

ПРОГРАММНЫЕ МЕТОДЫ УПРАВЛЕНИЯ И МОНИТОРИНГА СИСТЕМ
БЕЗОПАСНОСТИ ЗДАНИЙ

Аманбаева Гулзабира Данебай кызы

*Нукусский государственный технический университет
преподаватель-стажер кафедры "Инжиниринг кибербезопасности"*

Аннотация: В статье рассматриваются программные методы управления и мониторинга систем безопасности зданий в условиях цифровизации и роста требований к комплексной защите объектов. Показано, что традиционные системы безопасности, основанные на разрозненных аппаратных решениях, не обеспечивают необходимого уровня интеграции, оперативности реагирования и аналитической обработки данных. В работе предложен программно-ориентированный подход к построению системы управления безопасностью зданий, основанный на модульной архитектуре, централизованном сборе данных и автоматизированной обработке событий. Описаны основные функциональные модули программного обеспечения, алгоритм функционирования системы, а также принципы мониторинга и принятия решений в режиме реального времени. Отмечены преимущества предложенных программных методов с точки зрения масштабируемости, гибкости настройки и повышения эффективности эксплуатации систем безопасности. Полученные результаты могут быть использованы при разработке интеллектуальных систем управления безопасностью административных, жилых и промышленных объектов.

Ключевые слова: система безопасности здания, программное обеспечение, мониторинг, управление, автоматизация, архитектура системы, обработка событий.

ВВЕДЕНИЕ

Обеспечение безопасности зданий и сооружений является одной из приоритетных задач в современных условиях урбанизации, цифровой трансформации и роста техногенных и социальных рисков. Административные, жилые и промышленные объекты требуют комплексной защиты от несанкционированного доступа, пожаров, аварийных ситуаций и других угроз, способных нанести материальный ущерб и создать опасность для жизни людей. На практике системы безопасности зданий, как правило, включают в себя охранную сигнализацию, системы видеонаблюдения, контроль и управление доступом, пожарную сигнализацию и средства оповещения. Однако большинство существующих решений функционируют как автономные подсистемы, что существенно ограничивает возможности централизованного управления, анализа данных и оперативного реагирования на инциденты. Отсутствие единой программной платформы приводит к увеличению нагрузки на операторов, снижению эффективности мониторинга и росту эксплуатационных затрат.

В условиях активного развития информационных технологий возрастает роль программных методов управления и мониторинга, позволяющих интегрировать

различные подсистемы безопасности в единое информационное пространство. Программно-ориентированные решения обеспечивают централизованный сбор данных, их обработку в реальном времени, автоматизацию принятия решений и гибкую настройку сценариев реагирования на события. Это особенно актуально для объектов с высокой плотностью пользователей и сложной инфраструктурой. Целью данной статьи является анализ и описание программных методов управления и мониторинга систем безопасности зданий, а также обоснование архитектурных и функциональных решений программного обеспечения, обеспечивающего эффективную и масштабируемую работу комплексной системы безопасности. В рамках работы рассматриваются ключевые компоненты программной системы, принципы её функционирования и преимущества по сравнению с традиционными подходами.

Анализ существующих систем безопасности зданий

В условиях цифровизации инфраструктуры и усложнения архитектуры современных зданий системы безопасности приобретают всё более комплексный характер. Современное здание представляет собой не только физический объект, но и сложную киберфизическую систему, в которой взаимодействуют инженерные коммуникации, информационные сети, программные платформы и пользователи. В этой связи системы безопасности зданий перестают быть исключительно набором охранных или пожарных средств и трансформируются в интегрированные программно-аппаратные комплексы, обеспечивающие мониторинг, управление и анализ состояния объекта в режиме реального времени. Анализ существующих систем безопасности показывает, что эффективность защиты напрямую зависит от уровня программной интеграции и степени автоматизации процессов управления. Международный опыт разработки и внедрения систем безопасности зданий характеризуется ориентацией на централизованные программные платформы, обеспечивающие интеграцию различных подсистем в единое информационное пространство. В странах Европы, США и Восточной Азии системы безопасности активно внедряются в рамках концепций «умного здания» и «умного города», где программное обеспечение играет ключевую роль в сборе, обработке и интерпретации данных. Такие системы, как правило, объединяют видеонаблюдение, контроль и управление доступом, охранную и пожарную сигнализацию, а также системы оповещения и управления эвакуацией. Центральным элементом является программная платформа, обеспечивающая унифицированный интерфейс управления и мониторинга, что существенно снижает нагрузку на операторов и повышает оперативность реагирования.

Одной из характерных особенностей международных решений является использование модульной архитектуры программного обеспечения. Каждый функциональный компонент реализуется в виде отдельного программного модуля, который может быть добавлен, модифицирован или заменён без необходимости полной переработки системы. Это обеспечивает высокую масштабируемость и адаптивность решений, что особенно важно для крупных объектов, таких как бизнес-

центры, аэропорты, медицинские учреждения и промышленные комплексы. Программные методы управления в таких системах включают корреляцию событий из различных источников, автоматическую классификацию инцидентов и формирование сценариев реагирования в зависимости от уровня угрозы. В международной практике также активно применяются программные методы аналитической обработки данных. Например, системы видеонаблюдения дополняются программными модулями видеоаналитики, позволяющими автоматически обнаруживать подозрительное поведение, скопления людей или несанкционированное проникновение в охраняемые зоны. Аналогичным образом данные от датчиков доступа и сигнализации используются для построения временных и пространственных моделей поведения пользователей внутри здания.

В отличие от международных подходов, локальные системы безопасности зданий, широко применяемые в странах Центральной Азии, включая Узбекистан, в большинстве случаев характеризуются фрагментарностью и ограниченным уровнем программной интеграции. На практике системы видеонаблюдения, пожарной сигнализации и контроля доступа часто внедряются как независимые решения, поставляемые различными производителями и функционирующие на основе собственных программных средств. Это приводит к отсутствию единого центра управления и необходимости использования нескольких программных интерфейсов для мониторинга состояния объекта. Во многих административных зданиях, образовательных учреждениях и жилых комплексах программное обеспечение систем безопасности выполняет вспомогательную функцию и используется преимущественно для визуализации видеопотоков или регистрации тревожных событий. Программные методы анализа данных и автоматизации управления либо отсутствуют, либо реализованы на минимальном уровне. В результате оператор системы безопасности вынужден самостоятельно анализировать поступающую информацию и принимать решения в ручном режиме, что существенно увеличивает время реакции на инциденты и повышает вероятность ошибок.



Рис.1. Структурная схема программно-интегрированной системы безопасности здания

Дополнительной проблемой локальных систем является ограниченная масштабируемость и сложность модернизации. При необходимости расширения здания или добавления новых функциональных подсистем требуется закупка дополнительного оборудования и установка специализированного программного обеспечения, которое не всегда совместимо с уже существующей инфраструктурой. Отсутствие стандартизированных программных интерфейсов и протоколов взаимодействия приводит к росту затрат на сопровождение системы и снижению её надёжности в долгосрочной перспективе. Рисунок 1 демонстрирует общую структуру системы безопасности здания, в которой основные подсистемы (видеонаблюдение, контроль доступа, пожарная и охранная сигнализация) интегрированы в единую



программную платформу управления. Платформа обеспечивает централизованный сбор и обработку данных, а также формирование управляющих воздействий. Результаты мониторинга отображаются в центре мониторинга и доступны через мобильные устройства, что обеспечивает оперативное реагирование на инциденты. Представленная структура подчёркивает ключевую роль программного обеспечения в интеграции и автоматизации процессов безопасности.

Сравнительный анализ международных и локальных систем безопасности зданий показывает, что ключевым фактором эффективности является не столько уровень аппаратного оснащения, сколько качество программных методов управления и мониторинга. Международные системы демонстрируют преимущества в части централизованного управления, автоматизации обработки событий и использования аналитических инструментов. Следует отметить, что большинство существующих систем безопасности, как международных, так и локальных, реализуют преимущественно реактивный подход к управлению. Программное обеспечение фиксирует факт возникновения инцидента и инициирует заранее заданные действия, не обеспечивая полноценной поддержки принятия решений и прогнозирования угроз. Это особенно критично в условиях сложных объектов с большим количеством пользователей и высокой плотностью событий, где требуется не только оперативное реагирование, но и превентивное управление безопасностью.

Архитектура программного обеспечения системы управления безопасностью зданий является ключевым фактором, определяющим её надёжность, масштабируемость и функциональную полноту. В условиях современного здания, представляющего собой сложный объект с большим количеством инженерных и информационных подсистем, программное обеспечение должно обеспечивать не только сбор и отображение данных, но и их интеллектуальную обработку, поддержку принятия решений и автоматизацию управляющих воздействий. Именно архитектурные решения определяют, насколько эффективно система сможет интегрировать разнородные источники данных и обеспечить устойчивую работу в режиме реального времени. На каждом уровне архитектуры реализуются специализированные программные модули, взаимодействующие между собой посредством стандартизированных интерфейсов и протоколов обмена данными.

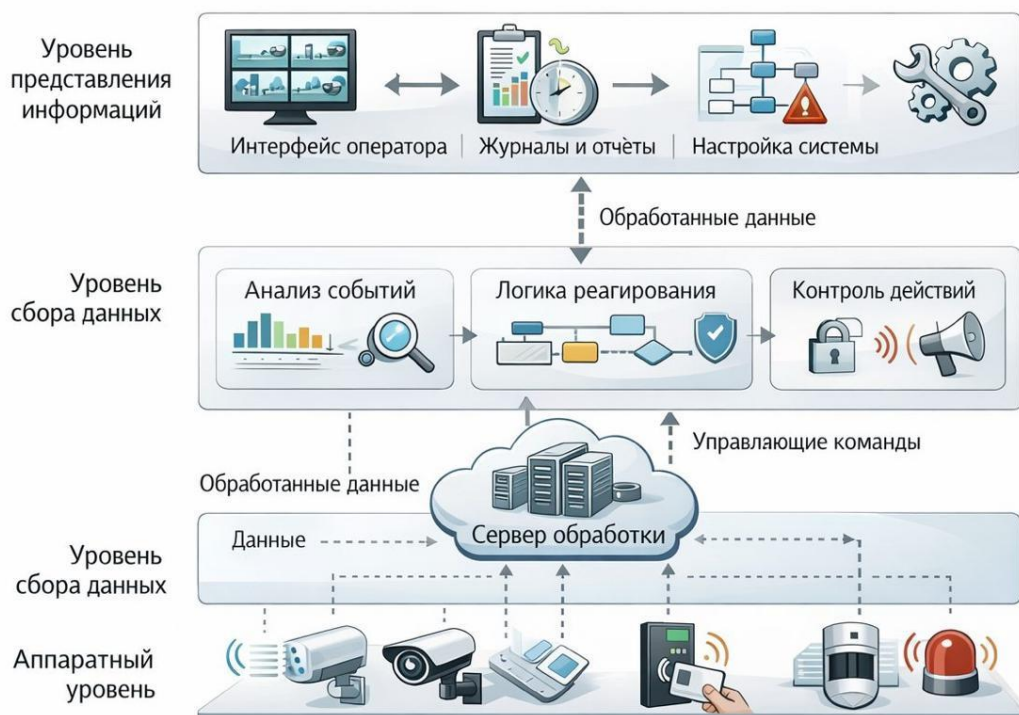


Рис.2. Многоуровневая архитектура программного обеспечения управления безопасностью здания

Первый уровень архитектуры — уровень сбора данных — предназначен для взаимодействия с аппаратными средствами системы безопасности. К данному уровню относятся программные драйверы и интерфейсные модули, обеспечивающие получение данных от датчиков движения, видеокамер, контроллеров доступа, пожарных извещателей и других устройств. Программное обеспечение уровня сбора данных выполняет функции первичной обработки, фильтрации и нормализации информации, приводя её к унифицированному виду для последующей передачи на уровень обработки. Рисунок 2 отражает многоуровневую архитектуру программного обеспечения системы управления безопасностью здания, включающую аппаратный уровень, уровень сбора данных, уровень обработки и уровень представления информации. Аппаратный уровень формирует первичные данные с датчиков и устройств безопасности, которые передаются на сервер обработки. На уровне анализа и реагирования выполняется обработка событий, принятие решений и формирование управляющих команд. Уровень представления обеспечивает взаимодействие с пользователем через интерфейс оператора, журналы, отчёты и средства настройки системы.

Уровень обработки данных представляет собой центральное звено архитектуры программного обеспечения управления безопасностью зданий. На данном уровне реализуются основные программные методы анализа, корреляции и интерпретации событий. Сюда входят модули обработки тревожных сигналов, логики принятия

решений, а также механизмы управления исполнительными устройствами. Программное обеспечение данного уровня обеспечивает агрегацию данных, поступающих из различных подсистем безопасности, и формирует целостное представление о текущем состоянии объекта. Использование централизованной обработки позволяет выявлять взаимосвязи между событиями, которые невозможно определить при разрозненной работе отдельных подсистем. Одной из важнейших задач уровня обработки является реализация сценариев реагирования на инциденты. В архитектуре программного обеспечения такие сценарии задаются в виде правил и алгоритмов, определяющих последовательность действий при возникновении определённых условий.

Следующим уровнем архитектуры является уровень представления и взаимодействия с пользователем. Данный уровень включает в себя графические интерфейсы оператора, панели мониторинга, отчётные модули и средства администрирования системы. Программное обеспечение уровня представления должно обеспечивать наглядное и интуитивно понятное отображение информации о состоянии безопасности здания, включая визуализацию тревожных событий, планов помещений и временных диаграмм. Особое значение имеет возможность настройки интерфейса под различные роли пользователей, такие как оператор, администратор или технический специалист. Важным архитектурным принципом программного обеспечения управления безопасностью является модульность. Модульная архитектура позволяет разрабатывать и внедрять функциональные компоненты системы независимо друг от друга, что существенно упрощает процесс расширения и модернизации. Например, добавление нового модуля аналитики или интеграция дополнительной подсистемы безопасности может быть выполнена без остановки работы всей системы. Такой подход особенно актуален для зданий, инфраструктура которых развивается поэтапно.

С точки зрения обеспечения надёжности архитектура программного обеспечения должна предусматривать механизмы резервирования и восстановления. В системах безопасности недопустимы длительные простои, поскольку они напрямую влияют на уровень защищённости объекта. Поэтому архитектурные решения должны включать резервирование серверных компонентов, дублирование каналов связи и сохранение данных о событиях в устойчивых хранилищах. Программное обеспечение должно обеспечивать корректное восстановление работы системы после сбоев без потери критически важной информации.

Отдельного внимания заслуживает вопрос масштабируемости архитектуры программного обеспечения. Современные здания и комплексы могут включать сотни и тысячи устройств безопасности, количество которых со временем увеличивается. Архитектура системы должна обеспечивать возможность горизонтального и вертикального масштабирования, позволяя добавлять новые узлы обработки данных и расширять функциональность без кардинальных изменений программной структуры. Использование распределённых вычислительных моделей и сетевых сервисов способствует решению данной задачи. В контексте информационной безопасности



архитектура программного обеспечения управления безопасностью зданий должна учитывать угрозы несанкционированного доступа к данным и управляющим функциям системы. Это требует реализации механизмов аутентификации, авторизации и разграничения прав доступа пользователей. Архитектурные решения должны обеспечивать защиту каналов передачи данных и целостность информации, поскольку компрометация программного обеспечения может привести к серьёзным последствиям для безопасности объекта.

Алгоритм функционирования программной системы управления и мониторинга безопасности зданий определяет логику взаимодействия всех компонентов архитектуры и обеспечивает целостность процессов сбора данных, их обработки и формирования управляющих воздействий. В отличие от традиционных систем безопасности, где программное обеспечение выполняет преимущественно роль интерфейса отображения информации, в программно-ориентированном подходе алгоритм становится центральным элементом системы, реализующим функции анализа, принятия решений и автоматического реагирования на события. Основой алгоритма является непрерывный цикл обработки данных, начинающийся с поступления информации от аппаратных средств безопасности. Данные, получаемые от датчиков движения, контроллеров доступа, пожарных извещателей и систем видеонаблюдения, поступают в программную систему в виде потоков событий. На данном этапе алгоритм обеспечивает синхронизацию входных данных, их временную маркировку и проверку на корректность. Это позволяет исключить ложные срабатывания, связанные с техническими сбоями или ошибками передачи информации.

Рис.3. Модульная структура программной системы управления безопасностью здания

После первичной обработки данные передаются на этап логической интерпретации, где осуществляется классификация событий по типу и уровню критичности. Алгоритм функционирования системы предполагает использование

заранее определённых правил, определяющих, какие события относятся к нормальным, а какие требуют повышенного внимания. Например, однократное срабатывание датчика движения в рабочее время может быть отнесено к допустимым событиям, тогда как аналогичное срабатывание в ночное время автоматически классифицируется как потенциальная угроза. Такой подход позволяет программной системе адаптировать логику реагирования в зависимости от контекста. Рисунок 3 иллюстрирует модульную структуру программной системы управления безопасностью здания, в которой центральным элементом является программная платформа управления. Платформа обеспечивает взаимодействие функциональных модулей мониторинга, управления доступом, обработки событий и сценариев реагирования. Каждый модуль выполняет специализированные задачи и обменивается данными через централизованное программное ядро. Представленная структура обеспечивает гибкость, масштабируемость и возможность поэтапного расширения системы безопасности.

Следующим этапом алгоритма является корреляция событий, поступающих из различных подсистем безопасности. На этом уровне программная система анализирует взаимосвязи между событиями, происходящими в разных зонах здания и в различные моменты времени. Корреляция позволяет выявлять сложные сценарии угроз, которые не могут быть обнаружены при анализе отдельных сигналов. Например, одновременное срабатывание системы контроля доступа и видеонаблюдения в охраняемой зоне может свидетельствовать о попытке несанкционированного проникновения и требовать немедленного реагирования.

Особое место в алгоритме функционирования системы занимает механизм принятия решений. На основе результатов анализа и корреляции событий программное обеспечение формирует управляющие воздействия в соответствии с заданными сценариями реагирования. Такие сценарии представляют собой формализованные алгоритмы действий, определяющие последовательность операций при возникновении конкретных ситуаций. Например, при обнаружении пожара алгоритм может автоматически активировать систему оповещения, разблокировать эвакуационные выходы и передать информацию в соответствующие службы. Важным требованием к алгоритму является возможность гибкой настройки сценариев без необходимости изменения исходного кода программного обеспечения.

Алгоритм функционирования системы также предусматривает взаимодействие с пользователем в процессе принятия решений. В ситуациях, не требующих немедленного автоматического реагирования, программное обеспечение может формировать рекомендации для оператора, предоставляя ему информацию о возможных вариантах действий. Такой режим работы позволяет сочетать автоматизацию с контролем со стороны человека, что особенно важно для сложных и нестандартных ситуаций. Программная система при этом сохраняет все действия оператора в журнале событий, обеспечивая возможность последующего анализа.

Неотъемлемой частью алгоритма является механизм обратной связи, обеспечивающий контроль выполнения управляющих воздействий. После инициирования действий, таких как блокировка доступа или включение оповещения,

программное обеспечение получает подтверждение от исполнительных устройств и фиксирует результаты в системе. Это позволяет своевременно обнаруживать неисправности и корректировать работу системы в случае отклонений от заданного сценария. Алгоритм функционирования системы предусматривает обработку ошибок и переход в безопасное состояние при возникновении критических сбоев.

Дополнительным элементом алгоритма является накопление и анализ статистических данных о работе системы безопасности. Программное обеспечение осуществляет хранение информации о событиях, действиях операторов и состоянии оборудования в базе данных. На основе этих данных формируются отчёты, позволяющие оценить эффективность функционирования системы и выявить потенциальные уязвимости. Такой аналитический подход создаёт предпосылки для внедрения методов прогнозирования и превентивного управления безопасностью зданий.

Программная реализация системы управления и мониторинга безопасности зданий основана на принципах модульности, масштабируемости и надёжности, что позволяет адаптировать программное обеспечение под объекты различного назначения и сложности. При разработке системы использовался программно-ориентированный подход, при котором ключевое внимание уделялось логике обработки событий, взаимодействию модулей и обеспечению устойчивой работы в режиме реального времени. Архитектурные и алгоритмические решения, описанные в предыдущих разделах, были реализованы в виде функционально завершённого программного комплекса, обеспечивающего централизованное управление подсистемами безопасности.

Программное обеспечение реализовано в виде серверно-клиентской системы, где серверная часть отвечает за сбор, обработку и хранение данных, а клиентская — за визуализацию и управление. Серверный компонент включает модули взаимодействия с аппаратными средствами безопасности, обработки событий и управления сценариями реагирования. Клиентская часть реализует пользовательские интерфейсы для операторов и администраторов системы, обеспечивая доступ к информации о текущем состоянии объекта, журналам событий и средствам настройки параметров системы. Такой подход позволил обеспечить чёткое разделение ответственности между компонентами и повысить устойчивость системы к отказам отдельных элементов.

В процессе реализации особое внимание уделялось вопросам совместимости программного обеспечения с разнородными аппаратными средствами. Для этого были реализованы унифицированные программные интерфейсы, обеспечивающие взаимодействие с различными типами датчиков и контроллеров. Использование абстрактных интерфейсов позволило снизить зависимость программного обеспечения от конкретных производителей оборудования и упростить процесс интеграции новых устройств. Это особенно важно в условиях практической эксплуатации, где инфраструктура безопасности может расширяться и модернизироваться поэтапно.

Одним из ключевых аспектов программной реализации является обеспечение надёжности и отказоустойчивости системы. Программное обеспечение

предусматривает механизмы резервирования данных, автоматического восстановления соединений с аппаратными средствами и сохранения критически важной информации о событиях. В случае возникновения сбоев в работе отдельных компонентов система переходит в безопасное состояние, обеспечивая сохранение функциональности базовых подсистем безопасности. Такие меры позволяют минимизировать риск потери данных и обеспечить непрерывность мониторинга.

Практическое внедрение разработанной программной системы управления безопасностью было ориентировано на условия эксплуатации в зданиях с высокой интенсивностью событий, таких как административные и образовательные объекты. В ходе опытной эксплуатации система обеспечивала централизованный мониторинг состояния подсистем безопасности и автоматическую обработку тревожных событий. Использование программных методов корреляции данных позволило сократить количество ложных срабатываний и повысить точность классификации инцидентов, что положительно сказалось на работе операторов системы.

Результаты внедрения показали, что программно-ориентированный подход позволяет существенно снизить время реакции на инциденты по сравнению с традиционными разрозненными системами. Автоматизация сценариев реагирования обеспечила оперативное выполнение действий без необходимости постоянного вмешательства оператора. Это особенно важно в критических ситуациях, где задержка в принятии решений может привести к серьёзным последствиям. Кроме того, централизованный интерфейс управления упростил процесс мониторинга и снизил нагрузку на персонал службы безопасности.

Дополнительным результатом внедрения стало повышение прозрачности и управляемости системы безопасности здания. Накопление и анализ данных о событиях, действиях операторов и состоянии оборудования позволили сформировать аналитическую базу для оценки эффективности работы системы. На основе полученных данных возможно выявление узких мест в инфраструктуре безопасности и планирование мероприятий по её совершенствованию. Таким образом, программная система выполняет не только оперативные, но и аналитические функции, поддерживая процессы управления безопасностью на стратегическом уровне. Эксплуатация программного обеспечения также показала его гибкость в части адаптации под изменяющиеся условия. Возможность настройки сценариев реагирования и параметров мониторинга без изменения программного кода позволила оперативно учитывать специфику объекта и требования пользователей. Это подтверждает целесообразность использования модульной архитектуры и программных методов управления, ориентированных на долгосрочную эксплуатацию и развитие системы.

В целом, результаты программной реализации и внедрения свидетельствуют о высокой эффективности предложенного подхода к управлению и мониторингу систем безопасности зданий. Разработанное программное обеспечение обеспечивает интеграцию разнородных подсистем, автоматизацию обработки событий и повышение уровня защищённости объектов. Полученные результаты подтверждают практическую значимость программных методов управления безопасностью и создают основу для

дальнейших исследований в направлении интеллектуализации систем безопасности зданий.

Заклучение

В ходе проведённого исследования были рассмотрены программные методы управления и мониторинга систем безопасности зданий, ориентированные на интеграцию разнородных подсистем в рамках единой программной платформы. Показано, что в современных условиях традиционные подходы, основанные на автономной работе отдельных технических решений, не обеспечивают необходимого уровня оперативности, гибкости и аналитической поддержки процессов управления безопасностью. В связи с этим программно-ориентированный подход к построению систем безопасности зданий является обоснованным и перспективным направлением развития. В статье проведён анализ существующих международных и локальных систем безопасности зданий, который позволил выявить ключевые проблемы, связанные с фрагментацией инфраструктуры, ограниченной масштабируемостью и высокой зависимостью от конкретных производителей оборудования. Установлено, что основным фактором повышения эффективности систем безопасности является не только уровень аппаратного оснащения, но и качество программных методов обработки данных, корреляции событий и автоматизации принятия решений. Это подтверждает необходимость перехода к централизованным программным решениям, обеспечивающим целостное управление безопасностью объектов.

Предложенная архитектура программного обеспечения управления безопасностью зданий основана на многоуровневом и модульном подходе, обеспечивающем разделение функций сбора данных, обработки информации и взаимодействия с пользователем. Такая архитектура позволяет повысить надёжность и отказоустойчивость системы, упростить процесс её расширения и адаптации под конкретные условия эксплуатации. Реализация алгоритма функционирования системы, включающего сбор, анализ и интерпретацию данных, а также формирование сценариев реагирования, обеспечивает снижение времени реакции на инциденты и уменьшение влияния человеческого фактора.

Результаты программной реализации и практического внедрения подтвердили эффективность предложенных программных методов управления и мониторинга систем безопасности зданий. Централизованная обработка событий, автоматизация сценариев реагирования и использование аналитических инструментов позволили повысить прозрачность работы системы и улучшить качество управления безопасностью объекта. Полученные результаты свидетельствуют о практической применимости разработанного программного решения и его соответствии современным требованиям к системам безопасности зданий.

1. S. Mitra, "Gesture Recognition: An Overview," IEEE Transactions on Systems, Man, and Cybernetics, 2020.
2. LI, X.; WU, X.; ZHANG, Y. Deep learning for sign language recognition: A review. IEEE Transactions on Neural Networks and Learning Systems, v. 31, n. 8, p. 2612–2630, 2020.
3. Fei Wang, Ronglin Hu, Ying Jin, «Research on gesture image recognition method based on transfer learning», Procedia Computer Science, Volume 187, 2021, Pages 140-145,
4. Seitnazarov K. K., Turemuratova B. K., Aytanov A. K. Stages and Methods of Data Collection for Developing an Artificial Intelligence Model for Recognizing Letters of the Karakalpak Sign Language //2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM). – IEEE, 2024. – С. 2530-2534.
5. К.К.Сеитназаров, Б.К.Туремуратова. Разница Между Глубоким И Машинным Обучением // Periodica Journal of Modern Philosophy, Social, 2022
6. Murphy, Kevin P. Machine learning: a probabilistic perspective. MIT press, 2012.
7. К.К.Сеитназаров, Б.К.Туремуратова. Применение технологии искусственного интеллекта в системе дистанционного образования// Новости образования: исследование в XXI веке, 2022.