Министерство образования и науки Российской Федерации

федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки 09.04.03 Прикладная информатика
Кафедра Программной инженерии

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Информационная система мониторинга и оценки угроз информационной безопасности технологии "умный дом"

УДК 728.37:004.896.056

Студент

Группа	ФИО	Подпись	Дата
8КМ51	В.И. Абдрашитова		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Н.Ю. Хабибулина	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
ассистент	К.А. Баннова	к.э.н.		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	М.И. Пустовойтова	к.х.н.		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ПИ	М.А. Иванов	к.т.н.		

Томск – 2017 г.

Запланированные результаты обучения по ООП

Код результатов	Результат обучения (выпускник должен быть готов)
Профессиональные компетенции	
Р1	Применять глубокие естественнонаучные и математические знания для решения научных и инженерных задач в области прикладной информатики.
Р2	Применять глубокие специальные знания в области информатики для решения междисциплинарных инженерных задач.
Р3	Уметь ставить перед собой и решать задачи инженерного характера, связанные с созданием программных средств информационных и автоматизированных систем, с использованием изученных моделей и аналитических методов.
Р4	Выполнять инновационные инженерные проекты по разработке программных средств автоматизированных систем различного назначения и направленности с использованием современных систем и методов проектирования.
Р5	Планировать и проводить теоретические и экспериментальные исследования в области проектирования программных средств автоматизированных систем с использованием современных технологий, при этом используя отечественный и зарубежный опыт. Критически оценивать полученные данные и делать выводы.
Р6	Осуществлять сопровождение процессов проектирования, внедрения и эксплуатации программных систем различного назначения.
Универсальные компетенции	
Р7	Использовать глубокие знания по проектному менеджменту для ведения инновационной инженерной деятельности с учетом юридических аспектов защиты интеллектуальной собственности.
Р8	Осуществлять коммуникации в профессиональной среде и в обществе в целом, разрабатывать документацию, презентовать и

Код результатов	Результат обучения (выпускник должен быть готов)
	защищать результаты инженерной деятельности.
Р9	Эффективно работать индивидуально и в качестве члена и руководителя группы, в том числе междисциплинарной и международной, при решении инновационных инженерных задач.
Р10	Демонстрировать личную ответственность и готовность следовать профессиональной этике и нормам ведения инженерной деятельности. Демонстрировать глубокие знания правовых, социальных, экологических и культурных аспектов инженерной деятельности.
Р11	Демонстрировать способность к самостоятельному обучению, непрерывному самосовершенствованию в инженерной деятельности.

Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки 09.04.03 Прикладная информатика
Кафедра Программной инженерии

УТВЕРЖДАЮ:
Зав. кафедрой ОСУ
_____ _____ _____М.А.Иванов___
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

магистерской диссертации

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	**ФИО**
8КМ51	В.И. Абдрашитова

Тема работы:

Информационная система мониторинга и оценки угроз информационной безопасности технологии "умный дом"	
Утверждена приказом директора (дата, номер)	01.03.2014 №1484/с

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе *(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).*	Программный продукт должен иметь возможность настройки состава системы «умный дом», выполнять мониторинг состояния системы «умный дом» и оценку возникающих угроз информационной безопасности.

Перечень подлежащих исследованию, проектированию и разработке вопросов *(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).*	1. Аналитический обзор предметной области. 2. Обзор и сравнение существующих решений. 3. Разработка классификации угроз информационной безопасности. 4. Проектирование информационной системы мониторинга и оценки угроз информационной безопасности технологии «умный дом» 5. Разработка прототипа информационной системы мониторинга и оценки угроз информационной безопасности технологии «умный дом» 6. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение 7. Социальная ответственность
Перечень графического материала *(с точным указанием обязательных чертежей)*	

Консультанты по разделам выпускной квалификационной работы

(с указанием разделов)

Раздел	Консультант
Социальная ответственность	М.И. Пустовойтова
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	К.А. Баннова
Приложение A. An overview of smart homes and information security of smart homes	Т.В. Сидоренко Е.С. Чердынцев

Названия разделов, которые должны быть написаны на русском и иностранном языках:

Обзор технологии «Умный дом»

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент каф. ПИ	Хабибулина Н.Ю.	к.т.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8КМ51	Абдрашитова В.И.		

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки: 09.04.03 Прикладная информатика
Уровень подготовки: магистр
Кафедра: Программной инженерии
Период выполнения: осенний семестр 2015 г. – весенний семестр 2017 г.

Форма представления работы: магистерская диссертация

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
03.04.2017	Обзор технологии «Умный дом»	5
03.04.2017	Объект и методы исследования	10
17.04.2017	Классификация угроз информационной безопасности	15
01.05.2017	Проектирование системы информационной безопасности	25
20.05.2017	Прототип системы информационной безопасности	20
17.05.2017	Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	10
17.05.2017	Социальная ответственность	10
23.05.2017	Приложение А. An overview of smart homes and information security of smart homes.	5

Составил преподаватель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Н.Ю. Хабибулина	к.т.н.		

СОГЛАСОВАНО:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ПИ	М.А. Иванов	к.т.н.		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8КМ51	В.И. Абдрашитова

Институт	Институт кибернетики	**Кафедра**	Программной инженерии
Уровень образования	Магистратура	**Направление/специальность**	Прикладная информатика

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих*	Стоимость ресурсов проведения разработки системы информационной безопасности технологии «умный дом». Ставки налогов и отчислений, применяемые в ТПУ.
2. *Нормы и нормативы расходования ресурсов*	
3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого потенциала, перспективности и альтернатив проведения НИ с позиции ресурсоэффективности и ресурсосбережения*	Оценка конкурентоспособности, рассмотрение альтернатив проведения НИ.
2. *Планирование и формирование бюджета научных исследований*	Планирование этапов разработки программы, определение трудоемкости, построение диаграммы Ганта, формирование бюджета НТИ.
3. *Определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования*	Сравнительный анализ интегральных показателей эффективности.
Перечень графического материала *(с точным указанием обязательных чертежей)***:**	
1. *Оценка конкурентоспособности технических решений* 2. *Альтернативы проведения НТИ* 3. *График проведения и бюджет НТИ* 4. *Матрица SWOT* 5. *Оценка ресурсной, финансовой и экономической эффективности НТИ*	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент	К.А. Баннова	к.э.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8КМ51	В.И. Абдрашитова		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8КМ51	В.И. Абдрашитова

Институт	Институт кибернетики	**Кафедра**	Программной инженерии
Уровень образования	Магистратура	**Направление/специальность**	Прикладная информатика

Исходные данные к разделу «Социальная ответственность»:	
1. *Описание рабочего места (рабочей зоны, технологического процесса, механического оборудования) на предмет возникновения:* – *вредных проявлений факторов производственной среды (метеоусловия, вредные вещества, освещение, шумы, вибрации, электромагнитные поля, ионизирующие излучения)* – *опасных проявлений факторов производственной среды (механической природы, термического характера, электрической, пожарной и взрывной природы)* – *негативного воздействия на окружающую природную среду (атмосферу, гидросферу, литосферу)* – *чрезвычайных ситуаций (техногенного, стихийного, экологического и социального характера)*	Рабочее место – учебный кабинет с персональным компьютером. - Возможно возникновение вредных проявлений факторов производственной среды: • Недостаточная освещенность рабочей зоны • Отклонение показателей микроклимата • Повышенный уровень шума на рабочем месте • Повышенный уровень электромагнитных излучений - Возможно возникновение опасных проявлений факторов производственной среды: • Электрический ток • Возможности возникновения пожара - Возможно возникновение негативного воздействия на окружающую природную среду: утилизация компьютеров и другой оргтехники
2. *Знакомство и отбор законодательных и нормативных документов по теме*	- ГОСТ 12.1.003 – 83 - ГОСТ 12.1. 045 – 84 - ГОСТ 12.2.032 – 78 - Р 2.2.2006 – 05 - СанПиН 2.2.1/2.1.1.1278 – 03 - СанПиН 2.2.2/2.4.1340 – 03 - СанПиН 2.2.4.3359-16 - СанПиН 2.2.4.548 – 96 - СанПиН 2.2.4.1191 – 03 - СН 2.2.4/2.1.8.562 – 96 - СНиП 2.04.05 – 91 - СНиП 21 – 01 – 97 - СНиП 23 – 03 – 2003
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Анализ выявленных вредных факторов проектируемой производственной среды в следующей последовательности:* – *физико-химическая природа вредности, её связь с разрабатываемой темой;* – *действие фактора на организм человека;* – *приведение допустимых норм с необходимой размерностью (со ссылкой на соответствующий нормативно-технический документ);* – *предлагаемые средства защиты (сначала коллективной защиты, затем – индивидуальные защитные средства)*	Анализ выявленных вредных факторов: - Отклонение показателей микроклимата - Повышенный уровень шума - Повышенный уровень электромагнитных излучений - Повышенное уровень ионизирующих излучений - Недостаточная освещенность рабочей зоны

2. *Анализ выявленных опасных факторов проектируемой произведённой среды в следующей последовательности* – *механические опасности (источники, средства защиты;* – *термические опасности (источники, средства защиты);* – *электробезопасность (в т.ч. статическое электричество, молниезащита – источники, средства защиты);* – *пожаровзрывобезопасность (причины, профилактические мероприятия, первичные средства пожаротушения)*	Анализ выявленных опасных факторов: - Статическое электричество - Короткое замыкание - Пожароопасность
3. *Охрана окружающей среды:* – *защита селитебной зоны* – *анализ воздействия объекта на атмосферу (выбросы);* – *анализ воздействия объекта на гидросферу (сбросы);* – *анализ воздействия объекта на литосферу (отходы);* – *разработать решения по обеспечению экологической безопасности со ссылками на НТД по охране окружающей среды.*	Анализ негативного воздействия на окружающую природную среду: утилизация компьютеров и другой оргтехники
4. *Защита в чрезвычайных ситуациях:* – *перечень возможных ЧС на объекте;* – *выбор наиболее типичной ЧС;* – *разработка превентивных мер по предупреждению ЧС;* – *разработка мер по повышению устойчивости объекта к данной ЧС;* – *разработка действий в результате возникшей ЧС и мер по ликвидации её последствий*	Возможные чрезвычайные ситуации: - Пожар
5. *Правовые и организационные вопросы обеспечения безопасности:* – *специальные (характерные для проектируемой рабочей зоны) правовые нормы трудового законодательства;* – *организационные мероприятия при компоновке рабочей зоны*	- Рабочее место при выполнении работ сидя регулируется ГОСТом 12.2.032 – 78 - Организация рабочих мест с электронно-вычислительными машинами регулируется СанПиНом 2.2.2/2.4.1340 – 03
Перечень графического материала:	
При необходимости представить эскизные графические материалы к расчётному заданию (обязательно для специалистов и магистров)	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	М.И. Пустовойтова	к.х.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8КМ51	В.И. Абдрашитова		

Реферат

Выпускная квалификационная работа 122 с., 27 рис., 20 табл., 40 источников, 7 прил.

Ключевые слова: система умный дом, информационная безопасность, угрозы информационной безопасности, классификация угроз информационной безопасности, оценка угроз информационной безопасности.

Объектом исследования являются система «умный дом» и угрозы информационной безопасности технологии «Умный дом».

Цель работы – проектирование системы мониторинга и оценки угроз информационной безопасности технологии «Умный дом», настраиваемую под любую конфигурацию системы «умный дом».

В процессе исследования проводились обзор технологии «Умный дом», существующих решений и методов построения систем для защиты информационной безопасности систем «умный дом», классификация угроз информационной безопасности.

В результате исследования спроектирована система информационной безопасности технологии «Умный дом» и разработан прототип системы информационной безопасности.

Область применения: жилые помещения, в которых установлена система «умный дом».

Результаты работы позволяют разработать в будущем систему информационной безопасности, настраиваемую под систему «умный дом» любого вида, для обеспечения или повышения уровня информационной безопасности системы.

Определения, обозначения, сокращения

В данной работе приведены следующие термины:

система «умный дом»: Совокупность подключенных в общую сеть устройств, выполняющих определенные действия с минимальным участием человека.

«умные» устройства: Устройства, выполняющие определенные действия с минимальным участием человека.

технология «Умный дом»: Технология построения системы «умный дом».

информационная безопасность: Состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере.

«облако»: Облачное хранилище данных.

«идеальное» состояние: Состояние системы, в котором отсутствуют угрозы информационной безопасности.

В работе приведены следующие обозначения и сокращения:

УД – технология «умный дом»;

Система УД – система «умный дом»;

ИБ – информационная безопасность;

КЦД – конфиденциальность, целостность и доступность информации;

ПО – программное обеспечение;

НТИ – научно-техническое исследование;

ПДУ – предельно допустимый уровень;

ПК – персональный компьютер;

ИКТ – информационно-коммуникационные технологии;

ПЭВМ – персональная электронно-вычислительная машина.

Оглавление

Введение

Система «умный дом» является аппаратно-программным комплексом, внутри которого обрабатывается большой поток информации, в связи с чем система «умный дом» подвержена угрозам информационной безопасности. К сожалению, современные разработки в области технологии УД не содержат единой методологии описания систем УД, поэтому отсутствует и единая методология обнаружения и оценки угроз информационной безопасности технологии «умный дом».

Угрозы информационной безопасности зависят от методов построения системы УД, применяемых технологий и обрабатываемой информации, что подтверждают авторы статьи [1], представленной на Международном симпозиуме «Надежность и качество». Тестирование нескольких общедоступных систем УД, проводимое компанией AV-TEST [2], доказывает наличие проблем с информационной безопасностью в предлагаемых компаниями системах УД. Многие существующие решения для дополнительной защиты информационной безопасности УД используют метод работы, заключающийся в подключении к роутеру и мониторинге потока информации между подключенными к Wi-Fi устройствами. Данный метод ограничивает круг поддерживаемых устройств. Также некоторые из существующих решений осуществляют дополнительный сбор и отправку данных о работе устройств УД в облачное хранилище, что может стать дополнительной угрозой. Приведенные аспекты анализа состояния области информационной безопасности технологии УД доказывают актуальность рассматриваемой темы.

Цель работы – проектирование информационной системы мониторинга и оценки угроз информационной безопасности технологии «умный дом» и разработка прототипа спроектированной системы.

Объект исследования: технология «умный дом» и угрозы информационной безопасности, возникающие в ней. Предмет исследования:

методы проектирования системы информационной безопасности технологии «умный дом».

Практическая и научная новизна: разработка классификации уязвимостей и угроз системы УД, основанной на связи объекта управления и угрозы, проектирование и разработка прототипа системы информационной безопасности, настраиваемой под конкретную систему УД.

Практическая значимость результатов – спроектированная система информационной безопасности технологии «умный дом» может быть использована для обеспечения информационной безопасности в любых системах УД.

Результатом работы являются спроектированная система информационной безопасности технологии УД и разработанный прототип системы. Промежуточные и конечные результаты работы прошли апробацию на следующих конференциях:

– XIII Международная научно-практическая конференция студентов, аспирантов и молодых ученых «Молодежь и современные информационные технологии», г. Томск, 9-13 ноября 2015 г.;

– XIV Международная научно-практическая конференция студентов, аспирантов и молодых ученых «Молодежь и современные информационные технологии», г. Томск, 7-11 ноября 2016 г.;

– XXI Международная научно-техническая конференция студентов, аспирантов и молодых ученых «Научная сессия ТУСУР-2016», г. Томск, 25-27 мая 2016 г.;

– XXII Международная научно-техническая конференция студентов, аспирантов и молодых ученых «Научная сессия ТУСУР-2017», г. Томск, 10-12 мая 2017 г.

1. Обзор технологии «Умный дом»

1.1. Умный дом

Под термином «умный дом» (УД) принято понимать совокупность подключенных в общую сеть устройств, выполняющих определенные действия с минимальным участием человека. Идея создания УД в приближенном к сегодняшнему пониманию этого термина появилась в конце 20 века. Один из первых таких домов был описан в журнале «Popular Mechanics» в 1950 году [3]. Термин «умный дом» был введен в 1984 году американской Ассоциацией жилищно-строительных компаний [4] и к 2000 году идея «умных домов» имела достаточное распространение в Европе и, особенно, в США. В России первые упоминания о существовании технологии домашней автоматизации появились лишь около 1990 года [5, 6].

Технология УД используется для различных целей, можно выделить основные из них [7]:

– тепло- и энергосбережение;
– повышение комфорта;
– обеспечение безопасности.

Различные предприятия применяют технологию УД в основном для энергосбережения и безопасности, использование технологии для жилых помещений может быть для всех вышеописанных целей.

Компании-производители систем УД предлагают различные вариации систем: готовые решения «под ключ» и настраиваемые под требования конкретного клиента. Также на рынке представлены отдельные «умные» продукты (в основном выпускаемые производителями техники), которые пользователь может самостоятельно объединить в систему УД.

Системы «умный дом» не имеют единой методологии описания. Как компании, так и исследователи технологии УД, имеют различные подходы к описанию системы УД. Наиболее чаще встречаемый подход – разделение

системы УД на различные подсистемы. Обобщенное описание видов подсистем УД представлено на рисунке 1.

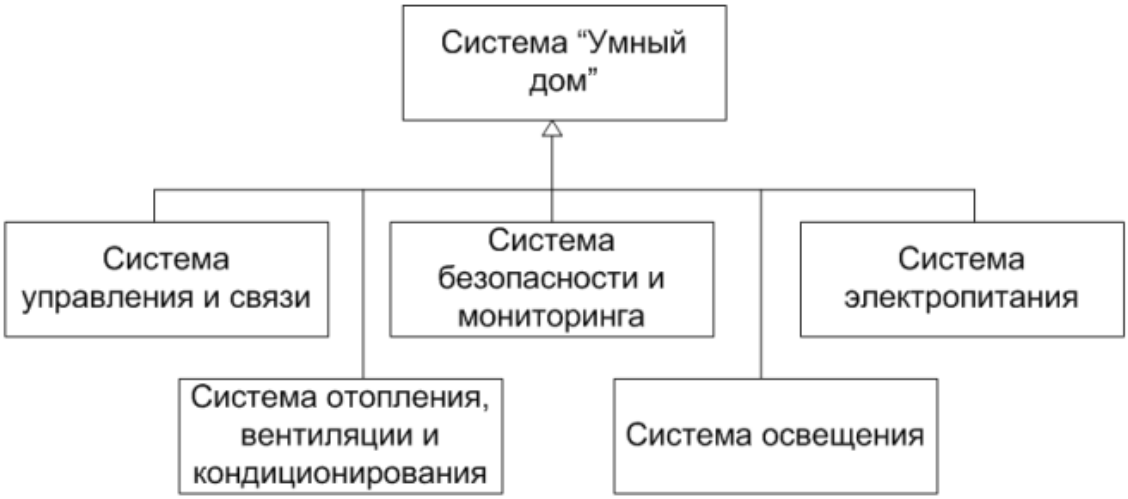

Рисунок 1 – Подсистемы «умного дома»

1.2.Защита информационной безопасности

Система УД является объектом информатизации, подверженным угрозам информационной безопасности [8]. Угрозы информационной безопасности системы зависят от методов построения системы, используемых технологий и обрабатываемых информационных потоков [1], поэтому не существует единой методологии способа защиты информационной безопасности.

Многие системы УД имеют встроенный компонент защиты информационной безопасности, но, к сожалению, данный компонент не всегда осуществляет высокий уровень защиты. В некоторых системах компонент информационной безопасности может даже отсутствовать. По этой причине некоторые компании начали производство дополнительных средств защиты информационной безопасности технологии УД, но, если компания является производителем «умных» устройств, то в большинстве случаев разрабатываемое средство защиты способно работать только с «умными устройствами» этой компании.

В 2014 году компания AV-TEST, являющаяся независимым институтом информационной безопасности, провела тестирование [2] нескольких общедоступных систем УД. AV-TEST исследовала:

– наличие шифрованной связи между элементами УД;

– использование активной аутентификации;

– возможность внешней манипуляции;

– уровень защищенности удаленного доступа.

Результаты тестирования семи систем УД показали:

– лишь три системы обеспечивают информационную безопасность;

– две системы недостаточно защищены и могут быть подвержены внутренним атакам;

– две системы имеют очень слабую информационную защиту и могут быть подвержены как внутренним, так и внешним атакам.

Проведенное тестирование доказывает, что даже пользователям готовых решений не следует забывать об информационной защите и при необходимости использовать дополнительные средства защиты, а производителям УД нужно выпускать продукты с более высоким уровнем защиты.

1.3.Существующие решения защиты информации систем «умный дом»

Как было сказано ранее, компании-производители средств защиты информации для УД, которые одновременно являются производителями «умных» устройств, чаще всего разрабатывают средства защиты для своих устройств. Но другие компании производят универсальные средства защиты информации. Далее рассмотрены несколько примеров таких устройств.

Один из распространенных методов работы на рынке устройств дополнительной информационной защиты УД – подключение к роутеру и мониторинг потока информации между подключенными к Wi-Fi устройствами.

Три ярких примера подобных устройств:

– Dojo, разработанное небольшой израильской компании Dojo-Labs [9];

– CUJO, разработанное группой калифорнийских исследователей [10];

– Bitdefender Box, производимое крупной компанией Bitdefender [11].

Основной недостаток данных устройств обусловлен выбором метода работы, что ограничивает защищаемые устройства. Так же устройства Dojo и CUJO осуществляют дополнительный сбор и отправление в «облако» данных о работе устройств, для определения новых угроз. Дополнительный сбор данных может являться дополнительной угрозой информационной безопасности, так как удаленное «облако» может быть так же подвержено атаке хакеров.

Существуют так же и более функциональные средства защиты информационной безопасности, которые могут контролировать всю сеть УД и не собирают дополнительные данные. Пример подобных устройств – серия устройств Cisco ASA 5500-X с функциями FirePOWER [12], производимая одной из крупнейших IT-компаний Cisco. Но предлагаемые функциональность и качество имеют соответствующую цену и сложность установки и эксплуатации, так как подобные устройства разработаны в основном для использования в средних и крупных компаниях, которые имеют необходимый персонал или возможность использования достаточно дорогостоящего сервисного обслуживания.

1.4. Модель построения системы мониторинга информационной безопасности

Отсутствие единой методологии построения защиты информационной безопасности технологии УД объясняет различные структуры и методы работы средств защиты. Разработку данных средств можно условно разделить на следующие этапы:

– описание модели системы УД;

– описание модели угроз информационной безопасности;

– разработка методов оценки угроз;

– разработка автоматического механизма мониторинга состояния защиты УД.

Методы оценки угроз основываются на модели системы УД и модели угроз, могут использовать список наиболее вероятных угроз и критерии: источники угроз, уязвимости, возможные последствия и др.

Один из примеров списка наиболее вероятных угроз [13] содержит следующие угрозы:

– хакерские атаки на центральный сервер;

– влияние вирусных и троянских программ на работу системы;

– перехват информации, передаваемой по проводным и беспроводным каналам связи;

– доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паролей и других реквизитов разграничения доступа;

– доступ к сети неавторизованных пользователей;

– наличие нарушителей в числе обслуживающего персонала;

– ошибки пользователя;

– кража (злоумышленный вывод) из строя аппаратуры;

– перебои в сети электропитания;

– стихийные бедствия;

– поломка аппаратуры системы;

– ошибки программного обеспечения;

– утечка информации через побочные электромагнитные излучения и наводки;

– утечка информации по акустоэлектрическому каналу.

2. Объект и методы исследования

Цель работы – проектирование информационной системы мониторинга и оценки угроз информационной безопасности (ИБ) технологии «умный дом» и разработка прототипа спроектированной системы.

Исследуемый объект – системы «умный дом» и возникающие в них угрозы информационной безопасности. Так как угрозы информационной безопасности зависят от методов построения системы, используемых технологий и обрабатываемых информационных потоков, исследуемые системы УД были сужены до систем «умный дом», применяемых в жилых домах.

Проектируемая система информационной системы мониторинга и оценки угроз информационной безопасности технологии «умный дом» основана на модели средства информационной безопасности, выделенной в процессе анализа литературных источников. Модель проектируемой системы:

– описание модели системы УД;

– описание модели угроз информационной безопасности;

– разработка методов оценки угроз;

– разработка автоматического механизма мониторинга состояния защиты УД.

Для проектирования системы информационной безопасности используются основные методы системного анализа и технологии разработки программного обеспечения. Системный анализ применяется для разрешения трудно формализуемых и слабо структурированных проблем для сведения сложной проблемы к взаимосвязанной иерархии более простых задач [14].

В результате аналитического обзора предметной области было принято решение использовать способ описания системы «умный дом» путем разделения системы на подсистемы, т.к. данный способ используется многими исследователями и производителями систем УД. В системе «умный дом» были выделены следующие подсистемы:

– подсистема управления и связи;

– подсистема безопасности и мониторинга;
– подсистема электропитания;
– подсистема освещения;
– подсистема отопления;
– подсистема вентиляции;
– подсистема кондиционирования;
– подсистема мультимедиа.

Далее предлагается разбиение подсистем на компоненты, объекты управления и элементы: датчик и исполнительный механизм. Компоненты отвечают за работу с объектами управления, а у объекта управления должен быть указан тип подсистемы. Все объекты управления в УД имеют датчик для считывания необходимых данных и исполнительный механизм, выполняющий какое-либо действие. Показатель датчика и действие исполнительного механизма непосредственно влияют на состояние объекта и состояние информационной безопасности всей системы УД, поэтому для них должны определяться ограничения.

Получение данных о составе системы УД предполагается следующими способами:

1. Пользователь самостоятельно описывает каждый элемент системы УД.

2. Система ИБ автоматически собирает данные с системы УД и определяет на их основе состав системы УД.

Для построения классификации угроз информационной безопасности технологии УД было решено использовать список наиболее вероятных угроз, описанный в предыдущем разделе и использовать следующие критерии:

– величина отклонения значения датчика или исполнительного механизма;
– возможные источники угрозы;
– возможные последствия угрозы;

– уязвимости.

Список угроз определяется экспертами для различных объектов управления в зависимости от подсистем, в которых они располагаются, и в зависимости от степени отклонения данных датчика или исполнительного механизма.

Метод мониторинга состояния УД основывается на следующих этапах:

– описание системы УД пользователя;
– получение данных с системы УД;
– анализ данных, сравнение с установленными ограничениями;
– определение подсистемы и объекта, в котором возникла угроза;
– оценка угрозы по определенному экспертами списку угроз.

Для описания модели системы УД и угроз в проектируемой системе выбран язык XML, для описания структуры данных файлов выбран язык XML-Schema. Выбор языков описания данных обусловлен большой вложенностью и большим объемом данных, формат XML эффективен в работе именно с такими данными. XML – расширяемый язык разметки, который позволяет создать любую необходимую для конкретной области применения разметку. Структуру XML-файла можно описать с помощью спецификации XML-Schema, которая определяет правила документа. XML имеет реализации «парсеров» (программы для анализа разметки) для всех современных языков программирования. Также XML поддерживается на низком аппаратном, микропрограммном и программном уровнях в современных аппаратных решениях.

Для разработки прототипа спроектированной системы выбраны:

– среда разработки Microsoft Visual Studio 2013;
– язык программирования C#;
– система для построения клиентского приложения Windows Presentation Foundation (WPF).

Выбор инструментов обусловлен в первую очередь имеющимся опытом работы.

Выбор версии среды разработки определен исходя из поддержки данной версии более новыми версиями, наличия при этом современного базового функционала и широкого распространения. Дополнительным плюсом сред разработки Visual Studio является наличие инструментов для работы с XML и XML-Schema файлами, в том числе автоматическая проверка при редактировании XML-файла, если в нем указана XML-Schema.

Система WPF выбрана по причине возможности использования любого .NET-совместимого языка программирования вместе с языком XAML. WPF и XAML объединяются в полнофункциональную систему представления для создания визуально привлекательных классических приложений Windows, включающих в себя пользовательский интерфейс, мультимедиа и сложные бизнес-модели.

Язык программирования C# имеет несколько классов для эффективной и быстрой работы с XML-документами, выбираемые в зависимости от поставленных задач.

3. Классификация угроз информационной безопасности системы «умный дом»

Для описания классификации угроз информационной безопасности технологии «умный дом» используются наиболее вероятные угрозы, уязвимости, возможные последствия [13] и критерии анализа угроз [15].

Выбор списка наиболее вероятных угроз был определен в предыдущем разделе. Было выделено три критерия для анализа угроз: источник угрозы, уязвимости безопасности информации, подсистема УД, в которой возникла угроза. Критерии источник угрозы и уязвимости безопасности информации делятся на категории и подкатегории.

Категории, подкатегории и примеры:

1. Источник угрозы
   a. Антропогенные источники
      i. Внешние (I.A.1 - I.A.6):
         – криминальные структуры, потенциальные преступники, хакеры и другие.
      ii. Внутренние (I.B.1 - I.B.4):
         – основной персонал, вспомогательный персонал, и другие.
   b. Техногенные источники
      i. Внешние (II.A.1 - II.A.3):
         – средства связи, сети инженерных коммуникации и другие.
      ii. Внутренние (II.B.1 - II.B.4):
         – некачественные технические средства обработки информации, некачественные программные средства обработки информации и другие.
   c. Стихийные источники (III.A.1 - III.A.7)
      – пожары, землетрясения, наводнения, ураганы и другие.
2. Уязвимости безопасности информации
   a. Объективные (A.I - A.IV):

– сопутствующие техническим средствам излучения, определяемые особенностями элементов, определяемые особенностями защищаемого объекта и другие.

b. Субъективные (B.I, B.II):

– ошибки и нарушения.

c. Случайные (C.I, C.II):

– сбои, отказы и повреждения.

После определения необходимых данных была построена классификация угроз информационной безопасности технологии «умный дом». Фрагмент полученной классификации представлен в таблице 1.

Таблица 1 – Фрагмент классификации угроз

Угроза (тип атаки)	**Источник угрозы**	**Уязвимость**	**Уязвимости безопасности информации**	**Возможные последствия**	**Подсистема**
Хакерские атаки на центральный сервер	I.A.1, I.A.2, I.A.3, I.A.4, I.A.5, I.A.6, I.B.1, I.B.2, I.B.3, I.B.4	Подключение сети «Умного дома» к Интернет. Отсутствие (неэффективность) механизмов защиты периметра сети	A.I.a, A.I.b A.II.a, A.II.b, A.III.b, A.IV.b, B.I.a, B.I.b, B.I.c, B.II.a, B.II.c, B.II.d C.I.a, C.I.c	Нарушение работы, либо выход из строя центрального сервера, и всей системы. Нарушение конфиденциальности, целостности и доступности информации (КЦД).	управления и связи
Перехват информации, передаваемой по проводным и беспроводным каналам связи	I.A.1, I.A.2, I.A.3, I.A.4, I.A.5, I.A.6, I.B.1, I.B.2, I.B.3, I.B.4 II.A.1, II.B.1,II.B.2	Возможность доступа злоумышленника к проводным каналам или к зоне устойчивого перехвата радиосигналов сети. Отсутствие (неэффективность) механизмов защиты трафика	A.I.a, A.I.b A.II.a, A.II.b A.III.a, A.III.b A.IV.a, A.IV.b B.I.a, B.I.b, B.I.c B.II.a, B.II.b B.II.c, B.II.d C.I.a,C.I.b,C.I.c, C.I.d, C.II.b	Нарушение конфиденциальности информации передаваемой по каналу. Возможен доступ к управлению системой.	управления и связи; безопасности и мониторинга; электропитания; освещения; отопления; вентиляции; кондиционирования; мультимедиа;
Доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паро-лей и других реквизитов разграничения доступа	I.A.1, I.A.2, I.A.3, I.A.4, I.A.5, I.A.6, I.B.1, I.B.2, I.B.3, I.B.4	Отсутствие (неэффективность) механизмов аутентификации и идентификации	A.I.a, A.I.b,A.II.a, A.II.b,A.III.a, A.III.b,A.IV.b B.I.a, B.I.b, B.I.c B.II.a, B.II.b, B.II.c, B.II.d, C.I.a,C.I.b,C.I.c, C.I.d,C.II.a,C.II.b	Нарушение КЦД информации, находящейся внутри сети.	управления и связи;

4. Проектирование системы информационной безопасности

Проектирование информационной системы заключается в определении функциональных требований пользователя системы, определении основных компонентов будущей системы и этапов ее работы, разработке алгоритмов. Для разработки описанных моделей используется унифицированный язык моделирования UML.

4.1. Функциональные требования

Для описания функциональных требований к разрабатываемой системе была построена диаграмма вариантов использования (рис.2).

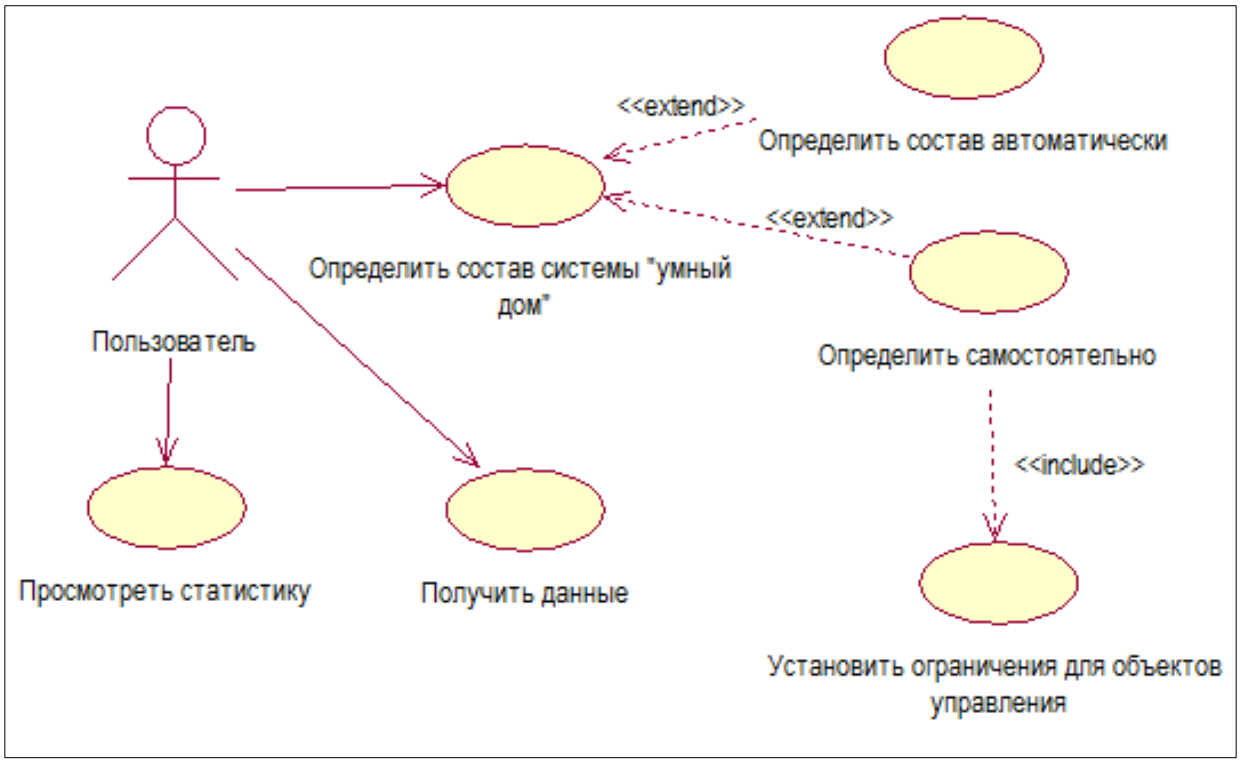

Рисунок 2 – Диаграмма вариантов использования

Диаграмма вариантов использования показывает основные функциональные требования:

1. Определить систему УД:

   a. автоматически, путем определения «идеального» состояния УД;

b. определить самостоятельно, устанавливая при этом ограничения для объектов управления;

2. Получить данные о составе УД;

3. Просмотреть статистику об обнаруженных угрозах;

4.2.Компоненты системы

На основе функциональных требований были выделены основные этапы работы проектируемой системы:

1. Определение состава системы УД и установка ограничений одним из способов:

a. получение «идеального» состояния системы УД,

b. добавление пользователем вручную каждого элемента системы УД и ограничений для них.

2. Получение данных с системы УД.

3. Проверка всех полученных данных (мониторинг) в режиме реального времени.

4. Генерация оповещений о состоянии системы УД.

На основе полученных данных были определены основные компоненты системы ИБ и построена диаграмма компонентов (рисунок 3).

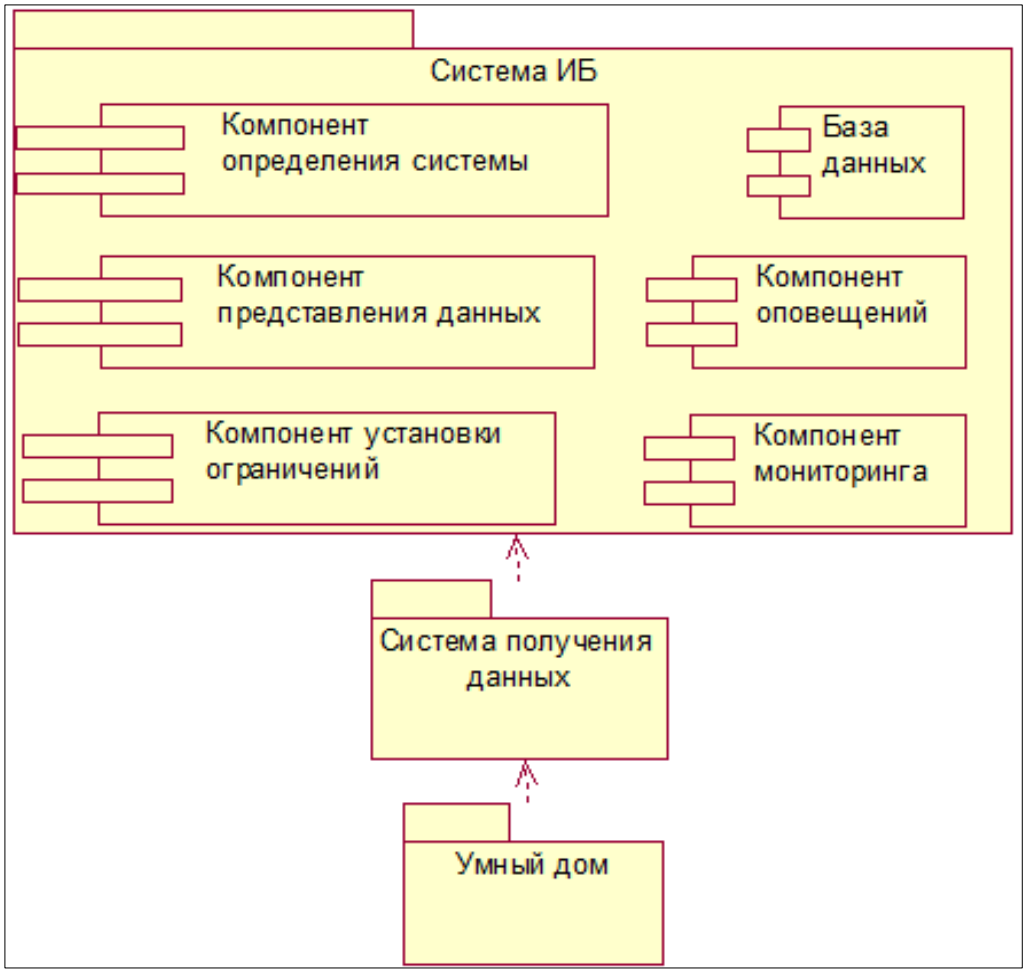

Рисунок 3 – Диаграмма компонентов

Подробнее о выбранных компонентах системы:

– компонент определения системы необходим для определения состава системы УД из полученных данных;

– компонент представления данных служит для отображения пользователю полученных системой ИБ данных;

– компонент установки ограничений необходим для автоматического определения ограничений для показаний элементов системы УД из полученных данных;

– база данных служит для хранения данных о составе системы УД, классификации угроз ИБ и данных, используемых системой ИБ;

– компонент мониторинга осуществляет мониторинг состояния системы УД, путем проверки входящих данных и определения несоответствий;

– компонент оповещений служит для информирования пользователя об обнаруженных угрозах или подозрительных действиях;

4.3. Алгоритмы системы

После определения функциональных требований к системе информационной безопасности, основных этапов работы системы и основных компонентов системы были разработаны алгоритмы и построены диаграммы деятельности для следующих основных действий системы ИБ:

1. Алгоритм определения пользователем состава системы УД и установки ограничений для объектов управления.
2. Алгоритм автоматического определения состава системы УД и ограничений объектов управления.
3. Алгоритм мониторинга состояния системы УД.

4.3.1. Алгоритм определения состава системы УД пользователем

Данный алгоритм выполняется системой ИБ при определении состава системы УД и установка ограничений путем добавления пользователем вручную каждого элемента системы УД и ограничений для них.

Для отображения алгоритма была построена диаграмма деятельности (рисунок 4).

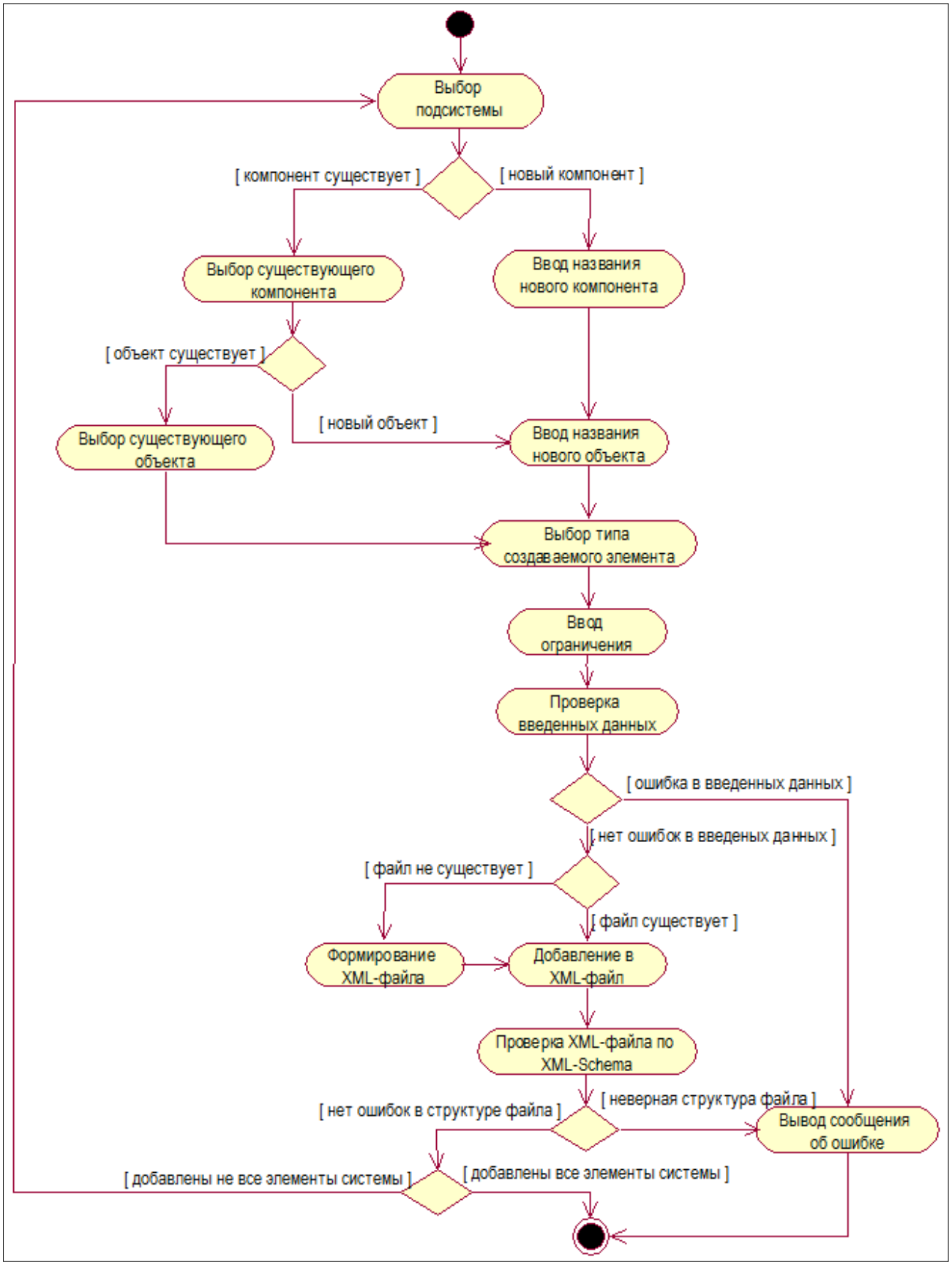

Рисунок 4 – Алгоритм определения пользователем состава системы УД

4.3.2. Алгоритм автоматического определения состава системы УД

Алгоритм выполняется системой ИБ при определении состава системы УД и установка ограничений путем получения «идеального» состояния системы УД. Для отображения алгоритма была построена диаграмма деятельности (рисунок 5).

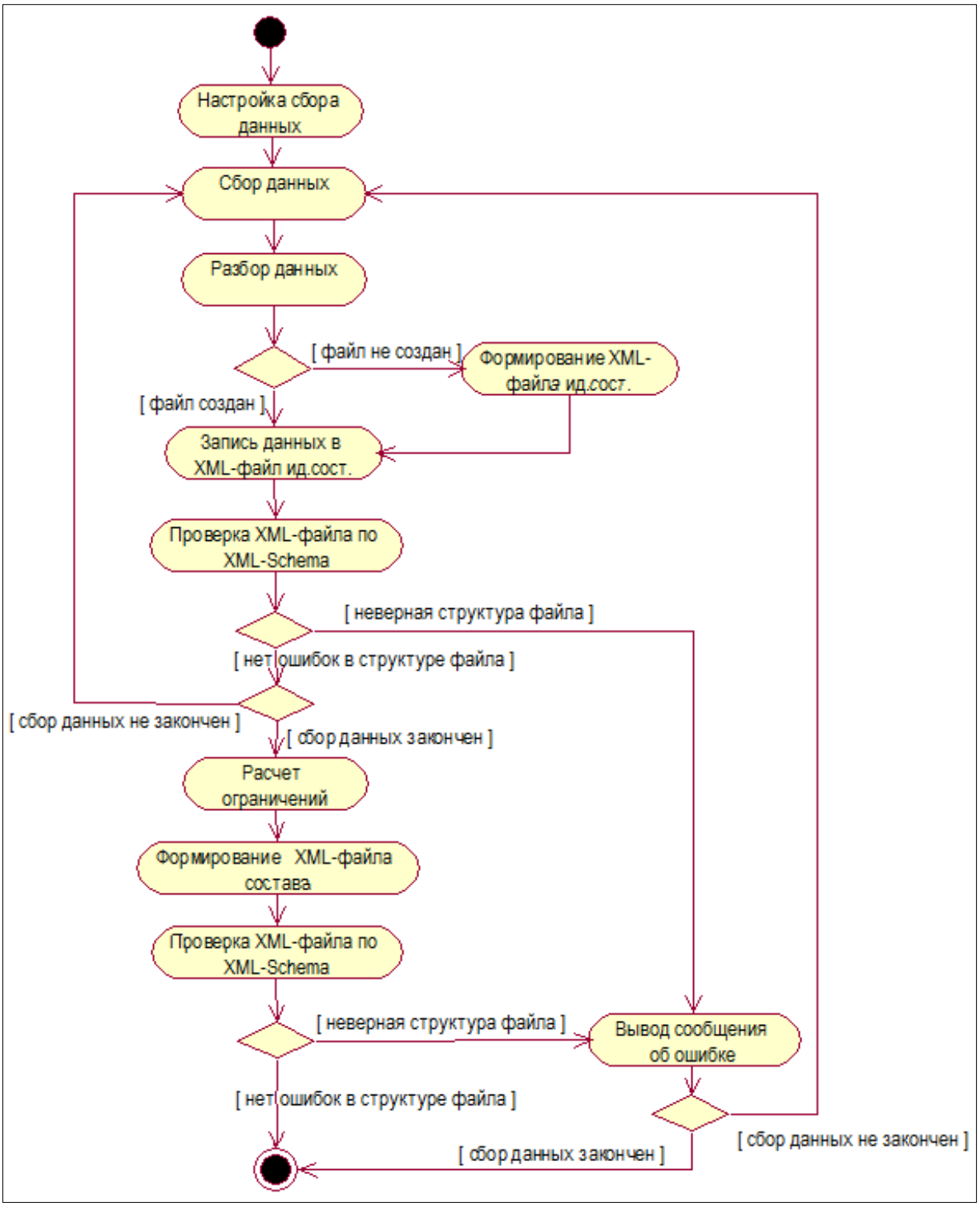

Рисунок 5 – Алгоритм автоматического определения состава системы УД

4.3.3. Алгоритм мониторинга состояния системы УД

Алгоритм заключается в проверке всех полученных данных с системы УД в режиме реального времени. Для отображения алгоритма была построена диаграмма деятельности (рисунок 6).

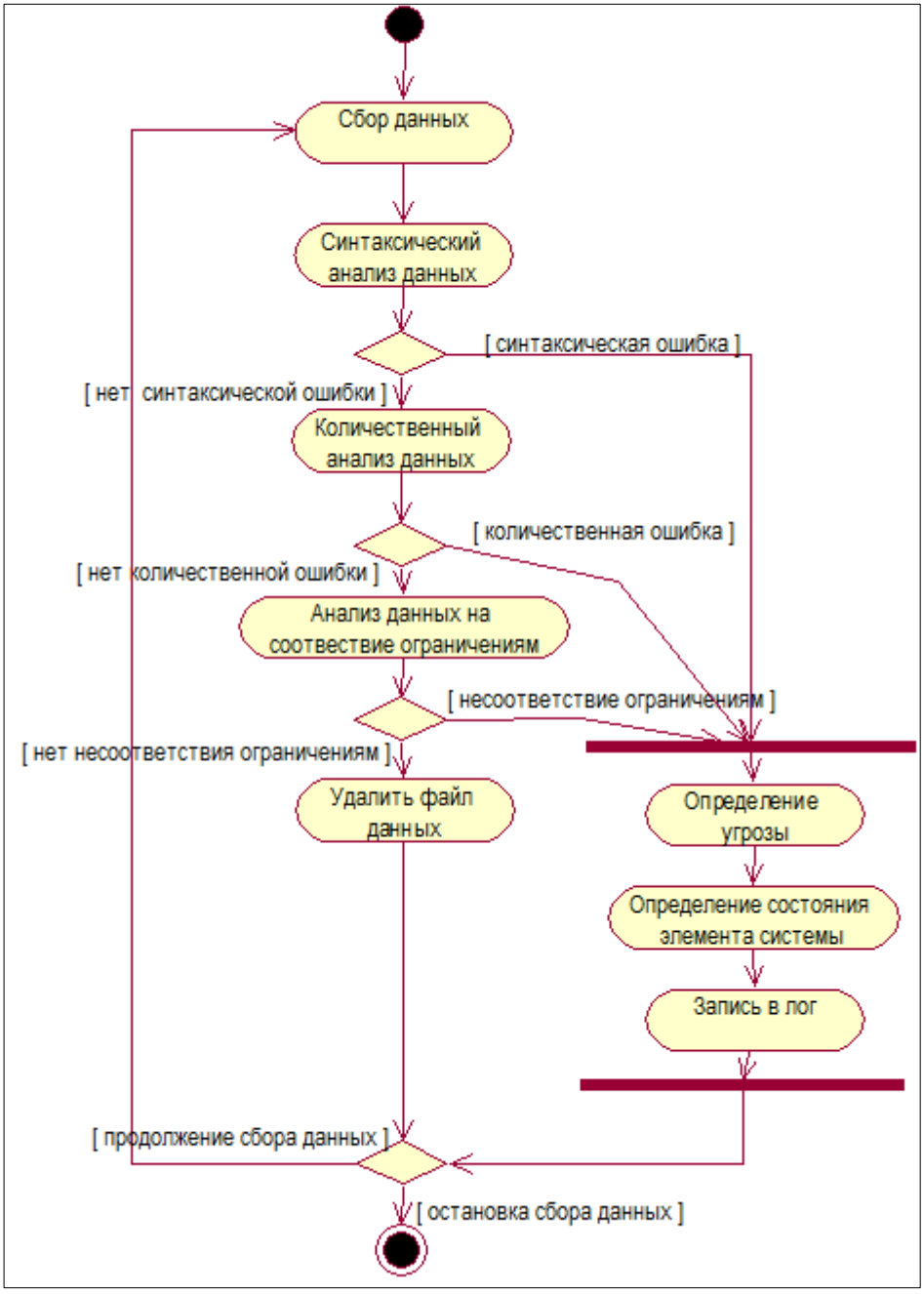

Рисунок 6 – Алгоритм мониторинга состояния системы УД

4.4. Структура описания данных

В проектируемой системе информационной безопасности для описания данных о составе системы «умный дом», ограничениях показаний элементов

системы и для описания угроз информационной безопасности выбран формат XML. Структуры XML-файлов были описаны на языке XML Schema.

4.4.1. Структура данных для описания состава системы «умный дом»

При определении состава системы УД пользователем самостоятельно, путем определения каждого элемента системы, формируется XML-файл описания системы УД. Графическое представление схемы описания состава системы УД показано на рисунке 7, содержание файла приведено в приложении Б.

Используемые обозначения:

1. System – система УД;
2. Subsystem – подсистема;
3. Component – компонент подсистемы;
4. Object – объект управления;
5. Sensor – датчик, Actuator – исполнительный механизм;
6. Name – название, Type – тип элемента;
7. Min – минимальное значение, Max – максимальное значение;
8. Average – ограничение.

Следующие элементы имеют атрибуты:

– System, атрибут Name (название системы УД);

– Subsystem/Component/Object/Sensor/Actuator, атрибут ID (идентификатор);

– Average, атрибут Same (определяет является ли ограничение постоянным);

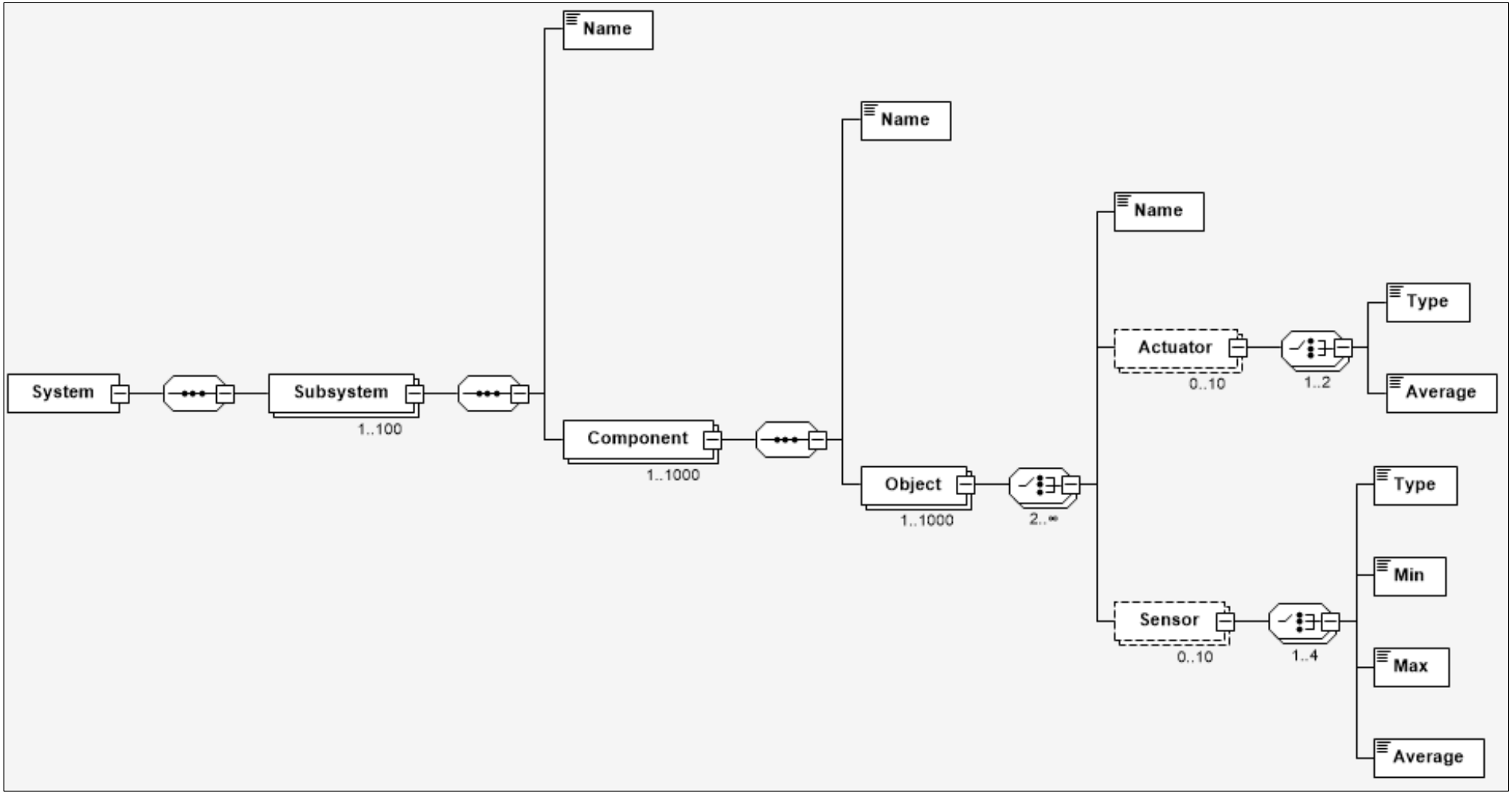

Рисунок 7 – Графическое представление схемы описания состава системы «умный дом»

4.4.2. Структура данных для описания «идеального» состояния системы «умный дом»

При автоматическом способе определения состава системы УД сначала формируется файл с «идеальным» состоянием системы, затем рассчитываются ограничения для элементов системы, и формируется файл с описанием состава системы УД. Графическое представление файла, описывающего структуру «идеального» состояния системы УД представлено на рисунке 8, содержание файла приведено в приложении В.

Используемые обозначения:

1. System – система УД;
2. Subsystem – подсистема;
3. Component – компонент подсистемы;
4. Object – объект управления;
5. Sensor – датчик, Actuator – исполнительный механизм;
6. Name – название, Type – тип элемента;
7. Min – минимальное значение, Max – максимальное значение;
8. Average – ограничение,
9. Values/Value – значения/значение показателя элемента.

Следующие элементы имеют атрибуты:

– System, атрибуты:

Name(название системы УД), DateFrom/DateTo (дата начала/дата окончания сбора данных), EverySec (интервал сбора данных), Round (степень округления значения показателя элемента);

– Subsystem/Component/Object/Sensor/Actuator, атрибут ID – идентификатор;

– Average, атрибут Same – определяет является ли ограничение постоянным;

– Value, атрибут DateTime – дата и время получения данных;

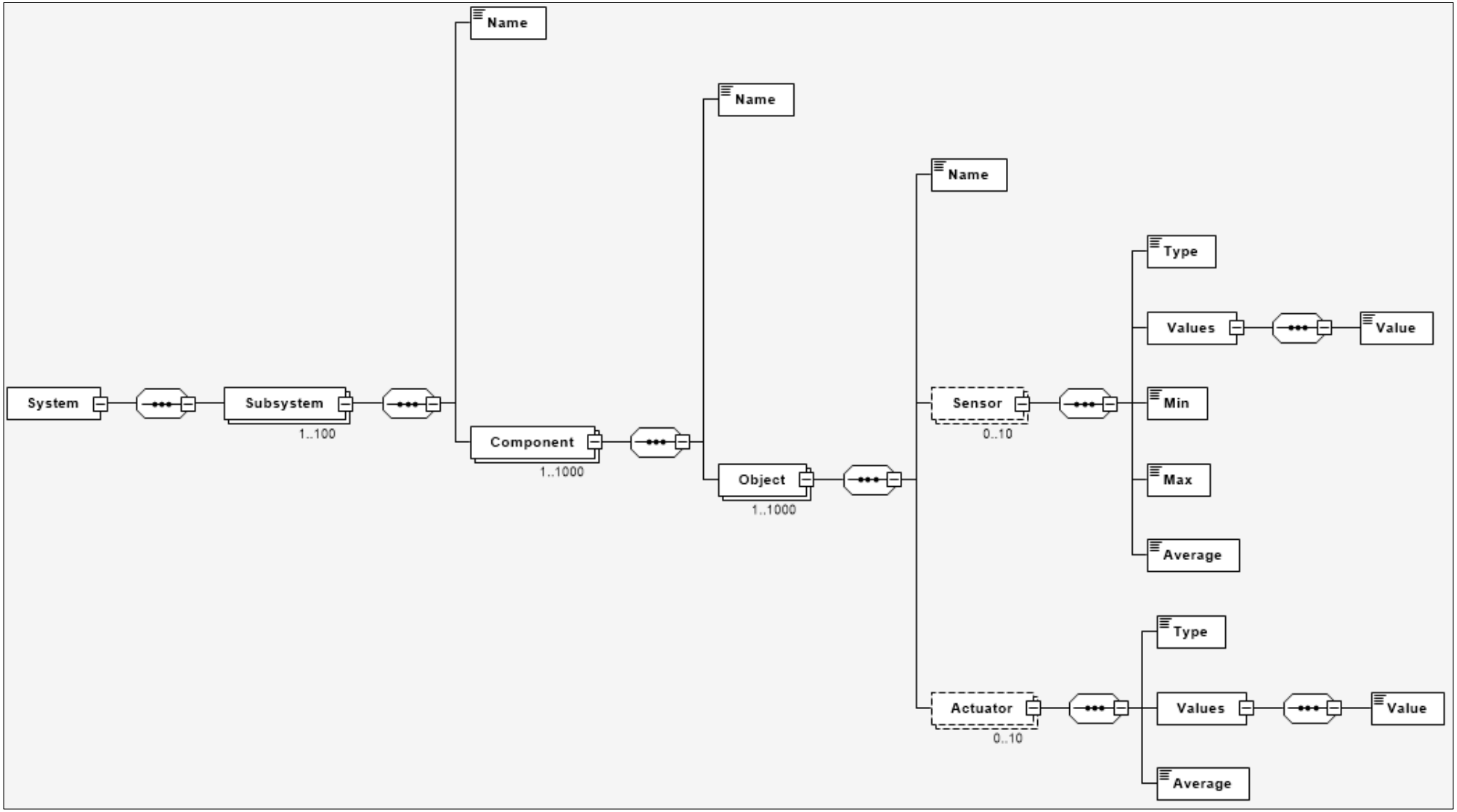

Рисунок 8 – Графическое представление схемы описания «идеального» состояния системы УД

4.4.3. Структура данных для описания угроз системы «умный дом»

Графическое представление схемы описания угроз ИБ системы УД показано на рисунке 9, содержание файла приведено в приложении Г.

Используемые обозначения:

1. Threats – угрозы, Threat – угроза;
2. Object – объект управления;
3. Sensor – датчик;
4. Actuator – исполнительный механизм;
5. Condition – условие;
6. Consequences – возможные последствия, Consequence – возможное последствие;
7. Sources – источники, Source – источник;
8. Causes – возможные причины, Cause – возможная причина.

Следующие элементы имеют атрибуты:

- Object, атрибуты SubsystemID (идентификатор подсистемы) и
- Name (название);
- Condition, атрибуты Type (тип отклонения) и ID (идентификатор);
- Threat, атрибуты Name (название угрозы), ID;
- Consequence/Source/Cause, атрибут ID.

Примеры типов отклонения:

- Тип = 00 (любое отклонение от ограничений);
- Тип = 1 (0% - 20% отклонение от ограничений);
- Тип = 2 (20% - 40% отклонение от ограничений);
- Тип = 3 (40% - 60% отклонение от ограничений);
- Тип = 4 (60% - 80% отклонение от ограничений);
- Тип = 5 (80% - 100% отклонение от ограничений);
- Тип = 100 (100% отклонение от ограничений);

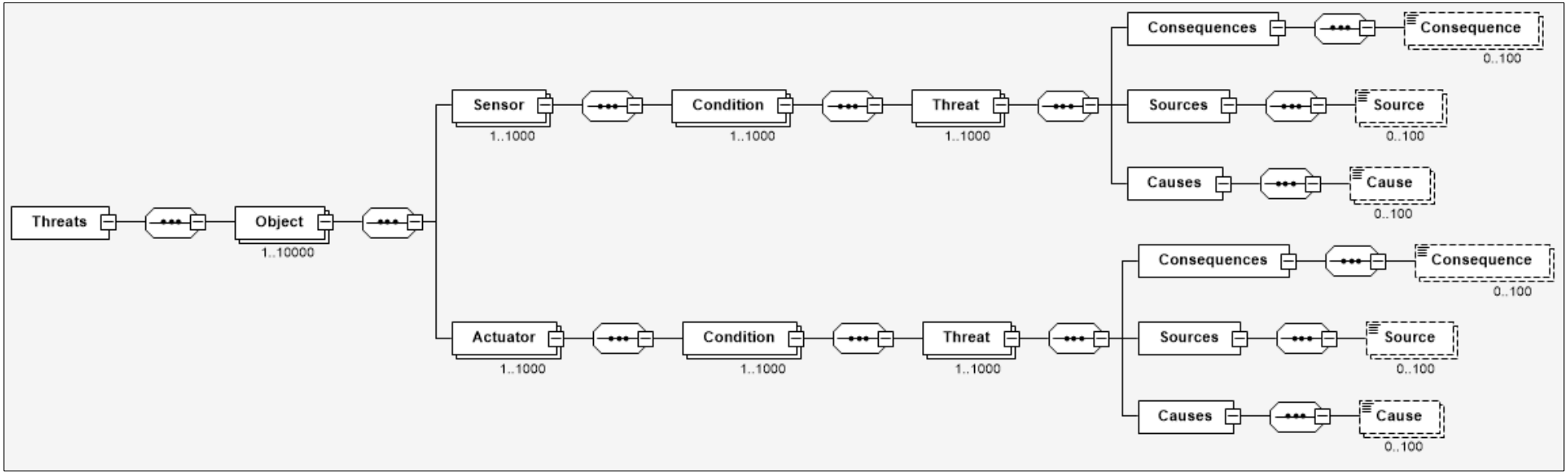

Рисунок 9 – Графическое представление схемы описания угроз системы «умный дом»

5. Прототип системы информационной безопасности

В разрабатываемом прототипе системы информационной безопасности для «умного дома» к описанным в предыдущем разделе компонентам системы добавлен компонент генерирования данных. Данный компонент использует файл-образец, для определения состава системы УД и значения показателей объектов управления. Значения показателей файла-образца используются при генерации случайных значений в генерируемых файлах. Файлы генерируются в отдельном потоке программы. Листинг 1 демонстрирует поток генерирования файлов (каждые две секунды) с данными и запуска их мониторинга.

Листинг 1 – Поток генерирования и мониторинга файлов

```
private static void ThreadStartGenerateFiles()//поток для генерирования файлов данных и
запуска их мониторинга
        {
            while (do_generate)
            {
                mw.GenerateFile();//метод генерирования файлов-данных

                if (do_monitoring)
                {
                    while (generated_files.Count != 0)//пока есть файлы для генерирования
                    {
                        Monitoring();
                    }
                }
                Thread.Sleep(2000);//2sec
            }
                }
```

Пример содержимого файла-образца представлен на рисунке 10.

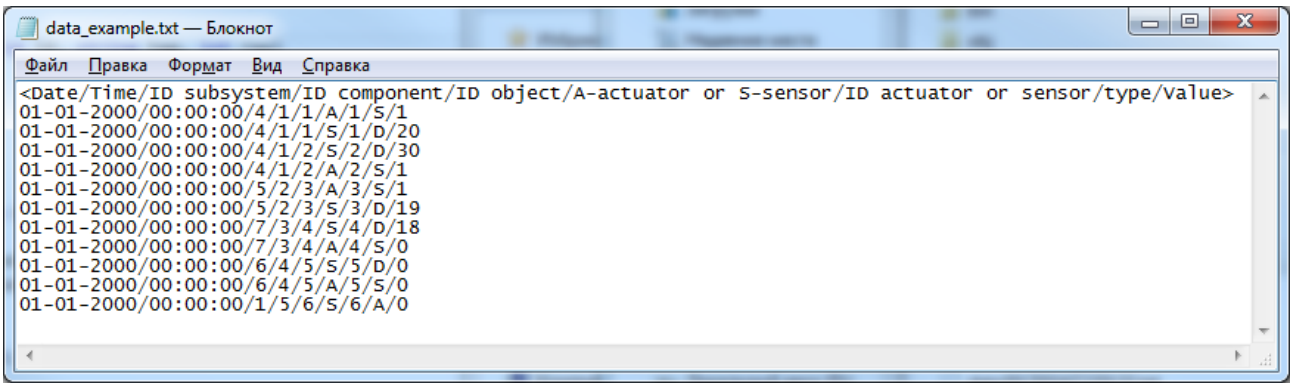

Рисунок 10 – Пример файла образца

При запуске прототипа приложения необходимо определить состав системы УД, после чего станут доступны кнопки для управления мониторингом. Интерфейс основного окна до определения состава системы представлен на рисунке 11.

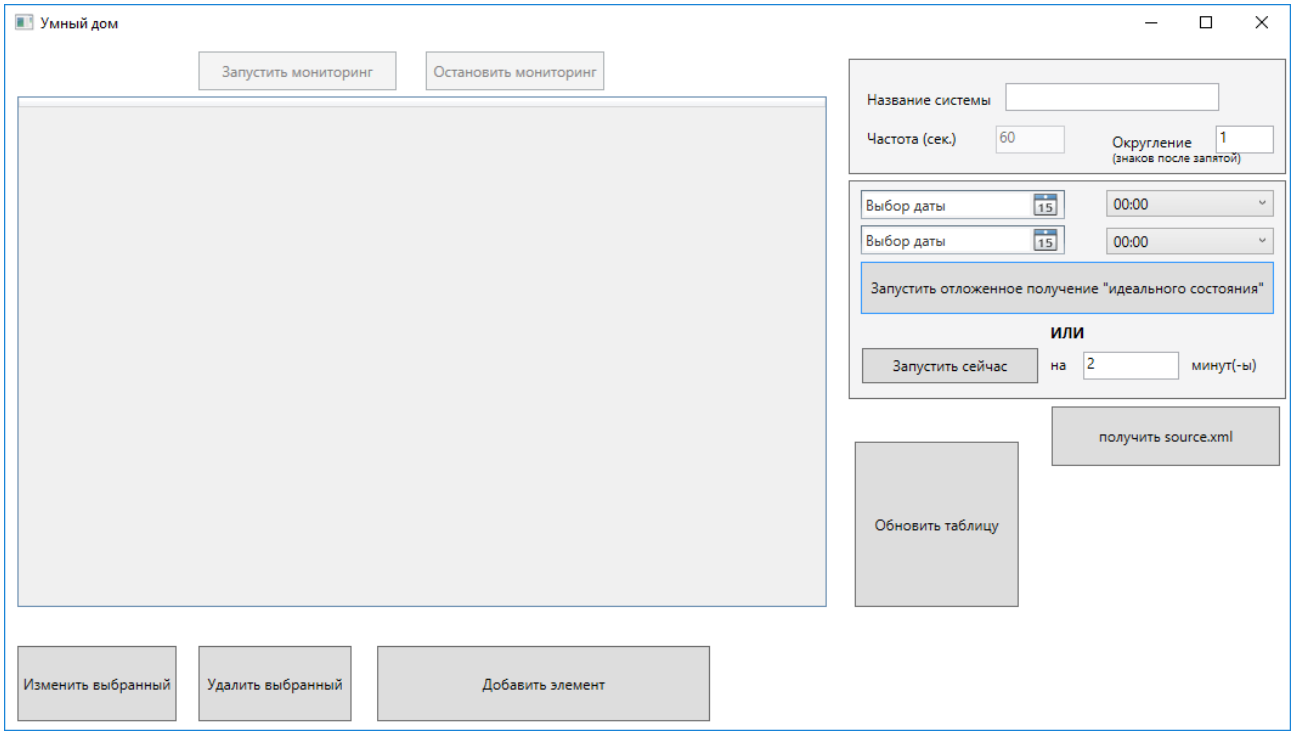

Рисунок 11 – Интерфейс основного окна до определения состава системы

5.1. Формирование «идеального» состояния системы «умный дом»

Для автоматического получения состава системы УД, необходимо в правой части основного окна определить настройки получения «идеального состояния»:

- указать название системы УД,
- определить частоту сбора данных (частота генерирования файлов с данными),
- указать степень округления значений показаний (по умолчанию установлено округление до одного знака после запятой),
- обозначить дату и время начала и окончания отложенного сбора данных или определить время окончания для сбора данных в текущий момент времени.

Панель настройки автоматического сбора данных представлена на рисунке 12.

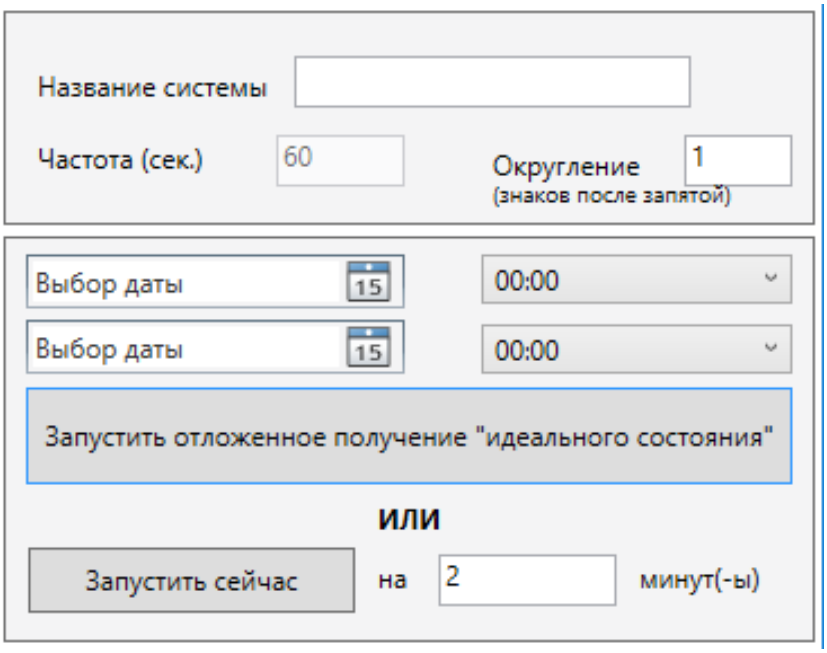

Рисунок 12 – Панель настройки автоматического сбора данных

В приложении Д представлен листинг метода получения «идеального состояния». Листинг 2 демонстрирует фрагмент кода, добавляющего элементы датчик или исполнительный механизм и данные элементов в XML-файл «идеальное состояние».

Листинг 2 – Фрагмент метода добавления элементов

```
//добавление нового элемента с одним значением
if (xdoc.Descendants(elem_tagname).Where(x => x.Attribute("ID").Value == elem_id).Count() ==
0)
{
        XmlElement elem = doc.CreateElement(elem_tagname);
        elem.SetAttribute("ID", elem_id);
        root_for_element.AppendChild(elem);

        XmlElement elem1 = doc.CreateElement("Type");
        string type_ = "";
        if (elem_tagname == "Actuator")//actuator
        {
                type_ = Actuator_types[type];
        }
        else if (elem_tagname == "Sensor")//sensor
        {
                type_ = Sensor_types[type];
        }
        elem1.InnerText = type_;
        elem.AppendChild(elem1);
        XmlElement elem2 = doc.CreateElement("Values");
        elem.AppendChild(elem2);
        element_for_value = elem2;
```

```
XmlElement elem3 = doc.CreateElement("Value");
elem3.SetAttribute("DateTime", date + "T" + time);
elem3.InnerText = value;
elem2.AppendChild(elem3);
}
else //Добавление следующих полученных значений элемента
{
        xpath = "System/Subsystem[@ID='" + subsystem_id + "']/Component[@ID='" +
        component_id + "']/Object[@ID='" + object_id + "']/" + elem_tagname + "[@ID='"
        + elem_id + "']/Values";
        XmlElement elem4 = doc.CreateElement("Value");
        elem4.SetAttribute("DateTime", date + "T" + time);
        elem4.InnerText = value;
        doc.SelectSingleNode(xpath).AppendChild(elem4);
}
```

5.2.Определение состава системы «умный дом»

Для самостоятельного определения пользователем состава системы УД необходимо на основном окне выбрать кнопку «Добавить элемент», после чего откроется окно для добавления/редактирования элемента. Интерфейс окна добавления элемента представлен на рисунке 13.

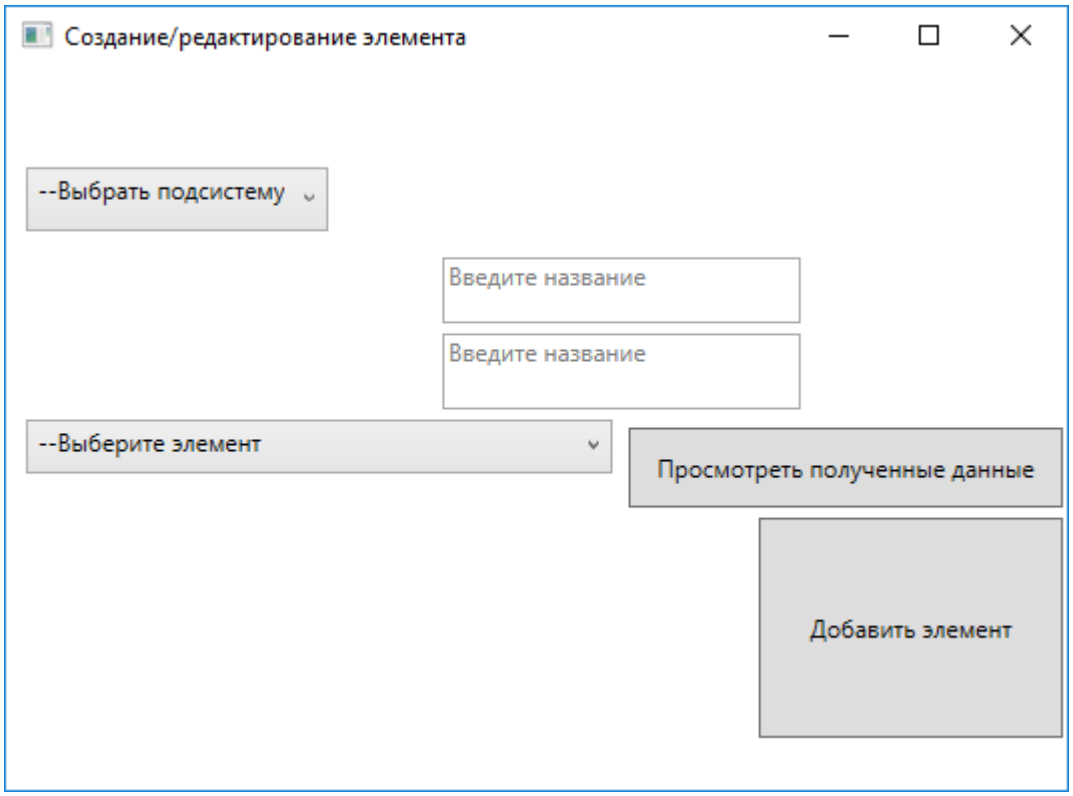

Рисунок 13 – Интерфейс окна добавления элемента

Пользователю необходимо выбрать из выпадающего списка подсистему, ввести названия для компонента подсистемы и объекта управления (или выбрать из существующих, если они были добавлены ранее), выбрать

создаваемый элемент. После выбора элемента, станут доступны выпадающий список для определения типа элемента, текстовые поля для определения ограничений. Пример заполненной формы для создания датчика элемента управления лампочки представлен на рисунке 14. Листинг метода для добавления новых элементов представлен в приложении Е.

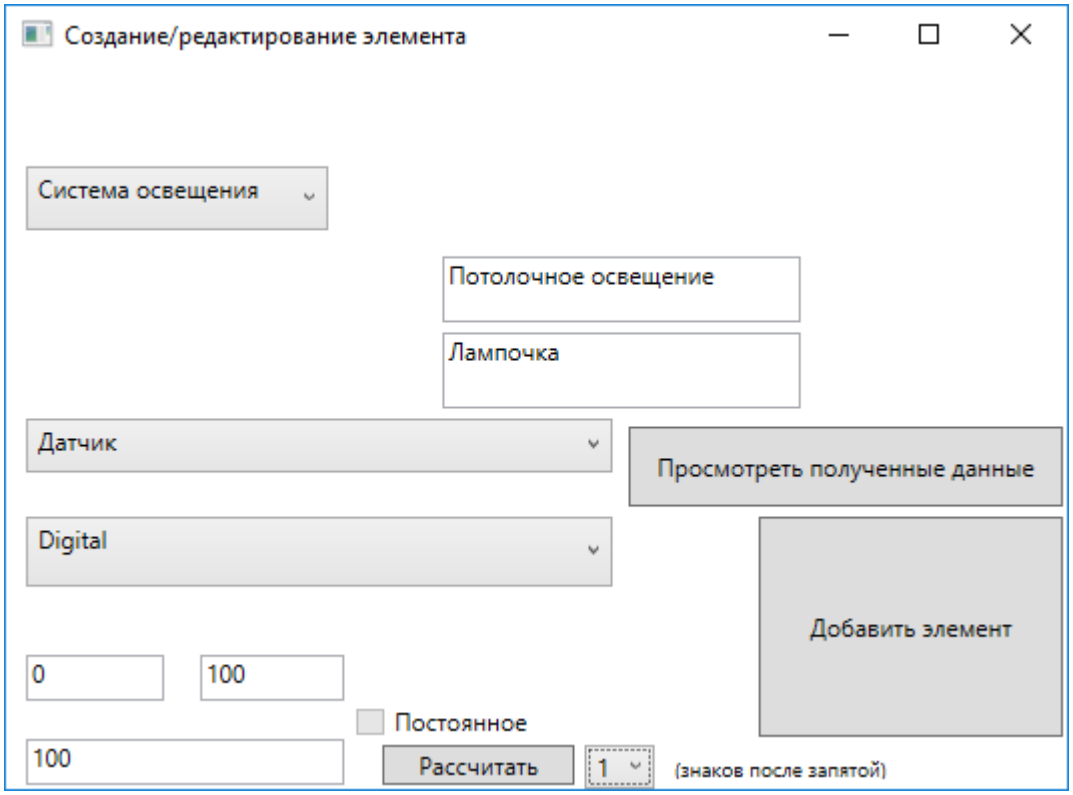

Рисунок 14 – Интерфейс заполненного окна добавления элемента

После определения состава системы в таблице на основном окне приложения появятся данные об элементах. Данные в таблице можно сортировать по убыванию и возрастанию какого-либо столбца. Пример заполненной таблицы с данными представлен на рисунке 15.

SubsystemName	SubsystemID	ComponentName	ComponentID	ObjectName	ObjectID	Average	Min	Max	ID	Type	Name	State
Система освещения	4	Потолочное освещение	1	Лампочка	1	83	--	--	1	Switch	Actuator	green
Система освещения	4	Потолочное освещение	1	Лампочка	1	24,5	11	38	1	Digital	Sensor	green
Система освещения	4	Потолочное освещение	1	Лампочка	2	33,7	5	54	2	Digital	Sensor	green
Система освещения	4	Потолочное освещение	1	Лампочка	2	83	--	--	2	Switch	Actuator	green
Система отопления	5	Отопление жилых комна	2	Батарея	3	16,2	7	28	3	Digital	Sensor	green
Система отопления	5	Отопление жилых комна	2	Батарея	3	83	--	--	3	Switch	Actuator	green
Система кондиционирова	7	Общее кондиционирова	3	Кондиционер	4	18,2	1	30	4	Digital	Sensor	green
Система кондиционирова	7	Общее кондиционирова	3	Кондиционер	4	16	--	--	4	Switch	Actuator	green
Система вентиляции	6	Вентиляция окон	4	Окно	5	0	0	30	5	Digital	Sensor	green
Система вентиляции	6	Вентиляция окон	4	Окно	5	16	--	--	5	Switch	Actuator	green
Система управления и свя	1	Сервер	5	Системный блок	6	1	0	1	6	Analog	Sensor	green

Рисунок 15 – Таблица с данными

Листинг 3 демонстрирует метод для заполнения таблицы данными из XML-файла с составом системы.

Листинг 3 – Метод для заполнения таблицы

```
private void fulltable()//заполнение таблицы данными из source.xml
        {
            //данные из xml
            XDocument doc = XDocument.Load(path);
            var result = doc.Descendants("Average").Select(x => new
            {
                SubsystemName = x.Parent.Parent.Parent.Parent.Element("Name").Value,
                SubsystemID = x.Parent.Parent.Parent.Parent.Attribute("ID").Value,
                ComponentName = x.Parent.Parent.Parent.Element("Name").Value,
                ComponentID = x.Parent.Parent.Parent.Attribute("ID").Value,
                ObjectName = x.Parent.Parent.Element("Name").Value,
                ObjectID = x.Parent.Parent.Attribute("ID").Value,
                Average = x.Value,
                Min = x.Parent.Element("Min") != null ? x.Parent.Element("Min").Value : "--
",
                Max = x.Parent.Element("Max") != null ? x.Parent.Element("Max").Value : "--
",
                ID = x.Parent.Attribute("ID").Value,
                Type = x.Parent.Element("Type").Value,
                Name = x.Parent.Name.ToString(),
                State = "green"
            });
            dgrid.ItemsSource = result;//заполняем таблицу

            elements_count = dgrid.Items.Count;//записываем количество элементов системы УД
            FullLists();//заполняем списки с имеющимися ID подсистем,компонетов,объектов,
элементов
                }
```

Такие данные элементов как название и ограничение можно изменять, для этого необходимо выполнить двойное нажатие на необходимой ячейке или выбрать строку в таблице и нажать кнопку «Изменить выбранный». В первом варианте откроется окно для редактирования конкретного значения данных элемента (рисунок 16), во втором откроется заполненное данными элемента окно добавления/редактирования элемента, описанное ранее.

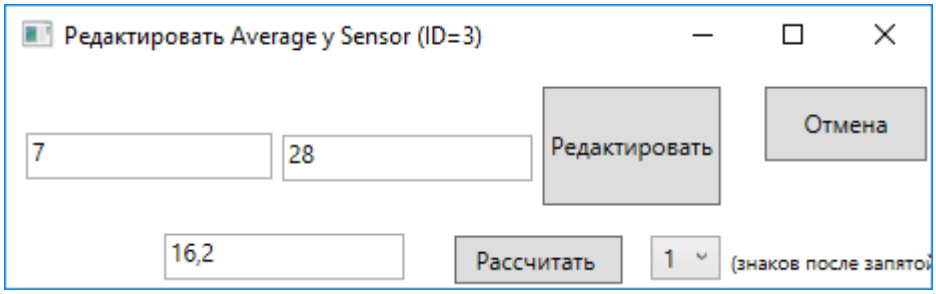

Рисунок 16 – Пример редактирования ячейки таблицы

5.3.Мониторинг состояния системы «умный дом»

Для запуска мониторинга состояния системы УД на главном окне необходимо выбрать кнопку «Запустить мониторинг». При необходимости мониторинг состояния УД можно оставить, выбрав кнопку «Остановить мониторинг». При обнаружении угроз и несоответствии показаний датчика или исполнительного механизма объектов управления, в таблице с данными изменяется значение элемента в столбце «State» (статус) и строка элемента подсвечивается цветом. Пример внешнего вида таблицы с данными, в которых обнаружены угрозы, представлен на рисунке 17.

SubsystemName	SubsystemID	ComponentName	ComponentID	ObjectName	ObjectID	Average	Min	Max	ID	Type	Name	State
Система освещения	4	Потолочное освещение	1	Лампочка	1	83	--	--	1	Switch	Actuator	green
Система освещения	4	Потолочное освещение	1	Лампочка	1	24,5	11	38	1	Digital	Sensor	red
Система освещения	4	Потолочное освещение	1	Лампочка	2	33,7	5	54	2	Digital	Sensor	red
Система освещения	4	Потолочное освещение	1	Лампочка	2	83	--	--	2	Switch	Actuator	green
Система отопления	5	Отопление жилых комна	2	Батарея	3	16,2	7	28	3	Digital	Sensor	red
Система отопления	5	Отопление жилых комна	2	Батарея	3	83	--	--	3	Switch	Actuator	green
Система кондиционирова	7	Общее кондиционирова	3	Кондиционер	4	18,2	1	30	4	Digital	Sensor	red
Система кондиционирова	7	Общее кондиционирова	3	Кондиционер	4	16	--	--	4	Switch	Actuator	green
Система вентиляции	6	Вентиляция окон	4	Окно	5	0	0	30	5	Digital	Sensor	red
Система вентиляции	6	Вентиляция окон	4	Окно	5	16	--	--	5	Switch	Actuator	green
Система управления и свя	1	Сервер	5	Системный блок	6	1	0	1	6	Analog	Sensor	red

Рисунок 17 – Пример таблицы с обнаруженными угрозами

Листинг метода для мониторинга данных представлен в приложении Ж. Метод для определения угрозы представлен в листинге 4. В методе проверки данных при обнаружении ошибок определяется их вид, список описанных ошибок показан в таблице 2.

Листинг 4 – Метод определения угрозы

```
private static int GetThreatID(string tagname, string elemid, int dev)//определение ID
угрозы
        {
            int threat_id = -1;
            XDocument xdoc = XDocument.Load(path);
            string name="";

            switch (tagname)
            {
                case ("S"):
                    tagname = "Sensor";
                    break;
                case ("A"):
                    tagname = "Actuator";
                    break;
            }
            //получаем название объекта, в кот.обнаружена угроза
```

```
            var v = xdoc.Descendants("Object").Where(x =>
x.Element(tagname).Attribute("ID").Value == elemid).Elements("Name");
            foreach (XElement e in v)
            { name = e.Value; }
            XmlDocument doc = new XmlDocument();
            doc.Load("..\\..\\threat.xml");
            if (doc.SelectSingleNode("//Object[@Name='" + name +
"']//'"+tagname+"'//Condition[@Type='" + GetConditionType(dev) + "']") != null)//если в
threat.xml есть объект с заданным условием
            {
                threat_id = Convert.ToInt32(doc.SelectSingleNode("//'" + tagname +
"'//Condition[@Type='" + GetConditionType(dev) + "']//Threat/@ID").Value);
            }
            if (doc.SelectSingleNode("//Object[@Name='" + name + "']//'" + tagname +
"'//Condition[@Type='" + "00" + "']") != null)//угроза для любого отклонения
            {
                threat_id = Convert.ToInt32(doc.SelectSingleNode("//'" + tagname +
"'//Condition[@Type='" + "00" + "']//Threat/@ID").Value);
            }
            return threat_id;
                }
```

Таблица 2 – Список ошибок

№ ошибки	Вид ошибки
1	Ошибка в формате даты
2	Ошибка в формате времени
3	Ошибка в формате ID подсистемы
4	Ошибка в формате ID компонента
5	Ошибка в формате ID объекта
6	Ошибка в формате вида элемента
7	Ошибка в формате ID элемента
8	Ошибка в формате типа элемента
9	Ошибка в формате значения элемента
33	Не найдена подсистема с заданным ID
44	Не найден компонент с заданным ID
55	Не найден объект с заданным ID
771	Не найден датчик с заданным ID
772	Не найден исполнительный механизм с заданным ID
8810	У датчика с заданным ID не указан тип
881	Неверный тип датчика
8820	У исполнительного механизма с заданным ID не указан тип
882	Неверный тип исполнительного механизма
99	Данные сенсора не соответствуют ограничениям
100	Неверное количество элементов данных
103	Во входном массиве отсутствуют данные по подсистеме
104	Во входном массиве отсутствуют данные по компоненту
105	Во входном массиве отсутствуют данные по объекту
1071	Во входном массиве отсутствуют данные по датчику
1072	Во входном массиве отсутствуют данные по исполнительному механизму

Двойное нажатие на статус элемента открывает окно с подробными сведениями о возможной угрозе. Пример сведений об угрозе, обнаруженной в датчике вскрытия корпуса сервера системы управления, представлен на рисунке 18.

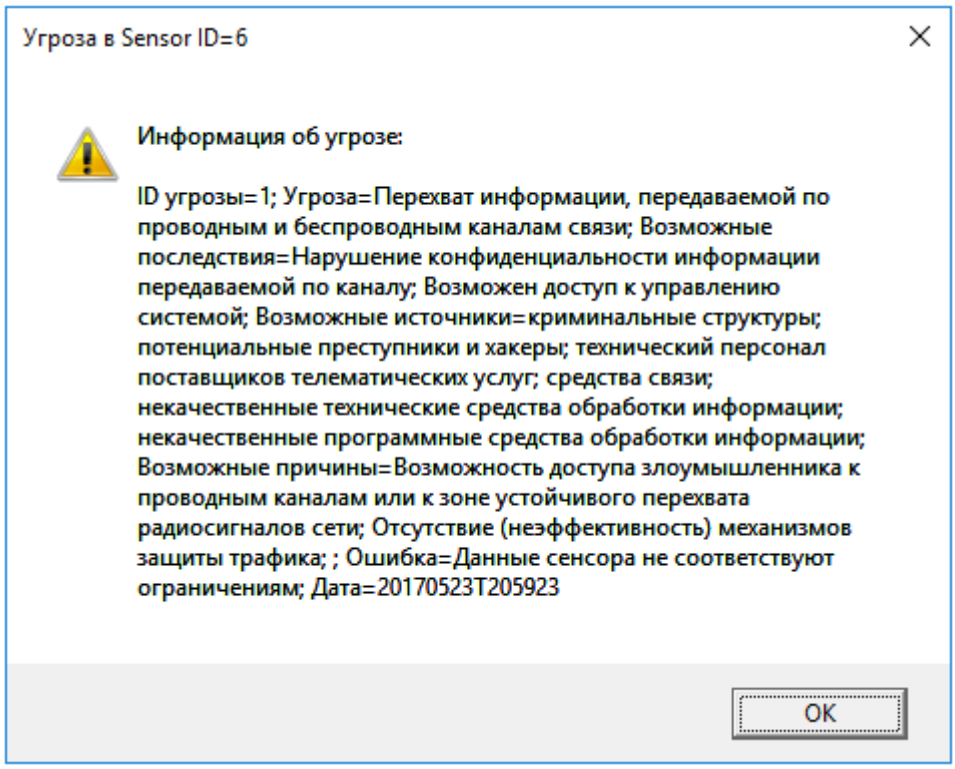

Рисунок 18 – Окно сведений о возможных угрозах

При отсутствии данных об угрозе система ИБ представляет пользователю данные об ошибке и дату ее обнаружения. Пример сведений о неизвестной угрозе, обнаруженной в датчике открытия окна, представлен на рисунке 19.

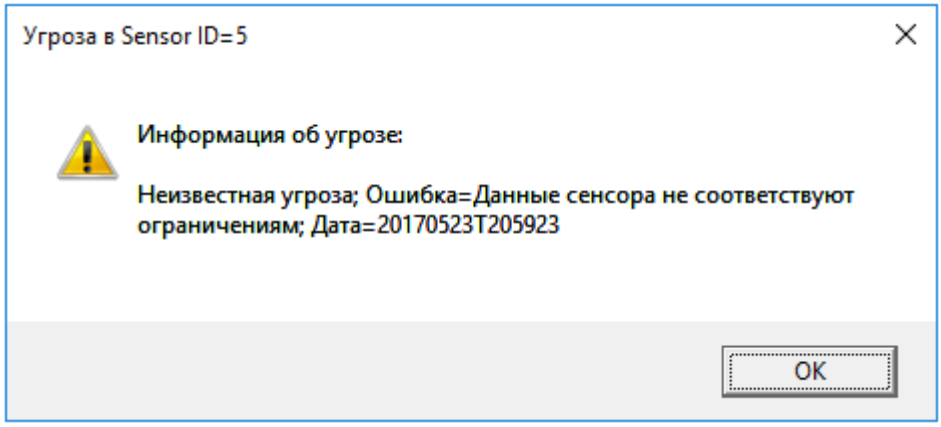

Рисунок 19 – Окно сведений о неизвестной угрозе

6. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

При работе над проектной и научно-исследовательской деятельностью немаловажную роль играет определение экономического обоснования. Данный раздел является обязательной частью магистерской диссертации, в котором проводятся:

- определение потенциальных потребителей,
- оценка конкурентоспособности разработки,
- выявление слабых сторон разработки и определение вариантов минимизации влияния угроз
- определение перечня предполагаемых работ, определение трудоемкости работ и построение графика работ,
- планирование бюджета,
- расчет затрат на разработку,
- определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования.

Проведенные работы позволят выделить преимущества и недостатки разработки, внедрения и эксплуатации разрабатываемого программного продукта, оценить его коммерческий потенциал, определить возможные варианты повышения его эффективности и помогут спланировать весь процесс работы над разработкой.

Магистерская диссертация представляет собой разработку информационной системы мониторинга и оценки угроз информационной безопасности технологии «умный дом».

6.1.Оценка коммерческого потенциала и перспективности

6.1.1. Потенциальные потребители результатов исследования

«Умный дом» (УД) - система устройств, выполняющих необходимые действия и решающие определенные задачи без участия человека. Существует огромное количество различных по составу и назначению систем УД. Среди них можно выделить системы, использующиеся на различных предприятиях, и те, которые используются в жилых домах. Также можно выделить: УД, производимые специализирующимися в данной сфере компаниями (готовые «под ключ» или настраиваемые пользователем), и самостоятельно подключенные пользователем в свою систему «умный дом» устройства.

Из-за отсутствия единой технологии построения систем существует проблемы с обеспечением информационной безопасности. В некоторых системах имеются слабые средства защиты или даже отсутствуют. Особенно велика вероятность недостаточной информационной безопасности в системах, используемых в жилых домах: во многих случаях системы для жилых домов выбираются с относительно невысокой стоимостью, а в некоторых случаях - собираются и настраиваются самостоятельно. На рисунке 20 показана ориентировочная сегментация рынка систем «умный дом» по следующим критериям: тип потребителя и вид системы УД. Сегментирование проведено по виду системы защиты информационной безопасности (ИБ), используемой в УД:

- встроенная система защиты – система ИБ, разрабатываемая производителем используемой системы УД и включенная в ее комплектацию.
- дополнительная система защиты – система ИБ, разрабатываемая различными компаниями для использования в УД конкретных производителей или (реже) в любых УД.
- слабая система защиты (встроенная или дополнительная) или ее отсутствие.

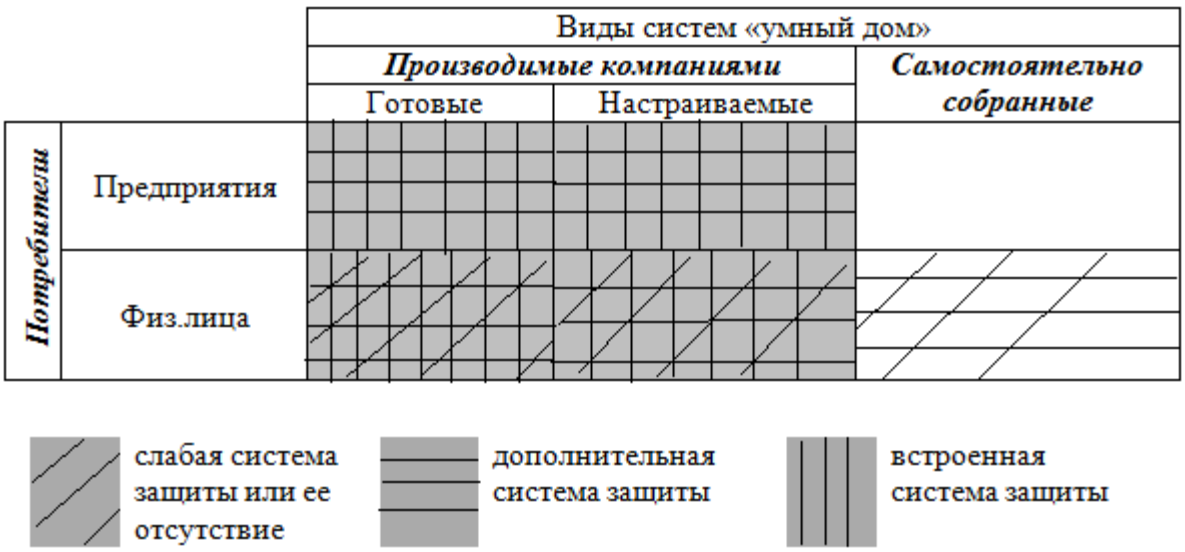

Рисунок 20 – Сегментация рынка системы УД

Проведенная оценка рынка показывает:

- предприятия используют только системы УД, производимые специализирующимися компаниями, с достаточным уровнем защиты;
- физ. лица пользуются системами УД с низким уровнем защиты, в независимости от вида системы.

Разрабатываемый продукт предназначен для личного использования физическими лицами в системах «умный дом» любого вида.

6.1.2. Анализ конкурентных технических решений

Определение существующих на рынке конкурентных решений и анализ их слабых и сильных сторон позволяют определить эффективность научной разработки и ее конкурентоспособность. Результаты анализа позволяют определить возможные необходимые изменения разработки для повышения конкурентоспособности.

Основными конкурентами разрабатываемого продукта являются следующие программные продукты для защиты «умного дома»:

1. Dojo – устройство, разработанное в Израиле небольшой компанией Dojo-Labs. Первая информация о продукте появилась во второй

половине 2015 года. Старт продаж планировался на начало 2016 года. В настоящий момент на официальной сайте производителя есть только возможность предварительного заказа.

2. CUJO – устройство, разработанное группой калифорнийских исследователей. Первая информация о разработке появилась во второй половине 2015 года. Создатели проекта собирали средства для его реализации на краудфандинговой площадке. Старт продаж планировался на март 2016 года. В настоящий момент официальный сайт производителя не функционирует, не удалось найти достоверной информации о возможности приобретения продукта.
3. Bitdefender Box – продукт, разработанный крупной румынской компанией Bitdefender, выпускающей различные антивирусные продукты. Продукт представлен в 3 вариациях на официальном сайте компании. Но возможность приобретения и использования продукта доступна только жителям США, Японии и Франции. Продукт не сертифицирован для остальных стран.
4. Cisco ASA 5500-X - with FirePOWER Services – серия устройств с интегрированными угрозоориентированными межсетевыми экранами. Является разработкой крупной американской компании Cisco, разрабатывающей сетевое оборудование в основном для крупных организаций и телекоммуникационных предприятий.

Для сравнения конкурентных решений была построена оценочная карта.

Таблица 3 – Оценочная карта для сравнения конкурентных технических решений (разработок)

Критерии оценки	**Вес критерия**	**Баллы**					**Конкурентоспособность**				
		$Б_ф$	$Б_{к1}$	$Б_{к2}$	$Б_{к3}$	$Б_{к4}$	$К_ф$	$К_{к1}$	$К_{к2}$	$К_{к3}$	$К_{к4}$
1	2	3	4	5	6	7	8	9	10	11	12
Технические критерии оценки ресурсоэффективности											
1. Удобство в эксплуатации (соответствует требованиям потребителей)	0,15	4	5	5	5	3	0,6	0,75	0,75	0,75	0,45
2. Качество дизайна	0,02	3	5	5	3	3	0,06	0,1	0,1	0,06	0,06
3. Возможность настройки работы	0,15	5	2	2	2	5	0,75	0,3	0,3	0,3	0,75
4. Функциональная мощность (предоставляемые возможности)	0,15	4	2	2	3	5	0,6	0,3	0,3	0,45	0,75
5. Простота эксплуатации	0,1	4	5	5	5	3	0,4	0,5	0,5	0,5	0,3
6. Качество интеллектуального интерфейса	0,03	5	5	5	5	4	0,15	0,15	0,15	0,15	0,12
7. Дополнительный сбор данных	0,05	5	3	3	5	5	0,25	0,15	0,15	0,25	0,25
Экономические критерии оценки эффективности											
1. Конкурентоспособность продукта	0,1	5	3	3	4	5	0,5	0,3	0,3	0,4	0,5
2. Цена	0,15	4	5	5	5	2	0,6	0,75	0,75	0,75	0,3
3. Срок выхода на рынок	0,1	4	3	1	5	5	0,4	0,3	0,1	0,5	0,5
Итого	**1**						**4,31**	**3,6**	**3,4**	**4,11**	**3,98**

Слабые стороны конкурентов:

- конкурент 4 уступает в удобстве эксплуатации, так как продукт в основном рассчитан для использования на предприятиях, где непосредственно взаимодействующие с продуктом сотрудники обычно сначала проходят инструктаж или обучение работе с данным продуктом;
- у конкурентов 1-3 существует возможность лишь минимальной настройки работы продукта;
- конкуренты 1-3 уступают в функциональной мощности, их продукты могут работать только с приборами, использующими интернет-соединение;
- конкурент 1-2 используют дополнительный сбор и отправку данных о работе своих продуктов;
- конкуренты 1-3 имеют меньшую конкурентоспособность из-за описанных выше слабостей.

После проведенного анализа конкурентных технических решений можно увидеть, что создаваемый продукт является конкурентоспособным. Основными преимуществами разработки являются:

- функциональная мощность и возможность настройки работы продукта под индивидуальные требования потребителя;
- сохранение удобства и достаточной простоты эксплуатации разработки, не требующей специальных навыков и знаний;
- относительно невысокая цена разрабатываемого продукта;
- отсутствие сбора дополнительных данных о работе продукта.

Данные критерии являются важными свойствами продукта для потенциальных потребителей.

6.1.3. Технология QuaD

Технология QUality ADvisor позволяет оценить качество новой разработки и ее перспективность на рынке, а также принять решение о целесообразности

вложения денежных средств в разработку. Для этого стоится оценочная карта, описывающая показатели оценки качества разработки и показатели оценки коммерческого потенциала разработки и рассчитанные средневзвешенное значение показателей. Средневзвешенное значение показателя качества и перспективности определяет качество и перспективность научной разработки в зависимости от диапазона значений, в котором оно находится:

- от 100 до 80 – разработка считается перспективной.
- от 79 до 60 – перспективность выше среднего.
- от 69 до 40 – перспективность средняя.
- от 39 до 20 – перспективность ниже среднего.
- от 19 и ниже – перспективность крайне низкая.

Таблица 4 – Оценочная карта для сравнения конкурентных технических решений (разработок)

Критерии оценки	**Вес критерия**	**Баллы**	**Макс. балл**	**Относительное**	**Средневзвешенное значение**
1	2	3	4	5	6
Показатели оценки качества разработки					
1. Удобство в эксплуатации (соответствует требованиям потребителей)	0,2	85	100	0,85	0,17
2. Качество дизайна	0,02	50	100	0,5	0,01
3. Возможность настройки работы	0,2	90	100	0,9	0,18
4. Функциональная мощность (предоставляемые возможности)	0,2	85	100	0,85	0,17
5. Простота эксплуатации	0,1	70	100	0,7	0,07
6. Качество интеллектуального интерфейса	0,08	70	100	0,7	0,056
Показатели оценки коммерческого потенциала разработки					
1. Конкурентоспособность продукта	0,1	70	100	0,7	0,07
2. Цена	0,1	64	100	0,64	0,064
Итого	**1**				**0,79**

Полученные результаты в оценочной карте показывают, что качество и перспективность заработки научной разработки выше среднего. Полученное средневзвешенное значение показателя равно 79, что означает перспективность разработки выше среднего. Возможно, следует рассмотреть возможные варианты повысить показатель до перспективного.

6.1.4. SWOT-анализ

SWOT-анализ дает четкое представление о факторах внешней и внутренней среды и указывает, в каких направлениях нужно действовать, используя сильные стороны, чтобы максимизировать возможности и свести к минимуму угрозы и слабые стороны. С помощью этого метода можно обозначить основные проблемы проекта, определить пути решения и перспективу развития.

Результатом анализа является разработка маркетинговой стратегии или гипотезы для дальнейшей проверки, данные представлены в таблице 5.

Таблица 5 – SWOT-анализ

	Сильные стороны научной разработки: С1. Функциональная мощность; С2. Возможность настройки под индивидуальные требования потребителя; С3. Относительно невысокая цена. С4. Отсутствие дополнительного сбора данных.	**Слабые стороны научной разработки:** Сл1. Невысокое качество дизайна; Сл2. Недостаточная простота эксплуатации.
Возможности: В1. Рост количества пользователей систем «умный дом» для жилых домов. В2. Повышение осведомленности пользователей систем «умный дом» о необходимости защиты информационной безопасности их систем. В3. Ограничение в законодательстве РФ на использование иностранного ПО.	В2С1С2 Улучшение функционала и гибкости продукта для удовлетворения выросших потребностей потребителей. В3С3 Возможность повышения цены, из-за отсутствия зарубежных конкурентов на рынке.	Сл1В1В2 Возможно увеличение требований к дизайну продукта, следует обратиться к дизайнерам для его улучшения. Сл1В1В2 Увеличение количества пользователей может привести к увеличению пользователей, для которых критична простота эксплуатации.
Угрозы: У1. Отсутствие спроса на данную разработку. У2. Ужесточение требований в законодательстве РФ относительно программных продуктов и информационных технологий. У3. Развитие конкурентных разработок.	У1У3С4 Снижение цены на продукт может повысить спрос. У1У3С1 Улучшение функциональной мощности может повысить спрос. У2С1 Изучить требования законодательства и возможности перепроектирования соответствующего функционала.	У1У3Сл1 Приглашение дизайнера в команду разработчиков проекта. У1У3Сл2 Упрощение эксплуатации поможет повысить спрос на продукт.

Таким образом, в результате SWOT-анализа были рассмотрены сильные и слабые стороны разработки, выявлены возможные перспективы ее создания и рассмотрены варианты минимизации влияния угроз.

Основные слабые стороны научной разработки низкое качество дизайна и сложность эксплуатации. В первом случае при любых возможностях и угрозах следует обратиться к дизайнеру. Во втором – постараться упростить эксплуатацию продукта. Кроме изменения спроса из-за различных одновременно источником возможностей и угроз является законодательство: ввод ограничения для иностранного ПО может значительно повысить спрос на разработку, понизив конкуренцию, ужесточение требований для разрабатываемых ПО может потребовать переработки или доработки части функционала продукта.

6.2.Планирование научно-исследовательских работ

6.2.1. Структура работ в рамках научного исследования

В данном разделе определяется необходимый перечень этапов и работ и осуществляется распределение исполнителей.

Рабочая группа состоит из руководителя ВКР (руководитель) и студента (инженер). Примерный порядок этапов и работ, распределение исполнителей по данным видам работ приведен в таблице 6.

Работы разделены на три основных этапа: подготовительный, основной и заключительный. На подготовительном этапе определяется направление, изучается состояние науки и разработок данной тематики и утверждается тема научного исследования. Затем на основном этапе стоится классификация, проектируется и разрабатывается продукт. На заключительном этапе анализируются результаты работы и подготавливаются отчетные материалы. Полученные в разделе данные необходимы для дальнейшего планирования работ.

Таблица 6 – Перечень этапов, работ и распределение исполнителей

Основные этапы	**№ раб**	**Содержание работ**	**Должность исполнителя**
Подготовительный	1	Выбор направления исследования	Руководитель, инженер
	2	Анализ предметной области	Инженер
	3	Аналитический обзор литературы	Инженер
	4	Утверждение темы исследования	Руководитель, инженер
Основной	1	Построение классификации оценивания угроз инф. безопасности	Инженер
	2	Разработка структуры описания данных	Инженер
	3	Проектирование программного продукта	Инженер
	4	Разработка алгоритмов работы программного продукта	Инженер
	5	Разработка прототипа программного продукта	Инженер
Заключительный	1	Анализ полученных результатов	Руководитель, инженер
	2	Составление пояснительной записки	Инженер
	3	Подготовка и оформление презентации дипломного проекта	Инженер

6.3.Определение трудоемкости выполнения работ

Основную часть стоимости разработки составляют трудовые затраты, поэтому важно определить трудоемкость каждого из участников научно-исследовательской работы. Большие трудовые затраты связаны с возможным большим сроком работы над научной разработкой.

Трудоемкость выполнения научного исследования оценивается в человеко-днях и зависит от множества трудно учитываемых факторов. Рассчитанные значения трудоемкости и длительности работ приведены в таблице 7 следующего раздела.

6.3.1. Разработка графика проведения научного исследования

Диаграмма Ганта – тип столбчатых диаграмм, который используется для иллюстрации плана или графика работ для выполнения какого-либо проекта. Работы изображаются столбцами (лентами), обозначающими их начало и окончание.

Для удобства построения графика, длительность каждого из этапов работ из рабочих дней переведем в календарные дни. Временные параметры рассчитаны для трех вариантов исполнений, в зависимости от выбранного языка программирования для разработки прототипа продукта:

- исполнение 1 – текущее (C#),
- исполнение 2 – Java,
- исполнение 3 – C++.

Все рассчитанные значения, необходимые для построения диаграммы Ганта сведем в таблицу (табл. 7). Затем строится календарный план-график для максимальных по времени исполнений работ (таблица 8). График строится с разбивкой по месяцам и декадам (10 дней) за период времени дипломирования. Выполняемые работы на графике выделены различным цветом в зависимости от исполнителей, ответственных за данную работу: зеленый цвет – работу выполняет инженер, желтый цвет – работу выполняет руководитель.

Таблица 7 – Временные показатели проведения научного исследования

Название работы/ исполнители	**Трудоёмкость работ**									**Длительность работ в рабочих днях** T_{pi}			**Длительность работ в календарных днях** T_{ki}		
	t_{min}, человеко-дни			t_{max}, человеко-дни			$t_{ожi}$, человеко-дни								
	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3
Выбор направления исследования /Р,И	7	7	7	21	21	21	12,6	12,6	12,6	6,3	6,3	6,3	9	9	9
Анализ предметной области /И	28	28	28	60	60	60	40,8	40,8	40,8	40,8	40,8	40,8	60	60	60
Аналитический обзор литературы /И	28	28	28	60	60	60	40,8	40,8	40,8	40,8	40,8	40,8	60	60	60
Утверждение темы исследования /Р,И	2	2	2	7	7	7	4	4	4	2	2	2	3	3	3
Построение классификации оценивания угроз инф. безопасности /И	60	60	60	90	90	90	72	72	72	72	72	72	106	106	106
Разработка структуры описания данных /И	30	35	40	60	65	70	42	47	52	42	47	52	62	69	77
Проектирование программного продукта /И	30	40	50	60	70	80	42	52	62	42	52	62	62	77	92
Разработка алгоритмов работы программного продукта /И	30	40	50	90	100	110	54	64	74	54	64	74	80	95	109
Разработка прототипа программного продукта /И	30	40	50	90	120	120	54	72	78	54	72	78	80	106	115
Анализ полученных результатов /Р,И	7	7	7	21	21	21	12,6	12,6	12,6	6,3	6,3	6,3	9	9	9
Составление пояснительной записки /И	14	14	14	60	60	60	32,4	32,4	32,4	32,4	32,4	32,4	48	48	48
Подготовка и оформление презентации дипломного проекта /И	2	2	2	10	10	10	5,2	5,2	5,2	5,2	5,2	5,2	8	8	8
Итого										**398**	**441**	**472**	**587**	**650**	**696**

Таблица 8 – Календарный план-график проведения НИОКР по теме

№	Вид работ	T_{ki}	Продолжительность выполнения работ																											
			сен			окт			нояб			дек			янв			фев			март			апр			май			ию
			1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
1	Выбор направления исследования /Р,И	9																												
2	Анализ предметной области /И	60																												
3	Аналитический обзор литературы /И	60																												
4	Утверждение темы исследования /Р,И	3																												
5	Построение классификации угроз инф. безопасности /И	106																												
6	Разработка структуры описания данных /И	77																												
7	Проектирование программного продукта /И	92																												
8	Разработка алгоритмов работы программного продукта /И	109																												
9	Разработка прототипа программного продукта /И	115																												
10	Анализ полученных результатов /Р,И	9																												
11	Составление пояснительной записки /И	48																												
12	Подготовка и оформление презентации проекта /И	8																												

Полученные данные подтверждают возможность большой длительности работы над научной работой. Основная часть работ выполняется инженером (студентом), около двух месяцев нужно на изучение материалов и почти семь месяцев необходимо на разработку. Сравнение вариантов исполнения показывает отличие продолжительности выполнения работ:

- первого исполнения от второго – 43 дня,
- первого исполнения от третьего – 74 дня.

Такое отличие в продолжительности связано с дополнительным изучением материалов и более сложного процесса разработки при выборе второго или третьего варианта исполнения.

6.3.2. Бюджет научно-технического исследования (НТИ)

При планировании бюджета НТИ должно быть обеспечено полное и достоверное отражение всех видов расходов, связанных с его выполнением. Так расходы напрямую влияют на необходимую величину бюджета и на цену продукта. В первом случае при необходимости большого бюджета появится необходимость поиска дополнительного финансирования, что также может увеличить продолжительность работ. При повышении цены может понизиться спрос и конкурентоспособность. Планирование бюджета является важным пунктом перед началом работ.

В процессе формирования бюджета НТИ используется следующая группировка затрат по статьям:

- материальные затраты;
- основная заработная плата исполнителей темы;
- дополнительная заработная плата исполнителей темы;
- отчисления во внебюджетные фонды (страховые отчисления);
- накладные расходы.

6.3.3. Расчет материальных затрат НТИ

Данная статья включает стоимость всех материалов, используемых при разработке проекта. При проведении данного научного исследования затраты зависят от выбора языка программирования для разработки прототипа программного продукта. Так при выборе языка C++ дополнительно понадобятся справочник по языку и онлайн-курсы, при выборе языка JAVA – только справочник, при выборе языка C# дополнительных материалов не нужно. При любом варианте исполнения для разработки и тестирования прототипа нужно приобрести USB-флеш-накопитель. Материальные затраты, необходимые для данной разработки, заносятся в таблицу 9.

Таблица 9 – Материальные затраты

Наименование	**Ед. изм.**	**Количество**			**Цена за ед., руб.**			**Затраты на материалы, ($З_м$), руб.**		
		Исп.1	**Исп.2**	**Исп.3**	**Исп.1**	**Исп.2**	**Исп.3**	**Исп.1**	**Исп.2**	**Исп.3**
USB-флеш-накопитель, 32 ГБ	шт.	1	1	1	1000	1000	1000	1000	1000	1000
Справочник по языку программирования	шт.	0	1	1	0	1000	1000	0	1000	1000
Онлайн-курсы по языку программирования	шт.	0	0	1	0	0	15000	0	0	15000
							Итого:	**1000**	**2000**	**17000**

6.3.4. Основная заработная плата исполнителей темы

В данную статью включается основная заработная плата научного руководителя и студента (инженера). Расчет затрат на основную заработную плату приведен в таблице 10.

Согласно приказу ТПУ №5994 от 25.05.2016 основная заработная плата руководителя проекта (доцент, к.т.н.) составляет 26300 рублей. Основную заработную плату инженера (студент) возьмем условно как 7864,11 рублей.

Таблица 10 – Затраты на основную заработную плату

Исполнители	Среднедневная заработная плата $C_{зп}$ (руб.)	Трудоемкость (t_i), человеко-дни			Затраты на основную зарплату (руб.)		
		Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3
Руководитель	1554,09	14	14	14	21757,27	21757,27	21757,27
Инженер	464,70	397	440	471	184484,87	204466,86	218872,48
				Итого:	**206242,14**	**226224,13**	**240629,75**

Большие затраты на основные заработные платы связаны с большими трудовыми затратами исполнителей. Проанализировав полученные величины затрат можно сделать вывод, что первый вариант исполнения выгоднее второго примерно на 20 000 рублей и выгоднее третьего примерно на 40 000 рублей.

6.3.4.1. Дополнительная заработная плата исполнителей темы

Дополнительная заработная плата включает заработную плату за неотработанное рабочее время, но гарантированную действующим законодательством. Дополнительная заработная плата равна произведению основной заработной платы на коэффициент дополнительной заработной платы (на стадии проектирования принимается равным 0,12 – 0,15). Значения дополнительной заработной платы исполнителей приведены в таблице 11.

6.3.4.2. Отчисления во внебюджетные фонды

В данной статье расходов отражаются обязательные отчисления по установленным законодательством Российской Федерации нормам органам государственного социального страхования (ФСС), пенсионного фонда (ПФ) и медицинского страхования (ФФОМС) от затрат на оплату труда работников.

На основании пункта 1 ст.58 закона №212-ФЗ для учреждений осуществляющих образовательную и научную деятельность вводится

пониженная ставка – 27,1%. Значения дополнительной заработной платы исполнителей и отчисления во внебюджетные фонды приведены в таблице 9.

Таблица 11 – Отчисления во внебюджетные фонды

Исполнитель	**Основная заработная плата, руб.**			**Дополнительная заработная плата, руб.**		
	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3
Руководитель проекта	21757,27	21757,27	21757,27	3263,59	3263,59	3263,59
Инженер	184484,87	204466,86	218872,48	27672,73	30670,03	32830,87
Коэффициент отчислений во внебюджетные фонды	0,271					
Итого						
Исполнение 1	**64275,36**					
Исполнение 2	**70502,75**					
Исполнение 3	**74992,26**					

6.3.4.3. Накладные расходы

Накладные расходы учитывают прочие затраты организации, не попавшие в предыдущие статьи расходов: печать и ксерокопирование материалов исследования, оплата услуг связи, электроэнергии и т.д.

Накладные расходы в ТПУ составляют 60% от суммы прямых затрат на разработку. Учитываемые статьи:

- материальные затраты,
- затраты на основную заработную плату,
- затраты на доп. Заработную плату,
- отчисления во внебюджетные фонды.

Величины накладных при различных исполнениях: исполнение 1: 181472,29 рублей, исполнение 2: 199596,30 рублей, исполнение 3: 221229,88 рублей. Накладные расходы при первом исполнении меньше, чем при остальных исполнениях.

6.3.4.4. Формирование бюджета затрат НТИ

Рассчитанная величина затрат научно-исследовательской работы является основой для формирования бюджета затрат проекта. Определение бюджета затрат на научно-исследовательский проект по каждому варианту исполнения показан в табл. 12.

Таблица 12 – Расчет бюджета затрат НТИ

Наименование статьи	Сумма, руб.		
	Исп.1	Исп.2	Исп.3
1. Материальные затраты НТИ	1000,00	2000,00	17000,00
2. Затраты по основной заработной плате исполнителей темы	206242,14	226224,13	240629,75
3. Затраты по дополнительной заработной плате исполнителей темы	30936,32	33933,62	36094,46
4. Отчисления во внебюджетные фонды	64275,36	70502,75	74992,26
5. Накладные расходы	181472,29	199596,30	221229,88
6. Бюджет затрат НТИ	483926,11	532256,80	589946,35

Вывод: Используя данные, полученные в пунктах 6.3.1 – 6.3.4, был рассчитан бюджет затрат научно-исследовательской работы для четырех вариантов исполнения. Наиболее низким по себестоимости оказался проект в первом варианте исполнения, затраты на его полную реализацию составляют 483926,11 рублей. Наиболее высоким по себестоимости оказался проект в третьем варианте исполнения, затраты на его полную реализацию составляют 589946,35 рублей, что почти на 100 000 рублей больше.

6.4. Определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования

Определение эффективности важно при поиске финансирования, потенциальных клиентов и определения целесообразности начала научной разработки. Определение эффективности происходит на основе расчета интегрального показателя эффективности научного исследования. Для его

нахождения необходимо также определить средневзвешенные величины: финансовая эффективность и ресурсоэффективность.

После определения интегрального финансового показателя, оценивается бюджет затрат, определяющий интегральный показатель финансовой эффективности. Затем рассчитывается интегральный показатель ресурсоэффективности (таблица 13). Первый вариант исполнения имеет наибольшее значение данного показателя.

Таблица 13 – Сравнительная оценка характеристик вариантов исполнения

Объект исследования / Критерии	Весовой коэффициент параметра	Исп.1	Исп.2	Исп.3
1. Удобство в эксплуатации (соответствует требованиям потребителей)	0,2	5	5	5
2. Качество дизайна	0,25	5	4	3
3. Возможность настройки работы	0,15	5	5	5
4. Функциональная мощность (предоставляемые возможности)	0,1	5	5	5
5. Простота эксплуатации	0,2	4	4	4
6. Качество интеллектуального интерфейса	0,1	5	5	4
ИТОГО	1	**4,9**	**4,88**	**4,78**

Сравнительная эффективность разработки, представлена в таблице 14.

Таблица 14 – Сравнительная эффективность разработки

№ п/п	Показатели	Исп.1	Исп.2	Исп.3
1	Интегральный финансовый показатель разработки	0,82	0,90	1
2	Интегральный показатель ресурсоэффективности разработки	4,9	4,88	4,78
3	Интегральный показатель эффективности	5,97	5,41	4,78
4	Сравнительная эффективность вариантов исполнения	1	0,9	0,8

Полученная сравнительная эффективность первого варианта исполнения больше остальных, что обозначает наиболее эффективный вариант решения с позиции финансовой и ресурсной эффективности.

Вывод: В ходе выполнения работы были выделены потенциальные потребители разрабатываемого продукта, определены конкурентные решения. Сравнение характеристик научной работы и конкурентных решений, проведенные анализы по технологии QuaD и SWOT помогли выявить слабые и сильные места разработки, которые будут учтены в дальнейшем. Проведенные работы определили, что разработка является конкурентоспособной. SWOT-анализ также предоставил возможность выстроить стратегии при различных появившихся на рынке возможностях и угрозах.

Затем были спланированы и распределены работы, определены продолжительности и трудоемкости работ для различных вариантов исполнений. Планирование работ позволит скоординировать работы лучшим образом для большего результата.

Также были рассчитаны величины различных затрат научно-исследовательских работ. В результате данных расчетов были получены следующие бюджеты затрат НТИ:

- затраты исполнения 1 составили 483926,11 рублей,
- затраты исполнения 2 составили 532256,80 рублей,
- затраты исполнения 3 составили 589946,35 рублей.

Можно сделать вывод, что первый вариант исполнения является наименее затратный для реализации проекта. Сравнение значений интегральных показателей эффективности позволило выбрать наиболее эффективный вариант решения проекта - исполнение 1. С позиций технической и финансовой ресурсоэффективности можно сделать вывод о том, что научно – техническое решение, представленное в первом варианте исполнения, является более предпочтительным.

7. Социальная ответственность

При работе над научно-исследовательской и проектной деятельностью имеет важное значение обеспечение безопасности охраны труда и окружающей среды, которые регламентируются в соответствии с международным стандартом ICCSR26000:2011 «Социальная ответственность организации».

Данный раздел является обязательной частью магистерской диссертации и состоит из оценки условий труда и микроклимата рабочей среды, выявления и анализа вредных и опасных факторов труда. Также рассматриваются вопросы техники безопасности, пожарной профилактики и охраны окружающей среды, даются рекомендации по созданию оптимальных условий труда.

Магистерская диссертация представляет собой разработку информационной системы мониторинга и оценки угроз информационной безопасности технологии «умный дом» и предполагает непосредственную работу с персональным компьютером. Деятельность, осуществляемая программистом, относится к категории умственного труда. По степени физической тяжести работа программиста относится к категории легких работ [16], так как производится в положении сидя и не требует физического напряжения, расход энергии составляет до 120 ккал в час.

Работа выполнялась на кафедре ПИ в 204 аудитории Кибернетического Центра ТПУ.

7.1. Техногенная безопасность

Персональный компьютер – основное оборудование, которое использовалось на протяжении выполнения ВКР.

7.1.1. Отклонение показателей микроклимата

Постоянное отклонение от нормальных параметров микроклимата приводит к перегреву или переохлаждению человеческого организма и связанным с ними негативным последствиям: при перегреве – к обильному потоотделению, учащению пульса, головокружению, резкой слабости, появлению судорог, в тяжелых случаях – возникновению теплового удара, при переохлаждении возникают простудные заболевания, хронические воспаления суставов, мышц и др. [17].

В помещениях, где осуществляется работа на компьютерах, для создания комфортных для работы условий должны быть соблюдены необходимые параметры микроклимата. В санитарных нормах СанПиН 2.2.4.548-96 установлены величины параметров микроклимата, создающие комфортные условия [16].

Таблица 15 – Оптимальные величины показателей микроклимата на рабочих местах производственных помещений

Период года	Категория работ по уровню энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Ia (до 139)	22 - 24	21 - 25	60 - 40	0,1
Теплый	Ia (до 139)	23 - 25	22 - 26	60 - 40	0,1

Таблица 16 – Допустимые величины показателей микроклимата на рабочих местах производственных помещений

Период года	Категория работ по уровню энергозатрат, Вт	Температура воздуха, °С		Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с	
		диапазон ниже оптимальных величин	диапазон выше оптимальных величин			для диапазона температур воздуха ниже опт. величин, не более	для диапазона температур воздуха выше оптимальных величин, не более
Холодный	Ia (до 139)	20,0 – 21,9	24,1 - 25,0	19,0 - 26,0	15 - 75	0,1	0,1
Теплый	Ia (до 139)	21,0 - 22,9	25,1 - 28,0	20,0 - 29,0	15 - 75	0,1	0,2

Помещение, в котором располагается рабочее место, оснащено системой центрального отопления и приточно-вытяжной вентиляцией, которые определяют параметры микроклимата. Значения параметров микроклимата: влажность 46%, скорость движения воздуха 0,1 м/с, температура летом 23-24°С, зимой 22-23°С. Основываясь на требуемых значениях параметров, описанных в таблице 16, можно сделать вывод, что показатели микроклимата соответствуют нормам.

Таблица 17 – Нормы подачи свежего воздуха в помещения с компьютерами

Характеристика помещения	Объемный расход подаваемого в помещение свежего воздуха, м3 /на одного человека в час
Объем до 20м^3 на человека 20…40м^3 на человека Более 40м^3 на человека	Не менее 30 Не менее 20 Естественная вентиляция

Объем рабочих помещений не должен быть меньше 19,5 $м^3$/человека с учетом максимального числа одновременно работающих в смену.

7.1.2. Повышенный уровень шума на рабочем месте

Повышенный уровень шума на рабочем месте может нанести ущерб здоровью работника и сильно снизить производительность труда. Работники, подверженные длительному шумовому воздействию, испытывают раздражительность, головные боли, повышенную утомляемость и другие недомогания. Эти последствия снижает производительность работника, его качество и безопасность труда [18]. Для снижения уровня шума стены и потолок помещений, содержащих компьютеры, могут быть облицованы звукопоглощающими материалами.

По субъективным ощущениям уровень шума на рабочем месте не превышает предельные уровни звука [19] и не оказывает отрицательное влияние на работника.

Таблица 18 – Предельные уровни звука (в соответствии с СНиП 23 – 03 – 2003).

Назначение помещений или территорий	Уровень звукового давления (эквивалентный уровень звукового давления) L, дБ, в октавных полосах частот со среднегеометрическими частотами, Гц									Уровень звука L_A (эквивалентный уровень звука $L_{AЭКВ}$), дБА	Максимальный уровень звука $L_{Aмакс}$, дБА
	31,5	63	125	250	500	1000	2000	4000	8000		
1 Рабочие помещения административно-управленческого персонала производственных предприятий, лабораторий, помещения для измерительных и аналитических работ	93	79	70	63	58	55	52	50	49	60	70

7.1.3. Повышенный уровень электромагнитных излучений

Максимальный уровень рентгеновского излучения на рабочем месте оператора компьютера обычно не превышает 10мкбэр/ч, а интенсивность ультрафиолетового и инфракрасного излучений от экрана монитора лежит в пределах 10…100мВт/м^2.

Использование мониторов с пониженным уровнем излучения позволит снизить воздействия рентгеновского излучения, также этому способствует установка защитных экранов. Также необходимо соблюдать регламентированные режимы труда и отдыха. ПДУ электромагнитных полей на рабочих местах пользователей ПК и другими средствами ИКТ [20] представлены в таблице 19.

Таблица 19 – ПДУ электромагнитных полей на рабочих местах

Нормируемые параметры		**ПДУ**
Напряженность электрического поля	5 Гц - < 2 кГц	25 В/м
	2 кГц - < 400 кГц	2,5 В/м
Напряженность магнитного поля	5 Гц - < 2 кГц	250 нТл
	2 кГц - < 400 кГц	25 нТл
Плотность потока энергии	300 МГц - 300 ГГц	10 мкВт/см^2
Напряженность электростатического поля		15 кВ/м

7.1.4. Повышенный уровень ионизирующих излучений

Источник ионизирующего излучения при работе с компьютером – дисплей монитора. Ионизирующее излучения при воздействии на организм может вызвать торможение функций кроветворных органов, нарушение свертываемости крови, понизить сопротивляемость организма инфекционным заболеваниям и др.

При выполнении дипломной работы использовался монитор с низким уровнем излучения: расстояние до дисплея составляет 20 см, при котором доза облучения равна 50 мкбэр/час. По нормам [21] в любой точке на расстоянии 5 см от дисплея и корпуса ВДТ конструкция ВДТ и ПЭВМ

должна обеспечивать мощность экспозиционной дозы рентгеновского излучения не более 7,7*10 А/кг.

7.1.5. Недостаточная освещенность рабочей зоны

Недостаточное освещение на рабочем месте влияет на работу зрительного аппарата человека, а также его эмоциональное состояние, и способно вызвать усталость центральной нервной системы [22].

Освещение подразделяется на три вида: естественное, искусственное и совмещенное. Естественное освещение - освещение помещений дневным светом. Искусственное освещение используется в темное время суток и днем, при несоответствии нормам значений коэффициента естественного освещения. Совмещенное освещение представляет собой недостаточное естественное освещение дополнено искусственным освещением [23].

Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий [24] представлены в таблице 20.

Таблица 20 – Нормы освещенности (в соответствии с СанПиН 2.2.1/2.1.1.1278-03)

Помещения	Рабочая поверхность и плоскость нормирования КЕО и освещенности (Г – горизонтальная, В – вертикальная) и высота плоскости над полом, м	Естественное освещение		Совмещенное освещение		Искусственное освещение				
		КЕО e_н, %		КЕО e_н, %		Освещенность, лк				
		При верхнем или комбинированном освещении	При боковом освещении	При верхнем или комбинированном освещении	При боковом освещении	При комбинированном освещении		При общем освещении	Показатель дискомфорта, М, не более	Коэффициент пульсации освещенности, К_п, %, не более
						всего	от общего			
1	2	3	4	5	6	7	8	9	10	11
Административные здания (министерства, ведомства, комитеты, префектуры, муниципалитеты управления, конструкторские и проектные организации, научно-исследовательские учреждения и т.п.)										
1. Кабинеты, рабочие комнаты, офисы, представительства	Г – 0,8	3,0	1,0	1,8	0,6	400	200	300	40	15

7.1.6. Электробезопасность

На рабочем месте используются клавиатура, мышь, монитор и системный блок. Все эти предметы имеют токи статического электричества, которые могут привести к возникновению разрядов при прикосновении. Для человека данные разряды не опасны, но возникновение заряда с большим электрическим потенциалом породит вокруг себя электрическое поле с повышенной напряженностью, которое может нанести вред человеку. Продолжительное пребывание человека в таком электрическом поле влияет на центральную нервную систему и сердечно-сосудистую систему. Избыточный электрический заряд может быть опасен и для компьютера, его наличие может привести к поломке компьютера. Для снижения токов статического электричества на рабочем месте используются различные нейтрализаторы и увлажнители воздуха.

7.2.Региональная безопасность

Экологическая безопасность является важным аспектом при осуществлении какой-либо деятельности. Одним из важных факторов является способ утилизации отходов. Утилизация компьютерного оборудования является сложным процессом, по причине наличия сложной структуры оборудования. Для переработки многих компонентов компьютера необходимо выполнить сортировку, затем гомогенизацию и помол или переплавка для возможности повторного использования.

Люминесцентные лампы являются чрезвычайно опасным видом отходов, так как содержат от 3 мг до 5 мг ртути. Наличие ртути исключает возможность утилизировать вышедшие из строя лампы в обычный контейнер с отходами. Люминесцентные лампы требуют утилизации специальными коммунальными службами, занимающимися вывозом специальных отходов. Транспортировка таких отходов должна выполняться только организациями, специализирующимися на утилизации опасных отходов.

7.3. Организационные мероприятия обеспечения безопасности

Одно рабочее место пользователя ПЭВМ должно иметь площадь не менее 6 $м^2$. При использовании персональных компьютеров на рабочем месте нужно учитывать расстояние между рабочими столами с мониторами.

Рабочие места с ПЭВМ не должны быть расположены вблизи силовых кабелей и вводов, технологического оборудования, создающего помехи в работе ПЭВМ.

Такие показатели микроклимата производственного помещения как температура, относительная влажность и скорость движения воздуха соответствовать действующим санитарным нормам микроклимата производственных помещений.

Внутренняя отделка помещений, в которых используются компьютеры, должна быть выполнена с использованием диффузно-отражающих материалов с коэффициентами отражения:

- для потолка от 0,7 до 0,8;
- для стен от 0,5 до 0,6;
- для пола от 0,3 до 0,5.

Поверхность пола не должна быть скользкой, она должна представлять собой ровную и удобную для влажной уборки поверхность. Также поверхность должна иметь антистатические свойства.

Обязательными требованиями является наличие углекислотного огнетушителя для тушения пожара и аптечка первой медицинской помощи.

Согласно СанПиНу 2.2.4.3359-16 при 8-часовой рабочей смене на ВДТ и ПЭВМ перерывы в работе должны составлять от 10 до 20 минут каждые два часа работы.

7.4. Особенности законодательного регулирования проектных решений

Согласно статье 91 трудового кодекса РФ, продолжительность рабочего времени в неделю не должна превышать 40 часов. Для работников-

инвалидов I или II группы устанавливается сокращенная продолжительность рабочего времени - не более 35 часов в неделю, в соответствии с статьей 92 трудового кодекса РФ. Также возможно применение гибкого режима рабочего времени. В соответствии с медицинским заключением беременным женщинам по их заявлению должны быть снижены нормы выработки, сохранив при этом средний заработок (ст. 254 ТК РФ).

7.5.Безопасность в чрезвычайных ситуациях

Состояние защищённости личности, имущества, общества и государства от пожаров представляет собой пожарную безопасность. Пожарная безопасность должна быть обеспечена системой пожарной защиты и системой предотвращения пожара.

Опасный фактор пожара (ОФП):

- пламя и искры;
- тепловой поток;
- повышенная температура окружающей среды;
- повышенная концентрация токсичных продуктов горения и термического разложения;
- пониженная концентрация кислорода;
- снижение видимости в дыму.

Действия при пожаре в здании:

- При наличии телефона, «112» или «01» сообщить о пожаре и своем местоположении;
- Не входить в места с высокой концентрацией дыма и видимостью менее чем 10 метров;
- Покинуть помещение, используя запасные и основные пути эвакуации;
- Попутно отключить электроэнергию;
- Передвигаться к выходу на четвереньках, при этом закрывая рот и нос подручными средствами защиты;

- Плотно закрыть дверь при выходе;

Если дым и пламя в соседних помещениях не позволяет выйти наружу:

- Стараться не поддаваться панике;
- Проверить возможности спуститься по пожарной лестнице или выйти на крышу;
- При отсутствии возможности эвакуироваться для защиты от дыма и тепла необходимо как можно надёжнее герметизировать своё помещение:
- Плотно закрыть двери, окна и форточки, заткнуть щели изнутри, используя при этом любую, желательно мокрую, ткань;
- При наличии воды, постоянно смачивать двери и пол.

Рабочее место располагается в 204 аудитории кибернетического центра ТПУ. Пожарная безопасность в ТПУ обеспечивается в соответствии с требованиями ФЗ пожарной безопасности № 69-ФЗ от 21.12.1994 г., правилами противопожарного режима в РФ. На рисунке 21 представлен план эвакуации второго этажа кибернетического центра.

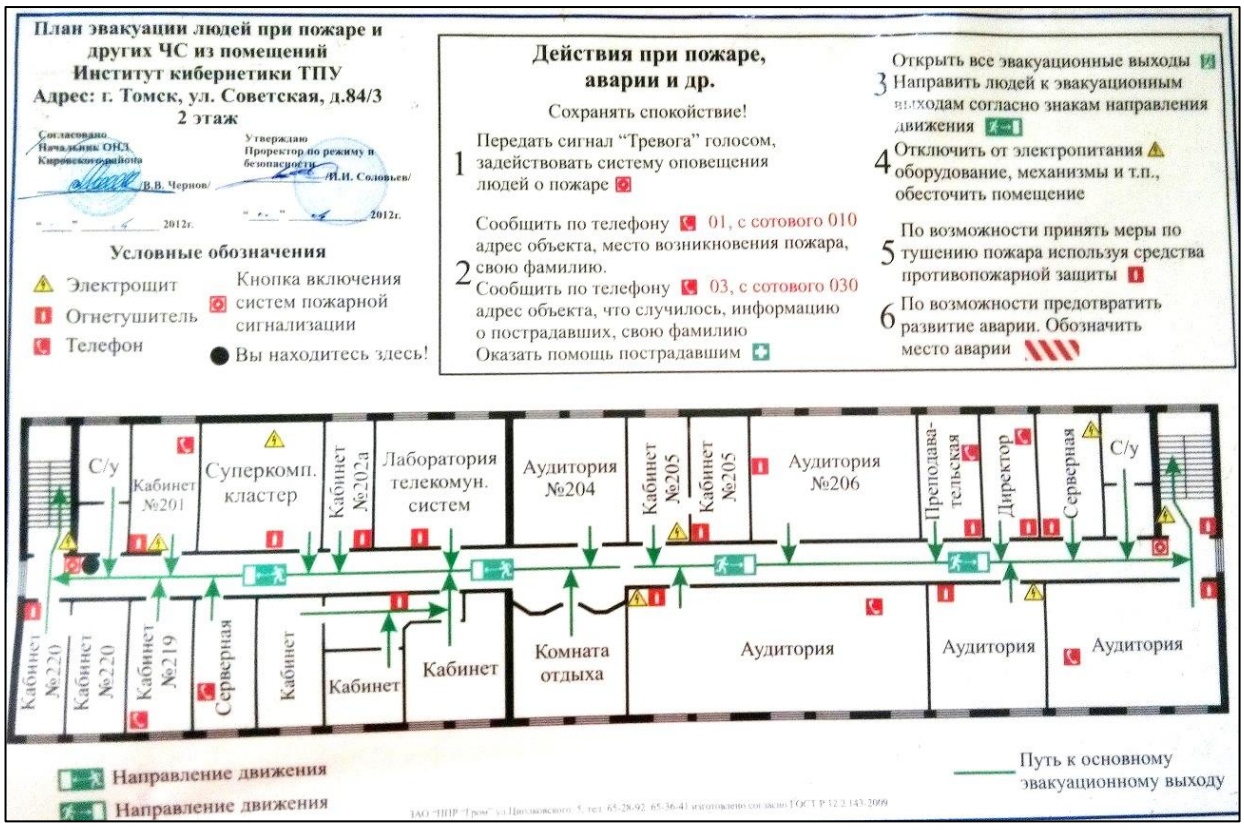

Рис. 21 План эвакуации

Заключение

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

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

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

Результаты работы доказывают работоспособность информационной системы и позволяют сделать вывод о возможности разработки средства защиты систем «умный дом», настраиваемого пользователем под его систему УД. Данное средство защиты осуществляет мониторинг состояния всей системы и оценивает найденные угрозы.

Список публикаций

1. Абдрашитова, В.И. Объектно-ориентированный подход к моделированию системы информационной безопасности технологии "Умный дом" [Электронный ресурс] / В. И. Абдрашитова, Н. Ю. Хабибулина // Молодежь и современные информационные технологии : сборник трудов XIII Международной научно-практической конференции студентов, аспирантов и молодых ученых, г. Томск, 9-13 ноября 2015 г.в 2 т. / Национальный исследовательский Томский политехнический университет (ТПУ), Институт кибернетики (ИК) ; под ред. Т. Е. Мамоновой [и др.]. — 2016. — Т. 2. — [С. 147-148]. — Заглавие с титульного экрана. — Свободный доступ из сети Интернет. — Adobe Reader. Режим доступа: http://earchive.tpu.ru/handle/11683/17014
2. Абдрашитова, Венера Исхаковна. Объектный подход к моделированию системы информационной безопасности технологии "Умный дом" [Электронный ресурс] / В. И. Абдрашитова, Н. Ю. Хабибулина // Научная сессия ТУСУР-2016 : материалы Международной научно- технической конференции студентов, аспирантов и молодых ученых, г. Томск, 25-27 мая 2016 г.в 6 ч. / Томский государственный университет систем управления и радиоэлектроники (ТУСУР). — 2016. — Ч. 4. — [С. 173-176]. — Заглавие с экрана. — Свободный доступ из сети Интернет. Режим доступа: https://storage.tusur.ru/files/44766/2016_4.pdf#page=174
3. Абдрашитова, Венера Исхаковна. Угрозы информационной безопасности технологии "умный дом" [Электронный ресурс] / В. И. Абдрашитова, Н. Ю. Хабибулина // Научная сессия ТУСУР-2016 : материалы Международной научно- технической конференции студентов, аспирантов и молодых ученых, г. Томск, 25-27 мая 2016 г.в 6 ч. / Томский государственный университет систем управления и радиоэлектроники (ТУСУР). — 2016. — Ч. 4. — [С. 176-179]. — Заглавие с экрана. — Свободный доступ из сети Интернет. Режим доступа: https://storage.tusur.ru/files/44766/2016_4.pdf#page=177

4. Абдрашитова, Венера Исхаковна. Информационное обеспечение системы информационной безопасности технологии "Умный дом" [Электронный ресурс] / В. И. Абдрашитова, Н. Ю. Хабибулина // Молодежь и современные информационные технологии : сборник трудов XIV Международной научно-практической конференции студентов, аспирантов и молодых ученых, г. Томск, 7-11 ноября 2016 г.в 2 т. / Национальный исследовательский Томский политехнический университет (ТПУ), Институт кибернетики (ИК) ; под ред. В. С. Аврамчук [и др.]. — Томск: Изд-во ТПУ, 2016. — Т. 2. — [С. 33-34]. — Заглавие с титульного экрана. — Свободный доступ из сети Интернет. Режим доступа: http://earchive.tpu.ru/handle/11683/37071
5. Абдрашитова, Венера Исхаковна. Информационная система мониторинга и оценки угроз информационной безопасности технологии «умный дом» [Электронный ресурс] / В. И. Абдрашитова, Н. Ю. Хабибулина // Научная сессия ТУСУР-2017 : материалы Международной научно- технической конференции студентов, аспирантов и молодых ученых, г. Томск, 10-12 мая 2017 г.в 8 ч. / Томский государственный университет систем управления и радиоэлектроники (ТУСУР). — 2017. — Ч. 5. — [С. 176-178]. — Заглавие с экрана. — Свободный доступ из сети Интернет. Режим доступа: https://storage.tusur.ru/files/61043/2017_5.pdf#page=177

Дипломы

1. Диплом II-степени за доклад «Угрозы информационной безопасности технологии "умный дом"», XXI Международная научно- техническая конференция «Научная сессия ТУСУР-2016».
2. Диплом II-степени за доклад «Информационная система мониторинга и оценки угроз информационной безопасности технологии «умный дом», XXII Международная научно- техническая конференция «Научная сессия ТУСУР-2017».

Список используемых источников

1. Малыш В.Н., Букреев Д.С. Анализ угроз информационной безопасности системы «умный дом» //Труды международного симпозиума «Надежность и качество». 2012. – Т.1.
2. Test: Smart Home Kits Leave the Door Wide Open – for Everyone [Электронный ресурс]. – URL: https://www.av-test.org/en/news/news-single-view/test-smart-home-kits-leave-the-door-wide-open-for-everyone , свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 18.05.2017 г.
3. Push-Button Manor. Popular Mechanics Magazine /N.Y., 1950. – № 410426 – 298 с.
4. National Association of Home Builders [Электронный ресурс] – URL: https://www.nahb.org, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 20.05.2017 г.
5. Всесоюзная книжная палата. Летопись газетных статей – М.: Всесоюзная книжная палата, 1993. – В. 1-13.
6. Академия наук СССР. Япония – М., 1993.
7. Гаврилов А.В. Искусственный домовой //Искусственный интеллект и принятие решений. 2012. – 02/2012. – С.77-89.
8. Защита информации. Объект информатизации. Факторы, воздействующие на информацию: ГОСТ Р 51275-2006. – Введ. 2008.02.01.– М.: Стандартинформ, 2007. – 8с.
9. Дарья Хохлова. Dojo – устройство для защиты «умного» дома от взлома. [Электронный ресурс]. – URL: https://vc.ru/p/dojo, свободный. – Загл. с экрана. – Яз. рус. Дата обращения: 18.05.2017 г.
10. Дарья Хохлова. CUJO – система защиты «умного» дома. [Электронный ресурс]. – URL: https://vc.ru/p/cujo, свободный. – Загл. с экрана. – Яз. рус. Дата обращения: 18.05.2017 г.

11. Обзор Bitdefender Box [Электронный ресурс]. – URL: https://www.comss.ru/page.php?id=2397, свободный. – Загл. с экрана. – Яз. рус. Дата обращения: 18.05.2017 г.
12. Новое решение Cisco по безопасности следующего поколения (NGFW+NGIPS+AMP) [Электронный ресурс]. – URL: https://habrahabr.ru/company/cisco/blog/237759, свободный. – Загл. с экрана. – Яз. рус. Дата обращения: 18.05.2017 г.
13. Снегуров А.В., Ткаченко Е.А., Кравченко А.Д. Риски информационной безопасности систем, построенных по технологии «умный дом» //Восточно-Европейский журнал передовых технологий. 2011. – №3(52) Т.4 2011 – С.30-34.
14. Перегудов Ф.И., Тарасенко Ф.П. Основы системного анализа. – Томск: Изд-во НТЛ, 1997. – 396 с.
15. Вихорев С.В. Классификация угроз информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения: 1.05.2017).
16. СанПиН 2.2.4.548-96. Гигиенические требования к микроклимату производственных помещений.
17. Экология и безопасность жизнедеятельности: Учеб. пособие для вузов/ Д.А. Кривошеин, Л.А.Муравей, Н.Н. Роева и др.; Под ред. Л.А. Муравья. – М.: ЮНИТИ-ДАНА, 2000. - 447 с.
18. Борьба с шумом на производстве: Справочник / Е.Я. Юдин, Л.А. Борисов; Под общ. ред. Е.Я. Юдина – М.: Машиностроение, 1985. – 400с., ил.
19. СНиП 23 – 03 – 2003. Защита от шума.
20. СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах.

21. Р 2.2.2006 – 05. Руководство по гигиенической оценке факторов рабочей среды и трудового процесса. Критерии и классификация условий труда.
22. Самгин Э.Б. Освещение рабочих мест. – М.: МИРЭА, 1989. – 186с.
23. Справочная книга для проектирования электрического освещения. / Под ред. Г.Б. Кнорринга. – Л.: Энергия, 1976.
24. СанПиН 2.2.1/2.1.1.1278-03. Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий.
25. Smart Homes & Buildings Association [Электронный ресурс] – URL: https://shabawebsite.wordpress.com, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 17.05.2017 г.
26. Tiago D. P. Mendes, Radu Godina, Eduardo M. G. Rodrigues, Joao C. O. Matias, Joao P. S. Catalao. Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources// Energies. – 2015 vol.8 – P. 7279 – 7311.
27. Diane J. Cook. Multi-agent smart environments// Journal of Ambient Intelligence and Smart Environments – IOS Press, 2009. – Vol. 1, P. 47–51
28. Location-aware Services and Interfaces in Smart Homes using Multiagent Systems/ Juan R. Velasco, Ivan Marsá Maestre, Andrés Navarro, Miguel A. López, Antonio J. Vicente, Enrique de la Hoz, Alvaro Paricio and Miriam Machuca/4th KES International Symposium, KES-AMSTA 2010 Gdynia, Poland, June 23-25, 2010, Proceedings Part II
29. Junestrand, S. Being private and public at home – an architectural perspective on smart home//School of Architecture, Royal School of Technology. – Stockholm, 2004
30. InCONTEXT blog. Smart Home survey Latam unveiled [Электронный ресурс] – URL: https://contextworld.wordpress.com/2017/02/17/smart-

home-survey-latam-unveiled, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 17.05.2017 г.

31. The Independent IT-Security Institute AV-TEST [Электронный ресурс] – URL: https://www.av-test.org/en, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 18.05.2017 г.
32. DojoLab [Электронный ресурс] – URL: https://www.dojo-labs.com, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 15.05.2017 г.
33. TechCrunch. Dojo Is Designed To Protect Your Smart Home From Itself [Электронный ресурс] – URL: https://techcrunch.com/2015/11/19/dojo-labs, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 15.05.2017 г.
34. WIRED. This Fancy Rock Wants to Protect Your Connected Devices [Электронный ресурс] – URL: https://www.wired.com/2015/11/this-fancy-rock-wants-to-protect-your-connected-devices/#slide-6, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 15.05.2017 г.
35. CUJO [Электронный ресурс] – URL: https://www.getcujo.com, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 01.05.2017 г.
36. Indiegogo. CUJO. The Smart Way To Fight Hacking. [Электронный ресурс] – URL: https://www.indiegogo.com/projects/cujo-the-smart-way-to-fight-hacking-security#, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 15.05.2017 г.
37. Bitdefender BOX – IoT Security Solution For All Connected Devices [Электронный ресурс] – URL: https://www.bitdefender.com/box, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 15.05.2017 г.
38. Cisco Corporate Overview and Resources. The Network [Электронный ресурс] – URL: https://newsroom.cisco.com/overview, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 15.05.2017 г.

39. Cisco Systems, Inc [Электронный ресурс] – URL: https://info.sourcefire.com/2015NSSNGIPSReport-CDC.html, свободный. – Загл. с экрана. – Яз. англ. Дата обращения: 15.05.2017 г.
40. Security and Resilience of Smart Home Environments – Good Practices and Recommendations // European Union Agency for Network and Information Security (ENISA)/ Dr. Cédric Lévy-Bencheton, Ms. Eleni Darra, Mr. Guillaume Tétu, Dr. Guillaume Dufay, Dr. Mouhannad Alattar. –2015. – P.77

Приложение А

Раздел 1
An overview of smart homes and information security of smart homes

Студент:

Группа	ФИО	Подпись	Дата
8КМ51	В.И. Абдрашитова		

Консультант кафедры ПИ:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Е.С. Чердынцев	к.т.н.		

Консультант – лингвист кафедры ИЯИК:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
зав. каф.	Т.В. Сидоренко	к.пед.н.		

1.1.Smart home

One of the major definitions of smart home is the integration of technology and services through home networking for a better quality of living [25]. Smart homes differ in infrastructure and purpose of use. General purposes of using smart home systems [26]:

- energy efficiency and management,
- health care,
- entertainment,
- security.

Optimizing the individual functions selection of smart home is determined by specific user requirements. Smart home systems can be used in different small and large enterprises in general for energy management and security or in houses for any purposes. Many companies offer full construction or customized solutions. Also a lot of electronics manufacturers (Samsung, Philips, Apple etc.) produce smart devices that can be connected into manually assembled smart home system. Company`s products contain a protocol, which allows communication between all products, remote control and central controller. Unfortunately, all products of different manufacturers can`t communicate via the same protocol.

Researchers apply different approaches to describe a smart home system. Some of them describe it like a multi-agent system [27, 28], other researchers consider a system containing different kinds of subsystems, which is a more common approach used both by researchers and by smart home companies. For example, some companies (Vera Control, Control4, Notion etc.) distinguish 4-6 subsystems, others (HomeSeer, Smart Home Systems etc.) distinguish about 10-12 subsystems. One of the common system infrastructures [29] is shown in figure 1.

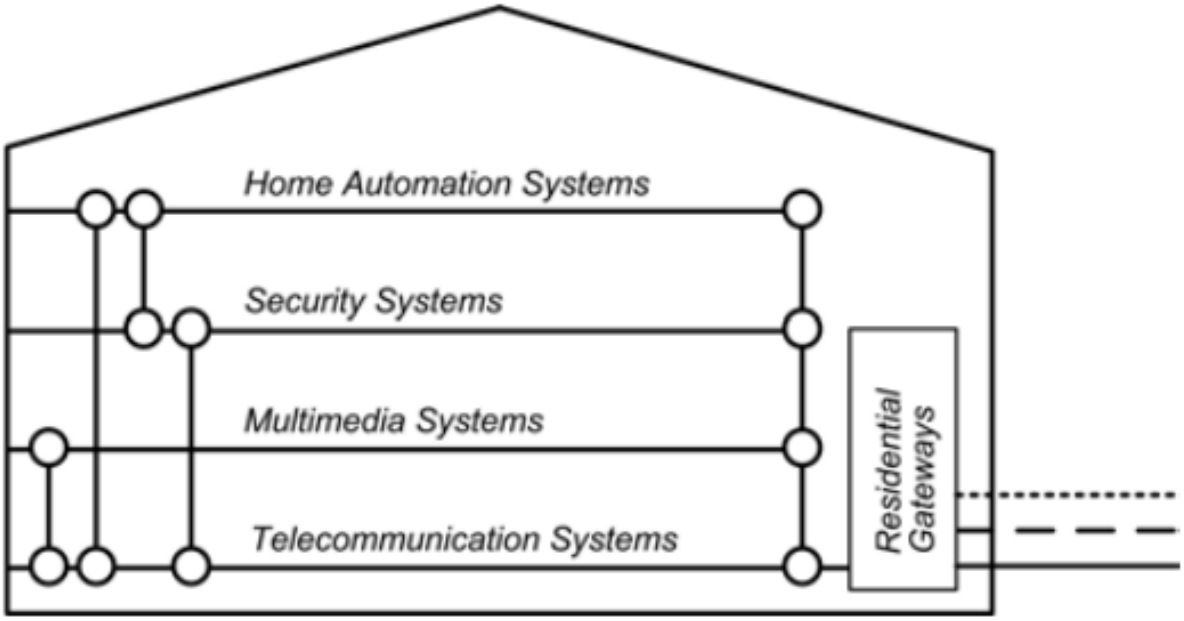

Fig.1 Common smart home system infrastructure

1.2.Security issue

Security is not just about cryptography, but it is also about assessing the risk of threats in a given environment or situation and developing safeguards and measures to eliminate against these risks. A smart home system has a large number of connected smart devices which communicate with each other mainly via wired and wireless network. A large flow of information in the system is of big interest for hackers. Regretfully, people are more concerned about the physical risks of owning a smart home product than the cyber risks [30]. But this is the list of risk examples:

- a hacker could thieve personal data through information interception from a network;
- a hacker could disable alarm or open doors and windows by accessing smart home control subsystem;
- a burglar could detect if house is empty by remotely accessing cameras.

Unfortunately, not all smart homes provide effective information security, some systems do not have any information security tool, so and owners of smart homes should not forget about their information security.

In 2014 the independent IT-Security Institute AV-TEST [31] carried security test [2] of seven starter kits for smart home solutions, which are primarily sold by large companies.

Products tested by AV-TEST experts:

- iConnect from eSaver,
- tapHome from EUROiSTYLE,
- Gigaset Elements from Gigaset,
- iComfort from REV Ritter,
- RWE Smart Home from RWE,
- QIVICON from Deutsche Telekom,
- XAVAX MAX! from Hama.

Testers analyzed the protection concept used by each product, focusing on tested protection functions:

- encrypted communication between system components,
- active authentication to control a system,
- manipulation by external parties,
- secure remote control.

Products and test results were represented AV-TEST experts in the table and are shown in figure 2.

Product	**Gigaset Elements**	**RWE Smart Home**	**QIVICON**	**iComfort**	**tapHome**	**iConnect**	**XAVAX MAX!**
Provider	**Gigaset**	**RWE**	**Deutsche Telekom**	**REV Ritter**	**EUROiSTYLE**	**eSaver**	**Hama**
Components and software supplied	Gateway, door sensor, movement sensor and the "Gigaset Elements" smartphone app	Gateway, socket switch (on/off), wall switch (2 buttons), radiator thermostat, online portal, mobile online portal, local portal and the "RWE SmartHome" smartphone app	Gateway, socket switch (on/off), radiator thermostat, smoke detector and the "Smart Home" smartphone app	Gateway, 2 socket switches (on/off) and the "REV iComfort" smartphone app	Gateway, socket switch (on/off), dimmable socket and the "tapHOME Hausautomatisierung" smartphone app	Gateway, 2 socket switches (on/off) and the "eSaver Cloud" smartphone app	Gateway, 2 radiator thermostats, eco wall switch (with an eco/auto option), window contact, MAX desktop software and an online portal
Protection Functions Provided							
Encrypted communication	YES	YES	YES	NO	NO	YES	PARTIALLY
Active authentication	YES	YES	YES	NO	YES	Only for Web access	Only for Web access
Manipulation by external parties	Not possible	Not possible	Not possible	Not possible	Not possible	Susceptible to manipulations	Susceptible to manipulations
Secure remote control	Effective protection	Effective protection	Effective protection	Remote control not possible	Remote control not possible	Susceptible to manipulations	Susceptible to manipulations
Test result	**Good protection**	**Good protection**	**Good protection**	**Vulnerable protection**	**Vulnerable protection**	**Insufficient protection**	**Insufficient protection**
Explanation	An effective protection concept	An effective protection concept	An effective protection concept	No protection against internal attacks	No protection against internal attacks	No protection against internal and external attacks	No protection against internal and external attacks
Comments	None	Configuration only possible with Internet access	Encryption methods could be even better	Malicious software that has broken into the local network can infiltrate the system	Malicious software that has broken into the local network can infiltrate the system	No barriers for attackers; remote access vulnerable	Incomplete encryption gives attackers free rein of the system

Fig. 2 Results of AV-TEST test

Only three kits are well secured against attacks, while other kits are poor protected against internal and, in some cases, external attacks. Gigaset Elements, RWE Smart Home and QIVICON have good protection against attacks and unauthorized access. These three kits use encrypted communications between components, have active authentication and are not being injected with a malicious code. iComfort and tapHome are not protected against internal attacks, especially iComfort which doesn't use active authentication. The iConnect and XAVAX MAX! kits are remote access vulnerable and have no protection against internal and external attacks.

This test covers only seven products but demonstrates the importance of high level security. An insecure smart home solution may provide intruders with a back door leading into home network. However, such products don't have a security standard, for this reason the development of effective security protection is a problem.

Smart homes with poor security protection can use additional protection tools. Security companies and some electronics manufacturer that have been exploring ways of securing smart from cyber-attacks develop this kind of protection tools, but not all of them can be connected to any kind of smart home system.

1.3. Existing solutions for smart home security protection

Dojo is security device developed by a small Israeli company “Dojo-Labs” [32]. The development was first mentioned in the Internet in autumn 2015 [33]. The launch of sales was planned for the beginning of 2016. At this moment Dojo is available to pre-order at the official website.

The company is aimed to create a consumer-friendly security and control interface at the network layer that is capable of spotting and blocking anomalous behavior of connected devices on home network. Dojo is a physical object that looks like a rock and a small white box. The device has a really attractive design. The

designer of the device calls it “a digital pet rock, that’s kind of innocuous, and is just going to sit in the corner” [34].

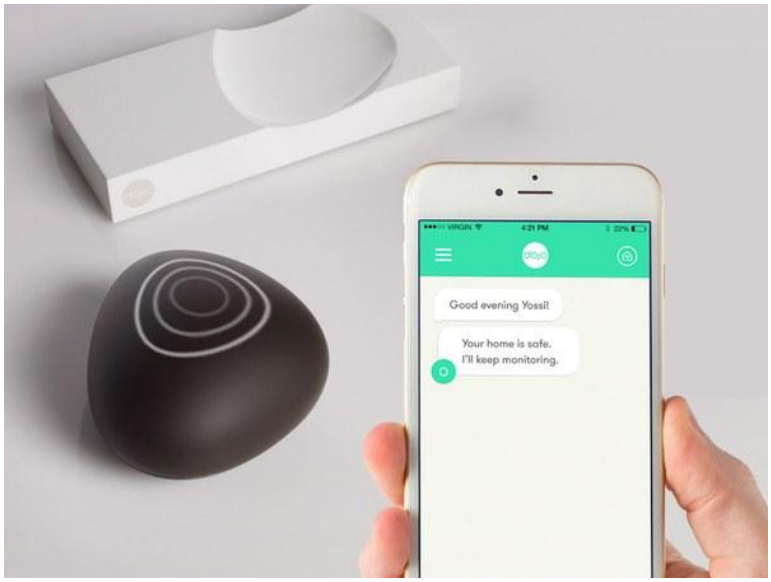

Fig.3 Three components of Dojo

The Dojo’s white box plugs into Wi-Fi router and monitors all network traffic in real time and detects anomalies and threats. “Digital pet rock” has lighting systems to indicate security status. It’s the only function of this component except for the design. Dojo is controlled via smartphones “Dojo App”. All notifications appear in the application which allows the user to know about issues before they affect his privacy or security.

Dojo is connected to the cloud to learn metadata from user’s devices and improve threats detecting. It’s a smart solution to increase the known threats database, but it is also of great interest for hackers. “One cloud-based server with huge amount of metadata” - sounds quite inviting. Another disadvantage is no interaction with non-Internet-connected devices which can be affected by threats too.

CUJO is a security device developed by a group of Californian researchers [35]. It was first mentioned in the Internet in autumn 2015. The founders of the project received funding at the crowdfunding website [36]. The launch of sales was planned for March 2016. At present, there is no information about a possibility to buy or pre-order the device, the official website shows the “404 Error” page.

Fig.4 Design of CUJO

To protect devices from a broad range of attacks CUJO uses a multilayer approach that combines both firewall and antivirus. It acts as a gateway between devices and for connection to the Internet. CUJO is very similar to Dojo. It is not just the names. CUJO has a attractive design with “eyes” - indicators. Just like Dojo, the device plugs into Wi-Fi router and monitors traffic. CUJO is controlled by a smartphone and uses a cloud too. The device has the same disadvantages as CUJO.

Bitdefender Box is developed by Bitdefender, a large Romanian company specialized in antivirus products. There are three product variations for different protection levels and a number of connected devices on the official website [37]. Unfortunately, Bitdefender Box is certified for use only in the USA, France and Japan. That is why the device is currently available only in these countries.

Fig.5 Design of Bitdefender Box

Bitdefender BOX continuously scans, identifies and highlights network security flaws. It looks for hidden backdoors and inadequately secured management ports.

The product works like two previous devices: a box-shaped device, a modem, a smartphone application and a cloud. It has still the same disadvantages.

The company specialization and large experience allowed not collecting extra data. It turns out to be the main advantage of Bitdefender Box.

Cisco ASA 5500-X - with FirePOWER Services is a series of devices with integrated threat-oriented firewalls manufactured by a huge multinational American company “Cisco Systems, Inc.” (Cisco). Cisco specializes into Internet of Things, domain security, and energy management. Cisco develops and manufactures networking hardware, telecommunications equipment and other products [38]. Among the major customers are large and small enterprises.

These devices are firewalls with extended function of connection monitoring which provides transparency and awareness of the context of the application. The series has simple design, which seems to be typical for such devices.

Fig.6 Design of Cisco ASA 5500-X - with FirePOWER Services

The main advantage of this series is high security effectiveness confirmed by tests [39]. It’s a high-tech product with a corresponding price. The series is developed for small and large enterprises and requires quite a difficult installation and maintenance and, as a result, highly-qualified staff.

1.4.Model of smart home security tool

All smart home security devices have different structure and use different algorithms, but it is possible to identify a common model. The development of smart home security tools may be divided into several stages:

- description of an entire system formal model,
- description of a threat model,
- development of threat assessment algorithms,
- design of an automatic mechanism to monitor the security status.

As mentioned earlier, smart home systems can be described on the basis of different approaches. The presentation and categories of threats also differ from analysis to analysis in researches. The development of threat assessment algorithms should be built on a formal model of entire system and a threat model. Threat assessment algorithms may also use special threat assessment criteria: sources of threat, possible consequences, vulnerability and a list of the most likely threats. An automatic mechanism to monitor the security status of smart home generally depends on the used protocols and the type of network.

The European Union Agency for Network and Information Security (ENISA) analyzed researches of threats [40] and offered the following threats groups:

- Physical attacks (physical manipulation of devices).
- Unintentional damage (accidental).
- Disasters and Outages.
- Damage/Loss (IT Assets).
- Failures/Malfunctions
- Eavesdropping/Interception/Hijacking (as well as Nefarious Activity/Abuse)
- Legal (as described in the ENISA documentation, this is another possible consequence of the same attacks).

Приложение Б

XML Schema-файл для XML-файла состава системы

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="System" type="systemcomponents"/>
  <xs:complexType name="systemcomponents">
    <xs:sequence>
      <xs:element name="Subsystem" type="subsystemcomponents" minOccurs="1"
maxOccurs="100"/>
    </xs:sequence>
    <xs:attribute name="Name" type="xs:string" use="required"/>
  </xs:complexType>
  <xs:complexType name="subsystemcomponents">
    <xs:sequence>
      <xs:element name="Name" type="xs:string"/>
      <xs:element name="Component" type="componentcomponents" minOccurs="1"
maxOccurs="1000"/>
    </xs:sequence>
    <xs:attribute name="ID" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:positiveInteger">
          <xs:minInclusive value="1"/>
          <xs:maxInclusive value="100"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:complexType>
  <xs:complexType name="componentcomponents">
    <xs:sequence>
      <xs:element name="Name" type="xs:string"/>
      <xs:element name="Object" type="objectcomponents" minOccurs="1" maxOccurs="1000"/>
    </xs:sequence>
    <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
  </xs:complexType>
  <xs:complexType name="objectcomponents">
    <xs:choice minOccurs="2" maxOccurs="unbounded">
      <xs:element name="Name" type="xs:string"/>
      <xs:element name="Actuator" type="actuatorcomponents" minOccurs="0" maxOccurs="10"/>
      <xs:element name="Sensor" type="sensorcomponents" minOccurs="0" maxOccurs="10"/>
    </xs:choice>
    <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
  </xs:complexType>
  <xs:complexType name="sensorcomponents">
    <xs:choice minOccurs="1" maxOccurs="4">
      <xs:element name="Type">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="Analog"/>
            <xs:enumeration value="Digital"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="Min" type="xs:integer"/>
      <xs:element name="Max" type="xs:integer"/>
      <xs:element name="Average">
        <xs:complexType>
          <xs:simpleContent>
            <xs:extension base="xs:integer">
              <xs:attribute name="Same" use="required">
                <xs:simpleType>
                  <xs:restriction base="xs:string">
```

```
                <xs:enumeration value="Yes"/>
                <xs:enumeration value="No"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>
  </xs:element>
</xs:choice>
<xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
</xs:complexType>
<xs:complexType name="actuatorcomponents">
<xs:choice minOccurs="1" maxOccurs="2">
  <xs:element name="Type">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="Switch"/>
        <xs:enumeration value="Action"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="Average">
    <xs:complexType>
      <xs:simpleContent>
        <xs:extension base="xs:string">
          <xs:attribute name="Same" use="required">
            <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:enumeration value="Yes"/>
                <xs:enumeration value="No"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>
  </xs:element>
</xs:choice>
<xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
</xs:complexType>
        </xs:schema>
```

Приложение В

XML Schema-файл для XML-файла «идеального» состояния системы

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="System" type="systemcomponents"/>
  <xs:complexType name="systemcomponents">
    <xs:sequence>
      <xs:element name="Subsystem" type="subsystemcomponents" minOccurs="1"
maxOccurs="100"/>
    </xs:sequence>
    <xs:attribute name="Name" type="xs:string" use="required"/>
    <xs:attribute name="DateFrom" type="xs:string" use="required"/>
    <xs:attribute name="DateTo" type="xs:string" use="required"/>
    <xs:attribute name="EverySec" type="xs:positiveInteger" use="required"/>
    <xs:attribute name="Round" type="xs:positiveInteger" use="required"/>
  </xs:complexType>
  <xs:complexType name="subsystemcomponents">
    <xs:sequence>
      <xs:element name="Name" type="xs:string"/>
      <xs:element name="Component" type="componentcomponents" minOccurs="1"
maxOccurs="1000"/>
    </xs:sequence>
    <xs:attribute name="ID" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:positiveInteger">
          <xs:minInclusive value="1"/>
          <xs:maxInclusive value="100"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:complexType>
  <xs:complexType name="componentcomponents">
    <xs:sequence>
      <xs:element name="Name" type="xs:string"/>
      <xs:element name="Object" type="objectcomponents" minOccurs="1" maxOccurs="1000"/>
    </xs:sequence>
    <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
  </xs:complexType>
  <xs:complexType name="objectcomponents">
    <xs:sequence>
      <xs:element name="Name" type="xs:string"/>
      <xs:element name="Sensor" type="sensorcomponents" minOccurs="0" maxOccurs="10"/>
      <xs:element name="Actuator" type="actuatorcomponents" minOccurs="0" maxOccurs="10"/>
    </xs:sequence>
    <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
  </xs:complexType>
  <xs:complexType name="sensorcomponents">
    <xs:sequence>
      <xs:element name="Type">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="Analog"/>
            <xs:enumeration value="Digital"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="Values" type="sensorvaluescomponents"/>
      <xs:element name="Min" type="xs:positiveInteger"/>
      <xs:element name="Max" type="xs:positiveInteger"/>
      <xs:element name="Average">
        <xs:complexType>
```

```
        <xs:simpleContent>
          <xs:extension base="xs:positiveInteger">
            <xs:attribute name="Same" use="required">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="Yes"/>
                  <xs:enumeration value="No"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
  <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
</xs:complexType>
<xs:complexType name="actuatorcomponents">
  <xs:sequence>
    <xs:element name="Type">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Switch"/>
          <xs:enumeration value="Action"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="Values" type="actuatorvaluescomponents"/>
    <xs:element name="Average">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
            <xs:attribute name="Same" use="required">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="Yes"/>
                  <xs:enumeration value="No"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
  <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
</xs:complexType>
<xs:complexType name="actuatorvaluescomponents">
  <xs:sequence>
    <xs:element name="Value">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="actuatorvaluetype">
            <xs:attribute name="DateTime" type="xs:dateTime" use="required"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:simpleType name="actuatorvaluetype">
  <xs:restriction base="xs:string">
    <xs:enumeration value="ON"/>
```

```
    <xs:enumeration value="OFF"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="sensorvaluetype">
  <xs:restriction base="xs:integer"/>
</xs:simpleType>
<xs:complexType name="sensorvaluescomponents">
  <xs:sequence>
    <xs:element name="Value">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="sensorvaluetype">
            <xs:attribute name="DateTime" type="xs:dateTime" use="required"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
        </xs:schema>
```

Приложение Г

XML Schema-файл для XML-файла угроз «умного дома»

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Threats">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Object"  minOccurs="1" maxOccurs="10000">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Sensor"   maxOccurs="1000">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="Condition" minOccurs="1" maxOccurs="1000">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="Threat" type="threatcomponents"  minOccurs="1"
maxOccurs="1000"/>
                        </xs:sequence>
                        <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
                        <xs:attribute name="Type" type="xs:positiveInteger" use="required"/>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
              <xs:element name="Actuator"  maxOccurs="1000">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="Condition" minOccurs="1" maxOccurs="1000">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="Threat" type="threatcomponents"  minOccurs="1"
maxOccurs="1000"/>
                        </xs:sequence>
                        <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
                        <xs:attribute name="Type" type="xs:positiveInteger" use="required"/>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
            <xs:attribute name="Name" type="xs:string" use="required"/>
            <xs:attribute name="SubsystemID" type="xs:positiveInteger" use="required"/>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="threatcomponents">
    <xs:sequence>
      <xs:element name="Consequences" type="consequencescomponents"/>
      <xs:element name="Sources" type="sourcescomponents"/>
      <xs:element name="Causes" type="causescomponents"/>
    </xs:sequence>
    <xs:attribute name="ID" type="xs:positiveInteger" use="required"/>
    <xs:attribute name="Name" type="xs:string" use="required"/>
  </xs:complexType>
  <xs:complexType name="consequencescomponents">
    <xs:sequence>
```

```
    <xs:element name="Consequence" minOccurs="0" maxOccurs="100">
      <xs:complexType mixed="true">
        <xs:attribute name="ID" type="xs:positiveInteger"/>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="sourcescomponents">
  <xs:sequence>
    <xs:element name="Source" minOccurs="0" maxOccurs="100">
      <xs:complexType mixed="true">
        <xs:attribute name="ID" type="xs:positiveInteger"/>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="causescomponents">
  <xs:sequence>
    <xs:element name="Cause" minOccurs="0" maxOccurs="100">
      <xs:complexType mixed="true">
        <xs:attribute name="ID" type="xs:positiveInteger"/>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
        </xs:schema>
```

Приложение Д

Листинг Д.1 – Метод получения «идеального» состояния

```
private void Get_source_usual(bool now, string datefrom, string dateto)
        {
            DateTime d1 = DateTime.Now;//дата и время при нажатии кнопки для получения
идеального состояния
            DateTime current = d1;
            DateTime next;
            DateTime d2 = d1;
            int tm = 0;
            string dates = "";//логи для метода
            string doc_path = "..\\..\\source_usual.xml";
            try
            {
                string system_name = textbox.Text;//данные с формы
                string everysec = textbox1.Text;//
                string round = textbox2.Text;//
                string datefrom_ = datefrom;//дата начала в формате xml
                datefrom_ = datefrom_.Replace(".", ":");
                datefrom_ = datefrom_.Replace(" ", "T");
                string dateto_ = dateto;//дата окончания в формате xml
                dateto_ = dateto_.Replace(".", ":");
                dateto_ = dateto_.Replace(" ", "T");
                int current_it = 0;//номер итерации

                int count = GetCount(datefrom, dateto, everysec);//рассчитываем количество
необходимых итераций
                dates += "count=" + count.ToString() + "\r\n";

                StreamWriter sw = File.CreateText(doc_path);//создаем файл с корневым тегом
и атрибутами
                {
                    sw.WriteLine("<?xml version=\"1.0\" encoding=\"utf-8\"
standalone=\"no\"?>");
                    sw.WriteLine("<System Name=\"" + system_name + "\" DateFrom=\"" +
datefrom_ + "\" DateTo=\"" + dateto_ + "\" EverySec=\"" + everysec + "\" Round=\"" + round +
"\" xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
xsi:noNamespaceSchemaLocation=\"schema source usual.xsd\">");
                    sw.WriteLine("</System>");
                }
                sw.Close();

                string xpath;
                XmlDocument doc = new XmlDocument();
                String condition = null;
                String date = null;
                String time = null;
                String subsystem_id = null;
                String component_id = null;
                String object_id = null;
                String elem_tagname = null;
                String elem_id = null;
                String type = null;
                String value = null;
                String input_path = "";

                if (!now)                               //Ждем начала сбора данных
                {
                    TimeSpan ts = Convert.ToDateTime(datefrom) - d1;
                    tm = Convert.ToInt32(Math.Ceiling(ts.TotalSeconds));
                    tm = tm * 1000;
```

```
                    dates = "wait=" + tm.ToString() + "msec" + "\r\n";
                    System.Threading.Thread.Sleep(tm);
                    dates += "after sleep time is " + DateTime.Now.ToString() + "\r\n";
                }

                while (current_it <= count)//пока текущая итерация меньше количества
запланированных итераций
                {
                    current = DateTime.Now;//текущее время дата
                    next = current.AddSeconds(Convert.ToDouble(everysec));//время дата для
следующей итерации
                    dates += "current_it=" + current_it + "   current=" + current.ToString()
+ ",  next=" + next.ToString() + "\r\n";

                    if (current_it != 0)//если это не первая итерация, то ждем начала
времени этой итерации, если было запущено отложенное получение идеального состояния
                    {
                        TimeSpan ts = next - current;
                        tm = (Convert.ToInt32(Math.Floor(ts.TotalSeconds)) - 2) * 1000;
                        System.Threading.Thread.Sleep(tm);
                        dates += "after sleep " + tm.ToString() + "msec   in  current_it=" +
current_it + ",   time is " + DateTime.Now.ToString() + "\r\n";
                    }

                    current_it++;
                    input_path = GenerateFile();//генерируем файл

                    foreach (string line in File.ReadLines(input_path,
Encoding.UTF8))//разбор файла
                    {
                        if (line[0] != '<')
                        {
                            XmlNode root_for_element = null;
                            XmlNode root_for_object = null;
                            XmlNode root_for_component = null;
                            XmlNode root = null;
                            XmlElement element_for_value = null;
                            doc.Load(doc_path);
                            XDocument xdoc = XDocument.Load(doc_path);
                            int s_id;
                            int c_id;
                            int o_id;
                            int ind;
                            string tmp = "";

                            ind = line.IndexOf("/");
                            date = line.Substring(0, ind);
                            tmp = line.Remove(0, ind + 1);

                            ind = tmp.IndexOf("/");
                            time = tmp.Substring(0, ind);
                            tmp = tmp.Remove(0, ind + 1);

                            ind = tmp.IndexOf("/");
                            subsystem_id = tmp.Substring(0, ind);
                            tmp = tmp.Remove(0, ind + 1);

                            ind = tmp.IndexOf("/");
                            component_id = tmp.Substring(0, ind);
                            tmp = tmp.Remove(0, ind + 1);

                            ind = tmp.IndexOf("/");
                            object_id = tmp.Substring(0, ind);
```

```
                            tmp = tmp.Remove(0, ind + 1);

                            ind = tmp.IndexOf("/");
                            elem_tagname = tmp.Substring(0, ind);
                            if (elem_tagname == "A")
                            { elem_tagname = "Actuator"; }
                            else if (elem_tagname == "S")
                            { elem_tagname = "Sensor"; }
                            tmp = tmp.Remove(0, ind + 1);

                            ind = tmp.IndexOf("/");
                            elem_id = tmp.Substring(0, ind);
                            tmp = tmp.Remove(0, ind + 1);

                            ind = tmp.IndexOf("/");
                            type = tmp.Substring(0, ind);
                            tmp = tmp.Remove(0, ind + 1);

                            value = tmp;

                            s_id = xdoc.Descendants("Subsystem").Where(x =>
x.Attribute("ID").Value == subsystem_id).Count();
                            c_id = xdoc.Descendants("Component").Where(x =>
x.Attribute("ID").Value == component_id).Count();
                            o_id = xdoc.Descendants("Object").Where(x =>
x.Attribute("ID").Value == object_id).Count();


                            if (s_id != 0 && c_id != 0 && o_id != 0)//создание элемента в
существующих подсистеме, объекте и компоненте
                            {
                                condition = "all_old";
                            }
                            else if (s_id == 0)//все новое, такой подсистемы еще нет в файле
                            {
                                condition = "all_new";
                            }
                            else if (s_id != 0 && c_id == 0)//создание нового компонента и
объекта, в существующей подсистеме
                            {
                                condition = "component_new";
                            }
                            else if (s_id != 0 && c_id != 0 && o_id == 0)//создание нового
объекта, в существующем компоненте и подсистеме
                            {
                                condition = "object_new";
                            }

                            switch (condition)
                            {
                                case "1"://////actuator or sensor
                                    {
                                        //добавление нового элемента с одним значением
                                        if (xdoc.Descendants(elem_tagname).Where(x =>
x.Attribute("ID").Value == elem_id).Count() == 0)
                                        {
                                            XmlElement elem =
doc.CreateElement(elem_tagname);

                                            elem.SetAttribute("ID", elem_id);
                                            root_for_element.AppendChild(elem);

                                            XmlElement elem1 = doc.CreateElement("Type");
                                            string type_ = "";
```

```
                                    if (elem_tagname == "Actuator")//actuator
                                    {
                                        type_ = Actuator_types[type];
                                    }
                                    else if (elem_tagname == "Sensor")//sensor
                                    {
                                        type_ = Sensor_types[type];
                                    }
                                    elem1.InnerText = type_;
                                    elem.AppendChild(elem1);

                                    XmlElement elem2 = doc.CreateElement("Values");
                                    elem.AppendChild(elem2);
                                    element_for_value = elem2;

                                    XmlElement elem3 = doc.CreateElement("Value");
                                    elem3.SetAttribute("DateTime", date + "T" +
time);

                                    elem3.InnerText = value;
                                    elem2.AppendChild(elem3);
                                }
                                else //Добавление следующих полученных значений
элемента
                                {
                                    xpath = "System/Subsystem[@ID='" + subsystem_id
+ "']/Component[@ID='" + component_id + "']/Object[@ID='" + object_id + "']/" + elem_tagname
+ "[@ID='" + elem_id + "']/Values";

                                    XmlElement elem4 = doc.CreateElement("Value");
                                    elem4.SetAttribute("DateTime", date + "T" +
time);

                                    elem4.InnerText = value;
                                    doc.SelectSingleNode(xpath).AppendChild(elem4);
                                }
                                doc.Save(doc_path);
                                break;
                            }
                        case "all_old":///подсистема,компонент и объект существуют
                            {
                                xpath = "System/Subsystem[@ID='" + subsystem_id +
"']/Component[@ID='" + component_id + "']/Object[@ID='" + object_id + "']";
                                root_for_element = doc.SelectSingleNode(xpath);
                                goto case "1";
                            }
                        case "object_new":
                            {
                                if (root_for_object == null)//если сюда пришли не из
"component_new", то получаем компонент, в котором будем создавать объект
                                {
                                    xpath = "System/Subsystem[@ID='" + subsystem_id
+ "']/Component[@ID='" + component_id + "']";
                                    root_for_object = doc.SelectSingleNode(xpath);
                                }
                                XmlElement elem0 = doc.CreateElement("Object");
                                elem0.SetAttribute("ID", object_id);
                                root_for_object.AppendChild(elem0);

                                XmlElement elem01 = doc.CreateElement("Name");
                                elem0.AppendChild(elem01);

                                root_for_element = elem0;
                                goto case "1";

                            }
```

```
                                case "component_new":
                                    {
                                        if (root_for_component == null)//если сюда пришли не
из "all_new", то получаем подсистему, в которой будем создавать компонент
                                        {
                                            xpath = "System/Subsystem[@ID='" + subsystem_id
+ "']";
                                            root_for_component =
doc.SelectSingleNode(xpath);
                                        }

                                        XmlElement elem1 = doc.CreateElement("Component");
                                        elem1.SetAttribute("ID", component_id);
                                        root_for_component.AppendChild(elem1);
                                        XmlElement elem11 = doc.CreateElement("Name");
                                        elem1.AppendChild(elem11);
                                        root_for_object = elem1;
                                        goto case "object_new";

                                    }
                                case "all_new":
                                    {
                                        xpath = "System";
                                        root = doc.SelectSingleNode(xpath);
                                        XmlElement elem00 = doc.CreateElement("Subsystem");
                                        elem00.SetAttribute("ID", subsystem_id);
                                        root.AppendChild(elem00);
                                        XmlElement elem001 = doc.CreateElement("Name");
                                        elem00.AppendChild(elem001);
                                        root_for_component = elem00;
                                        goto case "component_new";
                                    }
                            }
                        }

                    }
                }

                d2 = DateTime.Now;
                dates += "after get data time is " + d2.ToString() + "\r\n";
                DeleteGeneratedFiles();//удаляем сгенерированные файлы

                ////////////////////////////////////////
                ////////////////////////////////average

                String average;
                doc.Load(doc_path);
                XDocument xdoc2 = XDocument.Load(doc_path);
                var all_sen = xdoc2.Descendants("Sensor");
                var all_act = xdoc2.Descendants("Actuator");

                foreach (XElement sen in all_sen)
                {
                    var obj = sen.Descendants("Value")
                                .Select(y => Convert.ToInt32(y.Value));//список всех
значений сенсора

                    average = Math.Round(obj.Average(), Convert.ToInt32(round)).ToString();
                    int min = obj.Min();
                    int max = obj.Max();
                    sen.Add(new XElement("Min", min.ToString()));
                    sen.Add(new XElement("Max", max.ToString()));
```

```
                    XElement aver = new XElement("Average", average.ToString());
                    sen.Add(aver);

                    if (min == max)
                    {
                        aver.SetAttributeValue("Same", "Yes");
                    }
                    else
                    {
                        aver.SetAttributeValue("Same", "No");
                    }
                }

                foreach (XElement act in all_act)
                {
                    var obj = act.Descendants("Value")
                                .Select(y => y.Value);//список всех значений активатора

                    int on = 0;
                    bool same = false;
                    string tmp = "";
                    int obj_count = obj.Count();

                    foreach (string val in obj)
                    {
                        if (val == "1")
                        {
                            on++;
                        }
                        tmp = val;
                    }

                    if (on == obj_count || on == 0)
                    {
                        same = true;
                    }


                    XElement aver = new XElement("Average");
                    act.Add(aver);

                    if (same)
                    {
                        aver.SetAttributeValue("Same", "Yes");
                        aver.Value = (tmp == "1") ? "100" : "0";

                    }
                    else
                    {
                        aver.SetAttributeValue("Same", "No");
                        aver.Value = (Math.Round(Convert.ToDecimal(on * 100 /
obj_count))).ToString();
                        //MessageBox.Show( "obj.count=" + obj_count.ToString() + ", on=" +
on + ", aver value="+aver.Value.ToString());
                    }
                }
                xdoc2.Save(doc_path, SaveOptions.None);
            }
            catch (Exception ex)
            {
                MessageBox.Show("Exception in get source_usual.xml=" + ex.Message + "\r\n" +
"Source=" + ex.Source + "\r\n" + "StackTrace=" + ex.StackTrace);
            }
```

```
            finally
            {
                MessageBox.Show("done everything");
                DateTime d3 = DateTime.Now;
                dates += "after all time is " + d3.ToString();
                //MessageBox.Show(dates);
                //MessageBox.Show("d1=" + d1.ToString() + "\r\n" + "current=" +
current.ToString() + "\r\n" + "d2=" + d2.ToString() + "\r\n" + "d3=" + d3.ToString());
            }

                  }
```

Приложение Е

Листинг Е.1 – Метод добавления элемента

```
private void Add()////добавление новых элементов
        {
        try
            {
                bool res_getid = getID();//false - ошибка при получении ID для новых
элементов

                if (res_getid == false || (is_new_component == null || is_new_object == null
|| /*is_sensor*/element_tagname == null ||
                    (is_new_component == true && is_new_object == false) ||
                   subsystem_id == null || subsystem_id == "" ||
                    component_id == null || component_id == "" ||
                    object_id == null || object_id == ""  ||
                    element_id == null || element_id == "" || element_type == null ||
element_type == "" || element_average == null || element_average == ""))
                {
                    MessageBox.Show("Ошибка при добавлении элемента:" + "\r\n" +
                    "тип элемента = " + element_type + "\r\n" +
                    "average = " + element_average);
                }


                else
                {
                    //выражение для корневого элемента - нижний существующий, в который
будет добавляться новый
                    string xpath;
                    string doc_path=file_path;
                    XmlDocument doc = new XmlDocument();

                    String condition=null;
                    XmlNode root_for_element=null;
                    XmlNode root_for_object=null;
                    XmlNode root_for_component = null;
                    XmlNode root=null;

                    if (is_new_component == false && is_new_object == false)//создание
элемента в существующих объекте и компоненте
                    {
                        condition = "all_old";
                        doc.Load(doc_path);
                    }
                    else if (doc.SelectSingleNode("//Subsystem[@ID='" + subsystem_id + "']")
== null)//если нет такой подсистемы
                    {
                        condition = "all_new";
                        if (!File.Exists(file_path))//создание всего, такого файла еще нет
                        {
                            StreamWriter sw = File.CreateText(doc_path);
                            {
                                sw.WriteLine("<?xml version=\"1.0\" encoding=\"utf-8\"
standalone=\"no\"?>");
                                sw.WriteLine("<System Name=\"system_name\"
xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
xsi:noNamespaceSchemaLocation=\"schema source.xsd\">");
                                sw.WriteLine("</System>");
                            }
                            sw.Close();
```

```
                    } doc.Load(doc_path);

                }
                else if (/*is_new_subsystem == false && */is_new_component ==
true)//создание нового компонента, т.е. и нового объекта тоже
                {
                    condition = "component_new";
                    doc.Load(doc_path);
                }
                else if (/*is_new_component == false &&*/ is_new_object ==
true)//создание нового объекта, но в существующем компоненте
                {
                    condition = "object_new";
                    doc.Load(doc_path);
                }



                    switch (condition)
                    {

                        case "1":
                            {
                                //Create a new node - actuator or sensor
                                XmlElement elem = doc.CreateElement(element_tagname);
                                elem.SetAttribute("ID", element_id);
                                //Add the node to the document.
                                root_for_element.AppendChild(elem);

                                XmlElement elem1 = doc.CreateElement("Type");
                                elem1.InnerText = element_type;
                                elem.AppendChild(elem1);

                                XmlElement elem2 = doc.CreateElement("Average");
                                elem2.SetAttribute("Same", "No");
                                elem2.InnerText = element_average;
                                elem.AppendChild(elem2);
                                if (element_tagname == "Sensor")
                                {
                                    XmlElement elem3 = doc.CreateElement("Max");
                                    elem3.InnerText = element_max;
                                    elem.AppendChild(elem3);
                                    XmlElement elem4 = doc.CreateElement("Min");
                                    elem4.InnerText = element_min;
                                    elem.AppendChild(elem4);
                                }
                                doc.Save(doc_path);
                                MessageBox.Show("Готово");
                                break;
                            }
                        case "all_old":
                            {
                                xpath = "//Subsystem[@ID='" + subsystem_id +
"']/Component[@ID='" + component_id + "']/Object[@ID='" + object_id + "']";
                                root_for_element = doc.SelectSingleNode(xpath);
                                goto case "1";
                            }
                        case "object_new":
                            {
                                if (root_for_object == null)//если сюда пришли не из
"component_new", то получаем компонент, в котором будем создавать объект
                                {
```

```
                                        xpath = "//Subsystem[@ID='" + subsystem_id +
"']/Component[@ID='" + component_id + "']";
                                        root_for_object = doc.SelectSingleNode(xpath);
                                    }
                                    XmlElement elem0 = doc.CreateElement("Object");
                                    elem0.SetAttribute("ID", object_id);
                                    root_for_object.AppendChild(elem0);

                                    XmlElement elem01 = doc.CreateElement("Name");
                                    elem01.InnerText = object_name;
                                    elem0.AppendChild(elem01);

                                    root_for_element = elem0;
                                    goto case "1";

                                }
                            case "component_new":
                                {
                                    if (root_for_component == null)//если сюда пришли не из
"all_new", то получаем подсистему, в которой будем создавать компонент
                                    {
                                        xpath = "//Subsystem[@ID='" + subsystem_id + "']";
                                        root_for_component = doc.SelectSingleNode(xpath);
                                    }
                                    XmlElement elem000 = doc.CreateElement("Component");
                                    elem000.SetAttribute("ID", component_id);
                                    root_for_component.AppendChild(elem000);
                                    XmlElement elem0001 = doc.CreateElement("Name");
                                    elem0001.InnerText = component_name;
                                    elem000.AppendChild(elem0001);

                                    root_for_object = elem000;
                                    goto case "object_new";

                                }
                            case "all_new":
                                {
                                    xpath = "System";
                                    root = doc.SelectSingleNode(xpath);

                                    XmlElement elem00 = doc.CreateElement("Subsystem");
                                    elem00.SetAttribute("ID", subsystem_id);
                                    root.AppendChild(elem00);
                                    XmlElement elem001 = doc.CreateElement("Name");
                                    elem001.InnerText = subsystem_name;
                                    elem00.AppendChild(elem001);

                                    root_for_component = elem00;
                                    goto case "component_new";
                                }
                        }

                    }
                this.Close();

            }
             catch (Exception ee)
             {
                 MessageBox.Show("Ошибка добавления: "+"\r\n" +
ee.Message+"\r\n"+ee.StackTrace+"\r\n"+ee.Source);
             }
                   }
```

Приложение Ж

Листинг Ж.1 – Метод мониторинга данных

```
private static void Monitoring()//поток для мониторинга данных в data.txt
        {
                string data = generated_files[0];
                int error = 0;//код ошибки=номеру данных или =100, если не совпадает
количество элементов в файле
                string tmp = "";//временная переменная для хранения отдельных данных из
строки
                int tmp_num = 1;//номер данных: 1-date, 2-time, 3-id subsystem, 4-id
component, 5-id object, 6-element(S or A), 7-id element, 8-element type, 9-element value
                int row = -1;//индекс строки
                int c_ind = -1;//индекс символа в строке
                string elemtagname="";//A-активатор или S-сенсор
                string elemid = "";//id элемента для проверки типа элемента
                string xpath = "";//путь для проверки вложенности
                var file = File.ReadAllLines(data);
                List<string> list1 = new List<string>(file);

                if (list1.Count != elements_count)//если не совпадает количество элементов
                {
                    error = 100;
                    WriteLog(error, -1, data);
                    int ind = 0;
                    string subsystem_id;
                    string component_id;
                    string object_id;
                    string s_id;
                    string a_id;
                    string tag;
                    //списки с элементами системы, определенными в составе системы
                    List<string> act_source = Actuators_in_source;
                    List<string> sen_source = Sensors_in_source;
                    List<string> sub_source = Subsystems_in_source;
                    List<string> com_source = Components_in_source;
                    List<string> obj_source = Objects_in_source;
                    /////
                    //проверяем кол-во подсистем (количественный анализ данных)
                    foreach (string str in list1)
                    {
                        tmp = "";
                        ind = str.IndexOf("/");
                        tmp = str.Remove(0, ind + 1);//delete date
                        ind = tmp.IndexOf("/");
                        tmp = tmp.Remove(0, ind + 1);//delete time
                        ind = tmp.IndexOf("/");
                        subsystem_id = tmp.Substring(0, ind);//subsystem id
                        tmp = tmp.Remove(0, ind + 1);//delete subsystem id
                        ind = tmp.IndexOf("/");
                        component_id = tmp.Substring(0, ind);//component_id
                        tmp = tmp.Remove(0, ind + 1);
                        ind = tmp.IndexOf("/");
                        object_id = tmp.Substring(0, ind);//object_id
                        tmp = tmp.Remove(0, ind + 1);
                        ind = tmp.IndexOf("/");
                        tag = tmp.Substring(0, ind);
                        if (tag == "A")
                        {
                            tmp = tmp.Remove(0, ind + 1);
                            ind = tmp.IndexOf("/");
                            a_id = tmp.Substring(0, ind);
```

```
                        tmp = tmp.Remove(0, ind + 1);
                        act_source.Remove(a_id);
                    }
                    else
                    {
                        tmp = tmp.Remove(0, ind + 1);
                        ind = tmp.IndexOf("/");
                        s_id = tmp.Substring(0, ind);
                        tmp = tmp.Remove(0, ind + 1);
                        sen_source.Remove(s_id);
                    }
                    sub_source.Remove(subsystem_id);
                    sub_source.Remove(component_id);
                    obj_source.Remove(object_id);
                }
                if (sub_source.Count > 0)
                {
                    foreach (string s in sub_source)
                    {
                        WriteLog(103, -1, data, Convert.ToInt32(s));//запись ошибки в
лог
                    }
                }
                ///////Проверяем количество компонентов//
                else
                {
                    if (com_source.Count > 0)
                    {
                        foreach (string s in com_source)
                        {
                            WriteLog(104, -1, data, Convert.ToInt32(s));//запись ошибки
в лог
                        }
                    }
                    else///////Проверяем количество objects//
                    {
                        if (obj_source.Count > 0)
                        {
                            foreach (string s in obj_source)
                            {
                                WriteLog(105, -1, data, Convert.ToInt32(s));
                            }
                        }
                        else//////Actuators and Sensors
                        {
                            if (act_source.Count > 0)
                            {
                                foreach (string s in act_source)
                                {
                                    WriteLog(1072, -1, data, Convert.ToInt32(s));
                                    int th_id = GetThreatID("Actuator",s,100);
                                    Bad_actuators.Add(Convert.ToInt32(s),
Get_threat_info(th_id, 1072, data.Substring(10, 15)));//добавляем в список активаторов с
угрозами
                                }
                            }
                            if (sen_source.Count > 0)
                            {
                                foreach (string s in sen_source)
                                {
                                    WriteLog(1071, -1, data, Convert.ToInt32(s));
                                    int th_id = GetThreatID("Sensor",s,100);
```

```
                                        Bad_sensors.Add(Convert.ToInt32(s),
Get_threat_info(th_id, 1071, data.Substring(10,15)));//добавляем в список сенсоров с
угрозами
                                    }
                                }
                            }
                        }
                    }
                }

                else
                {
                    foreach (string str in list1)
                    {
                        error = 0;
                        tmp = "";
                        tmp_num = 1;
                        c_ind = -1;
                        elemtagname = "";
                        elemid = "";
                        row++;
                        xpath = "";

                        foreach (char c in str)
                        {
                            c_ind++;

                            if (!c.Equals('/'))
                            {
                                tmp += c;
                            }
                            if (c.Equals('/') || c_ind == str.Length - 1)
                            {
                                switch (tmp_num)
                                {
                                    case 6:
                                        elemtagname = tmp;
                                        break;
                                    case 3:
                                        xpath += "//Subsystem[@ID='" + tmp + "']";
                                        break;
                                    case 4:
                                        xpath += "//Component[@ID='" + tmp + "']";
                                        break;
                                    case 5:
                                        xpath += "//Object[@ID='" + tmp + "']";
                                        break;
                                    case 7:
                                        elemid = tmp;
                                        break;
                                }
                                error = CheckDataStructure(tmp_num, tmp);//проверяем
правильность структуры каждой строки в полученных данных
                                if (error != 0)//ошибка в структуре полученных данных
                                {
                                    WriteLog(error, row, data);
                                }
                                else if (tmp_num == 3 || tmp_num == 4 || tmp_num == 5 ||
tmp_num == 7 || tmp_num == 8 || tmp_num == 9)//нет ошибки в структуре, проверяем состав
                                {
                                    if (tmp_num != 9)//если это не данные с элемента, а id-
ки
                                    {
```

```
                                        error = CheckSystemStructure(tmp_num, tmp,
elemtagname, elemid, xpath);//проверяем совпадает ли состав системы
                                    }
                                    if (error != 0)//ошибка в составе
                                    {
                                        WriteLog(error, row, data);
                                    }
                                    else if (error == 0 && tmp_num == 9)//если это данные с
элемента
                                    {
                                        error = CheckValue(tmp, elemtagname,
elemid);//проверяем данные элемента на соответсвие ограничениям//метод возвращает
%отклонения или 0
                                        if (error != -1)//ошибка в данных элемента
                                        {
                                            if (elemtagname == "S")
                                            {
                                                WriteLog(99, row, data,
Convert.ToInt32(elemid));
                                                error = GetThreatID(elemtagname, elemid,
error);//threat id
                                                if
(Bad_sensors.ContainsKey(Convert.ToInt32(elemid)))
                                                {

Bad_sensors.Remove(Convert.ToInt32(elemid));
                                                }
                                                Bad_sensors.Add(Convert.ToInt32(elemid),
Get_threat_info(error, 99, data.Substring(10,15)));//добавляем в список сенсоров с угрозами
                                            }
                                            if (elemtagname == "A")//actuator
                                            {
                                                error = GetThreatID(elemtagname, elemid,
error);//threat id
                                            }
                                            if (error != -1)//если найдена угроза
                                            {
                                                WriteLog(error, -1, "",
Convert.ToInt32(elemid));
                                            }
                                        }
                                        else//если нет ошибок в данных
                                        {
                                            File.Delete(data);//удаляем файл
                                        }
                                    }
                                }
                                tmp = "";
                                tmp_num++;
                            }
                        }
                    }
                }
                generated_files.RemoveAt(0);
                if (Bad_actuators.Count != 0 || Bad_sensors.Count != 0)
                {
                    //updatetable();
                    Write_dictionary_to_list();
                    Bad_sensors.Clear();
                    Bad_actuators.Clear();
                }

                }
```