

УДК 004.89:004.7

Роль искусственного интеллекта в управлении сетями следующего поколения (AIOps for Networks): обзор современных возможностей и ограничений

Е.А. Колесников✉, В.Н. Кострова

Воронежский институт высоких технологий, Воронеж, Россия

В статье рассматривается роль искусственного интеллекта (ИИ) в управлении современными сетевыми инфраструктурами в парадигме AIOps. Показано, что рост сложности сетей, обусловленный внедрением облачных технологий, SD-WAN, периферийных вычислений и новых стандартов связи, делает традиционные методы управления неэффективными. Анализируются ключевые возможности AIOps, включающие автоматизацию сбора и корреляции телеметрии, предиктивную аналитику, обнаружение аномалий и использование естественного языка для взаимодействия с сетью. Особое внимание уделяется концепции агентного ИИ как следующему этапу эволюции автономных сетей. Рассматриваются ограничения технологии, связанные с качеством данных, проблемами доверия к решениям ИИ и необходимостью верификации результатов. Сделан вывод о том, что AIOps становится обязательным элементом сетей следующего поколения, трансформируя роль сетевого инженера.

Ключевые слова: AIOps, искусственный интеллект, управление сетями, сети следующего поколения, агентный ИИ, автономные сети, машинное обучение.

The Role of Artificial Intelligence in Next-Generation Network Management (AIOps for Networks): A Review of Current Capabilities and Limitations

E.A. Kolesnikov✉, V.N. Kostrova

Voronezh Institute of High Technologies, Voronezh, Russia

The article examines the role of artificial intelligence (AI) in managing modern network infrastructures within the AIOps paradigm. It is shown that the increasing complexity of networks due to the adoption of cloud technologies, SD-WAN, edge computing, and new communication standards renders traditional management methods ineffective. Key AIOps capabilities are analyzed, including automation of telemetry collection and correlation, predictive analytics, anomaly detection, and the use of natural language for network interaction. Special attention is paid to the concept of agentic AI as the next stage in the evolution of autonomous networks. Technology limitations related to data quality, problems of trust in AI decisions, and the need for result verification are discussed. It is concluded that AIOps is becoming a mandatory element of next-generation networks, transforming the role of the network engineer.

Keywords: AIOps, artificial intelligence, network management, next-generation networks, agentic AI, autonomous networks, machine learning.

Введение

Современные сетевые инфраструктуры находятся в состоянии активной трансформации. Распределенные архитектуры на базе виртуализации, SD-WAN, облачных технологий и периферийных вычислений становятся основой для поддержки

новых цифровых экосистем [1]. Объем и скорость потоков операционных данных, генерируемых такими средами, значительно превышают возможности ручного управления со стороны человека [2].

В этих условиях традиционные подходы к мониторингу и устранению неполадок, основанные на ручном анализе журналов и статических информационных панелях, перестают быть эффективными. Ответом на вызовы времени стала концепция AIOps (Artificial Intelligence for IT Operations) – применение технологий искусственного интеллекта (ИИ) и машинного обучения для автоматизации и повышения качества операционного управления ИТ-инфраструктурами, включая сетевой сегмент [3].

Целью настоящей работы является систематизация современных представлений о роли искусственного интеллекта в управлении сетями следующего поколения, анализ ключевых возможностей, предоставляемых AIOps, и выявление существующих ограничений, препятствующих его повсеместному внедрению.

Современное состояние и предпосылки внедрения AIOps

Концепция AIOps (Artificial Intelligence for IT Operations) была введена аналитической компанией Gartner в 2016 году и обозначает класс решений, использующих большие данные и машинное обучение для усиления ИТ-операций. За прошедшие годы интерес к технологии неуклонно рос, достигнув пика в 2024–2025 годах, что подтверждается данными поисковых запросов и аналитическими отчетами [4].

Основной предпосылкой внедрения AIOps является критический уровень сложности современных сетей. Микросервисная архитектура приложений, распределенные облачные среды и необходимость обеспечения связности для удаленных сотрудников создают нагрузку на сеть, с которой не справляются унаследованные инструменты [1]. Автоматизация на основе ИИ рассматривается как необходимое условие повышения надежности сетевой инфраструктуры.

Согласно исследованию Heavy Reading (Omdia), проведенному в 2025 году при участии RADCOM, 47% операторов связи уже достигли уровня автономности в assurance-операциях для отдельных сценариев, а более 74% планируют внедрение AI-агентов в течение двух лет [4]. Около 40% предприятий уже в той или иной степени используют AIOps, причем наиболее высокая доля внедрения наблюдается в регулируемых и интенсивно использующих данные отраслях [5].

Ключевыми драйверами ускоренного внедрения AIOps выступают, во-первых, взрывной рост числа подключенных устройств (IoT, промышленные датчики, мобильные терминалы), что приводит к лавинообразному увеличению сетевого трафика и событий [4]. Во-вторых, переход к модели «сеть как услуга» (NaaS) требует мгновенной реакции на изменения спроса и автоматического масштабирования ресурсов [8]. В-третьих, ужесточение требований к отказоустойчивости и времени восстановления (SLA) в таких сферах, как финансы, телемедицина и автономный транспорт, делает ручное управление неприемлемо медленным [5]. Таким образом, AIOps становится не просто технологическим трендом, а необходимым инструментом для сохранения конкурентоспособности операторов связи и предприятий [4].

Ключевые возможности AIOps в управлении сетями

Анализ современных решений и публикаций позволяет выделить несколько ключевых функциональных возможностей, которые AIOps предоставляет для управления сетями следующего поколения.

Автоматизация сбора и корреляции данных. Сеть генерирует огромные объемы разнородных данных: потоки, журналы конфигураций, метрики производительности, данные о событиях безопасности. AIOps-платформы способны агрегировать эту информацию из различных источников, включая потоки сетевого трафика, файлы конфигурации и данные от критически важных сервисов [2]. Ключевым преимуществом является использование потоковой телеметрии (например, на основе протокола gNMI), которая обеспечивает передачу данных в реальном времени при наступлении события, а не по результатам периодического опроса, как в традиционных системах [6]. Это позволяет AIOps-системам постоянно сравнивать наблюдаемое состояние сети с целевым, обнаруживать отклонения и оперативно информировать операторов [3]. Применение алгоритмов машинного обучения для корреляции событий позволяет преобразовывать множество разрозненных и зачастую ложных срабатываний в ограниченное число инцидентов с понятным контекстом [2]. Это радикально снижает уровень шума и восстанавливает доверие дежурных смен к инструментам мониторинга.

Предиктивная аналитика и обнаружение аномалий. Одной из наиболее востребованных возможностей является прогнозирование проблем до того, как они повлияют на пользователей. Анализируя исторические данные, AIOps способна предсказывать исчерпание пропускной способности, деградацию производительности приложений и другие потенциальные сбои [5]. Это позволяет перейти от реактивного подхода к проактивному управлению, устраняя проблемы на ранних стадиях. Обнаружение аномалий выходит за рамки простых пороговых значений. Системы AIOps обучаются на нормальном поведении сети и способны выявлять статистически значимые отклонения, которые могут свидетельствовать о начинающихся проблемах или атаках [6]. В частности, AIOps может помочь выявить подозрительную киберактивность, анализируя сетевые паттерны [7].

Взаимодействие на естественном языке и агентный ИИ. Значительным прорывом стало внедрение интерфейсов на естественном языке, позволяющих инженерам взаимодействовать с сетью без необходимости изучения сложных синтаксисов командных строк или языков запросов [6]. Примером такой реализации является виртуальный ассистент Marvis от HPE (Juniper) или Ask EDA от Nokia [2]. Инженер может задать вопрос: «Почему недоступен коммутатор spine1?» и получить развернутый ответ с анализом первопричины, например, о случайно удаленной конфигурации BGP-соседа [6]. Следующим этапом эволюции становится агентный ИИ (Agentic AI). В отличие от простых чат-ботов, AI-агенты способны не только отвечать на вопросы, но и самостоятельно выполнять действия в сети для решения проблем [7]. Они могут взаимодействовать друг с другом, собирать контекст из различных систем, планировать последовательность действий и выполнять их в рамках заданных политик. Согласно исследованию Heavy Reading (Omdia), более 74% операторов связи планируют развернуть AI-агентов в своих процессах в течение ближайших двух лет [4].

Цифровые двойники для верификации изменений. Критически важной функцией, обеспечивающей безопасность автоматизации, является использование цифровых двойников сети. Перед тем как применить изменение, предложенное AI-ассистентом или агентом, оно может быть протестировано на виртуальной копии сети, точно отражающей состояние реальной инфраструктуры. Это позволяет проверить корректность конфигурации, выявить возможные конфликты и предотвратить простои, вызванные человеческой ошибкой или «галлюцинациями» больших языковых моделей [7]. По данным опроса, 58% операторов уже используют цифровые двойники с контролем со стороны человека для валидации решений ИИ перед их применением в продуктивной среде [4].

Замкнутая автоматизация (closed-loop automation). Помимо диагностики и рекомендаций, современные AIOps-решения всё чаще реализуют полностью автоматизированный цикл: мониторинг → анализ → принятие решения → изменение конфигурации → повторный мониторинг. Это позволяет устранять типовые инциденты (например, перегрузка канала или сбой BGP-сессии) без участия человека, что сокращает время восстановления с часов до секунд [4]. Согласно опросу Heavy Reading, 47% операторов уже внедрили такие автономные сценарии, а ещё 30% планируют сделать это в ближайший год [4]. При этом критическим условием остаётся верификация всех изменений через цифровые двойники, чтобы избежать каскадных отказов [7].

Ограничения и вызовы при внедрении AIOps

Несмотря на впечатляющие возможности, внедрение AIOps сопряжено с рядом существенных ограничений и вызовов, которые необходимо учитывать.

Качество и унификация данных. Эффективность любой AIOps-платформы напрямую зависит от качества данных, на которых она обучается и которые анализирует. Проблемы с качеством данных (неполнота, противоречивость, наличие шума) могут приводить к неточным выводам и ошибочным рекомендациям [5]. Исследования показывают, что 52% операторов по-прежнему работают с разрозненными системами, где данные существуют в изолированных «силосах», что делает унификацию архитектуры данных и использование API критически важным условием для прогресса в области AIOps [4].

Доверие и объяснимость решений. Разрыв в восприятии ценности AIOps между руководителями и практикующими инженерами, зафиксированный в ряде исследований, указывает на проблему доверия [5]. Если в 2023 году только 20% практикующих специалистов видели высокую ценность от внедрения AIOps против 59% руководителей, это говорит о том, что инструменты либо не решали реальных проблем, либо были «черным ящиком», решениям которого сложно доверять. В связи с этим особую важность приобретает объяснимость результатов – способность системы показать, почему она пришла к тому или иному выводу.

Интеграция с унаследованными системами. Многие предприятия имеют сложную инфраструктуру, включающую legacy-системы, которые плохо интегрируются с современными AIOps-платформами. Основными препятствиями называются интеграция с устаревшими OSS/BSS системами (55% респондентов) и наличие «дата-сilo» (54%) [4]. Преодоление этих барьеров требует значительных инвестиций и времени.

Эволюция роли сетевого инженера. Внедрение AIOps не означает замену человека, но кардинально меняет его функции. Инженер превращается из «пожарного», постоянно тушащего инциденты, в стратега, формулирующего цели, обучающего AI-системы и контролирующего их работу [7]. Это требует новых компетенций, включая понимание принципов работы ИИ, умение формулировать запросы и интерпретировать результаты, а также навыки управления автоматизированными процессами. Возникает потребность в обучении персонала и изменении корпоративной культуры [5].

Отдельного внимания заслуживают риски, связанные с безопасностью самих AIOps-систем. Поскольку AI-агенты получают широкие полномочия по изменению конфигурации сети, злоумышленник при компрометации такой системы может нанести критический ущерб [7]. Это требует внедрения строгих механизмов аутентификации, разграничения прав и аудита действий AI-агентов [4]. Кроме того, возникают этические

вопросы: кто несёт ответственность за сбой, вызванный ошибочным решением ИИ? Как избежать дискриминации разных классов трафика при автоматическом управлении качеством обслуживания? [7] Решение этих проблем лежит в плоскости разработки отраслевых стандартов, обязательного страхования рисков и создания независимых органов по сертификации AIOps-решений [5].

Вычислительная сложность и стоимость развёртывания. Модели машинного обучения, способные обрабатывать терабайты телеметрии в реальном времени, требуют значительных вычислительных ресурсов (GPU-кластеры, распределённые хранилища). Это накладывает высокие требования к инфраструктуре и может быть экономически неоправданно для небольших компаний [5]. Кроме того, обучение и тонкая настройка AI-моделей требуют участия высококвалифицированных специалистов по данным, дефицит которых на рынке сохраняется [8]. Следовательно, для широкого распространения AIOps необходимы более эффективные алгоритмы и готовые отраслевые решения, снижающие порог входа.

Заключение

Проведенный анализ позволяет сделать вывод, что AIOps является не временным трендом, а фундаментальным сдвигом в парадигме управления сетями. Рост сложности сетей следующего поколения, включающих SD-WAN, частные сети 5G, современные стандарты Wi-Fi и периферийные вычисления, делает использование искусственного интеллекта обязательным условием для обеспечения их надежной и эффективной работы [1].

Современные возможности AIOps охватывают автоматизацию сбора и корреляции телеметрических данных, предиктивную аналитику для упреждающего выявления проблем, обнаружение аномалий, взаимодействие на естественном языке и использование агентного ИИ для автономного выполнения рутинных операций. Важным компонентом становятся цифровые двойники, позволяющие безопасно тестировать изменения перед применением в продуктивной среде [4, 7].

Вместе с тем, существуют значительные ограничения, связанные с качеством и унификацией данных, необходимостью обеспечения объяснимости решений и доверия к ним со стороны инженеров, а также сложностью интеграции с унаследованными системами. Преодоление этих вызовов требует системного подхода, инвестиций в инфраструктуру данных и, что не менее важно, в развитие компетенций персонала [5].

Будущее сетевого управления видится в автономных системах, где AI-агенты будут выполнять функции операторов первого уровня, а человек сосредоточится на стратегических задачах и управлении исключительными ситуациями [7]. В этом контексте AIOps выступает ключевым инструментом, трансформирующим операционную деятельность и открывающим возможности для построения действительно самооптимизирующихся сетей.

СПИСОК ИСТОЧНИКОВ

1. Doyle K. How AIOps enables next-generation networking / K. Doyle // TechTarget [Электронный ресурс]. – URL: <https://www.techtarget.com/searchnetworking/opinion/Next-gen-network-management-difficult-without-AIOps> (дата обращения: 25.02.2026).
2. Lapteff A. Ask EDA: AIops built for network engineers / A. Lapteff // Nokia Blog [Электронный ресурс]. – URL: <https://www.nokia.com/blog/ask-eda-aiops-built-for-network-engineers/> (дата обращения: 25.02.2026).

3. Wagar C. The progression of AIOps in today's network environment / C. Wagar // Nokia Blog [Электронный ресурс]. – URL: <https://www.nokia.com/blog/the-progression-of-aiops-in-todays-network-environment/> (дата обращения: 25.02.2026).
4. From Ambition to Action: The Future of AIOps and Agentic AI in Telecom // RADCOM [Электронный ресурс]. – URL: <https://radcom.com/further-reading/from-ambition-to-action-the-future-of-aiops-and-agentic-ai-in-telecom/> (дата обращения: 25.02.2026).
5. Vasiliou L. SRE Report Retrospectives – Have AIOps Predictions Held Up? / L. Vasiliou, D. Chikura // Catchpoint Systems [Электронный ресурс]. – URL: <https://www.catchpoint.com/blog/sre-report-retrospectives---have-aiops-predictions-held-up> (дата обращения: 25.02.2026).
6. HPE Accelerates Self-driving Network Operations with New Mist Agentic AI-native Innovations // HPE [Электронный ресурс]. – URL: <https://www.hpe.com/us/en/newsroom/press-release/2025/08/hpe-accelerates-self-driving-network-operations-with-new-mist-agentic-ai-native-innovations.html> (дата обращения: 25.02.2026).
7. Townsend W. RESEARCH PAPER: IBM – Unlocking Resiliency Through Network Intelligence / W. Townsend, P. Moorhead // Moor Insights & Strategy [Электронный ресурс]. – URL: <https://moorinsightsstrategy.com/research-papers/research-paper-ibm-unlocking-resiliency-through-network-intelligence/> (дата обращения: 25.02.2026).
8. Paul S. Key enterprise networking predictions for 2026 / S. Paul // Express Computer [Электронный ресурс]. – URL: <https://www.expresscomputer.in/guest-blogs/key-enterprise-networking-predictions-for-2026/131429/> (дата обращения: 25.02.2026).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Колесников Евгений Андреевич, студент 1 курса аспирантуры, Воронежский институт высоких технологий, Воронеж, Россия.

e-mail: zhenya.kolesnikov.2001@gmail.com

Кострова Вера Николаевна, доктор технических наук, профессор, Воронежский институт высоких технологий, Воронеж, Россия.

e-mail: kostrova_v@mail.ru