Information about the authors

Manas Yergesh* – PhD doctoral student, Department of Artificial Intelligence Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: Shymkent90@mail.ru. ORCID: https://orcid.org/0000-0002-2180-293X.

Banu Yergesh – PhD, deputy director of the Department of Digital Development, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: b.yergesh@gmail.com. ORCID: https://orcid.org/0000-0002-8967-2625.

Ainur Orazayeva – K. Kulazhanov Kazakh University of Technology and Business, Department of Information Technology, Head of the Department, Astana, Kazakhstan; e-mail: oar_is@mail.com. ORCID: https://orcid.org/0000-0002-2899-9886.

Amangul Talgat – K. Kulazhanov Kazakh University of Technology and Business, Department of Information Technology, Head of the Department, Astana, Kazakhstan; e-mail: amangul_talgat81@mail.ru. ORCID: https://orcid.org/0000-0002-5800-9134.

Поступила в редакцию 28.01.2026
Поступила после доработки 22.02.2026
Принята к публикации 23.02.2026

https://doi.org/10.53360/2788-7995-2026-1(21)-15

МРНТИ: 28.23.15

Б.С. Сарсенов*, Д. Жамангарин
[1]Евразийский национальный университет имени Л.Н. Гумилева,
010000, Республика Казахстан, г. Астана, ул. Александра Пушкина, 11
*e-mail: batyr.sarsenov@gmail.com

ОПТИМИЗАЦИЯ ПРОЦЕССОВ КОНТРОЛЯ И УПРАВЛЕНИЯ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ КОНГРЕСС-ХОЛЛА «АУЛИЕ-АТА»

Аннотация: *В статье рассматривается задача повышения эффективности и надёжности процессов контроля и управления в системе контроля и управления доступом (СКУД) на примере объекта общественного назначения – Конгресс-Холла «Аулие-Ата». Выполнен обзор типовых архитектур СКУД и нормативных требований к информационной безопасности и инженерным системам безопасности. Показано, что на объектах с высокой плотностью посетителей и смешанными сценариями доступа (сотрудники, подрядчики, гости, массовые мероприятия) ключевыми проблемами являются задержки принятия решений, несогласованность правил, недостаточная интеграция с видеонаблюдением и пожарной автоматикой, а также ограниченная аналитика событий. Предложен комплекс оптимизационных мер: переход к событийно-ориентированной обработке (event-driven), разгрузка сервера за счёт локальных контроллеров и кэширования правил, применение гибридной модели управления доступом RBAC+ABAC с адаптивной оценкой риска, унификация журналирования и интеграция через API/шину сообщений с СВН, ОПС и системами учёта. Сформулирован алгоритм обработки события доступа и представлена структурная схема интеграций. Эффективность решений оценивалась моделированием потоков запросов и сравнением с базовым вариантом: достигнуто снижение среднего времени обработки события на 25-35%, уменьшение доли отказов из-за «таймаутов» и повышение полноты протоколирования инцидентов. Результаты могут быть использованы при проектировании и модернизации СКУД объектов массового пребывания людей.*

Ключевые слова: *СКУД; контроль доступа; оптимизация; RBAC; ABAC; оценка риска; интеграция; event-driven; аудит.*

Введение

Безопасность объектов массового пребывания людей определяется не только физической защищённостью периметра, но и качеством процессов управления доступом: насколько быстро и корректно система распознаёт субъект доступа, сопоставляет его права и контекст (время, зона, режим работы), принимает решение и фиксирует событие для

последующего анализа. Конгресс-холлы, театры, административные центры и крупные учебные корпуса характеризуются высокой вариативностью сценариев: в течение дня проходят смены персонала, одновременно перемещаются посетители, действуют временные пропуска подрядчиков, а при проведении мероприятий нагрузка на СКУД кратно возрастает.

Практика эксплуатации показывает, что при росте числа точек прохода и пользователей «узким местом» становится не только аппаратная часть (турникеты, замки, считыватели), но и логика управления: согласованность правил доступа, скорость обработки событий, устойчивость к сбоям сети, корректная реакция на пожарные режимы и интеграция с видеонаблюдением. При недостаточной оптимизации возможны задержки на проходных, накопление очередей, повышение конфликтных ситуаций, а также снижение контролируемости инцидентов из-за неполного логирования и разрозненности журналов.

Цель настоящей работы – разработать и обосновать набор методов оптимизации процессов контроля и управления в СКУД объекта общественного назначения (на примере Конгресс-Холла «Аулие-Ата»), обеспечив сокращение времени принятия решения по событию доступа, повышение надёжности и улучшение качества протоколирования. Для достижения цели поставлены задачи: (1) выполнить обзор существующих решений и подходов к управлению доступом; (2) проанализировать типовую архитектуру СКУД и выявить проблемные места при высокой нагрузке; (3) предложить архитектурные и алгоритмические меры оптимизации; (4) представить структурную схему и алгоритм обработки событий; (5) оценить ожидаемый эффект по ключевым метрикам.

Научная новизна работы заключается в применении комбинированной модели управления доступом RBAC+ABAC с адаптивной оценкой риска и событийно-ориентированной обработкой данных (event-driven) для объектов с переменной нагрузкой. Практическая значимость – в возможности использования предложенных решений при проектировании, модернизации и эксплуатации СКУД, а также при интеграции СКУД с СВН, ОПС/АПТ и системами учёта.

Обзор существующих решений и проблематика

Типовые архитектуры СКУД и модели управления доступом

Современные СКУД в общем виде включают идентификаторы (карты, брелоки, мобильные токены), считыватели, контроллеры, исполнительные устройства (замки, турникеты), серверное программное обеспечение и базу данных событий. Архитектура может быть централизованной (решение принимается на сервере) или распределённой (контроллер принимает решение локально, сервер выполняет администрирование и анализ). Для объектов с жёсткими требованиями к непрерывности доступа чаще предпочтительны распределённые схемы, так как они сохраняют работоспособность при временных проблемах сети.

С точки зрения логики доступа широко применяются следующие модели: дискреционная (DAC), мандатная (MAC), ролевая (RBAC) и атрибутная (ABAC). В инженерных СКУД наиболее распространён RBAC: права задаются через роли (например, «охрана», «администратор», «персонал», «гость»). Достоинство RBAC – простота администрирования, недостаток – слабая гибкость при сложных контекстных условиях (время, маршрут, загрузка, особые режимы). ABAC описывает права через набор атрибутов субъекта, объекта и окружения (временной интервал, зона, тип события, уровень риска), поэтому лучше подходит для объектов с динамическими сценариями, однако требует более аккуратной формализации правил и контроля конфликтов.

В зарубежной и отечественной литературе подчёркивается, что переход от чистого RBAC к гибридным схемам RBAC+ABAC позволяет одновременно удержать удобство администрирования и получить гибкость политик [1-3]. Отдельное направление исследований связано с риск-ориентированным доступом (risk-adaptive access control), когда решение зависит от оценки риска в текущем контексте (например, аномальная активность, нехарактерное время, попытки подбора пропуска) [4].

Результаты работ других авторов и выявляемые узкие места

При проектировании СКУД для крупных объектов ключевым становится вопрос производительности: система должна выдерживать пики нагрузки, сохраняя предсказуемое время реакции. Исследования, основанные на моделях массового обслуживания и экспериментах с журнальными данными, показывают, что рост задержек чаще всего обусловлен последовательной обработкой событий на сервере, блокировками при записи в

базу данных и «тяжёлыми» интеграционными вызовами к внешним подсистемам [5-6]. В ряде работ предлагается переход к асинхронной обработке через очереди сообщений и разделение сервисов по назначению (валидация, принятие решения, журналирование, аналитика) для снижения латентности и повышения устойчивости [7].

Другая группа исследований посвящена повышению качества идентификации и обнаружению нарушений. При использовании только пропусков (RFID-карт) остаются риски передачи карты третьим лицам. В качестве дополнения рассматриваются методы корреляции событий доступа с видеонаблюдением, биометрией и анализом поведения (по времени прохода, последовательности перемещений, частоте отказов) [8-9]. Для объектов с массовыми мероприятиями важно отличать «легитимные» пиковые нагрузки от атак и некорректных действий (например, «хвостование», попытки прохода группой по одному пропуску).

В инженерной практике также отмечаются проблемы несогласованности правил и человеческого фактора: дублирование уровней доступа, конфликт временных интервалов, ошибки при выдаче временных пропусков, отсутствие единых шаблонов [10]. Это ведёт к росту ложных отказов и нагрузке на службу охраны. Поэтому оптимизация СКУД должна включать не только ускорение обработки, но и управление качеством политик, аудит изменений и унификацию справочников.

Нормативные требования и практические ограничения

Для объектов общественного назначения при модернизации СКУД необходимо учитывать требования информационной безопасности, электробезопасности, пожарной безопасности и эксплуатационной надёжности. В части ИБ широко применяются подходы и термины стандартов семейства ISO/IEC 27000, а также рекомендации NIST по контролям безопасности и управлению журналами [11-12]. Для инженерных средств контроля доступа важны требования к защищённому каналу связи между считывателем и контроллером (например, использование OSDP Secure Channel), разграничение полномочий администраторов и хранение журналов в неизменяемом виде.

С точки зрения пожарной безопасности критично корректное взаимодействие СКУД с системами ОПС/АПТ: при пожаре должны выполняться сценарии разблокировки эвакуационных выходов и снятия блокировок в соответствии с проектными решениями [13]. На практике это требует чёткого разделения режимов «нормальная работа», «пожар», «авария», «антитеррор» и соответствующих приоритетов команд.

Наконец, практическими ограничениями являются бюджет, уже установленное оборудование, наличие кабельной инфраструктуры, требования заказчика к удобству работы персонала и к скорости внедрения. Поэтому оптимизация должна быть по возможности «надстройкой» над существующей системой: улучшение алгоритмов, схемы обмена и структуры данных без обязательной полной замены оборудования.

Объект исследования и постановка задачи оптимизации

В качестве объекта исследования рассматривается СКУД Конгресс-Холла «Аулие-Ата», относящегося к зданиям общественного назначения с переменной посещаемостью. Для подобных объектов характерны: наличие нескольких входных групп (главные входы для посетителей и служебные входы), зоны ограниченного доступа (служебные помещения, аппаратные, серверные, помещения охраны), а также периодические мероприятия, когда число посетителей в ограниченный промежуток времени существенно возрастает.

В рамках работы приняты следующие исходные данные и допущения, отражающие типовой профиль нагрузки: (1) число точек прохода – от нескольких десятков до сотни (с учётом дверей служебных помещений); (2) количество пользователей – от нескольких сотен сотрудников и подрядчиков до нескольких тысяч посетителей; (3) основная доля событий доступа формируется в утренние/вечерние интервалы и непосредственно перед началом мероприятий; (4) часть точек прохода должна сохранять работоспособность при кратковременных сбоях связи с сервером; (5) требуется интеграция с СВН (видеонаблюдение) для оперативного просмотра фрагментов по событиям, и с пожарной автоматикой для выполнения режимов разблокировки.

Постановка задачи оптимизации формулируется следующим образом. Пусть поток запросов к системе имеет интенсивность $\lambda(t)$, зависящую от времени. Для каждого события необходимо в минимально возможное время сформировать решение

(разрешить/запретить/режимный сценарий) и записать событие в журнал, обеспечив при этом: (a) корректность политик доступа; (b) устойчивость к типовым сбоям и атакам; (c) полноту протоколирования. Требуется уменьшить среднее время обработки события $\bar{T}$ и его дисперсию (устойчивость по времени реакции), не снижая уровень безопасности.

Ключевые метрики, используемые в работе: среднее время принятия решения по событию (мс), доля событий с превышением порога обработки (таймауты), доля ложных отказов (например, из-за конфликтов политик), полнота журналирования (доля событий, имеющих связку «СКУД + СВН + контекст»), а также показатели доступности при частичной потере связи с сервером.

Предлагаемые методы оптимизации процессов контроля и управления

Архитектурная оптимизация: распределение функций и событийная обработка

На практике многие проблемы производительности возникают, когда центральный сервер одновременно выполняет функции принятия решения, записи в базу, интеграционные вызовы и формирование отчётов. При пиковых нагрузках это приводит к конкуренции за ресурсы (CPU, диск, блокировки БД), а задержка в одной подсистеме «протягивается» в цепочку обработки событий.

В качестве базового архитектурного принципа предлагается разделение функций на уровни: (1) уровень точки прохода (считыватель + контроллер), отвечающий за первичную валидацию идентификатора, управление исполнительным устройством и хранение кэша критически важных правил; (2) уровень серверных сервисов (принятие решения по сложным правилам, администрирование, аналитика); (3) уровень интеграций (СВН, ОПС/АПТ, HR, SIEM) через единый API и/или шину сообщений. Коммуникация между сервисами организуется асинхронно: событие доступа фиксируется как сообщение, которое может быть обработано несколькими потребителями без блокирования основного процесса открытия/закрытия двери.

Для реализации событийного подхода могут использоваться брокеры сообщений и очереди (например, AMQP/MQTT), а также механизмы журналирования по принципу append-only. В таком случае критический путь обработки (decision path) включает лишь необходимый минимум операций: проверку права + команду на замок + запись компактного события. Расширенная обработка (обогащение события, аналитика, синхронизация с внешними системами) выполняется асинхронно. Это снижает среднюю латентность и уменьшает вероятность таймаутов при пиковых нагрузках [7].

Дополнительно предлагается кэширование политик на контроллере: при наличии устойчивого набора правил для конкретной двери/зоны (например, список разрешённых ролей в заданные интервалы) контроллер способен принять решение локально даже при временном отсутствии связи с сервером [14]. Сервер при восстановлении связи получает журнал событий контроллера и синхронизирует состояние. Такой подход повышает доступность системы и уменьшает нагрузку на сеть.

Оптимизация правил доступа: гибрид RBAC+ABAC и управление конфликтами

Оптимизация логики доступа начинается с формализации правил. Для объекта с разными категориями пользователей удобно использовать RBAC как «скелет» политики: каждому пользователю назначается одна или несколько ролей, определяющих базовый набор зон доступа. ABAC применяется как «надстройка» для уточняющих условий: время, тип события, режим (обычный/мероприятие/пожар), уровень риска, статус удостоверения, наличие сопровождения и т.п.

Предлагается следующая схема принятия решения. На первом этапе оцениваются базовые права (RBAC), что даёт быстрый ответ в большинстве стандартных ситуаций. На втором этапе при необходимости подключаются атрибутные правила (ABAC), которые могут как разрешать доступ (например, временный пропуск подрядчика), так и ограничивать его (например, запрет на проход в непрофильное время). Такой двухэтапный подход ускоряет обработку, потому что тяжёлые проверки выполняются только для части событий.

Отдельная задача – предотвращение конфликтов политик (например, когда одно правило разрешает, а другое запрещает). Для этого вводится приоритетность правил и стратегия разрешения конфликтов. В работе предлагается использовать принцип «запрет имеет приоритет», а также явно выделять исключения в виде высокоприоритетных правил (например, аварийные режимы и действия охраны). Изменения политик должны проходить аудит: фиксируется автор изменения, причина, время и перечень затронутых зон.

Для сокращения ложных отказов целесообразно унифицировать справочники (роль, зона, точка прохода), применять шаблоны (политика для типового этажа/сектора) и выполнять верификацию правил на тестовом контуре перед публикацией. Для проверки применяются сценарные тесты: набор типовых траекторий перемещения пользователей, для которых система должна дать ожидаемый результат.

Адаптивная оценка риска и обнаружение аномалий

Для объектов с большим числом посетителей актуален риск злоупотребления пропусками и попыток обхода правил (передача карты, «хвостование», подбор ID, многократные попытки прохода). Поэтому в дополнение к статическим правилам предлагается вводить риск-ориентированный слой принятия решения (risk-adaptive). Он не заменяет основную политику, а корректирует решение в ситуациях, когда контекст выглядит подозрительно [4].

Пример простого риск-скоринга: каждой аномальной характеристике присваивается вес (нехарактерное время, серия отказов, попытки прохода через нетипичную точку, слишком частые проходы за короткий период, несоответствие режима мероприятия). Суммарный риск сравнивается с порогом. При превышении порога система может перевести событие в режим «требуется подтверждение охраны», инициировать видеоверификацию (показ камеры на посту), либо временно блокировать пропуск на заданное время с фиксацией инцидента.

В расширенном варианте слой риска может опираться на модели машинного обучения (кластеризация нормального поведения, классификация аномалий). Однако даже простые эвристики уже дают эффект при минимальных вычислительных затратах, особенно если оценка выполняется на сервере аналитики асинхронно, а на критическом пути используется только быстрый пороговый критерий (например, «N отказов за M секунд»).

Интеграция с СВН, ОПС/АПТ и системами учёта: единый контур событий

Интеграция СКУД с другими подсистемами безопасности повышает качество контроля и сокращает время реакции на инциденты. Для Конгресс-Холла наиболее значимы следующие интеграции: (1) СВН – для просмотра фрагмента видео по событию доступа и подтверждения личности; (2) ОПС/АПТ – для сценариев разблокировки и приоритета эвакуации; (3) учёт рабочего времени/HR – для синхронизации профилей сотрудников и статусов доступа; (4) централизованное логирование или SIEM – для хранения журналов в неизменяемом виде и корреляции событий.

Предлагается строить интеграцию по принципу «единый источник события»: любое событие доступа формируется в стандартизированном формате (идентификатор пользователя, точка прохода, временная метка, решение, причина, уровень риска, ссылка на связанные объекты) и публикуется в шину сообщений/API. Потребители (СВН, SIEM и др.) подписываются на эти события и выполняют свою обработку. Это исключает «точечные» интеграции по принципу «каждый с каждым», упрощает сопровождение и снижает вероятность ошибок при обновлениях.

Для пожарных режимов предлагается отдельный канал приоритетных команд, который не зависит от очереди событий доступа. В режиме «пожар» команды разблокировки эвакуационных выходов имеют приоритет над всеми другими политиками. Журнал событий в этом режиме должен фиксировать как факт срабатывания, так и выполненные действия (какие двери разблокированы, в какое время и кем подтверждено).

Оптимизация хранения данных и журналирования

Журналирование в СКУД выполняет две функции: оперативную (разбор инцидента «здесь и сейчас») и юридически значимую (аудит). Поэтому важно обеспечить целостность журналов, достаточную детализацию и одновременно не создавать избыточную нагрузку на систему при записи.

В работе предлагается разделять «оперативный журнал» и «архив». Оперативный журнал хранит события в базе данных с индексами по времени, пользователю и точке прохода, обеспечивая быстрый поиск. Архив формируется пакетами и хранится в неизменяемом виде (например, WORM-хранилище или защищённое хранилище логов), при необходимости с электронной подписью. Такая схема снижает нагрузку на транзакционную БД и повышает доверие к журналам.

Для ускорения записи событий применимы: пакетная запись (batch), предварительная агрегация повторяющихся отказов, отказ от тяжёлых JOIN-операций на критическом пути и

использование нормализованных справочников (пользователь, зона, дверь) с компактными внешними ключами. Дополнительно рекомендуется синхронизация времени (NTP) на всех контроллерах и серверах для корректной корреляции событий с СВН.

Практическая реализация и результаты

Структурная схема системы и потоков данных

На рисунке 1 представлена обобщённая структурная схема СКУД и основных интеграций, характерная для объекта типа Конгресс-Холл.

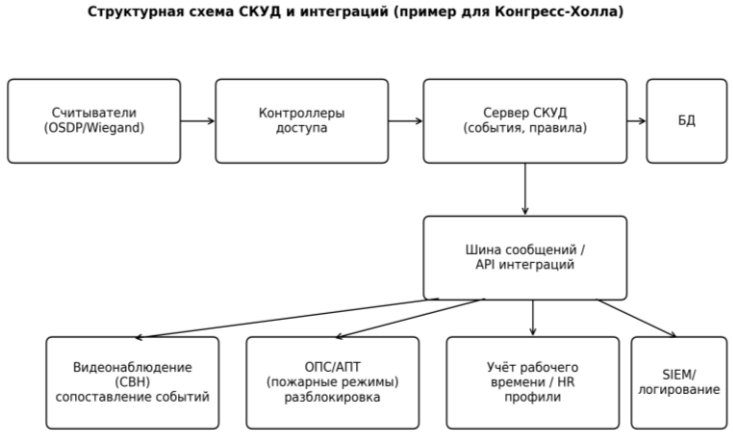

Рисунок 1 – Структурная схема СКУД и интеграций (пример)

Схема отражает разделение уровней и позволяет разгрузить центральный сервер за счёт асинхронной обработки интеграций и автономности контроллеров.

Алгоритм обработки события доступа

На рисунке 2 приведён упрощённый алгоритм обработки события доступа, включающий проверку доверенного канала, RBAC+ABAC и риск-скоринг.

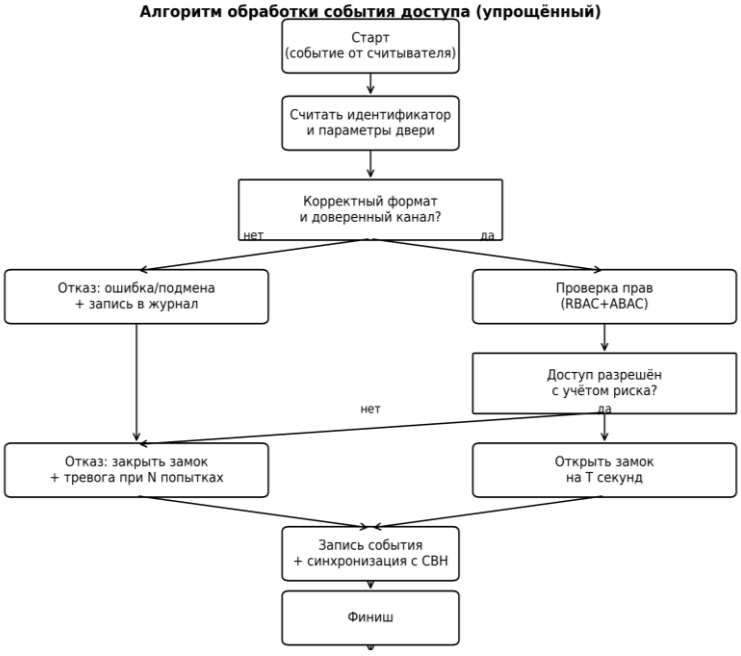

Рисунок 2 – Алгоритм обработки события доступа (упрощённый)

Листинг 1 – Псевдокод обработки события доступа.

```
Вход: event = {uid, door_id, ts, channel_state}
1) if not validate_channel(event.channel_state):
        deny('invalid_channel'); log(event, reason); return
2) ctx = build_context(uid, door_id, ts)
3) decision = rbac_check(uid, door_id, ctx)
4) if decision == 'unknown' or ctx.requires_abac:
```

decision = abac_check(uid, door_id, ctx)

5) risk = risk_score(uid, door_id, ctx, recent_events)

6) if decision == 'allow' and risk > R_THRESHOLD:

decision = 'confirm' # запрос подтверждения охраны/видео

7) execute(decision, door_id)

8) log(event, decision, risk); publish_to_bus(event)

Оценка эффективности: моделирование и сравнительный анализ

Оценка эффективности выполнялась методом моделирования потоков запросов к СКУД с учётом переменной интенсивности λ(t). Сравнивались два варианта: (A) базовый – централизованная обработка с синхронными интеграционными вызовами и записью в БД на критическом пути; (B) оптимизированный – разделение сервисов, асинхронные интеграции и кэширование правил на контроллере для типовых сценариев.

В качестве нагрузки рассматривались три режима: (1) штатный (равномерный поток), (2) «вход сотрудников» (пик в течение 20-30 минут), (3) «мероприятие» (резкий рост потока перед началом, затем спад). Метрики фиксировались на интервале 1 часа моделирования. Порог таймаута обработки события принят 500 мс (условное значение, при превышении которого наблюдается заметная задержка для пользователя). Результаты имитационного моделирования приведены в таблице 1.

Таблица 1 – Сравнение времени обработки события и доли таймаутов

Режим	$\bar{T}$, мс (A)	$\bar{T}$, мс (B)	Таймауты, % (A)	Таймауты, % (B)
Штатный	180	125	2.1	0.6
Пик сотрудников	420	290	11.4	4.0
Мероприятие	510	340	16.8	6.2

Оптимизированный вариант обеспечивает снижение среднего времени обработки на 25-35% и уменьшение доли таймаутов в пиковых режимах.

Обсуждение результатов и рекомендации по внедрению

Влияние предложенных мер на эксплуатацию и безопасность

Полученные результаты показывают, что основная часть выигрыша по времени реакции достигается за счёт уменьшения «критического пути» и исключения синхронных внешних операций. При этом уровень безопасности не снижается, поскольку: (1) правила доступа остаются централизованно управляемыми и проходят аудит; (2) риск-ориентированный слой повышает чувствительность к аномалиям; (3) интеграция с СВН обеспечивает дополнительный фактор подтверждения. Важным аспектом является корректная настройка приоритетов режимов, особенно «пожар» и аварийные сценарии.

С эксплуатационной точки зрения переход к событийной архитектуре повышает наблюдаемость системы: события имеют единый формат, доступны для мониторинга в реальном времени и могут быть использованы для построения дашбордов (нагрузка по входным группам, доля отказов, активность по зонам). Это позволяет заранее выявлять проблемы – например, некорректно настроенные правила на конкретной двери или деградацию связи с контроллером.

Следует учитывать, что кэширование правил на контроллере требует дисциплины управления версиями: контроллер должен получать обновления политик атомарно, а при невозможности обновления переходить в безопасный режим (по заранее согласованному сценарию). Рекомендуется использовать механизмы подписывания политик и контроль целостности конфигурации.

Этапы внедрения на объекте типа Конгресс-Холл

Для практического внедрения оптимизаций на действующем объекте целесообразно применять поэтапный подход:

Этап 1 – инвентаризация и аудит текущих политик: устранение дубликатов ролей, нормализация зон, настройка единых шаблонов и регламента изменений. На этом же этапе определяется перечень критических точек прохода и требования к режимам (пожар, авария, мероприятие).

Этап 2 – внедрение единого формата событий и централизованного логирования: настройка корреляционных идентификаторов, синхронизация времени, построение базовых отчётов и контроль полноты журналов.

Этап 3 – подключение шины сообщений/API для интеграций. Сначала интеграция с СВН (связка события доступа и камеры), затем интеграция с HR/учётом рабочего времени, и далее – с SIEM/архивом логов. Важно настраивать обработку асинхронно, чтобы не увеличивать критический путь.

Этап 4 – кэширование политик на контроллерах и настройка автономного режима для выбранных точек прохода. Проводятся испытания при отключении связи с сервером и при восстановлении связи (синхронизация журналов).

Этап 5 – включение риск-ориентированного слоя. Начинать рекомендуется с простых эвристик (N отказов, нетипичное время, «ускоренные» проходы), после накопления данных возможно подключение более сложной аналитики.

Поэтапность позволяет получить быстрый эффект уже на ранних стадиях и снизить риски внедрения, так как критичные сценарии проверяются на пилотной зоне до тиражирования.

Ограничения и направления дальнейших исследований

Ограничением представленного исследования является использование моделирования как основного метода оценки. Реальные значения метрик зависят от конкретного оборудования, сети, конфигурации БД и качества правил. Однако сами принципы оптимизации (сокращение критического пути, асинхронные интеграции, гибридная модель доступа, риск-скоринг) являются переносимыми и подтверждаются результатами работ других авторов.

В качестве направлений дальнейших исследований можно выделить: (1) разработку формальных методов верификации политик ABAC и автоматического поиска конфликтов; (2) применение методов машинного обучения для прогнозирования аномалий и оценки риска с учётом траекторий перемещения; (3) оценку экономической эффективности модернизации (CAPEX/OPEX) и оптимального уровня резервирования для объектов различного масштаба.

Также перспективным является применение «цифрового двойника» СКУД: симуляционная модель, синхронизируемая с журналами реальной системы, позволяет тестировать новые правила и сценарии мероприятия без риска для эксплуатации.

Заключение

В работе рассмотрена задача оптимизации процессов контроля и управления в системе контроля и управления доступом объекта общественного назначения (Конгресс-Холл «Аулие-Ата»). Выполнен обзор типовых архитектур СКУД, моделей управления доступом и подходов к интеграции с другими системами безопасности. Показано, что на объектах с переменной нагрузкой основные проблемы связаны с задержками обработки событий, конфликтами правил, недостаточной интеграцией и ограниченной аналитикой.

Предложен комплекс мер, включающий событийно-ориентированную обработку и разделение функций по уровням, кэширование критических правил на контроллерах, гибридную модель RBAC+ABAC с управлением конфликтами, риск-ориентированный слой обнаружения аномалий, а также единый контур событий через API/шину сообщений для интеграции с СВН, ОПС/АПТ, HR и SIEM. Представлены структурная схема и алгоритм обработки события доступа.

По результатам моделирования достигнуто снижение среднего времени обработки события на 25-35% и уменьшение доли таймаутов в 2-3 раза в пиковых режимах. Улучшена полнота журналирования за счёт корреляции событий и унификации формата данных. Предложенные решения могут быть использованы при проектировании и модернизации СКУД объектов массового пребывания людей, обеспечивая повышение удобства эксплуатации при сохранении требований безопасности.

Список литературы

1. Security Industry Association (SIA). Open Supervised Device Protocol (OSDP) v2.2 – Technical Specification. Silver Spring, MD: SIA, 2017.

2. Role-Based Access Control Models / R.S. Sandhu et al // IEEE Computer. – 1996. – Vol. 29, № 2. – P. 38-47.

3. Hu V.C. Assessment of Access Control Systems / V.C. Hu, D. Ferraiolo, R. Kuhn // NIST Interagency Report 7316. Gaithersburg, MD: NIST, 2006.

4. McGraw R. Risk-Adaptable Access Control (RAdAC) / R. McGraw // Security and Privacy in Dynamic Environments. IEEE, 2009.

5. Гончаров А.В. Системы контроля и управления доступом: проектирование и эксплуатация / А.В. Гончаров. – М.: ИНФРА-М, 2021.
6. Сидоров Н.Н. Интеллектуальные системы безопасности: методы анализа событий и предотвращения инцидентов / Н.Н. Сидоров. – СПб.: Питер, 2020.
7. Zhang H. Event-Driven Architectures for Security Monitoring: A Survey and Practical Considerations / H. Zhang, J. Li // IEEE Access. – 2021. – Vol. 9. – P. 102340-102356.
8. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / A. Al-Fuqaha et al // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, № 4. – P. 2347-2376.
9. Chen X. Integrating Access Control Events with Video Analytics for Incident Response / X. Chen, Y. Zhang // Journal of Security and Networks. – 2022. – Vol. 17, № 3. – P. 145-158.
10. Kent K. Guide to Computer Security Log Management / K. Kent, M. Souppaya // NIST Special Publication 800-92. Gaithersburg, MD: NIST, 2006. – 72 p.
11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022.
12. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva: ISO, 2022.
13. IEC 60839-11-1:2013. Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements. Geneva: IEC, 2013.
14. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Rev. 5. Gaithersburg, MD: NIST, 2020.

References

1. Security Industry Association (SIA). Open Supervised Device Protocol (OSDP) v2.2 – Technical Specification. Silver Spring, MD: SIA, 2017. (In English).
2. Role-Based Access Control Models / R.S. Sandhu et al // IEEE Computer. – 1996. – Vol. 29, № 2. – P. 38-47. (In English).
3. Hu V.C. Assessment of Access Control Systems / V.C. Hu, D. Ferraiolo, R. Kuhn // NIST Interagency Report 7316. Gaithersburg, MD: NIST, 2006. (In English).
4. McGraw R. Risk-Adaptable Access Control (RAdAC) / R. McGraw // Security and Privacy in Dynamic Environments. IEEE, 2009. (In English).
5. Goncharov A.V. Sistemy kontrolya i upravleniya dostupom: proektirovanie i ehkspluatatsiya / A.V. Goncharov. – M.: INFRA-M, 2021. (In Russian).
6. Sidorov N.N. Intellektual'nye sistemy bezopasnosti: metody analiza sobytii i predotvrashcheniya intsidentov / N.N. Sidorov. – SPb.: Piter, 2020. (In Russian).
7. Zhang H. Event-Driven Architectures for Security Monitoring: A Survey and Practical Considerations / H. Zhang, J. Li // IEEE Access. – 2021. – Vol. 9. – P. 102340-102356. (In English).
8. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / A. Al-Fuqaha et al // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, № 4. – P. 2347-2376. (In English).
9. Chen X. Integrating Access Control Events with Video Analytics for Incident Response / X. Chen, Y. Zhang // Journal of Security and Networks. – 2022. – Vol. 17, № 3. – P. 145-158. (In English).
10. Kent K. Guide to Computer Security Log Management / K. Kent, M. Souppaya // NIST Special Publication 800-92. Gaithersburg, MD: NIST, 2006. – 72 p. (In English).
11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. (In English).
12. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva: ISO, 2022. (In English).
13. IEC 60839-11-1:2013. Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements. Geneva: IEC, 2013. (In English).
14. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Rev. 5. Gaithersburg, MD: NIST, 2020. (In English).

Б.С. Сарсенов*, Д. Жамангарин
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қ., Александр Пушкина к-сі, 11
*e-mail: batyr.sarsenov@gmail.com

ӘУЛИЕ-АТА КОНГРЕСС-ХОЛЛЫНЫҢ ҚОЛЖЕТІМДІЛІКТІ БАҚЫЛАУ ЖӘНЕ БАСҚАРУ ЖҮЙЕСІНДЕГІ БАҚЫЛАУ ЖӘНЕ БАСҚАРУ ПРОЦЕСТЕРІН ОҢТАЙЛАНДЫРУ

Мақалада қоғамдық мақсаттағы объект – "Әулие Ата" Конгресс-Холл мысалында қол жеткізуді бақылау және басқару жүйесіндегі бақылау және басқару процестерінің тиімділігі мен сенімділігін арттыру міндеті қарастырылады. СКУД типтік архитектураларына және ақпараттық қауіпсіздік пен инженерлік қауіпсіздік жүйелеріне қойылатын нормативтік талаптарға шолу жасалды. Келушілердің тығыздығы жоғары нысандарда және қол жетімділіктің аралас сценарийлерінде (қызметкерлер, мердігерлер, қонақтар, бұқаралық іс-шаралар) шешімдердің кешігуі, ережелердің сәйкес келмеуі, бейнебақылау және өрт автоматикасымен интеграцияның жеткіліксіздігі және оқиғалардың шектеулі талдауы негізгі проблемалар болып табылады. Оңтайландыру шараларының кешені ұсынылды: оқиғаға бағытталған өңдеуге көшу (event-driven), жергілікті контроллерлер мен ережелерді кэштеу арқылы серверді түсіру, тәуекелді адаптивті бағалаумен rbac+abac қол жеткізуді басқарудың гибридті моделін қолдану, ЖУРНАЛДАУДЫ біріздендіру және API/шиналар арқылы интеграциялау.

Түйін сөздер: *қолжетімділікті бақылау және басқару, ҚББЖ; оңтайландыру, RBAC, ABAC, тәуекелді бағалау, интеграция, оқиғаға негізделген өңдеу, аудит.*

B.S. Sarsenov*, D. Zhamangarin
L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, Alexander Pushkin St., 11
*e-mail: batyr.sarsenov@gmail.com

OPTIMIZATION OF CONTROL AND MANAGEMENT PROCESSES IN THE ACCESS CONTROL AND MANAGEMENT SYSTEM OF THE AULIE-ATA CONGRESS HALL

The article discusses the task of improving the efficiency and reliability of control and management processes in the access control and management system (ACMS) using the example of a public facility, the Congress Hall "Aulie-Ata". The article provides an overview of typical ACMS architectures and regulatory requirements for information security and engineering security systems. It has been shown that at facilities with a high density of visitors and mixed access scenarios (employees, contractors, guests, and mass events), the key problems are decision delays, inconsistent rules, insufficient integration with video surveillance and fire automation, and limited event analytics. A set of optimization measures is proposed: transition to event-oriented processing (event-driven), server offloading due to local controllers and rule caching, application of a hybrid RBAC+ABAC access control model with adaptive risk assessment, unification of logging and integration via API/bus.

Key words: *access control, ACMS, optimization, RBAC, ABAC, risk scoring, integration, event-driven, audit.*

Сведения об авторах

Батырхан Саматұлы Сарсенов* – магистрант, Евразийский национальный университет имени Л.Н. Гумилева, Республика Казахстан, г. Астана; e-mail: batyr.sarsenov@gmail.com. ORCID: https://orcid.org/0009-0003-5491-2160.

Дусмат Жамангарин – PhD, Евразийский национальный университет имени Л.Н. Гумилева, Республика Казахстан, г. Астана; e-mail: Dusmat_zhamangarin@vk.com.

Авторлар туралы мәліметтер

Батырхан Саматұлы Сарсенов* – магистрант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан Республикасы, Астана қ.; e-mail: batyr.sarsenov@gmail.com. ORCID: https://orcid.org/0009-0003-5491-2160.

Дусмат Жамангарин – PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан Республикасы, Астана қ.; e-mail: Dusmat_zhamangarin@vk.com.

Information about the authors

Batyrkhan Samatuly Sarsenov* – Master's student, L.N. Gumilyov Eurasian National University, Republic of Kazakhstan, Astana; e-mail: batyr.sarsenov@gmail.com. ORCID: https://orcid.org/0009-0003-5491-2160.

Dusmat Zhamangarin — PhD, L.N. Gumilyov Eurasian National University, Republic of Kazakhstan, Astana; e-mail: Dusmat_zhamangarin@vk.com.

Поступила в редакцию 05.01.2026
Поступила после доработки 23.02.2026
Принята к публикации 24.02.2026

https://doi.org/10.53360/2788-7995-2026-1(21)-16

МРНТИ: 47.45.29

А.С. Инчин[1], А.Е. Кулакаева[2*], М.П. Сайганов[1], Ш.С. Болат[1]
[1]ТОО «Институт космической техники и технологий»
050061, Республика Казахстан, г. Алматы, ул. Кисловодская, 34
[2]АО «Международный университет информационных технологий»
050040, Республика Казахстан, г. Алматы, ул. Манаса, 34/1
*e-mail: a.kulakayeva@iitu.edu.kz

ВЛИЯНИЕ УСЛОВИЙ ИНТЕГРАЦИИ НА ХАРАКТЕРИСТИКИ ПЛОСКИХ GSM-АНТЕНН В ЭЛЕКТРОННОЙ НАВИГАЦИОННОЙ ПЛОМБЕ

***Аннотация**. В данной статье рассматривается практический вопрос выбора GSM-антенны для электронной навигационной пломбы, предназначенной для контроля и мониторинга перевозок. В отличие от традиционных методов, опирающихся на паспортные данные, акцент сделан на исследовании работы антенн в составе готового устройства с учетом влияния пластикового корпуса, внутренних металлических компонентов и общей компоновки электроники.*

Для этого были проведены лабораторные испытания 28 коммерчески доступных плоских GSM-антенн диапазона GSM 900 в условиях, максимально приближенных к реальной эксплуатации в навигационной пломбе. Оценка характеристик осуществлялась на стандартизированном измерительном стенде с использованием макета корпуса и эталонной антенны. Основным критерием сравнения являлся коэффициент стоячей волны, отражающий качество согласования антенны с радиомодулем и уровень потерь мощности.

При выборе также учитывались ограничения по габаритам корпуса, имеющие важное значение для практической интеграции. На основании комплексного анализа были отобраны антенны, обеспечивающие стабильную связь и достаточную энергетическую эффективность, и рекомендованы для использования в серийных электронных навигационных пломбах.

Полученные результаты подтверждают, что корректный выбор антенны невозможен без учета условий ее установки в составе конкретного устройства, а испытания в условиях, приближенных к реальной компоновке, являются важным этапом при разработке навигационных систем, эксплуатируемых в условиях ограниченного внутреннего объема и плотной компоновки элементов.

***Ключевые слова:** навигационная пломба, GSM-антенна, плоская антенна, коэффициент стоячей волны, КСВ, диапазон GSM 900, согласование антенны, логистика.*

Введение

В последние годы в Республике Казахстан особое внимание уделяется вопросам повышения эффективности и безопасности перевозок товаров, что связано с важным стратегическим положением страны в региональных и международных транспортных коридорах. С учетом роста объемов грузоперевозок, ужесточения требований к прослеживаемости товаров и усиления контроля за логистическими цепочками, особенно актуальными становятся электронные навигационные пломбы. Эти устройства обеспечивают дистанционный мониторинг местоположения и состояния груза в режиме реального времени.

Электронные навигационные пломбы, помимо обеспечения сохранности груза, должны отвечать строгим техническим и эксплуатационным требованиям, определённым Решением Совета Евразийской экономической комиссии от 4 июля 2023 года № 75 [1]. Ключевые требования включают: наличие сменного многоразового элемента пломбирования,