УДК 64.061.4

АКТУАЛЬНЫЕ ПРОБЛЕМЫ УПРАВЛЕНИЯ ВОРОТАМИ И ШЛАГБАУМАМИ ВО ДВОРАХ МНОГОКВАРТИРНЫХ ДОМОВ

CURRENT ISSUES IN THE MANAGEMENT OF GATES AND BARRIERS IN THE COURTYARDS OF APARTMENT BUILDINGS

Геращенко Алексей Валерьевич
генеральный директор,
АО Атмос
aoatmos@inbox.ru

Данилюк Сергей Сергеевич
старший преподаватель,
Московский государственный технический университет имени Н.Э. Баумана
vin.90@mail.ru

Кайа Михаил Ибрахимович
студент 4 курса,
Московский государственный технический университет имени Н.Э. Баумана
mikhail.kaya@mail.ru

Самолин Григорий Константинович
студент 4 курса,
Московский государственный технический университет имени Н.Э. Баумана
gsamolin2@mail.ru

Аннотация. В статье приведен взгляд исследователей на вопросы управле ния пре граж да ющими управляемыми устройствами (воротами и шлагбаумами) во дво рах много квартирных домов как элементов системы контроля и управления досту пом (СКУД).
Авторы выявляют и показывают ряд существующих проблем дистанцион ного управления воротами и шлагбаумами дворов много квартирных домов. Опи сываются проблемы надёжности и отказоустойчивости, информационной безопасности, задержек и синхронизации, влияния внешних факторов, а также проблема человеческого фактора и эксплуатационные проблемы.
Предлагаются пути повышения надёжности и безопасности систем управ ления преграждающими устройствами, в частности, применение распределён ной архи тек туры с локальными контроллерами и гибридизации применяемых кана лов связи.
Особое внимание уделяется вопросу удобства и экономии времени поль зо вателей дистанционного управления воротами и шлагбаумами, а также вопро су защищенности системы управления. Авторы делают вывод, что баланс между этими вопросами является ключевым при построении «идеальной» СКУД придомовой территории.

Ключевые слова: СКУД, преграждающие устройства, управление преграждающими устройствами, дворы многоквартирных домов, дистанционное управление, проблемы дистанционного управления, экономия времени.

Gerashchenko Aleksey Valeryevich
CEO of JSC Atmos
aoatmos@inbox.ru

Danilyuk Sergey Sergeyevich
Senior Lecturer,
Bauman Moscow State Technical University
vin.90@mail.ru

Kaya Mihail Ibrahimovich
4th-year student,
Bauman Moscow State Technical University
mikhail.kaya@mail.ru

Samolin Grigory Konstantinovich
4th-year student,
Bauman Moscow State Technical University
gsamolin2@mail.ru

Annotation. The article presents the researchers' perspective on the management of access-blocking controllable devices – namely gates and barriers – in the courtyards of multi-apartment residential buildings, considered as elements of an access control and management system (ACMS).
The authors identify and examine a number of existing problems associated with the remote management of gates and barriers in residential building courtyards. The problems addressed include reliability and fault tolerance, information security, latency and synchronization, the influence of external factors, as well as the human factor and operational challenges.
Approaches to improving the reliability and security of barrier device management systems are proposed – in particular, the adoption of a distributed architecture with local controllers and the hybridization of communication channels employed.
Special attention is given to the convenience and time efficiency of remote gate and barrier management for end users, as well as to the security of the management system. The authors conclude that achieving a balance between these considerations is paramount in designing an «ideal» ACMS for residential premises.

Keywords: Access control and management systems, physical barriers, barrier control, apartment building courtyards, remote control, remote control issues, time saving.

Преграждающие управляемые устройства как элемент системы контроля доступа

Обеспечение безопасности придомовых территорий многоквартирных домов (МКД) в современных условиях неразрывно связано с применением преграждающих управляемых устройств (ПУУ) – технических средств, предназначенных для физического ограничения въезда на придомовую терри торию и регулирования доступа транспортных средств и пешеходов. К таким устройствам относятся автоматические ворота и шлагбаумы, оснащённые исполнительными механизмами, обеспечивающими управление их состоянием по командам извне.

В структуре системы контроля и управления доступом (СКУД) преграждающие устройства занимают исполнительный уровень и функционируют во взаимодействии с контроллерами, средствами идентификации и подсистемами управления. С точки зрения степени автоматизации целесообразно различать автоматический режим работы, при котором решение о допуске принимается на основе заранее заданных алгоритмов и сигналов от средств идентификации без участия оператора, и автоматизированный режим, предполагающий вмешательство человека-оператора при принятии решения. В условиях МКД наиболее распространено автоматизированное управление: доступ предоставляется как по идентификатору (радиобрелок, код), так и по команде от жильца через доступный канал связи.

Выбор способа и архитектуры управления напрямую определяет как удобство эксплуатации, так и перечень возникающих проблем. В практике управления въездными устройствами дворов МКД применяются три принципиальных архитектурных подхода:

Централизованная архитектура предполагает управление всеми устройствами из единого узла. Она проста в реализации, однако весьма уязвима – отказ центрального элемента или канала связи нарушает работу всей системы.

Распределённая архитектура переносит часть функций управления на локальные контроллеры вблизи исполнительных устройств, что повышает отказоустойчивость и позволяет сохранять автономную работу при потере связи с центральным узлом.

Иерархическая архитектура сочетает оба подхода и применяется в крупных комплексах с множеством точек доступа, обеспечивая эффективное масштабирование, однако требует более сложного проектирования и сопровождения.

Анализ проблем дистанционного управления преграждающими устройствами

Дистанционное управление воротами и шлагбаумами дворов МКД сопряжено с рядом проблем, которые можно систематизировать по нескольким группам.

Проблемы надёжности и отказоустойчивости. Устойчивость дистанционного управления определяется прежде всего характеристиками канала передачи команд. Кратковременные нарушения связи приводят к задержкам выполнения команд и образованию очередей у въезда. Длительные отказы способны полностью исключить дистанционное управление. Особую опасность представляет неопределённое состояние устройства при прерывании связи: система управления лишается информации об актуальном положении створки или стрелы, что затрудняет принятие верных решений. Дополнительным фак тором риска является отсутствие проработанных резервных режимов: при их отсутствии отказ связи может приводить либо к полной блокировке въезда, либо к неконтролируемому открытию, что недопустимо с точки зрения безопасности.

Проблемы информационной безопасности. Широко применяемые в дворовых СКУД радиоканальные пульты управления (брелоки) сопряжены с рисками перехвата и подбора кода. Устройства, использующие устаревшие протоколы без динамической смены кода, поддаются атакам с использованием доступного радиооборудования. При интеграции управляющего оборудования в IP-инфраструктуру объекта возникают угрозы, характерные для сетевых систем: несанкционированный доступ к каналу передачи команд, модификация управляющих сигналов, компрометация учётных данных операторов. Недоста точное разграничение прав доступа внутри системы управления повышает вероятность как преднамеренных, так и непреднамеренных нарушений режима доступа.

Проблемы задержек и синхронизации. Задержки при передаче управляющих команд могут приводить к рассогласованию между ожидаемым и фактическим состоянием устройства. При интенсивном потоке транспортных средств даже кратковременные задержки снижают пропускную способность въезда и вызывают конфликтные ситуации среди жильцов. Потеря или задержка сообщений о состоянии устройства лишает оператора актуальной картины и приводит к ошибочным командам управления.

Человеческий фактор и эксплуатационные проблемы. В автоматизированных системах управления ошибки, связанные с высокой нагрузкой на оператора, недостаточной подготовкой персонала или некорректной интерпретацией состояния системы, приводят к нарушениям пропускного режима. Несвоевременное техническое обслуживание и некорректная настройка параметров усугубляют ситуацию: в условиях дистанционного контроля выявление подобных проблем затруднено, что увеличивает время реакции и снижает надёжность системы в целом.

Влияние внешних факторов. Оборудование, устанавливаемое на придомовой территории, подвержено климатическим воздействиям, электромагнитным помехам и нестабильности электропитания. Сбои электропитания и повреждение линий связи способны одновременно затронуть несколько элементов системы, после чего преграждающие устройства должны автоматически перейти в заранее предусмотренные безопасные режимы работы. Отсутствие таких режимов в типовых решениях является распространённым недостатком.

Направления повышения надёжности и безопасности систем управления преграждающими устройствами

На основе проведённого анализа формулируется комплекс технических, организационных и программных мер, позволяющих существенно снизить влияние выявленных проблем применительно к условиям дворов МКД.

Применение распределённых архитектур с локальными контроллерами является одним из ключевых технических подходов к повышению отказоустойчивости. Локальный контроллер, размещённый вблизи преграждающего устройства, обеспечивает его автономную работу при временной потере связи с центральным узлом. Обязательным условием является проработка алгоритмов безопасного поведения устройства при сбоях: система должна исключать как неконтролируемое открытие, так и бессрочную блокировку въезда.

Резервирование каналов связи и источников электропитания позволяет сохранить работоспособность системы при воздействии внешних фак торов. Наличие резервной линии передачи данных и автономного источника питания исключает единственную точку отказа по питанию и связи. Дополнительно применяются механизмы контроля состояния канала и автоматического переключения на резервный маршрут передачи команд.

Защита канала управления от несанкционированного воздействия требует применения современных протоколов с динамической сменой кода вместо устаревших радиоканальных решений с фиксированным кодом, использования защищённых протоколов обмена данными при сетевом управлении, а также обязательной аутентификации источника команды – проверки принадлежности номера отправителя или идентификатора устройства списку авторизованных пользователей. Применение белого списка авторизованных источников команд совместно с проверкой формата и корректности сообщения позволяет отсеять несанкционированные и ошибочные воздействия на исполнительный механизм.

Повышение удобства использования при сохранении защищённости канала управления является самостоятельным направлением. Традиционное встречающееся управление по GSM-связи (с использованием голосовых звонков), несмотря на более высокий уровень контролируемости по сравнению с радиобрелоками, уступает последним в удобстве: жильцу необхо димо извлечь телефон, найти телефонный номер соответствующего ПУУ, через которое он в данный момент въезжает на территорию и дождаться совершения голосового вызова. Перспективным решением является реализация кнопочного пульта, автоматически формирующего и отправляющего команду по сети сотовой связи, что объединяет удобство физического радиобрелока и защищённость идентифицированного канала связи.

Организационные меры включают регламентацию действий операторов, распределение ролей и полномочий, обучение персонала и ведение журнала событий. На программном уровне применяются разграничение прав доступа, ограничение частоты обработки команд (защита от повторных воздействий) и корректная обработка ошибочных сообщений без зависания системы.

Перспективным направлением развития является гибридизация каналов управления – одновременная поддержка нескольких способов подачи команды (сотовая связь, локальная сеть, физический идентификатор) с единым механизмом авторизации, что повышает доступность системы и её устойчивость к отказу отдельного канала. Дальнейшая интеграция систем управления въездными устройствами в комплексные платформы безопасности МКД, в том числе с функциями видеонаблюдения и распознавания государственных номеров транспортных средств, обеспечивает переход от реактивного к проактивному управлению доступом.

Заключение

Проведённый анализ показывает, что управление воротами и шлагбаумами во дворах многоквартирных домов представляет собой область с рядом технических и организационных проблем, ещё ждущих своего решения. Наиболее распространённые решения на базе радиоканальных пультов с фиксированным кодом уязвимы к перехвату и не обеспечивают требуемого уровня контролируемости канала управления. Системы дистанционного управления, использующие сетевые или сотовые каналы связи, подвержены отказам связи и требуют проработки резервных режимов, защиты от несанкционированного доступа и механизмов авторизации команд.

Повышение надёжности и безопасности систем управления преграждающими устройствами дворов МКД достигается сочетанием распределённой архитектуры с локальными контроллерами, резервирования каналов связи и питания, защищённого идентифицированного канала управления и

организационных мер разграничения доступа. При этом ключевым критерием для данного класса объектов остаётся баланс между удобством (в частности, экономией времени) использования и уровнем защищённости – решение должно быть доступно жильцам с различным уровнем технической грамотности, не требовать специализированного оборудования и при этом обеспечивать авторизацию каждой команды управления. Совокупность сформулированных принципов составляет методическую основу для разработки программно-аппаратных комплексов управления въездными ПУУ придомовых территорий.

Список литературы:

1. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М. : Горячая линия – Телеком, 2010. – 272 с.: ил. [Электронный ресурс]. – URL : https://www.rgsec.ru/wp-content/uploads/download/skud-kniga.pdf?x55562 (Дата обращения: 12.12.2025).
2. Волхонский В.В. Системы контроля и управления доступом. Учебное пособие [Электронный ресурс]. – URL : https://books.ifmo.ru/file/pdf/1709.pdf (Дата обращения: 12.12.2025).
3. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний [Электронный ресурс]. – URL: https://skd-gate.ru/files/legislative-acts/gost-i-sp/gost_r_54831_2011_skud_upu.pdf (Дата обращения: 09.12.2025).
4. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний [Электронный ресурс]. – URL : https://armo-training.ru/assets/files/gost/gost-r-51241.pdf (Дата обращения 10.12.2025).
5. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования [Электронный ресурс]. – URL : https://ohranatruda.ru/upload/iblock/93c/4293815831.pdf (Дата обращения 10.12.2025).

List of references:

1. Vorona V.A., Tikhonov V.A. Access Control and Management Systems. – M. : Goryachaya Liniya-Telecom, 2010. – 272 p. [Electronic resource]. – URL : https://www.rgsec.ru/wp-content/uploads/download/skud-kniga.pdf?x55562 (Accessed: 12.12.2025).
2. Volkhonsky V.V. Access Control and Management Systems. Tutorial [Electronic resource]. – URL : https://books.ifmo.ru/file/pdf/1709.pdf (Accessed: 12.12.2025).
3. GOST R 54831-2011 Access Control and Management Systems. Controlled Barrier Devices. General Technical Requirements. Test Methods [Electronic resource]. – URL : https://skd-gate.ru/files/legislative-acts/gost-i-sp/gost_r_54831_2011_skud_upu.pdf (Accessed: 09.12.2025).
4. GOST R 51241-2008 Access control and management means and systems. Classification. General technical requirements. Test methods [Electronic resource]. – URL : https://armo-training.ru/assets/files/gost/gost-r-51241.pdf (Accessed: 10.12.2025).
5. GOST R 53704-2009. Comprehensive and integrated security systems. General technical requirements [Electronic resource]. – URL : https://ohranatruda.ru/upload/iblock/93c/4293815831.pdf (Accessed 10.12.2025).