СОВРЕМЕННЫЕ ПОДХОДЫ К МОНИТОРИНГУ ИТ-ИНФРАСТРУКТУРЫ В УСЛОВИЯХ РАСПРЕДЕЛЕННЫХ И ОБЛАЧНО-ОРИЕНТИРОВАННЫХ АРХИТЕКТУР

В.С. Станолевич, *магистрант*
Научный руководитель: *К.А. Батенков, д-р техн. наук, профессор*
Московский технический университет связи и информатики
(Россия, г. Москва)

DOI:10.24412/2500-1000-2026-2-1-254-259

Аннотация. *В статье рассмотрены современные подходы к мониторингу ИТ-инфраструктуры в условиях цифровой трансформации и широкого внедрения облачных и микросервисных архитектур. Проанализированы методы сетевого мониторинга, включая потоковую телеметрию и стандартизированные механизмы экспорта данных, а также подходы к контролю доступности интернет-ресурсов и оценке пользовательского опыта. Особое внимание уделено интеграции различных классов телеметрии (метрики, логи, трассировки) в рамках комплексной системы наблюдаемости и применению интеллектуальных методов анализа данных и концепции AIOps. Обоснована необходимость комплексного подхода к мониторингу для повышения устойчивости, управляемости и надежности функционирования современных информационных систем.*

Ключевые слова: *мониторинг ИТ-инфраструктуры; сетевая телеметрия; IPFIX; RUM; observability; обнаружение аномалий; AIOps.*

В условиях цифровой трансформации и широкого внедрения облачных, виртуализированных и микросервисных архитектур обеспечение устойчивости и доступности ИТ-инфраструктуры приобретает критическое значение. Современные информационные системы характеризуются высокой степенью распределенности, динамичностью конфигураций и сложностью межсервисных взаимодействий, что существенно усложняет процессы эксплуатации и диагностики инцидентов. В этих условиях мониторинг ИТ-инфраструктуры выступает не только инструментом контроля работоспособности отдельных компонентов, но и ключевым элементом обеспечения надежности и управляемости цифровых сервисов в целом. Особое значение приобретают мониторинг сетевой инфраструктуры, контроль доступности интернет-ресурсов и внешних сервисов, а также комплексный анализ состояния вычислительных и прикладных подсистем. Целью настоящей работы является анализ современных подходов к мониторингу ИТ-инфраструктуры, включая методы сбора и обработки телеметрических данных, а также обоснование необходимости комплексного применения сетевого, сервисного и инфраструктурного мониторинга для повышения устойчивости функционирования информационных систем.

Мониторинг сети как базовый уровень контроля ИТ-инфраструктуры

Сетевая инфраструктура является базовым уровнем функционирования распределенных информационных систем, обеспечивая транспорт взаимодействия между вычислительными узлами, сервисами и внешними ресурсами. Нарушения в работе сетевых компонентов приводят к деградации прикладных сервисов независимо от состояния серверной и программной подсистем, поэтому сетевой мониторинг рассматривается как первичный контур контроля ИТ-инфраструктуры.

Традиционные механизмы мониторинга основывались на периодическом опросе устройств и анализе агрегированных счетчиков интерфейсов. Развитие высоконагруженных и программируемых сетей обусловило переход к потоковой телеметрии (streaming telemetry), обеспечивающей передачу детализированных измерений в режиме, близком к реальному времени [1]. Это позволяет формировать непрерывные временные ряды метрик и применять методы интеллектуального анализа для выявления отклонений.

По уровню охвата сетевой мониторинг классифицируется на одноточечный, маршрутный, сетевой и гибридный [1] (рис. 1). Одноточечный мониторинг ориентирован на контроль состояния отдельных устройств и интерфейсов, маршрутный – на анализ характеристик передачи данных между конечными точками, а сетевой – на формирование целостного представления о состоянии топологии за счет агрегирования данных и корреляции событий.

Современные методы сетевого мониторинга активно используют анализ потоковых данных (flow-based monitoring), включая экспорт статистики потоков по протоколу IPFIX [2]. Применение стандартизированных механизмов экспорта потоковой информации обеспечивает формирование агрегированных характеристик трафика и создает основу для последующего анализа распределения потоков и выявления отклонений. Результаты практических экспериментов по применению потоковой телеметрии в реальных сетевых средах подтверждают эффективность интеграции сетевых метрик с аналитическими механизмами обнаружения аномалий и позволяют сократить время выявления деградаций [3].

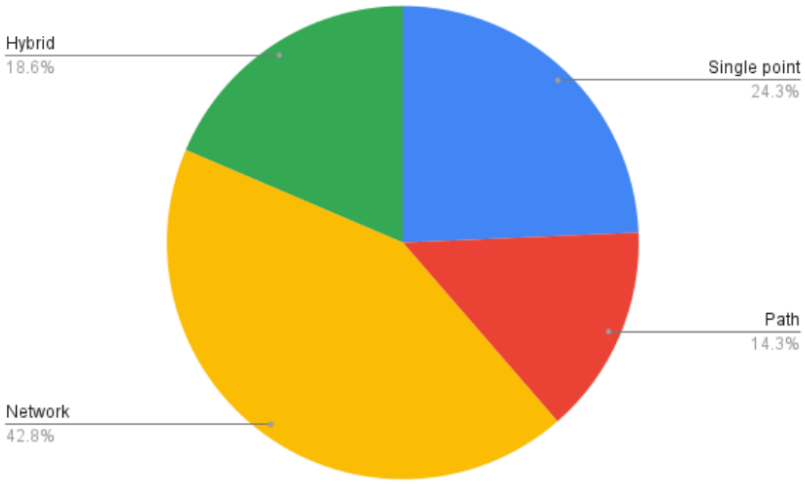

Рис. 1. Классификация подходов к сетевому мониторингу [1]

Рост объема телеметрических данных обусловил необходимость применения алгоритмов обнаружения аномалий в потоковых временных рядах. Современные исследования подтверждают эффективность методов потокового анализа при выявлении сетевых отклонений и перегрузок [4, 5]; сравнительные оценки показывают, что адаптивные модели позволяют фиксировать изменения сетевого поведения на ранних стадиях и сокращать время реакции на инциденты [5]. Важным направлением развития сетевого мониторинга является использование программируемых плоскостей обработки данных и технологий eBPF, обеспечивающих внедрение измерительных механизмов непосредственно в сетевую среду [6]. Это позволяет осуществлять детализированный сбор телеметрии с минимальными накладными расходами.

Практическая реализация подобных систем предполагает интеграцию сетевых метрик с централизованными средствами визуализации и корреляции событий [7], что обеспечивает переход от локального контроля отдельных устройств к комплексному анализу состояния сетевой инфраструктуры.

Мониторинг интернет-ресурсов и внешних сервисов

В условиях широкого использования облачных платформ и распределенных приложений значительная часть бизнес-критичных процессов зависит от корректного функционирования внешних интернет-ресурсов и сторонних сервисов. Даже при стабильной работе внутренней сетевой инфраструктуры деградация DNS-разрешения, ошибки TLS-сертификатов, сбои API-партнеров или увеличение времени отклика веб-интерфейсов способны привести к нарушению предоставления услуг. В этой связи мониторинг интернет-ресурсов рассматривается как самостоятельный уровень контроля, дополняющий внутренний сетевой мониторинг.

Контроль внешней доступности веб-ресурсов традиционно включает измерение времени отклика (latency), анализ кодов ответа HTTP, оценку процента доступности (uptime) и проверку корректности обработки транзакций. Однако такие проверки отражают лишь техническую доступность сервиса. Для более полной оценки качества взаимодействия используются два взаимодополняющих подхода: синтетический мониторинг и мониторинг реального пользовательского опыта (Real User Monitoring, RUM). Архитектура реализации RUM предполагает внедрение клиентского агента и централизованную агрегацию телеметрии, как показано на рисунке 2 [8].

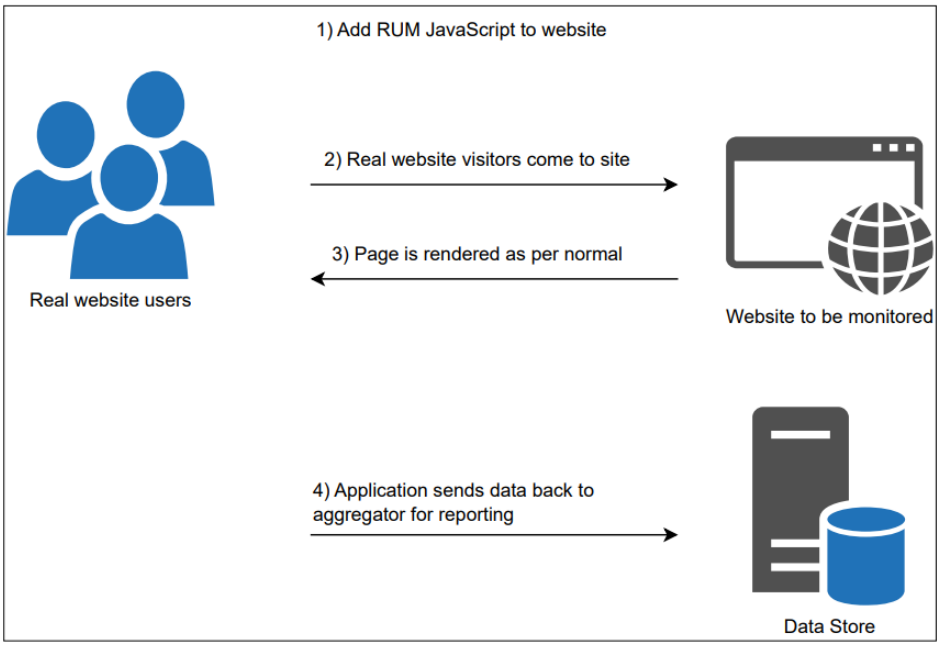

Рис. 2. Типовая схема функционирования Real User Monitoring [8]

Синтетический мониторинг основан на выполнении заранее заданных сценариев взаимодействия с веб-приложением из различных географических точек. Он позволяет воспроизводить типовые пользовательские действия и измерять параметры выполнения транзакций вне зависимости от фактического пользовательского трафика [9]. Преимуществом данного подхода является контролируемость сценариев и возможность раннего выявления деградации, однако он не отражает реальное распределение пользовательской нагрузки.

Мониторинг реального пользовательского опыта (RUM), напротив, основан на сборе телеметрии непосредственно из браузеров или клиентских приложений пользователей. Он позволяет анализировать фактические задержки загрузки страниц, производительность рендеринга и взаимодействия с интерфейсом, а также выявлять региональные особенности деградации. В научных обзорах подчеркивается, что совмещение синтетических проверок и RUM обеспечивает более полную картину состояния интернет-сервиса, позволяя выявлять как инфраструктурные, так и клиентские проблемы [8].

Критически важным элементом мониторинга интернет-ресурсов является контроль системы доменных имен (DNS) и параметров криптографической защиты соединений. Нарушения в работе DNS-инфраструктуры могут приводить к полной недоступности сервиса при сохранении работоспособности серверной части. Аналогично, ошибки в конфигурации TLS или истечение срока действия сертификатов приводят к отказу установления защищенного соединения. В современных практиках мониторинга предусматривается регулярная проверка корректности разрешения доменных имен, цепочек сертификатов и параметров шифрования.

Интеграция мониторинга интернет-ресурсов с общей системой наблюдаемости позволяет коррелировать данные о пользовательском опыте с сетевыми и инфраструктурными метриками. Применение централизованных систем телеметрии и распределенной трассировки запросов обеспечивает выявле-

ние первопричин деградации на стыке внутренних и внешних компонентов системы [10]. В условиях высокой динамики облачных сервисов особое значение приобретает автоматизированная обработка событий и логов с применением методов интеллектуального анализа, позволяющих выявлять аномалии в поведении сервисов и снижать время реакции на инциденты [11,12].

Комплексный мониторинг ИТ-инфраструктуры

Современные информационные системы представляют собой распределенные, динамически масштабируемые и многослойные архитектуры, включающие сетевую инфраструктуру, вычислительные ресурсы, контейнерные среды, прикладные сервисы и внешние зависимости. В таких условиях изолированный мониторинг отдельных подсистем не обеспечивает адекватной оценки устойчивости функционирования ИТ-среды. Возникает необходимость построения комплексной системы наблюдаемости, интегрирующей данные различных уровней: от сетевой телеметрии до прикладных логов и пользовательских метрик.

Комплексный мониторинг предполагает объединение трех ключевых классов телеметрии: метрик, логов и трассировок. Метрики отражают количественные характеристики состояния компонентов (нагрузка, задержка, пропускная способность), логи фиксируют события и ошибки, а распределенные трассировки позволяют проследить путь запроса через цепочку микросервисов. Концепция объединения этих данных в единую систему observability активно развивается в современных исследованиях и практических решениях [6, 10].

Сетевой мониторинг, рассмотренный в разделе 1, формирует первичный поток телеметрии, включая данные о потоках трафика, параметрах маршрутов и состоянии сетевых устройств. Мониторинг интернет-ресурсов и пользовательского опыта, описанный в разделе 2, предоставляет информацию о фактической доступности и производительности сервисов с точки зрения конечного пользователя. Однако только их интеграция с инфраструктурными метриками серверов, контейнеров и приложений позволяет осуществлять корреляцию событий и выявлять первопричины инцидентов.

Ключевым направлением развития комплексного мониторинга является применение интеллектуальных методов обработки телеметрических данных. Современные исследования в области потокового обнаружения аномалий демонстрируют эффективность алгоритмов, способных выявлять отклонения в динамических временных рядах в режиме реального времени [4, 5]. Дополнительно, систематические обзоры методов анализа логов подтверждают перспективность использования машинного обучения для автоматизации выявления инцидентов и снижения нагрузки на операторов [2, 10].

Интеграция различных источников телеметрии требует построения централизованной архитектуры сбора и обработки данных, включающей механизмы агрегации, нормализации, долговременного хранения и корреляции событий. В контейнеризированных и облачно-ориентированных средах особое значение приобретает мониторинг состояния кластерных компонентов и рабочих нагрузок, включая поды, сервисы и узлы оркестратора Kubernetes, что обеспечивается встроенными механизмами observability и возможностью интеграции с внешними системами мониторинга [13]. Практические реализации подобных систем предполагают использование агентов сбора данных, централизованных коллекторов, хранилищ временных рядов и аналитических модулей обработки телеметрии [7]. При этом стандартизированные протоколы экспорта потоковой информации, такие как IPFIX [2], обеспечивают совместимость компонентов и унификацию форматов передаваемых данных.

Развитие концепции AIOps усиливает возможности комплексного мониторинга за счет внедрения алгоритмов интеллектуального анализа и автоматизированной обработки событий. В рамках данной парадигмы осуществляется корреляция метрик, логов и сетевых показателей с целью выявления скрытых зависимостей и прогнозирования потенциальных отказов [14]. Такой подход позволяет перейти от реактивного реагирования на инциденты к проактивному управлению устойчивостью ИТ-инфраструктуры.

Заключение. Проведенный анализ современных подходов к мониторингу ИТ-инфраструктуры показал, что обеспечение устойчивости функционирования цифровых систем требует интеграции сетевого, сервисного и инфраструктурного уровней контроля в единую систему наблюдаемости. Развитие потоковой телеметрии, стандартизированных механизмов экспорта данных, методов обнаружения аномалий и концепции AIOps формирует технологическую основу для перехода от изолированного мониторинга отдельных компонентов к комплексному управлению состоянием распределенных сред. Совмещение сетевой аналитики, мониторинга интернет-ресурсов и обработки логов с использованием интеллектуальных алгоритмов позволяет сократить время выявления инцидентов и повысить предсказуемость поведения ИТ-систем.

Библиографический список

1. Yaseen N. From Counters to Telemetry: A Survey of Programmable Network-Wide Monitoring // Network. – 2025. – Vol. 5, № 3. – Art. 38. – 29 p. – DOI: 10.3390/network5030038.

2. Claise B., Trammell B. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information: RFC 7011. – Reston, VA: IETF, 2013. – ISSN: 2070-1721.

3. Makonyi K., Abrahamsson H., Henriksson D., Hock D., Kremling S., Lipp F., Salisbury J., Sandell J. On the use of streaming telemetry data for network health monitoring and anomaly detection: Experiences from the AI-NET-PROTECT field trial // Proceedings of the 19th Swedish National Computer Networking and Cloud Computing Workshop (SNCNW 2024). – 2024. – 4 p.

4. Cao Y., Ma Y., Zhu Y., Ting K.M. Revisiting streaming anomaly detection: benchmark and evaluation // Artificial Intelligence Review. – 2024. – Vol. 58. – Art. 8. – 25 p. – DOI: 10.1007/s10462-024-10995-w.

5. Iglesias Vázquez F., Hartl A., Zseby T., Zimek A. Anomaly detection in streaming data: A comparison and evaluation study // Expert Systems with Applications. – 2023. – Vol. 223. – Art. 120994. – 29 p. – DOI: 10.1016/j.eswa.2023.120994.

6. Soldani D., Nahi P., Bour H., Jafarizadeh S. eBPF: A New Approach to Cloud-Native Observability, Networking and Security for Current (5G) and Future Mobile Networks (6G and Beyond) // IEEE Access. – 2023. – Vol. 11. – P. 57174-57202. – DOI: 10.1109/ACCESS.2023.3281480.

7. Pragathi B.C., Maddirala H., Sneha M. Implementing an Effective Infrastructure Monitoring Solution with Prometheus and Grafana // International Journal of Computer Applications. – 2024. – Vol. 186, № 38. – P. 7-15. – DOI: 10.5120/ijca2024923873.

8. Lorber N., Seiser M., Weisl K. Real User Monitoring (RUM): A Comparative Survey. – Graz University of Technology, 2024. – [Электронный ресурс]. – Режим доступа: https://courses.isds.tugraz.at/iaweb/surveys/ws2024/iaweb-ws2024-g4-survey-real-user-monitoring.pdf.

9. Google Cloud. Synthetic Monitoring in Cloud Monitoring is now Generally Available. – [Электронный ресурс]. – Режим доступа: https://cloud.google.com/blog/products/devops-sre/synthetic-monitoring-in-cloud-monitoring-is-now-ga.

10. OpenTelemetry Documentation. – [Электронный ресурс]. – Режим доступа: https://opentelemetry.io/docs/.

11. De la Cruz Cabello M., Prince Sales T., Machado M. R. AIOps for log anomaly detection in the era of LLMs: A systematic literature review // Intelligent Systems with Applications. – 2025. – Vol. 28. – Art. 200608. – 18 p. – DOI: 10.1016/j.iswa.2025.200608.

12. Ali S., Boufaied C., Bianculli D. et al. A comprehensive study of machine learning techniques for log-based anomaly detection // Empirical Software Engineering. – 2025. – Vol. 30. – Art. 129. – 60 p. – DOI: 10.1007/s10664-025-10669-3.

13. Kubernetes Documentation. Observability. – [Электронный ресурс]. – Режим доступа: https://kubernetes.io/docs/concepts/cluster-administration/observability/.

14. Zota R.D., Bărbulescu C., Constantinescu R. A Practical Approach to Defining a Framework for Developing an Agentic AIOps System // Electronics. – 2025. – Vol. 14, № 9. – Art. 1775. – DOI: 10.3390/electronics14091775.

MODERN APPROACHES TO IT INFRASTRUCTURE MONITORING IN DISTRIBUTED AND CLOUD-ORIENTED ARCHITECTURES

V.S. Stanolevich, *Graduate Student*
Supervisor: *K.A. Batenkov, Doctor of Technical Sciences, Professor*
Moscow Technical University of Communications and Informatics
(Russia, Moscow)

Abstract. *The paper analyzes modern approaches to IT infrastructure monitoring in the context of digital transformation and the widespread adoption of cloud-native and microservice-based architectures. Network monitoring methods, including streaming telemetry and standardized flow export mechanisms, are examined alongside approaches to monitoring Internet resources and assessing end-user experience. Particular attention is given to the integration of multiple telemetry types (metrics, logs, and traces) within a unified observability framework and to the application of intelligent data analysis methods and AIOps concepts. The necessity of a comprehensive monitoring approach for improving the reliability, manageability, and resilience of contemporary information systems is substantiated.*

Keywords: *IT infrastructure monitoring; network telemetry; IPFIX; RUM; observability; anomaly detection; AIOps.*