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

УДК004.415.2.031.43

Кундро
Евгений Валерьевич

# МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ «УМНЫЙ ДОМ»

**АВТОРЕФЕРАТ**

на соискание степени магистра технических наук
по специальности 1-23 80 08 – Психология труда, инженерная психология, эргономика

Научный руководитель
Т. Г. Таболич, кандидат технических наук, доцент

Минск 2019

# ВВЕДЕНИЕ

Система «умный дом» - это программно-аппаратный комплекс, который объединяет в себе оборудование, решающее различные задачи по управлению системами жизнеобеспечения (отопление, газоснабжение, водоснабжение, электроэнергия, система пожарной безопасности, охрана здания) и создающее комфорт в помещении (система освещения, управление бытовыми приборами, жалюзи). Система «умный дом» обрабатывает огромные потоки информации. В этой связи система «умный дом» подвергается угрозам информационной безопасности. Повышенный уровень автоматизации влечёт за собой новые проблемы безопасности. Появляется необходимость устранения возможности внедрения злоумышленников в автоматизированные системы.

На данный момент, к сожалению, разработки в области технологии «умный дом» не содержат единой методологии описания систем «умный дом», поэтому отсутствует и единая методология обнаружения и оценки угроз информационной безопасности системы «умный дом».

Угрозы информационной безопасности зависят напрямую от методов построения системы «умный дом», а также от применяемых технологий и обрабатываемой информации. Тестирование нескольких общедоступных систем «умный дом» доказывает наличие проблем с информационной безопасностью в предлагаемых компаниями системах «умный дом». Многие существующие решения для дополнительной защиты информационной безопасности «умного дома» используют метод работы, который заключается в подключении к роутеру и мониторинге потока информации между подключенными к Wi-Fi устройствами. Данный метод ограничивает круг поддерживаемых устройств. Также некоторые из решений, существующих на данный момент, осуществляют дополнительный сбор и отправку данных о работе устройств «умного дома» в облачное хранилище, что является дополнительной угрозой. Приведенные аспекты анализа состояния области информационной безопасности технологии «умный дом» доказывают актуальность рассматриваемой темы.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Проведенный анализ технологии «умный дом» и существующих решений защиты информации систем «умный дом» показал отсутствие единой методологии описания систем «умный дом» и, следовательно, отсутствие единой методологии обнаружения и оценки угроз информационной безопасности «умного дома». В результате анализа была построена модель системы информационной безопасности для систем «умный дом» и сформирован список наиболее вероятных угроз информационной безопасности систем «умный дом».

Предложена классификация вероятных угроз информационной безопасности систем «умный дом», связывающая возможные угрозы с объектами управления системы «умный дом». Данная классификация позволяет определять и оценивать найденные в системе «умный дом» угрозы информационной безопасности. Для увеличения количества известных угроз и улучшения качества оценки угроз классификация может быть дополнена экспертами.

Спроектирована система информационной безопасности технологии «умный дом», разработаны алгоритмы работы системы, структуры описания данных и прототип информационной системы. Основные функции системы: определение состава системы «умный дом» и установка ограничений для показаний объектов управления пользователем или автоматически, мониторинг данных системы «умный дом» и генерация оповещений о состоянии системы «умный дом». При существовании в системе «умный дом» неизвестной угрозы система оповещает пользователя о подозрительных данных. Разработанная система использована для проведения имитационных экспериментов, в ходе которых в системе информационной безопасности генерировались исходные данные для имитации действий системы «умный дом», и анализа выявления возможных угроз информационной безопасности.

Для достижения поставленной цели в этой диссертации поставлены и решены следующие задачи:

- выделить и проанализировать основные угрозы информационной безопасности «умного дома»;
- разработать классификацию уязвимостей и угроз системы «умный дом», основанной на связи объекта управления и угрозы;
- спроектировать и разработать прототип системы безопасности, настраиваемой по под конкретную систему «умный дом».

# КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выбранной темы, дается краткая характеристика её разработанности, определяется объект и предмет исследования, цель и задачи.

Первая глава «Анализ существующих методов и подходов к проектированию системы безопасности объекта индивидуального строительства, оснащенного системой «умный дом»» носит теоритический характер и состоит из трех подразделов.

В подразделах 1.1 «Анализ и характеристика основных угроз информационной безопасности систем типа «умный дом»» и 1.2 «Анализ методов и существующих подходов защиты информации систем «умный дом»» рассматривается система «умный дом» в целом, а также рассматриваются и анализируются существующие методы, средства и решения позволяющие парировать и успешно избегать атаки на систему и угрозы безопасности. Методы оценки угроз основываются на модели системы «умный дом», а также на модели угроз, необходимо использовать список наиболее вероятных угроз и критерии: источники угроз, возможные последствия, уязвимости. В результате аналитического обзора предметной области принимается решение использовать способ описания системы «умный дом» путем разделения системы на подсистемы, так как данный способ используется многими исследователями и производителями систем «умный дом».

В подразделе 1.3 описаны краткие выводы по первой главе.

Во вторая главе «Теоретическая и практическая разработка методики обеспечения информационной безопасности системы «умный дом»» описывается метод мониторинга состояния системы. Для построения классификации угроз информационной безопасности используется список наиболее вероятных угроз. Также описывается метод мониторинга состояния системы.

Для описания классификации угроз информационной безопасности технологии «умный дом» используются наиболее вероятные угрозы, уязвимости, возможные последствия и критерии анализа угроз. Выделяются критерии для анализа угроз. С помощью диаграммы вариантов использования указываются основные функциональные требования. Определяются функциональные требования к системе информационной безопасности, описываются основные этапы работы системы и основные компоненты системы, разрабатываются алгоритмы, строятся диаграммы деятельности.

Разрабатываются следующие алгоритмы, лежащие в основе проектируемой системы:

1. Алгоритм определения пользователем состава системы «умный дом» и установки ограничений для объектов управления.

2. Алгоритм автоматического определения состава системы «умный дом» и ограничений объектов управления.

3. Алгоритм мониторинга состояния системы «умный дом».

В третьей главе «Разработка и испытание прототипа системы информационной безопасности, мониторинг состояния системы «умный дом»» разрабатывается и анализируется прототип системы информационной безопасности. В разрабатываемом прототипе используется компонент генерирования данных, с дальнейшим запуском их мониторинга. Завершающим этапом является мониторинг состояния всей системы, при обнаружении угроз и несоответствии показаний датчика или исполнительного механизма объектов управления изменяется статус элемента и пользователю поступает сообщение. Приводится список возможных ошибок, а также описывается метод определения угроз.

# ЗАКЛЮЧЕНИЕ

В данной работе проводится анализ основных информационных рисков системы «умный дом». Проектируется система информационной безопасности технологии «умный дом», разрабатываются алгоритмы работы системы, структуры описания данных и прототип информационной системы. Анализируется целесообразность построения комплексной системы информационной безопасности. Разработанная система использована для проведения имитационных экспериментов, в ходе которых в системе информационной безопасности генерировались исходные данные для имитации действий системы «умный дом», и анализа выявления возможных угроз информационной безопасности.

# СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Кундро, Е. В. Защита информации в проекте «Умный дом» / Е. В. Кундро // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 31–38.

Кундро, Е. В. Информационная безопасность системы «Умный дом» / Е. В. Кундро // 54-я науч. конф. аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»: материалы конференции по направлению 8: Информационные системы и технологии (Минск, 21 апреля 2018 года) / редкол. В. И. Пачинин, А. А. Охрименко. – Часть 2. – Минск: БГУИР, 2018. – 16 с. – С. 11.