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

Номер зачетной книжки _____
Преддипломная практика зачтена с оценкой
_____ (_____)
(цифрой) (прописью)

_____
(подпись руководителя практики от БГУИР)
_____._____.2022

ОТЧЕТ
по преддипломной практике
Место прохождения практики: ОАО “Белгазпромбанк”

Сроки прохождения практики: с __.___.2022 по ___.___.2022

Руководитель практики от предприятия:
_____ М. Ю. Кузнецова
(подпись руководителя)
М.П.

Студент группы 850701
_____ Д. А. Филипцов
(подпись студента)
Руководитель практики от БГУИР
Шемаров А. И. − канд. техн. наук, доцент кафедры ЭВС

Минск 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день микроэлектронику трудно представить без такой важной составляющей, как микроконтроллеры. На помощь человеку приходят всё больше и больше электронных помощников. Мы привыкли к ним и часто даже не подозреваем, что во многих подобных устройствах работает микроконтроллер.

Микроконтроллерные технологии очень эффективны. Одно и то же устройство, которое раньше собиралось на традиционных элементах, будучи собрано с применением микроконтроллеров, становится проще. Оно не требует регулировки и меньше по размерам. Кроме того, с применением микроконтроллеров появляются практически безграничные возможности по добавлению новых потребительских функций и возможностей к уже существующим устройствам.

Микроконтроллеры применяются в телевизорах, мобильных телефонах, игровых приставках, стиральная машина, калькулятор – это те самые устройства, которые имеют как минимум один микроконтроллер. В случае данного дипломного проекта на микроконтроллере выполняется коммуникационный контроллер с шифрованием данных для системы «Умный дом».

Устройства систем типа «Умный дом» используются в быту для облегчения осуществления ежедневных рутинных действий в домашней обстановке. Обычно это регулирование параметров микроклимата, управление «умной» бытовой техники дистанционно, охранные системы и системы санкционированного доступа в помещение. Для реализации подобных систем необходимо подключение множества различных устройств друг к другу и/или к общему командному серверу.

Одной из важнейших проблем таких сетей на данный момент является их незащищённость от несанкционированного доступа. Эту проблему и должно решать разрабатываемое в данном проекте устройство, выполняя шифрование трафика домашней сети.

О КОМПАНИИ

Открытое акционерное общество «Белгазпромбанк» начинает свою деятельность с 27 сентября 1990 года под названием Коммерческий банк «Экоразвитие». В результате неоднократных переименований и преобразований от 28 ноября 1997 года №16 было зарегистрировано совместное белорусско-российское ОАО «Белгазпром».

Сегодня Белгазпромбанк стал системообразующим банком для предприятий негосударственного сектора экономики. Рост капитала позволил осуществлять крупнейшие проекты в масштабе страны. Накопленный опыт работы, квалифицированный персонал, влиятельные акционеры, доверие клиентов — все это создает хорошие предпосылки для дальнейшего движения вперед. Белгазпромбанк не останавливается в своем развитии, постоянно совершенствуя качество обслуживания клиентов, ведь основная цель нашей деятельности — содействие в формировании в Республике Беларусь эффективного среднего класса в условиях рыночной экономики.

В функциональные обязанности системного аналитика входят коммуникации с бизнес-заказчиками и командой разработчиков, формирование концепции разработки ПО, детальное описание алгоритмов, бизнес-правил, ограничений в SRS, внедрение новых решений и бизнес-процессов, помощь в тестировании разработанного на основании SRS ПО.

1 ОБЗОР АНАЛОГИЧНЫХ РАЗРАБОТОК

Большинство разработчиков систем умного дома не раскрывает подробностей про то, имеется ли в их продукте встроенная защита передачи данных. Делается это по нескольким причинам. Во-первых, основная масса потребителей не компетентна в достаточной мере для проведения сравнительного анализа, а так же не слишком заинтересована в мерах обеспечения повышенной безопасности сети. Во-вторых, производители не стремятся публиковать информацию об этих характеристиках собственных систем, чтобы избежать интереса злоумышленников к их разработкам в сфере информационной безопасности.

Рассмотрим некоторые стандарты сетевых протоколов, а также готовые решения на рынке и способы защиты информации в них.

ZigBee является одной из самых распространённых в использовании на данный момент спецификацией сетевых протоколов для интернета вещей (IoT). Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Кроме того, спецификация ZigBee содержит возможность выбора алгоритма маршрутизации в зависимости от требований приложения и состояния сети, механизм стандартизации приложений — профили приложений, библиотека стандартных кластеров, конечные точки, привязки, гибкий механизм безопасности, а также обеспечивает простоту развертывания, обслуживания и модернизации.

Шифрование данных в ZigBee основано на протоколе 802.15.4. Алгоритм шифрования, используемый в ZigBee, — это AES (Advanced Encryption Standard) с длиной ключа 128 бит (16 байт). Алгоритм AES используется не только для шифрования информации, но и для проверки отправляемых данных. Эта концепция называется проверкой целостности данных и достигается при помощи кода целостности сообщения (MIC), также называемого кодом аутентификации сообщения (MAC), который добавляется к сообщению. Этот код обеспечивает целостность заголовка MAC и прикрепленных данных полезной нагрузки.

Он создается путем шифрования частей кадра MAC-адреса IEEE с использованием ключа сети, поэтому, если мы получим сообщение от недоверенного узла, мы увидим, что MAC-адрес, сгенерированный для отправленного сообщения, не соответствует тому, который был бы

сгенерирован с использованием текущего секретного ключа, поэтому мы можем отбросить это сообщение. MAC может иметь разный размер: 32, 64, 128 бит, однако всегда создается с использованием 128-битного алгоритма AES. Его размер - это просто длина битов, которая прикреплена к каждому кадру. Чем больше размер, тем безопаснее (хотя сообщение может принять меньшую полезную нагрузку). Защита данных осуществляется путем шифрования поля полезных данных с помощью 128-битного ключа.

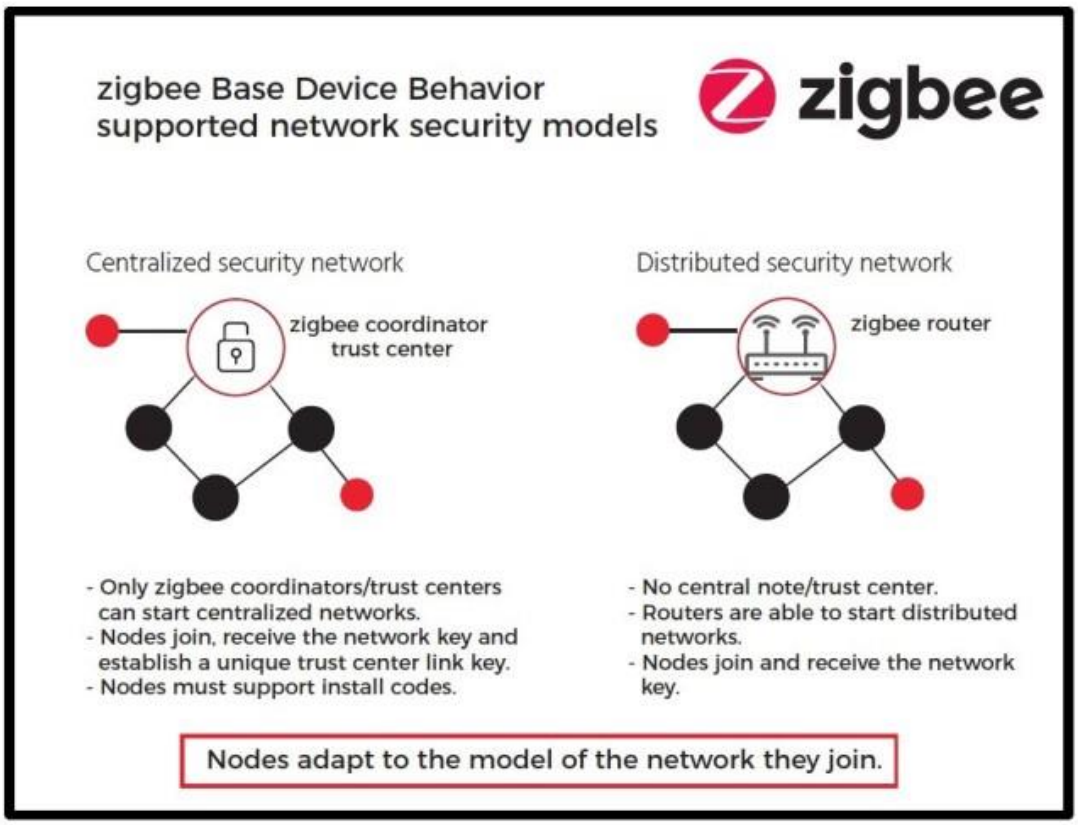

Рисунок 1.1 – Модели безопасности ZigBee

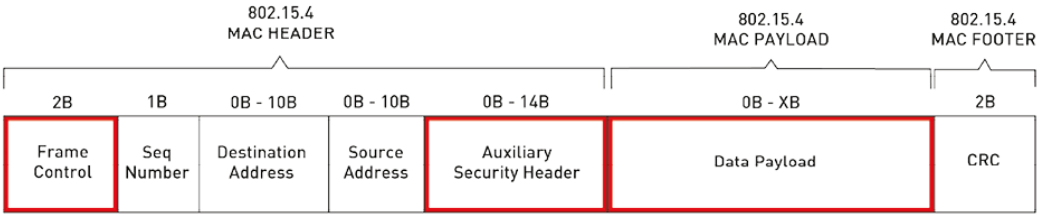

Рисунок 1.2 – Структура посылки в протоколе IEEE 802.15.4

Системы умного дома разработчика MiMiSmart также используют передовой алгоритм шифрования Advanced Encryption Standard (AES), который широко используется в банковской сфере в том числе. Так что

можно прийти к выводу, что данное шифрование довольно популярна на рынке IoT.

Рисунок 1.3 – Схема устройства систем умного дома MiMiSmart

KNX — коммуникационная шина, широко используемая для автоматизации зданий. Стандарт шины KNX стал развитием более ранней разработки EIB (European Installation Bus). EIB — устаревшее обозначение, но оно продолжает использоваться, особенно в Европе. Иногда используется обозначение EIB/KNX.Продукция KNX распространялась под несколькими торговыми марками. Наиболее известны Instabus, ABB i-Bus, Tebis, Theben.

Рисунок 1.4 – KNX-Transceiver-Board фирмы Elmos

Автоматизация дома и зданий с KNX безопасна. Данная технология соответствует всем необходимым правилам безопасности. Технология KNX Secure стандартизирована в соответствии с EN 50090-3-4, что означает, что KNX успешно блокирует хакерские атаки на цифровую инфраструктуру сетевых зданий. Таким образом, сводится к минимуму риск цифровых взломов.

Кроме того, KNX Secure соответствует самым высоким стандартам шифрования (согласно ISO 18033-3, таким как шифрование AES 128 CCM), чтобы эффективно предотвращать атаки на цифровую инфраструктуру зданий и достигать высочайшего уровня защиты данных.

KNX Secure гарантирует максимальную защиту. KNX IP Secure расширяет протокол IP таким образом, что все передаваемые телеграммы и данные полностью зашифрованы. KNX Data Secure эффективно защищает данные пользователя от несанкционированного доступа и манипуляций с помощью шифрования и аутентификации.

Рисунок 1.5 – Xiot – разработчик KNX Secure

Control4 — поставщик систем автоматизации и сетевых систем для дома и бизнеса, предлагающий персонализированную и унифицированную систему умного дома для автоматизации и управления подключенными устройствами, включая освещение, аудио, видео, климат-контроль, внутреннюю связь и безопасность. Control4 использует AES для шифрования данных, а также иные средства защиты персональной информации, которые не раскрываются компанией.

Рисунок 1.6 – Компания Control4

Z-Wave — это распространённый радио протокол передачи данных, предназначенный для домашней автоматизации. Характерной особенностью Z-Wave является стандартизация от физического уровня, до уровня приложения. Т.е. протокол покрывает все уровни OSI классификации, что позволяет обеспечивать совместимость устройств разных производителей при создании гетерогенных сетей.

Что позволяет делать технология Z-Wave:

- Управление освещением (реле/диммеры), шторами, рольставнями и воротами.
- Управление жалюзи и другими моторами (10-230 В).
- Включение/выключение любых нагрузок до 3.5 кВт (модуль в розетку или встраиваемое реле).

- Дистанционное управление с ПДУ.
- Управление обогревом (электрические тёплые полы с защитой от перегрева, электро котлы и радиаторы, термостаты для водяных клапанов радиаторов).
- Управление кондиционерами (через ИК интерфейс имитируя пульт).
- Детектирование тревожных событий (датчики движения, открытия двери/окна, протечки, сухие контакты).
- Мониторинг состояния (датчики температуры, влажности, освещённости).
- Управление A/V аппаратурой (по протоколу Z-Wave или через ИК интерфейс имитируя пульт).
- Связь с любым программным обеспечением через ПК контроллер.
- Сбор данных со счётчиков.

В различных готовых решениях на основе данной технологии для шифрования обычно используется AES128. На пример в модулях ZM2102 на одном кристалле SD3402.

Рисунок 1.7 – Модуль ZM2102

2 РАЗРАБОТКА СТРУКТУРЫ МОДУЛЯ КОММУНИКАЦИОННОГО КОНТРОЛЛЕРА

2.1 Разбиение устройства на модули

Используя функциональную спецификацию, необходимо выполнить декомпозицию разрабатываемого устройства на модули, которые реализуют выполняемые функции. После разбиения на модули нужно выделить отдельно аппаратные и отдельно программные модули.

Выполнив декомпозицию, необходимо построить модульную структуру аппаратных средств устройства, основу которых составляет управляющая микро-ЭВМ, в которую входит:

1) процессорный модуль, предназначенный для обработки информации;
2) модуль генератора тактовых импульсов (ГТИ), который предназначен для синхронизации работы системы;
3) модуль интерфейса ввода и модуль интерфейса вывода;
4) модуль преобразования входного сигнала;
5) модуль преобразования выходного сигнала;
6) модуль памяти, предназначенный для хранения программного обеспечения.

На рисунке 2.1 представлена общая модульная структура аппаратных средств коммуникационного контроллера.

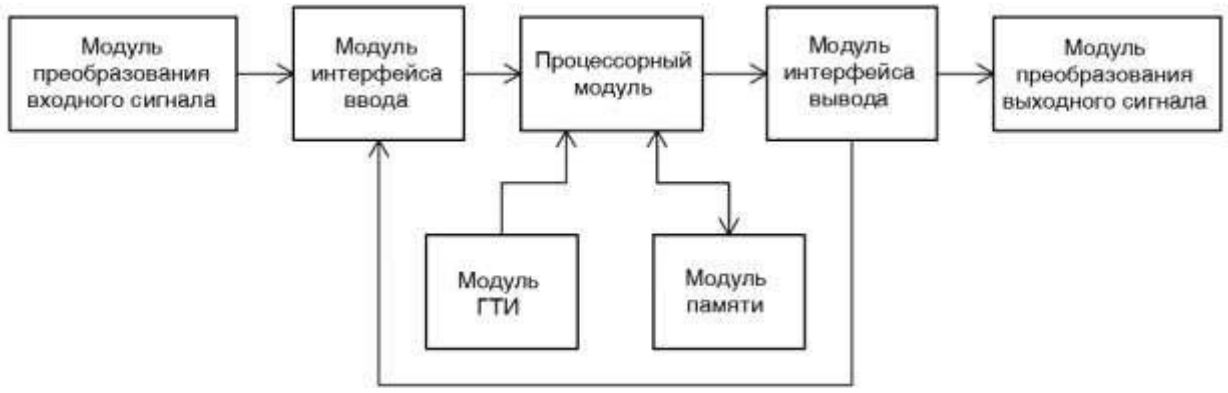

Рисунок 2.1 – Общая модульная структура аппаратных средств устройства

Далее систему управления коммуникационного контроллера необходимо разбить на функциональные модули. На основании функциональной спецификации можно сделать вывод, что система состоит из трёх частей: вход,

выход и функции.

Входной модуль выполняет считывание данных с контроллера системы «Умный дом» по заранее определённому интерфейсу.

Выходной модуль осуществляет вывод обработанных, зашифрованных и сформированных определённым образом данных на контроллер сетевой передачи данных (на пример радиоимодуль) по заранее определённому интерфейсу.

Для функций можно выделить следующие модули:

1) модуль блочного шифрования данных;
2) модуль сцепления зашифрованных блоков;
3) модуль обмена ключами шифрования;
4) модуль протоколирования данных;
5) модуль проверки целостности полученных данных.

После декомпозиции на функциональные модули необходимо изобразить функционально-модульную структуру коммуникационного контроллера, которая отражает иерархию входящих в нее модулей.

На высшем уровне модульной структуры располагается исполнительный модуль, который содержит средства, необходимые для реализации функций шифрования и протоколирования (микроконтроллер). Входной и выходной модули находятся на нижнем уровне иерархии.

Полученная модульная структура фотодатчика изображена на рисунке 2.2.

Рисунок 2.2 – Функционально-модульная структура коммуникационного контроллера

Распределение функций по модулям коммуникационного контроллера выглядит следующим образом:

1) исполнительный модуль выполняет:

– блочное шифрование,
– сцепление зашифрованных блоков,
– обмен ключами шифрования,
– проверку целостности данных;

2) входной модуль выполняет считывание данных по определённому протоколу;
3) выходной модуль выполняет вывод данных по определённому протоколу.

Полная функционально-модульная структура контроллера, содержащая функции для каждого модуля, изображена на рисунке 2.3.

Рисунок 2.3 – Полная функционально-модульная структура коммуникационного контроллера

2.2 Выбор соотношения между аппаратными и программными средствами

Различные функции шифрования, указанные в функционально-модульной структуре, реализуются управляющей микро-ЭВМ (микроконтроллером) в результате выполнения основной программы посредством последовательного вызова функций соответствующих программных модулей системы.

На рисунке 2.4 представлена связь между программными и аппаратными средствами коммуникационного контроллера с шифрованием

данных для системы «Умный дом».

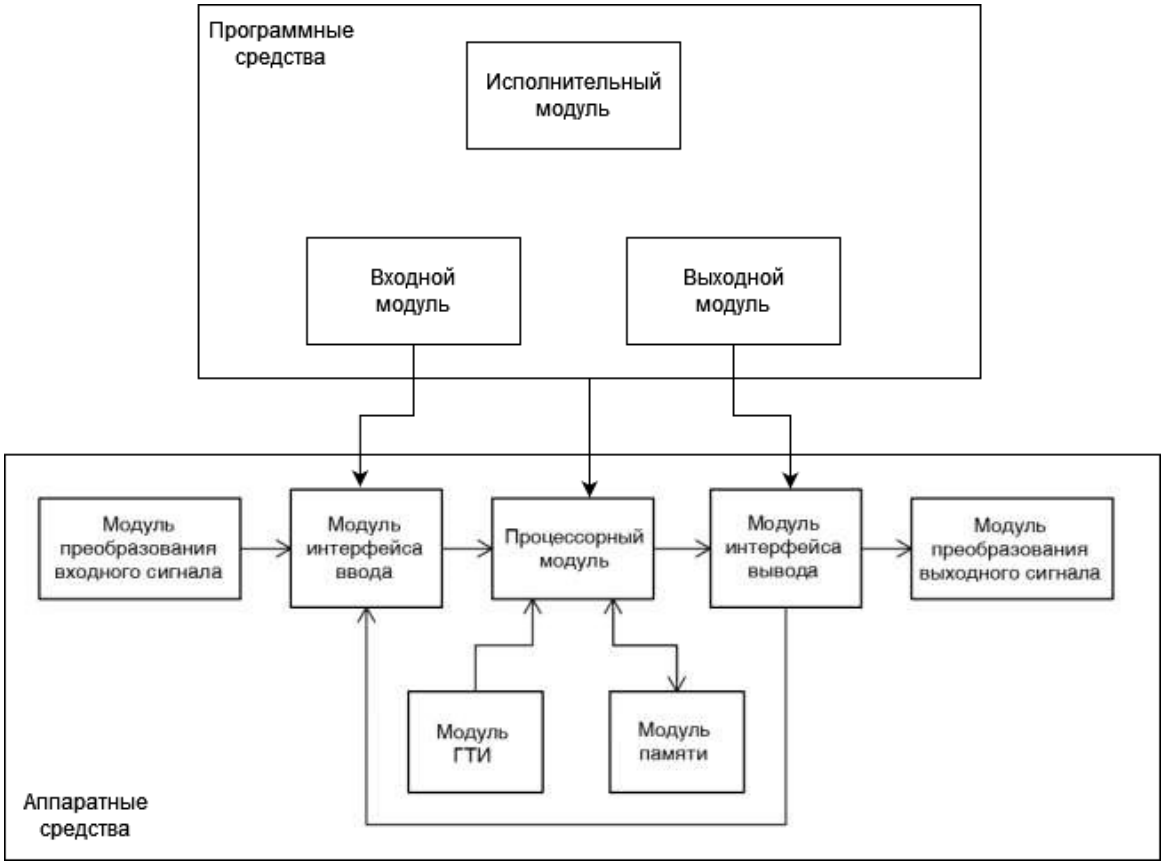

Рисунок 2.4 – Связь между аппаратными и программными средствами

2.3 Описание структурной схемы

Головным модулем структурной схемы является процессорный модуль (микроконтроллер). Он выполняет функции блочного шифрования, сцепления зашифрованных блоков, обмена ключами шифрования, проверки целостности данных. В модуле памяти хранятся коды, константы и переменные программного обеспечения процессорного модуля. В отдельный блок можно выделить модуль генератора тактовых импульсов (ГТИ).

Входной и выходной модули необходимы для координирования операций ввода-вывода информации. Они будут представлены портами микропроцессора. В данном работе периферийными устройствами будут служить интерфейсы устройств системы «Умный дом» и радиомодуля для отправки и получения данных по сети – все они будут подключены к входному и выходному модулям.

ЗАКЛЮЧЕНИЕ

В ходе прохождения преддипломной практики осуществлялось выполнение отражённых в данном отчёте глав дипломного проекта.

В ходе выполнения данного проекта были разобраны аналогичные проекты на рынке, проведён их анализ и выявлены общие черты большинства продуктов, а именно использование самого распространённого на данный момент в сфере интернета вещей метода шифрования AES 128. Были разработаны и обоснованы общая модульная структура, функционально-модульная структура, и структура связи между аппаратными и программными средствами.

В ходе прохождения преддипломной практики также были получены реальные практические навыки такие, как чёткая формулировка и соблюдение содержания технического задания, взаимодействия с коллегами и заказчиком для выполнения поставленных задач, изучение и соблюдение техники безопасности на производстве, работа с банковской информационной системой БИСКВИТ. Приобретённые навыки позволят в будущем быть более компетентным работником, быстрее и проще влиться в реальный рабочий процесс.