НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ «МИФИ»

ФАКУЛЬТЕТ КИБЕРНЕТИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАФЕДРА «КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

Направление 09.03.01 Группа К6-12В

«УТВЕРЖДАЮ»
Заведующий кафедрой
_____ М.А. Иванов
"____"_____2016 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ (ДИПЛОМНЫЙ ПРОЕКТ)

Фамилия, имя, отчество студента: **Клюев Дмитрий Владимирович**

Тема работы: **Разработка программно аппаратной платформы с возможностью защищенного хранения информации и защищенными протоколами передачи информации.**

Срок сдачи студентом готовой работы: **1 июня 2016 г.**

Руководитель работы: **Даньшин Вадим Владимирович**

Место выполнения: **НИЯУ МИФИ**

1. **Исходные данные:**

1.1. Система предназначена для хранения критически важных данных в flash памяти микроконтроллера в защищенном виде.
1.2. Flash память должна хранить константы, алгоритм работы и другую ключевую информацию защищаемого ПО.
1.3. Система должна выполнять следующие функции:
1.3.1. Обеспечивать защиту данных от несанкционированного доступа.
1.3.2. Производить форматирование содержимого памяти микроконтроллера при несанкционированном доступе.
1.3.3. Иметь защищенный протокол взаимодействия микроконтроллера и ПК.

2. **Содержание задания:**

2.1. Обзорная часть
2.1.1. Изучение спецификации Arduino Pro Micro, МК Atmega32u4. Подготовка рабочего места. Установка необходимых драйверов для микроконтроллера (МК). Выбор среды разработки. Изучение возможностей среды. Проверка взаимодействия среды разработки с МК. Загрузка в МК тестовой прошивки. Создать ISP программатор из дополнительной платы Arduino. Загрузка прошивки через ISP программатор.
2.1.2. Изучение спецификации загрузчика и адреса размещения загрузчика в flash памяти МК.
2.1.3. Изучение основных векторов атак на МК. Изучение power glitch
2.1.4. Изучение основных векторов атак на МК. Изучение. clock glitch
2.1.5. Изучение переключения FUSE битов УФ излучением и применение микропроб для перепрограммирования регистров контроллера.
2.1.6. Изучение физического избирательного повреждения топологии кристалла с целью выведения из строя отдельных его узлов.
2.1.7. Изучение FUSE битов и принципов их работы.
2.1.8. Изучение учета времени работы МК и хода времени на рабочей станции ПК.
2.2. Текст пояснительной записки
2.2.1. Описание протокола взаимодействия микроконтроллера и ПК.
2.2.2. Описание схемы алгоритма работы МК. Интерфейс, функции, описание автоматических тестов.
2.2.3. Описание схемы алгоритма типовой программы для ПК.
2.2.4. Описание подсистемы принятия решения о форматировании памяти.
2.2.5. Схема алгоритма.
2.2.6. Описание подсистемы подсчета реального времени.
2.2.7. Описание подсистемы, реализующую функцию проверки и перезаписи состояния FUSE битов МК при его запуске.
2.3. Программа
2.3.1. Реализация функции записи нулей в flash память МК в пределах заданного диапазона адресов.
2.3.2. Реализация функции побайтового чтения содержимого flash памяти с выполнением отправки значений в com порт.
2.3.3. Реализация функции чтения/очистки eeprom памяти МК.
2.3.4. Создание программы, реализующую функцию проверки и перезаписи состояния FUSE битов МК при его запуске. Данную функцию встроить в загрузчик.
2.3.5. Реализовать подсистему подсчета реального времени в формате Unix time stamp. Реализация с кварцем. Реализация на внутреннем тактовом генераторе. Зависимость внутренней RC цепочки от времени. Команды коррекции времени. Ограничения на возможности корректирования времени.

2.3.6. Реализация ГПСЧ на 12 разрядном XOR.
2.3.7. Реализация полиморфного протокола общения с рабочей станцией пользователя на XOR с динамически изменяющимся ключом.
2.3.8. Разработать планировщик задач в очереди прерываний. Ограничение очереди 1 секунда. Ограничение времени прерывания.
2.3.9. Разработка подсистемы авторизации ПК-сервера на ключе МК.
2.3.10. Подсистема принятия решения о форматировании памяти. Подсистема ограничения количества вызова различных функций в единицу времени, подсистема ограничений на допустимый температурный диапазон для режимов работы МК, ограничения на последовательности команд (перебор пароля), ограничения на "накрутку" времени в меньшую сторону, получение команд с ПК на старт форматирования, форматирование чипа вследствие превышения порога изменения приема радиостанций ФМ диапазона.
2.3.11. Реализация таблиц хранения служебных переходов для алгоритмов программы ПК (кодируем последовательности вызова блоков алгоритма программы ПК в блоке памяти ПЗУ флэш МК).

2.4. Тесты
2.4.1. Разработать автоматический тест подсистемы подсчета реального времени.
2.4.2. Реализация тестовой программы для ПК на языке processing. Интерфейсы, функции, тесты
2.4.3. Разработка тестов подсистемы авторизации ПК-сервера на ключе МК.

3. Основная литература:

1. Евстифеев А.В. Микроконтроллеры AVR семейства Mega. Руководство пользователя. — М.: Издательский дом «Додэка-XXI», 2007. — 592 с: ил. (Серия «Программируемые системы»).
2. DATASHEET 8-bit Microcontroller with 16/32K bytes of ISP Flash and USB Controller. Atmel Corporation, 2015. — 438 с.. www.atmel.com
3. Мортон Дж. Микроконтроллеры AVR. Вводный курс. /Пер. с англ. – М.: Издательский дом «Додэка-XXI», 2006. – 272 с.: ил. (Серия «Мировая электроника»).

4. Отчетный материал:

пояснительная записка;
макетно-экспериментальная часть:

1. Листинги отлаженных программ.
2. Материалы тестирования и отладки.
3. Дистрибутив автоматизированной системы на CD.
4. Руководство пользователя / администратора.

Дата выдачи задания: 15 февраля 2016 г.

Руководитель _____ В.В. Даньшин

Задание принял к исполнению _____ Д.В. Клюев

Рецензент задания _____

для работ, выполняемых в сторонних организациях