Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 681.586:004.8

Ньян Лин Хтет

Модели и алгоритмы для обеспечения кибер- и энергобезопасности информационной системы «Умный дом»

диссертация на соискание степени магистра технических наук
по специальности 7-06-0713-03
«Радиосистемы и радиотехнологии»

АВТОРЕФЕРАТ

_____Ньян Лин Хтет

Научный руководитель Лапцевич АлександрАнатольевич
Кандидат технических наук,доцент

Минск 2026

ВВЕДЕНИЕ

В современную эпоху стремительного научно-технического прогресса технологии Интернета вещей (IoT) стали неотъемлемой частью повседневной жизни, превращая традиционные дома в интеллектуальные киберфизические экосистемы — системы «умного дома» (Smart Home Systems, SHS). Современный «умный дом» — это сложная многоуровневая платформа, объединяющая разнородное оборудование (датчики, контроллеры, исполнительные механизмы), беспроводные и проводные протоколы связи (Wi-Fi, Zigbee, Z-Wave, KNX), облачные сервисы и интеллектуальные интерфейсы управления. Интеграция этих компонентов позволяет автоматизировать процессы жизнеобеспечения, повысить комфорт и оптимизировать энергопотребление.

Однако быстрое расширение функциональности устройств IoT создает серьезные проблемы безопасности. Большинство потребительских «умных» устройств имеют ограниченные вычислительные ресурсы и выпускаются со значительными уязвимостями: неизменяемые пароли по умолчанию, отсутствие надежных механизмов обновления прошивки и слабое шифрование каналов связи. В отличие от традиционных ИТ-систем, в «умном доме» цифровые угрозы напрямую приводят к рискам физической безопасности, угрожая конфиденциальности, сохранности имущества и здоровью жильцов.

В целом, результатом данной диссертации является всестороннее понимание (идентификация) рисков кибербезопасности, связанных с внедрением систем «умного дома», а также модель кибербезопасности, детализирующая протоколы маршрутизации пакетов данных для обмена информацией.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами :
Диссертационная работа выполнена в соответствии с научными направлениями исследований УО «Белорусский государственный университет информатики и радиоэлектроники», связанными с разработкой

комплексных систем кибербезопасности, интеллектуального управления и интеграции энергосберегающих технологий в рамках концепции «Умный дом» (Smart Home Systems).

Цель работы:
Целью работы является повышение уровня энергетической и информационной безопасности информационной системы «Умный дом» путем разработки комплексных моделей прикрытия от дестабилизирующих воздействий, алгоритмов обнаружения кибератак и оптимизации систем резервного электроснабжения.

Задачи исследования:
Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить архитектуру, уязвимости и риски информационной системы «Умный дом» в контексте обеспечения триады CIA (конфиденциальность, целостность, доступность).
2. Провести классификацию внешних и внутренних угроз энергетической и информационной безопасности.
3. Разработать математические модели прикрытия системы от дестабилизирующих воздействий.
4. Разработать алгоритмы обнаружения и нейтрализации кибератак (включая DoS/DDoS, MitM) на компоненты «Умного дома».
5. Создать модель оптимизации параметров системы бесперебойного питания (ИБП, АКБ) на основе возобновляемых источников энергии.
6. Разработать программное обеспечение для имитационного моделирования и верификации предложенных решений.
7. Оценить эффективность разработанной комплексной системы безопасности.

Объект исследования:
Объектом исследования является информационная система «Умный дом» (Smart Home System), интегрированная с локальной системой энергоснабжения и элементами автоматизации.

Предмет исследования:
Предметом исследования являются процессы, модели, алгоритмы и программно-аппаратные методы обеспечения информационной и

энергетической безопасности, а также защиты от несанкционированного доступа и дестабилизирующих факторов в «Умном доме».

Положения, выносимые на защиту

1. Комплексная классификация и математические модели прикрытия ИС «Умный дом» от внешних и внутренних угроз информационной и энергетической безопасности.
2. Алгоритмы оперативного обнаружения, изоляции и нейтрализации сетевых кибератак на интеллектуальные компоненты и API-интерфейсы системы.
3. Методика оптимизации и управления резервным энергоснабжением «Умного дома» с использованием ИБП и возобновляемых источников энергии в условиях аварийных отключений.

Научная новизна:

Разработан интегрированный подход, объединяющий информационную и энергетическую безопасность «Умного дома» в единую защищенную экосистему.

Предложены модифицированные алгоритмы обнаружения аномального трафика

(кибератак), адаптированные под низковычислительные устройства Интернета

вещей (IoT).

Разработана математическая модель динамического распределения резервной

мощности, учитывающая приоритетность критически важных узлов ИС.

Практическая значимость работы

Практическая ценность результатов исследования заключается в создании инженерных методик и программных модулей, которые могут быть непосредственно использованы при проектировании и развертывании безопасных систем «Умного дома». Внедрение разработанных алгоритмов позволяет снизить риск успешных кибератак, предотвратить потерю данных и обеспечить непрерывность функционирования критических систем жизнеобеспечения при сбоях в электросети.

Структура и объем диссертации

Диссертационная работа состоит из введения, 4 глав, заключения и списка использованных источников. Общий объем работы составляет 104 страницы.

В тексте содержится необходимый иллюстративный материал (рисунки и таблицы), отражающий результаты моделирования. Список литературы включает актуальные отечественные и зарубежные научные публикации.

Публикации и выступления на конференциях:

1. Ньян Л. Х. Современные коммуникационные технологии и инфраструктура для эффективных интеллектуальных транспортных систем в устойчивых умных городах/ Ньян Л. Х. // Секция №4 «Актуальные аспекты организации сетей телекоммуникаций и инфокоммуникационных систем».//XXVI Международной научно-технической конференции «Новые информационные технологии в телекоммуникациях и почтовой связи» (Республика Беларусь, Минск, 21–22 мая 2026 года), Минск: БГАС, 2026.
2. Коронец В. Г, Ньян Л. Х. Алгоритмы динамической оптимизации энергопотребления в системе информационной безопасности “Умный дом” / Коронец В. Г ,Ньян Л. Х. // Секция №2: «Инфокоммуникационные технологии и обеспечение информационной безопасности»// XXVI Международной научно-технической конференции «Новые информационные технологии в телекоммуникациях и почтовой связи» (Республика Беларусь, Минск, 21–22 мая 2026 года), Минск: БГАС, 2026.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В главе 1 «Концепция энергетической и информационной безопасности в системе "Умный дом"» проведен системный анализ архитектуры современных SHS. Обоснована взаимосвязь между физическим уровнем электропитания и цифровым уровнем управления. Определены ключевые уязвимости гетерогенных устройств IoT (слабое шифрование, отсутствие обновлений прошивок) и сформулированы базовые требования к концепции комплексной безопасности.

В главе 2 «Анализ угроз и модели обеспечения прикрытия информационной системы "Умный дом"» разработана усовершенствованная матричная модель взаимодействия дестабилизирующих факторов (8 факторов нестабильности и 5 источников угроз). Предложена гибридная модель внутренней защиты, сочетающая атрибутивный доступ (ABAC) и ограничение локальной зоны (геозонирование). Доказана необходимость модернизации каналов связи KNX до уровней KNX Data Secure (на уровне данных) и KNX IP

Secure (AES-128 CCM на сетевом уровне) с добавлением временных меток пакетов.

В главе 3 «Разработка алгоритмов обеспечения энергетической безопасности и устойчивости системы» предложены алгоритмы динамической оптимизации энергопотребления. Разработаны методы эффективной интеграции возобновляемых источников энергии (солнечных панелей) и алгоритмы балансировки нагрузки. Модель осуществляет приоритизацию потребителей, отключая второстепенные узлы и сохраняя питание критически важных элементов ИБ при авариях.

В главе 4 «Модель кибербезопасности системы "Умный дом" с использованием протоколов динамической маршрутизации в среде GNS-3» проведено имитационное моделирование предложенных решений. Для обнаружения аномального трафика успешно применены модели машинного обучения (Случайный лес, SVM, наивный байесовский классификатор). Для обеспечения целостности и невозможности удаления журналов событий интегрирована распределенная архитектура блокчейн (алгоритмы консенсуса PoA и PBFT). Проведен анализ безопасности сети при использовании протоколов динамической маршрутизации.

ЗАКЛЮЧЕНИЕ

В магистерской диссертации успешно решена важная научно-практическая задача по созданию комплексной системы кибер- и энергобезопасности «Умного дома». Предложенные математические модели прикрытия, интеллектуальные алгоритмы фильтрации атак на базе машинного обучения и блокчейна, а также методы оптимизации резервного питания подтвердили свою эффективность в ходе моделирования в GNS-3. Результаты работы создают надежную теоретическую и прикладную основу для проектирования защищенных интеллектуальных киберфизических систем нового поколения.