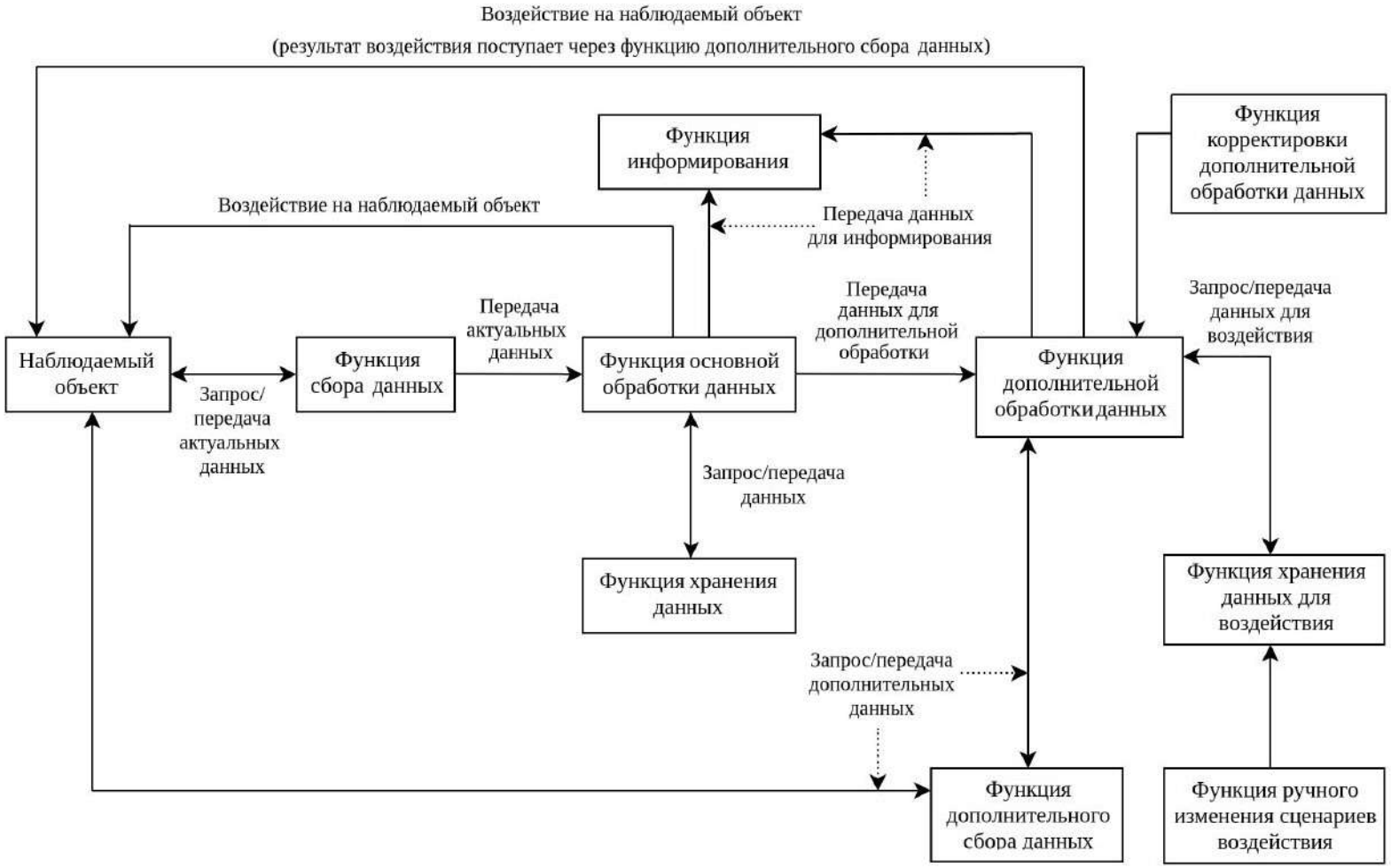

Рис. 2. Функциональный уровень

Обработка данных функциями

Актуальные данные с наблюдаемого объекта собираются при помощи функции сбора данных активным или пассивным способом. Далее данные передаются функции основной обработки данных, которая осуществляет разбор полученных данных и определяет необходимость воздействия на наблюдаемый узел по известным сценариям, передачи данных функции дополнительной обработки данных, передачи данных функции информирования, взаимодействие с функцией хранения данных.

Если требуется проведение дополнительной диагностики аномалии в работе компьютерной сети, то происходит уточняющий сбор данных с наблюдаемого объекта через функцию дополнительного сбора данных. Далее функция дополнительной обработки данных анализирует полученную информацию, после чего осуществляется передача данных функции информирования или функции хранения данных для воздействия. В случае изменения условий дополнительной обработки данных применяется функция корректировки дополнительной обработки данных. В случае необходимости ручного изменения рабочих сценариев применяется функция ручного изменения сценариев воздействия.

С точки зрения реализации функциональный компонент может быть как программным, так и аппаратно-программным решением.

4.3. Системный уровень

Системный уровень архитектуры системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий необходим для того, чтобы сформировать организацию взаимодействия компонент функционального уровня друг с другом, внешней средой, возможностями масштабирования, которые способствуют развитию такой системы.

В данном случае на системном уровне применяется модульный подход, где система разделяется на модули, которые логически связаны между собой с целью выполнения задач, поставленных перед системой мониторинга компьютерной сети с модулем дополнительной диагностики аномалий.

На рисунке 3 представлено взаимодействие модулей системного уровня архитектуры системы мониторинга КС с модулем дополнительной диагностики аномалий.

Система мониторинга КС собирает данные с наблюдаемого объекта, сохраняет в базу данных, проводит основную обработку собранных данных. В случае необходимости передает данные модулю информирования. Если требуется дополнительная диагностика, то данные передаются модулю дополнительной диагностики аномалий компьютерной сети. В результате дополнительной диагностики аномалий компьютерной сети (ДДА КС) данные передаются базе данных рабочих сценариев и модулю информирования, который предоставляет информацию системному инженеру.

В случае, если требуется ручная перенастройка модуля дополнительной диагностики аномалий КС, то системный инженер обращается к модулю ручного конфигурирования модуля ДДА КС и изменения рабочих сценариев, который взаимодействует с модулем дополнительной диагностики аномалий компьютерной сети. Если требуется ручное изменение рабочих сценариев, то также идет обращение к этому модулю.

Более детальное описание взаимодействия модулей с учетом функций представлено на рисунке 4.

Прежде чем системой проводится дополнительная диагностика аномалий в работе компьютерной сети, ею формируются входные данные для кластеризации аномалий се-

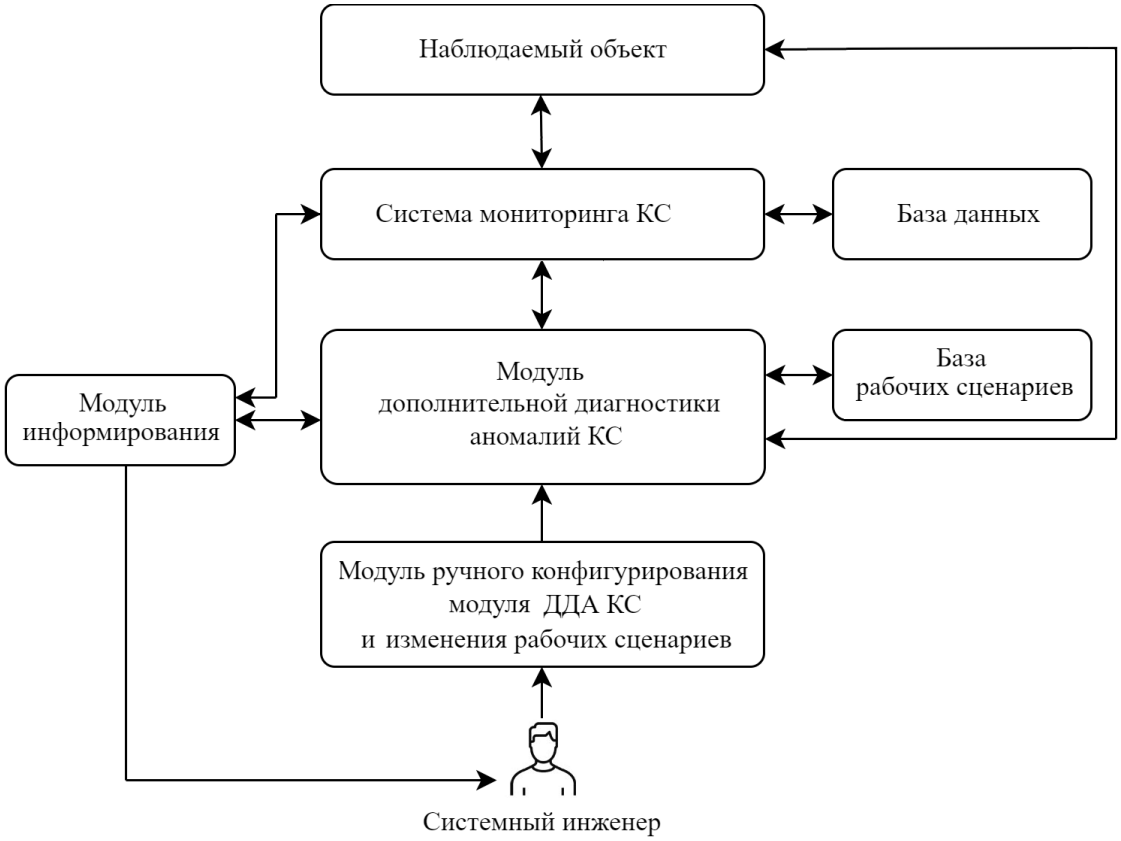

Рис. 3. Взаимодействие модулей на системном уровне архитектуры системы мониторинга

ти. Формирование данных для кластеризации аномалий в сети описано в статьях [10, 11]. После кластеризации аномалий в КС данные для дополнительной диагностики работы сети структурируются определенным образом.

Выходными данными являются сформированные рабочие сценарии, при помощи которых происходит воздействие на наблюдаемые объекты компьютерной сети. В случае критической ситуации выходными данными является информация о признаках для запуска специального сценария. В случае если нет необходимости проведения дополнительной диагностики функционирования компьютерной сети, то выходными являются данные по признакам для информирования о возникшей ситуации.

Входные данные для дополнительной диагностики компьютерной сети

На рисунке 5 схематично показано как происходит формирование множества триггеров признаков (триггеров) для дополнительной диагностики аномалий КС.

Сначала система мониторинга компьютерной сети собирает все значения всех наблюдаемых параметров. Далее для дополнительной диагностики работы КС выбираются критически значимые наблюдаемые параметры, и к этим параметрам прикрепляются триггеры, которые отражают состояние «нормы» для этих критически значимых параметров.

Такой блок данных необходим как для дельнейшей кластеризации аномалий КС, так и для формирования рабочего сценария в случае проведения дополнительной диагностики аномалий работы КС по методике, предложенной в статье [11].

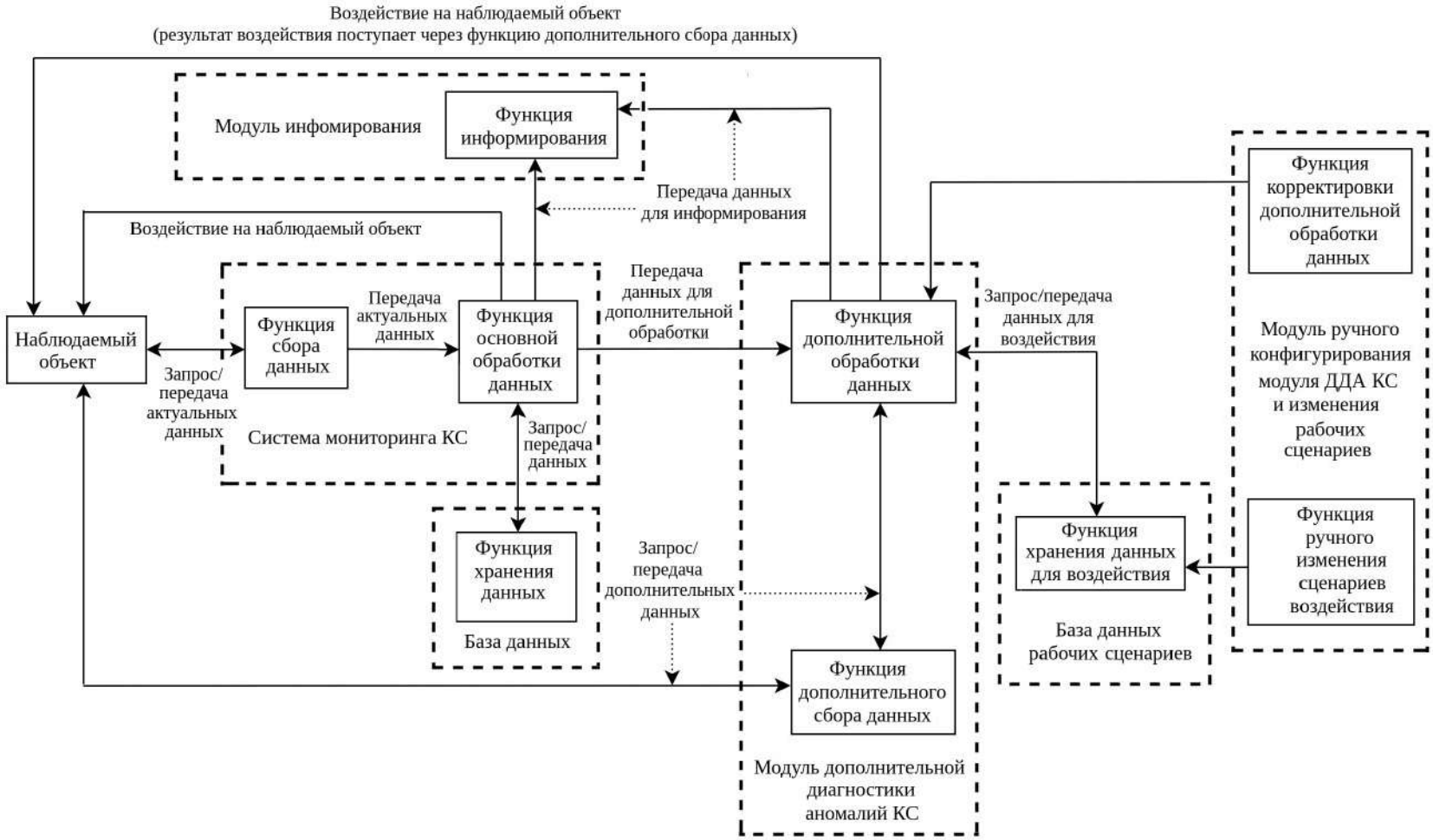

Рис. 4. Системный уровень

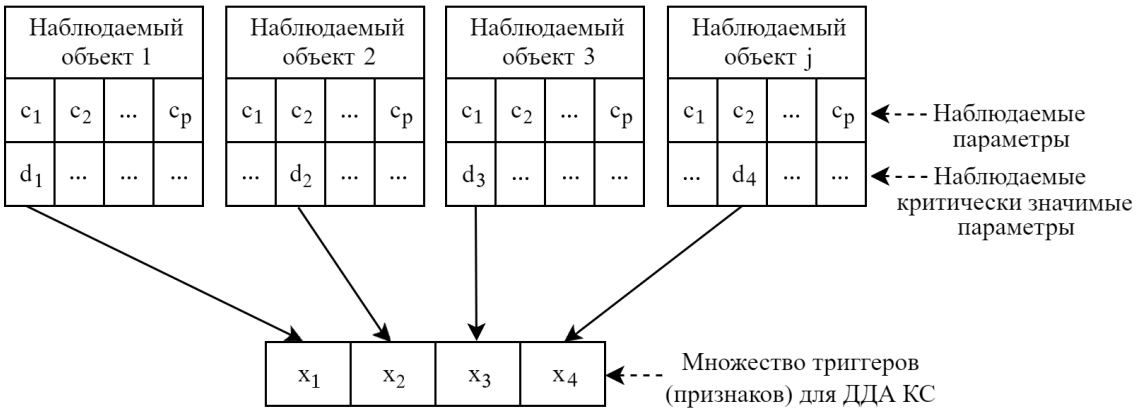

Рис. 5. Формирование признаков для дополнительной диагностики аномалий КС

После того как множество признаков сформировано в процессе дополнительной диагностики аномалий компьютерной сети, они передаются для формирования рабочего сценария.

4.4. Уровень структуры входных и выходных данных

Формирование рабочего сценария

Сам процесс формирования рабочего сценария отражен в методе формирования рабочих сценариев при дополнительной диагностике аномалий в работе КС, который описан в статье [11]. На рисунке 6 схематично показано, как происходит формирование рабочего сценария.

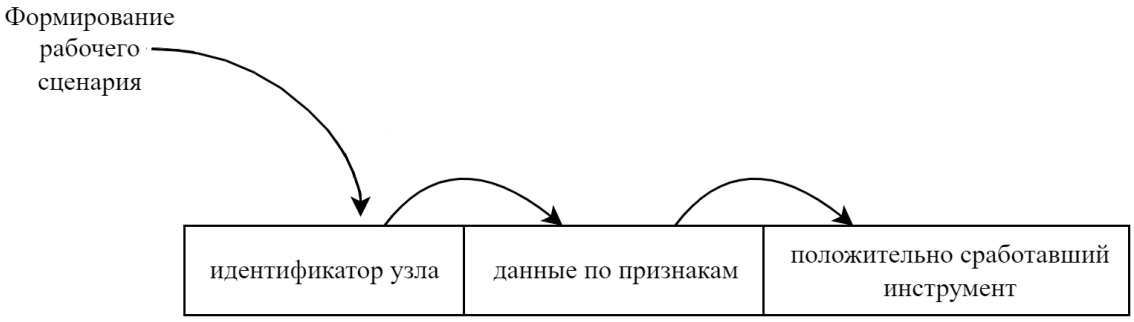

Рис. 6. Формирование рабочего сценария

Рабочий сценарий состоит из идентификатора наблюдаемого узла (объекта), данных по признакам, положительно сработавшего вспомогательного инструмента. Сначала добавляется идентификатор узла. Он известен, потому что взаимодействие между системой мониторинга и наблюдаемым узлом происходит по клиент-серверной архитектуре, в формате запрос-ответ. После этого добавляются данные по признакам, а далее положительно сработавший вспомогательный инструмент. Определение такого инструмента схематично представлено на рисунке 7.

Изначально выбирается первый инструмент по списку вспомогательных инструментов, который определяет системный инженер на основе имеющегося у него инструментария. Далее при помощи выбранного инструмента системой осуществляется воздействие

Рис. 7. Определение положительного рабочего инструмента при формировании рабочего сценария

на наблюдаемый узел. В случае если инструмент помог устранить возникшую аномалию в работе КС, критически значимый параметр вернулся в состояние нормы, то этот инструмент считается положительно сработавшим инструментом. Если нет, то отрицательно сработавшим инструментом, в рабочий сценарий он не добавляется, и происходит переход к следующему вспомогательному инструменту с фиксацией имеющихся признаков. Такой процесс выбора происходит до тех пор, пока не выявится положительно сработавший инструмент или инструменты не закончатся.

Выходные данные дополнительной диагностики компьютерной сети

Более детально рабочий сценарий представлен на рисунке 8, где информация структурирована относительно идентификатора наблюдаемого узла (объекта) и данных по признакам.

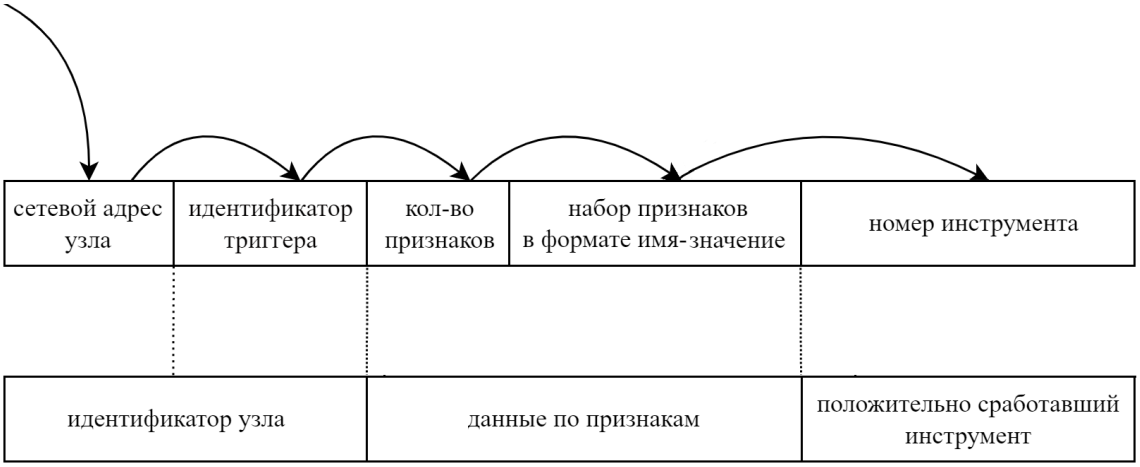

Рис. 8. Проверка рабочего сценария

Идентификатор наблюдаемого узла состоит из сетевого адреса узла и идентификатора триггера, который был положительно сработавшим (равен 1) относительно наблюдаемого узла в рамках формирования признаков для проведения дополнительной диагностики аномалий компьютерной сети. В данном случае, значение такого триггера, выбор

которого показан на рисунке 5, является одновременно признаком аномалии работы компьютерной сети и параметром, который отражает состояние нормы наблюдаемого узла. В случае если значение такого триггера равно 0, то воздействие на наблюдаемый узел не производится.

После того как идентификатор узла сформирован, формируются данные по признакам. Такие данные состоят их количества признаков и значения самих признаком. Это необходимо, чтобы можно было определить в случае проверки по базе данных рабочих сценариев, есть ли уже рабочий сценарий с нужным количеством и нужными сработавшими признаками аномалии компьютерной сети или нет.

Далее, когда сформированы идентификатор узла и данные по признакам, после выбора вспомогательного инструмента, номер соответствующего инструмента фиксируется в блоке данных, отражающий положительно сработавший инструмент. Этот процесс показан на рисунке 6.

Решения на основе предложенной архитектуры системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий позволяют организовать действия по систематизации и автоматизации процессов мониторинга за элементами функционирования компьютерной сети, своевременного выявления и оперативного реагирования на аномалии на различных участках сети. Однако применение таких решений должно опираться на преимущества и недостатки, которые отражены в таблице 1, чтобы получить необходимый результат от построения системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий.

Таблица 1. Преимущества и недостатки архитектуры системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий

Преимущества	Недостатки
Многоуровневый подход. Легче понять, какую составляющую системы можно дополнительно модернизировать и учитывать влияние такой модернизации на остальные части системы мониторинга КС	**Ручное определение перечня вспомогательных инструментов**. Системный инженер определяет, какие инструменты могут быть применены для дополнительной диагностики аномалии работы компьютерной сети
Модульность. Возможность масштабировать систему и изменять только отдельные модули в случае необходимости. Остальные модули могут быть без изменений	**Первоначальная конфигурация.** Требуется первоначальная конфигурация модуля диагностики аномалии работы компьютерной сети. Определение первоначальных диапазонов кластеризации и формирование списка вспомогательных инструментов
Нет привязки к определенной системе мониторинга сети. Архитектура системы мониторинга может являться основой как для модернизации имеющейся системы мониторинга, так и для создания новой системы мониторинга компьютерной сети	**Изменение количества признаков влияет на формирование рабочих сценариев.** В случае изменения количества признаков требуется формирование новых рабочих сценариев.
Эффективное хранение данных. Отдельное хранение данных по рабочим сценариям позволяет не нагружать основную базу данных системы мониторинга сети результатами вычислительных операций	**Последовательный выбор вспомогательных инструментов.** В случаях, когда нужный инструмент находится внизу списка вспомогательных инструментов дополнительной диагностики сети, необходимо дождаться пока проверятся все предыдущие вспомогательные инструменты

Преимущества	Недостатки
Возможность ручного изменения рабочих сценариев. В случае необходимости можно вручную изменить, добавить или удалить рабочий сценарий в соответствующей базе данных	**Отсутствие автоматического изменения имеющихся сценариев при добавлении новых вспомогательных инструментов диагностики сети.** В случаях, когда добавляется новый вспомогательный инструмент и этот инструмент может быть эффективнее других, то предыдущие рабочие сценарии с уже сформированными данными по инструментам могут быть изменены только вручную или удалены для автоматического формирования новых сценариев по тем же признакам
Отсутствие необходимости накапливать временные данные для ДДА КС. После первоначальной настройки модуля дополнительной диагностики аномалий компьютерной сети система может сразу работать, без ожидания накопления дополнительных статистических данных	

5. ЗАКЛЮЧЕНИЕ

В данной работе представлена многоуровневая архитектура системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий. Система на основе такой архитектуры позволяет решать задачи адаптивного управления относительно возникающих аномальных ситуаций в работе компьютерной сети. Предложенное архитектурное решение позволяет учитывать сформированное операционное управление при возникающих известных ситуациях и применять ситуативное управление в случаях выявления аномалий в работе компьютерной сети через создание рабочих сценариев. В такой архитектуре уровни логически взаимосвязаны между собой, что позволяют прослеживать то, как движутся потоки информации на информационном уровне, как связаны компоненты функционального уровня, как организуется работа модулей на системном уровне. Описаны преимущества и недостатки предложенного многоуровневого архитектурного решения системы мониторинга компьютерной сети, которое позволяет определить, в каких ситуациях такое решение может быть применимо для получения необходимого результата от системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий и что необходимо учитывать при реализации такого архитектурного решения.

В рамках данного исследования разрабатывалась многоуровневая архитектура системы мониторинга компьютерной сети с модулем дополнительной диагностики аномалий для своевременного выявления и быстрого реагирования на возникшие аномальные ситуации в КС, но не проводилось исследование по наилучшей программной реализации такой архитектуры. В данном направлении исследования продолжаются.

Список литературы

1. *Шардаков К. С.* Сравнительный анализ популярных систем мониторинга сетевого оборудования, распространяемых по лицензии GPL // Интеллектуальные технологии на транспорте. 2018. № 1(13). С. 44–48.

2. *Краснопер Д. И.* Системы мониторинга состояния сети и её компонентов // Новые информационные технологии в автоматизированных системах. 2010. № 13. С. 209–211.
3. *Salvador P. Valadas R.* A Network Monitoring System with a Peer-to-Peer Architecture // Proc. 3rd International Workshop on Internet Performance, Simulation, Monitoring and Measurement (Warsaw, 15–16 March 2005). Warsaw, 2005. P. 14–15.
4. *Dhillipan J., Vijayalakshmi N., Suriya S.* Network Monitoring System Using Ping Methodology and GUI // Recent Trends and Advances in Artificial Intelligence and Internet of Things. Intelligent Systems Reference Library. 2019. Vol. 172. P. 13–22. doi:10.1007/978-3-030-32644-9_2
5. *Eridani D., Widianto E. D., Augustinus R. D. O., Faizal A. A.* Monitoring System in Lora Network Architecture using Smart Gateway in Simple LoRa Protocol // International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). Yogyakarta, Indonesia, 2019. P. 200–204, doi:10.1109/ISRITI48646.2019.9034612
6. K*rinkin K., Kulikov I., Vodyaho A., N. Zhukova,* Architecture of a Telecommunications Network Monitoring System Based on a Knowledge Graph // 26th Conference of Open Innovations Association (FRUCT). Yaroslavl, Russia, 2020. P. 231–239. doi:10.23919/FRUCT48808.2020.9087429
7. *Maes S.*, ITSM and ESM in the Bigger World. Separation of Concerns: A Modern Approach of ITIL for the Enterprise // OSF Preprints. 2022. P. 1–19. doi:10.31219/osf.io/ugr3p
8. *Deutscher J., Felden C.,* Concept for implementation of cost effective Information Technology Service Management (ITSM) in organizations // IEEE/IFIP Network Operations and Management Symposium Workshops. Osaka, Japan, 2010. P. 167–168. doi:10.1109/NOMSW.2010.5486580
9. *Авилов М. И.* Система мониторинга компьютерной сети и определение ее критериев при проведении кибероучений // Известия СПбГЭТУ «ЛЭТИ». 2019. № 2. С. 43–47.
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. *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.
12. *Shikhaliyev R. H.* A mobile multi-agent-based conceptual architecture for the intelligent monitoring of computer networks // Problems of information technology. 2015. Vol. 6, № 2. P. 59–64. doi:10.25045/jpit.v06.i2.07
13. *Anuja A., Apoorva K.* Wi-Fi Enabled Personal Computer Network Monitoring System Using Smart Phone with Enhanced Security Measures // Procedia Computer Science. 2015. Vol. 70. P. 114–122. doi:10.1016/j.procs.2015.10.052
14. *Prashant K. S., Priti M., Subramanian E. K., Jean S. V., Ravi P. K. V.* Traffic flow monitoring in software-defined network using modified recursive learning // Physical Communication. 2023. Vol. 57. P. 101997. doi:10.1016/j.phycom.2022.101997
15. *Qunying C.* Wireless network signal monitoring based on LAN packet capture and protocol analysis on grid programming // Computer Communications. 2020. Vol. 157. P. 45–52. doi: 10.1016/j.comcom.2020.04.001
16. *Abdelhafidh M., Fourati M., Fourati L. C., Chouaya A.* Wireless sensor network monitoring system: Architecture, applications and future directions // International Journal of Communication Networks and Distributed Systems. 2019. Vol. 23, № 4. P. 413–451. doi:10.1504/IJCNDS.2019.102985
17. *Alip N., Fitri, I., Nathasia N. D.* Network Monitoring System Data Radar Penerbangan berbasis PRTG dan ADSB // Journal of Information Technology and Computer Science. 2018. Vol. 3, № 3. P. 127–134. doi:10.31328/jointecs.v3i3.818
18. *D. Harrington et al.* An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. 2002. [Online]. URL: https://tools.ietf.org/html/rfc3411 (дата обращения: 23.03.2023).
19. J. *Case et al.* Introduction to Version 3 of the Internet-standard Network Management Framework. 1999. [Online]. URL: https://tools.ietf.org/html/rfc2570/ (дата обращения: 23.03.2023).
20. *S. Waldbusser et al.* Introduction to the Remote Monitoring (RMON) Family of MIB Modules. 2003. [Online]. URL: https://tools.ietf.org/html/rfc3577 (дата обращения: 23.03.2023).

21. *B. Claise, ed.* Cisco Systems NetFlow Services Export Version 9. [Online]. 2004. URL: https://tools.ietf.org/html/rfc3954 (дата обращения: 23.03.2023).
22. *Vacche A. D., Lee S. K.* Zabbix Mastering. UK: Packt Publ., 2013. 358 p.
23. Renita J., Elizabeth N. E. Network's server monitoring and analysis using Nagios // International Conference on Wireless Communications, Signal Processing and Networking. Chennai, India, 2017. P. 1904–1909. doi:10.1109/WiSPNET.2017.8300092
24. *Chen Z., Xu G., Mahalingam V., Ge L., Nguyen J., Yu W., Lu C.* A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures // Big Data Research. 2016. Vol. 3. P. 10–23. doi:10.1016/j.bdr.2015.11.002
25. *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

Поступила в редакцию 06.03.2023, окончательный вариант — 23.03.2023.

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

Шичкина Юлия Александровна, доктор технических наук, профессор, заместитель заведующего кафедрой по научной работе кафедры вычислительной техники СПбГЭТУ «ЛЭТИ», shichkina@etu.ai

Computer tools in education, 2023
№ 1: 55–73
http://cte.eltech.ru
doi:10.32603/2071-2340-2023-1-55-73

Multilevel Architecture of a Computer Network Operation Monitoring System With an Anomaly Diagnostics Module

Avilov M. I.[1], Systems Engineer, ✉ avilovmaxim@gmail.com
Shichkina Yu. A.[1], Doctor sc., Professor, shichkina@etu.ai

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

Abstract

This article is a continuation of research that focuses on the timely detection and rapid response to anomalies in the computer network with a network monitoring system with additional anomaly diagnostics module. The multi-level architecture of the network monitoring system with the module of additional anomaly diagnostics, which takes into account the modular way of organizing such an information system. Described situations in which the proposed architecture can be applied, listed its advantages and disadvantages. Process of forming of working scenarios at processing of anomaly in functioning of computer network with the account of the given architecture of monitoring system with a module of additional diagnostics of anomalies of such network is also described. Approaches to the formation of input and output data when creating a work scenario are considered.

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

Citation: M. I Avilov and Yu. A. Shichkina, “Multilevel Architecture of a Computer Network Operation Monitoring System With an Anomaly Diagnostics Module,” Computer tools in education, no. 1, pp. 55–73, 2023 (in Russian); doi: 10.32603/2071-2340-2023-1-55-73

References

1. K. S. Shardakov, “Sravnitelnyi analiz populiarnykh sistem monitoringa setevogo oborudovaniia, rasprostraniaemykh po litsenzii GPL” [Comparative Analysis of the Popular Monitoring Systems for Network Equipment Distributed Under the GPL License], *Intellectual Technologies on Transport*, no. 1(13), pp. 44–48, 2018 (in Russian).
2. D. I. Krosnoper, “Sistemy monitoringa sostoianiia seti i ee komponentov” [Systems for monitoring the state of the network and its component], *New information technologies in automated systems*, no. 13, pp. 209–211, 2010 (in Russian).
3. P. Salvador and R. Valadas, “A Network Monitoring System with a Peer-to-Peer Architecture,” in *Proc. 3rd International Workshop on Internet Performance, Simulation, Monitoring and Measurement, March 15-16, 2005, Warsaw, Poland*, pp. 14–15, 2005.
4. J. Dhillipan, N. Vijayalakshmi, and S. Suriya, “Network Monitoring System Using Ping Methodology and GUI,” *Recent Trends and Advances in Artificial Intelligence and Internet of Things*, vol. 172, pp. 13–22, 2019; doi:10.1007/978-3-030-32644-9_2
5. D. Eridani, E. D. Widianto, R. D. O. Augustinus, and A. A. Faizal, “Monitoring System in Lora Network Architecture using Smart Gateway in Simple LoRa Protocol,” *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2019*, pp. 200–204, 2019; doi:10.1109/ISRITI48646.2019.9034612
6. K. Krinkin, I. Kulikov, A. Vodyaho, and N. Zhukova, “Architecture of a Telecommunications Network Monitoring System Based on a Knowledge Graph,” in *26th Conference of Open Innovations Association (FRUCT), Yaroslavl*, pp. 231–239, 2020 (in Russian) doi: 10.23919/FRUCT48808.2020.9087429
7. S. Maes, “ITSM and ESM in the Bigger World. Separation of Concerns: A Modern Approach of ITIL for the Enterprise,” *OSF Preprints*, pp. 1–19, 2022; doi:10.31219/osf.io/ugr3p
8. J. Deutscher and C. Felden, “Concept for implementation of cost effective Information Technology Service Management (ITSM) in organizations,” in *Proc. of IEEE/IFIP Network Operations and Management Symposium Workshops, Osaka, Japan, 2010*, pp. 167–168, 2010; doi:10.1109/NOMSW.2010.5486580
9. M. I. Avilov, “Role network monitoring system in the technical cyber defence exercise,” *Proceedings of Saint Petersburg Electrotechnical University*, no. 2, pp. 43–47, 2019 (in Russian).
10. M. I. Avilov, Yu. A. Shichkina, and M. S. Kupriyanov, “Monitoring of an information and communication computer network using a neural network module,” *Proceedings of Saint Petersburg Electrotechnical University*, no. 5, pp. 34–45, 2020 (in Russian).
11. M. I. Avilov, 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).
12. R. H. Shikhaliyev, “A mobile multi-agent-based conceptual architecture for the intelligent monitoring of computer networks,” *Problems of information technology*, vol. 6, no. 2, pp. 59–64, 2015; doi:10.25045/jpit.v06.i2.07
13. A. Anuja and K. Apoorva, “Wi-Fi Enabled Personal Computer Network Monitoring System Using Smart Phone with Enhanced Security Measures,” *Procedia Computer Science*, vol. 70, pp. 114–122, 2015; doi:10.1016/j.procs.2015.10.052
14. K. S. Prashant et al., “Traffic flow monitoring in software-defined network using modified recursive learning,” *Physical Communication*, vol. 57, p. 101997, 2023; doi:10.1016/j.phycom.2022.101997
15. C. Qunying, “Wireless network signal monitoring based on LAN packet capture and protocol analysis on grid programming,” *Computer Communications*, vol. 157, pp. 45–52, 2020; doi:10.1016/j.comcom.2020.04.001
16. M. Abdelhafidh, M. Fourati, L. C. Fourati, and A. Chouaya, “Wireless sensor network monitoring system: Architecture, applications and future directions,” *International Journal of Communication Networks and Distributed Systems*, vol. 23, no. 4, pp. 413–451, 2019; doi:10.1504/IJCNDS.2019.102985
17. N. Alip, I. Fitri, and N. D. Nathasia, “Network Monitoring System Data Radar Penerbangan berbasis PRTG dan ADSB,” *Journal of Information Technology and Computer Science*, vol. 3, no. 3, pp. 127–134, 2018; doi:10.31328/jointecs.v3i3.818
18. D. Harrington et al., “An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks,” in *tools.ietf.org*, 2002. [Online]. Available: https://tools.ietf.org/html/rfc3411

19. J. Case et al., “Introduction to Version 3 of the Internet-standard Network Management Framework,”in *tools.ietf.org*, 1999. [Online]. Available: https://tools.ietf.org/html/rfc2570/
20. S. Waldbusser et al., “Introduction to the Remote Monitoring (RMON) Family of MIB Modules,” in *tools.ietf.org*, 2003. [Online]. Available: https://tools.ietf.org/html/rfc3577
21. B. Claise, ed., “Cisco Systems NetFlow Services Export Version 9,”in *tools.ietf.org*, 2004. [Online]. Available: https://tools.ietf.org/html/rfc3954
22. A. D. Vacche and S. K. Lee, *Zabbix Mastering*, Birmingham, UK: Packt Publ., 2013.
23. J. Renita and N. E. Elizabeth, “Network’s server monitoring and analysis using Nagios,” in *Int. Conf. on Wireless Communications, Signal Processing and Networking, Chennai, India, 2017*, pp. 1904–1909, 2017; doi:10.1109/WiSPNET.2017.8300092
24. Z. Chen et al., “A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures,” *Big Data Research*, vol. 3, pp. 10–23, 2016; doi:10.1016/j.bdr.2015.11.002
25. V. V. Allakin, N. P. Budko, and N. V. Vasiliev, “A general approach to the construction of advanced monitoring systems for distributed information and telecommunications networks,” *Systems of Control, Communication and Security*, no. 4, pp. 125–227, 2021 (in Russian); doi:10.24412/2410-9916-2021-4-125-227

Received 06-03-2023, the final version — 23-03-2023.

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

Yulia Shichkina, Doctor of Sciences in Technology, Professor, Deputy Head for Scientific Work of the Department of Computer Science and Engineering, Saint Petersburg Electrotechnical University, shichkina@etu.ai