Научная статья
УДК 614.84; DOI: 10.61260/1998-8990-2025-4-182-200

МОДУЛЬНАЯ МОДЕЛЬ СИСТЕМЫ ОПОВЕЩЕНИЯ И УПРАВЛЕНИЯ ЭВАКУАЦИЕЙ ЛЮДЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ IOT

✉**Мельников Григорий Олегович;**
Синещук Юрий Иванович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***grinyam@list.ru***

Аннотация. Раскрывается роль информационной среды в обеспечении безопасности современного общества. Исследованы возможности и перспективы внедрения технологии Интернета вещей (Internet of Things, IoT) в системы оповещения и управления эвакуацией людей. Рассматриваются преимущества данного подхода, включая повышение точности мониторинга обстановки, сокращение времени реагирования на чрезвычайные ситуации. Особое внимание уделено вопросам интеграции устройств IoT с существующими системами пожарной сигнализации и видеонаблюдения, а также возможностям анализа больших объемов данных (Big Data) на объектах с массовым пребыванием людей. Проведен анализ применения интеллектуальных сенсоров, технологий машинного обучения и адаптивных алгоритмов управления эвакуацией, представлена модульная архитектура системы оповещения и управления эвакуацией людей. Рассматриваются преимущества на основе технологии IoT для объектов с массовым пребыванием людей. Рассмотрены функциональные модули системы – от обнаружения пожара и анализа данных до адаптивного планирования маршрутов эвакуации и интеллектуального оповещения. Предложен алгоритм взаимодействия модулей, обеспечивающих замкнутый цикл «обнаружение – анализ – решение – действие – контроль – защита». Особое внимание уделено вопросам кибербезопасности, защищенным протоколам передачи данных, а также механизмам обеспечения целостности и достоверности информации. Научная новизна работы заключается в разработке адаптивной модульной модели системы оповещения и управления эвакуацией людей. Рассматриваются преимущества с элементами предиктивного управления и встроенными средствами киберзащиты. Практическая значимость заключается в возможности применения предложенной архитектуры при проектировании интеллектуальных систем противопожарной защиты нового поколения и в совершенствовании расчетов пожарного риска на объектах с массовым пребыванием людей.

Ключевые слова: пожарная безопасность, массовое пребывание людей, управление эвакуацией, новые информационные технологии, интернет вещей, адаптивные системы, модульная архитектура, кибербезопасность

Для цитирования: Мельников Г.О., Синещук Ю.И. Модульная модель системы оповещения и управления эвакуацией людей на основе технологии IOT // Проблемы управления рисками в техносфере. 2025. № 4 (76). С. 182–200. DOI: 10.61260/1998-8990-2025-4-182-200.

Scientific article

A MODULAR MODEL OF WARNING SYSTEM AND EVACUATION MANAGEMENT BASED ON IOT TECHNOLOGY

✉**Melnikov Grigoriy O.;**
Sineshchuk Yury I.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***grinyam@list.ru***

Abstract. This article explores the role of the information environment in ensuring the security of modern society. It examines the potential and prospects for integrating Internet of Things technology into warning system and evacuation management. The advantages of this approach, including improved situational monitoring accuracy and reduced emergency response times, are discussed. Particular attention is paid to integrating IoT devices with existing fire alarm and video surveillance systems, as well as the potential for analyzing big data at crowded facilities. The article analyzes the use of intelligent sensors, machine learning technologies, and adaptive evacuation management algorithms, and presents a modular IoT-based PES architecture for crowded facilities. The article examines the system's functional modules, ranging from fire detection and data analysis to adaptive evacuation route planning and intelligent alerting. An algorithm for interaction between modules is proposed, providing a closed-loop «detection-analysis-decision-action-control-protection» process. Particular attention is paid to cybersecurity issues, secure data transmission protocols, and mechanisms for ensuring the integrity and reliability of information. The scientific novelty of this work lies in the development of an adaptive modular model of a fire safety system with predictive control elements and integrated cybersecurity tools. The practical significance lies in the potential application of the proposed architecture in the design of next-generation intelligent fire safety systems and in improving fire risk assessments at facilities with mass stay of people.

Keywords: fire safety, high-occupancy buildings, evacuation management, new information technologies, internet of things, adaptive systems, modular architecture, cybersecurity

For citation: Melnikov G.O., Sineshchuk Yu.I. A modular model of warning system and evacuation management based on iot technology // Problemy upravleniya riskami v tekhnosfere = Problems of risk management in the technosphere. 2025. № 4 (76). P. 182–200. DOI: 10.61260/1998-8990-2025-4-182-200.

Введение

Современные города характеризуются высоким уровнем урбанизации и концентрации инфраструктуры, что создает дополнительные риски возникновения чрезвычайных ситуаций различного характера. Обеспечение пожарной безопасности на различных объектах защиты с массовым пребыванием людей в условиях постоянного роста их конструктивной сложности и функциональности и, как следствие, расширения спектра угроз возникновения пожаров, а в более общем случае – чрезвычайных ситуаций, – это задача, требующая применения современных технологий, обеспечивающих оперативное, динамическое реагирование на проявление опасных факторов, нарушающих возможности нормальной жизнедеятельности человека. Сложность этой проблемы заключается в ее многогранности: от оценки вероятности возгорания до мониторинга состояния зданий и человеческого поведения в экстремальных ситуациях. Традиционные системы противопожарной защиты (СПЗ), включающие в общем случае в свой состав систему пожарной сигнализации (СПС), систему оповещения и управления эвакуацией (СОУЭ), системы пожаротушения и противодымной защиты, – несмотря на их многолетнюю практику применения, все чаще сталкиваются с ограничениями, связанными с отсутствием гибкости, способности к оперативной адаптации и учета динамических факторов, таких как изменения в эксплуатационных условиях, потоках людей

или температурных колебаниях. Эффективность работы существующих СОУЭ зависит от своевременности обнаружения угрозы, скорости передачи сигнала тревоги и четкости организации мероприятий по спасению людей. Используемые в этих системах методы обеспечения безопасности часто оказываются недостаточно эффективными вследствие ограниченной возможности оперативно реагировать на изменения окружающей среды и недостаточной информированности людей во время эвакуации.

Вопрос становится особенно острым, когда речь идет о современных многофункциональных зданиях с высокой плотностью людей, таких как торговые комплексы, стадионы, театры, кинотеатры, учебные заведения и т.д., функционирование которых предполагает широкое применение информационных систем и технологий. Здесь каждый фактор способен значительно повлиять на развитие чрезвычайной ситуации и поэтому системы безопасности таких объектов должны обладать способностью обрабатывать большие объемы разнообразной информации и формировать соответствующие управляющие воздействия в режиме реального времени, что может быть обеспечено применением новых информационных технологий (НИТ).

Цель данного исследования заключается в изучении потенциала внедрения НИТ в СПЗ, в частности IoT в СОУЭ. Работа сосредоточена на рассмотрении технических аспектов (сенсоры, механизмы передачи данных, протоколы) с преимущественным вниманием технологии IoT, которая в отличие от других НИТ обеспечивают непрерывный мониторинг и возможность адаптации системы в реальном времени без участия человека, что особенно критично в условиях пожара. А также с упором на выявление изменений, которые происходят в алгоритмах функционирования СОУЭ при учете динамичных данных.

Для достижения поставленной цели потребовалось решение следующих задач:

– провести эволюционный анализ среды обитания людей с обоснованием роли и места техносферы и информационной сферы жизнедеятельности человека;

– изучить существующие НИТ и возможности их применения в сфере пожарной безопасности;

– исследовать потенциал применения IoT для прогнозирования развития пожаров и управления эвакуацией;

– определить ключевые параметры, собираемые IoT-устройствами, которые обеспечивают повышение эффективности процессов эвакуации при пожарах в современных многофункциональных зданиях с массовым пребыванием людей;

– разработать модульную модель СОУЭ на основе технологии IoT.

Аналитическая часть

Стоит отметить, что в целом современный цивилизационный, технологический этап развития человечества характеризуется глобальным, интенсивным проникновением информационных систем и технологий во все области жизнедеятельности человека, общества, государства, приводит к формированию и постоянному возрастанию роли «информационной сферы» как доминирующей сферы жизнедеятельности человека, общества, государства [1, 2].

Попытки адекватно описать ключевые особенности текущего состояния цивилизации привели к переходу от концепций в 1985 г. VUCA-мира (Volatility – изменчивость, Uncertainty – неопределенность, Complexity – сложность, Ambiguity – двусмысленность) до в 2016 г. BANI-мира (Brittle – хрупкий, Anxious – тревожный, Nonlinear – нелинейный, Incomprehensible – непостижимый) и в 2022 г. – SHIVA-мира (Split – расщепленный, Horrible – ужасный, Inconceivable – невообразимый, Vicious – беспощадный, Arising – возрождающийся) [3].

В работе [4] обосновывается тезис о том, что современный турбулентный (бурный, хаотичный, неустойчивый) мир существенным образом изменяет взгляды и подходы к обеспечению безопасности, требует системного мультидисциплинарного взгляда на эту проблему.

Подчеркивая технологичность, технократизм взаимодействия человека и природы, на смену достаточно философскому, теоретическому понятию – «ноосфера» пришло понятие – «техносфера», определяемое как часть биосферы, где современный человек в процессе жизнедеятельности меняет среду вокруг себя, используя различные технические средства, системы и технологии [5]. Отличительной особенностью, характеризующей уровень развития техносферы, является широкое использование киберфизических (cyber-physical system – CPS) и социотехнических информационных систем. Примеры CPS включают промышленные системы управления, системы водоснабжения, робототехнические системы, интеллектуальные сети и т.д. К числу социотехнических (организационно-технических) можно отнести любую информационную систему, в которой человек (оператор, руководитель) принимает решение для осуществления воздействий на объект управления. Доминирующей тенденцией сегодняшнего дня можно назвать функциональную интеграцию киберфизических и социотехнических систем в виде социо-киберфизических систем, поскольку в этих системах происходит совмещение объектов различной природы, а по составу функций управления эти системы сравнялись с функциями управления человека-оператора или лица, принимающего решения [6–8].

Функционирование киберфизических и социотехнических информационных систем предполагает формирование определенной информационной сферы (среды, пространства).

Тогда, с определенной долей условности, современное представление о среде обитания человека можно отразить в виде, представленном на рис. 1 [9, 10].

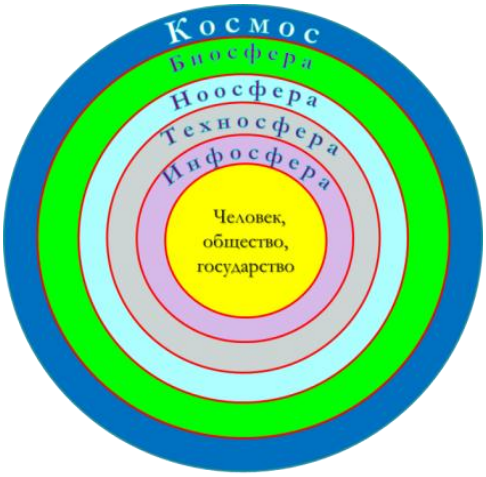

Рис. 1. **Модель среды обитания человека**

Таким образом, реалии современной цивилизации можно характеризовать как стадию киборгизации (симбиоза человека, техники и искусственного интеллекта), когда при осуществлении целенаправленных действий человек использует постоянно развивающиеся, сменяющие друг друга технологии, которые, в свою очередь, порождают и новый спектр угроз, требующих своего учета при проектировании и эксплуатации современных СПЗ [11].

Коммуникационные технологии обеспечивают интенсивный, устойчивый обмен мультимедийной информацией, улучшая координацию между различными функциональными устройствами. Технологии анализа больших данных (Big data) позволяют выявлять тенденции, закономерности в проявлении тех или иных деструктивных явлений и принимать упреждающие меры. Технологии искусственного интеллекта (ИИ, Artificial Intelligence – AI), интернета вещей (Internet of Things – IoT), «умного города» (smart-city) обеспечивают распознание объектов и ситуаций, контролируют общественные пространства, инфраструктуру, транспортные потоки [12, 13].

Внедрение робототехнических систем, технологий IoT, ИИ, сетей нового поколения (5G) в СПЗ открывает широкие возможности для повышения эффективности обнаружения угроз, оптимизации маршрутов эвакуации и автоматизации управления чрезвычайными ситуациями [14]. Наиболее перспективным направлением видится применение технологии IoT в различном сочетании с другими современными технологиями.

IoT – это технология объединения физических устройств в единую сеть, обеспечивающую сбор, передачу и обработку данных в реальном времени без участия человека. IoT способен придать СПЗ новый уровень функциональности. Технологии IoT обладают значительным потенциалом для повышения эффективности функционирования систем оповещения и эвакуации благодаря способности мгновенно фиксировать изменение условий и адаптироваться к возникающим угрозам. Интеллектуальные датчики, которые непрерывно мониторят широкий спектр параметров – от температуры и уровня задымления до концентрации опасных газов и других опасных факторов пожара, создают базу для формирования динамичных решений в режиме реального времени. Сложные механизмы сбора и обработки данных, построенные на облачных платформах и устойчивых протоколах связи, открывают доступ к проактивным методам управления безопасностью, что позволяет не только своевременно реагировать на чрезвычайные ситуации, но и прогнозировать вероятные угрозы, предотвращая риски.

Однако интеграция IoT в СПЗ имеет множество как технологических, так и методологических вызовов. Следует проанализировать ключевые особенности, касающиеся потенциала IoT, выявить проблемы применения этой технологии, проанализировать возможные пути модернизации СПЗ.

Например, исследования [15] и [16] предлагают довольно нестандартный подход для повышения эффективности процесса эвакуации людей. В работе рассматривается интеллектуальная система мониторинга и оповещения на основе IoT с использованием автономных роботов-проводников (рис. 2).

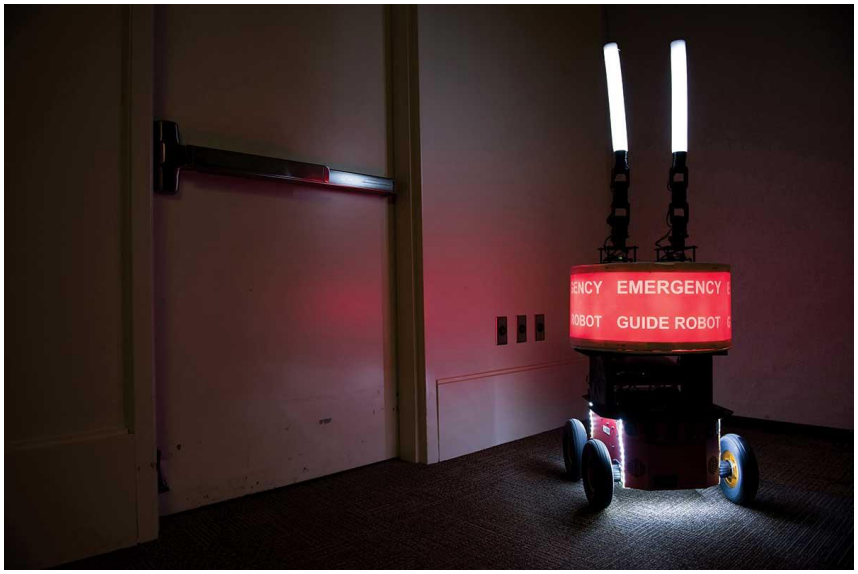

Рис. 2. **Автономный робот-проводник**

Работа данных интеллектуальных роботов основана на методе глубокого обучения с подкреплением (Deep Reinforcement Learning). При таком методе машинного обучения робот обучается взаимодействовать с окружением, получая «награды» за полезные действия и «штрафы» за ошибки. В результате у агента вырабатывается стратегия, позволяющая максимизировать ожидаемое суммарное вознаграждение (рис. 3).

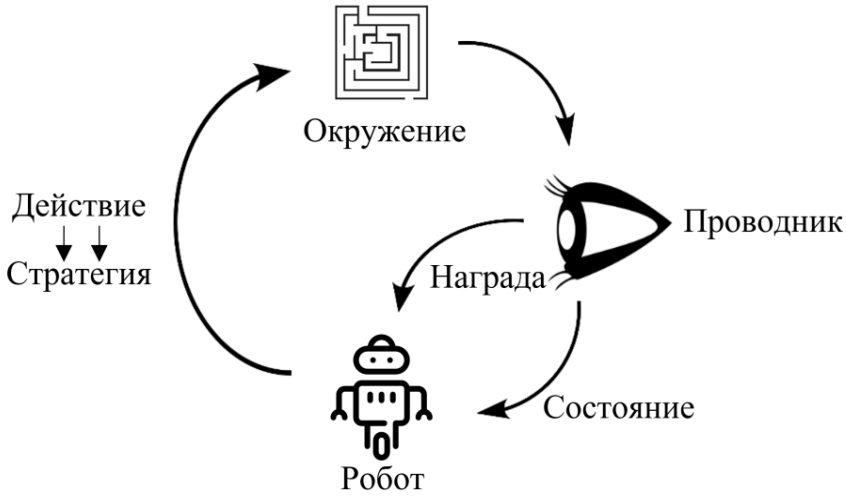

Рис. 3. **Схема сценария обучения с подкреплением (Deep Reinforcement Learning)**

Поскольку при пожаре даже высокотехнологичные роботы могут терять функциональность, если люди не поймут их указания или не доверятся им, поэтому помимо обучения с подкреплением используется метод взаимодействия с людьми (Human-Robot Interaction), в котором предполагается возможность безопасного физического контакта и взаимодействия роботов с людьми. При этом предлагается решение следующих ключевых задач:

– распознавание эмоций людей для определения паники, усталости или потери сознания;

– голосовые команды для передачи четких инструкций в задымленной или шумной среде;

– LED индикаторы или проекционные лазеры для указания безопасного пути в условиях плохой видимости;

– тактильная обратная связь (вибрация, поддерживающие рукоятки) для физической поддержки людей с ограниченными возможностями;

– быстрое формирование адаптивных маршрутов для обхода препятствий, блокированных путей и выходов.

Реализация указанных задач значительно способствует повышению доверия людей к роботам и улучшает координацию на путях эвакуации в условиях пожара. Дальнейшие исследования в данной области необходимы для оптимизации алгоритмов взаимодействия, повышения надежности роботов и адаптации систем эвакуации под реальные сценарии пожара. Таким образом, использование интеллектуальных роботов-проводников, связанных между собой с помощью IoT, в СПЗ (СОУЭ) позволяет значительно повысить эффективность эвакуации.

Следующий способ повышения эффективности процессов эвакуации при пожаре – применение дымовых пожарных извещателей с поддержкой IoT, которые не только обнаруживают пожар, но также собирают и передают данные о задымлении. В работе [17] авторами были проведены симуляции эвакуации при пожаре с использованием программной системы FDS (Fire Dynamics Simulator) на основе реальной планировки торгового центра в Тайване по следующим алгоритмам эвакуации, направленных на минимизацию воздействия опасных факторов пожара, в частности токсичного дыма, на людей при эвакуации:

– SIEP (Single Individual Evacuation Path) для одного человека. Данный алгоритм для индивидуальной эвакуации, который определяет наиболее быстрый и безопасный путь для одного человека с учетом токсичности дыма, данные о котором собираются пожарными извещателями с IoT;

– SGEP (Smoke-aware Group Evacuation Path) для нескольких людей. В этом случае алгоритм работает для групповой эвакуации, который учитывает не только токсичность дыма, но и заторы на путях эвакуации (рис. 4).

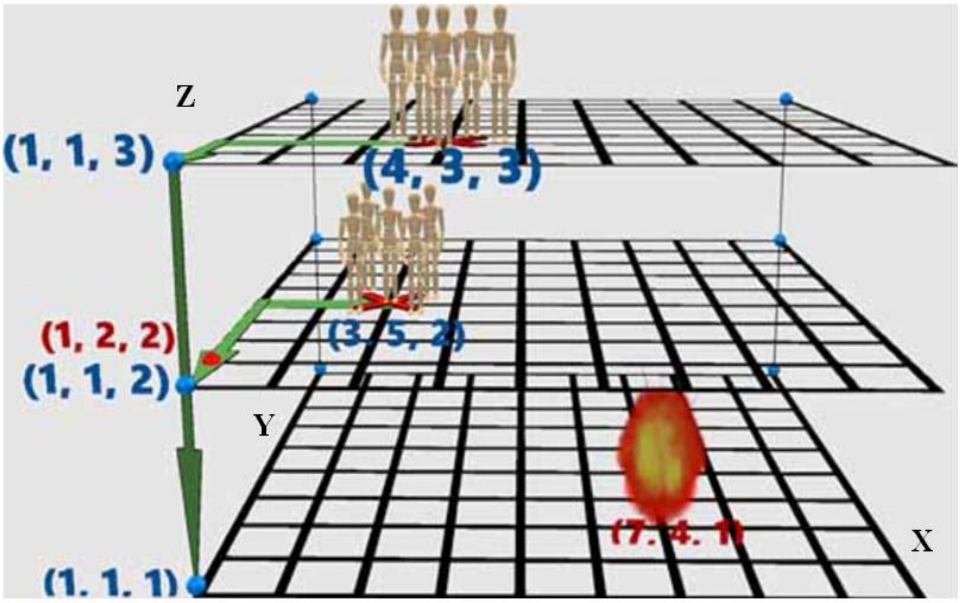

Рис. 4. **Пример моделирования (симуляции) групповой эвакуации (алгоритм SGEP) с сеткой датчиков дыма размером 10×10 в FDS**

В данном сценарии приняты следующие условия:

– скорость эвакуации: 1 переход за 1 временной интервал (30 с);

– пропускная способность узлов: не более 5 чел. одновременно;

– очаг возгорания расположен на первом этаже (7, 4, 1);

– проблема перегруженности узла (1, 1, 2).

Две группы по 5 чел. – стартующие из (3, 5, 2) и (4, 3, 3) – движутся к выходу (1, 1, 1). Через 6 интервалов (180 с) обе группы достигнут узла (1, 1, 2). Однако из-за ограничения потока (5 чел. за раз) на переходе (1, 1, 2) → (1, 1, 1) возникнет давка, что замедлит эвакуацию и повысит риск травм.

Решение: поочередное движение групп. Чтобы избежать одновременного прибытия 10 чел. в узел (1, 1, 2), одна из групп должна задержаться на 1 интервал (30 с). Возможны два варианта: группа из (4, 3, 3) ждет в узле (1, 1, 3) или группа из (3, 5, 2) ждет в узле (1, 2, 2).

Оптимальный выбор зависит от уровня задымленности. В результате моделирования на третьем этаже дым распространяется быстрее, чем на втором. Группа из (4, 3, 3) подвергается большему воздействию дыма, поэтому ей следует дать приоритет.

Сценарий эвакуации с задержкой:

1. 5-й интервал (150 с): группа (4, 3, 3) движется в (1, 1, 2), а группа (3, 5, 2) ждет в (1, 2, 2).

2. 7-й интервал (210 с): группа (4, 3, 3) достигает выхода (1, 1, 1).

3. 8-й интервал (240 с): группа (3, 5, 2) прибывает в (1, 1, 1).

Такой подход исключает давку, учитывает ограничение потока и снижает риск травм при эвакуации.

Внедрение IoT не только способствует своевременному обнаружению очагов пожара, но и позволяет формировать динамичные сценарии реагирования на основе анализа опасных факторов пожара, плотность людских потоков и доступность путей эвакуации. В контексте совершенствования эвакуации с помощью IoT исследования [18] демонстрируют значительный потенциал решений в плане адаптивного управления маршрутами эвакуации людей,

оптимизации взаимодействия систем оповещения и интеграции интеллектуальных алгоритмов принятия решений. В работах предлагается структура IoT технологии по уровням взаимодействия функционирования системы на примере «умных» зданий (рис. 5).

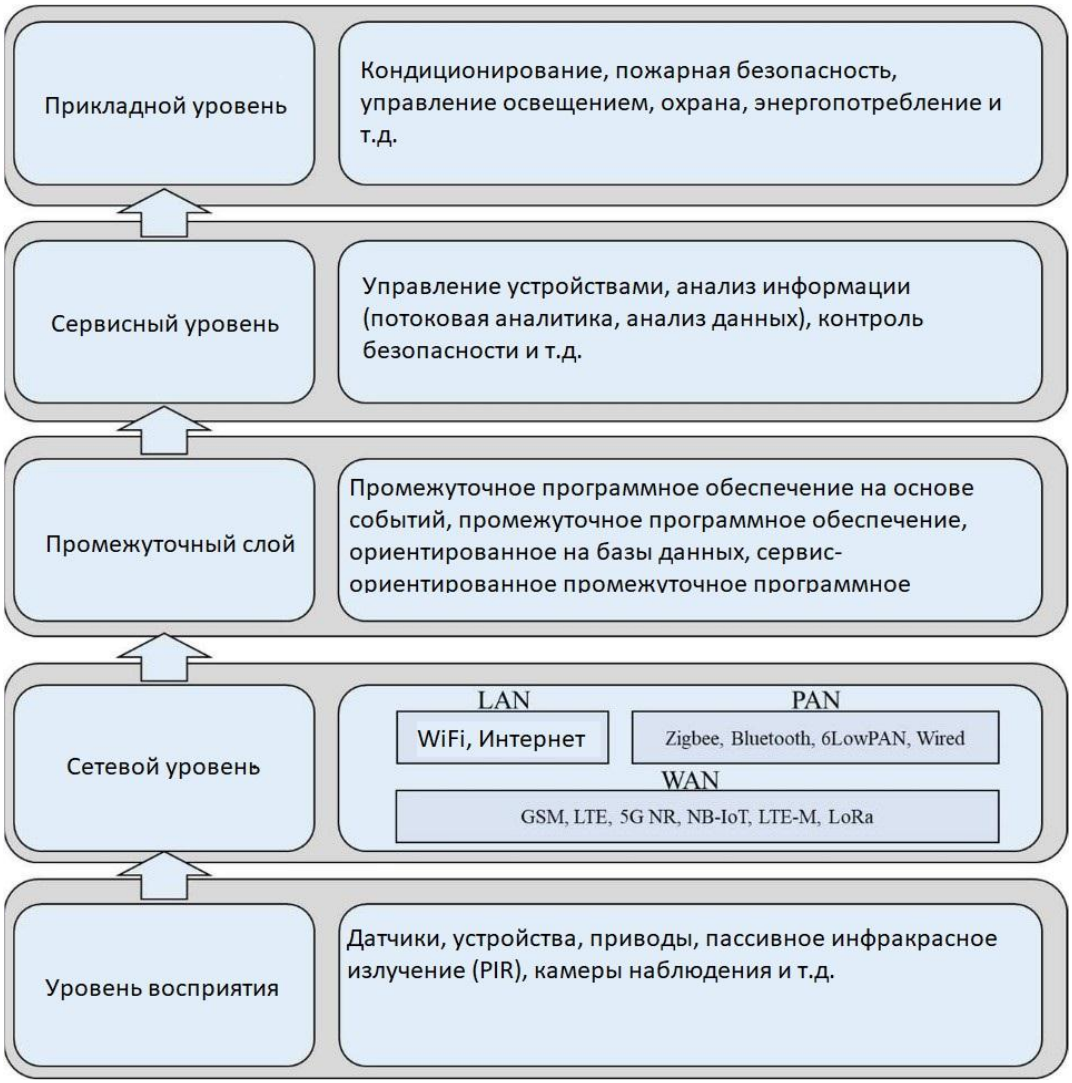

Рис. 5. **Пятиуровневая архитектура IoT для «умных» зданий**

В центре внимания – создание интеллектуальных систем оповещения, использование сенсоров и облачной обработки данных, а также преодоление угроз безопасности и устойчивости сетей. Авторы отмечают, что будущее эвакуации будет строиться на персонализированных и быстро адаптирующихся цифровых платформах.

Анализ представленных подходов к реализации СПЗ с поддержкой IoT, направленных на повышение эффективности процессов эвакуации людей за счет разработки наиболее оптимальных маршрутов на основе динамично обновляемой информации о пожаре в режиме реального времени, учитывающей не только характерные данные о пожаре, но и антропометрические и когнитивные данные людей, определяющих возможность прогнозировать уязвимые места эвакуации и управлять путями эвакуации, позволяет предложить обобщенную модульную модель СОУЭ, ориентированную на использование новых информационных технологий (НИТ) на объектах с массовым пребыванием людей (рис. 6).

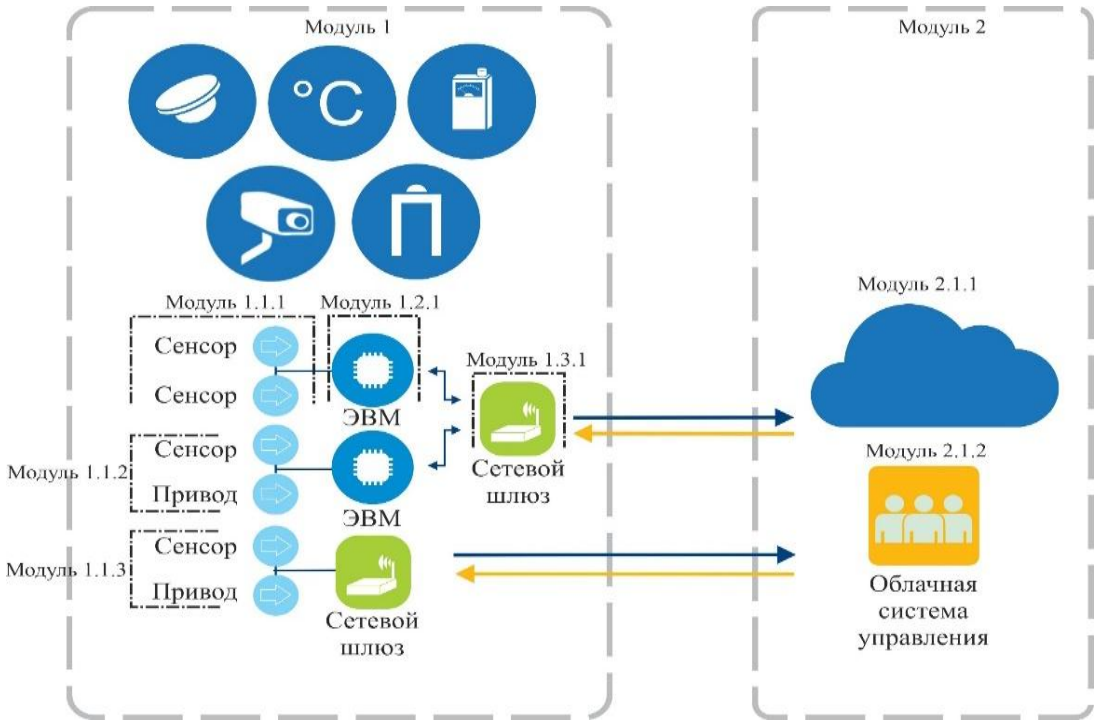

Рис. 6. **Обобщенная модульная модель СОУЭ на основе НИТ**

Модульная модель СОУЭ на основе IoT отличается от традиционных систем пожарной автоматики и обеспечивается в инновационном подходе к проектированию и интеграции разнообразных технологий ИИ. В отличие от традиционных моделей, предлагаемая модель строится по принципу адаптивного управления, где сценарии оповещения и маршруты эвакуации формируются и заранее, и в режиме реального времени – в зависимости от параметров защищаемого контингента и окружающей среды. Данная модель построена как гибкая, масштабируемая система, использующая датчики, камеры, шлюзы и аналитику для своевременного обнаружения пожаров, оповещения людей и координации эвакуации, где компоненты (модули) могут быть независимо разработаны, обновлены или заменены без влияния на всю систему. Что позволяет адаптировать её под разные объекты – от небольших офисов до крупных жилых комплексов. Общая архитектура следует базовым постулатам технологии IoT: сбор данных, обработка в реальном времени, принятие решений и обратная связь.

Ключевой особенностью предложенного подхода является реализация архитектуры в виде логически взаимосвязанных модулей. Модель состоит из центра управления (контроллер или координационный модуль (2) (КМ) на базе облачной платформы или edge-устройства) и функциональных модулей (1), соединенных через беспроводные сети (1.3.1). Модули взаимодействуют через защищенные протоколы IoT, такие как ZigBee, MQTT или CoAP, а с внешними системами и мониторингом МЧС – HTTPS обеспечивая низкую задержку и высокую надежность. Функциональные модули решает специализированную задачу: периферийные модули (1.1.1-3) – собирают данные с IoT-устройств (датчиков дыма, температуры, угарного газа, видеотрекинга и мобильных устройств); другие (1.2.1) – оценивают оперативную обстановку и степень опасности в каждой зоне объекта, а также отвечают за анализ состава и распределения контингента с учетом плотности, подвижности и поведенческих факторов, а также способности к самостоятельной эвакуации. Алгоритм функционирования системы предусматривает применение элементов машинного обучения для накопления поведенческих сценариев и повышения точности управляемых процессов на конкретных объектах.

Рассмотрим более конкретно состав и функциональное назначение модулей (рис .7).

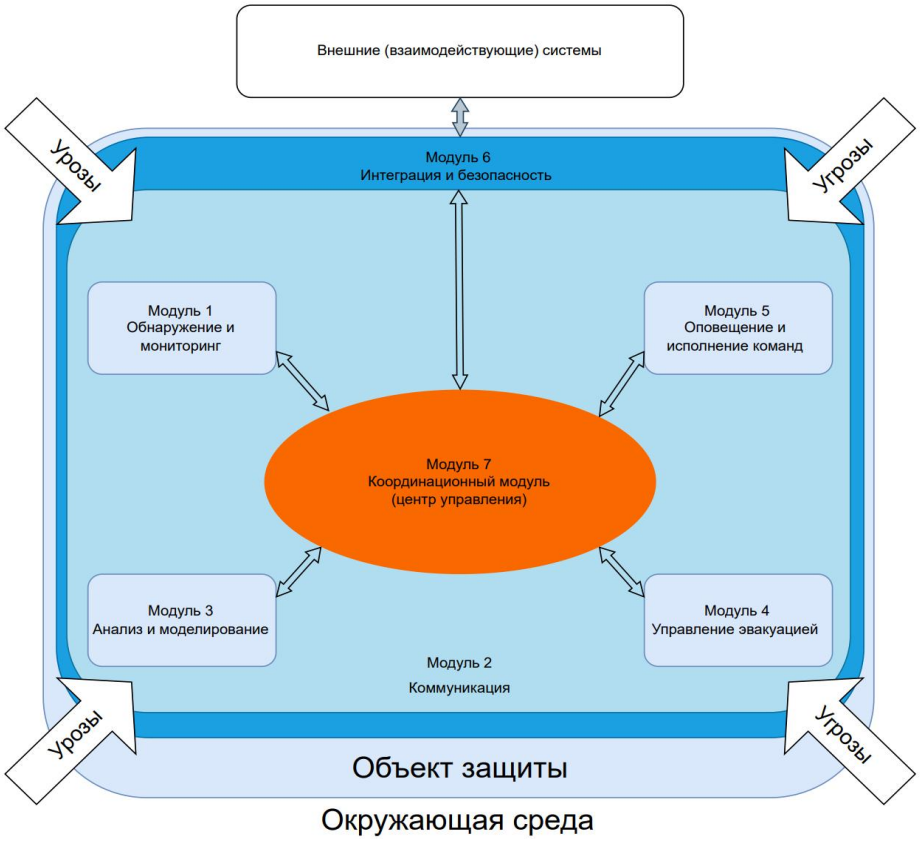

Рис. 7. **Функциональная структура модульной модели СОУЭ на основе IoT-технологии**

1. *Модуль обнаружения пожара и мониторинга.* Осуществляет непрерывный сбор данных разнообразными IoT-датчиками (дыма, тепла, распознавание пламени, концентрации CO/CO_2, движения, шума), камеры с ИИ-распознаванием, беспроводные передатчики, а также датчики положения и подсчета людей (системы подсчета на входах, BLE-маяки, инфракрасные барьеры, анализ видео). Датчики размещаются по всему объекту и подключаются к локальным узлам (устройствам) для первичной обработки. Модуль автоматически обнаруживает признаки пожара (дым, повышенная температура, огонь и др.) и мониторит окружающую среду в реальном времени. Данные агрегируются и передаются в КМ для анализа [19]. Данный модуль обеспечивает раннее предупреждение, снижая время реакции. Например, если датчик фиксирует дым в одном помещении, он активирует локальные сигналы и интегрируется с другими модулями для оценки распространения огня.

2. *Коммуникационный (сетевой) модуль.* Обеспечивает надёжную передачу информации между датчиками, вычислительными узлами и исполнительными устройствами системы. Включает IoT-шлюзы и концентраторы (с применением кабельной инфраструктуры), обеспечивающие связь датчиков с модулями системы. Используются беспроводные протоколы (ZigBee, Bluetooth, LoRaWAN, NB-IoT/модемы 4G/5G) и проводные (Ethernet). Данные с сенсоров передаются на локальные шлюзы, которые агрегируют их и передают на серверную часть. Протокол MQTT или CoAP обеспечивает «publish-subscribe» обмен сообщениями. Дополнительные каналы (SMS/GSM) могут задействоваться для аварийных уведомлений. Используемые технологии: стандартизированные протоколы IoT (MQTT, CoAP) для взаимодействия различных устройств; 5G-связь и NB-IoT для низкой задержки и высоких требований к отказоустойчивости; mesh-сети для масштабируемости. В ряде случаев могут использоваться IP-сети и беспроводные мосты для интеграции речевых панелей с КМ.

В исследовательских системах показано, что иерархическая сетевая архитектура позволяет эффективно управлять тысячами датчиков в здании [20]. Преимущества/недостатки: использование IoT-сетей даёт гибкость развертывания и масштабируемость, уменьшает объем кабельной проводки. В то же время связи могут быть уязвимы к отказам или помехам, что требует резервирования каналов и применения надёжных протоколов (шифрование и защита данных обязательны).

3. *Модуль анализа и моделирования* (вычислительные узлы). Обеспечивает сбор, фильтрацию, хранение и анализ поступающих данных от датчиков; детекция пожара и моделирование его развития; оценка плотности людей. Состоит из локальных (edge) серверов или шлюзов на базе Raspberry Pi/Intel NUC, облачные сервисы и базы данных. Включает алгоритмы предобработки сигналов, машинного обучения (нейронные сети, решающие деревья, алгоритмы распознавания образов) и геоинформационного анализа (BIM-модели зданий). Непрерывно поступающие измерения сканируются на признаки аварийных событий. Применяются алгоритмы корреляции показаний различных датчиков (умные дымовые извещатели), фильтрации шумов, а также обученные модели, предсказывающие распространение пожара и затруднения эвакуации. Используемые технологии: *Edge-computing* – вычисления на границе сети для снижения задержки (обнаружение на месте позволяет мгновенно реагировать); ИИ (глубокие нейронные сети, предиктивная аналитика) для оптимизации маршрутов эвакуации и прогнозирования опасных зон [21]; платформы IoT для агрегации данных. Например, модель DWM-Evac для планирования путей эвакуации при пожаре на основе технологии IoT комбинирует динамические графовые нейронные сети (DGNN) и оптимизационные алгоритмы (WHA, MDP) для построения безопасных путей эвакуации на основе IoT-датчиков [21]. Преимущества/недостатки: глубокая аналитика и машинное обучение повышают точность и адаптивность системы, позволяют реагировать на сложные сценарии. Минус – велика вычислительная сложность, необходимы «тяжёлые» вычислительные узлы и энергоснабжение для непрерывной работы.

4. *Модуль управления эвакуацией.* На основе обработанной информации формирует сценарии эвакуации (маршруты, очередность, сигналы оповещения). Базируется на программном обеспечении с эвакуационными алгоритмами, средствами симуляции (моделирование эвакуации, BIM-модели здания), базы эвакуационных сценариев. Может включать модули оценки риска пожара. Модуль постоянно обновляет план действий: при обнаружении пожара он рассчитывает наиболее безопасные выходы с учётом распространения пожара и числа людей в различных зонах. Обеспечивается динамическая корректировка плана – например, если определённый коридор перекрыт дымом, система перенаправляет эвакуирующихся по альтернативным путям эвакуации. Алгоритмы могут использовать методы поиска оптимальных путей и эвакуационные эвристики (например, упомянутые DGNN и MDP [22], или эвристические алгоритмы, повышающие вероятность успешной эвакуации [23]). Используемые технологии: интеллектуальный анализ (нейросети, эвристики) для поиска оптимальных путей; интеграция данных из BIM-модели здания для учёта его геометрии [24]; модули речевого синтеза и визуальные указатели для формирования инструкций. Преимущества/недостатки: такая система обеспечивает динамическое планирование и адаптивные эвакуационные сценарии, чего не может традиционная СОУЭ. Сложность модуля – в необходимости точной и актуальной информации: неточные данные о местоположении людей или запаздывающие сенсоры могут снизить эффективность.

5. *Модуль оповещения и исполнения команд.* Донесение инструкций эвакуации до людей и выполнение управляющих сигналов (включение звуковой сирены, световых маячков, поворот табло-указателей, управление дверями и вентиляцией). Состоит из аппаратуры звукового оповещения (громкоговорители, мигалки), цифровых табло и световых указателей, контроллеров систем пожарной автоматики (электрозамки дверей, заслонки вентиляции), средства массовой рассылки (SMS, push-уведомления). Принцип работы:

по команде от модуля управления эвакуацией подаётся голосовое сообщение или включаются световые сигналы по заранее запрограммированному сценарию. Установки могут давать приоритет эвакуационным сообщениям (отключать музыкальное оборудование и транслировать экстренную информацию). Специализированные «умные» табло могут динамически менять направление стрелок по заданному алгоритму [23, 24]. Используемые технологии: IP-ориентированные речевые панели, смарт-табло с сетевыми интерфейсами; дистанционный контроль по IoT (включение/выключение по сети); системы мультимодального оповещения (звуковые, визуальные и текстовые сообщения). Преимущества/недостатки: активное руководство эвакуируемыми (голосовые и визуальные подсказки) позволяет более точно направлять поток людей. Минусы – необходимость резервирования электропитания и проверок работоспособности; отказ такого модуля (например, обрыв сети к акустическому динамику) может привести к потере связи с эвакуируемыми.

6. *Модуль интеграции и безопасности.* Обеспечивает связь с внешними системами (базы данных, умный город, экстренные службы) через API и протоколы безопасности (TLS/MQTT с сертификатами, шифрование, блокчейн и др.). Поддерживает бесперебойную работу всех модулей, защищает систему от отказов. Включает резервные источники питания, failover-механизмы (аварийное переключение), дублирование серверов и каналов связи, криптографические модули, средства мониторинга сети. Модуль гарантирует совместимость с другими IoT-системами (например, видеонаблюдением или освещением) и защищает от киберугроз (мониторинг на вторжения). Использует системы резервирования (RAID, дублированные сети, 4G/LTE-модемы как запасные каналы), шифрование трафика (TLS/MQTT с сертификатами) и многофакторная аутентификация; блокчейн-технологии для защиты журналов событий [20]. Также управляет обновлениями модулей и обеспечивает устойчивость путем интеграции всей системы в более широкую инфраструктуру, с акцентом на кибербезопасность, чтобы предотвратить несанкционированные действия или ложные срабатывания. Преимущества/недостатки: высокая надёжность и защищённость (включая защиту персональных данных и предотвращение ложных срабатываний), однако усложняется архитектура системы, возрастают требования к вычислительным ресурсам (шифрование создает нагрузку) и квалификации обслуживающего персонала.

7. *Координационный модуль (КМ).* Обеспечение координации, маршрутизации, централизованного управления всеми модулями, единой информационной среды, управления сценариями эвакуации, синхронизации времени и данных между устройствами, а также интеграцию с внешними диспетчерскими системами (в том числе АПК «Безопасный город» и региональные центры управления МЧС России). Включает в себя промышленный сервер или микрокомпьютер (например, ARM/Intel – платформа), встроенные модули беспроводной связи, контроллеры ввода-вывода, блоки резервного питания, а также программное обеспечение брокера сообщений. В состав входят средства журналирования и киберзащиты (TLS/DTLS – шифрование, аутентификация устройств, контроль целостности данных).

КМ принимает телеметрию от сенсорных модулей, передает её в модуль аналитики для обработки, получает решения (сценарии эвакуации, команды управления) и направляет сигналы исполнительным устройствам. Одновременно ведёт журнал событий, отслеживает состояние всех узлов сети, диагностирует сбои и при необходимости инициирует резервное переключение на дублирующий канал или резервный сервер. В режиме реального времени модуль контролирует логическую целостность данных, синхронизирует действия модулей и обеспечивает их согласованное функционирование. В случае потери связи с модулем анализа КМ способен перейти в «автономный режим» и действовать по заранее заложенным сценариям (failsafe-алгоритмы). Главное преимущество – единая точка координации и контроля**,** что повышает управляемость и надёжность системы, упрощает диагностику, протоколирование и киберзащиту. КМ обеспечивает синхронизацию данных, приоритет критичных сообщений и централизованное обновление ПО. Недостатки – зависимость

от надёжности питания и связи, необходимость резервирования (второй сервер/шлюз), а также потенциальная уязвимость при неправильно реализованной аутентификации. Для устранения рисков применяют дублирование узлов и схему «master–backup» с автоматическим переключением.

Организация взаимодействия модулей может быть описана следующей событийно-ориентированной иерархией (алгоритмом) «сенсор → шлюз → аналитика → исполнительные устройства»:

1. Модуль 1 → Модуль 7: модуль обнаружения и мониторинга осуществляет непрерывный сбор параметров среды (температура, задымление, плотность людей) и при превышении порогов формирует сигналы, которые через коммуникационный модуль поступают в КМ, который выполняет предварительную фильтрацию ложных срабатываний, маршрутизацию данных, синхронизацию времени и передачу сообщений в модуль обработки и аналитики).

2. Коммуникационный (сетевой) модуль обеспечивает доставку сообщений от сенсоров к вычислительным узлам и обратно к исполнительным устройствам. → Передаёт агрегированные пакеты данных в модуль анализа и предиктивного моделирования и дублирует их в КМ по протоколам MQTT/CoAP поверх TLS.

3. Модуль 7 → Модуль 3: выполняет фильтрацию, корреляцию и прогноз развития пожара и задымления. Передаёт результаты расчётов и прогнозные сценарии в модуль 4.

4. Модуль 3 и 7 → Модуль 4: определяет оптимальные маршруты эвакуации и последовательность включения систем оповещения с учётом прогнозов и текущего состояния зон. → Формирует управляющие команды и передаёт их в модуль 7.

5. Модуль 7 → Модуль 5: осуществляет маршрутизацию и синхронизацию данных между всеми модулями, ведёт журнал событий и обеспечивает согласованное выполнение сценариев. → Направляет команды в модуль 5, контролирует их выполнение и принимает обратную информацию о состоянии оборудования (например, «Отправить SMS или push-уведомление: 'Эвакуация через северный коридор'").

6. Модуль 5 реализует команды управления: включает системы звукового и речевого оповещения, управляет световыми указателями, дверями и вентиляцией. → Передаёт подтверждения о выполнении действий и состояние устройств обратно в КМ.

7. Модуль 6 защищает все этапы обмена: шифрует каналы (TLS/DTLS), проверяет подлинность устройств (PKI, HMAC), контролирует целостность пакетов и ведет аудит событий. → Интегрирован во все уровни сети и взаимодействует с КМ, обеспечивая надёжность и киберустойчивость системы.

Рассмотренный процесс циклический: после действий возвращаемся к мониторингу для корректировки (например, если огонь распространяется). Обратная связь замыкает цикл (Модуль 1 мониторит изменения). Если риск низкий, процесс останавливается; иначе – итерация. Общее взаимодействие происходит в реальном времени через КМ, с failover (если он падает, модули переходят в автономный режим) и все модули могут запрашивать обновления от КМ.

В отличие от традиционной системы, данная модульная архитектура обладает высокой гибкостью за счет независимости модулей и при этом их синхронизированности, допускает горизонтальное масштабирование и замену компонентов без остановки системы, что соответствует принципам resilient IoT-систем [25].

Предложенная модель в силу своей универсальности может быть адаптирована под особенности конкретного объекта защиты. Например, адаптация под многоэтажное здание добавляет сложности: координация между этажами, ретрансляторы, маршруты эвакуации (лестницы, лифты), зоны риска и интеграция с внешними службами (МЧС России). КМ остаётся координатором, но теперь он управляет распределёнными модулями по этажам (например, локальные суб-модули на каждом этаже для отказоустойчивости).

Таким образом, модульная модель, по сути, представляет собой концепцию объединения физических объектов посредством беспроводных сетей связи и встроенных датчиков, позволяющих собирать и передавать данные о состоянии окружающей среды в режиме реального времени. Интеграция совокупности функциональных модулей, взаимодействующих на основе IoT-технологии, по сути, представляет собою сложную систему, реализующую следующие основные функции:

1. Детектирования опасности. Интеграция датчиков позволила повысить чувствительность и надежность выявления потенциальных угроз, минимизация риска ложных срабатываний.

2. Интеллектуальная навигация и маршрутизация. С помощью BLE-маяков GPS-модулей и Wi-Fi-сенсоров можно отслеживать перемещение людей внутри зданий и организовать автоматическое построение оптимальных маршрутов эвакуации с учетом текущих обстоятельств. Это позволило сократить время выхода из опасной зоны, снизить вероятность паники среди эвакуируемых.

3. Управления инженерными коммуникациями. Технология IoT применяется для автоматизации процессов открытия дверей, включения аварийного освещения, отключения электроэнергии и вентиляции в помещениях, подверженных воздействию огня или дыма. Такие меры способствуют созданию благоприятных условий для безопасной эвакуации, что уменьшает риск поражения электрическим током, распространения продуктов горения и ухудшения видимости.

4. Автоматизация информирования. Размещение интерактивных экранов, голосовых помощников, SMS-рассылки и мобильных приложений с функцией push-уведомлений способствует быстрому распространению инструкций по действиям в случае экстренной ситуации. Люди получают актуальную информацию о расположении ближайших выходов, местах размещения аптечек первой помощи и специализированных пунктов помощи.

В целом научная новизна работы обосновывается глубоким анализом работ по тематике применения технологий ИИ в области обеспечения пожарной безопасности на объектах с массовым пребыванием людей, который показал, что в наибольшей степени для повышения эффективности процессов оповещения и управления эвакуацией целесообразно применение IoT-технологии. Модульная модель СОУЭ на основе IoT представляет собой инновационный подход к проектированию систем пожарной автоматики, который отличается от традиционных централизованных систем с жесткой архитектурой, при этом сама модель может быть взята за основу при разработке перспективных СОУЭ. По своей сути этот подход заключается в адаптации принципов «модульной инженерии» из программного обеспечения к аппаратно-программным комплексам IoT-систем (СОУЭ), что позволяет динамически адаптироваться (масштабироваться) к изменениям в окружающей среде. Модель включает продвинутые алгоритмы предиктивной аналитики (на основе машинного обучения)/ИИ), которые анализируют данные в реальном времени от IoT-устройств. Новизна здесь – в комбинации модульной структуры с edge-компьютингом (возможность обработки данных на устройстве, а не в центре обработки данных или облаке), что снижает задержки, уменьшает нагрузку на сеть, повышает конфиденциальность и точность выработки решений по управлению процессом эвакуации.

Практическая значимость работы определяется возможностями предложенного инструментария: по оптимизации процессов эвакуации и снижения рисков, что, в конечном итоге, приводит к спасению жизней людей; по повышению эффективности процессов разработки, внедрения и применения системы, ее экономичности; по учету социальных (например, интеграция с зелеными технологиями – низкоэнергетичные датчики) и экологических (улучшает качество жизни, особенно для уязвимых групп – дети, пожилые, и помогает в кризисных ситуациях) аспектов.

При этом аргументировано, что применение этих технологий в системах противопожарной защиты приводит и к возникновению новых проблем, требующих своего

скорейшего решения в сфере информационной безопасности, а именно – увеличение уязвимости таких, по сути – информационных, систем перед кибератаками. Практика эксплуатации показывает, что отсутствие киберзащиты может привести к дестабилизации функционирования критически важных систем, что сопряжено с прямой угрозой жизни людей. Модульная модель предполагает новые механизмы кибербезопасности, такие как блокчейн для верификации данных или zero-trust модели для защиты от взломов. Это открывает новые направления в исследованиях по «резильентным (восстанавливаемым) системам безопасности». В целом предложенная модель вносит вклад в развитие «умных систем безопасности», где новизна измеряется междисциплинарным подходом – сочетанием инженерии, информатики и поведенческих наук.

Заключение

Целью данной работы является исследование содержания и возможностей применения технологий ИИ, в частности – IoT-технологии, которые могут быть применены в обеспечении пожарной безопасности различных объектов защиты, в частности – совершенствование СОУЭ на объектах с массовым пребыванием людей, и формулировка проблем, свойственных этой предметной области, с обоснованием направлений их решения. В качестве основного метода исследования применялся системный анализ процессов обеспечения пожарной безопасности и технологий ИИ, направленный на выявление проблемных ситуаций в рассматриваемой предметной области.

Анализ актуальных отечественных и зарубежных разработок показал, что интеллектуальные устройства и алгоритмы, основанные на глубоком обучении и адаптивных сценариях эвакуации, способны значительно сократить время реагирования и повысить вероятность успешной эвакуации. Результатом исследования является обоснование необходимости применения IoT-технологии для повышения эффективности процессов оповещения и управления эвакуацией при пожаре на объектах с массовым пребыванием людей и формулировка новых проблем, порождаемых использованием данной технологии, определяемых ее информационным характером и, связанных с этим, уязвимостями и киберугрозами.

Представленная модульная модель СОУЭ, ориентированная на использование IoT-технологии на объектах с массовым пребыванием людей, строится по принципу адаптивного управления, где сценарии оповещения и маршруты эвакуации формируются заблаговременно либо оперативно в процессе изменения обстановки – в зависимости от параметров защищаемого контингента и окружающей среды.

Таким образом, обозначается новый вектор развития систем противопожарной защиты, ориентированный на персонализированное, предиктивное и автоматизированное управление эвакуацией. Кроме того, внедрение IoT в СПЗ, формирует новый подход к расчету пожарного риска, предполагающий выявление и структурирование тех параметров, которые оказывают наибольшее влияние на его расчетные величины, обеспечивая взаимодействие с подсистемами пожарной сигнализации, противодымной вентиляции, системами автоматического пожаротушения, контроля доступа и диспетчеризации.

Список источников

1. Construction 4.0, Industry 4.0, and Building Information Modeling (BIM) for Sustainable Building Development within the Smart City / Yu. Chen [et al.] // Sustainability. 2022. № 14 (16). P. 10028. DOI: 10.3390/su141610028.

2. Шестакова И.Г. Новая темпоральность цифровой цивилизации: будущее уже наступило // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Гуманитарные и общественные науки. 2019. Т. 10. № 2. С. 20–29. DOI: 10.18721/JHSS.10202. EDN XBRISF.

3. Блинова О.А. VUCA, BANI, SHIVA – акронимы, объясняющие мир // Эффективный ответ на современные вызовы с учетом взаимодействия человека и природы, человека и технологий: материалы XV Междунар. науч.-техн. конф. Екатеринбург: Уральский государственный лесотехнический университет, 2024. С. 730–735. EDN IYPYHK.

4. Ковалев А.А. История безопасности как новая область западной исторической науки // Genesis: исторические исследования. 2021. № 12. С. 225–241. DOI: 10.25136/2409-868X.2021.12.34867. EDN WPAVZC.

5. Липаев А.А. К вопросу об определении понятия «техносфера» // Управление техносферой. 2023. Т. 6. № 4. С. 490–497. DOI: 10.34828/UdSU.2023.14.84.001. EDN HQDYIF.

6. Marwedel P. Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things // Springer Nature. 2021. С. 433. DOI: 10.1007/978-3-030-60910-8.

7. Kotenko I., Sineshchuk Yu., Saenko I. Optimizing Secure Information Interaction in Distributed Computing Systems by the Sequential Concessions Method // 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). Västerås, Sweden, 2020. P. 429–432. DOI: 10.1109/PDP50117.2020.00072.

8. Taha W.M., Taha A.E.M., Thunberg J. Cyber-Physical Systems: A Model-Based Approach // Springer Nature. 2021. С. 187. DOI: 10.1007/978-3-030-36071-9.

9. Аспекты техносферной безопасности в концепции системы национальной безопасности / Ю.И. Синещук [и др.] // Проблемы управления рисками в техносфере. 2024. № 2 (70). С. 8–19. DOI: 10.61260/1998-8990-2024-2-8-19. EDN MSBHFG.

10. Системные особенности обеспечения национальной безопасности в условиях глобальной цифровизации / Ю.И. Синещук [и др.] // Техносферная безопасность. 2024. № 4 (45). С. 87–105. EDN BCBTMM.

11. Малькова Т.П. Киборгизация: онтологические проблемы исследования // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2018. № 3 (89). С. 87–92. DOI: 10.30853/manuscript.2018-3.16. EDN XOQFNJ.

12. Gao Ya., Liu S., Yang L. Artificial intelligence and innovation capability: A dynamic capabilities perspective // International Review of Economics & Finance. 2025. Vol. 98. DOI: 10.1016/j.iref.2025.103923.

13. Мельников Г.О., Турсенев С.А. Интеграция технологии искусственного интеллекта для повышения эффективности эвакуации людей при пожаре // Природные и техногенные риски (физико-математические и прикладные аспекты). 2023. № 4 (48). С. 30–36. DOI: 10.61260/2307-7476-2024-2023-4-30-36. EDN DDHLPZ.

14. Мельников Г.О., Синещук Ю.И. Применение 5G и Интернета вещей в обеспечении безопасной эвакуации // Молодежная программа 28-ой Междунар. специализированной выставки-форума: сб. трудов Конкурса научно-исследовательских работ (Конкурс НИР). 2024. М.: Ассоциация «СИЗ», 2025. С. 38–41. EDN EWLPAV.

15. Li C.Y., Zhang F., Chen L. Robot-assisted pedestrian evacuation in fire scenarios based on deep reinforcement learning // Chinese Journal of Physics. 2024. Vol. 92. С. 494–531. DOI: 10.1016/J.CJPH.2024.09.008.

16. IoT based Smart Sensing and Alarming System with Autonomous Guiding Robots for Efficient Fire Emergency Evacuation / S.V. Tresa Sangeetha [et al.] // 2021 2nd International Conference for Emerging Technology (INCET). Belagavi, India, 2021. P. 1–6. DOI: 10.1109/INCET51464.2021.9456142.

17. Yen H.H., Lin C.H., Tsao H.W. Novel Smoke-Aware Individual Evacuation and Congestion-Aware Group Evacuation Algorithms in IoT-Enabled Multi-Story Multi-Exit Buildings // IEEE Access. 2022. Vol. 10. P. 119402–119418. DOI: 10.1109/ACCESS.2022.3221757.

18. Kodali R.K., Yerroju S. IoT based smart emergency response system for fire hazards // 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). Tumkur, India, 2017. P. 194–199. DOI: 10.1109/ICATCCT.2017.8389132.

19. Integrated IoT-based fire prevention and evacuation system for high-rise buildings / B. Maharmi [et al.] // Journal of Ocean, Mechanical and Aerospace-science and engineering. 2024. Т. 68. № 3. С. 161–168. DOI: 10.36842/jomase.v68i3.383.

20. From Inception to Innovation: A Comprehensive Review and Bibliometric Analysis of IoT-Enabled Fire Safety Systems / A.A.S. AlQahtani [et al.] // Safety. 2025. Т. 11. № 2. С. 41. DOI: 10.3390/safety11020041.

21. Zhang Z., Tan L., Tiong R.L.K. Fire emergency management of large shopping malls: IoT-based evacuee tracking and dynamic path optimization // Alexandria Engineering Journal. 2024. Vol. 107. P. 652–664. DOI: 10.1016/j.aej.2024.08.107.

22. Zhang Z., Tan L., Tiong R.L.K. Fire emergency management of large shopping malls: IoT-based evacuee tracking and dynamic path optimization // Alexandria Engineering Journal. 2024. Т. 107. С. 652–664. DOI: 10.1016/j.aej.2024.08.107.

23. Yen H.H., Lin C.H. Intelligent Evacuation Sign Control Mechanism in IoT-Enabled Multi-Floor Multi-Exit Buildings // Sensors. 2024. Т. 24. № 4. С. 1115. DOI: 10.3390/s24041115.

24. Fang H., Lo S., Lo J.T.Y. Building fire evacuation: An IoT-aided perspective in the 5G era // Buildings. 2021. Т. 11. № 12. С. 643. DOI: 10.3390/buildings11120643.

25. A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms / C. Berger [et al.] // ACM Computing Surveys (CSUR). 2021. Т. 54. № 7. С. 1–39.

References:

1. Construction 4.0, Industry 4.0, and Building Information Modeling (BIM) for Sustainable Building Development within the Smart City / Yu. Chen [et al.] // Sustainability. 2022. № 14 (16). P. 10028. DOI: 10.3390/su141610028.

2. Shestakova I.G. Novaya temporal'nost' cifrovoj civilizacii: budushchee uzhe nastupilo // Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Gumanitarnye i obshchestvennye nauki. 2019. T. 10. № 2. S. 20–29. DOI: 10.18721/JHSS.10202. EDN XBRISF.

3. Blinova O.A. VUCA, BANI, SHIVA – akronimy, ob"yasnyayushchie mir // Effektivnyj otvet na sovremennye vyzovy s uchetom vzaimodejstviya cheloveka i prirody, cheloveka i tekhnologij: materialy XV Mezhdunar. nauch.-tekhn. konf. Ekaterinburg: Ural'skij gosudarstvennyj lesotekhnicheskij universitet, 2024. S. 730–735. EDN IYPYHK.

4. Kovalev A.A. Istoriya bezopasnosti kak novaya oblast' zapadnoj istoricheskoj nauki // Genesis: istoricheskie issledovaniya. 2021. № 12. S. 225–241. DOI: 10.25136/2409-868X.2021.12.34867. EDN WPAVZC.

5. Lipaev A.A. K voprosu ob opredelenii ponyatiya «tekhnosfera» // Upravlenie tekhnosferoj. 2023. T. 6. № 4. S. 490–497. DOI: 10.34828/UdSU.2023.14.84.001. EDN HQDYIF.

6. Marwedel P. Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things // Springer Nature. 2021. S. 433. DOI: 10.1007/978-3-030-60910-8.

7. Kotenko I., Sineshchuk Yu., Saenko I. Optimizing Secure Information Interaction in Distributed Computing Systems by the Sequential Concessions Method // 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). Västerås, Sweden, 2020. P. 429–432. DOI: 10.1109/PDP50117.2020.00072.

8. Taha W.M., Taha A.E.M., Thunberg J. Cyber-Physical Systems: A Model-Based Approach // Springer Nature. 2021. S. 187. DOI: 10.1007/978-3-030-36071-9.

9. Aspekty tekhnosfernoj bezopasnosti v koncepcii sistemy nacional'noj bezopasnosti / Yu.I. Sineshchuk [i dr.] // Problemy upravleniya riskami v tekhnosfere. 2024. № 2 (70). S. 8–19. DOI: 10.61260/1998-8990-2024-2-8-19. EDN MSBHFG.

10. Sistemnye osobennosti obespecheniya nacional'noj bezopasnosti v usloviyah global'noj cifrovizacii / Yu.I. Sineshchuk [i dr.] // Tekhnosfernaya bezopasnost'. 2024. № 4 (45). S. 87–105. EDN BCBTMM.

11. Mal'kova T.P. Kiborgizaciya: ontologicheskie problemy issledovaniya // Istoricheskie, filosofskie, politicheskie i yuridicheskie nauki, kul'turologiya i iskusstvovedenie. Voprosy teorii i praktiki. 2018. № 3 (89). S. 87–92. DOI: 10.30853/manuscript.2018-3.16. EDN XOQFNJ.

12. Gao Ya., Liu S., Yang L. Artificial intelligence and innovation capability: A dynamic capabilities perspective // International Review of Economics & Finance. 2025. Vol. 98. DOI: 10.1016/j.iref.2025.103923.

13. Mel'nikov G.O., Tursenev S.A. Integraciya tekhnologii iskusstvennogo intellekta dlya povysheniya effektivnosti evakuacii lyudej pri pozhare // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty). 2023. № 4 (48). S. 30–36. DOI: 10.61260/2307-7476-2024-2023-4-30-36. EDN DDHLPZ.

14. Mel'nikov G.O., Sineshchuk YU.I. Primenenie 5G i Interneta veshchej v obespechenii bezopasnoj evakuacii // Molodezhnaya programma 28-oj Mezhdunar. specializirovannoj vystavki-foruma: sb. trudov Konkursa nauchno-issledovatel'skih rabot (Konkurs NIR). 2024. M.: Associaciya «SIZ», 2025. S. 38–41. EDN EWLPAV.

15. Li C.Y., Zhang F., Chen L. Robot-assisted pedestrian evacuation in fire scenarios based on deep reinforcement learning // Chinese Journal of Physics. 2024. Vol. 92. C. 494–531. DOI: 10.1016/J.CJPH.2024.09.008.

16. IoT based Smart Sensing and Alarming System with Autonomous Guiding Robots for Efficient Fire Emergency Evacuation / S.V. Tresa Sangeetha [et al.] // 2021 2nd International Conference for Emerging Technology (INCET). Belagavi, India, 2021. P. 1–6. DOI: 10.1109/INCET51464.2021.9456142.

17. Yen H.H., Lin C.H., Tsao H.W. Novel Smoke-Aware Individual Evacuation and Congestion-Aware Group Evacuation Algorithms in IoT-Enabled Multi-Story Multi-Exit Buildings // IEEE Access. 2022. Vol. 10. P. 119402–119418. DOI: 10.1109/ACCESS.2022.3221757.

18. Kodali R.K., Yerroju S. IoT based smart emergency response system for fire hazards // 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). Tumkur, India, 2017. P. 194–199. DOI: 10.1109/ICATCCT.2017.8389132.

19. Integrated IoT-based fire prevention and evacuation system for high-rise buildings / B. Maharmi [et al.] // Journal of Ocean, Mechanical and Aerospace-science and engineering. 2024. T. 68. № 3. S. 161–168. DOI: 10.36842/jomase.v68i3.383.

20. From Inception to Innovation: A Comprehensive Review and Bibliometric Analysis of IoT-Enabled Fire Safety Systems / A.A.S. AlQahtani [et al.] // Safety. 2025. T. 11. № 2. S. 41. DOI: 10.3390/safety11020041.

21. Zhang Z., Tan L., Tiong R.L.K. Fire emergency management of large shopping malls: IoT-based evacuee tracking and dynamic path optimization // Alexandria Engineering Journal. 2024. Vol. 107. P. 652–664. DOI: 10.1016/j.aej.2024.08.107.

22. Zhang Z., Tan L., Tiong R.L.K. Fire emergency management of large shopping malls: IoT-based evacuee tracking and dynamic path optimization // Alexandria Engineering Journal. 2024. T. 107. S. 652–664. DOI: 10.1016/j.aej.2024.08.107.

23. Yen H.H., Lin C.H. Intelligent Evacuation Sign Control Mechanism in IoT-Enabled Multi-Floor Multi-Exit Buildings // Sensors. 2024. T. 24. № 4. S. 1115. DOI: 10.3390/s24041115.

24. Fang H., Lo S., Lo J.T.Y. Building fire evacuation: An IoT-aided perspective in the 5G era // Buildings. 2021. T. 11. № 12. S. 643. DOI: 10.3390/buildings11120643.

25. A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms / C. Berger [et al.] // ACM Computing Surveys (CSUR). 2021. T. 54. № 7. S. 1–39.

Информация о статье:
Статья поступила в редакцию: 11.07.2025; одобрена после рецензирования: 05.10.2025;
принята к публикации: 26.11.2025

The information about article:
The article was submitted to the editorial office: 11.07.2025; approved after review: 05.10.2025;
accepted for publication: 26.11.2025

Информация об авторах:
Мельников Григорий Олегович, адъюнкт кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), e-mail: grinyam@list.ru, https://orcid.org/0009-0003-8459-7317, SPIN-код: 6971-4886
Синещук Юрий Иванович, профессор кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, заслуженный работник высшей школы Российской Федерации, e-mail: sinegal53@mail.ru, SPIN-код: 4663-4378

Information about the authors:
Melnikov Grigory O., associate professor of the department of fire safety of buildings and automated fire extinguishing systems of the Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), e-mail: grinyam@list.ru, https://orcid.org/0009-0003-8459-7317, SPIN: 6971-4886
Sineshchuk Yury I., professor of the department of fire safety of buildings and automated fire extinguishing systems of the Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, honored worker of the higher school of the Russian Federation, e-mail: sinegal53@mail.ru, SPIN: 4663-4378