УДК 004.272:004.413:004.056:004.75
DOI

АРХИТЕКТУРЫ ВЫСОКОНАГРУЖЕННЫХ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Белкин Е. Н. ORCID ID 0009-0007-5848-5433, Кондрашев А. С.

Акционерное общество «АЛГОНТ», Калуга, Российская Федерация,
e-mail: belkinen@algont.ru

Интеграция подсистем физической защиты, контроля доступа, периметровой охраны, пожарной сигнализации и интеллектуального видеонаблюдения на объектах с непрерывным режимом эксплуатации требует архитектуры, которая одновременно масштабируется, сохраняет управляемость и допускает подтверждение требований защиты информации. Цель исследования – сформировать архитектурную модель высоконагруженной комплексной системы безопасности и определить проектные решения, обеспечивающие доставку критических тревог, локальную автономность участков и единое представление состояния объекта. Материалами исследования служат публикации по интегрированным системам безопасности, обработке событий, киберфизическим системам, периферийной видеоаналитике и архитектуре нулевого доверия, а методами – системный анализ, структурное моделирование и формализация метрик нагрузки, задержки, доступности и риска. Предложена событийно-центричная распределенная модель с полевым, локальным вычислительным, адаптерным, событийным, объектно-семантическим, аналитическим, операторским и архивно-аудиторским контурами. Продемонстрировано применение модели к программному комплексу «АССаД-М5» и системе «АССаД-Видео», где ключевыми решениями являются единая семантика зон и оборудования, изоляция адаптеров, приоритетная доставка тревог, резервирование, метаданные видеоаналитики и сквозной аудит. Полученные результаты могут использоваться как архитектурная основа при дополнительной нормативной и стендовой проверке комплексов для объектов атомной отрасли, крупных производств и закрытых административно-территориальных образований.

Ключевые слова: комплексная система безопасности, система физической защиты, высоконагруженная архитектура, событийная обработка, единое информационное пространство, периферийная видеоаналитика, разграничение доступа

ARCHITECTURES OF HIGH-LOAD INTEGRATED SECURITY SYSTEMS

Belkin E. N. ORCID ID 0009-0007-5848-5433, Kondrashev A. S.

Joint Stock Company ALGONT, Kaluga, Russian Federation,
e-mail: belkinen@algont.ru

Integration of physical protection, access control, perimeter protection, fire alarm and intelligent video surveillance subsystems at continuously operated facilities requires an architecture that is simultaneously scalable, manageable and suitable for confirming information-security requirements. The purpose of the study is to develop an architectural model of a high-load integrated security system and to identify design solutions that ensure critical alarm delivery, local autonomy of facility sections and a unified representation of the facility state. The materials are publications on integrated security systems, event processing, cyber-physical systems, edge video analytics and zero trust architecture; the methods are systems analysis, structural modeling and formalization of load, latency, availability and risk metrics. An event-centric distributed model is proposed with field, local computing, adapter, event, object-semantic, analytical, operator and archival-audit domains. The model is applied to the ASSAD-M5 software complex and the ASSAD-Video system, in which the key solutions are unified semantics of zones and equipment, adapter isolation, priority alarm delivery, redundancy, video-analytics metadata and end-to-end audit. The results may be used as an architectural basis, subject to additional regulatory and bench verification, for security complexes at nuclear-industry facilities, large industrial sites and closed administrative-territorial entities.

Keywords: integrated security system, physical protection system, high-load architecture, event-driven processing, unified information space, edge video analytics, access control

Введение

Комплексные системы безопасности крупных промышленных и государственных объектов уже не могут рассматриваться как набор независимых подсистем. В одном контуре требуется связать контроль доступа, людские и транспортные контрольно-пропускные пункты, периметровую охрану, охранно-пожарную сигнализацию, видеонаблюдение, нейросетевую аналитику, архивы, рабочие места операторов, регламенты реагирования и средства защиты информации. Для объектов атомной отрасли, закрытых административно-территориальных образований и критической инфраструктуры такая интеграция определяет устойчивость эксплуатации: оператор должен видеть состояние защищенности объекта целиком, а автоматические сценарии должны работать с согласованной картиной зон, прав, событий и исполнительных устройств.

В настоящей статье высоконагруженной комплексной системой безопасности считается распределенный программно-технический комплекс, в котором число субъектов доступа достигает $U \geq 10^5$, число технических средств $D \geq 10^4$, число видеопотоков $C \geq 10^3$, объект разделен на множество зон Z с различными режимами, эксплуатация ведется непрерывно, критические тревоги должны доставляться за ограниченное время, а отказ центрального сегмента не должен отменять локально необходимые функции защиты. Пороговые значения U, D и C не являются нормативными; они используются как эмпирические границы класса задач, сформированные по проектному опыту авторов и параметрам стендовой модели. При таких порядках величин централизованная опросно-шлюзовая интеграция становится узким местом по очередям, архиву и операторскому контексту, а распределенная событийная обработка и локальная автономность становятся архитектурными требованиями.

Исследования интегрированных систем безопасности показывают необходимость структурного объединения подсистем, формализации состояния защищенности и обработки разнородных данных [1; 2]. Работы по сбору и корреляции событий безопасности подтверждают, что простая централизация журналов не обеспечивает своевременную реакцию без нормализации событий, выделения критических потоков и управляемого хранения [3-5]. Исследования защищенных архитектур автоматизированного управления и единого информационного пространства дополняют этот вывод требованиями к сервисному разделению, ролевой модели и единому представлению данных [6-8].

Формализация производительности, очередей и рискориентированной оценки опирается на методы экспериментального анализа компьютерных систем, моделирования очередей и количественного определения риска [9-11]. Работы по высоконагруженным приложениям и микросервисно-событийным архитектурам показывают, что масштабирование вычислительных узлов требует не только декомпозиции сервисов, но и управляемых потоков событий [12-14]. Зарубежные публикации по периферийной видеоаналитике и интеграции физического и кибермониторинга приходят к близкому выводу: крупный объект требует распределенной обработки, локальной автономности и отказоустойчивых контуров [15; 16]. Архитектура нулевого доверия усиливает этот вывод требованием постоянной проверки субъекта, устройства, контекста и действия [17; 18].

Проблема исследования состоит в том, что типовые комплексы безопасности часто остаются монолитными или механически интегрированными. Монолитная схема упрощает первичное внедрение, но плохо масштабируется при росте числа датчиков, камер, пользователей и сценариев. Интеграция через набор шлюзов сохраняет острова данных и затрудняет подтверждение защищенности. В таких условиях сложно обеспечить контролируемое время прохождения тревоги, обновление оборудования без нарушения доверенного ядра и единый контекст для оператора.

Цель исследования – предложить архитектуру высоконагруженной комплексной системы безопасности и продемонстрировать ее промышленную реализацию на примере программного комплекса «АССаД-М5» и системы «АССаД-Видео» разработки Акционерного общества «АЛГОНТ». Для достижения цели решаются задачи: выделить контуры распределенной архитектуры, описать каноническую модель события, уточнить методику измерения нагрузки и задержки, определить критерии доступности и риска, сопоставить модель с альтернативными подходами и сформулировать ограничения применимости.

Материалы и методы исследования

Материалом исследования послужили научные публикации по интегрированным системам безопасности, обработке событий, защищенным архитектурам управления, моделированию производительности компьютерных систем, периферийной видеоаналитике, событийно ориентированным микросервисам, модели нулевого доверия, физической защите и нормативному обеспечению критической инфраструктуры. Источники отбирались по тематическому соответствию задаче построения распределенных программно-технических комплексов безопасности; в библиографическое ядро включены проверяемые публикации с DOI, ISBN или ссылками на страницы первоисточников.

Методологическую основу составили системный анализ, структурное моделирование, декомпозиция на контуры ответственности и формализация проектных метрик. К общеизвестным практикам, использованным в работе, относятся адаптерный слой, событийные очереди, периферийная обработка видео, резервирование и разграничение доступа. Собственные архитектурные решения авторов состоят в их совместной композиции для системы физической защиты: объектно-событийное ядро, единая семантика зон и оборудования, изоляция

адаптеров от доверенного ядра, приоритетная доставка тревог, метаданные видеоаналитики и сквозная трассировка инцидента.

Эмпирическая часть выполнена как архитектурный кейс-анализ и нормированная имитационно-стендовая апробация пилотного контура. Публикуются относительные метрики; абсолютные параметры объекта не раскрываются. Стенд включал сервер событийного ядра и БД/архива, узел имитаторов адаптеров, сервер видеометаданных, два АРМ и локальный сервер времени. Модель задавала 48 зон, 12 КПП, 384 точки доступа, 512 охранно-периметровых сигналов, 256 видеоканалов и 28 тревожных сценариев.

Нагрузка формировалась 60-минутным обезличенным журналом; выполнялось 20 парных прогонов, первые 10 мин. исключались, поэтому для анализа использовались 50 мин. каждого прогона. Для событий фиксировались ID, источник, зона, тип, критичность и метки обнаружения, передачи, нормализации, корреляции, записи и отображения на АРМ. Узлы синхронизировались локальным NTP; исключались записи с неполными метками и расхождением времени более 100 мс, доля исключенных записей не превышала 1,3%. Сравнивались общая очередь и схема с приоритетным тревожным каналом; статистическая обработка включала медиану, среднее, σ, IQR, 95%-ный доверительный интервал и парный критерий Уилкоксона при α = 0,05.

Результаты исследования и их обсуждение

Результатом исследования является модель распределенной сертифицируемой архитектуры, где объектная семантика, событийная доставка, локальная автономность и аудит проектируются как единое целое. В такой модели событие безопасности инициирует корреляцию, уведомления, блокировки, переключения режимов доступа, вывод видеоподтверждения и формирование доказательной базы. Для воспроизводимости результата сначала фиксируются метрики события, маршрута тревоги и рискреакции, затем описываются контуры архитектуры, а промышленная реализация и стендовая апробация приводятся после теоретической части.

Формализация метрик нагрузки и задержки

Формализация носит прикладной характер: структура события и потоков использует подходы событийной обработки и event-driven architecture [3; 4; 14]. Ограничение емкости узлов и контроль хвостовой задержки опираются на методы экспериментального анализа производительности и моделирования очередей компьютерных систем [9; 10].

Событие безопасности задается кортежем:

$$e = \langle id, t, src, z, type, payload, sev, trust, acl, seq \rangle \tag{1}$$

где *id* – идентификатор; *t* – время; *src* – источник; *z* – зона объекта; *type* – тип события; *payload* – атрибуты; *sev* – критичность; *trust* – оценка доверия к источнику и каналу; *acl* – ограничения доступа; *seq* – монотонный номер для восстановления порядка. Поля критичности, доверия и прав доступа позволяют обрабатывать событие как управляемый объект, а не как простую строку журнала.

Суммарная интенсивность входного потока определяется выражением:

$$\lambda_{\Sigma} = \sum_{d \in D} \lambda_d + \sum_{c \in C} \left(\lambda_c^{meta} + \lambda_c^{alarm} \right) + \lambda_u + \lambda_{svc}, \tag{2}$$

где λ_d – поток событий от технического средства; λ_c^{meta} – поток видеометаданных; λ_c^{alarm} – поток тревог видеоаналитики; λ_u – действия пользователей; λ_{svc} – служебные события диагностики. Эти параметры измеряются по нормализованным журналам в заданном окне Δ, а для проектирования узлов обработки используется ограничение:

$$m_i \geq \mathrm{ceil}\left(\frac{\lambda_i}{\rho_i \mu_i} \right), \; 0 < \rho_i < 1, \tag{3}$$

где m_i – число узлов *i*-го контура, μ_i – измеренная производительность одного узла при воспроизведении тестового журнала, ρ_i – допустимая загрузка с учетом резерва. Для критических тревог ρ_i целесообразно ограничивать диапазоном 0,5–0,7, чтобы сохранить емкость для всплесков, отказов и переключений; μ_i определяется не паспортной характеристикой сервера, а результатом нагрузочного воспроизведения типового набора событий с контро-

лем p95/p99 задержки (значения, не превышаемые в 95% и 99% измеренных случаев). Задержка тревожного события раскладывается на составляющие:

$$T_{alarm} = T_{det} + T_{edge} + T_{net} + T_{norm} + T_{corr} + T_{store} + T_{ui} \ , \quad (4)$$

где T_{det} – обнаружение на датчике или в видеоаналитике; T_{edge} – локальная обработка; T_{net} – передача; T_{norm} – нормализация; T_{corr} – корреляция; T_{store} – фиксация в журнале; T_{ui} – отображение или передача в сценарий реагирования. Измерения исключают события с нарушением синхронизации времени выше заданного порога, поскольку такие события искажают разложение задержки. В «АССаД-М5» проектным ориентиром является доставка критических тревог на рабочие места и в сценарии реагирования в пределах единиц секунд, а для наиболее критичных контуров – целевое время порядка одной секунды при штатной работе сети и вычислительных узлов. Это достигается не только вычислительной мощностью, но и приоритетными очередями, локальной фильтрацией, резервированием маршрутов и отказом от передачи лишних данных в критический контур. Для устойчивой доставки требуется резервировать не только сервер, но и контроллеры, коммутаторы, линии связи, сервисы событийного ядра и процедуры восстановления.

Архитектурная модель и контуры ответственности

Предлагаемая модель представляет комплекс безопасности как федерацию контуров, объединенных событийным ядром и единой объектной моделью. В состав входят полевой контур технических средств, локальный вычислительный контур, адаптерный слой, событийное ядро, объектно-семантическое хранилище, контур правил и корреляции, видеоконтур, операторский контур, архивно-аудиторский контур и контур администрирования обновлений. Обобщенная схема представлена на рисунке.

Полевой контур включает точки доступа, турникеты, шлюзы, контроллеры дверей, датчики периметра, охранные и пожарные извещатели, камеры и исполнительные устройства. Локальный контур выполняет первичную обработку и поддерживает критические функции при потере связи с центром. Адаптеры преобразуют протоколы и модели состояний оборудования в каноническое событие с меткой времени, источником, зоной, качеством сигнала, критичностью и правами доступа. Видеоконтур передает в событийное ядро не полный поток, а метаданные: камеру, зону, координаты, вероятность, ссылку на архив и критичность; это согласуется с работами по периферийной видеоаналитике [15; 19]. В таблице 1 дано сравнение архитектурных подходов.

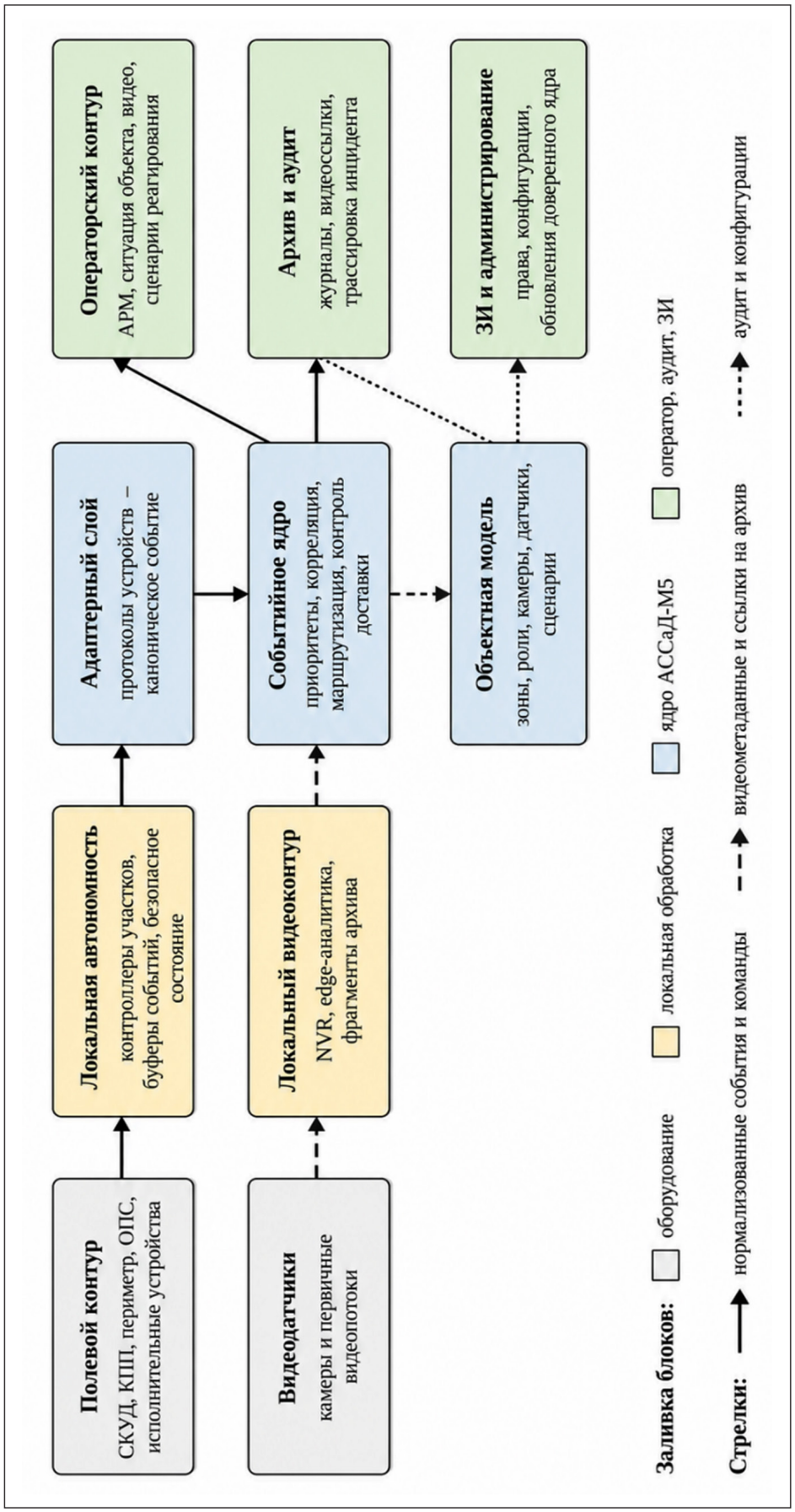
Ограничениями модели являются зависимость качества риск-оценки от корректности объектной модели, необходимость синхронизации времени, валидации адаптеров и регулярной проверки сценариев реагирования. Модель оптимальна для режимных объектов с большим числом технических средств, длительным сроком службы и требованиями к непрерывной эксплуатации; для малых объектов без развитой зональной структуры она может быть избыточной.

Таблица 1

Сравнение архитектурных подходов для комплексных систем безопасности

Подход	Преимущества	Ограничения	Область применения
Монолитная система	простое первичное внедрение, единая поставка	сложное масштабирование, риск единой точки отказа	небольшие объекты со стабильным составом оборудования
Набор шлюзов и подсистем	быстрое подключение разнородных устройств	острова данных, слабая корреляция, фрагментарный аудит	модернизация без жестких требований к единой реакции
Микросервисная EDA	масштабирование сервисов	нет семантики зон и регламентов физической защиты	информационные системы и мониторинг
Авторская модель	единая семантика, приоритет тревог, автономность, сквозной аудит	требует модели объекта, синхронизации времени, дисциплины конфигурации	режимные и долгоживущие объекты

Примечание: составлено авторами по результатам данного исследования.



Обобщенная архитектура высоконагруженного комплекса безопасности в логике комплекса «АССаД-М5» и системы «АССаД-Видео»
Примечание: составлено авторами по результатам данного исследования

Архитектурные решения для масштабирования и доверия

Единое информационное пространство хранит режимные связи объекта: зоны, двери, камеры, датчики, роли, сценарии и допустимые действия в штатном, тревожном или ограничительном режиме. Событийная архитектура заменяет периодический опрос управляемым потоком нормализованных сообщений, где тревоги периметра, пожарные события, несанкционированный доступ и отказ критического контроллера имеют иной режим доставки, чем статистика и диагностика. Локальная автономность снижает зависимость безопасности от центральной сети: удаленный участок периметра или пункт пропуска сохраняет режимы доступа, фиксацию событий и безопасное состояние при деградации связи. Для объектов высокой категории ответственности это согласуется с оценкой эффективности физической защиты и принципами устойчивых промышленных киберфизических систем [20; 21].

Модель нулевого доверия переносится из чисто информационной безопасности в физический контур: команда оператора, просмотр видеозаписи, изменение режима двери или обновление адаптера проверяются по роли, рабочему месту, зоне ответственности, времени, уровню допуска и состоянию объекта. Такая трактовка соответствует работам по zero trust для киберфизических систем [22]. Архивно-аудиторский контур фиксирует исходное событие, нормализацию, корреляцию, автоматический сценарий, действия оператора, переключение режимов, видеоссылки и закрытие тревоги, что обеспечивает воспроизводимую цепочку расследования; сходные требования к интегрированному удаленному управлению и защите критической инфраструктуры отмечаются в [23].

Рискориентированная реакция

Оперативная реакция на крупном объекте не может сводиться к правилу «датчик сработал – вывести тревогу»: часть событий вторична, часть требует подтверждения, часть зависит от режима объекта. Поэтому архитектура должна включать рискориентированную модель; используемая форма адаптирует классическое представление риска через сценарии, вероятности и последствия [11] к объектной модели системы физической защиты [20]:

$$R_z(t) = \sum_s C_s(z) \cdot P_s(t \mid E_{1:t}, M_z), \quad (5)$$

где $R_z(t)$ – риск для зоны z в момент t; $C_s(z)$ – ущерб сценария s; P_s – вероятность сценария с учетом событий $E_{1:t}$ и модели зоны M_z. Выбор действия задается как:

$$a_{opt} = \arg\min_{a \in A} \left\{ E\left[L(z,s,a) \mid E_{1:t} \right] + \mathrm{Cost}(a) \right\}, \quad (6)$$

где a_{opt} – оптимальное действие; a – возможное действие; A – множество допустимых действий; arg min – выбор действия с минимальным значением; z – зона объекта; s – сценарий события; $L(z,s,a)$ – потери при действии а; $E_{1:t}$ – накопленные к моменту t события; E – ожидаемые потери; $\mathrm{Cost}(a)$ – стоимость реакции.

Значения ущерба и потерь задаются экспертно-регламентной шкалой для зоны и сценария; вероятность сценария рассчитывается по накопленным событиям, модели зоны, критичности, доверию к источнику и текущему режиму объекта. Риск-модель используется для ранжирования сценариев и выбора допустимого действия в рамках утвержденного регламента.

Промышленная реализация и стендовая апробация

В промышленной реализации «АССаД-М5» выполняет роль ядра интеграции и управления системой физической защиты: объединяет технические средства безопасности и жизнеобеспечения, обеспечивает единый интерфейс оператора, правила доступа, журналирование и поддержку резервирования. События от пунктов пропуска, точек доступа, периметра, охранно-пожарной сигнализации, видеоконтуров и служебных средств нормализуются адаптерами и связываются с объектной семантикой.

Ключевые решения «АССаД-М5» включают объектно-событийное ядро, сертифицируемую адаптерную архитектуру, локальную работоспособность при отказе центрального сегмента, приоритетную доставку тревог и сквозной аудит. Адаптер отвечает за протокол и диагностику, но не обходит модель доступа, журналирование и правила критических сценариев; оператор получает событие, видеоподтверждение, состояние зоны и рекомендованный сценарий в одном интерфейсе.

Система «АССаД-Видео» обеспечивает масштабируемое видеонаблюдение и формирует для «АССаД-М5» высокоуровневые события.

Таблица 2

Нормированные результаты пилотной апробации

Показатель	Метод измерения	Базовая схема	Событийно-центричная модель
P95 задержки тревоги	метки источник-АРМ; 20 прогонов	1,00	Me 0,50; M 0,51; IQR 0,46–0,55; 95% ДИ 0,48–0,54; p < 0,01
P99 при всплеске фона	двукратный фон, Δ = 60 с; 20 прогонов	1,00	Me 0,63; M 0,64; σ 0,05; IQR 0,60–0,68; 95% ДИ 0,61–0,66; p < 0,01
Локальная автономность	отключение центра на 10 мин.	часть функций зависит от центра	режимы доступа и журнал сохраняются локально
Полнота аудита	цепочка «источник-корреляция-АРМ-архив»	фрагменты в разных журналах	цепочка восстанавливается сквозным идентификатором

Примечание: составлено авторами по результатам данного исследования.

В апробации видеоаналитика рассматривалась как источник метаданных для событийного ядра, а не как самостоятельное доказательство качества нейросетевой модели. Контрольная подвыборка включала IP-камеры 2 Мп, 25 кадр/с, ракурсы КПП, периметра и внутренней зоны при освещенности 80–500 лк в помещениях и 30–1000 лк на улице. Для классов «человек», «транспорт», «пересечение линии» и «оставленный предмет» при пороге вероятности 0,75 получены: precision 0,89–0,94, recall 0,82–0,88, F1 0,85–0,91, ложные тревоги 6–11% от переданных видеособытий. Сильная засветка, плотные осадки, полное перекрытие объекта и нестабильная камера являются ограничениями модели.

Стендовая апробация использовала один набор сценариев для двух схем. В базовой схеме события технических средств, видеометаданные, действия пользователей и диагностика поступали в общую очередь; в событийно-центричной схеме тревожный поток выделялся в приоритетный канал, фоновые события агрегировались локально, а маршрутизация выполнялась по зоне и типу сценария. Оценивались p95 задержки тревоги, p99 при всплеске фона, сохранение локальных функций при деградации связи и полнота аудита.

Таблица 2 показывает не абсолютную производительность объекта, а эффект архитектуры в одинаковых условиях стенда. Распределения задержек имели правосторонний хвост, поэтому вместе со средним и медианой использовались p95 и p99. Приоритетный канал и локальная фильтрация снизили p95 до медианы 0,50 от базового уровня; при двукратном фоне p99 составил медиану 0,63 от базового уровня. По 20 парным прогонам различия между базовой и событийно-центричной схемой значимы по критерию Уилкоксона ($p < 0,01$). Для повторения проверки фиксируются версии стенда, сценарии нагрузки, порог синхронизации и правила исключения записей.

Применимость подхода к объектам атомной отрасли и критической информационной инфраструктуры не подменяет нормативную оценку: требования к безопасности КИИ и защищенности значимых объектов КИИ задаются 187-ФЗ и Приказом ФСТЭК России № 239 [24; 25], а требования к физической защите ядерных материалов, ядерных установок и пунктов хранения – Постановлением Правительства РФ № 456 и НП-083-23 [26; 27]. Поэтому модель следует сопоставлять с категорией объекта, моделью угроз, актом классификации, техническим заданием и результатами стендовой проверки.

По данным Государственного реестра сертифицированных средств защиты информации ФСТЭК России и публичных карточек сертификатов, для «АССаД-Видео» указывается соответствие требованиям доверия по третьему уровню и требованиям руководящего документа по автоматизированным системам физической защиты по первому классу [28]. Сертификационные материалы приведены как пример промышленной апробации, а не как доказательство универсальности модели. Свойства архитектуры, в т.ч. малое доверенное ядро, изоляция адаптеров, управляемость конфигурации и сквозной аудит рассматриваются как архитектурные предпосылки сертифицируемости.

Новизна подхода состоит в совместном проектировании физической безопасности, видеонаблюдения, событийной обработки и защиты информации в одной киберфизической архитектуре. Новые результаты включают объектно-событийное ядро, сер-

тифицируемую подключаемую архитектуру, модель видеометаданных, федерацию локальных контуров и формализацию проектных метрик нагрузки, задержки, доступности и риска.

Заключение

Высоконагруженная комплексная система безопасности для атомной отрасли, крупных производств, закрытых административно-территориальных образований и иной критической инфраструктуры должна проектироваться как распределенная сертифицируемая киберфизическая система. Ее устойчивость определяется согласованной работой объектной модели, событийного ядра, локальной автономности, приоритетной доставки тревог, видеометаданных, резервирования, разграничения доступа, регламентированных обновлений и сквозного аудита.

Предложенная модель объединяет полевой, локальный вычислительный, адаптерный, событийный, объектно-семантический, аналитический, операторский и архивно-аудиторский контуры. Метрики интенсивности событий, задержки тревоги, доступности маршрута и риска могут использоваться как архитектурная основа при дополнительной нормативной и стендовой проверке, а кейс «АССаД-М5» и «АССаД-Видео» демонстрирует реализуемость модели, но не подменяет экспертизу конкретного объекта. Дальнейшее развитие связано с формальной верификацией сценариев, цифровыми двойниками объекта и расширением моделей доверия.

Список литературы

1. Куделькин В. А., Янников И. М., Телегина М. В. Принципы создания интегрированных систем безопасности критически важных и потенциально опасных объектов // Интеллектуальные системы в производстве. 2017. Т. 15. № 1. С. 105–109. DOI: 10.22213/2410-9304-2017-1-105-109.

2. Куделькин В. А., Янников И. М., Габричидзе Т. Г. Особенности обработки данных в интеллектуальной интегрированной системе безопасности объектов и территорий // Интеллектуальные системы в производстве. 2017. Т. 15. № 4. С. 94–101. DOI: 10.22213/2410-9304-2017-4-94-101.

3. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34. DOI: 10.15622/sp.54.1.

4. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. № 4 (47). С. 5–27. DOI: 10.15622/sp.47.1.

5. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия // Безопасность информационных технологий. 2018. Т. 25. № 4. С. 42–51. DOI: 10.26583/bit.2018.4.04.

6. Сухих Я. А., Правиков Д. И., Кузичкин А. А. Разработка защищенных архитектур автоматизированных систем управления технологическими процессами // Безопасность информационных технологий. 2020. Т. 27. № 2. С. 97–117. DOI: 10.26583/bit.2020.2.08.

7. Буйневич М. В., Ложкина О. В., Ярошенко А. Ю. Архитектурные модели комплексной и интегрированной безопасности информационных систем: сравнительный анализ подходов // Вестник Санкт-Петербургского университета ГПС МЧС России. 2021. № 1. С. 100–108. URL: https://cyberleninka.ru/article/n/arhitekturnye-modeli-kompleksnoy-i-integrirovannoy-bezopasnosti-informatsionnyh-sistem-sravnitelnyy-analiz-podhodov (дата обращения: 30.05.2026).

8. Мещеряков Р. В., Жуковский О. И., Сенченко П. В., Гриценко Ю. Б., Милихин М. М. Особенности архитектуры единого информационного пространства при управлении сложными технологическими процессами // Доклады ТУСУР. 2017. Т. 20. № 4. С. 75–81. DOI: 10.21293/1818-0442-2017-20-4-75-81.

9. Jain R. The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling. New York: Wiley, 1991. 720 p. URL: https://www.wiley.com/en-mx/search?pq=9780471503361 (дата обращения: 16.06.2026). ISBN: 978-0-471-50336-1.

10. Harchol-Balter M. Performance Modeling and Design of Computer Systems: Queueing Theory in Action. Cambridge: Cambridge University Press, 2013. 574 p. URL: https://www.cambridge.org/9781107027503 (дата обращения: 16.06.2026). ISBN: 978-1-107-02750-3.

11. Kaplan S., Garrick B. J. On the Quantitative Definition of Risk // Risk Analysis. 1981. Vol. 1. No. 1. P. 11–27. DOI: 10.1111/j.1539-6924.1981.tb01350.x.

12. Филисов Д. А. Архитектура высоконагруженных приложений // Universum: технические науки. 2023. №10-1(115).С.49–53.DOI:10.32743/UniTech.2023.115.10.16138.

13. Карпович М. Н. Особенности проектирования микросервисно-событийных архитектур для высоконагруженных распределенных систем обработки информации // Труды БГТУ. Серия 3: Физико-математические науки и информатика. 2023. № 1 (266). С. 89–95. DOI: 10.52065/2520-6141-2023-266-1-15.

14. Rahmatulloh A., Nugraha F., Gunawan R., Darmawan I. Event-Driven Architecture to Improve Performance and Scalability in Microservices-Based Systems // Proceedings of the 2022 International Conference Advancement in Data Science, E-learning and Information Systems. IEEE. 2022. P. 1–6. DOI: 10.1109/ICADEIS56544.2022.10037390.

15. Xu R., Razavi S., Zheng R. Edge Video Analytics: A Survey on Applications, Systems and Enabling Techniques // IEEE Communications Surveys & Tutorials. 2023. DOI: 10.1109/COMST.2023.3323091.

16. Fausto A., Gaggero G. B., Patrone F., Girdinio P. Marchese M. Toward the Integration of Cyber and Physical Security Monitoring Systems for Critical Infrastructures // Sensors. 2021. Vol. 21. № 21. Article 6970. DOI: 10.3390/s21216970.

17. Syed N. F., Shah S. W., Shaghaghi A., Anwar A., Baig Z., Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey // IEEE Access. 2022. Vol. 10. P. 57143–57179. DOI: 10.1109/ACCESS.2022.3174679.

18. He Y., Huang D., Chen L., Ni Y., Ma X. A Survey on Zero Trust Architecture: Challenges and Future Trends // Wireless Communications and Mobile Computing. 2022. Article ID 6476274. DOI: 10.1155/2022/6476274.

19. Rossi F., Saponara S. Edge HPC Architectures for AI-Based Video Surveillance Applications // Electronics. 2024. Vol. 13. № 9. Article 1757. DOI: 10.3390/electronics13091757.

20. El Wely I. C., Chetaine A. Analysis of Physical Protection System Effectiveness of Nuclear Power Plants Based on Performance Approach // Annals of Nuclear Energy. 2021. Vol. 152. Article 107980. DOI: 10.1016/j.anucene.2020.107980.

21. Alves J., Sousa P., Cruz T. J., Mendes J. A. Review of Architecture Features for Distributed and Resilient Industrial Cyber-Physical Systems // Journal of Manufacturing Systems. 2025. Vol. 82. P. 1069–1090. DOI: 10.1016/j.jmsy.2025.07.012.

22. Hasan S., Amundson I., Hardin D. Zero-Trust Design and Assurance Patterns for Cyber-Physical Systems // Journal of Systems Architecture. 2024. Vol. 155. Article 103261. DOI: 10.1016/j.sysarc.2024.103261.

23. Isern J., Jimenez-Perera G., Medina-Valdes L., Chaves P., Pampliega D., Ramos F., Barranco F. A Cyber-Physical System for Integrated Remote Control and Protection of Smart Grid Critical Infrastructures // Journal of Signal Processing Systems. 2023. Vol. 95. P. 1127–1140. DOI: 10.1007/s11265-023-01842-2.

24. Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. URL: https://publication.pravo.gov.ru/document/view/0001201707260023 (дата обращения: 28.06.2026).

25. Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_294287/ (дата обращения: 28.06.2026).

26. Постановление Правительства РФ № 456 от 19.07.2007 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» // Правительство России. URL: https://government.ru/docs/all/60604/ (дата обращения: 28.06.2026).

27. НП-083-23. Требования к физической защите ядерных материалов, ядерных установок и пунктов хранения ядерных материалов // Библиотека ЯРБ. URL: https://nrs-journal.ru/sections/official_documents/NP-083-23_112/ (дата обращения: 28.06.2026).

28. Сертификат № 4472. СПО системы видеонаблюдения «АССаД-Видео» // Государственный реестр сертифицированных средств защиты информации ФСТЭК России. URL: https://reestr.fstec.ru/reg3; публичная карточка: https://service.securitm.ru/source/szi/show/4472 (дата обращения: 28.06.2026).

Конфликт интересов: Авторы заявляют о наличии следующего конфликта интересов: авторы являются представителями организации-разработчика рассматриваемых систем. Данное обстоятельство раскрыто в рукописи; выводы статьи основаны на архитектурном анализе, формализованных проектных метриках и опубликованных научных источниках.

Conflict of interest: The authors declare the following conflict of interest: the authors are representatives of the organization that develops the systems considered in the paper. This circumstance is disclosed in the manuscript; the conclusions are based on architectural analysis, formalized design metrics and published scientific sources.

Финансирование: Авторы заявляют об отсутствии внешнего финансирования.

Financing: The research was performed without external funding.