Надеждин Евгений Николаевич
д-р техн. наук, профессор
Хамаганов Роман Тимурович
магистрант

ФГАОУ ВО «Российский государственный
гуманитарный университет»
г. Москва

К ВОПРОСУ АНАЛИЗА УСТОЙЧИВОСТИ РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ УМНОГО ДОМА

Аннотация: *в статье рассматривается задача анализа факторов риска нарушения функциональности интеллектуальной информационной системы «Умный дом» с использованием нечетких когнитивных карт. Функциональность системы определяется качеством сетевого взаимодействия, надёжностью электропитания, корректностью программного обеспечения, совместимостью протоколов, действиями пользователя и внешними воздействиями. Предложено разделение факторов на внешние и внутренние с выделением трёх уровней критичности. Особое внимание уделено факторам, способным привести к полной или частичной недоступности системы: отказу электропитания, сбоям локальной сети, выходу из строя центрального контроллера и исполнительных устройств, несанкционированному доступу и нарушению механизмов управления.*

Ключевые слова: *интернет вещей, умный дом, устойчивость функционирования, задача анализа факторов риска, центральный контроллер, сетевое взаимодействие.*

На этапе активного развития цифровых технологий всё большее распространение получают информационные системы (ИС) умного дома, объединяющие датчики, исполнительные устройства, контроллеры, сетевое оборудование и средства автоматизации. Такие системы позволяют повысить комфорт,

безопасность и энергоэффективность жилых помещений за счёт автоматического управления освещением, климатом, охранными устройствами, инженерными коммуникациями и другими элементами домашней инфраструктуры. Одним из перспективных направлений здесь является повышение качества реализации нормативных услуг, предлагаемых системами умного дома. Современные ИС умного дома, построенные на основе интеграции технологий Интернета вещей, сетевого взаимодействия, датчиков, исполнительных устройств и средств автоматизации, обладают значительным потенциалом в вопросах повышения комфорта, безопасности и энергоэффективности жилой среды [1; 3]. При этом эффективность функционирования таких систем во многом определяется их устойчивостью к воздействию дестабилизирующих факторов, способных нарушать процессы обмена данными, выполнения управляющих команд, работу сценариев автоматизации и доступ пользователя к основным функциям системы [2; 5].

Целью настоящей статьи является анализ и классификация дестабилизирующих факторов, влияющих на устойчивость работы ИС умного дома, а также определение степени их критичности с учётом возможных сценариев нарушения функционирования системы.

В соответствии с рекомендациями современной теории управления устойчивость будем рассматривать как комплексное свойство управляемой системы поддерживать свою функциональность и сохранять в допустимых пределах рабочие характеристики и (или) определяющие параметры при действии дестабилизирующих факторов различной природы.

Традиционно для количественной оценки условий устойчивости линейных автоматических систем управления используют специальные методики, предусматривающие аналитический расчет, моделирование и частотный анализ. Для упрощенного инженерного анализа устойчивости ИС умного дома разработаны специальные методы и инструментальные средства. В общем случае для автоматизированных систем управления, отличающихся нестационарностью, многорежимностью и нелинейностью, наиболее предпочтительны интеллектуальные технологии.

Один из универсальных подходов к проблеме оценки факторов риска нарушения устойчивости процесса управления связан с применением метода экспертных оценок. На содержательном уровне задачу многофакторного анализа указанной проблемы можно сформулировать следующим образом.

Заданы архитектура и характеристики интеллектуальной информационной системы (ИИС) «Умный дом». Известна статистика пробной эксплуатации ИИС.

Требуется с привлечением группы профильных экспертов дать комплексную оценку факторов риска нарушения функциональности ИИС «Умный дом», построить математическую модель проблемной ситуации, обусловленной воздействием на ИС умного дома комплекса дестабилизирующих факторов, и осуществить ранжирование факторов по степени их влияния на устойчивость функционирования ИИС.

Для реализации задачи исследования может быть применена известная методика когнитивного анализа факторов риска с использованием нечетких когнитивных карт (НКК) В.Б. Силова [4, с. 143]. Одним из ответственных этапов идентификации модели проблемной ситуации в виде НКК являются выделение и структуризация множества определяющих факторов.

Функционирование ИС умного дома зависит от большого количества различных факторов. В ходе анализа основных проблем систем умного дома [1; 4], а также на основании результатов проведённого исследования Ходжамаммедова М.М. в части обеспечения работоспособности и защищённости IoT-устройств [5], стало возможным разделить дестабилизирующие факторы, влияющие на работоспособность систем умного дома, на две явных категории.

1. Внешние, которые представляют собой негативные воздействия на систему, источник которых находится за пределами системы умного дома.

2. Внутренние, которые возникают внутри самой системы умного дома и связаны с особенностями её построения, конфигурации, эксплуатации и технического состояния самих физических компонентов.

На рисунке 1 представлена структурная схема, отражающая классификацию дестабилизирующих факторов, влияющих на работоспособность ИС умного дома.

Внешние и внутренние факторы, как правило, имеют различную природу происхождения, однако могут приводить к сходным последствиям: нарушению связи между устройствами, некорректному выполнению команд, снижению уровня безопасности, потере данных и отказу отдельных функций. Следовательно, при проектировании и последующей эксплуатации систем умного дома необходимо учитывать не только сам факт возникновения сбоя, но и возможные сценарии его влияния на устойчивость функционирования всей системы. Для корректной оценки важности и величины влияния каждого дестабилизирующего фактора необходимо ввести уровни критичности. Для демонстрации предлагаемого подхода выделим три степени критичности.

1. Высокая критичность. Фактор способен привести к полной недоступности системы или нарушению работы критически важных функций.

2. Средняя критичность. Подобные факторы могут вызывать частичное нарушение функционирования системы, ограничение отдельных сценариев автоматизации и (или) сужение возможностей для осуществления контроля и управления системой.

3. Низкая критичность. Такие факторы влияют преимущественно на удобство эксплуатации, не нарушая ключевые функции системы и не создавая существенных рисков для пользователя.

Дестабилизирующие факторы целесообразно рассматривать не изолированно друг от друга, а с точки зрения их совокупного влияния на устойчивость функционирования системы. Для этого необходимо учитывать не только сам факт возникновения сбоя, но и возможные сценарии развития событий после его проявления. Как видно из таблицы 1, наиболее критичными для функционирования систем умного дома являются факторы, связанные с электропитанием, сетевым взаимодействием, работой центрального контроллера, исполнительных устройств, а также наличием резервных механизмов управления [1].

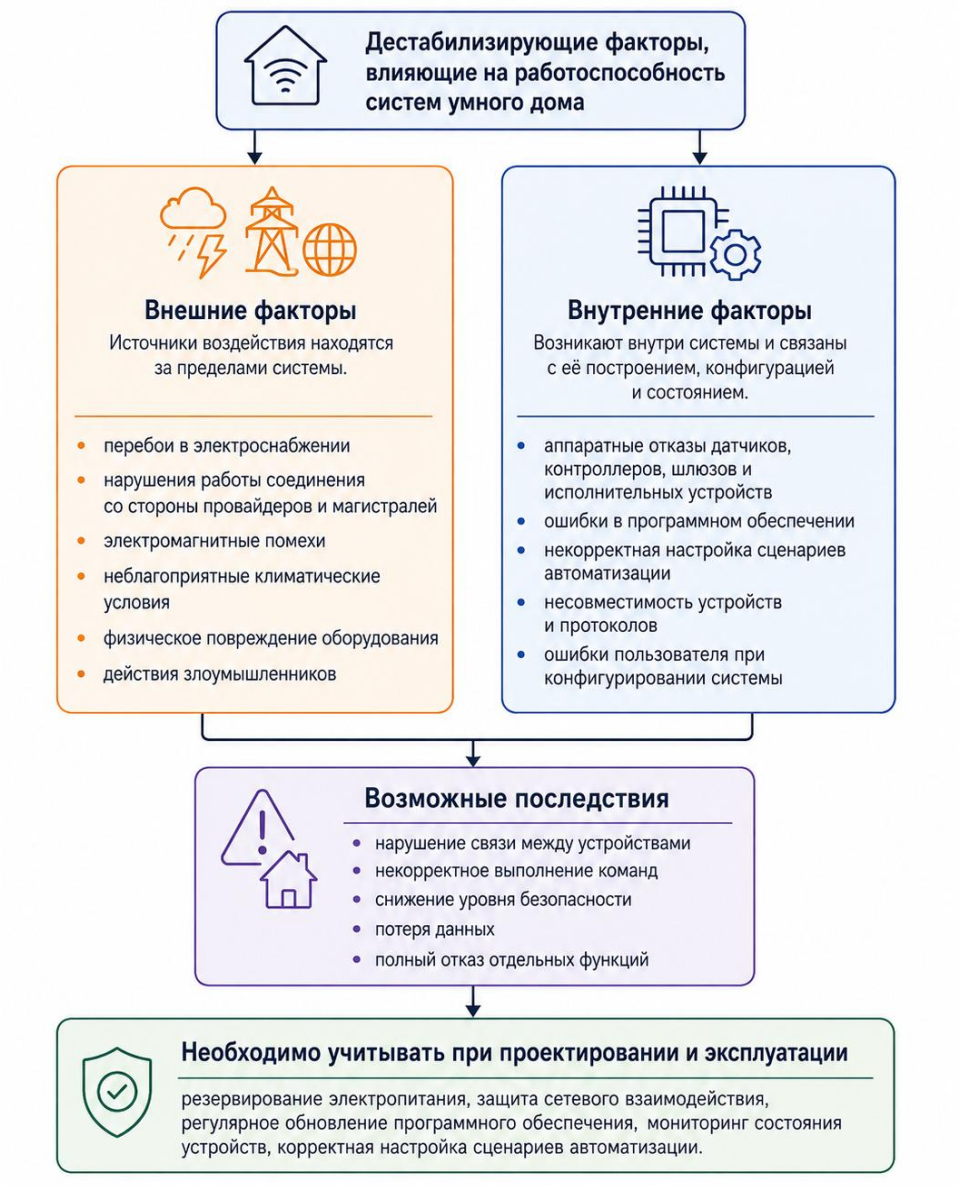

Рис. 1. Дестабилизирующие факторы функционирования информационных систем умного дома

Таблица 1

Дестабилизирующие факторы систем умного дома

Категория фактора	Фактор	Критичность	Вероятные сценарии развития событий
Внешний	Выход из строя электропитания	Высокая	Прекращение работы контроллера системы и/или её компонентов
Внутренний	Сбои локальной сети	Высокая	Потеря связи между устройствами
Внешний	Отсутствие доступа к сети Интернет	Низкая	Утеря возможности удалённого управления. Невозможность

			обновления программного обеспечения устройств
Внутренний	Выход из строя центрального контроллера	Высокая	Нарушение координации работы устройств системы
Внутренний	Выход из строя датчиков	Средняя	Получение неполных или недостоверных данных о состоянии среды, и, как следствие, некорректная работа компонентов и функционирования системы
Внутренний	Выход из строя исполнительных устройств	Высокая	Невозможность выполнения команд пользователя или автоматических сценариев
Внутренний	Ошибки программного обеспечения	Средняя	Некорректная обработка команд, зависание приложения, некорректное выполнение сценариев, самопроизвольное включение или отключение устройств
Внутренний	Несовместимость устройств и протоколов	Средняя	Нарушение соединения и невозможность взаимодействия между компонентами системы
Внутренний	Перегрузка системы	Средняя	Рост задержек при обработке команд, снижение скорости реакции системы
Внешний	Ошибки пользователя	Средняя	Неправильная настройка сценариев, отключение важных уведомлений
Внешний	Несанкционированный доступ к системе	Высокая	Возможность злоумышленника манипулировать устройствами
Внешний	Физическое повреждение устройств	Средняя	Полный или частичный отказ отдельных модулей устройств
Внешний	Неблагоприятные условия эксплуатации	Средняя	Перегрев, переохлаждение, повышенная влажность или загрязнение оборудования

Нештатное отключение электропитания крайне пагубно для обрабатываемой и хранящейся на носителе информации. Особо восприимчивы к этому фактору модули памяти IoT-устройств. Данный фактор технически можно ослабить. Достаточно использовать источники бесперебойного питания (ИБП), резервный блок в которых обеспечит непрерывность подачи электротока на целевое оборудование. Вместе с этим большинство современных ИБП оснащены системами оповещения о сбоях.

Сбои локальной сети могут возникать из-за физических повреждений кабелей, неисправного оборудования или конфликтов распределения компьютерных сетей. Особенность данного фактора заключается в том, что система может

оставаться физически исправной, но её элементы перестают взаимодействовать как единый комплекс.

Нарушения доступа к сети Интернет существенно ограничивают функции, связанные с удалённым управлением, облачными сервисами, мобильными приложениями, голосовыми помощниками и внешними уведомлениями. При этом механизмы локальных взаимодействий могут оставаться в штатном режиме. В то же время существуют системы, которые во многом зависимы от облачных инфраструктур, из-за этого разрыв Интернет-соединения может привести к нарушениям функционирования системы умного дома.

Центральный контроллер является ключевым элементом системы умного дома, так как он координирует работу датчиков, исполнительных устройств и сценариев автоматизации. При отказе контроллера датчики могут продолжать фиксировать события, но команды на исполнительные устройства формироваться не будут, что снижает управляемость и безопасность системы. Во многих современных структурах Интернета-вещей предусмотрено ручное и/или прямое управление оборудованием.

Выход из строя датчиков приводит к потере или искажению информации о состоянии окружающей среды и объектов управления. Например, неисправные датчики движения, температуры, дыма, протечки воды или открытия двери могут пропустить важное событие либо, наоборот, вызвать ложное срабатывание. Поскольку датчики являются основным источником данных для принятия решений, их отказ напрямую влияет на корректность автоматизации и своевременность реакции системы. Данный фактор наиболее сильно влияет на безопасность здоровья и жизни пользователя, а также на сохранность и обеспечение целостности его имущества.

Исполнительные устройства отвечают за практическое выполнение управляющих воздействий: включение света, перекрытие воды, открытие замков, управление отоплением, вентиляцией, шторами и другими элементами. Их выход из строя означает, что система может правильно обнаружить событие и сформировать команду, но фактическое действие выполнено не будет.

Ошибки программного обеспечения связаны с некорректной работой прошивок устройств, мобильных приложений, серверных компонентов, контроллера или сценариев автоматизации. Они могут проявляться в виде зависаний, неправильной обработки данных, потери настроек, некорректного выполнения команд или конфликтов между сценариями.

Несовместимость устройств и протоколов возникает при попытке объединить в одной системе оборудование разных производителей, использующее различные стандарты связи и форматы обмена данными.

Перегрузка системы возникает при превышении допустимого количества подключённых устройств, интенсивности сетевого обмена или объёма обрабатываемых данных (EPS). Это может привести к замедлению реакции системы, задержкам выполнения команд, сбоям сценариев, зависанию контроллера или потере отдельных сообщений. Особенно часто такой фактор проявляется в сложных системах, где одновременно работают камеры, датчики, голосовые помощники, климат-контроль системы и другие.

Ошибки пользователя связаны с неправильной настройкой, эксплуатацией или обслуживанием системы умного дома. Пользователь может некорректно задать сценарии, отключить важные устройства, установить слабые пароли, удалить необходимые правила автоматизации или неправильно подключить оборудование. Несанкционированный доступ к системе представляет собой угрозу безопасности, при которой постороннее лицо получает возможность управлять устройствами, просматривать данные или изменять настройки умного дома. Физическое повреждение устройств связано с механическим воздействием на элементы системы умного дома. Повреждение корпуса, контактов, антенн, разъёмов или внутренних компонентов может привести к полной неработоспособности устройства, ухудшению связи или нестабильной передаче данных. Неблагоприятные условия эксплуатации включают воздействие повышенной влажности, пыли, высокой или низкой температуры, вибраций, перепадов напряжения и электромагнитных помех. В паспорте изделия производитель указывает условия эксплуатации и любые отклонения от этих и есть неблагоприятные, благодаря

этому конечный пользователь может заранее подобрать необходимые устройства с учётом особенностей воздействия окружения в целевом помещении на это самое устройство. Отсутствие резервных механизмов управления означает, что при отказе основного канала связи, контроллера, электропитания или программного обеспечения пользователь не имеет альтернативного способа управлять системой. Наличие резервных механизмов, таких как ручное управление, автономные сценарии, резервное питание или локальный доступ, повышает устойчивость системы и уменьшает ущерб, обусловленный отказами оборудования.

Выводы.

1. Проведённый анализ показал, что устойчивость работы систем умного дома зависит от совокупного влияния технических, программных, сетевых, эксплуатационных и внешних факторов. Их изолированное рассмотрение не позволяет в полной мере оценить возможные последствия отказов, поскольку один и тот же фактор в разных архитектурах системы может приводить к различным сценариям нарушения функционирования.

2. Практическая значимость рассмотренного подхода заключается в возможности использовать классификацию дестабилизирующих факторов и уровни их критичности при проектировании, эксплуатации и модернизации систем умного дома. Это позволяет заранее выявлять наиболее уязвимые элементы системы, снижать вероятность отказов и минимизировать последствия их возникновения.

Список литературы

1. Вольвач А.В. Уязвимости системы «Умный дом» / А.В. Вольвач, Н.С. Поддубная // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – №1(52). – С. 49–52. DOI 10.17072/1993-0550-2021-1-49-52. EDN RZZWTY

2. Калюх Е.Д. «Умный дом»: преимущества и скрытые угрозы / Е.Д. Калюх, Д.В. Тихоненко // Актуальные проблемы авиации и космонавтики. – 2022. – Т. 2. – С. 408–410. – URL: https://kmu.itmo.ru/file/download/application/43690 (дата обращения: 17.05.2026).

3. Рычкова В.А. Надежность системы «Умный дом» как основного критерия эффективности функционирования объекта / В.А. Рычкова // Вестник науки и образования. – 2019. – №4-2(58). – С. 31–34. EDN YYABGP

4. Надеждин Е.Н. Математические методы и модели поддержки принятия решений / Е.Н. Надеждин. – М.: КНОРУС, 2026. – 240 с. EDN CJLVXV

5. Ходжамаммедов М.М. Безопасность Интернета вещей (IoT): защита умных устройств и сенсорных сетей от взлома / М.М. Ходжамаммедов // Международный научный журнал. – 2024. – URL: https://cyberleninka.ru/article/n/bezopasnost-interneta-veschey-iot-zaschita-umnyh-ustroystv-i-sensornyh-setey-ot-vzloma (дата обращения: 17.05.2026).