

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITYDOI: <https://doi.org/10.60797/IRJ.2026.172.39> EDN: OQJRAL**МЕТОД ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ КРИТИЧЕСКОГО ПОТОКА СОБЫТИЙ ПРИ ПЕРЕГРУЗКЕ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ**

Научная статья

Белкин Е.Н.^{1,*}, Кондрашев А.С.², Гориславец Д.В.³, Мазин А.В.⁴¹ ORCID : 0009-0007-5848-5433;^{1, 2, 3} АО «АЛГОНТ», Калуга, Российская Федерация⁴ Московский государственный технический университет имени Н. Э. Баумана, Москва, Российская Федерация

* Корреспондирующий автор (belkinen[at]algont.ru)

Предложена: 29.07.2026; Принята: 13.10.2026; Опубликовано: 16.10.2026

Аннотация

Цель исследования — разработать метод сохранения доступности критического потока событий распределенной системы физической безопасности при перегрузке без скрытой потери тревог. Метод А4 сочетает доверенное назначение классов P0–P3, резерв P0, взвешенное обслуживание, сквозное обратное давление, ограниченные очереди, семантическую агрегацию и идемпотентность. Основная нагрузочная серия включала 450 часовых запусков трех архитектур, дополнительные факторная, метрологическая и атакующая серии — 210 запусков. При фоне 4× медиана прогонного p99 P0 составила 7,41 с для общей FIFO-очереди, 2,25 с для двухочередного контроля и 1,38 с для метода А4; снижение относительно контроля — 38,7%, относительно нижней границы A0 — 81,4%. В методе А4 не наблюдалось потерь P0 как минимум для 3,6 млн событий на отдельном уровне нагрузки; односторонняя 95%-я верхняя граница по правилу трех — $8,3 \times 10^{-7}$ на событие. При 5× медиана прогонного p99 достигла 1,74 с, поэтому точка нарушения внутреннего SLA 1,5 с локализована между 4× и 5×. В серии с поддельной рекомендацией P0 доверенная классификация отклонила 100% атакующих сообщений из критического класса и сохранила медиану p99 легитимного P0 равной 1,43 с; контроль, принимавший рекомендацию источника, дал 9,86 с и 2,74% потерь. Выводы относятся к описанной стендовой конфигурации; перенос на иные реализации требует повторной настройки ресурсов, проверки синхронизации времени и воспроизведения объектового профиля нагрузки.

Ключевые слова: система физической безопасности, доступность информации, шторм событий, приоритетная очередь, хвостовая задержка, обратное давление, семантическая агрегация, устойчивость к перегрузке.

A METHOD FOR ENSURING THE AVAILABILITY OF A CRITICAL EVENT FLOW DURING A LOAD SHIFT IN A DISTRIBUTED PHYSICAL SECURITY SYSTEM

Research article

Belkin E.N.^{1,*}, Kondrashev A.S.², Gorislavets D.V.³, Mazin A.V.⁴¹ ORCID : 0009-0007-5848-5433;^{1, 2, 3} ALGONT JSC, Kaluga, Russian Federation⁴ Bauman Moscow State Technical University, Moscow, Russian Federation

* Corresponding author (belkinen[at]algont.ru)

Suggested: 29.07.2026; Accepted: 13.10.2026; Published: 16.10.2026

Abstract

The aim of the study is to develop a method for maintaining the availability of the critical event flow of a distributed physical security system under overload conditions without any hidden loss of alarms. The A4 method combines trusted assignment of classes P0–P3, a P0 reserve, weighted service, end-to-end backpressure, limited queues, semantic aggregation and idempotence. The main load test series consisted of 450 one-hour runs of the three architectures, with additional factorial, metrological and attack test series comprising 210 runs. In a 4× background, the median p99 P0 was 7.41 s for the general FIFO queue, 2.25 s for the two-queue control and 1.38 s for method A4; the reduction relative to the control was 38.7%, and relative to the lower bound of A0 was 81.4%. In the A4 method, no P0 losses were observed for at least 3.6 million events at a single load level; the one-sided 95% upper bound by the rule of three was 8.3×10^{-7} per event. At 5×, the median run-time p99 reached 1.74 s, therefore the point of violation of the internal 1.5 s SLA is located between 4× and 5×. In the series with a spoofed P0 recommendation, the trusted classification rejected 100 per cent of attacking messages from the critical class and maintained a median p99 of legitimate P0 equal to 1.43 s; the control, which accepted the source's recommendation, yielded 9.86 s and a 2.74% loss rate. The conclusions apply to the described test-bed configuration; porting to other implementations requires re-configuration of resources, verification of time synchronisation and reproduction of the object-based load profile.

Keywords: physical security system, information availability, event storm, priority queue, tail latency, backpressure, semantic aggregation, overload resilience.

Введение

Современная система физической безопасности крупного объекта представляет собой распределенный киберфизический комплекс. Камеры, контроллеры доступа, датчики, локальные узлы, серверы и автоматизированные рабочие места объединяются системой сбора и обработки информации (ССОИ), которая нормализует сообщения, связывает их с зонами, формирует инциденты и поддерживает управляющие действия. Подходы к интеграции и защищенному объединению подсистем рассмотрены в [1], [2].

Нарушение доступности ССОИ проявляется не только полным отказом, но и запаздыванием тревоги за допустимое время реагирования. Исследования охватывают хранение и корреляцию событий, защищенные архитектуры и объединение кибер- и физических наблюдений [3], [4], [5], [7]. Однако при шторме событий средняя задержка может оставаться приемлемой, тогда как высокие перцентили быстро растут; для распределенных сервисов именно хвост распределения определяет риск нарушения времени реакции [8].

Теория очередей задает условия устойчивости и запас производительности [9], [10], справедливое обслуживание ограничивает захват ресурса [11], а стадийные архитектуры локализуют перегрузку [12]. Современные решения используют admission control, координацию сервисов и обратную связь по хвостовой задержке [13], [14], [15]; потоковые платформы поддерживают повторную доставку и согласованное состояние [16], [17], [18]. Они, однако, не определяют субъект назначения высшего приоритета, допустимые способы агрегации и критерии отличия управляемого сокращения детализации от скрытой потери тревоги. Для киберфизического контура доступность и предсказуемость имеют самостоятельную ценность [19].

Научная проблема состоит в необходимости одновременно ограничить влияние фоновой нагрузки и сохранить проверяемость обработки. Цель исследования — разработать и экспериментально проверить метод доступности критических событий, основанный на доверенной классификации, резервировании и управляемом ограничении фона без скрытого удаления тревог. Новизна заключается не в отдельных механизмах, а в их защищенной предметно-ориентированной композиции: высший класс назначает доверенное ядро, резерв поддерживается на сквозном критическом пути, а сокращение фона допускается лишь через семантически разрешенные и аудируемые преобразования. Метод тем самым задает субъект назначения приоритета, границы деградации и критерии ее проверяемости.

Методы и принципы исследования

2.1. Формализация задачи, критерии и модель угроз

Для события e фиксируются время формирования источником $t_{src}(e)$ и время завершения критического этапа доставки $t_{out}(e)$. В критический этап включены прием, проверка минимального набора атрибутов, постановка в очередь, корреляция, минимальная запись аудита и отображение оператору. Сквозная задержка определяется выражением (1).

$$L(e) = t_{out}(e) - t_{src}(e). \quad (1)$$

Множество сообщений разделено на классы P0–P3. К P0 относятся события, непосредственно связанные с предотвращением опасного последствия; P1 включает значимые тревоги и подтвержденную аналитику; P2 — изменения состояния, действия оператора и конфигурационные события; P3 — диагностику, статистику и повтор неизменного состояния. Фоновый рост в эксперименте создавался преимущественно P2–P3, а расписание P0 оставалось одинаковым для сравниваемых схем.

Прогонным р99 называется 99-й перцентиль сквозных задержек P0 в 50-минутном измерительном окне одного часового запуска. Заранее заданная гипотеза требовала при фоне $4\times$ обеспечить р99 не более 1,5 с, снизить его не менее чем на 50% относительно A0 и исключить физическую потерю P0. Потерей считалось отсутствие и исходного события, и предусмотренного политикой проверяемого представления. Агрегация не считалась потерей при сохранении первого и последнего времени серии, числа повторов, максимальной критичности и записи правила.

Порог 1,5 с является внутренним SLA стенда. ГОСТ Р 52436-2024 устанавливает для доставки тревожного извещения от приемно-контрольного прибора до АРМ интегрированной системы безопасности или пульта предел 15 с [20], но этот участок не тождественен исследуемому сквозному пути. Для стендового проектирования 15-секундный предел разложен на бюджет: формирование и выдача извещения контроллером — 4,0 с; локальный адаптер — 2,0 с; транспорт — 2,0 с; исследуемый путь ССОИ — 1,5 с; отображение и первичное восприятие оператором — 1,0 с; резерв восстановления и джиттера — 4,5 с. Исследуемый путь расходует 10% общего предела и 15% функциональной части бюджета без резерва. Такое разбиение является проектным бюджетом стенда, а не нормативно установленной декомпозицией ГОСТ; на объекте его следует согласовывать с регламентом реагирования.

Модель угроз предусматривает компрометацию источника или адаптера, способного формировать корректно оформленный фон и завышать рекомендуемую критичность. Нарушитель не контролирует доверенное ядро, версии правил, сервер времени и минимальный аудит. Основная нагрузочная серия воспроизводила легитимный рост P2–P3 при неизменном P0. Дополнительная атакующая серия воспроизводила локальный всплеск из одной зоны: компрометированный адаптер в течение 10 мин передавал 3000 сообщений/с с рекомендацией P0 при неизменном легитимном потоке P0 40–60 событий/с; сравнивались метод A4 и контроль A4-U, непосредственно принимавший рекомендацию источника. За пределами подтверждаемой области остаются компрометация доверенного ядра, массовый поток семантически обоснованных P0 и отказ всех копий хранилища.

2.2. Метод устойчивой приоритетной обработки

Класс обслуживания назначается доверенным ядром после проверки типа события, зоны, режима объекта, идентичности источника и достаточности технических атрибутов. Полевое устройство или адаптер передает только рекомендуемую критичность. Политика предусматривает, что одно это поле не является основанием для повышения сообщения до P0; тем самым захват зарезервированного ресурса ограничивается на уровне проектных правил, пока

доверенное ядро и их версии не скомпрометированы. Правила классификации и деградации версионизируются. Политика обслуживания приведена в таблице 1.

Таблица 1 - Классы событий и политика обслуживания

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.1>

Класс	Типовые события	Обслуживание	Допустимая деградация
P0	Пожар, нападение, критический отказ защиты	Отдельная очередь, резерв емкости, строгий приоритет, минимальный аудит	Только свертка доказуемых повторов с сохранением первого, последнего и счетчика; скрытое удаление запрещено
P1	Тревога доступа, вскрытие, подтвержденная аналитика	Высокий вес, ограниченная очередь, эскалация	Отложенное вторичное обогащение
P2	Изменение состояния, действия оператора, конфигурационные события	Взвешенное справедливое обслуживание	Пакетирование и семантическая агрегация с сохранением переходов
P3	Диагностика, статистика, повтор неизменного состояния	Остаточная емкость, обратное давление, локальный spool	Снижение частоты, замена серии проверяемым агрегатом

Для P0 выделяются отдельная логическая очередь, ограниченный буфер и зарезервированный пул потребителей; P1–P3 обслуживаются по взвешенной справедливой дисциплине. Свободный резерв временно используется другими классами и возвращается при появлении P0. Условия (2) требуют, чтобы интенсивность P0 была меньше зарезервированной производительности, а сумма остальных классов — меньше остаточной емкости. При нарушении второго условия вход P2–P3 ограничивается вместо накопления неограниченной очереди.

$$\lambda_0 < \mu_{0, \text{res}} ; \sum_{k=1}^3 \lambda_k < \mu_{\text{total}} - \mu_{0, \text{res}} . \quad (2)$$

Число экземпляров обработчика m_i рассчитывается по измеренной производительности μ_i и допустимой загрузке ρ_i , сохраняющей запас на хвостовую задержку и отказ одного узла. В μ_i включается полный критический путь — проверка конверта, обращение к окну повторов, назначение приоритета, минимальный аудит и маршрутизация, а не только операция брокера. Проектное условие имеет вид (3).

$$m_i \geq \left\lceil \frac{\lambda_i}{\rho_i \mu_i} \right\rceil . \quad (3)$$

Емкость буфера определяется огибающей $A_p(\Delta)$ максимального прихода за окно Δ и гарантированным обслуживанием $S_p(\Delta)$. Минимальная емкость класса p рассчитывается по условию (4), которое учитывает короткие коррелированные всплески, возникающие при одном физическом инциденте одновременно на множестве устройств.

$$B_p(\Delta) \geq \max \{0, A_p(\Delta) - S_p(\Delta)\} . \quad (4)$$

Обозначения: e — событие; $t_{\text{src}}(e)$ и $t_{\text{out}}(e)$ — время формирования и завершения критического этапа; m_i — число экземпляров обработчика i ; μ_i — измеренная производительность одного экземпляра; ρ_i — допустимая загрузка; $A_p(\Delta)$ — максимальный приход класса p за окно Δ ; $S_p(\Delta)$ — гарантированное обслуживание за то же окно; Δ — длительность расчетного окна.

Обратное давление передается от потребителя к брокеру, адаптеру и локальному узлу. Для опрашиваемых источников увеличивается интервал не критической диагностики; для потоковых применяются ограничитель скорости и локальный spool. Если управление потоком недоступно, адаптер агрегирует только разрешенные повторы: переходы состояния, тревоги, действия оператора, изменения режима и команды не агрегируются. При исчерпании фонового раздела фиксируются диапазон номеров, причина и счетчик; резерв P0 отделен от фонового spool. Повторная доставка обрабатывается идемпотентно по `event_id` и ключу (`src`, `epoch`, `seq`), а пропуск после тайм-аута становится наблюдаемым признаком неполноты [16], [17], [18].

Соотношения (2)–(4) задают достаточные условия устойчивости и нижние границы ресурсов, но не являются прямой моделью р99. Параметры выбирались в два этапа: сначала проверялись ограничения по интенсивности, производительности и огибающей всплеска, затем резерв уточнялся предварительной серией по хвостовой задержке. Связь расчетных условий с конфигурацией и измерениями приведена в таблице 2.

Таблица 2 - Связь проектных условий, настроек и измерений

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.2>

Параметр	Расчетное основание и настройка	Экспериментальная проверка
Резерв P0	Условие $C_{P0} > \lambda_{P0, \max}$, где $\lambda_{P0, \max} = 60$ событий/с. Резерв 30% выбран по предварительной серии 15/30/40%.	1×: среднее прогонное p99 0,72 с; 4×: медиана 1,38 с (IQR 1,34–1,43). Резерв 40% снижал p99 до 1,17 с, но повышал p95 фонового класса на 21%.
Буфер P0	$B_{P0} \geq \sup \Delta[A_{P0}(\Delta) - S_{P0}(\Delta)]$. Принято 180 000 сообщений; при 60 событий/с это соответствует 3000 с входа даже при нулевом обслуживании.	В 50-минутном окне на измеренных уровнях физическая потеря P0 в методе не зарегистрирована.
Контроль конфигурации	Для изоресурсного сравнения фиксируются суммарные лимиты CPU и памяти, число обработчиков, prefetch и параметры пулов; различаются только топология очередей и политики. Числовой манифест приведен в таблице 3. В полной схеме prefetch = 32.	Различие при 1× не трактуется как прирост вычислительной емкости. Для всех вариантов выдержаны одинаковые суммарные лимиты и емкость очередей.

Логическая схема метода показана на рисунке 1. В исследованной конфигурации для P0 использованы резерв 30 %, предварительная выборка 32 сообщения и отдельная очередь емкостью 180 000 сообщений.



Рисунок 1 - Архитектура устойчивой приоритетной обработки

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.3>

2.3. Дизайн экспериментальной проверки

Эксперимент представлял парное сравнение трех основных архитектур: A0 — общая FIFO-очередь и единый пул потребителей как нижняя граница; A1 — практический контроль с mTLS, RBAC, очередями «критические/прочие», журналом только для добавления и проверками готовности; A4 — предлагаемый метод, далее единообразно «метод A4». Основным считается сравнение A1–A4, а A0 показывает цену отсутствия изоляции. Для кумулятивной абляции определены $A2 = A1 + \text{доверенная классификация } P0\text{--}P3 + \text{четыре ограниченные очереди} + \text{резерв } 30\% \text{ для } P0$, но без сквозного обратного давления и семантической агрегации; $A3 = A2 + \text{сквозное обратное давление и отделенный локальный spool при отключенной семантической агрегации}$; $A4 = A3 + \text{семантическая агрегация, идемпотентный повтор и обязательный аудит деградации}$. Во всех вариантах фиксировались одинаковые суммарные лимиты CPU и памяти, число обработчиков, предварительная выборка, параметры пулов и общая емкость очередей; различались только топология и политики. Встроенный приоритет брокера отдельно не исследовался: без доверенного назначения класса и сквозного ограничения входа он не предотвращает захват приоритета и перенос перегрузки; после доверенной классификации он совместим с методом A4.

Стенд включал три серверных узла по 8 vCPU и 16 ГБ оперативной памяти, четыре локальных узла по 4 vCPU и 8 ГБ, два автоматизированных рабочих места и отдельный сервер времени и мониторинга. Использовались KVM/QEMU 8.2, Ubuntu Server 24.04 LTS, Docker Engine 27, RabbitMQ 3.13, PostgreSQL 16 и Python 3.12; брокер и аудит размещались на отдельных NVMe-томах, сетевой контур имел пропускную способность 1 Гбит/с.

Модель объекта содержала 48 зон, 12 контрольно-пропускных пунктов, 384 точки доступа, 512 охранных и инженерных сигналов, 256 каналов видеометаданных и 28 регламентов реагирования. Имитатор поддерживал до 2048 логических устройств. Штатная интенсивность составляла 3000 событий/с; в основной серии исследовались уровни 1×, 2×, 4×, 5× и 6×. Дополнительно для метода A4 исследован промежуточный уровень 4,5× в отдельной серии из 30 запусков. Поток P0 сохранялся в диапазоне 40–60 событий/с, а рост создавался диагностикой, повторными состояниями и видеометаданными. Профиль генератора evtgen 2.4.1 / storm-p0p3-v3 фиксировал P1 на уровне 120 событий/с, распределял остальной фон между P2 и P3 в отношении 1:3 и каждые 5 мин создавал 15-секундный коррелированный всплеск 2,4×; применялись правила class-policy 1.7.3 и degradation-policy 1.4.2.

Таблица 3 - Параметры экспериментальной серии

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.4>

Параметр	Значение
Серверное ядро	3 узла; 8 vCPU и 16 ГБ ОЗУ на узел
Локальный контур	4 узла; 4 vCPU и 8 ГБ ОЗУ на узел
Программный профиль	KVM/QEMU 8.2; Ubuntu Server 24.04 LTS; Docker Engine 27; RabbitMQ 3.13; PostgreSQL 16; Python 3.12
Модель объекта	48 зон; 12 КПП; 384 точки доступа; 512 сигналов; 256 каналов видеометаданных; 28 регламентов
Нагрузка	3000 событий/с в режиме 1×; уровни основной серии 1×, 2×, 4×, 5× и 6×; дополнительный уровень 4,5× только для A4; P0 — 40–60 событий/с
Генератор и правила	evtgen 2.4.1; профиль storm-p0p3-v3; P1 = 120 событий/с; P2:P3 = 1:3; всплеск 2,4× длительностью 15 с каждые 5 мин; class-policy 1.7.3; degradation-policy 1.4.2
Сравниваемые схемы	A0 — общая FIFO; A1 — две очереди; A2 — A1 + классификация P0–P3 и резерв P0; A3 — A2 + сквозное обратное давление; A4 — полный метод
Изоресурсный манифест	RabbitMQ: 3×(1,5 vCPU; 2 ГБ); PostgreSQL-аудит: 3×(1,5 vCPU; 3 ГБ); обработчики: 18×(0,67 vCPU; 1 ГБ); суммарный лимит — 21 vCPU и 33 ГБ; prefetch = 32; 48 каналов брокера; пул БД = 64; пул HTTP/RPC = 128; суммарная емкость очередей = 600 тыс.; A0: 600 тыс.; A1: 180/420 тыс.; A2–A4 P0/P1/P2/P3: 180/90/150/180 тыс.; локальный spool: 4×256 тыс.
Повторы	Основная серия: 5 уровней × 30 блоков × 3 архитектуры = 450 часовых запусков; факторный план 2×2 при 4× = 120, включая 60 запусков F10/A2 и F11/A3, использованных также в кумулятивной абляции; метрологическая серия = 30; атакующая серия = 60; дополнительная серия A4 при 4,5× = 30; всего 690 запусков. Первые 10 мин — прогрев, последующие 50 мин — измерение.
Статистический анализ	Прогонные p50, p95 и p99; парный критерий Вилкоксона; коррекция Холма; ВСа-интервалы; для факторного плана — главные эффекты и взаимодействие с блочным бутстрепом
Рандомизация	Блочная: случайная перестановка трех основных архитектур внутри сопоставимого блока
Синхронизация времени	NTPv4, chrony 4.5, изолированная сеть; телеметрия смещения с периодом 1 с; дополнительная серия 30 запусков A4 при 4×

Единицей сравнения был сопоставимый блок: один входной журнал воспроизводился на А0, А1 и А4. На каждом из пяти общих уровней сформировано по 30 блоков: 150 блоков и 450 часовых запусков основной серии. Факторный план 2×2 при 4× включал 120 запусков; 60 запусков конфигураций F10/A2 и F11/A3, использованных в кумулятивной абляции, входили в эти 120 и отдельно не суммировались. Метрологическая серия включала 30 запусков, атакующая парная серия — 60. Дополнительная серия А4 при 4,5× включала 30 запусков; всего выполнено 690 часовых запусков. Зачетные серии проведены с 16 марта по 7 августа 2026 г.; суммарное стендовое время составило 690 ч без предварительной серии настройки резерва. В каждом запуске 10 мин отводились на прогрев и 50 мин — на измерение. Фон масштабировался сжатием временной шкалы при неизменном расписании Р0. Блочная рандомизация реализована случайной перестановкой трех основных схем внутри блока; между запусками очищались очереди, кэши и локальные буферы, создавались новые эпохи источников [21].

Метки времени фиксировались от источника до отображения. В повторной метрологической серии использовались NTPv4 и chrony 4.5 на отдельном сервере времени в изолированной сети; смещение каждого узла регистрировалось раз в 1 с. Максимальное абсолютное смещение составило 2,6 мс, 99,9-й перцентиль — 1,4 мс, среднеквадратический джиттер — 0,42 мс; консервативная суммарная неопределенность двух конечных меток не превышала 5,2 мс. Для каждого запуска рассчитывались р50, р95 и р99. Средние прогонных оценок описывают нагрузочную кривую; основными при 4× являются медиана, IQR и парный сдвиг. Парные ряды сравнивались критерием Вилкоксона с поправкой Холма; 95%-е ВСа-интервалы и сдвиг Ходжеса–Лемана получены по 10 000 блочным ресэмплированиям, размер эффекта — рангово-бисериальная корреляция. Значения р относятся к разностям прогонных р99, а не к проценту снижения.

Основные результаты

Таблица 4 показывает средние по 30 прогонным оценкам, а рисунок 2 — медианы и IQR прогонного р99 для А0, А1 и А4 на общих уровнях нагрузки как описательную нагрузочную кривую. Дополнительная точка 4,5× исследована только для А4 и приведена в таблице 4. При 1× среднее прогонное р99 равно 0,92 с для А0 и 0,72 с для метода А4. Различие не трактуется как прирост вычислительной емкости: коррелированные микровсплески присутствуют и при штатной средней интенсивности, а отдельный путь Р0 уменьшает блокировку «головы очереди». Проверка основной гипотезы относится к 4×.

Таблица 4 - Средние прогонные оценки задержки Р0 при росте фоновой нагрузки

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.5>

Фон	р95 А0, с	р95 А1, с	р95 А4, с	р99 А0, с	р99 А1, с	р99 А4, с
1×	0,49	0,44	0,41	0,92	0,80	0,72
2×	1,09	0,68	0,56	2,41	1,20	0,91
4×	3,28	1,18	0,83	7,44	2,26	1,39
4,5×	—	—	0,96	—	—	1,56
5×	5,27	1,81	1,08	12,22	3,48	1,76
6×	8,60	2,93	1,35	19,11	5,41	2,47

Примечание: n = 30 на точку; 4,5× — только А4

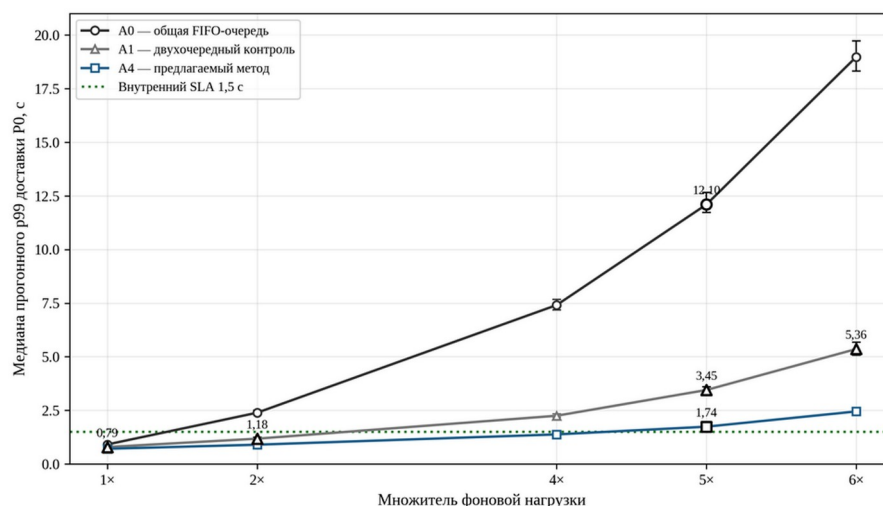


Рисунок 2 - Медиана прогнозного р99 доставки P0, с, в зависимости от множителя фоновой нагрузки
DOI: <https://doi.org/10.60797/IRJ.2026.172.39.6>

Примечание: $n = 30$ на точку, вертикальные отрезки — IQR

При четырехкратной фоновой нагрузке среднее прогножное р95 критического потока уменьшилось с 3,28 до 0,83 с. Медиана прогнозного р99 составила 7,41 с для A0, 2,25 с для A1 и 1,38 с для метода A4. Относительное снижение по формуле (5) равно 81,4% относительно A0 и 38,7% относительно практического контроля A1. Статистический критерий применялся к парным разностям прогножных р99; процентное снижение является описательной величиной.

$$\eta_{99} = \frac{p_{99, \text{base}} - p_{99, \text{method}}}{p_{99, \text{base}}} \cdot 100\% \quad (5)$$

В 30 прогонах метода A4 при 4× прогножное р99 находилось в диапазоне 1,26–1,49 с; медиана составила 1,38 с, IQR — 1,34–1,43 с, среднее — 1,39 с (95% ДИ 1,37–1,41 с). Внутренний предел 1,5 с выполнен во всех этих прогонах; наблюдаемых физических потерь P0 не было. В метрологической серии медиана составила 1,39 с против 1,38 с в основной серии; разность 0,01 с сопоставима с межсерийной вариативностью, но превышает зарегистрированную временную неопределенность 5,2 мс.

Таблица 5 - Физические потери P0 и семантическая агрегация

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.7>

Показатель	1×	2×	4×	5×	6×
Потери P0: A0, %	0,000	0,018	1,742	4,126	8,631
Потери P0: A1, %	0,000	0,000	0,004	0,019	0,071
Потери P0: метод A4, %	0,000	0,000	0,000	0,000	0,000
Потери всех классов: A0, %	0,000	0,020	1,794	4,288	8,867
Повторные P3, замененные агрегатами в A4, %	0,000	0,000	0,022	0,154	0,436
Сформировано и доставлено P0 методом A4, не менее, млн	3,6	3,6	3,6	3,6	3,6

После итоговой сверки event_id потери P0 при 4× составили 1,742% для A0 и 0,004% для A1; в методе A4 потерь не наблюдалось. При минимальной интенсивности P0 40 событий/с, 50-минутном измерительном окне и 30 прогонах число сформированных и доставленных методом событий на каждом отдельном уровне составляет не менее $N = 40 \times 3000 \times 30 = 3\,600\,000$. При допущении независимых бернуллиевских исходов для отдельных событий ориентировочная односторонняя 95%-я верхняя граница по правилу трех равна $3/N = 8,33 \times 10^{-7}$; при округлении вверх до двух значащих цифр — $8,3 \times 10^{-7}$ на событие, или 0,000083%. Это допущение не выполняется строго: события

внутри 15-секундных всплесков коррелированы, запуски выполнялись на общем оборудовании, а внутри сопоставимого блока воспроизводился один и тот же журнал. Поэтому событийную границу $8,3 \times 10^{-7}$ следует трактовать как оптимистичную условную оценку, а не как кластерно-устойчивый доверительный предел. Если единицей анализа считать независимый часовой запуск, то при нуле запусков с потерями из 30 точная односторонняя 95%-я верхняя граница вероятности хотя бы одной потери в запуске составляет 9,5%. Обе оценки относятся к отдельному уровню нагрузки, а не к объединенной серии.

В контролях потеря возникала при переполнении конечных входных буферов: новое сообщение отвергалось, а подтвержденные брокером сообщения не удалялись. После нагрузки event_id генератора сверялись с идентификаторами сообщений, завершивших критический этап, и допустимых агрегатов. Потерей считалось событие, отсутствующее в обоих множествах. В методе отдельный резерв P0 и ограничение P2–P3 обратным давлением и агрегацией предотвращали скрытое удаление P0 при переполнении фонового раздела.

Цена приоритизации для фоновых классов оценивалась отдельно при $4\times$ и $6\times$. В таблице 6 значения внутри ячейки перечислены в порядке P1/P2/P3. Физической потерей считалось отсутствие исходного события и допустимого представления; агрегация учитывалась отдельно.

Таблица 6 - Задержки, физические потери и агрегация фоновых классов P1–P3

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.8>

Архитектура	Фон	p95 P1/P2/P3, с	p99 P1/P2/P3, с	Потери P1/P2/P3, %	Агрегация P1/P2/P3, %
A0	$4\times$	3,02/3,35/3,61	6,72/7,52/7,96	1,210/1,780/1,820	0/0/0
A0	$6\times$	8,10/9,31/10,04	18,35/21,68/23,21	7,950/8,850/8,930	0/0/0
A1	$4\times$	1,22/3,74/4,58	2,34/8,19/9,71	0,006/0,031/0,047	0/0/0
A1	$6\times$	2,91/10,74/13,55	5,99/27,18/34,42	0,091/0,413/0,682	0/0/0
A4	$4\times$	1,11/2,77/3,16	1,99/5,68/6,37	0/0/0	0/0/0,022
A4	$6\times$	2,36/7,78/9,86	4,87/18,54/23,79	0/0/0	0/0/0,436

Примечание: $n = 30$

При $4\times$ метод A4 сохранил нулевую физическую потерю P1–P3; p99 составили 1,99/5,68/6,37 с, а 0,022% повторных P3 были заменены проверяемыми агрегатами. При $6\times$ p99 выросли до 4,87/18,54/23,79 с; в пределах 50-минутного измерительного окна потерь не зарегистрировано, доля агрегированных P3 составила 0,436%. Следовательно, защита P0 сопровождалась контролируемым ростом задержки P2–P3 и аудируемой сверткой P3, а не скрытым удалением фоновых событий в наблюдавшемся окне.

Нулевая физическая потеря P1–P3 при $6\times$ относится только к выбранной длительности наблюдения. При суммарной емкости локального pool 4×256 тыс. = 1024 тыс. сообщений и наблюдаемом росте 17,8 тыс. сообщений/мин расчетное время его исчерпания составляет 57,5 мин. Следовательно, при сохранении нестационарного режима физические потери фоновых классов могли возникнуть за пределами либо вблизи границы часового запуска; отсутствие потерь при $6\times$ не является установившимся свойством режима.

Агрегировались только повторные P3: серия заменялась записью с первым и последним временем, счетчиком, максимальной критичностью и версией правила. Доля 0,022% отражает объем сообщений, но не их концентрацию во всплесках. При $4\times$ максимальная доля повторных P3, замененных агрегатами в отдельном 15-секундном всплеске, составила 0,58%; медиана прогонных максимумов — 0,51% (IQR 0,47–0,55%). Снижение среднего p99 A3 → A4 с 1,54 до 1,39 с нельзя отнести только к агрегации: кумулятивное сравнение не отделяет ее от идемпотентного повтора и аудита деградации. Поэтому этот переход остается описательным; независимые эффекты резерва и обратного давления оцениваются факторным планом ниже.

Описательная статистика и парные сравнения прогонного p99 при $4\times$ приведены в таблицах 7 и 8; сравнения выполнялись внутри сопоставимых блоков.

Таблица 7 - Описательная статистика прогонного p99 доставки P0 при $4\times$ DOI: <https://doi.org/10.60797/IRJ.2026.172.39.9>

Архитектура	n	Медиана, с	IQR, с	Среднее (95 % ДИ), с	min–max, с
Общая очередь	30	7,41	7,18–7,67	7,44 (7,29–7,59)	6,84–8,12
Две очереди	30	2,25	2,17–2,34	2,26 (2,20–2,32)	2,05–2,49
Метод A4	30	1,38	1,34–1,43	1,39 (1,37–1,41)	1,26–1,49

Таблица 8 - Парные сравнения прогонного р99 доставки P0 при 4×

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.10>

Сравнение А–В	Δмед. (95 % ДИ), с	W	p	pHolm	r_rb
A0 – A4	6,02 (5,79–6,27)	0	$1,86 \times 10^{-9}$	$5,59 \times 10^{-9}$	1,000
A0 – A1	5,15 (4,91–5,39)	0	$1,86 \times 10^{-9}$	$5,59 \times 10^{-9}$	1,000
A1 – A4	0,86 (0,78–0,95)	0	$1,86 \times 10^{-9}$	$5,59 \times 10^{-9}$	1,000

Во всех 30 блоках парные разности имели одинаковый знак: $W = 0$, $r_rb = 1,000$, $pHolm = 5,59 \times 10^{-9}$. Для $n = 30$ это минимально достижимое двустороннее значение при полном разделении выборок; оно характеризует межпрогонную воспроизводимость на данном стенде, но не переносимость на иные реализации. ВСа-интервалы отражают только межпрогонную изменчивость и не включают конфигурационную неопределенность; временная погрешность оценивалась отдельно метрологической серией. Медианный парный выигрыш метода A4 составил 6,02 с относительно A0 и 0,86 с относительно A1.

Сопоставление архитектур A0–A4 при 4× показано на рисунке 3. A1 снизила медиану р99 до 2,25 с, но не обеспечила предел 1,5 с. Метод A4 дополнительно уменьшил медиану на 38,7% относительно A1. Поэтому именно A1–A4 является основным практическим сравнением; снижение на 81,4% относительно A0 следует трактовать как оценку относительно нижней границы, а не типовой производственной архитектуры.

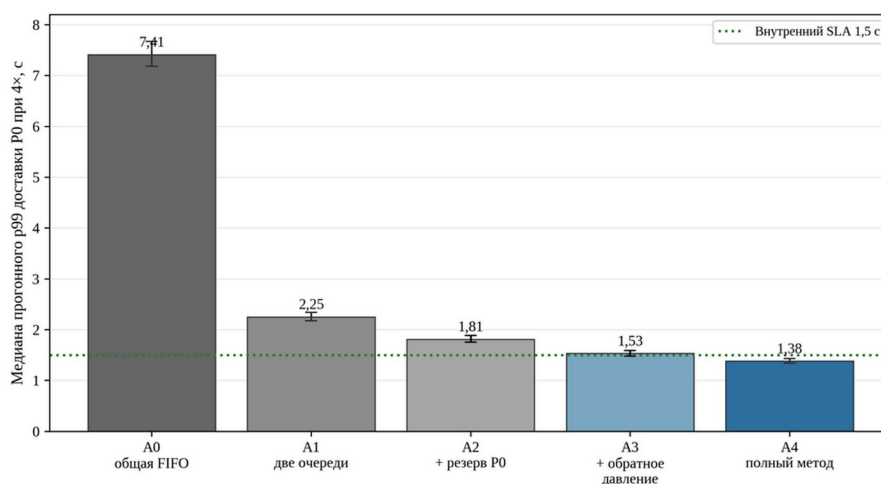


Рисунок 3 - Медиана прогонного р99 доставки P0 при 4×, с, для A0–A4

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.11>Примечание: $n = 30$, вертикальные отрезки — IQR

Кумулятивная абляция A0–A4 выполнялась при одинаковых лимитах CPU, памяти, обработчиков и хранилища; для A2 и A3 проведено по 30 запусков при 4×. Эти 60 запусков одновременно образуют ячейки F10/A2 и F11/A3 факторного плана и входят в указанные 120 запусков, а не добавляются к ним. Описательные средние прогонного р99 составили 2,26 с для A1, 1,82 с для A2, 1,54 с для A3 и 1,39 с для A4. Медианы A2 и A3 составили соответственно 1,81 с (IQR 1,75–1,88) и 1,53 с (IQR 1,48–1,59).

Для разделения вкладов выполнен факторный план 2×2 по факторам «резерв P0» и «сквозное обратное давление» при общей топологии P0–P3 и отключенной семантической агрегации. Конфигурации F00, F10 = A2, F01 и F11 = A3 запускались по 30 раз на одном и том же наборе журналов. Кумулятивный переход A3→A4 по-прежнему не атрибутирует независимый эффект семантической агрегации.

Таблица 9 - Факторный план «резерв P0 × сквозное обратное давление» при 4×

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.12>

Конф.	Резерв P0	Обратное давление	Медиана р99, с	IQR, с	Среднее (95 % ДИ), с
F00	нет	нет	2,35	2,28–2,44	2,37 (2,31–2,43)

Конф.	Резерв P0	Обратное давление	Медиана p99, с	IQR, с	Среднее (95 % ДИ), с
F10/A2	да	нет	1,81	1,75–1,88	1,82 (1,77–1,87)
F01	нет	да	2,03	1,97–2,11	2,05 (2,00–2,10)
F11/A3	да	да	1,53	1,48–1,59	1,54 (1,50–1,58)

Примечание: $n = 30$

Конфигурации F00 и A1 сопоставимы по суммарным ресурсам и входным журналам, но не образуют чистого однофакторного сравнения: одновременно различаются гранулярность классов, число и емкость очередей, а также дисциплина обслуживания. Описательно F00 с медианой 2,35 с (IQR 2,28–2,44) уступает A1 с медианой 2,25 с (IQR 2,17–2,34), причем межквартильные диапазоны не пересекаются. Следовательно, переход к четырем ограниченным очередям и доверенной классификации без резерва P0 и сквозного обратного давления сам по себе выигрыша не дал; вероятной причиной являются дополнительные издержки маршрутизации и фрагментация общей емкости обслуживания. Причинный эффект этих различий по сравнению F00–A1 не идентифицируется; F00 используется как базовая ячейка только внутри факторного плана.

Главные эффекты определялись как разность средних откликов на верхнем и нижнем уровнях соответствующего фактора, а эффект взаимодействия — как полуконтраст $[(F11-F10)-(F01-F00)]/2$, то есть в той же шкале факторного эффекта. Оцененный главный эффект резерва составил $-0,53$ с (95% ДИ $-0,59...-0,47$; $p < 0,001$), обратного давления — $-0,30$ с ($-0,36...-0,24$; $p < 0,001$); взаимодействие $+0,02$ с ($-0,02...0,06$; $p = 0,24$). Это подтверждает самостоятельный вклад обоих механизмов на данном стенде и не выявляет статистически значимого взаимодействия.

Предварительная серия настройки резерва при $4\times$ выполнялась до основной серии и не входила в 690 запусков. При резерве 15% среднее прогонное p99 P0 составляло 2,18 с, при 30% — 1,39 с, при 40% — 1,17 с. Последний вариант повышал p95 фонового класса на 21%, поэтому выбран компромисс 30%, а не максимальный резерв.

Четыре раздела аудита обеспечивали 45 592 записи/с; при $4\times$ использовалось 32,6 % этой производительности, при $6\times$ — 50,1%, поэтому аудит не был устойчивым узким местом. Внутренний SLA выполнен на уровнях $1\times$, $2\times$ и $4\times$. В дополнительной серии A4 при $4,5\times$ среднее прогонное p99 составило 1,56 с, медиана — 1,55 с (IQR 1,49–1,61; min-max 1,43–1,69); в 20 из 30 запусков предел 1,5 с был превышен, при этом потерь P0 не зарегистрировано. Поэтому пересечение порога локализовано между $4\times$ и $4,5\times$. При $5\times$ среднее прогонное p99 метода A4 составило 1,76 с, медиана — 1,74 с (IQR 1,68–1,81). Среднее заполнение фонового раздела при $5\times$ стабилизировалось около 63%; линейный уклон за последние 20 мин составил 0,07 процентного пункта/мин (95% ДИ $-0,02...0,16$), а после прекращения нагрузки очередь опустошалась до 5% за 84 с. При $6\times$ заполнение превысило 95% через 16,0 мин, локальный spool рос со скоростью 17,8 тыс. сообщений/мин, время опустошения составило 641 с; режим $6\times$ признан нестационарным. Таким образом, установленная стендовая граница SLA не отождествляется с универсальной вычислительной емкостью иных реализаций.

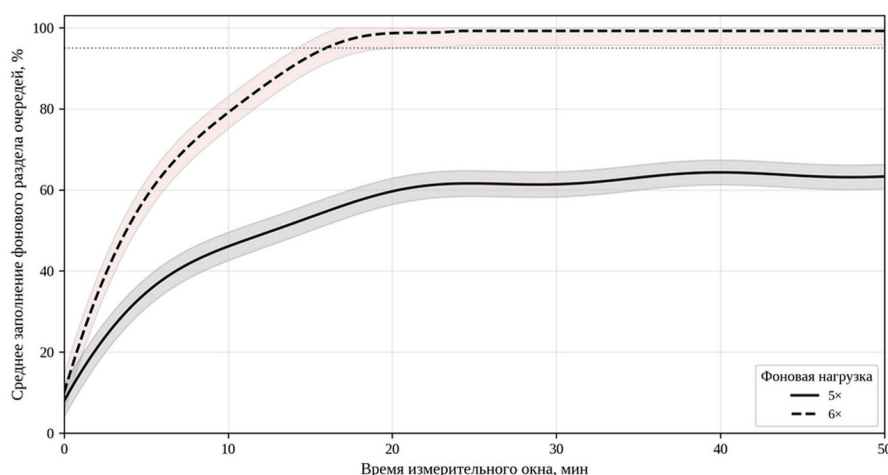


Рисунок 4 - Среднее заполнение фонового раздела очередей, %, при $5\times$ и $6\times$

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.13>

Примечание: $n = 30$, затенение — 95 %-й доверительный интервал

В атакующей серии при $4\times$ сравнивались метод A4 и контроль A4-U, принимавший рекомендацию источника как фактический класс. В каждом из 30 парных блоков один адаптер из одной зоны в течение 10 мин формировал 3000 сообщений/с с рекомендацией P0 при неизменном легитимном потоке P0 40–60 событий/с.

Таблица 10 - Результаты серии с массовым завышением рекомендуемой критичности при 4×

DOI: <https://doi.org/10.60797/IRJ.2026.172.39.14>

Вариант	Допуск атаки в P0, %	Медиана p99 легитимного P0, с	IQR, с	Потери легитимного P0, %	Макс. заполнение P0, %
A4	0,0	1,43	1,38–1,48	0,00	8,7
A4-U	100,0	9,86	9,21–10,62	2,74	100,0

Примечание: $n = 30$

Доверенная классификация отклонила 100% атакующих сообщений из P0 и сохранила проверяемое представление всех входов в аудите; медиана p99 легитимного P0 составила 1,43 с без потерь. В A4-U резерв P0 был полностью занят, медиана p99 достигла 9,86 с, потери легитимного P0 — 2,74%. Эксперимент подтверждает свойство только для указанного профиля, версии правил и нескомпрометированного ядра; он не покрывает семантически обоснованный массовый поток P0.

Обсуждение

Строгий приоритет изолирует критический поток только в пределах очереди или планировщика. Без ограничения входа перегрузка переносится в адаптер, брокер, базу данных или аудит. В полной конфигурации A4 сквозное обратное давление, ограниченные буферы и семантически допустимая агрегация образуют контур управляемой деградации, а регистрация преобразований сохраняет наблюдаемость. Факторный план независимо подтвердил вклад резерва P0 и сквозного обратного давления; семантическая агрегация проверена только как часть полной композиции, поэтому ее самостоятельный причинный эффект не заявляется. В отличие от универсальных решений [13], [14], [15], метод A4 связывает допустимое сокращение детализации с семантикой события и версией политики. Отечественные исследования отказоустойчивости киберфизических систем и перераспределения вычислительной нагрузки также подчеркивают необходимость согласования защитных контрмер с моделью угроз и наблюдаемым состоянием распределенного контура [22], [23].

Доверенное назначение приоритета является архитектурным результатом для информационной безопасности: источник, непосредственно маркирующий сообщения как P0, способен захватить резерв. Проверка идентичности, типа, зоны, режима и атрибутов переносит решение в доверенную область. Атакующая серия показала, что при исследованном профиле метод A4 сохранил критический ресурс, тогда как A4-U его исчерпал. Это не превращает проектное свойство в безусловную гарантию: результат ограничен нескомпрометированным ядром, конкретными версиями правил и одним профилем локального всплеска.

Нулевая наблюдаемая потеря P0 при не менее чем 3,6 млн событий на уровень не является универсальной гарантией. Интенсивность P0 сохранялась в проектном диапазоне 40–60 событий/с. Массовый поток событий, которые доверенное ядро обоснованно классифицирует как P0, способен исчерпать конечный резерв; для него требуются квоты по источнику и зоне, корреляция зависимых тревог, аварийная свертка доказуемых повторов и горизонтальное масштабирование критического контура.

Исследование проверяет устойчивость к перегрузке, но не общую отказоустойчивость: не выполнялись отказы потребителя, перезапуск брокера, сетевое разделение и фактическое исчерпание spool. Часть оборудования имитировалась, а стенд меньше предельного масштаба территориальной системы. Внешняя достоверность ограничена сервисно-ориентированными ССОИ с брокером сообщений. Метрологическая и атакующая серии выполнены только для A4 при 4× и не охватывают дрейф параметров на иных реализациях; временные ряды при 4,5×, 5× и 6× характеризуют один выбранный профиль нагрузки. Полный факторный план не включал семантическую агрегацию, поэтому ее независимый эффект остается неидентифицированным.

Заключение

1. Разработан метод A4 как защищенная предметно-ориентированная композиция доверенного назначения P0–P3, резерва P0, взвешенного обслуживания, сквозного обратного давления, ограниченных очередей, семантически допустимой агрегации, идемпотентности и обязательной регистрации деградации. Экспериментальная проверка относится к композиции в целом; самостоятельный вклад количественно идентифицирован для резерва P0 и сквозного обратного давления, тогда как независимый эффект семантической агрегации не установлен. Ограничение недоверенной рекомендации является проектным свойством политики и действует при нескомпрометированном доверенном ядре.

2. При 4× медиана прогонного p99 составила 1,38 с против 2,25 с у практического двухочередного контроля и 7,41 с у нижней границы A0; снижение равно 38,7% и 81,4% соответственно. Наблюдаемых потерь P0 не было как минимум для 3,6 млн событий на отдельный уровень. Событийная граница $8,3 \times 10^{-7}$ по правилу трех справедлива только при условной независимости событий и из-за корреляции всплесков является оптимистичной; при единице анализа «часовой запуск» верхняя односторонняя 95%-я граница вероятности хотя бы одной потери составляет 9,5% для нуля запусков с потерями из 30. Парная статистика подтверждает межпрогонную воспроизводимость на стенде, но не переносимость на иные реализации. При 4× физические потери P1–P3 не зарегистрированы. При 6× их отсутствие относится только к 50-минутному измерительному окну: расчетное исчерпание spool при сохранении наблюдаемого роста составляет 57,5 мин, поэтому режим не является стационарно без потерь. Цена защиты P0 проявилась в росте p99 P2–P3 и в аудируемой агрегации 0,022 % и 0,436 % повторных P3 при 4× и 6× соответственно.



3. На уровнях 1×, 2× и 4× внутренний SLA 1,5 с выполнен. На дополнительном уровне 4,5× медиана p99 составила 1,55 с (IQR 1,49–1,61), а предел был превышен в 20 из 30 запусков; стендовая точка нарушения SLA локализована между 4× и 4,5×. На 5× медиана p99 составила 1,74 с, а при 6× очередь вошла в нестационарный режим. Факторный план подтвердил самостоятельный вклад резерва P0 и сквозного обратного давления. Атакующая серия для одного профиля поддельной рекомендации P0 показала сохранение медианы 1,43 с и отсутствие потерь у A4 против 9,86 с и 2,74% потерь у A4-U. Метод применим как основа проектирования и нагрузочной приемки после проверки на объектовых журналах, документирования ресурсов и повторной метрологической оценки на целевой реализации.

Конфликт интересов

Е.Н. Белкин, А.С. Кондрашев и Д.В. Гориславец являются работниками АО «АЛГОНТ», деятельность которого связана с разработкой комплексных систем безопасности. Рукопись не содержит сравнительной оценки коммерческих продуктов. А.В. Мазин заявляет об отсутствии финансовых и нефинансовых конфликтов интересов. Иных конфликтов интересов авторы не заявляют.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

E.N. Belkin, A.S. Kondrashev and D.V. Gorislavets are employees of 'ALGONT' JSC, a company involved in the development of integrated security systems. The manuscript does not contain a comparative assessment of commercial products. A.V. Mazin declares that he has no financial or non-financial conflicts of interest. The authors declare no other conflicts of interest.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Куделькин В.А. Принципы создания интегрированных систем безопасности критически важных и потенциально опасных объектов / В.А. Куделькин, И.М. Янников, М.В. Телегина // Интеллектуальные системы в производстве. — 2017. — Т. 15. — № 1. — С. 105–109. — DOI: 10.22213/2410-9304-2017-1-105-109.
2. Белкин Е.Н. Построение защищенных интегрированных систем безопасности объектов УИС / Е.Н. Белкин, Д.А. Зайончковская // Информатизация и техническое обеспечение уголовно-исполнительной системы Российской Федерации: проблемы, решения и перспективы развития : материалы II Всероссийской научно-практической конференции, Тверь, 4–5 октября 2023 г. — Тверь: НИИИТ ФСИН России, 2023. — С. 28–34. — EDN: OHZOJH. — URL: <https://www.elibrary.ru/item.asp?id=60033173> (дата обращения: 24.07.2026).
3. Kotenko I. Systematic Literature Review of Security Event Correlation Methods / I. Kotenko, D. Gaifulina, I. Zelichenok // IEEE Access. — 2022. — Vol. 10. — P. 43387–43420. — DOI: 10.1109/ACCESS.2022.3168976.
4. Maosa H. A Hierarchical Security Event Correlation Model for Real-Time Threat Detection and Response / H. Maosa, K. Ouazzane, M.C. Ghanem // Network. — 2024. — Vol. 4. — № 1. — P. 68–90. — DOI: 10.3390/network4010004.
5. Seid E. Towards Security Attack Event Monitoring for Cyber Physical-Systems / E. Seid, O. Popov, F. Blix // Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023). — 2023. — P. 723–733. — DOI: 10.5220/0011803400003405.
6. Сухих Я.А. Разработка защищенных архитектур автоматизированных систем управления технологическими процессами / Я.А. Сухих, Д.И. Правиков, А.А. Кузичкин // Безопасность информационных технологий. — 2020. — Т. 27. — № 2. — С. 97–117. — DOI: 10.26583/bit.2020.2.08.
7. Fausto A. Toward the Integration of Cyber and Physical Security Monitoring Systems for Critical Infrastructures / A. Fausto, G.B. Gaggero, F. Patrone [et al.] // Sensors. — 2021. — Vol. 21. — № 21. — Art. 6970. — DOI: 10.3390/s21216970.
8. Dean J. The Tail at Scale / J. Dean, L.A. Barroso // Communications of the ACM. — 2013. — Vol. 56. — № 2. — P. 74–80. — DOI: 10.1145/2408776.2408794.
9. Harchol-Balter M. Performance Modeling and Design of Computer Systems: Queueing Theory in Action / M. Harchol-Balter. — Cambridge : Cambridge University Press, 2013. — 574 p.
10. Kleinrock L. Queueing Systems / L. Kleinrock. — New York: Wiley, 1975. — Vol. 1. Theory. — 417 p.
11. Demers A. Analysis and Simulation of a Fair Queueing Algorithm / A. Demers, S. Keshav, S. Shenker // Proceedings of ACM SIGCOMM '89. — 1989. — P. 1–12. — DOI: 10.1145/75246.75248.
12. Welsh M. SEDA: An Architecture for Well-Conditioned, Scalable Internet Services / M. Welsh, D. Culler, E. Brewer // Proceedings of the 18th ACM Symposium on Operating Systems Principles. — 2001. — P. 230–243. — DOI: 10.1145/502034.502057.
13. Cho I. Overload Control for μ s-scale RPCs with Breakwater / I. Cho, A. Saeed, J. Fried [et al.] // 14th USENIX Symposium on Operating Systems Design and Implementation. — 2020. — P. 299–314. — URL: <https://www.usenix.org/conference/osdi20/presentation/cho> (accessed: 24.07.2026).
14. Wang Z. Autothrottle: A Practical Bi-Level Approach to Resource Management for SLO-Targeted Microservices / Z. Wang, P. Li, C.-J. M. Liang [et al.] // 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24). — 2024. — P. 149–165. — URL: <https://www.usenix.org/conference/nsdi24/presentation/wang-zibo> (accessed: 28.07.2026).



15. Xing J. Rajomon: Decentralized and Coordinated Overload Control for Latency-Sensitive Microservices / J. Xing, A. Giannoukos, P. Loh [et al.] // 22nd USENIX Symposium on Networked Systems Design and Implementation (NSDI 25). — 2025. — P. 21–36. — URL: <https://www.usenix.org/conference/nsdi25/presentation/xing> (accessed: 28.07.2026).
16. Wang G. Consistency and Completeness: Rethinking Distributed Stream Processing in Apache Kafka / G. Wang, L. Chen, A. Dikshit [et al.] // Proceedings of the 2021 International Conference on Management of Data (SIGMOD '21). — 2021. — P. 2602–2613. — DOI: 10.1145/3448016.3457556.
17. Kreps J. Kafka: A Distributed Messaging System for Log Processing / J. Kreps, N. Narkhede, J. Rao // Proceedings of the NetDB. — 2011. — P. 1–7.
18. Gencer C. Hazelcast Jet: Low-latency Stream Processing at the 99.99th Percentile / C. Gencer, M. Topolnik, V. Ďurina [et al.] // Proceedings of the VLDB Endowment. — 2021. — Vol. 14. — № 12. — P. 3110–3121. — DOI: 10.14778/3476311.3476387.
19. Stouffer K. Guide to Operational Technology (OT) Security / K. Stouffer [et al.]. — NIST SP 800-82 Rev. 3. — Gaithersburg: National Institute of Standards and Technology, 2023. — DOI: 10.6028/NIST.SP.800-82r3.
20. ГОСТ Р 52436-2024. Приборы приемно-контрольные охранные. Классификация. Общие технические требования и методы испытаний. — Москва: Российский институт стандартизации, 2024. — 24 с.
21. Jain R. The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling / R. Jain. — New York: Wiley, 1991. — 685 p.
22. Басан Е.С. Методика выбора эффективных контрмер для повышения отказоустойчивости киберфизических систем / Е.С. Басан, О.И. Силин, М.Г. Фирсова // Вопросы кибербезопасности. — 2025. — № 1 (65). — С. 28–40. — DOI: 10.21681/2311-3456-2025-1-28-40.
23. Мельник Э.В. Онтологический подход к решению задачи перераспределения вычислительной нагрузки в распределенной системе мониторинга с мобильными компонентами на базе распределенного реестра / Э.В. Мельник, И.Б. Сафроненкова, А.Ю. Таранов // Известия Южного федерального университета. Технические науки. — 2023. — № 5. — С. 163–173. — DOI: 10.18522/2311-3103-2023-5-163-173.

Список литературы на английском языке / References in English

1. Kudelkin V.A. Principy sozdaniya integrirovannykh sistem bezopasnosti kriticheski vazhnykh i potencial'no opasnykh ob"ektov [Principles of creating integrated security systems for critical and potentially hazardous facilities] / V.A. Kudelkin, I.M. Yannikov, M.V. Telegina // Intellektual'nye sistemy v proizvodstve [Intelligent Systems in Manufacturing]. — 2017. — Vol. 15. — № 1. — P. 105–109. — DOI: 10.22213/2410-9304-2017-1-105-109. [in Russian].
2. Belkin E.N. Postroenie zashhishhennykh integrirovannykh sistem bezopasnosti ob"ektov UIS [Construction of protected integrated security systems for penal-system facilities] / E.N. Belkin, D.A. Zayonchkovskaya // Informatizatsiya i tehicheskoe obespechenie ugolovno-ispolnitel'noy sistemy Rossijskoj Federacii: problemy, resheniya i perspektivy razvitiya [Informatization and Technical Support of the Penal System of the Russian Federation: Problems, Solutions and Development Prospects]. Proceedings of the 2nd All-Russian Scientific and Practical Conference, Tver, 4–5 October 2023. — Tver: NIIIT FSIN of Russia, 2023. — P. 28–34. — EDN: OHZOJH. — URL: <https://www.elibrary.ru/item.asp?id=60033173> (accessed: 24.07.2026). [in Russian].
3. Kotenko I. Systematic Literature Review of Security Event Correlation Methods / I. Kotenko, D. Gaifulina, I. Zelichenok // IEEE Access. — 2022. — Vol. 10. — P. 43387–43420. — DOI: 10.1109/ACCESS.2022.3168976.
4. Maosa H. A Hierarchical Security Event Correlation Model for Real-Time Threat Detection and Response / H. Maosa, K. Ouazzane, M.C. Ghanem // Network. — 2024. — Vol. 4. — № 1. — P. 68–90. — DOI: 10.3390/network4010004.
5. Seid E. Towards Security Attack Event Monitoring for Cyber Physical-Systems / E. Seid, O. Popov, F. Blix // Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023). — 2023. — P. 723–733. — DOI: 10.5220/0011803400003405.
6. Sukhikh Ya. A. Razrabotka zashhishhennykh arhitektur avtomatizirovannykh sistem upravleniya tehnologicheskimi processami [Development of secure architectures for industrial process control systems] / Ya.A. Sukhikh, D.I. Pravikov, A.A. Kuzichkin // Bezopasnost' informacionnykh tehnologij [IT Security]. — 2020. — Vol. 27. — № 2. — P. 97–117. — DOI: 10.26583/bit.2020.2.08. [in Russian].
7. Fausto A. Toward the Integration of Cyber and Physical Security Monitoring Systems for Critical Infrastructures / A. Fausto, G.B. Gaggero, F. Patrone [et al.] // Sensors. — 2021. — Vol. 21. — № 21. — Art. 6970. — DOI: 10.3390/s21216970.
8. Dean J. The Tail at Scale / J. Dean, L.A. Barroso // Communications of the ACM. — 2013. — Vol. 56. — № 2. — P. 74–80. — DOI: 10.1145/2408776.2408794.
9. Harchol-Balter M. Performance Modeling and Design of Computer Systems: Queueing Theory in Action / M. Harchol-Balter. — Cambridge : Cambridge University Press, 2013. — 574 p.
10. Kleinrock L. Queueing Systems / L. Kleinrock. — New York: Wiley, 1975. — Vol. 1. Theory. — 417 p.
11. Demers A. Analysis and Simulation of a Fair Queueing Algorithm / A. Demers, S. Keshav, S. Shenker // Proceedings of ACM SIGCOMM '89. — 1989. — P. 1–12. — DOI: 10.1145/75246.75248.
12. Welsh M. SEDA: An Architecture for Well-Conditioned, Scalable Internet Services / M. Welsh, D. Culler, E. Brewer // Proceedings of the 18th ACM Symposium on Operating Systems Principles. — 2001. — P. 230–243. — DOI: 10.1145/502034.502057.
13. Cho I. Overload Control for μ s-scale RPCs with Breakwater / I. Cho, A. Saeed, J. Fried [et al.] // 14th USENIX Symposium on Operating Systems Design and Implementation. — 2020. — P. 299–314. — URL: <https://www.usenix.org/conference/osdi20/presentation/cho> (accessed: 24.07.2026).



14. Wang Z. Autothrottle: A Practical Bi-Level Approach to Resource Management for SLO-Targeted Microservices / Z. Wang, P. Li, C.-J. M. Liang [et al.] // 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24). — 2024. — P. 149–165. — URL: <https://www.usenix.org/conference/nsdi24/presentation/wang-zibo> (accessed: 28.07.2026).
15. Xing J. Rajomon: Decentralized and Coordinated Overload Control for Latency-Sensitive Microservices / J. Xing, A. Giannoukos, P. Loh [et al.] // 22nd USENIX Symposium on Networked Systems Design and Implementation (NSDI 25). — 2025. — P. 21–36. — URL: <https://www.usenix.org/conference/nsdi25/presentation/xing> (accessed: 28.07.2026).
16. Wang G. Consistency and Completeness: Rethinking Distributed Stream Processing in Apache Kafka / G. Wang, L. Chen, A. Dikshit [et al.] // Proceedings of the 2021 International Conference on Management of Data (SIGMOD '21). — 2021. — P. 2602–2613. — DOI: 10.1145/3448016.3457556.
17. Kreps J. Kafka: A Distributed Messaging System for Log Processing / J. Kreps, N. Narkhede, J. Rao // Proceedings of the NetDB. — 2011. — P. 1–7.
18. Gencer C. Hazelcast Jet: Low-latency Stream Processing at the 99.99th Percentile / C. Gencer, M. Topolnik, V. Ďurina [et al.] // Proceedings of the VLDB Endowment. — 2021. — Vol. 14. — № 12. — P. 3110–3121. — DOI: 10.14778/3476311.3476387.
19. Stouffer K. Guide to Operational Technology (OT) Security / K. Stouffer [et al.]. — NIST SP 800-82 Rev. 3. — Gaithersburg: National Institute of Standards and Technology, 2023. — DOI: 10.6028/NIST.SP.800-82r3.
20. GOST R 52436-2024. Pribory priemno-kontrol'nye okhrannye. Klassifikatsiya. Obshchie tekhnicheskie trebovaniya i metody ispytaniy [Control panels for use in security application. Grading. General technical requirements and test methods]. — Moscow: Russian Institute for Standardization, 2024. — 24 p. [in Russian]
21. Jain R. The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling / R. Jain. — New York: Wiley, 1991. — 685 p.
22. Basan E.S. Metodika vybora effektivnykh kontrmer dlya povysheniya otkazoustoychivosti kiberfizicheskikh sistem [A methodology for selecting effective countermeasures to improve the fault tolerance of cyber-physical systems] / E.S. Basan, O.I. Silin, M.G. Firsova // Voprosy kiberbezopasnosti [Cybersecurity Issues]. — 2025. — № 1 (65). — P. 28–40. — DOI: 10.21681/2311-3456-2025-1-28-40. [in Russian].
23. Melnik E.V. Ontologicheskii podkhod k resheniyu zadachi pereraspredeleniya vychislitel'noy nagruzki v raspredelennoy sisteme monitoringa s mobil'nymi komponentami na baze raspredelenного reestra [An ontological approach to computational-load redistribution in a distributed monitoring system with mobile components based on a distributed ledger] / E.V. Melnik, I.B. Safronenkova, A.Yu. Taranov // Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki [Proceedings of SFedU. Engineering Sciences]. — 2023. — № 5. — P. 163–173. — DOI: 10.18522/2311-3103-2023-5-163-173. [in Russian].