TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа – Инженерная школа информационных технологий и робототехники
Направление подготовки – 15.03.04 «Автоматизация технологических процессов и производств»
Отделение школы (НОЦ) – Отделение автоматизации и робототехники

БАКАЛАВРСКАЯ РАБОТА

Тема работы
Устройство обнаружения и предотвращения вторжений в сетях MODBUS

УДК 004.73.056.5

Студент

Группа	ФИО	Подпись	Дата
8Т8Б	Калинкин Ян Васильевич		

Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Зебзеев А.Г.	к.т.н.		

Со-руководитель (по разделу «Концепция стартап-проекта»)

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ШИП	Горюнова Н.Н.	к.э.н.		

КОНСУЛЬТАНТЫ:

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель ООД ШБИП	Мезенцева И.Л.	–		

Нормоконтроль

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Кузьминская Е.В.	к.т.н.		

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель ООП	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Громаков Е.И.	к.т.н.		

Томск – 2022 г.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ООП

Код компетенции	Наименование компетенции
Универсальные компетенции	
УК(У)-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК(У)-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
УК(У)-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде
УК(У)-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(-ых) языке(-ах)
УК(У)-5	Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах.
УК(У)-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
УК(У)-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности
УК(У)-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной дея-тельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
УК(У)-9	Способен проявлять предприимчивость в практической деятельности, в т.ч. в рамках разработки коммерчески перспективного продукта на основе научно-технической идеи
УК(У)-10	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
УК(У)-11	Способен формировать нетерпимое отношение к коррупционному поведению
Общепрофессиональные компетенции	
ОПК(У)-1	Способен использовать основные закономерности, действующие в процессе изготовления продукции требуемого качества, заданного количества при наименьших затратах общественного труда
ОПК(У)-2	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК(У)-3	Способен использовать современные информационные технологии, технику, прикладные программные средства при решении задач профессиональной деятельности
ОПК(У)-4	Способен участвовать в разработке обобщенных вариантов решения проблем, связанных с автоматизацией производств, выборе на основе

Код компетенции	Наименование компетенции
	анализа вариантов оптимального прогнозирования последствий решения
ОПК(У)-5	Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью
Профессиональные компетенции	
ПК(У)-1	Способен собирать и анализировать исходные информационные данные для проектирования технологических процессов изготовления продукции, средств и систем автоматизации, контроля, технологического оснащения, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством; участвовать в работах по расчету и проектированию процессов изготовления продукции и указанных средств и систем с использованием современных информационных технологий, методов и средств проектирования
ПК(У)-2	Способен выбирать основные и вспомогательные материалы для изготовления изделий, способы реализации основных технологических процессов, аналитические и численные методы при разработке их математических моделей, методы стандартных испытаний по определению физико-механических свойств и технологических показателей материалов и готовых изделий, стандартные методы их проектирования, прогрессивные методы эксплуатации изделий
ПК(У)-3	Готов применять способы рационального использования сырьевых, энергетических и других видов ресурсов, современные методы разработки малоотходных, энергосберегающих и экологически чистых технологий, средства автоматизации технологических процессов и производств
ПК(У)-4	Способен участвовать в постановке целей проекта (программы), его задач при заданных критериях, целевых функциях, ограничениях, разработке структуры его взаимосвязей, определении приоритетов решения задач с учетом правовых и нравственных аспектов профессиональной деятельности, в разработке проектов изделий с учетом технологических, конструкторских, эксплуатационных, эстетических, экономических и управленческих параметров, в разработке проектов модернизации действующих производств, создании новых, в разработке средств и систем автоматизации, контроля, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством в соответствии с техническими заданиями и использованием стандартных средств автоматизации расчетов и проектирования
ПК(У)-5	Способен участвовать в разработке (на основе действующих стандартов и другой нормативной документации) проектной и рабочей технической документации в области автоматизации технологических процессов и производств, их эксплуатационному обслуживанию, управлению жизненным циклом продукции и ее качеством, в мероприятиях по контролю соответствия разрабатываемых проектов и технической документации действующим стандартам, техническим условиям и другим нормативным документам

Код компетенции	Наименование компетенции
ПК(У)-6	Способен проводить диагностику состояния и динамики производственных объектов производств с использованием необходимых методов и средств анализа
ПК(У)-7	Способен участвовать в разработке проектов по автоматизации производственных и технологических процессов, технических средств и систем автоматизации, контроля, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством, в практическом освоении и совершенствовании данных процессов, средств и систем
ПК(У)-8	Способен выполнять работы по автоматизации технологических процессов и производств, их обеспечению средствами автоматизации и управления, готовностью использовать современные методы и средства автоматизации, контроля, диагностики, испытаний и управления процессами, жизненным циклом продукции и ее качеством
ПК(У)-9	Способен определять номенклатуру параметров продукции и технологических процессов ее изготовления, подлежащих контролю и измерению, устанавливать оптимальные нормы точности продукции, измерений и достоверности контроля, разрабатывать локальные поверочные схемы и выполнять проверку и отладку систем и средств автоматизации технологических процессов, контроля, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством, а также их ремонт и выбор; осваивать средства обеспечения автоматизации и управления
ПК(У)-10	Способен проводить оценку уровня брака продукции, анализировать причины его появления, разрабатывать мероприятия по его предупреждению и устранению, по совершенствованию продукции, технологических процессов, средств автоматизации и управления процессами, жизненным циклом продукции и ее качеством, систем экологического менеджмента предприятия, по сертификации продукции, процессов, средств автоматизации и управления
ПК(У)-11	Способен участвовать: в разработке планов, программ, методик, связанных с автоматизацией технологических процессов и производств, управлением процессами, жизненным циклом продукции и ее качеством, инструкций по эксплуатации оборудования, средств и систем автоматизации, управления и сертификации и другой текстовой документации, входящей в конструкторскую и технологическую документацию, в работах по экспертизе технической документации, надзору и контролю за состоянием технологических процессов, систем, средств автоматизации и управления, оборудования, выявлению их резервов, определению причин недостатков и возникающих неисправностей при эксплуатации, принятию мер по их устранению и повышению эффективности использования
ПК(У)-18	Способен аккумулировать научно-техническую информацию, отечественный и зарубежный опыт в области автоматизации технологических процессов и производств, автоматизированного управления жизненным циклом продукции, компьютерных систем управления ее качеством,
ПК(У)-19	Способен участвовать в работах по моделированию продукции, технологических процессов, производств, средств и систем

Код компетенции	Наименование компетенции
	автоматизации, контроля, диагностики, испытаний и управления процессами, жизненным циклом продукции и ее качеством с использованием современных средств автоматизированного проектирования, по разработке алгоритмического и программного обеспечения средств и систем автоматизации и управления процессами
ПК(У)-20	Способен проводить эксперименты по заданным методикам с обработкой и анализом их результатов, составлять описания выполненных исследований и подготавливать данные для разработки научных обзоров и публикаций
ПК(У)-21	Способен составлять научные отчеты по выполненному заданию и участвовать во внедрении результатов исследований и разработок в области автоматизации технологических процессов и производств, автоматизированного управления жизненным циклом продукции и ее качеством
ПК(У)-22	Способен участвовать: в разработке программ учебных дисциплин и курсов на основе изучения научной, технической и научно-методической литературы, а также собственных результатов исследований; в постановке и модернизации отдельных лабораторных работ и практикумов по дисциплинам профилей направления; способностью проводить отдельные виды аудиторных учебных занятий (лабораторные и практические), применять новые образовательные технологии, включая системы компьютерного и дистанционного обучения

TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа – Инженерная школа информационных технологий и робототехники
Направление подготовки – 15.03.04 Автоматизация технологических процессов и производств
Отделение школы (НОЦ) – Отделение автоматизации и робототехники

УТВЕРЖДАЮ:
Руководитель ООП

_____ _____ _____
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Бакалаврской работы

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

Студенту:

Группа	**ФИО**
8Т8Б	Калинкину Яну Васильевичу

Тема работы:

Устройство обнаружения и предотвращения вторжений в сетях MODBUS	
Утверждена приказом директора (дата, номер)	№47-13/с от 16.02.22

Срок сдачи студентом выполненной работы:	04.06.2022

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.).*	Объект исследования: устройство для обнаружения и предотвращения вторжений в сетях Modbus на базе микроконтроллера Цель работы: разработка, исследование и тестирование алгоритма анализа сетевого трафика Modbus устройством на базе микроконтроллера

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).*	Анализ предметной области; Сравнительный анализ рынка СЗИ АСУ ТП; Подбор элементной базы; Составление алгоритма работы устройства; Разработка программной реализации алгоритма.
Перечень графического материала *(с точным указанием обязательных чертежей)*	Код программного обеспечения Принципиальная электрическая схема Презентация в формате *.pptx

Консультанты по разделам выпускной квалификационной работы
(с указанием разделов)

Раздел	Консультант
Концепция стартап-проекта	Горюнова Наталия Николаевна
Социальная ответственность	Мезенцева Ирина Леонидовна

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

Заключение (Conclusion)

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	16.02.2022

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель ОАР ИШИТР	Тутов И. А.	–		16.02.2022

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8Т8Б	Калинкин Ян Васильевич		16.02.2022

TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа – Инженерная школа информационных технологий и робототехники
Направление подготовки – 15.03.04 «Автоматизация технологических процессов и производств»
Уровень образования – Бакалавриат
Отделение школы (НОЦ) – Отделение автоматизации и робототехники
Период выполнения – Весенний семестр 2021/2022 учебного года

Форма представления работы:

Бакалаврская работа

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	04.06.2022

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
	Основная часть	60
	Концепция стартап-проекта	20
	Социальная ответственность	20

СОСТАВИЛ:
Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Зебзеев А. Г.	к.т.н.		

Консультант (при наличии)

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель ОАР ИШИТР	Тутов И. А.	–		

СОГЛАСОВАНО:

Руководитель ООП

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОАР ИШИТР	Громаков Е. И.	к.т.н.		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«КОНЦЕПЦИЯ СТАРТАП-ПРОЕКТА»

Студенту:

Группа	ФИО
8Т8Б	Калинкину Яну Васильевичу

Школа	ИШИТР	Направление	15.03.04 «Автоматизация технологических процессов и производств»
Уровень образования	Бакалавр		

Перечень вопросов, подлежащих разработке:	
Проблема конечного потребителя, которую решает продукт, который создается в результате выполнения НИОКР (функциональное назначение, основные потребительские качества)	Повышение защищенности АСУ ТП от несанкционированного доступа
Способы защиты интеллектуальной собственности	Государственная регистрация программы для ЭВМ
Объем и емкость рынка	Объем рынка России: 2,054 млрд. руб.
Современное состояние и перспективы отрасли, к которой принадлежит представленный в ВКР продукт	Повышение спроса на СЗИ, снабжение КИИ средствами отечественного производства, повышение количества кибератак на АСУ из Интернета
Себестоимость продукта	20,69 тыс. руб.
Конкурентные преимущества создаваемого продукта	Защита технологических сетей на физическом уровне при отсутствии аналогичных средств
Сравнение технико-экономических характеристик продукта с отечественными и мировыми аналогами	На основании конкурентных преимуществ
Целевые сегменты потребителей создаваемого продукта	Любые АСУ с дистанционной передачей информации
Бизнес-модель проекта	Модель по А. Остервальдеру и И. Пинье
Производственный план	Увеличивающийся, начиная с 100 устройств в первый год
План продаж	Исходя из наценки в 100%
Перечень графического материала:	
При необходимости представить эскизные графические материалы(например, бизнес-модель)	Модель по А. Остервальдеру и И. Пинье, таблицы расчета бюджета проекта

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант по разделу «Концепция стартап-проекта» (со-руководитель ВКР):

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ШИП	Горюнова Наталия Николаевна	к.э.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8Т8Б	Калинкин Ян Васильевич		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО		
8Т8Б	Калинкину Яну Васильевичу		
Школа	**ИШИТР**	**Отделение (НОЦ)**	**Отделение автоматизации и робототехники**
Уровень образования	**Бакалавриат**	**Направление/ специальность**	**15.03.04 Автоматизация технологических процессов и производств**

Тема ВКР:

Устройство обнаружения и предотвращения вторжений в сетях MODBUS	
Исходные данные к разделу «Социальная ответственность»:	
Введение – Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика) и области его применения. – Описание рабочей зоны (рабочего места) при разработке проектного решения	Объект исследования: устройство для отслеживания и предотвращения вторжений в промышленных сетях MODBUS RTU на базе микроконтроллера, являющееся компонентом информационной безопасности контроллерного оборудования Область применения: информационная безопасность АСУ ТП, автоматизированные информационно-управляющие системы, локальные системы управления в энергетике, ЖКХ, нефтегазовой отрасли Рабочая зона: лаборатория Размеры помещения (климатическая зона*): 6*8 м. Количество и наименование оборудования рабочей зоны: персональный компьютер, отладочная плата с микроконтроллером, Ethernet-кабель, USB-кабель. Рабочие процессы, связанные с объектом исследования, осуществляющиеся в рабочей зоне: тестирование работоспособности устройства на монтажной плате, исследование эффективности устройства при реализации протоколов межмашинного взаимодействия, разработка дополнительных программных модулей.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Правовые и организационные вопросы обеспечения безопасности при разработке проектного решения – специальные (характерные при эксплуатации объекта исследования, проектируемой рабочей зоны) правовые нормы трудового законодательства; – организационные мероприятия при компоновке рабочей зоны.	Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 25.02.2022); ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования; ГОСТ 12.2.033-78 ССБТ. Рабочее место при выполнении работ стоя. Общие эргономические требования.
2. Производственная безопасность при разработке проектного решения: – Анализ выявленных вредных и опасных производственных факторов	**Вредные факторы:** 1. Отсутствие или недостатки необходимого искусственного освещения; 2. Физические статические перегрузки, связанные с рабочей позой; 3. Умственное перенапряжение, в том числе вызванное информационной нагрузкой; 4. Опасные и вредные производственные факторы, связанные с аномальными микроклиматическими

	параметрами воздушной среды на местонахождении работающего. **Опасные факторы:** 1. Опасные и вредные производственные факторы, связанные с электрическим током, вызываемым разницей электрических потенциалов, под действие которого попадает работающий. **Требуемые средства коллективной и индивидуальной защиты от выявленных факторов:** средства защиты от поражения электрическим током (предохранительные устройства, устройства автоматического отключения, контроля и сигнализации), осветительные приборы и искусственные источники света, устройства для кондиционирования воздуха и отопления, обогрева и охлаждения.
3. Экологическая безопасность при разработке проектного решения:	**Воздействие на селитебную зону:** попадание фракций электронных компонентов на территорию жилых и общественных помещений; **Воздействие на литосферу:** утилизация отходов при производстве составных элементов прибора; **Воздействие на гидросферу:** возможное попадание отходов производства компонентов в сточные воды; **Воздействие на атмосферу:** выбросы при производстве компонентов устройства.
4. Безопасность в чрезвычайных ситуациях при разработке проектного решения:	**Возможные ЧС**: ЧС техногенного характера: пожар, взрыв. **Наиболее типичная ЧС**: Пожар.
Дата выдачи задания для раздела по линейному графику	11.04.2022

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель ООД	Мезенцева Ирина Леонидовна	–		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8Т8Б	Калинкин Ян Васильевич		

Реферат

Выпускная квалификационная работа содержит 92 страницы, 18 рисунков, 14 таблиц, 53 источника, 4 приложения на 11 страницах.

Ключевые слова: информационная безопасность, кибератака, микроконтроллер, коммуникационный протокол, алгоритм.

Цель данной работы – разработка устройства для повышения степени защищенности сегментов сетей АСУ ТП, использующих коммуникационный протокол Modbus RTU. Предполагается программная реализация алгоритма анализа трафика на основе микроконтроллера и дальнейшее тестирование.

В рамках работы были разработаны структурная схема расположения устройства в сегменте технологической сети, программное обеспечение для микроконтроллера. Произведен подбор элементной базы для реализации устройства, разработана принципиальная электрическая схема подключений компонентов устройства. Разработанный алгоритм проверен на отладочной плате при симуляции трафика Modbus RTU.

В результате работы разработан первоначальный проектно-модифицируемый алгоритм анализа сетевого трафика Modbus RTU, отслеживающий и блокирующий несанкционированные запросы в сегменте технологической сети.

Область применения: промышленные предприятия, использующие точки удаленного доступа в составе АСУ ТП для дистанционной передачи информации.

Значимость работы заключается в оригинальности алгоритма анализа сетевого трафика и отсутствии прямых аналогов устройства на рынке средств защиты информации АСУ ТП.

В дальнейшем возможна модернизация устройства для работы с другими реализациями коммуникационного протокола путем добавления интерфейсных микросхем и использования более мощного микроконтроллера, а также доработкой алгоритма.

Оглавление

Обозначения и сокращения

В настоящей работе употреблены следующие обозначения и сокращения:

АСУ ТП – автоматизированная система управления технологическим процессом;

ИБ – информационная безопасность;

КИИ – критическая информационная инфраструктура;

ЛСУ – локальная система управления;

МК – микроконтроллер;

ПАК – программно-аппаратный комплекс;

ПЗУ – постоянное запоминающее устройство;

ПК – персональный компьютер;

ПЛК – программируемый логический контроллер;

ПО – программное обеспечение;

СЗИ – средства защиты информации;

УАПП – универсальный асинхронный приемопередатчик;

Введение

Управление технологическими процессами в наше время все чаще осуществляется при использовании АСУ ТП. Использование автоматизированных систем управления предполагает создание сложных технологических сетей с постоянным переносом информации. Каждый сегмент технологической сети имеет свое назначение, обрабатывает адресованный ему трафик и формирует ответные потоки информации. Для управления отдельными технологическими процессами часто формируются ЛСУ. Из таких систем полностью исключено человеческое присутствие и для принятия решений касательно регулирования, стабилизации и передачи информации о технологических параметрах не требуется вмешательство оператора. Все, что требуется для осуществления функционирования таких систем – электроэнергия и получаемые из других сегментов сети предприятия по определенному коммуникационному протоколу управляющие сигналы.

Для получения и обработки управляющих сигналов используются ПЛК или программируемые реле. Взаимодействие с контроллерным оборудованием может осуществляться посредством физического (RS-232, RS-485, Ethernet и т.д.) или беспроводного интерфейса (Wi-Fi, ZigBee и т.д.) с использованием модулей приема-передачи соответствующего формата [1, 2]. Для формирования сообщений существует многообразие протоколов взаимодействия – Modbus, Profibus, Foundation Fieldbus и т.д. [3].

Каждая АСУ, использующая удаленные точки доступа и беспроводные подключения, имеет уязвимость при удаленном управлении, и не всегда на рынке присутствуют СЗИ, которые в полной мере обеспечили бы защиту комплекса.

Целью данной работы является изучение современного рынка СЗИ, концепций ИБ АСУ ТП, а также реализация устройства, повышающего степень защищенности ЛСУ, использующих удаленные точки доступа при обработке промышленных протоколов взаимодействия, примером которого в данной работе является Modbus RTU.

1 Актуальность работы

Несмотря на удобство и практичность, АСУ, организованные с использованием удаленной передачи данных и массовыми протоколами взаимодействия, являются уязвимыми для направленных кибератак. Так, в 2021 г. эксперты InfoWatch ARMA выяснили, что более 4000 объектов АСУ ТП доступны через Интернет и, как следствие уязвимы для удаленных атак, при этом более 700 объектов имеют критические уязвимости [4]. «Лабораторией Касперского» были определены отдельные типы кибератак и уязвимостей, которые могут быть проэксплуатированы удаленно [5]. Также отдельно стоит выделить подтвержденные вендором критическую уязвимость коммуникационного протокола Modbus при осуществлении удаленного доступа [6]. Данная уязвимость требует отдельных организационных мер для устранения, например, использование сторонних средств межсетевого экранирования и контроля удаленного доступа.

Кроме того, экспертами InfoWatch ARMA было обнаружено, что уязвимые при использовании удаленного доступа объекты АСУ ТП часто используются в КИИ [4]. Дополнительную статистику предоставляет «Лаборатория Касперского», в соответствии с которой в 2021 г. в Российской Федерации 42,27% компьютеров АСУ были зафиксированы атаки вредоносным ПО, причем вредоносное воздействие было успешно заблокировано только на 21,40% устройств. Данный показатель является максимальным на 2021 г. в РФ, к концу года он упал более чем в два раза. В 28,67% случаев вредоносной активности ее источников являлся Интернет [7].

В целом, по заключению директора экспертного центра по промышленной кибербезопасности Антона Шипулина, уровень защиты промышленных предприятий и критической инфраструктуры в стране недостаточен, особенно с учетом того, что многие предприятия не стремятся присваивать своему объекту высокую категорию важности для настройки системы информационной безопасности и разделения производственного и офисного сегментов сети предприятия из-за значительных затрат [8]. При

увеличении количества вредоносных атак на АСУ ТП приведенная статистика становится еще более критичной [9].

Кроме того, выбор средств ИБ АСУ ТП, по убеждению многих специалистов АСУ ТП, недостаточно велик и рынок не всегда может предоставить потребителю удовлетворяющий его требованиям продукт. Кроме того, не всегда удается установить контакт с внешним поставщиком СЗИ [10].

При наличии активных уязвимостей технологических сетей, увеличении количества кибератак на АСУ ТП, малой насыщенности рынка средств ИБ АСУ ТП специалисты исследовательской компании MarketsanMarkets прогнозируют рост рынка средств ИБ до $22,5 млрд к 2025 г. [11].

Таким образом, вопрос ИБ АСУ ТП актуален и критически важен.

В связи с этим отдельными группами специалистов проводятся исследования и разработки новых методик и продуктов защиты информационной безопасности АСУ ТП. Компания Gartner предоставила концепцию адаптивной защиты, которая подразумевает следующие этапы: прогнозирование (Predict), предотвращение (Prevent), обнаружение (Detect) и реагирование (Respond). В соответствии с этой концепцией, эффективная система защиты должно динамически подстраиваться под существующие риски, предотвращать возможные угрозы, обнаруживать существующие аномалии сетевой инфраструктуры и выполнять все необходимые для нейтрализации кибератаки процессы [12].

Также в 2021 г. специалистами InfoWatch были рассмотрены тренды защиты информации в АСУ ТП: эшелонированная защита, безопасная программная среда и централизованное управления системой защиты и расследование инцидентов ИБ. Наиболее комплексным с прикладной точки зрения является тренд эшелонированной защиты – сегментирование корпоративной и технологической подсетей и отдельная защита рабочих станций и объектов АСУ ТП [13].

В связи с вышеперечисленными положениями, была предложена концепция устройства, напрямую осуществляющего анализ запросов,

направляемых к ПЛК, с целью обнаружения вредоносной активности, и автоматически выполняющего процессы блокировки вредоносных запросов и уведомления обслуживающего персонала о произошедшем событии. Таким образом, данное устройство должно осуществлять прямой контроль и анализ сетевого трафика, ввода в машинные носители информации, контроллерное оборудование и информационную сеть в совокупности, увеличивая степень ее защищенности. В соответствии с приказами ФСТЭК №31 от 14 марта 2014 г. и ФСТЭК №239 от 25 декабря 2017 г. такое устройство может быть использовано при организации АСУ 1 класса защищенности и 1 класса категории значимости [14, 15].

2 Проектирование устройства

2.1 Сравнительный анализ существующих решений

Несмотря на то, что не всегда продукты, представленные на рынке СЗИ АСУ ТП, соответствуют требованиям потребителя, и рынок в принципе недостаточно насыщен, различные вендоры предоставляют свои разработки, которые находят применение в АСУ ТП различных отраслей промышленности и КИИ.

Специалисты ресурса ANTI-MALWARE предоставили масштабные обзоры наложенных и встроенных средств защиты АСУ ТП [12, 16].

Наложенные СЗИ – средства, которые устанавливаются для защиты уже организованной системы без предварительной интеграции, в то время как встроенные СЗИ могут поставляться с компонентами организуемой АСУ ТП для интеграции в нее. Исходя из этого, встроенные и наложенные СЗИ могут выполнять разные функции, поскольку наложенные средства являют собой в основном более комплексные решения, отдельно предоставляемые вендорами СЗИ – средства для сегментирования подсетей, антивирусное ПО, системы авторизации и пр., а встроенные СЗИ нацелены на ведение журналов событий, шифрование протоколов и контроль конфигурации АСУ ТП.

Указанные выше особенности наложенных и встроенных СЗИ дают основание для отдельного сравнения продуктов на рынке средств ИБ. Будут рассмотрены такие разработчики СЗИ на отечественном рынке, как «АПРОТЕХ», «Информационные системы и стратегии», «Физприбор», «Лаборатория Касперского», «Positive Technologies» и т.д.

В таблицах 1 и 2 приведен сравнительный анализ некоторых средств ИБ АСУ ТП.

Таблица 1 – Сравнительный анализ наложенных СЗИ

	Kaspersky Industrial CyberSecurity (KICS)	PT Industrial Security Incident Manager (PT ISIM)	DATAPK
Принцип работы с сетевым трафиком	Работа с копией трафика (SPAN)	Работа с копией трафика (SPAN, TAP)	Активный и пассивный режимы работы с трафиком
Наличие контроля сетевого трафика	Неинтрузивный контроль трафика, отслеживание передаваемых запросов	Контроль эксплуатации уязвимостей, фактов неавторизованного управления	Алгоритм блокировки неодобренных потоков
Контроль удаленных подключений	Контроль беспроводных подключений (KICS for Nodes)	Контроль действий удаленных пользователей	Не уточняется
Защита от вредоносных программ	Обеспечение защиты от вредоносных программ (KICS for Nodes)	Выявление уязвимостей, эксплуатируемых вредоносным ПО	Не уточняется
Поддержка протокола Modbus	Modbus TCP (KICS for Networks)	Modbus TCP	Modbus RTU/TCP в режиме индикации, Modbus TCP в режиме сбора данных
Осуществление контроля действия персонала	Контроль действий пользователя (KICS for Nodes)	Не уточняется	Контроль доступа субъектов к системе

Исходя из приведенных выше данных, наиболее полную защиту АСУ ТП может предоставить решение Kaspersky Industrial CyberSecurity (в частности сервисы KICS for Nodes KICS for Networks), однако ввиду своего формата данный комплекс не обеспечивает прямого контроля трафика и нацелен на использование стандартных сетей Ethernet для протокола Modbus TCP, т.е. использование прикладных протоколов в ЛСУ формально уязвимо для.

Далее следует сравнение отечественных встроенных СЗИ.

Таблица 2 – Сравнительный анализ встроенных СЗИ

	IKS1000GP («Апротех»)	«СЭМ Про» («Информационные системы и стратегии»)	«Торнадо» («Модульные системы торнадо»)	«WhereShock» + «CoreShock» («Физприбор»)
Тип СЗИ	Шлюз IIoT	Защищенный ПЛК с Kaspersky OS	Комплекс защищенной АСУ ТП	Платформа для построения АСУ ТП
Основное предназначение	Сбор и обработка промышленных данных в рамках IIoT	Сбор и передача данных в облачную инфраструктуру с проверкой достоверности и безопасной загрузки	Комплексная защита АСУ ТП на уровнях станции оператора и сетевого узла Ethernet	Объединение данных АСУ ТП и ИТ-инфраструктуры, централизованное диспетчерское управление
Контроль удаленных подключений	В рамках IIoT	Подключения верхнего уровня при использовании Kaspersky Hybrid Cloud Security	Отсутствует	Не уточняется
Контроль сетевого трафика нижнего уровня	Безопасная загрузка прошивки ПЛК, обнаружение атак и аномалий	Отсутствует	Отсутствует	Отсутствует

Приведенная выше попытка анализа показала, что представленные продукты являют собой абсолютно различные по формату и назначению средства.

Тем не менее, краткие обзоры специалистов ресурса ANTI-MALWARE позволяют понять, что наложенные СЗИ не предоставляют прямой контроль, работая с копией сетевого трафика, получаемого либо с TAP-устройств, либо порта зеркалирования SPAN, а те средства, которые осуществляют прямой контроль, функционируют только как брандмауэр, блокируя неразрешенные потоки всей АСУ ТП [12].

В свою очередь, встроенные СЗИ часто представляют собой платформу для построения отдельной АСУ ТП и редко обеспечивают контроль прикладных протоколов на нижнем уровне системы, предлагая скорее системы администрирования отдельного сегмента технологической сети [16].

Средства, предлагающие контроль прикладных протоколо, представляя собой отдельное устройство, по большей части производятся зарубежными компаниями, однако в большинстве своем также предполагают функционирование по типу брандмауэра. Примером является устройство UserGate X10 [17]. Устройство обеспечивает контроль промышленных протоколов Modbus, MMS, OPC UA, IEC 104 и DNP3, блокируя недостоверные потоки информации.

Внешний вид устройства представлен на рисунке 1.

Рисунок 1 – Сетевой шлюз UserGate X10

В итоге сравнительного анализа и изучения краткого обзора наложенных и встроенных СЗИ, был сделан вывод, что обоснованной является разработка устройства, представляющего собой встраиваемое СЗИ, обеспечивающее интеллектуальный контроль и фильтрацию сетевого трафика при использовании удаленных точек доступа к ПЛК. Устройство должно быть проектно-компонуемым, т.е. быть потенциально используемым в уже готовых системах управления, что позволит не только строить систему ИБ с нуля, но и модифицировать уже имеющиеся ИБ и обеспечивать инженеру больший простор в принятии решений.

2.2 Разработка принципа работы устройства

Как ранее было обозначено, устройство должно обеспечивать прямой анализ трафика. Для этого разрабатываемое устройство должно устанавливаться в сеть между удаленной точкой доступа и целевым ПЛК, разделяя линию соединения. Таким образом, устройство должно иметь как минимум два интерфейсных входа-выхода: вход для получения запроса со стороны удаленной точки управления, выход для передачи информации на ПЛК. Получая запрос, устройство анализирует его состав и в случае успешного прохождения проверки (сравнения с записанными в память микроконтроллера разрешенными в проекте АСУ ТП командами) передает его далее на целевой ПЛК.

После получения запроса ПЛК, контроллер выполняет обработку запроса, выполняет соответствующие процессы и передает ответ по изначальному адресу запроса. Следовательно, необходима двухсторонняя передача информации по обоим интерфейсным входам.

Кроме того, необходимо предусмотреть механизм уведомления штатного специалиста предприятия, отвечающего за ИБ, об обнаруженных в трафике аномалиях или нарушениях. В случае несоответствия каких-либо информационных фрагментов полученного сообщения с разрешенными в АСУ ТП, для которой конфигурируется система ИБ, сообщение блокируется и не передается на целевой ПЛК, а на терминал специалиста по ИБ АСУ ТП

отправляется сообщение в соответствии с зафиксированным событием. Для данного процесса также следует реализовать дополнительный выход для связи с терминалом специалиста ИБ АСУ ТП предприятия.

Концепция устройства подразумевает контроль трафика команд ПЛК, соответственно, устройство должно поддерживать некоторый прикладной протокол взаимодействия. В соответствии с [6] данным протоколом выбран Modbus.

Данный протокол является одним из самых распространенных, поддерживается абсолютным большинством современных ПЛК, имеет открытую структуру, а также может быть модифицирован при реализации на отдельном производстве, поскольку спецификацией предложены зарезервированные для пользовательских решений коды функций [18].

Существуют три реализации протокола Modbus – Modbus ASCII, Modbus RTU и Modbus TCP. Все реализации различаются по формату, область применения той или иной реализации зависит от конфигурации и назначения сети. Структура фрейма каждой реализации приведена на рисунке 2 [19].

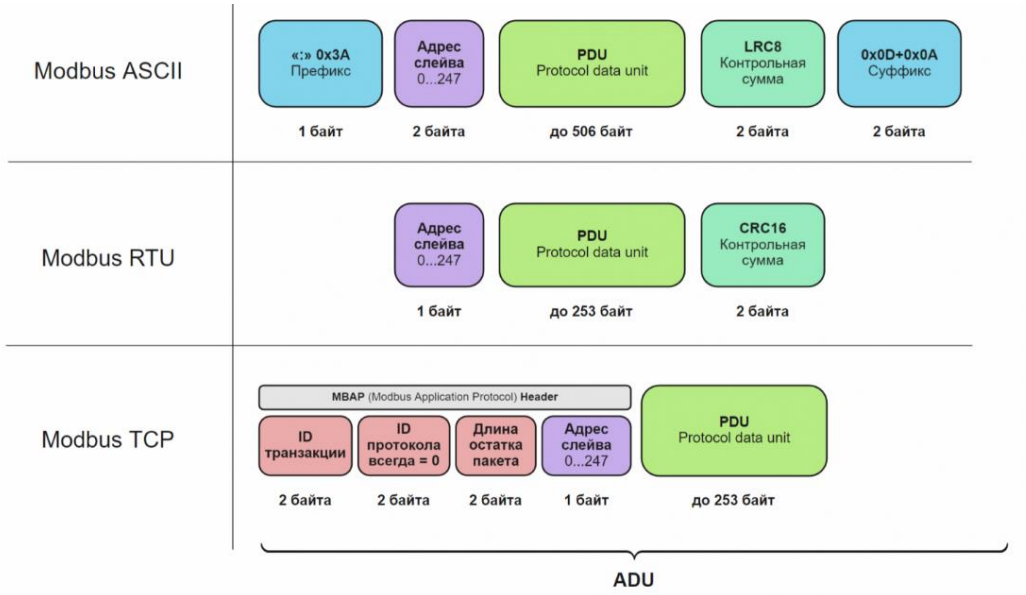


Рисунок 2 – Структура фреймов различных реализаций протокола Modbus

Наименьшую длину фрейма имеет реализация Modbus RTU. В дальнейшем при разработке устройства будет подразумеваться, что устройство поддерживает непосредственно реализацию Modbus RTU.

Таким образом, планируется разработка устройства, обеспечивающего прямой анализ и контроль трафика технологической сети Modbus RTU.

Подключение устройств, поддерживающих Modbus RTU, осуществляется посредством физических интерфейсов RS-232, RS-422 и RS-485.

Сравнительная иллюстрация контактов упомянутых интерфейсов приведена на рисунке 3.

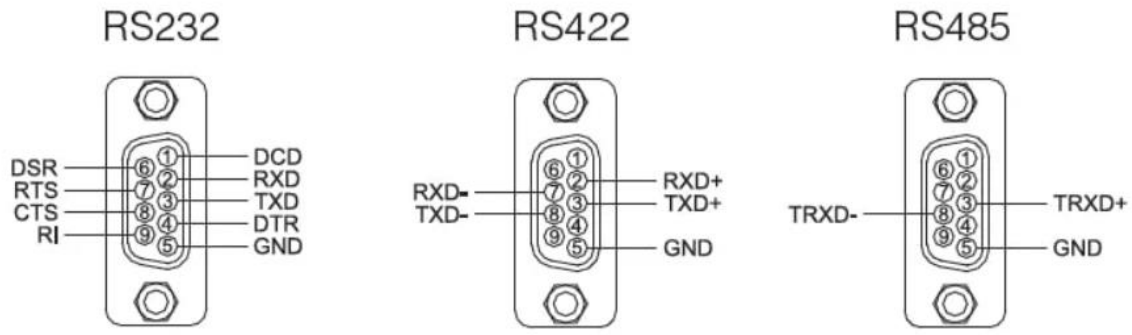


Рисунок 3 – Сравнение контактов разъемов интерфейсов RS-232, RS-422, RS-485

Приведенные интерфейсы имеют различное применение ввиду характерных технических отличий: RS-232 и RS-422 – полный дуплекс по типу передачи, RS-485 может осуществлять как полный дуплекс при четырехпроводной схеме подключения, так и полудуплекс при двухпроводной. Интерфейсы обеспечивают различную дальность передачи – RS-422 и RS485 применяются на дистанции до 1,2 км при скорости 9600 бод, RS-232 – около 15 метров при той же скорости. Различаются также топологии сетей с использованием данных интерфейсов - RS-232 и RS-422 используются для построения топологии точка-точка, а RS-485 позволяет организовать многоточечную топологию, объединяющую до 256 ведомых устройств [20].

Исходя из вышеописанного, наиболее рациональным является создание устройства с интерфейсными разъемами RS-485.

Поскольку работа с ведомыми устройствами по протоколу Modbus RTU осуществляется попеременно (ведомое устройство не инициирует передачу и только отвечает ведущему устройству), то следует использовать двухпроводную схему подключения и, соответственно, полудуплексный тип передачи.

Исходя из всего вышеописанного, устройство должно обеспечивать анализ и контроль трафика, прием и передачу сообщений Modbus RTU, а также передавать сообщения на терминал специалиста ИБ АСУ ТП, следовательно, устройство должно быть построено на базе микроконтроллера.

Вышеописанная схема предполагает как минимум два интерфейсных входа-выхода, а Modbus RTU использует для организации передачи данных интерфейс RS-485. Для обеспечения такой конфигурации микроконтроллер устройства должен иметь в составе как минимум два аппаратных УАПП, интерфейс для сообщения с терминалом специалиста ИБ АСУ ТП может быть организован программно.

Таким образом, сформирована концепция устройства на основе микроконтроллера, осуществляющего прямой анализ, фильтрацию и контроль сетевого трафика технологической сети или ее сегмента, использующего протокол Modbus RTU, и уведомляющего специалиста предприятия по ИБ АСУ ТП о происшествиях. Принципиальная схема расположения устройства на базе микроконтроллера в сети указана на рисунке 4.

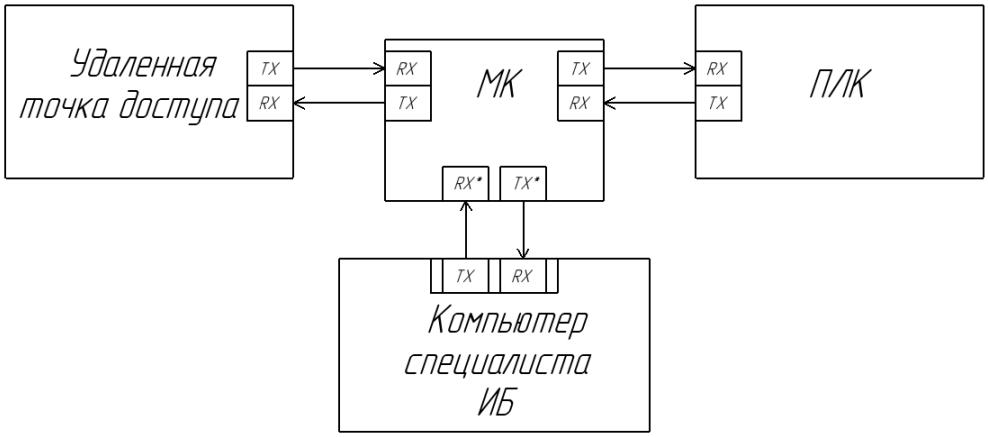


Рисунок 4 – Схема расположения устройства в сегменте технологической сети

2.3 Разработка аппаратной части

2.3.1 Выбор микроконтроллера

Ранее было упомянуто, что устройство должно быть построено на базе микроконтроллера.

Для выбора микроконтроллера необходимо определить спектр задач, которые должно выполнять устройство на техническом уровне. Исходя из предыдущего пункта сформирован следующий список осуществляемых процессов:

1. Алгоритм фильтрации сетевого трафика;
2. Приемо-передача фреймов Modbus RTU;
3. Осуществление работы двух аппаратных УАПП;
4. Хранение разрешенной в проекте АСУ ТП информации во внутренней памяти.

Таким образом, микроконтроллер должен обладать достаточной тактовой частотой ядра для обеспечения быстродействия при выполнении алгоритма фильтрации, шириной шины данных минимум 8 бит для обеспечения приема и обработки фрагментов сообщения Modbus RTU, минимум двумя аппаратными УАПП и достаточным объемом ПЗУ для хранения как исполняемого кода, так и разрешенных в проекте команд.

Кроме того, МК должен иметь удобные для промышленного применения контур питания и корпусное исполнение комфортного для быстрого модифицирования кода для применения в конкретном проекте и дальнейшего монтажа микроконтроллера на печатную плату.

Также следует исходить из идеи оптимального использования ресурсов – в проекте ресурсы микроконтроллера должны использоваться по максимуму, т.е. недостаток ресурсов, равно как и избыток незадействованных массивов памяти и интерфейсов, означает неэффективное использование ресурсов и неоптимальный выбор элементной базы для реализации проекта.

Для первоначальной разработки также следует учитывать порог вхождения в программирование микроконтроллеров и соответствующую производителю среду программирования.

Таким образом, в первую очередь стоит сосредоточиться на выборе 8-битных микроконтроллеров.

На рынке 8-битных МК наиболее популярны семейств AVR, ARM и PIC [21]. Поскольку линейки всех трех семейств достаточно обширны, следует заострить внимание на параметре, который сузил бы выбор МК. Таким параметром выбрано наличие двух аппаратных УАПП, поскольку ввиду маркетинга чаще выпускают МК с большим количеством доступных интерфейсов, чем с несколькими наборами одного типа интерфейса.

Далее был определен текущий ассортимент МК, из которого выбраны следующие МК одной категории: AVR ATmega162-16PU, STM8L151C8T6 и PIC18F23K22-I/SP. Типовые исполнения данных МК указаны на рисунке 5.

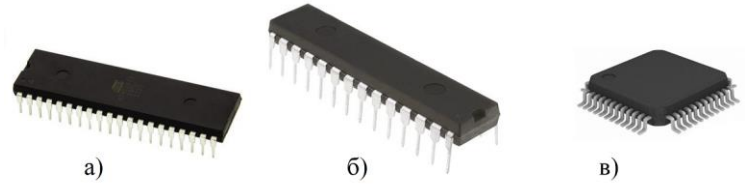


Рисунок 5 – Выбранные МК: а) ATmega162-16PU, б) PIC18F23K22-I/SP, в) STM8L151C8T6

Далее приведено сравнение данных МК по таким характеристикам, как напряжение питания, тактовая частота, количество УАПП, объем памяти и т.д.

Сравнение указанных микроконтроллеров приведено в таблице 3.

Таблица 3 – Сравнение технических характеристик различных МК

	ATmega162-16PU	PIC18F23K22-I/SP	STM8L151C8T6
Корпусное исполнение	DIP-40	28-SPDIP	LQFP-48
Тактовая частота	16 МГц	16 МГц	16 МГц
Тип памяти программ	flash	flash	flash
Объем памяти программ	16 кбайт	8 кбайт	64 кбайт
Количество УАПП	2	2	3
Типы интерфейсов	I2C, SPI, UART	I2C, SPI, UART	I2C, IRDA, SPI, UART
Напряжение питания	2,7…5,5 В	2,3…5,5 В	1,8…3,6 В
Стоимость	1470 руб.	1250 руб.	590 руб.

Исходя из представленной выше таблицы, можно сделать вывод, что наиболее удобным вариантом, несмотря на сравнительную дороговизну, является AVR ATmega162-16PU по следующим причинам:

1. Корпусное исполнение ATmega162-16PU и PIC18F23K22-I/SP лучше подходит для быстрого монтажа и подключения на отладочную плату или подключения к программатору.

2. Объем памяти ATmega162-16PU представляет среднюю величину из выбранных микроконтроллеров – 8 кбайт может быть недостаточно для вмещения всего исполняемого кода, а 64 кбайт вряд ли будут задействованы на большую часть.

3. Несмотря на преимущество использования дополнительного аппаратного УАПП, потенциал третьего интерфейса STM8L151C8T6 не будет задействован полностью, т.к. предполагается только его работа на передачу данных без получения.

4. Номинальное напряжение питания для МК ATmega162-16PU и PIC18F23K22-I/SP равно 5 В, а для STM8L151C8T6 – 3,3 В, что потребует более точной настройки цепи питания и сборки отдельного контура, что в конечном счете уменьшит ценовое преимущество STM8L151C8T6, поскольку для питания устройства предполагается использовать промышленный источник питания 24 В постоянного тока, и для МК с номинальным напряжением питания 5 В есть возможность воспользоваться типовыми схемами понижения напряжения.

2.3.2 Подбор интерфейсных микросхем

Для реализации устройства необходимо предусмотреть интерфейсные разъемы RS-485 и какой-либо разъем для связи устройства с терминалом специалиста по ИБ.

Поскольку разработка собственной интегральной микросхемы потребовала бы дополнительных временных затрат, а устройство в дальнейшем планируется дорабатывать, то предложено использовать готовые интегральные микросхемы.

Популярным решением для преобразования сигналов УАПП в сигналы интерфейса RS-485 является модуль HW-97, преобразователь UART в RS-485 на базе микросхемы конвертера физических уровней MAX485. Внешний вид данной микросхемы приведен на рисунке 6.

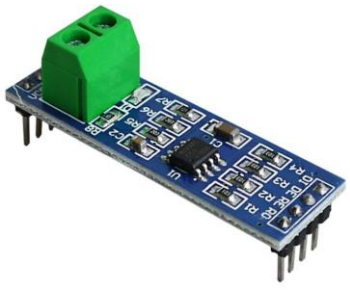


Рисунок 6 – Модуль HW-97, преобразователь UART в RS-485

Характеристики и контакты модуля указаны в таблицах 4 и 5.

Таблица 4 – Характеристики модуля HW-97

Напряжение питания, В	4,75…5,25
Чувствительность приемника, мВ	200
Номинальный ток питания, мА	10
Согласующий резистор, Ом	120
Количество приемников	1
Количество передатчиков	1
Режим работы	Полудуплексный

Таблица 5 – Назначение контактов модуля HW-97

DI (Driver Input)	Вход передатчика
DE (Driver Enable)	Разрешение работы передатчика
RE (Receiver Enable)	Разрешение работы приемника
RO (Receiver Output)	Выход приемника
A	Прямой вход приемника/Прямой выход передатчика
B	Инверсный вход приемника/Инверсный выход передатчика
VCC+	Питание
GND	Общий провод

Соответственно, оба аппаратных УАПП должны быть оснащены данной микросхемой.

Для связи устройства с терминалом специалиста по ИБ возможно использовать преобразователь USB-UART. На рынке представлено несколько реализаций данного устройства – на базе микросхем CP2102, PL2303, CH340, FT232R. Поскольку планируется использовать уже готовые модули, то выбор в данном случае не принципиален, но среди пользователей более популярна реализация на базе PL2303.

Стандартное исполнение преобразователя UART-USB на базе PL2303 представлено на рисунке 7.

Рисунок 7 – Реализация преобразователя UART-USB на базе PL2303

Характеристики данного модуля приведены в таблице 6, назначение контактов приведено в таблице 7.

Таблица 6 – Характеристики преобразователя UART-USB на базе PL2303

Напряжение питания, В	4…6
Номинальный ток питания, мА	19
Максимальный ток питания, мА	24

Таблица 7 – Назначение контактов преобразователя UART-USB на базе PL2303

VCCIO	Питание
GND	Общий провод
TXD	Выход передатчика
RXD	Вход приемника

Таким образом, описанные выше модули обеспечат взаимодействие с устройствами сегмента технологической сети – RS-485 обеспечит подключение к удаленной точке доступа и целевому ПЛК, а USB – к терминалу специалиста по ИБ АСУ ТП предприятия.

2.3.3 Схема питания устройства

Поскольку планируется питание устройства от промышленного 24 В блока питания постоянного тока, то необходимо составить каскад цепи питания, обеспечивающий понижение напряжения до номинальных 5 В микроконтроллера и защиту от высокочастотных помех промышленного импульсного блока питания.

Существуют готовые решения, например, FDD03-05S2 [22]. Данный блок питания при входном напряжении 18…36 В (номинальное 24 В) постоянного тока обеспечивает выходное напряжение 5 В при 500 мА, однако данный компонент существенно увеличивает себестоимость устройства, поэтому было принято решение составить каскад цепи питания самостоятельно.

Существуют типовые схемы с использованием стабилизатора напряжения по типу КР142ЕН5А. Данная микросхема и ее аналоги позволяют составить одноконтурный стабилизатор напряжения, поскольку некоторые аналоги (в частности LM7805CT, приведенного на рисунке 8) допускают входное напряжение до 35 В и обеспечивают выходное напряжение в 5 В (±2%), что удовлетворяет характеристикам AVR ATmega162-16PU.

Таким образом, можно воспользоваться типовой схемой стабилизатора постоянного напряжения, приведенной на рисунке 8 [23].

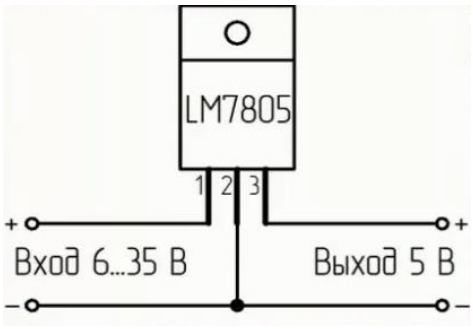


Рисунок 8 – Типовая схема подключения стабилизатора напряжения

Также для стабильности питания и подавления помех следует между 1 и 2 выводами подключить пленочный конденсатор 0,33 мкФ, а параллельно выходу – электролитический 0,1 мкФ. Также помимо основной нагрузки на выходе стабилизатора рекомендуется монтировать сопротивление 4,7 кОм.

Несмотря на возможное применение одноконтурной цепи питания, возможен резкий скачок напряжения, что понизит стабильность питания схемы. Для предотвращения подобного инцидента следует использовать

дополнительный контур стабилизации напряжения с 24 В до 12 В с использованием биполярного транзистора, указанный на рисунке 9.

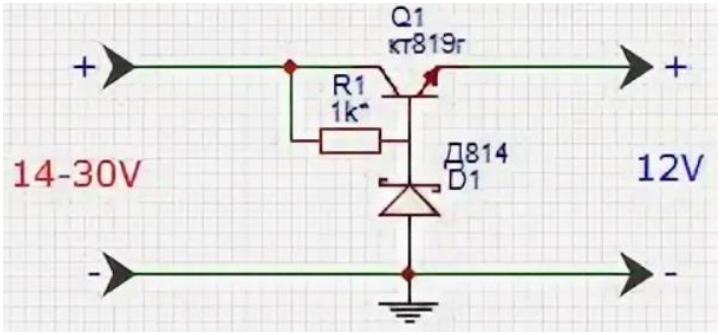


Рисунок 9 – Принципиальная электрическая схема стабилизатора напряжения с 24 до 12 В

Необходимо выбрать стабилитрон с номинальным напряжением стабилизации 12 В (например, КС212Ж) и биполярный транзистор (КТ819Г или его аналоги).

Также необходимо рассчитать номинал сопротивления R1 по мощности рассеяния стабилитрона.

Определим падение напряжения на сопротивлении R1:

$$U_{R1} = U_{вх} - U_{вых} = 24 - 12 = 12 \text{ В};$$

$$I_{ст} = \frac{P_{ст}}{U_{R1}} = \frac{0{,}125}{12} \text{ А};$$

$$R_1 = \frac{U_{R1}}{I_{ст}} = \frac{12}{\frac{0{,}125}{12}} = 1152 \text{ Ом}.$$

Следует использовать сопротивление большего номинала для обеспечения стабильности при скачках напряжения. Таким образом, принято R1 = 1,2 кОм.

Предельно допустимый ток стабилизации стабилитрона равен 11 мА, что больше полученного расчета: $0{,}011 > \frac{0{,}125}{12} \approx 0{,}0104$.

2.3.4 Корпус устройства

Предполагается крепление корпусного исполнения проектируемого устройства на DIN-рейку, поэтому выбран готовый корпус формата D3MG [24]. Стандартное исполнение приведено на рисунке 10.

Рисунок 10 – Корпус на DIN-рейку формата D3MG

Габариты корпуса: $53{,}3 \times 90{,}2 \times 57{,}5$ мм. С учетом описанных ранее компонентов данный корпус является достаточным по габаритам.

Также в комплекте с данным корпусом поставляется печатная плата одноименного формата, приведенная на рисунке 11.

Рисунок 11 – Печатная плата D3MG

Данная печатная плата будет использована для будущего монтажа схемы подключений устройства при тестировании прототипа.

Принципиальная схема подключений приведена в приложении А.

2.3.5 Расчет энергопотребления устройства

Для более корректного проектирования устройства следует приблизительно рассчитать потребляемую им мощность.

После обращения к технической документации на AVR ATmega162-16PU, определен номинальный ток питания: при тактовой частоте встроенного генератора 8 МГц максимальный ток питания составляет 16 мА. Также определен максимальный суммарный ток питания периферийных устройств: через выводы VCC и GND суммарный ток ограничен 200 мА для корпусного исполнения PDIP, а через один порт ток ограничен до 40 мА.

Как было описано ранее, к МК будет подключено 2 модуля HW-97 и преобразователь UART-USB. Также было принято решение подключить 2 светодиода: в цепь питания для индикации правильного подключения и к порту ввода-вывода для местной индикации обнаружения нарушения в сетевом трафике.

Суммарная мощность устройства будет определена по формуле 1:

$$P_S = P_{MK} + 2 \cdot P_{HW-97} + P_{PL2303} + P_{LEDgreen} + P_{LEDred}, \quad (1)$$

где

P_{MK} - мощность, потребляемая МК,

P_{HW-97} - мощность, потребляемая модулем HW-97,

P_{PL2303} - мощность, потребляемая преобразователем UART-USB,

$P_{LEDgreen}, P_{LEDred}$ - мощность, потребляемая зеленым и красным светодиодом соответственно.

В соответствии с законом Ома мощность радиоэлектронного компонента может быть определена по формуле 2:

$$P = U \cdot I, \quad (2)$$

где

U - рабочее напряжение компонента,

I - ток потребления.

Предварительно проверим соответствие суммы токов по выводам VCC – GND по формуле 3:

$$I_S = I_{MK} + I_{HW-97} + I_{PL2303} + I_{LEDgreen} + I_{LEDred}. \quad (3)$$

Согласно справочным данным, ток потребления круглых 3-мм светодиодов равен 20 мА, а напряжение питания зеленого – 3,2 В, красного – 2,1 В.

Рассчитаем суммарный ток:

$I_S = 16 + 10 + 24 + 20 + 20 = 90$ мА.

Следовательно, максимальная сумма токов не превышает паспортного значения в 200 мА, и ток питания ни одного из компонентов не превышает 40 мА.

Рассчитаем суммарную мощность:

$$P_S = U_{MK} \cdot I_{MK} + 2 \cdot U_{HW-97} \cdot I_{HW-97} + U_{PL2303} \cdot I_{PL2303} +$$
$$+U_{LEDgreen} \cdot I_{LEDgreen} + U_{LEDred} \cdot I_{LEDred} = 5 \cdot 0,016 + 2 \cdot 5 \cdot 0,01 + 5 \cdot 0,019 +$$
$$+3,2 \cdot 0,02 + 2,1 \cdot 0,02 = 0,381 \text{ Вт}.$$

Таким образом, ориентировочная суммарная мощность устройства не превышает 0,4 Вт, что позволяет воспользоваться любым доступным в ЛСУ источником питания 24 В постоянного тока без значительного увеличения нагрузки.

2.4 Разработка алгоритма работы устройства

Ранее концепция работы устройства была описана с точки зрения прикладного уровня, в данном подразделе будут обозначены особенности разработки алгоритма для МК.

Предполагается следующая обобщенная последовательность действий:

1. Устройство получает фрейм Modbus RTU;

2. Алгоритм обрабатывает полученное сообщение и анализирует его состав;

3.1. В случае успешного прохождения соответствия разрешенным в проекте запросам фрейм передается на целевой ПЛК;

3.2.1 В случае обнаружения несоответствия разрешенным в проекте запросам фрейм блокируется;

3.2.2 На терминал специалиста ИБ АСУ ТП посылается сообщение в соответствии с обнаруженным нарушением;

3.2.3 На адрес запроса отправляется сообщение-маска об успешной обработке команды для маскировки структуры целевого ПЛК.

4. В случае успеха п. 3.1 устройство получает ответный фрейм Modbus RTU от целевого ПЛК;

5. Устройство проводит проверку полученного ответа ПЛК;

6.1. Если в ответе ПЛК обнаружены дополнительные поля или аномалии, вызванные физическими нарушениями линии связи, то ответ ПЛК блокируется;

6.2. Если ответ ПЛК успешно прошел проверку, то ответ передается на адрес запроса.

Данный алгоритм представлен обобщенно, поскольку в зависимости от спецификации проекта перечень допустимых команд меняется, и, соответственно, меняется подход к обработке полученных команд, поэтому будет рассмотрен обобщенный алгоритм программно-аппаратных процессов устройства.

1. Определяются состояния и функции портов МК.

2. Инициализируются аппаратные УАПП для работы с протоколом Modbus RTU.

3. Инициализируется программный УАПП для работы с терминалом специалиста ИБ АСУ ТП.

4. Разрешаются глобальные прерывания.

Процессы 1-4 являются подготовительными и выполняются однократно при включении устройства. Дальнейшие процессы выполняются в бесконечном цикле при включенном устройстве.

5. Получение фрейма Modbus RTU по УАПП.

6. Сравнение полей полученного фрейма с уставкой.

7. Действие после проверки фрейма.

7.1. В случае соответствия отправка фрейма целевому ПЛК.

7.2. В случае несоответствия уведомление специалиста по ИБ АСУ ТП.

Обобщенный алгоритм в виде блок-схемы представлен в приложении Б.

2.5 Программные аспекты реализации устройства

Разработка устройства предполагает написание исполняемого кода на одном из языков программирования. Был сделан выбор для написания приложения для МК использовать язык Си.

Используется IDE Microchip Studio с компилятором GCC как наиболее подходящие для особенностей МК AVR.

В соответствии с ранее описанным алгоритмом, вложенными процессами являются инициализация аппаратного и программного УАПП, а также процедура сравнения полученного фрейма с разрешенными в проекте командами. Также имеет смысл рассмотрение отдельных аспектов использования УАПП.

2.5.1 Особенности аппаратного УАПП

МК AVR используют эффективную систему прерываний. Для использования УАПП предложено три вектора прерывания: RXC (прерывание по получении), TXC (прерывание по передаче), UDRE (прерывание по опустошении регистра данных).

Применение вектора прерывания TXC приводит к большей задержке между отправками байта (в AVR ATmega162 UDR восьмибитный), поскольку после помещения байта в регистр UDR происходит побитный перенос данных из UDR в сдвиговый регистр для отправки на линию TXD МК, и флаг прерывания активируется только по очищении сдвигового регистра, пока UDR пуст, в то время как флаг прерывания UDRE активируется при опустошении UDR без обращения внимания на состояние сдвигового регистра [25].

Кроме того, следует учитывать тот факт, что активация флага одного вектора прерывания при разрешенных глобальных прерываниях может приостановить выполнение другого вектора прерывания. Например, при включении устройства регистр UDR пуст, в связи с чем активируется флаг прерывания UDRE, в результате подпрограммы приема и передачи данных не могут быть инициализированы либо исполняются некорректно.

Разрешение выполнения всех глобальных прерываний AVR инициализируется командой sei(), однако разрешение прерываний отдельных интерфейсов, как и прочих параметров, регламентируется установкой битов в соответствующих регистрах. Для УАПП AVR настроечными регистрами являются UBBR (настройка скорости УАПП), UCSRA (регистр флагов), UCSRB (регистр настройки режимов приема-передачи, а также разрешения векторов прерываний) и UCSRS (регистр формата посылки). Таким образом, разрешение векторов прерываний TXC, RXC и UDRE разрешается установкой битов TXCIE, RXCIE и UDRIE соответственно, а режим работы определяется установлением битов RXEN (разрешение приема) и TXEN (разрешение передачи).

Во избежание приостановки обработки одного прерывания активацией флага другого прерывания следует воспользоваться командой cli(), которая запрещает глобальные прерывания (т.е. используется обратно sei()). При обработке какого-либо прерывания, выполнение которого критически важно, в начале обработчика прерывания следует применить команду cli(), что запретит взведение флагов других глобальных прерываний и возможную приостановку обработки целевого прерывания.

2.5.2 Реализация программного УАПП

Как ранее было обозначено, в устройстве будет задействовано два аппаратных УАПП и реализован программный.

В соответствии с концепцией устройства аппаратные УАПП функционируют попеременно на прием и передачу, а программный УАПП

применяется только для передачи уведомления на терминал специалиста ИБ АСУ ТП.

Фактически для организации передачи данных при использовании портов ввода-вывода общего назначения необходимо в зависимости от передаваемой последовательности битов устанавливать состояние порта в состояние логических нуля или единицы с определенной длительностью импульса, продиктованной заданной скоростью передачи УАПП.

Для реализации заданной задержки после установки состояния порта для передачи данных было принято решение использовать системный таймер-счетчик. При настройке системного таймера-счетчика AVR конфигурируются следующие регистры: TCCR (регистр источника тактирования и предделителя), OCRA (регистр сравнения) и TCNT (счетный регистр).

Количество счетов таймера для отсчета полупериодов импульсов определяется по формуле 4:

$$OCRA = \frac{F_{CPU}}{2 \cdot Baudrate} - T_{COM}, \quad (4)$$

где

F_{CPU} - тактовая частота ядра МК,

$Baudrate$ - скорость УАПП в бодах (9600, 19200 и т.д.),

T_{COM} - поправочные счеты таймера, определяемые экспериментально.

Для определения поправочных счетов был использован виртуальный симулятор ISIS Proteus.

В общем случае операция передачи байта подчиняется правилам передачи УАПП. В исходном состоянии линия передачи аппаратного УАПП установлена в высокий логический уровень, далее происходит стандартный аппаратный процесс передачи байта:

1. Старт-бит (установка низкого логического уровня) в течение двух полупериодов.

2. Последовательная установка состояния линии в высокий или низкий логический уровень с длительностью импульса в два полупериода в зависимости от передаваемого байта (повторяется 8 раз).

3. Стоп-бит (установка высокого логического уровня в течение минимум двух полупериодов).

Временная диаграмма передачи байта по УАПП приведена на рисунке 12.

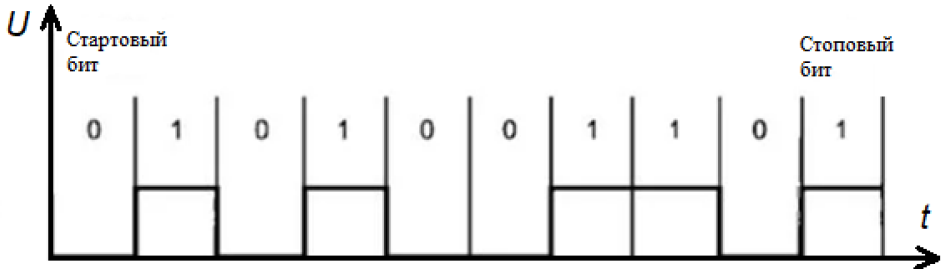


Рисунок 12 – Пример временной диаграммы состояния линии TXD при передаче байта

2.5.3 Операция анализа полученного фрейма

Ранее на рисунке 1 была приведена общая структура фрейма Modbus RTU.

Данный протокол поддерживает различные функции с соответствующим различным форматом, в следствие чего длина фреймов с различными кодами функций различается.

Например, команда записи состояния одного дискретного вывода в шестнадцатеричной форме выглядит следующим образом:

07 05 00 00 FF 00 5C 8C

В данной команде 07 – адрес ведомого устройства, 05 – код функции записи состояния дискретного вывода, 00 00 – адрес первого регистра (старший и младший байты), FF 00 – записываемое значение (старший и младший байты соответственно), 5C 8C – контрольная сумма (в зависимости от платформы реализации порядок старшего и младшего байт могут меняться).

Команда записи состояния нескольких дискретных выводов имеет следующий формат:

11 0F 00 13 00 0A 02 CD 01 BF 0B

В данном случае 11 – адрес ведомого устройства, 0F – код функции записи состояния нескольких дискретных выводов, 00 13 – адрес первого регистра, 00 0A – количество регистров (старший и младший байты), 02 – количество байт далее, CD 01 – значения записываемых состояний дискретных выводов, BF 0B – контрольная сумма.

Таким образом, для обработки команд с различными кодами функций алгоритм может быть модифицирован.

В общем случае при разработке процедуры сравнения полученного фрейма с зарегистрированными в проекте запросами рассмотрены следующие подходы:

1. Сравнение фиксированного количества полей при известном постоянстве формата используемых в проекте команд;

2. Анализ кода функции для выявления количества полей;

3. Выявление в посылке байта, содержащего дальнейшее количество байт.

2.6 Демонстрация работы алгоритма

Для первоначальной демонстрации алгоритма разработан тестовый проект, поддерживающий обработку шести команд записи состояния дискретных выводов: запись нуля и единицы для трех последовательных портов. Поскольку при отработке проекта не было возможности подключиться к реальному ПЛК, в качестве симулированных дискретных выводов представлены порты ввода-вывода МК с подключенными светодиодами, отражающими состояние порта МК.

Для разработки и отладки проекта используются такие программные продукты, как терминал t1.9 для работы с COM-портом ПК, симулятор мастер-запросов Modbus, а также отладочная плата с внутрисистемным программатором Pinboard RII.

Изначально разрабатываемое устройство поддерживает только адрес ведомого устройства **07**.

Первоначально проводится соединение отладочной платы и МК с COM-портом ПК по протоколу Modbus RTU (Рисунок 13):

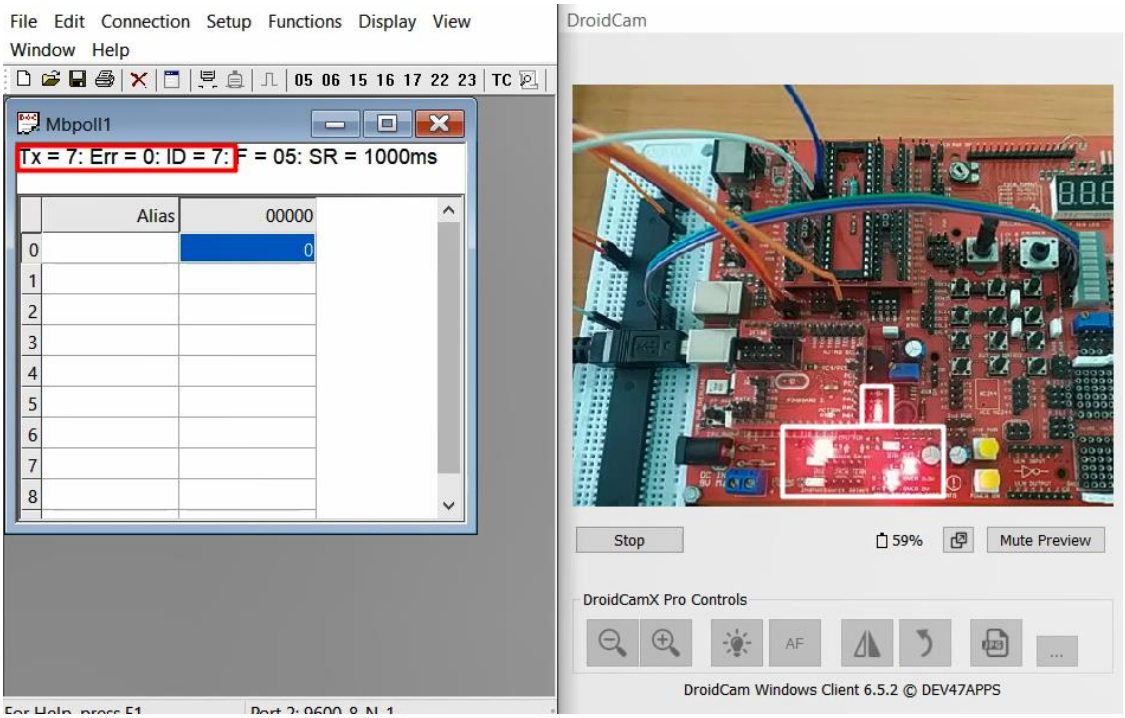


Рисунок 13 – Подключение МК к персональному компьютеру

Увеличивающийся счетчик переданных пакетов, нулевой счетчик ошибок, а также циклически зажигающиеся светодиоды приемопередатчика на плате сигнализируют об успешном подключении к ПК.

Далее реализованы команды записи состояния 1 трех дискретных выводов. Успешная обработка команды отражена зажегшимися светодиодами, подключенными к портам МК в правой части схемы (Рисунок 14, 15):

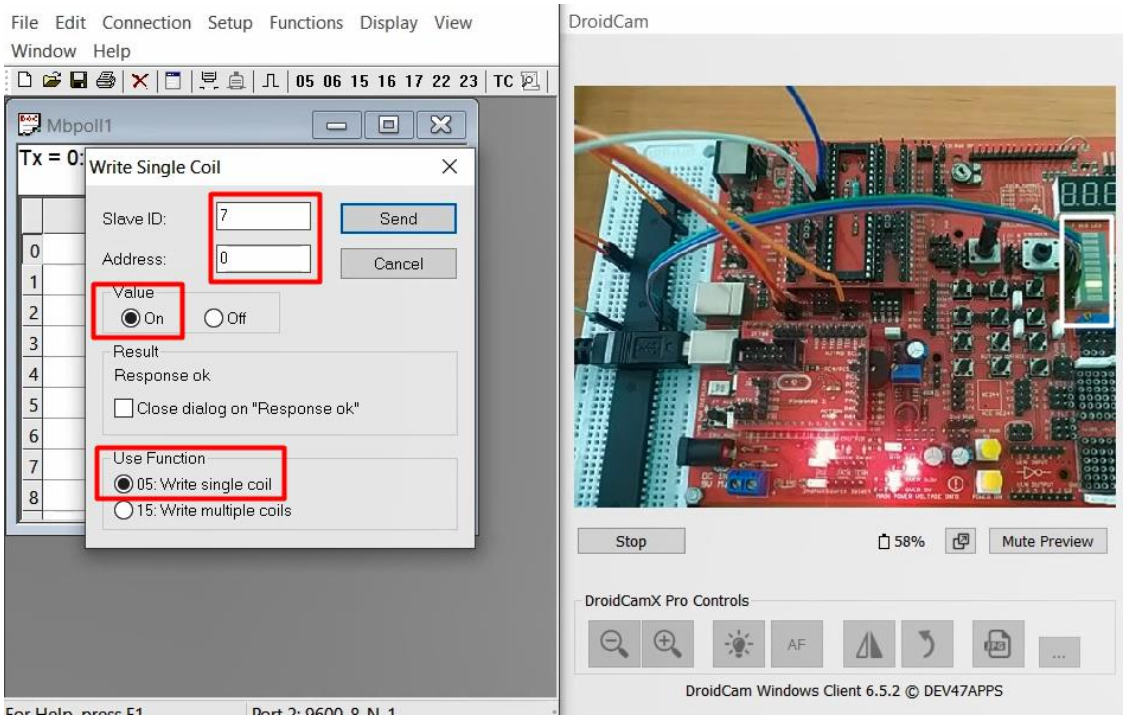


Рисунок 14 – Отправка команды на запись 1 на первом дискретном выводе

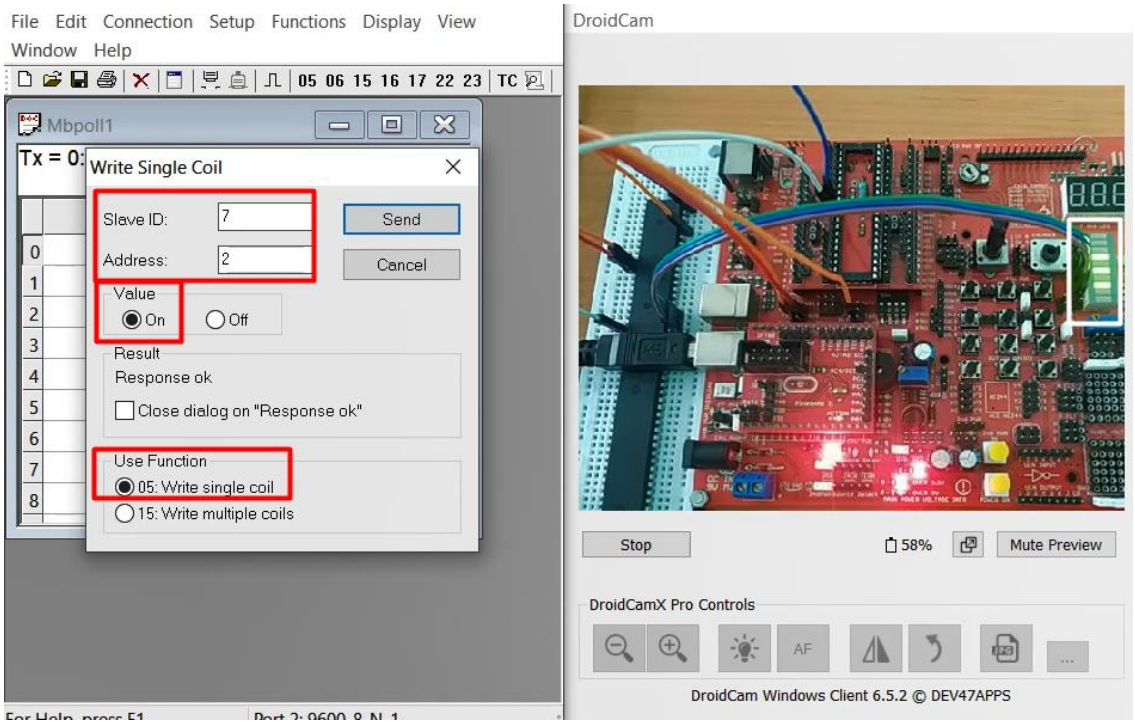


Рисунок 15 – Все дискретные порты записаны в состояние 1

Далее аналогично проверены команды записи 0 в данные порты, о чем свидетельствовали погасшие светодиоды.

После проверки работоспособности устройства и успешной проверки подключения была симулирована проверка нарушения в сетевом трафике. Допустим, что в исследуемой ЛСУ несколько ведомых устройств, и устройство с адресом 06 не поддерживает запись данных дискретных выводов. В таком случае подобный запрос фиксируется, и по программному УАПП отправляется уведомление о нарушении.

При демонстрации плата была подключена к ПК посредством двух COM-портов, первый использовался для обработки команд Modbus RTU, второй для работы с уведомлениями.

Далее представлены уведомления, отправляемые при обнаружении таких нарушений, как:

1. Обращение к незарегистрированному устройству.
2. Незарегистрированный код функции.
3. Попытка записи незарегистрированного регистра.

Обрабатываемые уведомления представлены на рисунках 16-18.

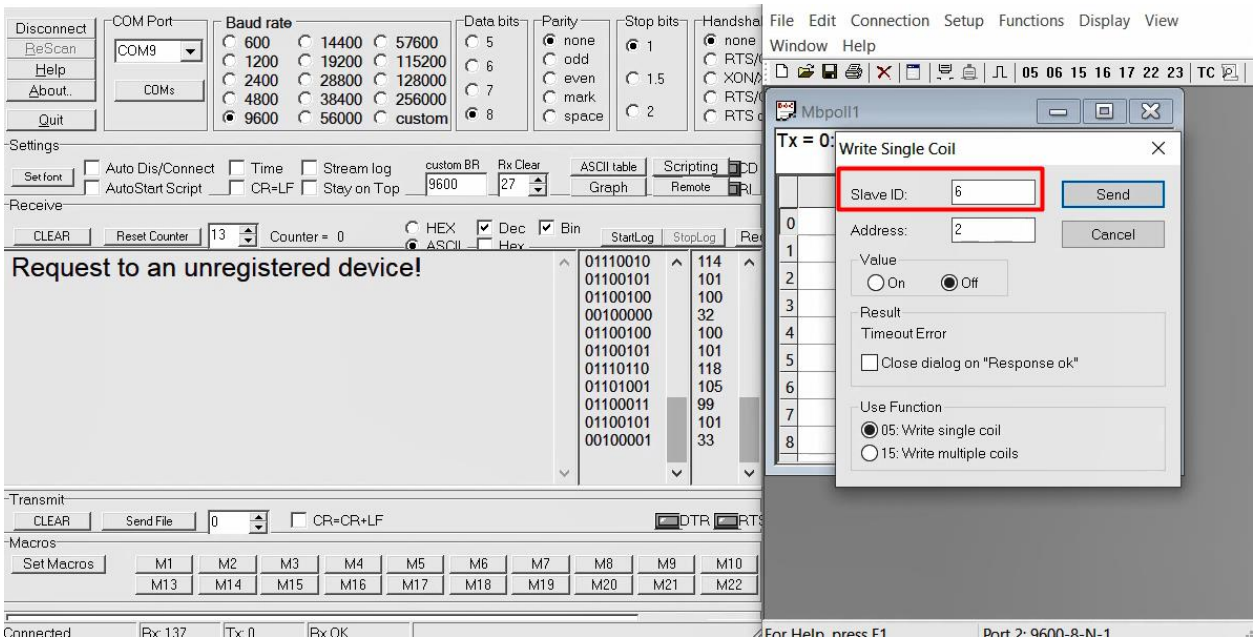


Рисунок 16 – Обращение к незарегистрированному устройству

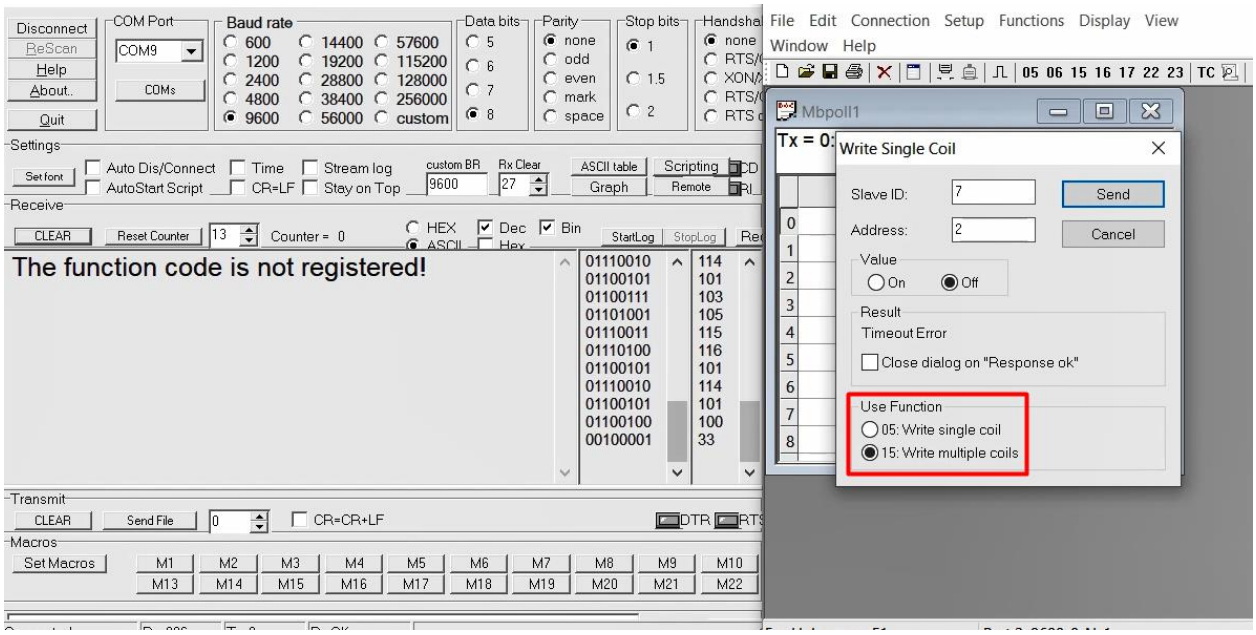


Рисунок 17 – Запрос с незарегистрированным кодом функции

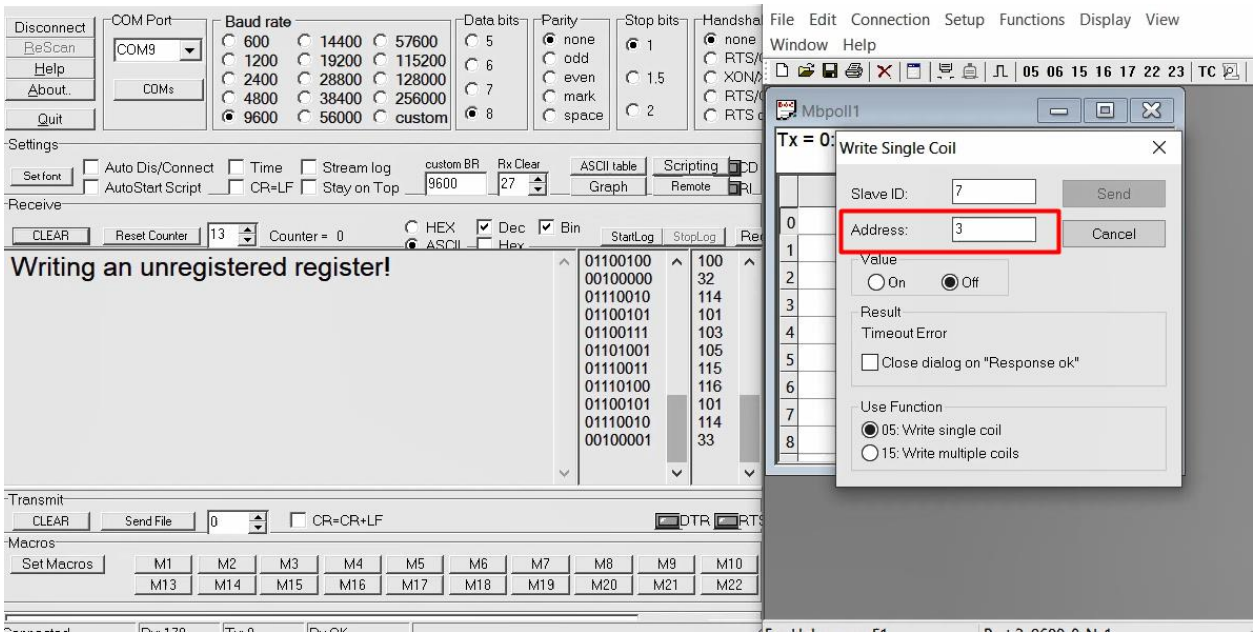


Рисунок 18 – Попытка записи незарегистрированной области памяти

В разработанном проекте предусмотрено обнаружение следующих нарушений с соответствующими уведомлениями:

1. «Запрос к незарегистрированному устройству!» («Request to an unregistered device!»);

2. «Код функции не зарегистрирован!» («Function code is not registered!»);

3. «Запись незарегистрированного регистра!» («Writing an unregistered register!»);

4. «Значение записи вне диапазона!» («The value of the writing is out of range!»);

5. «Пакет поврежден (CRC)» («Frame is damaged (CRC)»).

Исполняемый код демонстрационного проекта представлен в приложении В.

3 Концепция стартап-проекта

Сутью проекта является создание и вывод на рынок продукта в области информационной безопасности автоматизированных систем управления технологическим процессом. Цель данной разработки – увеличение защищенности локальных систем управления при удаленной приемо-передаче технической информации.

3.1 Описание продукта как результата НИР

В любой автоматизированной системе управления технологическим процессом происходит постоянный перенос потоков информации, входные потоки при вводе могут быть использованы для формирования управляющего воздействия и записи состояния конкретного исполнительного устройства, а выходные могут служить для диагностики системы и содержать данные о конфигурации и параметрах отдельных узлов и всего контура в целом.

При удаленной передаче информации прикладной коммуникационный протокол Modbus, часто используемый при построении систем управления, имеет уязвимость, что позволяет осуществлять несанкционированную деятельность – ввод, вывод, загрузку и выгрузку информации – что может привести к ущербу работе предприятия. Данная уязвимость зафиксирована в банке данных угроз безопасности информации ФСТЭК России [6].

Разрабатываемое устройство представляет собой программно-аппаратный комплекс на базе микроконтроллера, осуществляющего алгоритм

фильтрации и контроля сетевого трафика. На данном этапе предполагается работа с форматом Modbus RTU.

3.2 Интеллектуальная собственность

Ценность устройства заключается в исполняемом алгоритме фильтрации и контроля сетевого трафика, написанном в специализированном ПО на персональном компьютере, элементная база для корпусного исполнения устройства в ряде случаев может быть различной, следовательно, объектом интеллектуальной собственности является программа для ЭВМ. Для обеспечения защиты интеллектуальной собственности необходима регистрация программы в Федеральном институте промышленной собственности (Роспатент). Регистрация программы для обеспечивает защиту технологии следующими правовыми актами:

— часть четыре ГК РФ [26];

— Федеральный закон от 12.03.2014 N 35-ФЗ [27];

— Федеральный закон от 20.07.2020 N 217-ФЗ и т.д. [28].

Исходный текст программы защищен авторским правом.

В настоящее время идет процесс подачи заявки на регистрация разработанного алгоритма в Роспатенте.

3.3 Целевые сегменты потребителей

Рассматриваемым для продвижения устройства сегментом рынка является совокупность организаций и предприятий РФ, использующих автоматизированные системы управления технологическим процессом. Помимо обоснования актуальности разработки наличием активной уязвимости протокола необходимо составить опросник, ответы на вопросы в котором послужили бы дополнительным пунктом обоснования востребованности разработки.

Гипотетически, потенциальным потребителем рассматриваемого продукта является пользователь АСУ ТП, использующий или планирующий использовать удаленные точки ввода-вывода, считающий, что на его АСУ

возможна направленная кибератака, которая может привести к ущербу работе предприятия, а также неудовлетворенный стоимостью или функционалом используемых средств ИБ АСУ ТП.

Для выявления потенциальных потребителей относительно вышеуказанных положений по методу Customer Development сформирован следующий список вопросов:

1. Считаете ли Вы использование удаленных точек-ввода вывод подходящим решением для Вашей АСУ ТП?

2. Насколько вероятной Вы считаете кибератаку на ваш комплекс АСУ?

3. Были ли зафиксированы факты неправильной аутентификации или направленные атаки на АСУ ТП предприятия?

4. Насколько часто происходят подобные инциденты?

5. Какие организационные меры используются для предотвращения подобных инцидентов?

6. Какие ПАК ИБ АСУ ТП используются на Вашем предприятии?

7. Насколько высокой Вы считаете стоимость используемых средств ИБ по отношению к возможному ущербу при направленной кибератаке?

8. Насколько Вы удовлетворены работой данных программно-аппаратных комплексов в рамках специфики Вашего предприятия?

9. Насколько необходимыми Вы считаете установку дополнительных средств защиты помимо используемых?

10. Какая организационная работа проводится с персоналом для приобретения компетенций, необходимых для обеспечения информационной безопасности предприятия?

Указанные вопросы могут быть использованы для выявления потенциального покупателя продукта в будущем, поскольку информация, выявляемая с помощью данных вопросов, касается информационный безопасности предприятия и регламентируется Федеральным законом № 149-ФЗ от 27 июля 2006 г. и может быть получена при работе с корпоративными клиентами от лица организации-работодателя [29].

Кроме факта активной уязвимости, подтверждающего актуальность разработки и возможную востребованность пользователями АСУ ТП, эксперты по информационной безопасности заявили о возросшем в 2021 г. количестве кибератак на объекты критической инфраструктуры, что позволяет предположить увеличение спроса на отечественные средства информационной безопасности (в том числе в сфере АСУ ТП) и востребованность настоящей разработки государственными структурами [9].

Потенциальным потребителем предлагаемого устройства может быть любое предприятие РФ, использующее хотя бы один программируемый логический контроллер при построении и эксплуатации локальной системы управления с возможностью дистанционной приемо-передачи информации. В основном уязвимости ИБ и отсутствие сегментирования сетей характерны для средних предприятий: штат до 300 человек, сфера деятельности – обработка и производство, форма собственности коллективная, доход не более 2 млрд. руб., предприятия сосредоточены в европейской части РФ [30].

3.4 Объем и емкость рынка

Поскольку для точного определения количества ПЛК в РФ необходимо проводить дорогостоящее коммерческое исследование рынка ПЛК, заключающееся в анализе всего ассортимента производителей и поставщиков ПЛК, импорта, экспорта и уже имеющейся продукции, то принято решение провести косвенную оценку рынка ПЛК по данным из открытых источников. В соответствии с данными аналитиков DISCOVERY Research Group объем рынка ПЛК в РФ на 2018 г. составил 76 996 шт., причем темп прироста объема рынка составил -2% натурального объема рынка по сравнению с 2017 г. [31]. Примем данный показатель для косвенного расчета рынка ПЛК на 2022 г.:

$$Q_{22} = Q_{18} \cdot \gamma^4, \quad (4)$$

где

Q_{18} - натуральный объем рынка ПЛК на 2018 г;

γ - коэффициент роста рынка ПЛК.

$Q_{22} = 79996 \cdot (1 - 0,02)^4 \approx 73786.$

На данный момент по данным ресурса INNI.INFO в РФ 4097 компаний, разрабатывающих и поставляющих АСУ ТП, каждая из которых может приобрести как минимум один ПЛК для применения его в новом проекте автоматизации какого-либо производства [32]. Предположим, что для разработки нового проекта приемлемо использовать удаленный ввод-вывод информации АСУ ТП. Тогда для обеспечения безопасного удаленного обмена информацией компания может также приобрести устройство, рассматриваемое в данной работе.

В таком случае потенциальная емкость рынка по формуле 5:

$$E_{p(n)} = Q_{22} \cdot C, \quad (5)$$

где

C - стоимость продукта.

$E_{p(n)} = 73786 \cdot 17720 = 1307,49$ млн. руб.

Данное количество средств представляет теоретическую выручку от продажи готового устройства компаниям-потребителям, которые посредством применения устройства в проекте передадут его в пользование конечному потребителю-пользователю АСУ ТП.

Кроме того, возможна модернизация таких уже использующих АСУ ТП объектов, как котельные, насосные станции, водоочистные сооружения, пищевые комбинаты, химические и металлургические заводы, нефтегазовые объекты и т.п.

Потенциальными потребителями продукта являются средние либо крупные предприятия, поскольку в большинстве случаев объем и сложность производства какого-либо продукта определяет сложность информационной системы и объем обрабатываемых информационных потоков.

По данным Федеральной службы государственной статистики, в РФ с 2014 по 2017 гг. количество крупных и средних предприятий изменилось с 58959 до 51986 с указанной в таблице 8 закономерностью [33]:

Таблица 8 – Динамика количества средних и крупных предприятий в РФ

Период	Кол-во предприятий	Коэффициент роста, %
2014	58959	0
2015	57392	-2,66
2016	54994	-4,18
2017	51986	-5,47

Для прогноза количества средних и крупных предприятий в РФ возьмем усредненный коэффициент роста:

$$\gamma_{ср} = \frac{(-2,66 - 4,18 - 5,47)}{3} \approx 4,1.$$

Косвенно получим количество крупных и средних предприятий в РФ на 2022 г. по формуле 6:

$$N_{22} = N_{17} \cdot \gamma_{ср}{}^{5}, \quad (6)$$

где

N_{17} - количество крупных и средних предприятий на 2017 г.

$$N_{22} = 51986 \cdot (1 - 0,041)^{5} \approx 42168.$$

Предположим, что каждое из рассматриваемых предприятий использует хотя бы один ПЛК. В таком случае при модернизации производства потенциальная емкость рынка:

$$E_{р(м)} = 42168 \cdot 17720 = 747,22 \text{ млн.руб.}$$

Общая потенциальная емкость рынка:

$$E_{р(о)} = E_{р(п)} + E_{р(м)} = 1307,49 + 747,22 = 2,054 \text{ млрд.руб.}$$

3.5 Анализ современного рынка и перспектив развития отрасли

По мнению экспертов, рынок средств информационной безопасности АСУ ТП является одним из важнейших направлений защиты информации. В течение 2021 г. в Банк данных ФСТЭК России было передано 120 уязвимостей [34], а в 2020 г. было проведено исследование, в результате которого было выявлено, что 70% уязвимостей в АСУ ТП по всему миру могут быть использованы удаленно [35]. Актуальный и пока не переполненный рынок привлекает новые решения и инвестиции, в связи с чем специалисты исследовательской компании MarketsandMarkets прогнозируют увеличение рынка средств безопасности АСУ ТП до $22.5 млрд к 2025 г. [36]. Траты как на улучшение защищенности отдельных систем, так и на решение последствий уже произошедших инцидентов кибербезопасности контуров, которые не были своевременно защищены, в условиях увеличивающегося количества кибератак на АСУ ТП невозможно преувеличить.

Современное сообщество специалистов АСУ ТП следуют таким трендам, как эшелонированная защита, безопасная программная среда и централизованное управление системой защиты и расследование инцидентов информационной безопасности. Специалисты группы компаний InfoWatch дают объемное описание каждого из них [13].

Первый тренд заключается в том, что защита АСУ ТП должна быть многоступенчатой. Предполагается разделение технологической и корпоративной сетей с использованием нескольких сетевых экранов. Таким образом, при попытке атаковать систему нарушитель или вредоносное ПО столкнется с разнородной защитой, что позволит снизить вероятность поражения защиты системы независимыми векторами заражения. Из этого можно сделать вывод, что увеличение количества наложенных средств защиты улучшает комплексную защищенность АСУ ТП.

Безопасная программная среда предполагает контроль запускаемых в АСУ ТП приложений и ввода информации непосредственно на рабочую станцию оператора. По данным компании Bulletproof, нарушителю достаточно

нескольких десятков миллисекунд для атаки общедоступное работающее приложение, а ряд вредоносных программ распространяется посредством USB-носителей. Из этих положений следует, что требуется введение ограничений на запуск необязательных приложений, а также на физический ввод информации в АСУ ТП. В этом случае возможной мерой является введение удаленного доступа к АСУ ТП по разрешенным протоколам, которые, тем не менее, стоит оснащать отдельными средствами защиты в соответствии с первым трендом.

Третий тренд предполагает осуществление анализа всего происходящего в промышленной сети. Возможным дополнением к централизованной системе отслеживания нарушений и аномалий могут стать программно-аппаратные модули, установленные в отдельных узлах сети и отслеживающие изменения сетевого трафика непосредственно в этих узлах. Данная информация уже будет транслироваться в какой-либо центральный модуль сбора сведений или на рабочую станцию специалиста по информационной безопасности для формирования логики управления безопасностью системы.

Основными игроками на рынке средств информационной безопасности в РФ являются такие компании, как «Лаборатория Касперского», Positive Technologies и «Уральский Центр Систем Безопасности». Только отечественные решения в полной мере отвечают обязательным требованиям законодательства информационной безопасности АСУ ТП в РФ [12].

Таким образом, при увеличении числа угроз кибербезопасности, малой насыщенности рынка и развитии технологических трендов рынок средств информационной безопасности проявляет тенденции к расширению и наполнению.

3.6 Расчет себестоимости продукта

Себестоимость продукта формируется исходя из затрат на патентование, затрат на радиоэлектронные и монтажные компоненты, а также заработной платы специалистов, задействованных в проекте, аренды помещения и стоимости оборудования.

На производство одного экземпляра устройства уходит около 15 часов. При количестве рабочих часов в 2023 г. по производственному календарю в 1973 ч. при 8-часовой рабочем дне возможно произвести 131 устройство [37]. Примем план производства на первый год равным 100 устройств.

Стоимость комплектующих и расходных материалов составляет 5391 руб. на один экземпляр, для 100 экземпляров за год потребуется 539,1 тыс. руб.

Заработная плата инженера-программиста в среднем по томской области равна 44631 руб. в месяц, менеджера – 37998 руб. в месяц, годовые затраты на заработную плату составляют 991,55 тыс. руб.

Аренда производственного помещения 31 кв. м. с учетом коммунальных услуг составляет 15 тыс. руб. в месяц, годовая аренда составит 180 тыс. руб. [38].

Стоимость оборудования для работы инженера и менеджера со сроком эксплуатации 3 года составляет 61,3 тыс. руб.

Рассмотренные статьи расходов представлены в таблице 9.

Таблица 9 – Годовые расходы на производство продукта

Статья расходов	Сумма, тыс. руб.
Комплектующие и расходные материалы	539,10
Оплата труда	991,55
Начисления на оплату труда (30% от ОТ)	297,47
Аренда помещения	180,00
Оборудование	61,30
Итого	2069,42

Таким образом, себестоимость одного экземпляра устройства составит 20,69 тыс. руб.

3.7 Производственный план и план продаж

Как было описано ранее, себестоимость одного экземпляра устройства составила 20,69 тыс. руб. Примем наценку равной 20%, в таком случае стоимость

устройства составит 24,83 тыс. руб. и прибыль от продажи 100 устройств составит:

$$R_1 = (24,83 - 20,69) \cdot 100 = 414 \text{ тыс. руб.}$$

Данная сумма будет принята как план продаж на первый год функционирования стартапа.

Отводимое на изготовление одного устройства количество времени (20 ч.) позволит штатному инженеру отладить процесс адаптации исполняемого кода к АСУ заказчика и уменьшить время разработки до 12 ч. без потери комфорта, что позволит увеличить план продаж на второй год до 150 устройств. При повышении затрат на комплектующие себестоимость устройства составит 15,59 тыс. руб. и в таком случае наблюдается увеличение плана продаж:

$$R_2 = (15,59 \cdot 1,2 - 15,59) \cdot 150 = 468 \text{ тыс. руб.}$$

В дальнейшем увеличение производительности стоит производить только при найме второго инженера-программиста. В таком случае затраты увеличатся до 2127,43 тыс. руб. в год, а производственный план возможно увеличить до 300 единиц устройства. В таком случае годовые затраты увеличатся до 3873,82 тыс. руб., себестоимость устройства уменьшится до 12,91 тыс. руб. и при прежней наценке в 20% увеличение плана продаж составит:

$$R_3 = (12,91 \cdot 1,2 - 12,91) \cdot 300 = 775 \text{тыс. руб.}$$

3.8 Конкурентные преимущества создаваемого продукта

Устройство предназначено для прямого анализа и контроля трафика технологической сети и, как следствие для повышения защищенности АСУ ТП. Прямых аналогов предлагаемой разработки на данный момент нет, однако на рынке средств информационной безопасности АСУ представлены такие ПАК, как Kaspersky Industrial CuberSecutiry (KICS), PT Industrial Security Incident Manager (PT ISIM), DATAPK, IKS1000GP от АПРОТЕХ и ИТЭЛМА и т.п. Подобные ПАК разделяются на наложенные и встроенные средства защиты информации, отличаясь друг от друга отношением к целевой АСУ ТП –

наложенные средства устанавливаются вендором для защиты уже ранее построенной АСУ ТП, а встроенные средства поставляются в комплекте с прочими подсистемами и компонентами АСУ ТП.

Несмотря на то, что рассматриваемое в настоящей работе устройство не является прямым аналогом представленных на рынке средств защиты информации АСУ ТП ПАК, возможно провести конкурентный анализ по отдельным статьям.

Для анализа приняты такие решения, как KICS for Networks, UserGate X10, PT ISIM. Сравнение проводилось по таким пунктам, как принцип работы с трафиком, поддержка протокола Modbus, стоимость, наличие алгоритмов анализа трафика и фильтрации трафика, а также тип средства и внесено в таблицу 10.

Таблица 10 – Конкурентный анализ средств информационной защиты АСУ ТП

	KICS for Networks	UserGate X10	PT ISIM	Разрабатываемое устройство
Принцип работы с трафиком	Обработка копии трафика	Прямой контроль трафика	Обработка копии трафика	Прямой контроль трафика
Поддержка протокола Modbus	Поддерживается	Поддерживается	Поддерживается	Поддерживается
Наличие алгоритмов анализа трафика	Интеллектуальные алгоритмы анализа трафика и обнаружения аномалий	Алгоритм блокировки трафика с отдельного источника	Интеллектуальный анализ событий в сети	Алгоритм анализа, контроля и фильтрации трафика
Стоимость	ок. 100 тыс. руб.	-	-	24,83 тыс. руб.
Тип средства защиты	Наложенное средство	Встроенное средство	Наложенное средство	Встроенное средство

Поскольку особенности лицензирования представленных выше продуктов предполагают предоставление цены по запросу, то стоимость базовых комплектаций Usergate X10 и PT ISIM неизвестна.

Представленная выше таблица позволяет сделать вывод, что наложенные средства защиты работают с копией трафика, что вносит дополнительную задержку при анализе возможного нарушения, а также не воздействует на вредоносный трафик напрямую. В свою очередь наложенное средство Usergate X10 не имеет алгоритмов анализа и позволяет только блокировать или разрешать трафик с определенного источника.

Таким образом, преимуществами разрабатываемого устройства являются прямой контроль сетевого трафика и наличие алгоритма анализа и фильтрации запросов. Также разработка потенциально дешевле, поскольку имеет более узконаправленные функции и область применения.

3.9 Бизнес-модель проекта

Для графического отражения сути и оценки основных факторов деятельности проекта была составлена бизнес-модель по А. Остервальдеру [39]. Построенная модель отражена в приложении Г.

3.10 Стратегия продвижения продукта на рынок

Исходя из описанных ранее целевых сегментов потребителей, а также специфики рынка, наиболее удобными для продвижения продукта признаны следующие методы работы с клиентами:

— email-маркетинг;

— прямые продажи;

— работа в поисковых системах, контекстная реклама.

Для дополнительного продвижения продукта возможно посещение тематических научно-практических выставок и конференций, посвященных АСУ ТП и информационной безопасности для привлечения возможных клиентов и дополнительного продвижения технологии.

4 Социальная ответственность

Введение

Настоящая работа включает в себя проектирование устройства-модуля информационной безопасности АСУ ТП, позволяющего увеличить степень защищенности АСУ ТП при удаленной приемо-передаче технологической информации. Потенциальные пользователи разрабатываемого устройства – обслуживающий персонал АСУ ТП – инженеры АСУ ТП, инженеры-программисты, монтажники и т.д. Устройство разрабатывается в лабораторных условиях (площадь лаборатории 6 × 8 м). Устройство предназначается для осуществления автоматического анализа, контроля и фильтрации сетевого трафика при использовании конкретного прикладного протокола взаимодействия – на данном этапе рассматривается протокол Modbus RTU.

При разработке используются персональный компьютер и отладочная плата, расположенные в лаборатории. Рабочий процесс заключается в сборке схемы и тестировании устройства на монтажной плате, а также в разработке программного обеспечения устройства на языке Си.

В данном разделе также рассматриваются вопросы производственной и пожарной безопасности, охраны окружающей среды и эргономики.

4.1 Правовые и организационные вопросы обеспечения безопасности

4.1.1 Правовые нормы трудового законодательства

Такие положения взаимодействия сотрудника и организации, как режим рабочего времени, оплата труда перерывы в работе, выходные и нерабочие дни и пр., описаны в ТК РФ [40].

Максимальная продолжительность рабочего времени составляет 40 часов в неделю, также на протяжении рабочего дня работнику должен быть предоставлен перерыв не менее 30 минут и не более 2 часов для отдыха и принятия пищи.

Описанная работа, может быть определена как производимая сидя или стоя при незначительном физическом напряжении, следовательно. Тестирование

устройства на отладочной плате Pinboard RII является работой с электронным устройством малых габаритов и весом до 0.5 кг и персональным компьютером. Исходя из этого, данная деятельность может быть оценена второй категорией тяжести труда (IIа).

В соответствии с ТК РФ максимальная длительность непрерывной работы с персональным компьютером составляет 2 часа, и при второй категории тяжести труда работник должен иметь 2 перерыва по 15 минут – через 2 часа после начала рабочего дня и через 2 часа после обеденного перерыва.

4.1.2 Основные эргономические требования к компоновке рабочей зоны

Для разработки программной части и тестирования корректности работы алгоритма устройства используется персональный компьютер. При этом рабочее место должно соответствовать ГОСТ 12.2.032-78 «Система стандартов безопасности труда (ССБТ). Рабочее место при выполнении работ сидя. Общие эргономические требования» [41].

При необходимости подключения персонального компьютеру к корпоративной сети или подключения отладочной платы к персональному компьютеру необходимо произвести подключение устройств Etheret- или USB-кабелем. При этом данные процессы должны производиться при соблюдении ГОСТ 12.2.033-78 «Система стандартов безопасности труда (ССБТ). Рабочее место при выполнении работ стоя. Общие эргономические требования» [42].

4.2 Производственная безопасность

В соответствии с ГОСТ 12.0.003-2015 были определены вредные и опасные факторы, характерные для проводимых работ [43]. Данные занесены в таблицу 11.

Таблица 11 – Возможные опасные и вредные производственные факторы на рабочем месте инженера-программиста

Факторы (ГОСТ 12.0.003-2015)	Нормативные документы
Опасные и вредные производственные факторы, связанные со световой средой (некогерентными неионизирующими излучениями оптического диапазона электромагнитных полей) и характеризуемые чрезмерными (аномальными относительно природных значений и спектра) характеристиками световой среды, затрудняющими безопасное ведение трудовой и производственной деятельности	СП 52.13330.2016 Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95.
Физические статические перегрузки, связанные с рабочей позой	МР 2.2.9.2128-06 Комплексная профилактика развития перенапряжения и профессиональных заболеваний спины у работников физического труда.
Умственное перенапряжение, в том числе вызванное информационной нагрузкой	МР 2.2.9.2311-07. Состояние здоровья работающих в связи с состоянием производственной среды. Профилактика стрессового состояния работников при различных видах профессиональной деятельности.
Опасные и вредные производственные факторы, связанные с аномальными микроклиматическими параметрами воздушной среды на местонахождении работающего	ГОСТ 12.1.005-88. ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны.
Опасные и вредные производственные факторы, связанные с электрическим током, вызываемым разницей электрических потенциалов, под действие которого попадает работающий	ГОСТ 12.1.019-2017. ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты (с Поправкой). ГОСТ 12.1.038-82. ССБТ. Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов.

4.2.1 Отсутствие и недостатки искусственного освещения

Недостаточная освещенность рабочей зоны возникает из-за недостатка искусственного освещения в лаборатории и над столами с персональными компьютерами в частности.

Недостаточная освещенность опасна для работника увеличением зрительной нагрузки, что приводит к ухудшению зрения и головной боли, снижая общую работоспособность.

Средствами увеличения освещенности являются дополнительные осветительные приборы.

В соответствии с СП 52.13330.2016 приведена таблица 12 с допустимыми значениями освещенности [44].

Таблица 12 – Требования к освещению помещений промышленных предприятий

Искусственное освещение				
Освещенность, лк			Сочетание нормируемых величин объединенного показателя дискомфорта UGR и коэффициента пульсации	
При комбинированном освещении		При системе общего освещения	UGR, не более	$K_{п}$, %, не более
всего	от общего			
–	–	300	25	20

4.2.2 Физические статические перегрузки, связанные с рабочей позой

Данный фактор вызван длительным специфическим расположением работника относительно объекта исследования.

Длительное положение в одной рабочей позе со временем приводит к развитию заболеваний опорно-двигательного аппарата (остеохондроз, радикулит, фиброзы и т.д.) и сердечно-сосудистой системы (гипертония, атеросклероз).

Факт возможных физических статических перегрузок ввиду поддержания рабочей позы в соответствии с МР 2.2.9.2128-06 [45] подтверждает количество времени, проводимое в специфической позе – работник более 25% рабочего времени проводит в поддержании рабочей позы (в данном случае – сидя за рабочим столом и персональным компьютером).

В качестве профилактики развития профессиональных заболеваний, вызванных длительным поддержанием рабочей позы, рекомендуется во время установленных в течение рабочего дня перерывов менять положение тела, а также уделять 5-10 минут суставной разминке шеи и плечевого пояса.

4.2.3 Умственное перенапряжение

Умственное перенапряжение связано с разработкой программных модулей и алгоритмов ПО микроконтроллера.

Длительное умственное перенапряжение приводит к стрессовым проявлениям (неврозы, нарушения концентрации и сна).

В качестве профилактики подобных проявлений в соответствии с МР 2.2.9.2311-07 [46] работнику рекомендуется иметь ранее упомянутые перерывы в работе со сменой деятельности и суставной разминкой.

4.2.4 Отклонение показателей микроклимата

В рассматриваемых условиях к отклонению показателей микроклимата приводят перемещение человека по лаборатории, перемещение предметов (кабели, отладочная плата) и проведение работ с ними стоя или сидя и т.д. При энергозатратах подобной деятельности в 151 – 200 ккал/ч нарушения показателей микроклимата могут отрицательно отразиться на состоянии организма работника.

Продолжительная работа при отклонении показателей микроклимата, связанная с передвижением и перемещением объектов, со временем может привести к травмам и заболеваниям опорно-двигательной системы

(миофиброзы, растяжения и т.д.), периферической нервной системы (координаторные неврозы, невриты и т.д.).

Во избежание подобных последствий необходимо обеспечивать стабильные допустимые параметры микроклимата в соответствии с ГОСТ 12.1.005-88 [47]. Оптимальные параметры микроклимата приведены в таблице 13.

Таблица 13 – Оптимальные и допустимые величины показателей микроклимата на рабочих местах

Период года	Категория работ	Температура, °С					Относительная влажность, %		Скорость движения, м/с	
		оптимальная	допустимая				оптимальная	допустимая на рабочих местах постоянных и непостоянных, не более	оптимальная, не более	допустимая на рабочих местах постоянных и непостоянных
			верхняя граница		нижняя граница					
			на рабочих местах							
			постоянных	непостоянных	постоянных	непостоянных				
Холодный	Средней тяжести - IIа	18-20	23	24	17	15	40-60	75	0,2	Не более 0,3
Теплый	Средней тяжести - IIа	21-23	27	29	18	17	40-60	65 (при 26 °С)	0,3	0,2-0,4

В нормальных условиях рабочая среда отвечает данным показателям.

Для поддержания температуры в помещении в холодный период года используется отопление, для регуляции скорости движения и влажности воздуха следует использовать специализированные увлажнители и проветривать помещение.

4.2.5 Поражение электрическим током

При работе с персональным компьютером и отладочной платой в случае их неисправности или ошибки работника (неплотно соединенные контакты, поврежденные соединительные провода, короткое замыкание) может произойти поражение электрическим током.

Поражение электрическим током может привести к ожогу, судорожным сокращениям мышц, химическому разложению крови и механическому повреждению тканей.

В соответствии с ГОСТ 12.1.038-82 [48] в таблице 14 приведены предельно допустимые значения силы тока и напряжения прикосновения.

Таблица 14 – Предельно допустимые значения силы тока и напряжения прикосновения

Род тока	U, В	I, мА
	не более	
Переменный, 50 Гц	2,0	0,3
Переменный, 400 Гц	3,0	0,4
Постоянный	8,0	1,0

Поскольку сфера деятельности работника, чья квалификация должна соответствовать инженеру-программисту с упором в разработку ПО, ограничена работой с персональным компьютером (без его обслуживания) и отладочной платой, компоненты которой в момент работы не находятся под напряжением, то в соответствии с Приказом министерства труда и социальной защиты Российской федерации от 15.12.2020 N 903н [49] работнику должна быть присвоена I группа электробезопасности, что должно быть зафиксировано в соответствующем журнале инструктажа по электробезопасности.

Также необходимо определить категорию помещения по электробезопасности. В соответствии с ПУЭ [50] категория помещения лаборатории определена 1 категорией.

Мерами защиты при работе с электроприборами в данном случае служат устройства защитного заземления, автоматического отключения, контроля и сигнализации.

4.3 Экологическая безопасность

Данный раздел содержит описание факторов влияния проектирования устройства и разработки ПО на окружающую среду, а также источников ее загрязнения, возникающих в процессе работы.

4.3.1 Влияние объекта исследования на селитебную зону

При разработке проектного решения возможна неправильная утилизация неисправных компонентов персонального компьютера и радиоэлектронных компонентов, в результате чего компоненты, содержащие токсичные вещества (конденсаторы и пр.), а также физические фракции (корпуса, оболочки компонентов) могут попасть на жилые территории

4.3.2 Влияние объекта исследования на атмосферу

При производстве электронных комплектующих для персональных компьютеров и радиоэлектронных компонентов для проектируемого на отладочной плате устройства возникают побочные продукты производства, загрязняющие атмосферу. В соответствии с ГОСТ Р 58577-2019 [51] законодательно установлены ограничения на допустимое количество выбросов.

Также загрязнение атмосферы происходит за счет выбросов углекислого газа и прочих продуктов горения во время производства электроэнергии для питания персонального компьютера и отладочной платы соответственно. Электроснабжение корпуса университета осуществляется ТЭЦ-1 с мощностью 14,7 МВт. В соответствии с Постановлением Правительства РФ от 31 декабря 2020 г. N 2398 [52] данный объект относится ко второй (II) категории.

4.3.3 Влияние объекта исследования на гидросферу

Негативное влияние объекта исследования на гидросферу может произойти при неправильной утилизации компонентов персонального компьютера или радиоэлектронных компонентов. При неправильной утилизации (захоронении или утилизации вместе с бытовыми отходами) компоненты могут попасть в сточные, речные и грунтовые воды.

Для снижения вредоносного влияния объекта исследования на гидросферу необходимо сдавать вышедшие из строя компоненты в специализированные приемные пункты, из которых утилизированный продукт пойдет либо на переработку, либо на вторичное использование.

4.3.4 Влияние объекта исследования на литосферу

При неправильной утилизации компоненты электрооборудования, содержащие токсичные вещества или представляющие собой крупную фракцию отходов, могут попасть в почву. Необходимо сдавать электронные компоненты в специализированные пункты приема, откуда компоненты либо пойдут на вторичное использование, либо на переработку методом пиролиза, биометаллургии, электростатической сепарации и т.д.

4.4 Безопасность в чрезвычайных ситуациях

4.4.1 Анализ вероятных ЧС, которые может спровоцировать объект исследований

При разработке устройства на отладочной плате и при работе с персональным компьютером в лаборатории могут произойти такие чрезвычайные ситуации, как пожар вследствие короткого замыкания или контакта легковоспламеняющегося материала с выходами компонентов, находящимися под напряжением. Возникновение других ЧС техногенного характера маловероятно.

4.4.2 Обоснование мероприятий по предотвращению ЧС

Возможный пожар определен классом Е, поскольку возможно возгорание находящейся под напряжением цепи питания персонального компьютера.

При возникновении пожара вследствие короткого замыкания или другой неисправности электрооборудования необходимо воспользоваться углекислотными огнетушителями ОУ-5, ОУ-10 или порошковым ОП-10 в зависимости от того, каким огнетушителем оборудована лаборатория.

Также для предотвращения пожара необходимо соблюдение корректного обращения с оборудованием и проведения уборки на рабочем месте после окончания рабочего дня. Помещение должно быть оборудовано планом эвакуации из здания. Путь эвакуации должен быть свободен.

Поскольку в лаборатории присутствуют стенды и мебель, выполненные из пластика, а также присутствуют электроприборы, то в соответствии с СП 12.13130.2009 [53] данное помещение определяется категорией «Г» (умеренная пожароопасность).

Также во избежание возникновения ЧС не следует проводить коммутацию радиоэлектронных компонентов при поданном на отладочную плату питании, при выходе из строя комплектующих персонального компьютера следует прекратить работу и сообщить о неисправности системному администратору.

При возникновении пожара и невозможности самостоятельно его ликвидировать следует позвонить по номеру 101 и сообщить о возгорании и месте его возникновения, после чего покинуть помещение в соответствии с планом эвакуации.

Вывод по разделу

В ходе выполнения данного раздела ВКР приведены основные нормативы, регламентирующие воздействие вредных и опасных факторов при разработке проектного решения. По итогам анализа выявлено, что при

нормальных условиях параметры рабочей зоны соответствуют установленным нормативам.

Определена категория помещения по электробезопасности – I категория.

Группа персонала по электробезопасности определена аналогично – I группа.

Определена категория тяжести труда – в соответствии с условиями производимые рабочие процессы характеризуются тяжестью труда категории IIа.

Также рабочее помещение характеризовано категорией «Г» (умеренная пожароопасность) в соответствии с условиями.

Поскольку при разработке проектного решения используется электроэнергия, то объектом, оказывающим самое значительное негативное воздействие на окружающую среду, является ТЭЦ-1, снабжающая электроэнергией корпус университета, данный объект характеризуется категорией II.

Таким образом, были определены основные характеристики рабочей зоны, которые были сравнены со значениями из нормативной документации, в результате чего сделан вывод, что все требуемые параметры находятся в пределах нормы.

Заключение

В ходе выполнения настоящей работы выполнен анализ состояния ИБ АСУ ТП в Российской Федерации, а именно ассортимент рынка СЗИ АСУ ТП, а также состав нормативного обеспечения, регулирующего организацию систем ИБ АСУ ТП в РФ. Сделан вывод, что на рынке СЗИ АСУ ТП отсутствуют прямые аналоги разрабатываемого устройства и концепция разработки оригинальна.

Проведен подбор компонентной базы: выбран целевой МК и интерфейсные микросхемы для обеспечения взаимодействия в сегменте технологической сети с использованием интерфейсов RS-485 и USB. Разработана электрическая принципиальная схема подключений компонентов устройства, подобрано корпусное исполнение. Разработаны структурная схема расположения устройства в сегменте технологической сети, а также первоначальный алгоритм анализа сетевого трафика Modbus RTU с соответствующей блок-схемой. Создан тестовый проект с несколькими разрешенными командами Modbus RTU для демонстрации работы алгоритма. Проведенная работа позволяет как непосредственно приступить к реализации экземпляров устройства для эксплуатации, так и выстроить план дальнейшей модернизации устройства.

Подготовлено несколько публикаций по теме работы для участия в конференциях РНТК ТомскНИПИнефть, МСИТ и SIBINFO-2022.

Представленная разработка в дальнейшем может быть модернизирована с расширением функционала устройства и обработки трафика реализации протокола Modbus TCP. Также планируется модернизация алгоритма для маскирования структуры ЛСУ. В соответствии с проведенным анализом рынка СЗИ АСУ ТП и тенденций кибербезопасности различных отраслей промышленности и объектов КИИ РФ разработка устройства является актуальной.

Conclusion

In the course of this work, an analysis of the state of the ICS in the Russian Federation, namely, the range of the automated control system information security tools market, as well as the composition of regulatory support regulating the organization of automated control system security systems in the Russian Federation, was carried out.

The selection of the component base was carried out: the target MC and interface chips were selected to ensure interaction in the segment of the technological network using RS-485 and USB interfaces. An electrical schematic diagram of the connections of the device components has been developed, a case design has been selected.

The selection of the component base was carried out: the target MC and interface chips were selected to ensure interaction in the segment of the technological network using RS-485 and USB interfaces. An electrical schematic diagram of the connections of the device components has been developed, a case design has been selected. A block diagram of the device location in the segment of the technological network has been developed, as well as an initial algorithm for analyzing Modbus RTU network traffic with an appropriate block diagram. A test project has been created with several allowed Modbus RTU commands to demonstrate the operation of the algorithm. The work carried out allows both to directly start implementing copies of the device for operation, and to build a plan for further modernization of the device. Several publications on the topic of work have been prepared for participation in the conferences of RSTC TomskNIPIneft, MSIT and SIBINFO-2022.

The presented development can be upgraded in the future with the expansion of the functionality of the device and traffic processing implementation of the Modbus TCP protocol. It is also planned to modernize the algorithm for masking the local control system structure. In accordance with the analysis of the market of SPI automated process control systems and trends in cybersecurity of various industries and facilities of the CII of the Russian Federation, the development of the device is relevant.

Список публикаций студента

1. Тутов, И. А. Устройство для отслеживания вредоносной и нежелательной активности в промышленных сетях Modbus RTU / И. А. Тутов, Я. В. Калинкин // Молодежь и современные информационные технологии сборник трудов XVIII Международной научно-практической конференции студентов, аспирантов и молодых учёных, 22-26 марта 2021 г., г. Томск: / Национальный исследовательский Томский политехнический университет, Инженерная школа информационных технологий и робототехники ; под ред. Н. Г. Маркова [и др.] . — Томск : Изд-во ТПУ , 2021 . — [С. 458-459] . — Заглавие с титульного экрана. — [Библиогр.: с. 459 (5 назв.)]..

2. Калинкин, Я. В.. Разработка компонента информационной безопасности контроллерного оборудования / Я. В. Калинкин, И. А. Тутов // Молодежь и современные информационные технологии сборник трудов XIX Международной научно-практической конференции студентов, аспирантов и молодых учёных, 21-25 марта 2022 г., г. Томск: / Национальный исследовательский Томский политехнический университет, Инженерная школа информационных технологий и робототехники ; ред. кол. А. Ю. Дёмин, Н. Г. Марков, В. Г. Спицын [и др.] . — Томск : Изд-во ТПУ , 2022 . — [С. 309-310] . — Заглавие с титульного экрана. — [Библиогр.: с. 310 (4 назв.)]..

Список использованных источников

1. Беспроводные локальные сети. – Текст : электронный // Энциклопедия АСУ ТП : сайт. – 2014. – URL: https://www.bookasutp.ru/Chapter2_11_1.aspx (дата обращения 06.05.2022).

2. МКОН преобразователь протокола Modbus. – Текст : электронный // Оборудование для автоматизации ОВЕН : официальный сайт. – 2022. – URL: https://owen.ru/product/mkon (дата обращения 27.04.2022).

3. Промышленные сети и интерфейсы. – Текст : электронный // Энциклопедия АСУ ТП – 2014. – URL: https://www.bookasutp.ru/Chapter2_1.aspx (дата обращения 27.04.2022).

4. Исследование: более 4000 устройств АСУ ТП уязвимы для удаленных атак. – Текст : электронный // INFOWATCH – 2021. – URL: https://www.infowatch.ru/resources/blog/issledovanie-bolee-4-000-ustroystv-asu-tp-uyazvimy-dlya-udalennykh-atak (дата обращения 05.05.2022).

5. «Лаборатория Касперского» назвала основные киберугрозы 2021 года. – Текст : электронный // Коммерсантъ – 2020. – URL: https://www.kommersant.ru/doc/4583939 (дата обращения 06.05.2022).

6. BDU:2019-02550: Уязвимость протокола Modbus микропрограммного обеспечения программируемых логических контроллеров, позволяющая нарушителю выполнить команды запуска, остановки, выгрузки и загрузки данных на устройстве. – Текст : электронный // Банк данных угроз безопасности информации – 2017. – URL: https://bdu.fstec.ru/vul/2019-02550 (дата обращения 05.05.2022).

7. Статистика. – Текст : электронный // Kaspersky ICS cert – 2022. – URL: https://ics-cert.kaspersky.ru/statistics/ (дата обращения 26.04.2022).

8. Ульянов Н. Интернет угрожает. – Текст : электронный // ЭкспертРУ – 2021. – URL: https://expert.ru/expert/2021/40/internet-ugrozhayet/ (дата обращения 27.04.2022).

9. Борисов заявил о росте числа кибератак на критическую инфраструктуру. – Текст : электронный // SecurityLab.ru by Positive Technologies.

– 2021. – URL: https://www.securitylab.ru/blog/company/orange/351713.php (дата обращения 19.05.2022).

10. Кибербезопасность систем промышленной автоматизации в 2019 году. – Текст : электронный // Kaspersky ICS. – 2019. – URL: https://ics.kaspersky.ru/media/Kaspersky-ARC-ICS-2019-Trend-Report-Ru.pdf (дата обращения 19.05.2022).

11. В ближайшие годы ожидается рост рынка безопасности АСУ ТП. – Текст : электронный // SecurityLab.ru by Positive Technologies. – 2021. – URL: https://www.securitylab.ru/news/516326.php (дата обращения 19.05.2022).

12. Небайкин М. Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств защиты. – Текст : электронный // ANTI-MALWARE – 2022. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review#part61 (дата обращения 27.04.2022).

13. Душа И. 3 тренда защиты информации АСУ ТП в 2021 году. – Текст : электронный // INFOWATCH. – 2021. – URL: https://www.infowatch.ru/resources/blog/special-project/3-trenda-zaschity-informatsii-asu-tp-v-2021-godu (дата обращения 07.05.2022).

14. Приказ ФСТЭК России N 31: дата введения 2014-03-14. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 27.04.2022). – Текст : электронны.

15. Приказ ФСТЭК России от 25 декабря 2017 г. N 239: дата введения 2017-01-25. – URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 06.05.2022). – Текст : электронный.

16. Плотников И. Обзор встроенных средств кибербезопасности АСУ ТП. – Текст : электронный // ANTI-MALWARE. – 2022. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/Built-in-ICS-cybersecurity-tools (дата обращения 06.05.2022).

17. Лего П. Обзор UserGate X10, промышленного файрвола для защиты сетей АСУ ТП. – Текст : электронный // ANTI-MALWARE. – 2022. – URL: https://www.anti-malware.ru/reviews/UserGate-X10 (дата обращения 07.05.2022).

18. Сетевой протокол – Modbus. – Текст : электронный // Справочник по АСУ ТП. – 2009. – URL: https://www.sites.google.com/site/asutpklub/-/promyslennye-seti/modbus (дата обращения 07.05.2022).

19. Как общаются машины: протокол Modbus. – Текст : электронный // Хабр. – 2019. – URL: https://habr.com/ru/company/advantech/blog/450234/ (дата обращения 07.05.2022).

20. В чем отличия интерфейсов RS-232, RS-422 и RS-485? – Текст : электронный // IPC2U. – 2022. – URL: https://ipc2u.ru/articles/prostye-resheniya/otlichiya-interfeysov-rs-232-rs-422-rs-485/ (дата обращения 07.05.2022).

21. Микроконтроллеры 8051, PIC, AVR и ARM: отличия и особенности. – Текст : электронный // DIGITRODE.RU. – 2018. – URL: http://digitrode.ru/computing-devices/mcu_cpu/1253-mikrokontrollery-8051-pic-avr-i-arm-otlichiya-i-osobennosti.html (дата обращения 22.05.2022).

22. FDD03-5S2, DC/DC преобразователь. – Текст : электронный // CHIPDIP. – 2022. – URL: https://www.chipdip.ru/product/fdd03-05s2 (дата обращения 22.05.2022).

23. Схемы стабилизаторов напряжения – разновидности и устройство. – Текст : электронный // ODSTROY. – 2020. – URL: https://odstroy.ru/shema-stabilizatora-naprazenia-mikroshema-impulsnyj-integralnyj-i-prostoj/ (дата обращения 22.05.2022).

24. D3MG, корпус на DIN-рейку. – Текст : электронный // CHIPDIP. – 2022. – URL: https://www.chipdip.ru/product/d3mg?from=suggest_product (дата обращения 22.05.2022).

25. AVR. Учебный курс. Работа на прерываниях. – Текст : электронный // EasyElectronics. – 2022. – URL: https://yandexwebcache.net/yandbtm?fmode=inject&tm=1654465827&tld=com&lang=ru&la=1652861952&text=http%3A//easyelectronics.ru/avr-uchebnyj-kurs-rabota-

na-preryvaniyax.html&url=http%3A//easyelectronics.ru/avr-uchebnyj-kurs-rabota-na-preryvaniyax.html&l10n=en&mime=html&sign=47fb4c7c812a8b203686eccf5e3d1215&keyno=0 (дата обращения 22.05.2022).

26. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4): дата введения 2006-12018. – URL: http://www.consultant.ru/document/cons_doc_law_34683/ (дата обращения 22.05.2022). – Текст : электронный

27. Федеральный закон «О внесении в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации»: дата введения 2014-03-12. – URL: http://www.consultant.ru/document/cons_doc_LAW_160073/ (дата обращения 24.05.2022). – Текст : электронный.

28. Федеральный закон «О внесении в часть четвертую Гражданского кодекса Российской Федерации»: дата введения 2020-07-20. – URL: http://www.consultant.ru/document/cons_doc_LAW_357759/ (дата обращения 24.05.2022). – Текст : электронный.

29. Федеральный закон «Об информации, информационных технологиях и о защите информации»: дата введения 2006-07-27. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 19.05.2022). – Текст : электронный.

30. Статистика. – Текст : электронный // СПАРК ИНТЕРФАКС. – 2021. – URL: https://spark-interfax.ru/statistics (дата обращения 24.05.2022).

31. Анализ рынка PLC (программируемые логические контроллеры) в России. – Текст : электронный // P-RELIZ. – 2019. – URL: https://p-reliz.ru/reliz/2019-03-01-analiz-ryinka-plc-programmiruemyie-logicheskie-kontrolleryi-v-rossii.html (дата обращения 15.05.2022).

32. INNI.INFO : сайт. – Москва. – Обновляется в течение суток. – URL: https://inni.info/site/АСУ_ТП (дата обращения 15.05.2022). – Текст : электронный.

33. Число крупных и средних предприятий и организация в РФ, 2004-2017. – Текст : электронный // Рациональный числа. – 2017. – URL: https://rationalnumbers.ru/all/chislo-krupnyh-i-srednih-predpriyatiy-i-organizaciy-v-rf-2004-20/ (дата обращения 19.05.2020).

34. Лаборатория кибербезопасности АСУ ТП компании «Ростелеком-Солар» за два года передала ФСТЭК России информацию о 120 уязвимостях. – Текст : электронный // Ростелеком-Солар. – 2021. – URL: https://rt-solar.ru/events/news/2263/ (дата обращения 19.05.2022).

35. Более 70% уязвимостей в АСУ ТП могут быть проэксплуатированы удаленно. – Текст : электронный // SecurityLab.ru by Positive Technologies. – 2020. – URL: https://www.securitylab.ru/news/511354.php (дата обращения 19.05.2022).

36. В ближайшие годы ожидается рост рынка безопасности АСУ ТП. – Текст : электронный // SecurityLab.ru by Positive Technologies. – 2021. – URL: https://www.securitylab.ru/news/516326.php (дата обращения 19.05.2022).

37. Производственный календарь на 2023 год. – Текст : электронный // КонсультантПлюс. – 2022. – URL: http://www.consultant.ru/law/ref/calendar/proizvodstvennye/2023/ (дата обращения 20.05.2022).

38. Аренда офисных помещений в Томске : сайт. – Томск. – Обновляется в течение суток. – URL: https://www.avito.ru/tomsk/kommercheskaya_nedvizhimost/sdam/ofis-ASgBAQICAUSwCNRWAUCeww0UhNk5 (дата обращения 20.05.2022). – Текст : электронный.

39. Бизнес-модель Остервальдера: что это такое? – Текст : электронный // vc.ru. – 2020. – URL: https://vc.ru/s/productstar/135102-biznes-model-ostervaldera-chto-eto-takoe (дата обращения 24.05.2022).

40. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 25.02.2022). – URL: http://www.consultant.ru/document/cons_doc_law_34683/ (дата обращения 22.05.2022). – Текст : электронный.

41. ГОСТ 12.2.032-78 Система стандартов безопасности труда. Рабочее место при выполнении работ сидя. Общие эргономические требования: дата введения 1979-01-01. URL: https://docs.cntd.ru/document/1200003913 (дата обращения 21.05.2022). – Текст : электронный.

42. ГОСТ 12.2.033-78 Система стандартов безопасности труда. Рабочее место при выполнении работ стоя. Общие эргономические требования: дата введения 1979-01-01. URL: https://docs.cntd.ru/document/1200005187 (дата обращения 21.05.2022). – Текст : электронный.

43. ГОСТ 12.0.003-2015 Система стандартов безопасности труда. Опасные и вредные производственные факторы. Классификация: дата введения 2017-03-01. URL: https://docs.cntd.ru/document/1200136071 (дата обращения 15.05.2022). – Текст : электронный.

44. СП 52.13330.2016. Естественное и искусственное освещение: дата введения 2017-05-08. URL: https://docs.cntd.ru/document/456054197 (дата обращения 22.05.2022). – Текст : электронный.

45. МР 2.2.9.2128-06 Состояние здоровья работающих в связи с состоянием производственной среды. Комплексная профилактика развития перенапряжения и профессиональных заболеваний спины у работников физического труда: дата введения 2006-11-01 – URL: https://docs.cntd.ru/document/1200047515 (дата обращения 21.05.2022). – Текст : электронный.

46. МР 2.2.9.2311-07. Состояние здоровья работающих в связи с состоянием производственной среды. Профилактика стрессового состояния работников при различных видах профессиональной деятельности: дата введения 2008-03-18 – URL: https://docs.cntd.ru/document/1200072234 (дата обращения 21.05.2022). – Текст : электронный.

47. ГОСТ 12.1.005-88 Система стандартов безопасности труда. Общие санитарно-гигиенические требования к воздуху рабочей зоны: дата введения 1989-01-01 – URL: https://docs.cntd.ru/document/1200003608 (дата обращения 21.05.2022). – Текст : электронный.

48. ГОСТ 12.1.038-82 Система стандартов безопасности труда. Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов: дата введения 1983-07-01 – URL: https://docs.cntd.ru/document/5200313 (дата обращения 21.05.2022). – Текст : электронный.

49. Приказ Минтруда России N 903н «Об утверждении Правил по охране труда при эксплуатации электроустановок»: дата введения 2022-12-15 – URL: https://docs.cntd.ru/document/573264184 (дата обращения 22.05.2022). – Текст : электронный.

50. Правила устройства электроустановок: дата введения 2003-01-01 – URL: https://docs.cntd.ru/document/1200030216?marker=7D20K3 (дата обращения 21.05.2022). – Текст : электронный.

51. ГОСТ Р 58577-2019 Правила установления нормативов допустимых выбросов загрязняющих веществ проектируемыми и действующими хозяйствующими субъектами и методы определения этих нормативов: дата введения 2020-01-01 – URL: https://docs.cntd.ru/document/1200168569 (дата обращения 22.05.2022). – Текст : электронный.

52. Постановление Правительства Российской Федерации N 2398 Об утверждении критериев отнесения объектов, оказывающих негативное воздействие на окружающую среду, к объектам I, II, III и IV категорий: дата введения 2020-12-32 – URL: https://docs.cntd.ru/document/573292854 (дата обращения 22.05.2022). – Текст : электронный.

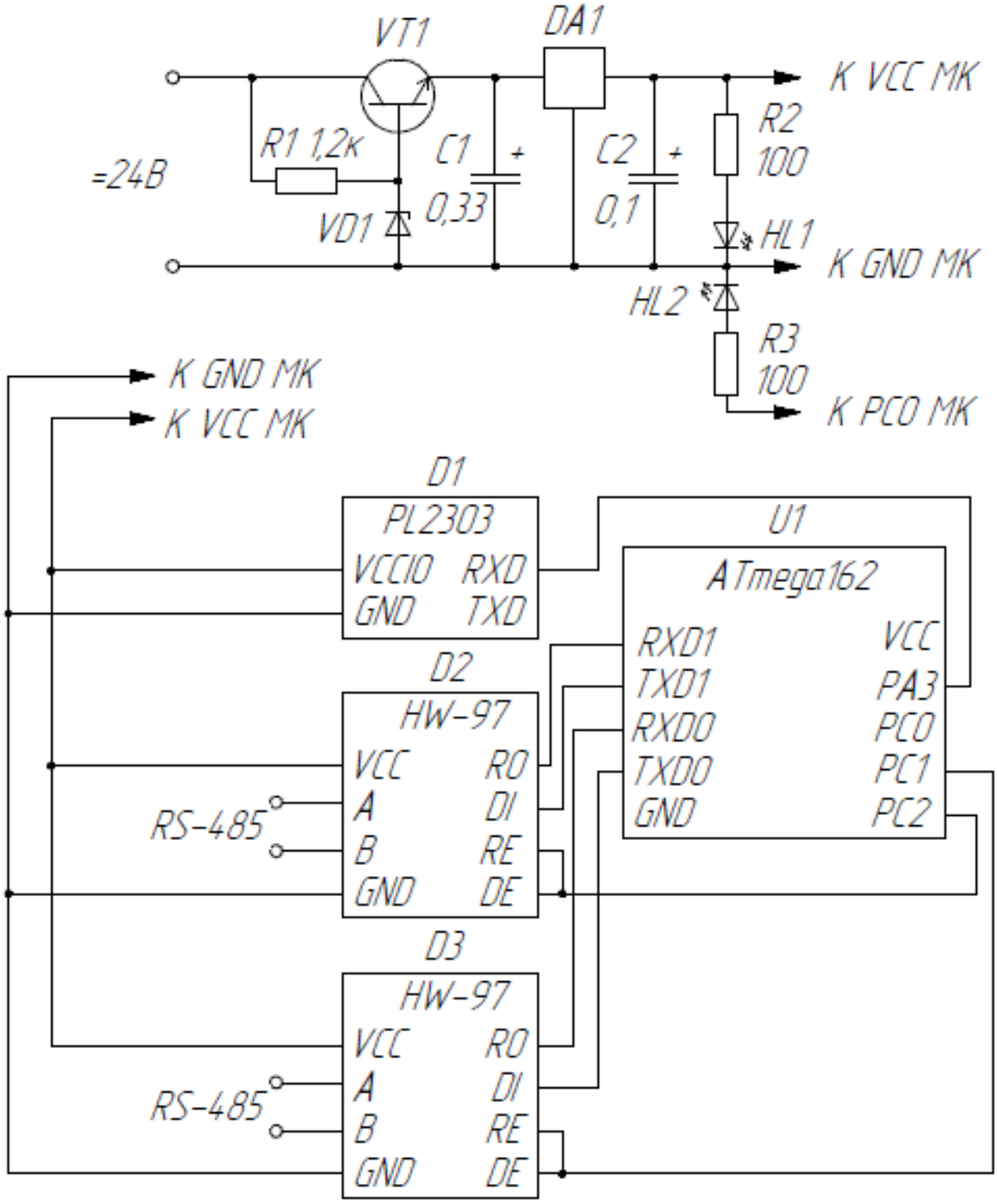
53. СП 12.13130.2009. Определение категорий помещений, зданий и наружных установок по взрывоопасной и пожарной опасности: дата введения 2009-05-01 – URL: https://docs.cntd.ru/document/1200071156 (дата обращения 22.05.2022). – Текст : электронный.

Приложение А

(Обязательное)

Схема электрическая принципиальная

ФЮРА.468332.001



Изм.	Лист	№ докум.	Подп.	Дата
Разраб.		Калинкин Я.В.		30.05
Пров.		Титов И.А.		
Т.контр.				
Н.контр.				
Утв.				

ФЮРА.468332.001

Подключение компонентов устройства

Лит.	Масса	Масштаб
У		
Лист	Листов 1	

Схема электрическая принципиальная

ТПУ ОАР ИШИТР гр. 8Т8Б

Перв. примен.

Справ. №

Подп. и дата

Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл.

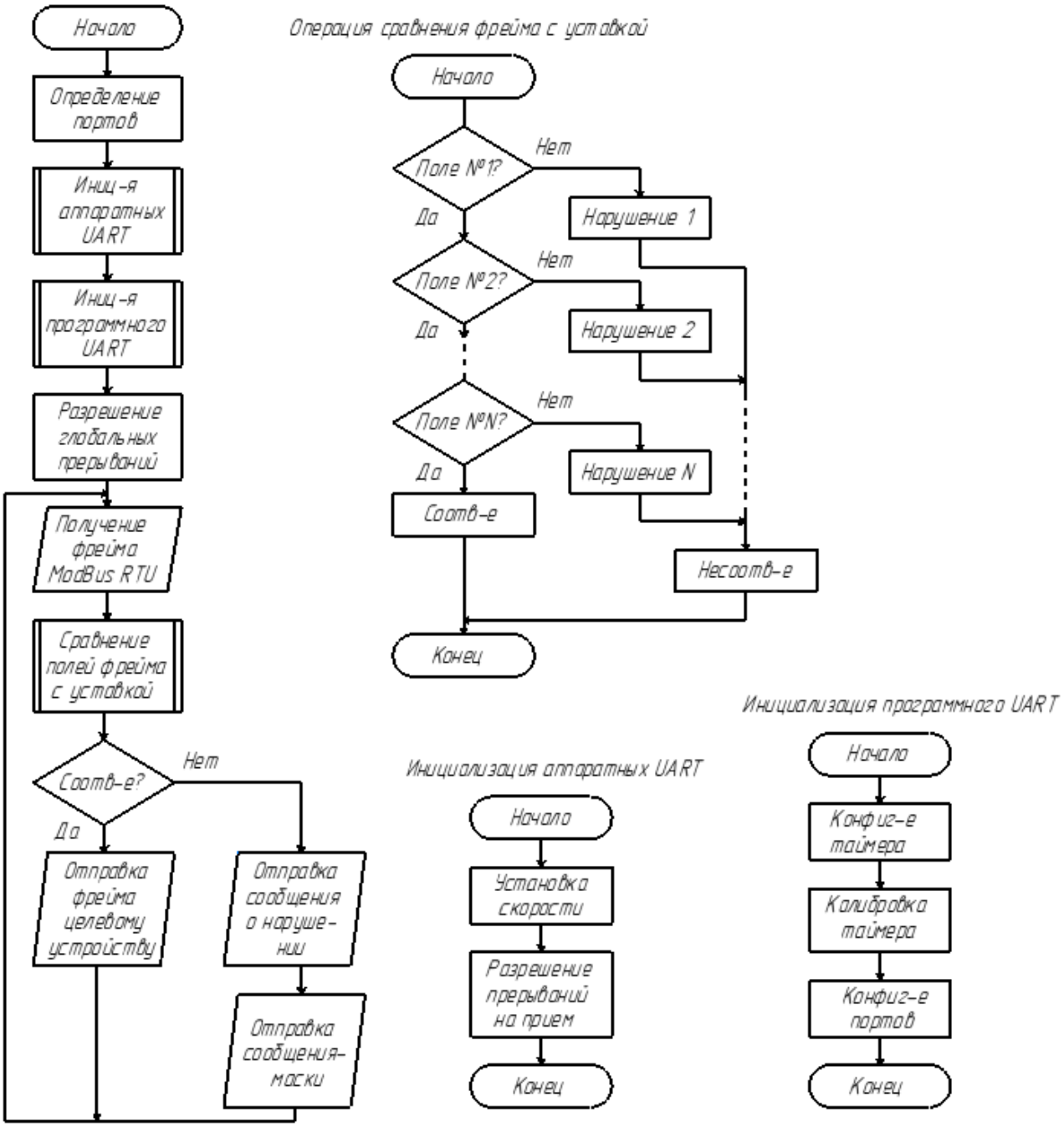
Копировал

Формат А4

Приложение Б

(Обязательное)

Блок-схема алгоритма



Приложение В

(Обязательное)

Исполняемый код для микроконтроллера

```
1. //Массивы с сообщениями
2. char message_MODBUS_RTU_01[34] = "Request to an unregistered
3. device!";
4. char message_MODBUS_RTU_02[36] = "The function code is not
5. registered!";
6. char message_MODBUS_RTU_03[33] = "Writing an unregistered
7. register!";
8. char message_MODBUS_RTU_04[41] = "The value of the writing is out
9. of range!";
10.   char message_MODBUS_RTU_05[22] = "Frame is damaged (CRC)";
11.
12.   //Переменные для обработки полученных данных и установления статуса
13.   проверки
14.   volatile uint8_t message_length = 0;
15.   volatile uint8_t message[8];
16.   volatile uint8_t ack_flag = 0;
17.   volatile uint8_t quantity = 0;
18.   volatile uint8_t index_1 = 0;
19.   volatile uint8_t data = 0;
20.   volatile uint8_t access_marker = 0;
21.   volatile uint8_t CRC16_order = 1;//Для порядка CRC: 0 - младшим
22.   вперед, 1 - старшим
23.
24.   // Инициализация программного UART
25.   void suart_init()
26.   {
27.         // Настройка таймера 1A
28.         TCCR1A = 0x00;
29.         TCCR1B |= (1 << CS10);
30.
31.         // Вычисление количества импульсов для отсчета времени
32.   полупериода t/2
33.         OCR1A = ((F_CPU/baudrate) / 2) - TIME_COM;
34.         TCNT1 = 0x00;
35.
36.         // Настройка портов
37.         SUART_DDR_TX |= (1 << SUART_PIN_TX);
38.         SUART_PORT_TX |= (1 << SUART_PIN_TX);
39.   }
40.
41.   // Пауза программного UART
42.   void suart_delay(uint8_t count)
43.   {
```

```
44.         // Обнуление регистра счета
45.         TCNT1 = 0x00;
46.
47.         // Сброс счетчика полупериодов
48.         pcount = 0x00;
49.
50.         // Стоим на месте пока не выйдет время
51.         while(pcount < count);
52.   }
53.
54.   // Передача байта
55.   void suart_tx(unsigned char data)
56.   {
57.         // Старт бит
58.         SUART_PORT_TX &= ~(1 << SUART_PIN_TX);
59.
60.         // Пауза
61.         suart_delay(2);
62.
63.         // Передача байта
64.         for(unsigned char i = 0; i < 8; i++)
65.         {
66.               if(((data >> i) & 0x01) != 0) // Если текущий бит 1
67.               {
68.                     SUART_PORT_TX |= (1 << SUART_PIN_TX);
69.               }
70.               else // Если текущий бит 0
71.               {
72.                     SUART_PORT_TX &= ~(1 << SUART_PIN_TX);
73.               }
74.               suart_delay(2);
75.         }
76.         // Стоп бит
77.         SUART_PORT_TX |= (1 << SUART_PIN_TX);
78.         suart_delay(2);
79.   }
80.
81.   // Передача строки
82.   void suart_tx_str(char str[])
83.   {
84.         sei();
85.         TIMSK |= (1 << OCIE1A);
86.         while (index_1 != message_length)
87.         {
88.               suart_tx(str[index_1]);
89.               index_1 = index_1 + 1;
90.         }
91.         index_1 = 0;
92.         TIMSK &= ~(1 << OCIE1A);
```

```
93.   }
94.
95.   //Команда симуляции записи состояния дискретного вывода
96.   void Command_DI_write(void) {
97.         if (message[4] == 0xFF)
98.         {
99.               switch (message[3])
100.              {
101.                    case 0x00: {
102.                          PORTC |= 0b00000001;
103.                    } break;
104.                    case 0x01: {
105.                          PORTC |= 0b00000010;
106.                    } break;
107.                    case 0x02: {
108.                          PORTC |= 0b00000100;
109.                    } break;
110.              }
111.        }
112.        else {
113.              switch (message[3])
114.              {
115.                    case 0x00: {
116.                          PORTC &= ~0b00000001;
117.                    } break;
118.                    case 0x01: {
119.                          PORTC &= ~0b00000010;
120.                    } break;
121.                    case 0x02: {
122.                          PORTC &= ~0b00000100;
123.                    } break;
124.              }
125.        }
126.  }
127.
128.  //Команда проверки соответствия поступившей команды
129.  void Command_check(void) {
130.        if (message[0] == 0x07)//Проверка адреса устройства
131.        {
132.              if (message[1] == 0x05)//Проверка кода функции
133.              {
134.                    if (message[2] == 0x0)//Проверка старшего байта
135.  адреса регистра
136.                    {
137.                          if (message[3] == 0x0 || message[3] == 0x01 ||
138.  message[3] == 0x02)//Проверка младшего байта адреса регистра
139.                          {
140.                                if (message[4] == 0x0 || message[4] ==
141.  0xFF)//Проверка старшего байта вводимого в регистр значения
```

```
142.                                {
143.                                      if (message[5] == 0x0)//Проверка
144. младшего байта вводимого в регистр значения
145.                                      {
146.                                            CRC16_Check();
147.                                      }
148.                                else {message_length = 41; ack_flag =4;}
149.                                }
150.                                else {message_length = 41; ack_flag =4;}
151.                          }
152.                          else {message_length = 33; ack_flag = 3;}
153.                    }
154.                    else {message_length = 33; ack_flag = 3;}
155. //Незадействованный регистр
156.              }
157.              else {message_length = 36; ack_flag = 2;}
158. //Необрабатываемая функция
159.        }
160.        else {message_length = 34; ack_flag = 1;}//Незадействованное
161. устройства
162.
163.        if (ack_flag == 0)//Если принято допустимое сообщение, то даем
164. разрешение на обработку команды
165.        {
166.              Command_DI_write();
167.        }
168. }
169.
170. void Send_message(void) { //Отправка сообщения
171.        if (index_1 < message_length-1)
172.        {
173.              switch (ack_flag)
174.              {
175.              case 0: data = message[index_1]; break;
176.              case 1: data = message_MODBUS_RTU_01[index_1]; break;
177.              case 2: data = message_MODBUS_RTU_02[index_1]; break;
178.              case 3: data = message_MODBUS_RTU_03[index_1]; break;
179.              case 4: data = message_MODBUS_RTU_04[index_1]; break;
180.              case 5: data = message_MODBUS_RTU_05[index_1]; break;
181.              }
182.              index_1 = index_1 + 1;
183.        }
184.        else
185.        {
186.              switch (ack_flag) {
187.              case 0: data = message[index_1]; break;
188.              case 1: data = message_MODBUS_RTU_01[index_1]; break;
189.              case 2: data = message_MODBUS_RTU_02[index_1]; break;
190.              case 3: data = message_MODBUS_RTU_03[index_1]; break;
```

```
191.            case 4: data = message_MODBUS_RTU_04[index_1]; break;
192.            case 5: data = message_MODBUS_RTU_05[index_1]; break;
193.            }
194.            index_1 = 0;
195.            UCSR0B |= (1<<RXEN0)|(1<<RXCIE0);
196.            access_marker = 0;
197.      }
198. }
199. //Прерывание по приеме UART0
200. ISR(USART0_RXC_vect) {
201.      cli();//Запрещаю прерывания, чтобы ничто отсюда не выдернуло
202.      data = UDR0;
203. //Записываю пришедший байт во внутреннюю переменную
204.      access_marker = 1;
205.      message[quantity] = data;
206.      quantity = quantity + 1;
207.      if (quantity == 8)
208.      {
209.            Command_check();
210.            quantity = 0;
211.            UCSR0B &= ~((1<<RXEN0)|(1<<RXCIE0));
212. //После сравнения запрещаю прием и прерывание RXC
213.            if (ack_flag == 0)//Если запрос удовлетворяет уставке,
214. нужно дать эхо на UART0
215.            {
216.                  UCSR0B |= (1<<TXEN0)|(1<<UDRIE0);//Разрешаю
217. отправку и прерывание по опустошению UDR0 (ответ)
218.            }
219.            else //Если запрос не поддерживается и нужно выдать
220. сообщение через UARTs
221.            {
222.                  //UCSR1B |= (1<<TXEN1)|(1<<UDRIE1);//Разрешаю
223. отправку сообщения на прерываниях UDR1
224.                  switch (ack_flag) {
225.                        case 1: message_length = 34;
226. suart_tx_str(message_MODBUS_RTU_01); break;
227.                        case 2: message_length = 36;
228. suart_tx_str(message_MODBUS_RTU_02); break;
229.                        case 3: message_length = 33;
230. suart_tx_str(message_MODBUS_RTU_03); break;
231.                        case 4: message_length = 41;
232. suart_tx_str(message_MODBUS_RTU_04); break;
233.                        case 5: message_length = 22;
234. suart_tx_str(message_MODBUS_RTU_05); break;
235.                  }
236.                  UCSR0B |= (1<<RXEN0)|(1<<RXCIE0);
237.            }
238.      }
239.      sei();//Разрешаю прерывания
```

```
240. }
241.
242. ISR(USART0_UDRE_vect) {
243.       cli();//Запрещаю прерывания, чтобы не выдернуло
244.       Send_message();//Отправка сообщения выше
245.       UCSR0B &= ~(1<<UDRIE0);//Запрещаю прерывание по опустощению
246. UDR
247.       UDR0 = data;//Кладу в UDR байт из сообщения
248.       UCSR0B |= (1<<TXCIE0);//Разрешаю прерывание по окончании
249. отправки
250.       sei();//Разрешаю прерывания
251. }
252.
253. ISR(USART0_TXC_vect) {
254.       if (access_marker == 1)//Если доступ был запрещен, т.е.
255. отправляем сообщение
256.       //Access denied, то разрешаем только прерывание на опустошение
257. UDR, чтобы класть туда
258.       //данные из буфера сообщения по байту
259.       {
260.             UCSR0B |= (1<<UDRIE0);
261.       }
262.       else {//Если доступ разрешен, то просто работаем на дальнейшее
263. получение
264.             ack_flag = 0;
265.             UCSR0B &= ~((1<<TXEN0)|(1<<TXCIE0));
266.             UCSR0B |= (1<<RXEN0)|(1<<RXCIE0);
267.       }
268. }
269.
270. ISR(USART1_UDRE_vect) {
271.       cli();//Запрещаю прерывания, чтобы не выдернуло
272.       Send_message();//Отправка сообщения выше
273.       UCSR1B &= ~(1<<UDRIE1);//Запрещаю прерывание по опустощению
274. UDR
275.       UDR1 = data;//Кладу в UDR байт из сообщения
276.       UCSR1B |= (1<<TXCIE1);//Разрешаю прерывание по окончании
277. отправки
278.       sei();//Разрешаю прерывания
279. }
280.
281. ISR(USART1_TXC_vect) {
282.       if (access_marker == 1)//Если доступ был запрещен,
283.       //то разрешаем только прерывание на опустошение UDR, чтобы
284. класть туда
285.       //данные из буфера сообщения по байту
286.       {
287.             UCSR1B |= (1<<UDRIE1);
288.       }
```

```
289.        else {//Если доступ разрешен, то просто работаем на дальнейшее
290.  получение
291.              ack_flag = 0;
292.              UCSR1B &= ~((1<<TXEN1)|(1<<TXCIE1));
293.              UCSR0B |= (1<<RXEN0)|(1<<RXCIE0);
294.        }
295.  }
296.
297.  int main(void)
298.  {
299.        DDRC = 0xFF;
300.        UARTInit();
301.        suart_init();
302.        sei();
303.        while (1)
304.        {
305.        }
306.  }
```

Приложение Г

(Обязательное)

Бизнес-модель проекта по Остервальдеру и Пинье

<table>
<tr>
<td rowspan="2">Ключевые партнеры
1. Поставщики комплектующих и расходных материалов;</td>
<td>Ключевые виды деятельности
1. Производство
ПАК для улучшения информационной безопасности АСУ ТП;
2. Решение проблем
Увеличение защищенности АСУ ТП с удаленным доступом</td>
<td rowspan="2">Ценностные предложения
1. Прямой анализ трафика технологической сети;
2. Сравнительная дешевизна решения;
3. Возможность оснащения устройством объектов с удаленным доступом.</td>
<td>Взаимоотношения с клиентами
1. Персональная техническая и консультационная поддержка.</td>
<td rowspan="2">Потребительские сегменты
1. Предприятия-пользователи АСУ ТП (B2B);
2. Объекты критической инфраструктуры (B2B, B2G).</td>
</tr>
<tr>
<td>Ключевые ресурсы
1. Интеллектуальные ресурсы;
2. Комплектующие и расходные материалы;
3. Персонал: инженерный и управленческий состав;
4. Финансы: начальные инвестиции.</td>
<td>Каналы сбыта
Прямые продажи заказчику.
Этапы сбыта:
1. Информационный: e-mail рассылка или презентация на конференции.
2. Продажный: разговор по телефону с заказчиком или получение заказа по электронной почте.
3. Доставка: почтовая доставка.
4. Постпродажный гарантийный ремонт.</td>
</tr>
<tr>
<td colspan="3">Структура издержек
Постоянные издержки: заработная плата, аренда помещения, ремонт оборудования и амортизационные расходы.
Переменные издержки: комплектующие и расходные материалы.</td>
<td colspan="3">Потоки поступления дохода
1. Продажа устройства;
2. Постпродажное обслуживание.</td>
</tr>
</table>