

службы и ставший мировым стандартом для быстрой обработки данных в кибербезопасности. Его ключевые преимущества: полная безопасность (клиентская обработка), интуитивность (drag-and-drop рецепты), масштабируемость (от веб-версии до Docker в корпоративном периметре). Разработанные в работе рецепты могут быть непосредственно применены в деятельности SOC, а сам инструмент рекомендован для включения в «джентльменский» набор аналитика информационной безопасности. Попробуйте операцию Magic на первой попавшейся подозрительной строке – и вы поймёте, почему CyberChef называют кибершвейцарским ножом.

#### СПИСОК ЛИТЕРАТУРЫ

- 1 CyberChef : The Cyber Swiss Army Knife // GitHub. – URL: <https://github.com/gchq/CyberChef> (date of access: 28.04.2026).
- 2 CyberChef Live Demo // GCHQ. – URL: <https://gchq.github.io/CyberChef/> (date of access: 28.04.2026).
- 3 **Давыдова, А.** CyberChef – швейцарский кибер-нож / А. Давыдова // Codeby.net. – 2024. – URL: <https://codeby.net/blogs/cyberchef-shvejsarskij-kiber-nozh/> (дата обращения: 28.04.2026).
- 4 CyberChef – инструмент, который заменяет десятки утилит // Хабр. – URL: <https://habr.com/ru/articles/cyberchef-instrument/> (дата обращения: 28.04.2026).
- 5 SANS Digital Forensics and Incident Response Poster // SANS Institute. – URL: <https://www.sans.org/posters/windows-forensic-analysis/> (date of access: 28.04.2026).

Получено 27.05.2026

---

ISSN 2227-1155. Сборник студенческих научных работ.  
Вып. 31. Гомель, 2026

---

УДК 621.314

*М. Е. ГОНЧАРОВ, В. Ю. АШУРКО (ЭМ-31)*

Научные руководители: старшие преподаватели *В. Е. МИНИН,*  
*С. В. КИСЕЛЕВА*

## **ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОЦЕССАХ DEVOPS**

Рассматриваются методологические и архитектурные аспекты интеграции технологий искусственного интеллекта в DevOps-практики (концепция AIOps). Проведён анализ стека наблюдаемости, пайплайнов обработки телеметрии и роли MLOps в управлении жизненным циклом моделей. Представлена методология оценки эффективности на основе количественных метрик (FPR, MTTR, TCO). Рассмотрены риски информационной безопасности, связанные с использованием генеративных моделей и систем автоматического реагирования, а также сформулированы требования к качеству данных и верификации алгоритмов.

Современная цифровая инфраструктура характеризуется высокой степенью распределённости, динамичностью и гетерогенностью компонентов. Поддержание работоспособности таких систем требует непрерывного мониторинга, оперативной диагностики инцидентов и высокой скорости доставки программных обновлений. Методология DevOps, объединяющая процессы разработки и эксплуатации, стала отраслевым стандартом, однако по мере усложнения архитектуры (переход к микросервисам, контейнеризация, оркестрация) возможности ручного анализа телеметрии и реагирования на сбои оказываются существенно ограниченными [1].

В данных условиях применение методов машинного обучения и анализа больших данных открывает возможности для автоматизации рутинных операций, повышения точности прогнозирования инцидентов и оптимизации использования вычислительных ресурсов. Концепция AIOps (Artificial Intelligence for IT Operations), формализованная в середине 2010-х годов, предполагает использование ИИ для корреляции событий, обнаружения аномалий, анализа корневых причин (Root Cause Analysis, RCA) и автоматизации реагирования [2]. Целью данной работы является систематизация архитектурных парадигм построения AIOps-систем, анализ методологии оценки их эффективности, а также выявление ключевых требований к данным, аспектов информационной безопасности и практик MLOps.

Центральной основой любой AIOps-системы является обеспечение наблюдаемости (observability), которая в современной инженерной практике базируется на трёх компонентах: метриках (metrics), журналах событий (logs) и распределённых трассировках (traces) [3]. В качестве ядра сбора и хранения метрик в open-source стеке широко используется Prometheus – система, адаптированная для динамических сред на базе Kubernetes [4]. Prometheus работает по pull-модели, периодически опрашивая endpoints экспортеров, что обеспечивает устойчивость к кратковременным сетевым сбоям.

Интеграция машинного обучения начинается на этапе предобработки телеметрии. Сырые временные ряды содержат шум, пропуски и сезонные зависимости, требующие нормализации и инженерии признаков (feature engineering) перед подачей в модель [5]. Для обнаружения аномалий применяются различные алгоритмы: от статистических методов до глубоких нейронных сетей-автоэнкодеров, которые обучаются воспроизводить нормальное поведение системы [6]. Выбор алгоритма зависит от характера нагрузки, доступности размеченных данных и вычислительных ограничений.

Результаты работы моделей интегрируются в систему оповещения через Alertmanager, обеспечивающий группировку, подавление дубликатов и маршрутизацию уведомлений [7]. Управление конфигурацией AIOps-инфраструктуры реализуется через подход GitOps: инструменты Argo CD и Flux используют Git как единый источник истины для декларативного описания состояния кластера, что обеспечивает версионирование и упрощает

откат изменений [8]. Оценка внедрения AIOps требует перехода от качественных описаний к строгой количественной методологии. Эффективность системы целесообразно анализировать на трёх уровнях: качество модели, операционные показатели и экономические затраты.

**Качество модели детекции аномалий** определяется следующими метриками: False Positive Rate (FPR) – доля нормальных состояний, ошибочно классифицированных как аномалии. Высокий FPR приводит к «усталости от оповещений» (alert fatigue), когда операторы начинают игнорировать предупреждения [9]. True Positive Rate (Recall) определяет долю реально произошедших инцидентов, успешно выявленных системой. Зависимость между TPR и FPR при варьировании порога классификации отображается на ROC-кривой. В задачах мониторинга оптимизация направлена на минимизацию FPR при сохранении приемлемого TPR [10].

**На операционном уровне** основным показателем является Mean Time to Resolve (MTTR). AIOps способствует снижению MTTR за счёт уменьшения Mean Time to Detect (MTTD) и автоматизации первичной диагностики. Важно учитывать, что снижение MTTR не является автоматическим следствием внедрения ИИ; оно требует зрелых процессов инцидент-менеджмента и интеграции с ITSM-системами [11].

**Экономическая целесообразность** оценивается через совокупную стоимость владения (Total Cost of Ownership, TCO), которая включает затраты на вычислительные ресурсы для обучения и инференса, хранение телеметрии, а также трудозатраты на поддержку моделей [12]. Внедрение должно сопровождаться этапом установления базовых значений и пилотным развёртыванием для объективной оценки влияния на процессы.

Выбор технологического стека для AIOps определяется балансом между гибкостью, скоростью внедрения и бюджетом. Сравнение подходов представлено в таблице 1.

*Таблица 1 – Сравнительный анализ open-source и коммерческих AIOps-решений*

| Характеристика      | Open-source стек (Prometheus, Grafana, Argo CD, KubeFlow)   | Коммерческие платформы (Datadog AI, Dynatrace, PagerDuty AIOps) |
|---------------------|-------------------------------------------------------------|-----------------------------------------------------------------|
| Гибкость            | Высокая – полный контроль над кодом и интеграциями          | Ограничена API вендора; vendor lock-in                          |
| Стоимость           | Нет лицензий; высокие затраты на поддержку и инфраструктуру | Подписка SaaS; включает поддержку и обновления                  |
| Скорость внедрения  | Низкая (месяцы); требует глубоких компетенций               | Высокая (дни/недели); готовые алгоритмы                         |
| Поддержка / SLA     | Сообщество и консультанты                                   | 24 / 7 от вендора, гарантия SLA                                 |
| Безопасность данных | Полный контроль, возможно on-premise                        | Зависит от политики вендора; требуется DPA                      |

Open-source стек обеспечивает полный контроль над архитектурой, однако требует значительных компетенций для интеграции компонентов и настройки пайплайнов MLOps. Коммерческие платформы предлагают готовые алгоритмы корреляции и детекции, сокращая время вывода в эксплуатацию, но формируют зависимость от вендора (vendor lock-in) [13]. В современных условиях наблюдается тенденция к гибридным архитектурам: open-source для сбора телеметрии и коммерческие платформы для расширенной аналитики.

Интеграция больших языковых моделей (LLM) в критические процессы DevOps вводит новые векторы угроз. Злоумышленник может модифицировать входные данные (комментарии в коде, логи), чтобы спровоцировать LLM на генерацию уязвимых конфигураций Helm-чартов или Terraform-манифестов (Prompt Injection). Для снижения риска применяется строгая валидация входных данных и обязательная статическая анализация (SAST) сгенерированного кода [14]. Передача журналов событий или конфигураций во внешние LLM-сервисы может привести к непреднамеренному экспорту секретов (API-ключей, PII). В качестве контрмер рекомендуется обязательная предварительная очистка (data masking), использование локально развёрнутых моделей и шифрование данных [15]. Системы автономного реагирования (auto-remediation), способные изменять состояние инфраструктуры, требуют обязательного принципа Human-in-the-Loop (HITL) для production-окружений [16]. Обработка данных должна соответствовать регуляторным требованиям; использование сторонних ИИ-сервисов требует заключения договоров об обработке данных (DPA) [17].

Качество AIOps-систем напрямую определяется репрезентативностью обучающих данных. Для корректного обучения моделей детекции аномалий необходимы исторические временные ряды, охватывающие различные режимы работы системы: штатную нагрузку, пиковые значения, плановые обслуживания и прошлые инциденты [5].

Ключевой проблемой является дрейф данных (data drift) – изменение статистических характеристик входных данных из-за обновления ПО или изменения бизнес-логики. Для противодействия применяются практики MLOps, адаптирующие принципы DevOps к жизненному циклу моделей [11]. Платформы, такие как Kubeflow, позволяют автоматизировать конвейеры переобучения по расписанию или при обнаружении статистического отклонения метрик от базовых [13]. MLOps обеспечивает версионирование данных и моделей, воспроизводимость экспериментов и стандартизацию деплоя. Без MLOps управление множеством моделей превращается в ручную операцию, подверженную ошибкам [12].

Интеграция технологий искусственного интеллекта в DevOps-практики представляет собой закономерный этап эволюции IT-операций. Переход от реактивного мониторинга к проактивной аналитике требует построения целостной архитектуры, объединяющей сбор телеметрии, предобработку данных, машинное обучение и автоматизированное управление конфигурацией.

Успешное внедрение AIOps невозможно без чёткой методологии оцен-

ки, базирующей на метриках FPR, MTTR и TCO, а также без учёта специфики жизненного цикла моделей через практики MLOps. Критически важным аспектом остаётся обеспечение информационной безопасности: защита от prompt injection, предотвращение утечек данных и сохранение человеческого контроля над критическими изменениями. Перспективными направлениями являются разработка стандартизированных бенчмарков для оценки AIОps-алгоритмов и интеграция методов объяснимого ИИ (ХАИ) для повышения доверия к автоматическим диагнозам.

## СПИСОК ЛИТЕРАТУРЫ

- 1 What Is AIОps? // Gartner. – URL: <https://www.gartner.com/en/information-technology/glossary/a-i-o-p-s> (date of access: 15.04.2026).
- 2 **Dang, Y.** AIОps: Real-World Challenges and Research Innovations / Y. Dang, Q. Lin, P. Huang // 2019 IEEE / ACM 41st ICSE: Companion Proceedings. – IEEE, 2019. – P. 5–6.
- 3 **Majors, C.** Distributed Systems Observability / C. Majors, L. Fong-Jones, G. Miranda. – Sebastopol : O'Reilly Media, 2018. – 288 p.
- 4 Prometheus Documentation. What is Prometheus? – URL: <https://prometheus.io/docs/introduction/overview/> (date of access: 20.04.2026).
- 5 **Chandola, V.** Anomaly Detection: A Survey / V. Chandola, A. Banerjee, V. Kumar // ACM Computing Surveys. – 2009. – Vol. 41, № 3. – P. 1–58.
- 6 Outlier Detection Using Replicator Neural Networks / S. Hawkins, H. He, G. Williams, R. Baxter // Data Warehousing and Knowledge Discovery. – Berlin : Springer, 2002. – P. 170–180.
- 7 Red Hat. AlertmanagerConfig documentation. – URL: <https://docs.openshift.com/container-platform/latest/monitoring/alertmanagerconfig.html> (date of access: 20.04.2026).
- 8 Declarative GitOps CD for Kubernetes // CD. Argo. – URL: <https://argocd.readthedocs.io/en/stable/> (date of access: 20.04.2026).
- 9 **Chen, M.** A Survey on Root Cause Analysis for Cloud-Native Systems / M. Chen, Y. Wang, X. Zhang // arXiv preprint arXiv:2305.01234. – 2023.
- 10 Cost of ownership for ML workloads // AWS. – URL: <https://aws.amazon.com/machine-learning/cost-optimization/> (date of access: 20.04.2026).
- 11 MLOps Principles // CNCF. – URL: <https://www.cncf.io/blog/2022/03/03/mlops-principles/> (date of access: 20.04.2026).
- 12 Hidden Technical Debt in Machine Learning Systems / D. Sculley, G. Holt, D. Golovin [et al.] // Advances in Neural Information Processing Systems. – 2015. – Vol. 28. – P. 2503–2511.
- 13 Pipelines // Kubeflow Documentation. – URL: <https://www.kubeflow.org/docs/components/pipelines/> (date of access: 20.04.2026).
- 14 Top 10 for Large Language Model Applications // OWASP. – URL: <https://owasp.org/www-project-top-10-for-large-language-model-applications/> (date of access: 18.04.2026).
- 15 AI Risk Management Framework (AI RMF 1.0) / NIST. – Gaithersburg : National Institute of Standards and Technology, 2023. – 45 p.
- 16 Responsible AI Standard // Microsoft. – URL: <https://www.microsoft.com/en->

УДК 316.36:342.4

*Р. П. ГОРБАЧ, М. И. ПУХТЕЕВ* (УД-11)

Научный руководитель – канд. ист. наук *Н. К. ТЕТЕРЮКОВ*

## **СЕМЕЙНАЯ ПОЛИТИКА В РЕСПУБЛИКЕ БЕЛАРУСЬ**

Рассматриваются основные направления семейной политики Республики Беларусь, вопросы защиты семьи, закрепленные в Конституции. Приводятся различные статистические данные. Анализируются неблагоприятные тенденции в контексте общемирового демографического спада и влияния западных либеральных ценностей. На основании данных Белстата и соцопросов Института социологии НАН Беларуси подтверждается высокая значимость семьи для белорусов.

Семья – это не только «ячейка общества», но и фундамент для построения успешного унитарного демократического социально-правового государства, каким и является Республика Беларусь. Укрепление института семьи способствует передаче традиций, основных семейных ценностей, а следовательно, это вклад в успешное завтра. Государственная политика нашей страны направлена на поддержку семьи, где отец – глава и опора для всего рода, источник накопленного в поколениях опыта, силы и мудрости предков, а мать – хранительница очага и духовный центр семьи, обеспечивающая гармонию и преемственность. Такая модель является основой стабильности общества и направлена на воспитание подрастающего поколения в духе патриотизма и уважения к исторически сложившимся традициям.

В соответствии с Конституцией Республики Беларусь брак, семья, материнство, отцовство и детство находятся под опекой государства [1].

Седьмым Всебелорусским народным собранием утверждена Концепция национальной безопасности Республики Беларусь, в которой отражены вопросы защиты института семьи и традиционных семейных ценностей.

В настоящее время в нашей стране особое внимание уделяется многодетным семьям: государство оказывает как правовую, так и материальную помощь, а также содействует оказанию условий для участия обоих родителей в воспитании детей [2, 3].

Сегодня в Республике Беларусь проживает свыше 2,6 млн семей, из которых более 43 % воспитывают несовершеннолетних детей. Ежегодно количество многодетных семей возрастает (2019 г. – порядка 106 тыс., 2025 г. –