УДК 004.89
© Т.В. Харченко, А.М. Малькута, Г.К. Крючков, 2025

Логирование, метрики и трассировка в современных системах: проблемы стоимости и идея автоматического повышения детализации

Т.В. Харченко
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
E-mail: tharchenko05@mail.ru
А.М. Малькута
студент 2 курса аспирантуры НИЯУ МИФИ, Москва
E-mail: AMMalkuta@mephi.ru
Г.К. Крючков
студент 2 курса аспирантуры НИЯУ МИФИ, Москва
E-mail: GKKryuchkov@mephi.ru

Аннотация: *В статье рассматривается роль наблюдаемости (логирование, метрики, трассировка) в распределённых системах и её влияние на операционные и финансовые показатели. На основе отраслевых исследований анализируются затраты на телеметрию с акцентом на журналирование и избыточный сбор данных, а также подходы к их оптимизации.*
Ключевые слова: *наблюдаемость, журналирование, метрики, трассировка, стоимость, инциденты.*

Logging, metrics and tracing in modern systems: cost issues and the idea of automatic detail management

T.V. Kharchenko
4st year undergraduate student at NRNU MEPhI, Moscow
E-mail: tharchenko05@mail.ru
A.M. Malkuta
2nd year postgraduate student at the NRNU MEPhI, Moscow
E-mail: AMMalkuta@mephi.ru
G.K. Kryuchkov
2nd year postgraduate student at the NRNU MEPhI, Moscow
E-mail: GKKryuchkov@mephi.ru

Abstract: *The paper examines the role of observability (logging, metrics and tracing) in distributed systems and its impact on operational and financial*

performance. Drawing on industry studies, it analyzes telemetry costs with a focus on logging and excessive data collection, and outlines cost-optimization approaches and the idea of temporarily increasing log detail during incidents.
Keywords: *observability, logging, metrics, tracing, cost, incidents.*

Наблюдаемость (observability) — это способность судить о внутреннем состоянии системы по данным, которые она производит. В программных системах это прежде всего журналы, метрики и трассировки. За последние годы такие системы стали сложнее: микросервисы, облака, распределённые топологии. Масштабность тренда подтверждает статистика: в 2024 году облачно-нативные практики внедрены у 89% организаций [1].

В таких условиях наблюдаемость перестала быть вспомогательной практикой и рассматривается как базовое требование эксплуатации. Её зрелость напрямую отражается на пользовательском опыте, стабильности и производительности сервисов. Недостаточная наблюдаемость в момент инцидента замедляет поиск первопричины и увеличивает стоимость простоя. В отдельных случаях потери достигают миллионов долларов в час, причём нередко, компании вообще не учитывают эти издержки [2]. Одновременно с этим, наблюдаемость – дорогостоящая практика, требующая соразмерных вложений. По профильным оценкам на неё приходится порядка 15–25% инфраструктурных затрат, причём журналы нередко оказываются самым затратным компонентом стека [3].

Данная статья преследует следующие цели: показать, как наблюдаемость влияет на ключевые операционные и финансовые показатели – доступность сервисов, время восстановления и выручку; проанализировать структуру затрат «тройного» стека телеметрии с отдельным акцентом на роль и стоимость журналирования; оценить, какие рыночные инструменты и подходы позволяют снижать расходы на наблюдаемость без ухудшения качества анализа инцидентов.

Как было сказано раннее, наблюдаемость превратилась в постоянную и значимую статью расходов, при этом её эффект на эксплуатацию можно измерить. Исследование New Relic показывает, что респонденты оценивают четырехкратную медианную окупаемость наблюдаемости (ROI) или, иными словами, на каждый $1 расходов респонденты оценивают $4 полученной ценности. Более того, у организаций со «сквозной наблюдаемостью» (видимость инфраструктуры, платформы, приложений и действий пользователей) фиксируется на 79% меньше годового простоя и на 48% ниже стоимость часа простоя, чем у менее зрелых команд [4].

При этом серьёзные инциденты остаются дорогими: по оценкам Uptime Institute, 54% респондентов сообщили о последнем инциденте дороже $100 000, а 16% – дороже $1 млн. При этом сами исследователи

предупреждают, что информация о простоях часто неполна и коммерчески чувствительна (то есть не все компании точно считают убытки). Это усиливает потребность в экономически обоснованной наблюдаемости: важно сопоставлять уровень видимости с реальными финансовыми рисками [5][6].

Практика показывает и «узкие места». В отчёте Logz.io заявлено, что у 82% компаний среднее время восстановления после инцидента (MTTR) превышает 1 час, причём доля растёт из года в год [7]. Можно сделать вывод о том, что накопление данных само по себе не гарантирует быстрый разбор инцидентов и что качество организации наблюдаемости не менее важно, чем её масштаб. Отдельные исследования фиксируют и «стоимостные» барьеры: 53% опрошенных указывают на цену и окупаемость как ключевую проблему при использовании инструментов наблюдаемости. На этом фоне появляются изменения тарифных моделей у провайдеров (например, перенос акцента с платы за «приём» журналов на хранение и аналитику), что отражает рост доли расходов именно на журналирование.

С точки зрения экономической целесообразности единая «норма окупаемости» для наблюдаемости отсутствует. Расходы носят постоянный характер и обычно растут вместе с объёмом телеметрии и сроком хранения: чем больше сервисов и трафика, тем больше журналов, метрик и трассировок требуется собрать и обработать. При этом выгоду нередко сложно точно измерить, поскольку она проявляется через сокращение времени простоя и восстановления, а также через косвенные эффекты (меньше откатов, стабильнее релизы).

Положительный эффект наблюдаемости зависит от чувствительности бизнеса к пользовательскому опыту и MTTR. Для массовых онлайн-сервисов и электронной коммерции наблюдаемость – инвестиция, так как быстрый разбор инцидентов напрямую связан с выручкой. В это же время в системах без прямого влияния на клиента наблюдаемость разумно трактовать как контролируемый операционный расход, при этом уровень видимости выбирается исходя из допустимого риска и целевых показателей. На практике удобно фиксировать долю инфраструктурного бюджета на наблюдаемость; отраслевые ориентиры — 15–25%, которые нужно соотносить с пользой для конкретной организации [3].

Стоит рассмотреть структуру расходов. По отраслевым обзорам больше половины бюджета на наблюдаемость уходит на журналирование. Остальные траты делятся между метриками и трассировками и сильно зависят от архитектуры и практик конкретной команды. В ряде материалов подчёркивается неэффективность «складирования всего подряд», свыше 70% затрат у некоторых организаций уходит на хранение журналов, к которым затем не обращаются. Отсюда вытекает необходимость внедрения

правил отбора записей и разумных сроков хранения (какие журналы сохранять, в каком объёме и на сколько времени) [9].

Почему так происходит. Журналы – это непрерывный поток подробных текстовых событий. По мере роста трафика и числа сервисов поток расширяется, а стоимость складывается из загрузки данных, их подготовки к поиску и сроков хранения. Метрики обычно хранятся как агрегированные числовые ряды, поэтому растут медленнее. Их главный риск – чрезмерная детализация меток (слишком много уникальных значений в подписи метрики), из-за чего резко увеличивается объём и нагрузка на хранилище. Трассировки чаще ограничивают выборочной записью: часть трасс пишут всегда, а «редкие и важные» – дополнительно отбирают при сбоях или аномалиях. Это стандартный способ удерживать объём трассировок под контролем без потери ключевого контекста.

Ограничение расходов на журналирование – нестандартная, хотя и очень актуальная проблема, если опираться на исследование. Повсеместной единой практики пока нет, но уже сложился набор рабочих приёмов, которые компании применяют чаще всего:

1. Отбор на входе.
   Сразу отсекать малоценные записи и лишние поля до отправки в систему журналирования. В хранилище попадает только нужное.
2. Дифференцированные сроки хранения.
   Критичные и аудиторские журналы хранить дольше, рутинные — значительно меньше. Для старых данных использовать более дешёвые уровни хранения.
3. Архив вместо постоянного индекса.
   Старые журналы уводить в недорогое архивное хранилище и подгружать из него только нужные фрагменты при расследованиях. Основной «поисковый» слой остаётся компактным.
4. Снижение детализации по ситуации.
   В обычном режиме — базовый уровень записей; повышенная детализация включается точечно и на короткое время во время инцидентов или тестов.
5. Ограничение объёма потока.
   Вводить разумные лимиты на количество и размер событий, а также «облегчать» записи: убирать шумные поля, объединять повторяющиеся сообщения в сводки.

Отдельным блоком компания настроила динамическое повышение детализации: при срабатывании алертов по ключевым метрикам система автоматически включала расширенное логирование только для затронутых сервисов и маршрутов. После стабилизации инцидента детализация возвращалась к базовому уровню, а собранные подробные журналы отправлялись в архив для последующего анализа. В результате расходы на

журналирование уменьшились примерно на 40 %, при этом среднее время расследования инцидентов сократилось почти на 20 %. Кейс наглядно показывает, что комбинация отбора на входе, многоуровневого хранения и управляемого увеличения детализации позволяет согласовать глубину наблюдаемости с реальными финансовыми ограничениями, а не просто «резать логи вслепую».

Совместная рабочая группа из SRE, разработчиков и финансовых аналитиков начала с инвентаризации потоков журналов и классификации событий по ценности для расследований. Выяснилось, что около трети логов никогда не использовались в постмортемах и могли быть агрегированы или вовсе отключены. Команда внедрила фильтрацию на стороне приложений, уменьшила объём подробных записей для «здорового» трафика и ввела дифференцированные сроки хранения: транзакционные и безопасность-критичные журналы стали хранить дольше и в более дорогом хранилище, малозначимые — короче и в дешёвом архивном слое.

Практический пример показывает, как эти подходы работают в реальной крупной компании. В одном из кейсов, описанных в отчёте New Relic [4], рассматривается глобальная e-commerce-платформа, которая тратила на стек наблюдаемости сопоставимые суммы с расходами на продуктивные базы данных. Объём логов превышал 20 ТБ в сутки, при этом значительная часть записей приходилась на низкоценные технические сообщения веб-серверов и промежуточных сервисов. Среднее время расследования инцидентов оставалось высоким, а попытки просто «урезать» сбор логов сопровождались риском потерять критичный контекст.

Проведённый обзор показал, что наблюдаемость в современных распределённых системах — не опциональная практика, а необходимое условие эксплуатации. Её влияние проявляется в операционных и финансовых метриках: сокращается время простоя и восстановления, стабилизируется качество релизов, поддерживается пользовательский опыт. Однако вместе с этим, наблюдаемость формирует существенные постоянные расходы, которые растут вместе с масштабом телеметрии; наибольший вклад, как правило, даёт журналирование. Сложившиеся на рынке подходы позволяют сдерживать затраты — от отбора записей на входе и дифференцированных сроков хранения до архивирования и ограниченной повышенной детализации «по ситуации». Практическая задача сводится к соразмерности: объём и глубина наблюдаемости должны соответствовать профилю риска и экономической целесообразности конкретной организации.

С учётом выявленных тенденций целесообразно углублять экономику наблюдаемости на уровне конкретных компонентов стека, в первую

очередь журналирования. Перспективным направлением выглядит переход от статического «всегда подробно» к управляемой детализации: детальная запись включается в момент инцидента и ограничивается по времени и области действия, при сохранении контекста для расследования. Такой подход обещает уменьшить постоянные издержки без потери качества анализа инцидентов и логично продолжает линию оптимизации, обозначенную в обзоре.

Список использованных источников:

1. Cloud Native 2024: Approaching a Decade of Code, Community, and Cloud Native // CNCF. URL: https://www.cncf.io/reports/cncf-annual-survey-2024/ (дата обращения: 03.10.2025). CNCF
2. UK and Irish businesses “severely underestimating” the cost of IT outages, with millions lost per hour // ITPro. URL: https://www.itpro.com/business/business-strategy/uk-and-irish-businesses-severely-underestimating-the-cost-of-it-outages-with-millions-lost-per-hour (дата обращения: 03.10.2025). itpro.com
3. Observability Costs: How Much Should I Spend On Observability? (Part 1) // Honeycomb. URL: https://www.honeycomb.io/blog/how-much-should-i-spend-on-observability-pt1 (дата обращения: 03.10.2025).
4. 2024 Observability Forecast Report // New Relic. URL: https://newrelic.com/resources/report/observability-forecast/2024 (дата обращения: 03.10.2025). New Relic+1
5. Annual Outage Analysis 2024 — Executive Summary // Uptime Institute. URL: https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2024.Resiliency.Survey.ExecSum.pdf (дата обращения: 03.10.2025). Uptime Institute
6. Annual Outage Analysis 2024 // Uptime Institute. URL: https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2024 (дата обращения: 03.10.2025). Uptime Institute
7. Observability Pulse 2024: Trends & Challenges // Logz.io. URL: https://logz.io/observability-pulse-2024/ (дата обращения: 19.10.2025). Logz.io
8. Sumo Logic Eliminates Ingest Fees for Observability Log Data // DevOps.com. URL: https://devops.com/sumo-logic-eliminates-ingest-fees-for-observability-log-data/ (дата обращения: 19.10.2025). DevOps.com
9. Honeycomb. How Much Should I Spend On Observability? (Part 2). URL: https://www.honeycomb.io/blog/how-much-should-i-spend-on-observability-pt2 (дата обращения: 19.10.2025).