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

ПРОЕКТИРОВАНИЕ ЕДИНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ МОНИТОРИНГА ТЕХНОЛОГИЧЕСКОЙ ПОДДЕРЖКИ ПЛАТЁЖНОГО ШЛЮЗА
DESIGN OF AN INTEGRATED INFORMATION SYSTEM FOR PAYMENT GATEWAY TECHNICAL SUPPORT MONITORING

Аннотация. Предложена концептуальная модель единой информационной системы мониторинга технологической поддержки платёжного шлюза. Сформированы функциональные и нефункциональные требования, определены архитектурные компоненты, модель события и порядок взаимодействия участников. Показано, как корреляция телеметрии и автоматизация маршрутизации обеспечивают переход от разрозненного контроля к управляемому сквозному процессу TO-BE.

Abstract. A conceptual model of an integrated monitoring information system for payment gateway technical support is proposed. Functional and non-functional requirements, architectural components, an event model, and participant interaction are defined. The paper shows how telemetry correlation and automated routing enable a transition from fragmented control to a manageable end-to-end TO-BE process.

Ключевые слова: Информационная система, платёжный шлюз, технологическая поддержка, мониторинг, корреляция событий, архитектура, TO-BE.

Keywords: Information system, payment gateway, technical support, monitoring, event correlation, architecture, TO-BE.

Введение

Разрозненный мониторинг платёжного шлюза не обеспечивает единого ответа на три практических вопроса технологической поддержки: что произошло, какие компоненты и участники затронуты, кто должен выполнить следующее действие. Даже при наличии достаточного количества журналов и метрик специалист вынужден вручную восстанавливать контекст операции. Проектируемая система должна преобразовать набор технических сигналов в управляемые события, связанные с сервисом, транзакцией, внешним участником и заявкой.

Цель статьи – разработать концептуальную модель единой информационной системы мониторинга технологической поддержки платёжного шлюза. Для достижения цели сформированы требования, определены компоненты архитектуры, предложена унифицированная модель события и описано взаимодействие участников в процессе TO-BE. Проектные решения опираются на требования менеджмента ИТ-услуг, защиты информации и практики наблюдаемости распределённых систем [1-9].

Требования к системе

Граница системы включает получение телеметрии, её нормализацию, обогащение справочными данными, корреляцию, формирование уведомления или инцидента, маршрутизацию и фиксацию действий. Исполнение платёжной операции и принятие финансового решения остаются за пределами системы мониторинга. Такое разделение исключает влияние аналитического контура на авторизацию платежа и позволяет применять минимально необходимые права доступа.

Таблица 1

Основные требования к единой системе мониторинга

Группа	**Требование**	**Ожидаемый результат**
Сбор	Приём метрик, журналов, трассировок, синтетических проверок и событий заявок	Полнота наблюдения
Нормализация	Единый формат времени, сервиса, среды, участника, критичности и идентификатора операции	Сопоставимость данных
Корреляция	Объединение связанных сигналов по контексту и временному окну	Одна карточка события
Маршрутизация	Назначение команды и канала по сервису, критичности и графику	Снижение времени реакции
Рабочее место	Хронология, зависимости, доказательства, действия и статус	Единый контекст расследования
Интеграция	Двусторонний обмен с системой заявок и каналами оповещения	Исключение повторного ввода
Аудит	Неизменяемая история доступа, решений и изменений правил	Контролируемость процесса
Аналитика	Расчёт MTTD, MTTA, MTTI, повторов и полноты контекста	Оценка результата

К нефункциональным требованиям относятся высокая доступность, масштабирование по потоку событий, контролируемая задержка обработки, отказоустойчивое хранение, синхронизация времени, разграничение доступа, шифрование каналов и данных, журналирование действий, маскирование платёжных реквизитов и управляемые сроки хранения. PCI DSS требует документировать процессы журналирования и мониторинга, а журналы использовать для выявления аномалий и расследования [3]. Следовательно, сбор диагностических данных не должен приводить к неконтролируемому копированию защищаемой информации.

Архитектурная модель

Предлагается слоистая интеграционная архитектура. Агенты, экспортёры и коннекторы принимают данные без изменения источников. Шина приёма отделяет скорость поступления от скорости обработки. Нормализатор преобразует форматы и добавляет контекст ресурса. Корреляционный модуль объединяет сигналы, применяет правила подавления и рассчитывает приоритет. Хранилища разделяются по типу данных и сроку хранения, а прикладной слой предоставляет панели, карточку события, отчётность и API интеграции.

Рисунок 1 – Концептуальная архитектура единой системы мониторинга

Архитектура должна поддерживать логи, метрики и трассировки как взаимодополняющие сигналы. Метрики показывают изменение состояния системы, журналы фиксируют дискретные события, а трассировки раскрывают путь запроса через распределённые компоненты [7]. Использование общего контекста ресурса и трассировки позволяет переходить из агрегированной метрики к конкретным операциям и связанным журналам [8]. При этом система не обязана хранить все типы данных в одной физической базе: единство обеспечивается общей моделью идентификаторов и поисковым интерфейсом.

Унифицированная модель события

Центральным объектом системы является событие мониторинга. Оно отделено от исходного сигнала: несколько сигналов могут быть объединены в одно событие, а событие после квалификации может стать инцидентом. Такая модель предотвращает создание заявки на каждое срабатывание и сохраняет связь с первичными данными.

Таблица 2

Состав унифицированного события мониторинга

Группа полей	**Примеры**	**Назначение**
Идентификация	event_id, trace_id, operation_id	Связь записей и операций
Время	occurred_at, observed_at, processed_at	Контроль задержек и последовательности
Источник	system, service, component, environment	Локализация объекта
Участник	GDS, ТКП, эквайер, внутреннее подразделение	Определение границы взаимодействия
Классификация	type, severity, confidence, status	Приоритизация и жизненный цикл
Воздействие	affected_service, transaction_count, user_impact	Оценка значимости
Маршрутизация	owner, escalation_policy, ticket_id	Назначение ответственности
Доказательства	metric_ref, log_ref, trace_ref, attachments	Воспроизводимость решения

Сырые сообщения сохраняются по ссылке и не копируются без необходимости в карточку события. Поля с платёжными реквизитами маскируются до поступления в общий контур. Доступ предоставляется по ролям, а обращения к данным и изменения правил регистрируются. Это согласует диагностическую полезность с принципом минимизации данных и требованиями информационной безопасности [2, 3].

Взаимодействие участников в процессе TO-BE

После поступления сигнала система автоматически добавляет сведения о сервисе и участнике, проверяет корреляционные правила и оценивает критичность. Если событие не требует действия, оно сохраняется для аналитики. При превышении порога система создаёт карточку, группирует зависимые сигналы, выбирает ответственную команду и направляет уведомление. Дежурный подтверждает событие, проверяет предложенный контекст и либо закрывает ложное срабатывание, либо переводит его в инцидент. При необходимости подключаются владелец сервиса, разработчик, специалист инфраструктуры и представитель внешнего участника.

Таблица 3

Распределение ответственности участников

Участник	**Ответственность**	**Результат в системе**
Система мониторинга	Сбор, корреляция, приоритизация и маршрутизация	Карточка события и уведомление
Дежурный специалист	Подтверждение, первичная диагностика, координация	Квалификация и журнал действий
Владелец сервиса	Оценка воздействия и приоритет восстановления	Решение по сервису
Техническая команда	Локализация причины и устранение	Диагноз, действие, результат
Внешний участник	Уточнение симптомов и подтверждение восстановления	Сообщение и подтверждение
Руководитель поддержки	Контроль SLA, качества правил и показателей	Отчёт и задача улучшения

Для уменьшения оповещательного шума применяются группировка, подавление зависимых уведомлений и временные исключения на период согласованных работ. Alertmanager демонстрирует эти базовые механизмы: группировку сходных оповещений, inhibition для подавления следствий известной причины и silences для временного отключения [9]. В проектируемой системе данные механизмы дополняются сервисной моделью, поэтому правило учитывает не только техническую метку, но и влияние на платёжную услугу.

Оценка ожидаемого эффекта и внедрение

Результат проекта следует оценивать не количеством подключённых источников, а изменением процесса. Базовые значения MTTD, MTTA и MTTI фиксируются до внедрения, затем сравниваются на одинаковых категориях событий. Дополнительно контролируются доля повторных уведомлений, доля событий с полным контекстом, точность автоматической маршрутизации и число ручных переходов между инструментами. Целевые значения устанавливаются после пилота, поскольку без фактической статистики произвольные проценты снижения не имеют доказательной силы.

Внедрение целесообразно проводить поэтапно. На первом этапе создаются каталог сервисов, модель события и единые правила идентификации. На втором подключаются источники одного критичного сценария и система заявок. На третьем настраиваются корреляция, маршрутизация и рабочее место дежурного. На четвёртом расширяется охват, вводятся показатели и цикл улучшения правил. Такой порядок позволяет проверить ценность архитектуры на ограниченном контуре и не связывает успех проекта с одновременной заменой всех инструментов.

Заключение

Разработана концептуальная модель единой информационной системы мониторинга технологической поддержки платёжного шлюза. Её ключевыми элементами являются интеграционный сбор телеметрии, нормализация, единая модель события, корреляция, управляемая маршрутизация и общая карточка расследования. Предложенное распределение ответственности сохраняет решение за специалистом, но устраняет повторный поиск данных и формализует передачу работы. Эффект системы может быть проверен по показателям скорости обнаружения, принятия в работу и локализации, а также по качеству контекста и оповещений.

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)