Костырева Лидия Валерьевна, магистрант
Российский новый университет
Kostyreva Lydia Valeryevna

Степанова Евгения Николаевна
кандидат педагогических наук, доцент кафедры
информационных систем в экономике и управления
Российский новый университет
Stepanova Evgeniya Nikolaevna

АНАЛИЗ ПРОБЛЕМ МОНИТОРИНГА В ПРОЦЕССЕ ТЕХНОЛОГИЧЕСКОЙ ПОДДЕРЖКИ ПЛАТЁЖНОГО ШЛЮЗА
ANALYSIS OF MONITORING PROBLEMS IN THE PAYMENT GATEWAY TECHNICAL SUPPORT PROCESS

Аннотация. Исследуется процесс мониторинга платёжного шлюза как составная часть технологической поддержки. Систематизированы источники телеметрии и организационные каналы получения сведений, предложена модель текущего процесса AS-IS, выделены основные потери времени и риски разрозненного инструментария. Сформирован набор показателей, пригодный для количественной оценки процесса и последующего обоснования единой системы мониторинга.

Abstract. The paper examines payment gateway monitoring as part of technical support. Telemetry sources and organizational information channels are systematized, an AS-IS process model is proposed, and the main time losses and risks caused by fragmented tools are identified. A set of indicators is formulated for quantitative process assessment and for substantiating an integrated monitoring system.

Ключевые слова: Платёжный шлюз, технологическая поддержка, мониторинг, наблюдаемость, журналы событий, инцидент, AS-IS.

Keywords: Payment gateway, technical support, monitoring, observability, event logs, incident, AS-IS.

Введение

Платёжный шлюз обеспечивает технологическое сопряжение информационных систем участников расчёта и передаёт сообщения, от своевременной обработки которых зависит доступность платёжной услуги. Для службы технологической поддержки существенны не только факты полного отказа, но и рост задержек, увеличение доли отклонённых операций, нарушение обмена с отдельным контрагентом и несогласованность статусов одной транзакции в разных системах. Поэтому мониторинг должен рассматриваться как сквозной процесс получения, сопоставления и интерпретации данных, а не как наблюдение за отдельной панелью.

Требования PCI DSS предусматривают документированные механизмы регистрации и мониторинга доступа к системным компонентам и данным держателей карт, а журналы должны поддерживать выявление аномалий и последующий анализ событий [3]. В распределённой системе одних журналов недостаточно: для установления причины сбоя необходимо связывать метрики, журналы и трассировки по времени, компоненту и идентификатору операции [7, 8]. При разрозненном хранении эти связи восстанавливаются специалистом вручную, что увеличивает время диагностики.

Цель исследования – выявить проблемы существующего процесса мониторинга технологической поддержки платёжного шлюза и сформировать показатели, по которым можно оценить эффект его оптимизации. Использованы методы процессного анализа, классификации источников данных, причинно-следственного анализа и сопоставления требований стандартов менеджмента услуг и информационной безопасности [1, 2].

Источники данных мониторинга

Информационная база мониторинга неоднородна. Машиночитаемую часть образуют журналы приложений, события операционной системы и сетевого оборудования, метрики производительности, трассировки запросов, результаты синтетических проверок и сведения о состоянии интеграционных интерфейсов. Организационную часть составляют обращения пользователей, сообщения GDS, ТКП, банков-эквайеров и иных контрагентов, записи в системе управления заявками, переписка и регламенты. Каждый источник отражает только часть ситуации и имеет собственную задержку обновления, структуру и правила доступа.

Таблица 1

Классификация источников данных мониторинга

Источник	Наблюдаемый признак	Ограничение при раздельном использовании
Метрики шлюза	Доступность, задержка, интенсивность, ошибки	Не раскрывают контекст конкретной операции
Журналы приложений	События обработки и диагностические сообщения	Разные форматы и уровни детализации
Распределённые трассировки	Путь запроса между компонентами	Требуют единого контекста и идентификаторов
Сетевой и инфраструктурный мониторинг	Состояние узлов, каналов и ресурсов	Слабая связь с бизнес-результатом платежа
Система заявок	Факт обращения, приоритет, ответственный, SLA	Инцидент регистрируется после обнаружения
Сообщения внешних участников	Наблюдения GDS, ТКП и эквайеров	Неодинаковая терминология и неполный контекст

Для корреляции источников целесообразно использовать единый идентификатор технической операции, временные метки с синхронизированным временем, наименование сервиса, среды и контрагента. Протокол syslog задаёт унифицированную структуру сообщения и разделяет содержание, источник и уровень серьёзности [5]. OpenTelemetry расширяет этот подход за счёт контекста трассировки: TraceId и SpanId позволяют связать журналы разных компонентов с одним прохождением запроса [8].

Модель процесса AS-IS

Типовой текущий процесс начинается либо с автоматического сигнала отдельного инструмента, либо с обращения внешнего участника. Дежурный специалист вручную проверяет несколько панелей и журналов, сопоставляет временные интервалы и идентификаторы, уточняет симптомы у контрагента, после чего создаёт или дополняет заявку. При отсутствии общего представления одна и та же проблема может породить несколько уведомлений и обращений. Эскалация зависит от опыта специалиста и полноты собранных им доказательств.

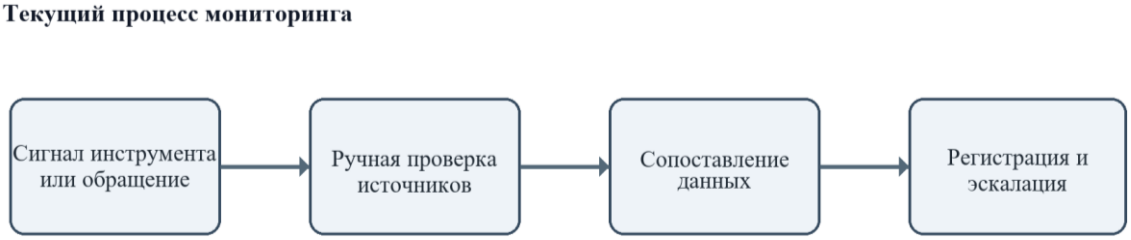

Рисунок 1. Укрупнённая модель процесса мониторинга AS-IS

Наиболее значимые проблемы процесса связаны не с отсутствием данных, а с отсутствием их управляемой связи. Во-первых, многократно выполняются поиск и копирование одних и тех же сведений. Во-вторых, задерживается определение зоны ответственности: инфраструктурный сбой, ошибка приложения и отказ внешнего интерфейса могут проявляться одинаково. В-третьих, отсутствует единая история события от первого сигнала до закрытия. В-четвёртых, раздельные правила оповещения создают повторные и низкоприоритетные уведомления, повышая риск пропуска действительно значимого сигнала.

Показатели оценки процесса

Для перехода от описания проблем к обоснованию проекта необходимы измеримые показатели. Их следует рассчитывать по единому набору временных отметок и разделять по критичности, сервису и участнику взаимодействия. В отличие от технической доступности отдельного узла показатели процесса отражают способность поддержки обнаружить, квалифицировать и локализовать отклонение.

Таблица 2

Предлагаемые показатели мониторинга и поддержки

Показатель	Способ расчёта	Назначение
MTTD	Среднее время от возникновения до обнаружения	Оценка скорости выявления
MTTA	Среднее время от сигнала до принятия в работу	Оценка реакции поддержки
MTTI	Среднее время до определения затронутого компонента	Оценка скорости локализации
Доля повторных уведомлений	Повторные сигналы / все сигналы	Контроль шума оповещений
Доля событий с полным контекстом	События с обязательными полями / все события	Контроль качества телеметрии
Доля ручных переходов	Ручные обращения к системам / расследования	Оценка фрагментации процесса
Точность маршрутизации	Верно назначенные обращения / все обращения	Оценка правил эскалации

Для оповещений необходимо различать запись наблюдения, предупреждение и инцидент. Практика SRE связывает срочное оповещение с воздействием на пользователя и необходимостью немедленного действия [6]. Механизмы группировки, подавления зависимых сигналов и временного отключения уведомлений, реализованные, например, в Alertmanager, уменьшают число дублирующих сообщений [9]. Однако эти механизмы эффективны только при наличии общей модели сервиса и правил владения.

Направления оптимизации

Первое направление состоит в нормализации телеметрии: единые обязательные поля, справочники сервисов и участников, правила времени и идентификации операций. Второе направление – централизованная корреляция метрик, журналов, трассировок и заявок. Третье – формализованная маршрутизация уведомлений с учётом критичности, затронутого сервиса и графика ответственности. Четвёртое – формирование единой карточки события, в которой сохраняются доказательства, решения, действия и результат. Пятое – управляемая обратная связь: после закрытия инцидента правила мониторинга уточняются на основании фактической причины и качества срабатывания.

Оптимизация не предполагает немедленную замену всех используемых продуктов. Практически оправдан интеграционный подход: существующие источники продолжают выполнять специализированные функции, а единая система принимает нормализованные события, связывает их с объектами сервисной модели и предоставляет общий рабочий контур. Это снижает риск миграции и позволяет внедрять целевую модель поэтапно.

Заключение

Анализ показал, что основной причиной потерь времени в мониторинге платёжного шлюза является фрагментация данных и действий поддержки. Разрозненные источники затрудняют корреляцию событий, порождают повторные уведомления и делают качество диагностики зависимым от индивидуального опыта. Предложенные показатели MTTD, MTTA, MTTI, доля повторных уведомлений, полнота контекста, доля ручных переходов и точность маршрутизации позволяют зафиксировать исходное состояние и проверить результат преобразований. Следующим этапом является разработка требований и модели единой информационной системы мониторинга

Список литературы:

1. ГОСТ Р ИСО/МЭК 20000-1-2021. Информационные технологии. Менеджмент услуг. Часть 1. Требования к системе менеджмента услуг. М.: Стандартинформ, 2021.

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva: ISO, 2022.

3. Payment Card Industry Data Security Standard: Requirements and Testing Procedures. Version 4.0.1. PCI Security Standards Council, 2024. URL: https://www.pcisecuritystandards.org/document_library/ (дата обращения: 22.09.2026).

4. Kent K., Souppaya M. Guide to Computer Security Log Management. NIST Special Publication 800-92. Gaithersburg: NIST, 2006. URL: https://csrc.nist.gov/publications/detail/sp/800-92/final (дата обращения: 22.09.2026).

5. Gerhards R. The Syslog Protocol. RFC 5424. IETF, 2009. URL: https://www.rfc-editor.org/rfc/rfc5424 (дата обращения: 22.09.2026).

6. Beyer B., Jones C., Petoff J., Murphy N. R. Site Reliability Engineering. Sebastopol: O'Reilly Media, 2016. URL: https://sre.google/sre-book/monitoring-distributed-systems/ (дата обращения: 22.09.2026).

7. OpenTelemetry. Observability Primer. URL: https://opentelemetry.io/docs/concepts/observability-primer/ (дата обращения: 22.09.2026).

8. OpenTelemetry. Logging Specification. URL: https://opentelemetry.io/docs/specs/otel/logs/ (дата обращения: 22.09.2026).

9. Prometheus Authors. Alertmanager. URL: https://prometheus.io/docs/alerting/latest/alertmanager/ (дата обращения: 22.09.2026)