МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет	*Кафедра*
вычислительной техники	«Вычислительная техника»

Направление подготовки: 09.04.01 «Информатика и вычислительная техника»

Магистерская программа: «Вычислительные машины, комплексы, системы и сети»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

МАГИСТРА

на тему

ЗАЩИЩЕННАЯ ПРОГРАММА ИНИЦИАЛИЗАЦИИ АППАРАТНОЙ ПЛАТФОРМЫ

Студент 03.06.20 Новиков Константин Борисович
(подпись, дата) (ФИО полностью)

Руководитель Н.Н. Коннов
(подпись, дата) (фамилия, инициалы)

Нормоконтролёр А.В. Кучин
(подпись, дата) (фамилия, инициалы)

Рецензент зам. специалиста ООО «Бизнес-программа»
(должность, место работы) (подпись, дата) А.В. Севастьянов
(фамилия, инициалы)

Работа допущена к защите (протокол зас. кафедры от 03.06.2020 №12)

Заведующий кафедрой М.А. Митрохин
(подпись) (фамилия, инициалы)

Работа защищена с отметкой отлично (протокол заседания ГЭК от 15.06.2020 № 6)

Секретарь ГЭК Е.И. Гурин
(подпись) (фамилия, инициалы)

Пенза 2020

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет
вычислительной техники

Кафедра
«Вычислительная техника»

«Утверждаю»
Заведующий кафедрой
М.А. Митрохин
«25» сентября 2019 г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
МАГИСТРА

1. Студент Новиков Константин Борисович гр. 18ВВ1м факультета вычислительной техники.
2.Тема работы «Защищенная программа инициализации аппаратной платформы».

Тема утверждена приказом ПГУ № 1039/о от " 30 " сентября 2019 г.

3. Руководитель магистерской диссертации к.т.н., доцент, профессор каф. ВТ ПГУ Коннов Н.Н.

4. Задание на работу (назначение разработки, исходные данные и т.п).
Назначение разработки – загрузка операционной системы из доверенного носителя.
Разработать программу, реализующую инициализацию и тестирование аппаратной платформы до передачи управления штатному загрузчику операционной системы, а также выполняющую функции доверенной загрузки.
5. Перечень подлежащих разработке вопросов
Требуется произвести анализ предметной области, сформировать перечень функций доверенной загрузки.

6. Календарный график выполнения работы

№ п/п	Наименование этапов работы	Объем работы	Срок выполнения	Подпись руководителя
1	Анализ предметной области	20	14.02.20	
2	Формирование перечня функций доверенной загрузки	20	20.02.20	
3	Выбор аппаратной платформы для реализации защищенной программы	20	08.03.20	
4	Доработка существующего доверенного загрузчика	90	20.03.20	
5	Реализация функций доверенной загрузки	70	02.04.20	
6	Отладка защищенной программы инициализации аппаратной платформы	40	08.05.20	
7	Оформление магистерской диссертации	30	17.05.20	

Дата выдачи задания " 25 " сентября 2019 г.

Руководитель магистерской диссертации _____ Коннов Н.Н.
(подпись, дата)

Задание к исполнению принял студент _____ Новиков К.Б.
(подпись, дата)

Работу к защите допустить
Декан факультета _____ Фионова Л.Р.
(подпись, дата)

РЕФЕРАТ

Магистерская диссертация содержит 80 листов, 16 рисунков, 9 источников, 2 приложения.

БАЗОВАЯ СИСТЕМА ВВОДА-ВЫВОДА, ЗАГРУЗЧИК ОПЕРАЦИОННОЙ СИСТЕМЫ, ДОВЕРЕННАЯ ЗАГРУЗКА.

Цель работы – разработать защищенную программу инициализации аппаратной платформы с функциями доверенной загрузки, которая может быть использована для инициализации системы на базе материнской платы российского производства.

Объектом разработки является программа, которая после компиляции может быть использована для замещения штатного образа ПО BIOS на материнской плате российского производства. Программа должна выполнять инициализацию и тестирование аппаратного обеспечения системы, а также осуществлять доверенную загрузку до передачи управления штатному загрузчику операционной системы.

Результатом проведенной работы является проект, удовлетворяющий поставленной задаче, а именно программа инициализации аппаратной платформы для процессорной платы Fastwel CPC1311 на аппаратной платформе Intel BayTrail. В защищенной программе реализованы функции доверенной загрузки, в том числе тестирование базовых аппаратных компонентов процессорной платы, контроль целостности программы, аутентификация пользователя и запрет загрузки в случае выявления ошибок в процессе выполнения тестов.

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ 5
ВВЕДЕНИЕ 6
1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ 7
1.1 Понятие доверенной загрузки операционной системы 7
1.2 Проблемы и способы решения современной реализации доверенной загрузки операционной системы 8
1.3 Понятие и выбор аппаратной платформы при реализации для нее защищенной программы инициализации аппаратной платформы 10
1.4 Выбор процессорной платы на базе выбранной аппаратной платформы 13
2 РАЗРАБОТКА ЗАЩИЩЕННОЙ ПРОГРАММЫ ИНИЦИАЛИЗАЦИИ АППАРАТНОЙ ПЛАТФОРМЫ 16
2.1 Разработка модуля ПО BIOS 18
2.2.1 Модуль процессорной платы 19
2.2.2 Модуль графического интерфейса 20
2.2.3 Модуль локализации 22
2.2 Модуль доверенной загрузки 23
2.2.1 Аутентификация пользователя 24
2.2.2 Контроль носителя, выбранного источником загрузки ОС 25
2.2.3 Тесты предпускового контроля 26
2.3 Бинарные вставки 27
3 ТЕСТИРОВАНИЕ ЗАЩИЩЕННОЙ ПРОГРАММЫ ИНИЦИАЛИЗАЦИИ АППАРАТНОЙ ПЛАТФОРМЫ 29
3.1 Процесс отладки 29
3.2 Процесс тестирования 30
4 РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ 32
4.1 Инсталляция 32
4.2 Эксплуатация 34
ЗАКЛЮЧЕНИЕ 41
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 42
ПРИЛОЖЕНИЕ А ЛИСТИНГИ ПРОГРАММЫ 43

Приложение А.1 Файл mainboard.c 43
Приложение А.2 Файл generate_locales.go 47
Приложение А.3 Файл codeLanguage.go 53
Приложение А.4 Файл graphics.c 64
ПРИЛОЖЕНИЕ В ПРЕЗЕНТАЦИЯ 76

СПИСОК СОКРАЩЕНИЙ

АПМДЗ – аппаратно-программный модуль доверенной загрузки

АРМ – автоматизированное рабочее место

МДЗ – модуль доверенной загрузки

НСД - несанкционированный доступ

ОС – операционная система

ПЗУ – постоянное запоминающее устройство

ПО – программное обеспечение

ПЭВМ – персональная электронная вычислительная машина

ВВЕДЕНИЕ

Важнейшей задачей в области обеспечения информационной безопасности автоматизированных систем является сохранение свойств информации, таких как доступность, целостность и конфиденциальность.

На автоматизированных рабочих местах, на которых обрабатывается конфиденциальная информация, для защиты от НСД к информации внутреннего нарушителя как правило применяется комплекс мероприятий, включающих в себя установку аппаратно-программных модулей доверенной загрузки [1].

Ситуация осложняется в случаях, когда необходимо обеспечить защиту от НСД к информации на объектах, критичных к способу и месту размещения АРМ. В данных случаях установка АПМДЗ может быть невозможна, т.к. изделие АРМ имеет малые габариты или увеличенное тепловыделение из-за потребляемой мощности. Отсутствие АПМДЗ не всегда возможно компенсировать рядом организационно-режимных мер. Отсутствие АПМДЗ в данных изделиях приводит к тому, что до или в процессе загрузки ОС появляется возможность осуществить преднамеренные попытки НСД к информации.

Для защиты от указанных угроз может быть применен подход по реализации в них процедуры доверенной загрузки.

Процедура доверенной загрузки – это процесс загрузки системного программного обеспечения после выполнения успешной аутентификации оператора изделия и исключительно с выбранного учтённого носителя.

В данной работе рассматривается вопрос разработки защищенной программы инициализации аппаратной платформы, реализующей процедуру доверенной загрузки.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

Защищенная программа инициализации аппаратной платформы – программа, выполняющая подготовку аппаратных средств ЭВМ к работе ОС и процедуру доверенной загрузки операционной системы.

Защищенная программа выполняется на этапе работы ПО BIOS и может быть встроена в существующий образ или полностью заменить ПО BIOS. В последнем случае защищенная программа инициализации аппаратной платформы должна реализовать функционал ПО BIOS.

1.1 Понятие доверенной загрузки операционной системы

Доверенная загрузка ОС – совокупность выполняемых до передачи управления штатному загрузчику ОС процедур, в результате выполнения которых принимается решение о разрешении или запрете передачи управления штатному загрузчику ОС и дальнейшей загрузки системы [2].

Доверенная загрузка как правило должна быть реализована в комплексах, выполняющих обработку информации, составляющую государственную тайну. Конкретный набор процедур, входящих в состав доверенной загрузки, составляется для каждого комплекса индивидуально в зависимости грифа обрабатываемой информации, условий эксплуатации комплекса и реализованных организационно-технических мер, направленных на защиту от НСД [3].

Ряд процедур, которые могут войти в состав доверенной загрузки:

1. Аутентификация пользователя;
2. Журналирование процесса инициализации аппаратной платформы;
3. Проверка работоспособности центрального процессора и ОЗУ;

4. Контроль целостности BIOS;
5. Контроль состава аппаратного обеспечения;
6. Контроль состава подключенных носителей информации;
7. Контроль выбранного метода и источника загрузки операционной системы.

По результатам выполнения процедур, указанных выше, может быть совершена передача управления загрузчику операционной системы для осуществления ее загрузки [4].

1.2 Проблемы и способы решения современной реализации доверенной загрузки операционной системы

Доверенная загрузка в текущий момент реализуется на аппаратно-программном уровне средствами АПМДЗ.

АПМДЗ – аппаратное устройство, устанавливаемое в контролируемую ПЭВМ по шине PCI (PCI, PCI E, miniPCI-E), предназначенное для осуществления доверенной загрузки на этапе загрузки ОС и функций защиты от НСД на этапе работы ОС [5].

АПМДЗ получают управление при вызове аппаратного прерывания со стороны BIOS, после чего начинают выполнение ряда процедур доверенной загрузки. В результате ее выполнения АПМДЗ возвращают управление BIOS для осуществления в дальнейшем загрузки ОС или подают питание на аппаратный вывод «Перезагрузка» материнской платы для запрета дальнейшей загрузки ОС.

Данное решение имеет ряд проблем при внедрении в контролируемый комплекс и при дальнейшей эксплуатации:

1. Потенциальное наличие в бинарном коде BIOS недекларированных возможностей, используя которые злоумышленник может обойти АПМДЗ по управлению;

2. Потенциальное наличие в аппаратной платформе (материнской плате, центральном процессоре и т.д.) недекларированных возможностей, используя которые злоумышленник может обойти АПМДЗ по управлению;

3. Невозможность внедрения в АРМ при неудовлетворении устройства АПМДЗ требованиям к габаритам или тепловыделению и энергопотреблению.

В ходе анализа вышеуказанных проблем были сформулированы методы их решения для повышения уровня доверия к системе и реализации доверенной загрузки при применении системы в комплексах, обрабатывающих государственную тайну:

1. Доверенная загрузка должна быть реализована программным средством, которое может быть установлено в АРМ вне зависимости от его аппаратной конструкции;

2. Программное средство (далее – защищенная программа инициализации аппаратной платформы) должно заместить штатный код ПО BIOS, реализуя его основные функции, и выполнять доверенную загрузку в процессе подготовки аппаратных средств ЭВМ к их использованию операционной системой.

3. Повышение доверия к АРМ может быть достигнуто, если в основе АРМ используется материнская плата российского производства, производители которой имеют документацию на схемотехнику платы и могут гарантировать отсутствие недекларированных возможностей в схемотехнике платы.

В качестве основы для защищенной программы инициализации аппаратной платформы может быть использован доверенный загрузчик

операционной системы, разработанный в ходе выполнения выпускной квалификационной работы.

1.3 Понятие и выбор аппаратной платформы при реализации для нее защищенной программы инициализации аппаратной платформы

Аппаратная платформа – совокупность системной логики, включающей в себя контроллеры памяти и периферийных устройств, и центрального процессора.

Защищенная программа инициализации аппаратной платформы, спроектированная для замещения штатного образа ПО BIOS материнской платы в составе АРМ, не может быть универсальной и должна быть доработана для каждой материнской платы, на которой она будет запущена. Поэтому на данном этапе важно выбрать аппаратную платформу, материнская плата на базе которой будет наиболее подходящей для потенциального использования в АРМ вместе с защищенной программой инициализации аппаратной платформы.

В ходе выполнения выпускной квалификационной работы было принято решение выбрать фирму Intel в качестве производителя системной логики аппаратной платформы. Материнские платы российского производства на базе аппаратных платформ данного производителя популярны на российском рынке и используются в АРМ, обрабатывающих информацию государственной важности. В качестве аппаратной платформы была выбрана Intel Haswell.

В ходе выполнения магистерской диссертации были выделены новые критерии выбора аппаратной платформы:

1. Наличие на отечественном рынке материнских плат на базе аппаратной платформы;

2. Год выпуска аппаратной платформы фирмы-производителем;

3. Наличие в проекте Coreboot, на базе которого разрабатывается доверенный загрузчик операционной системы, базового кода для аппаратной платформы;

4. Объем бинарных вставок от производителя системной логики, которые должны быть внедрены в ПО BIOS ее инициализации.

По приведенным выше критериям был проведен анализ перечня материнских плат российского производства на базе аппаратной платформы фирмы Intel. Рассматривались материнские платы крупного российского производител ЗАО НПФ «Доломант», выпускающих свою продукцию в России под брендом Fastwel. Результаты анализа представлены ниже (Таблица 1).

Таблица 1 - Сравнение аппаратных платформ по указанным критериям

Название критерия	Haswell	BayTrail	Skylake	KabyLake	ApolloLake
Наличие материнских плат на базе аппаратной платформы	1	1	1	1	1
Год выпуска аппаратной платформы	0.4 (2013 г)	0.4 (2013 г)	0.6 (2015 г)	1 (2017 г)	1 (2016 г)
Наличие базового исходного кода в проекте Coreboot	1	1	1	0	1

Продолжение таблицы 1

Название критерия	Haswell	BayTrail	Skylake	KabyLake	ApolloLake
Объем бинарных вставок от производителя системной логики в ПО BIOS	0.95 (64 Кбайт)	1 (50 Кбайт)	0 (4 Мбайт)	0 (4 Мбайт)	0 (8 Мбайт)
Общая оценка	3.35	3.4	2.6	2	3

По результатам проведения анализа была выбрана аппаратная платформа Intel BayTrail. Аппаратная платформа является «системой-на-чипе» - центральный процессор впаивается напрямую в материнскую плату без возможности его удаления и замены (далее – процессорная плата). Данная особенность позволит при разработке доверенного загрузчика операционной системы добавить поддержку только одного центрального процессора, название которого будет известно заранее, что упростит логику работы загрузчика и снизит объем бинарных вставок.

Решающим преимуществом аппаратной платформы Intel BayTrail является версия встроенного микроконтроллера Intel TXE, используемого на всех процессорных платах данной аппаратной платформы. Микроконтроллер установлен на материнской плате, запускается сразу после подачи питания на материнскую плату (т.е. до старта центрального процессора) и работает под управлением прошивки, исходный код для которой отсутствует. Как правило, прошивка для микроконтроллера внедряется в BIOS в качестве отдельной бинарной вставки.

В материнских платах на базе Intel BayTrail используется первая версия данного микроконтроллера, которая допускает исключение бинарной

вставки с прошивкой из состава BIOS. Это позволит значительно уменьшить объем BIOS, который компилируется не из исходного кода.

Таким образом, в качестве аппаратной платформы материнской (процессорной) платы, для которой будет разработана защищенная программа инициализации аппаратной платформы, была выбрана платформа Intel BayTrail.

1.4 Выбор процессорной платы на базе выбранной аппаратной платформы

Перед выбором процессорной платы, для которой будет разработана защищенная программа инициализации аппаратной платформы, сформированы критерии выбора:

1. Процессорная плата разработана с использованием системной логики аппаратной платформы Intel BayTrail;
2. Процессорная плата российского производства;
3. Процессорная плата имеет набор выходов, которые используются при подключении АПМДЗ (выход на шину PCI-E, выходы для подачи сигнала включения ПК);
4. Процессорная плата имеет наибольший перечень предоставляемых аппаратных интерфейсов, которые могут быть использованы потенциальным заказчиком;
5. Существует дешевый аналог процессорной платы, который может быть использован в качестве ее прототипа при разработке защищенной программы инициализации аппаратной платформы.

По вышеуказанным критериям выделен ряд процессорных плат российского производства на базе аппаратных платформ Intel BayTrail для выбора из их числа процессорной платы (Таблица 2).

Таблица 2 - Сравнение процессорных плат по указанным критериям

Название критерия	Fastwel CPC1311	Fastwel CPC310	Fastwel CPB909
Наличие выходов для подключения АПМДЗ	1	1	1
Количество интерфейсов, реализуемых на плате	1	0.8	0.8
Существует дешевый аналог	1	1	1
Общая оценка	3	2.8	2.8

В результате проведенного анализа было решено, что плата Fastwel CPC1311 является наиболее подходящей для разработки доверенного загрузчика операционной системы. Плата исполнена в формате PC-104 и предназначена для встраивания в плату-носитель с установленными на ней аппаратными интерфейсами. Подобное исполнение упрощает встраивание процессорной платы в АРМ, т.к. плата носитель может быть разработана с учетом габаритов и характеристик конечного изделия.

Fastwel CPC1311 имеет широкий перечень предоставляемых интерфейсов, которые могут быть использованы заказчиком при применении платы в своих проектах.

Так как рыночная стоимость отечественных плат высока, при разработке защищенной программы инициализации аппаратной платформы будет использована дешевая плата-аналог. Для Fastwel CPC1311 такой платой является Intel Minnowboard, которая реализует часть интерфейсов Fastwel CPC1311 и использует тот же чипсет и центральный процессор.

Разработанная для Intel Minnowboard защищенная программа может быть в дальнейшем с небольшими доработками портирована на плату Fastwel CPC1311.

2 РАЗРАБОТКА ЗАЩИЩЕННОЙ ПРОГРАММЫ ИНИЦИАЛИЗАЦИИ АППАРАТНОЙ ПЛАТФОРМЫ

Защищенная программа инициализации аппаратной платформы может быть представлена в виде логических модулей, которые реализуют ее функциональные возможности:

1. Модуль ПО BIOS – должен выполнять основные функции оригинального ПО BIOS после его замещения защищенной программой инициализации аппаратной платформы;

2. Модуль доверенной загрузки – должен выполнять функции доверенной загрузки, реализуемые защищенной программой инициализации аппаратной платформы;

3. Бинарные вставки от производителя системной логики – должны выполнять инициализацию аппаратных ресурсов платформы по алгоритмам, которые не раскрываются производителями.

Обобщенный алгоритм работы защищенной программы инициализации аппаратной платформы с учетом ее разделения на логические модули представлен ниже (Рисунок 1).

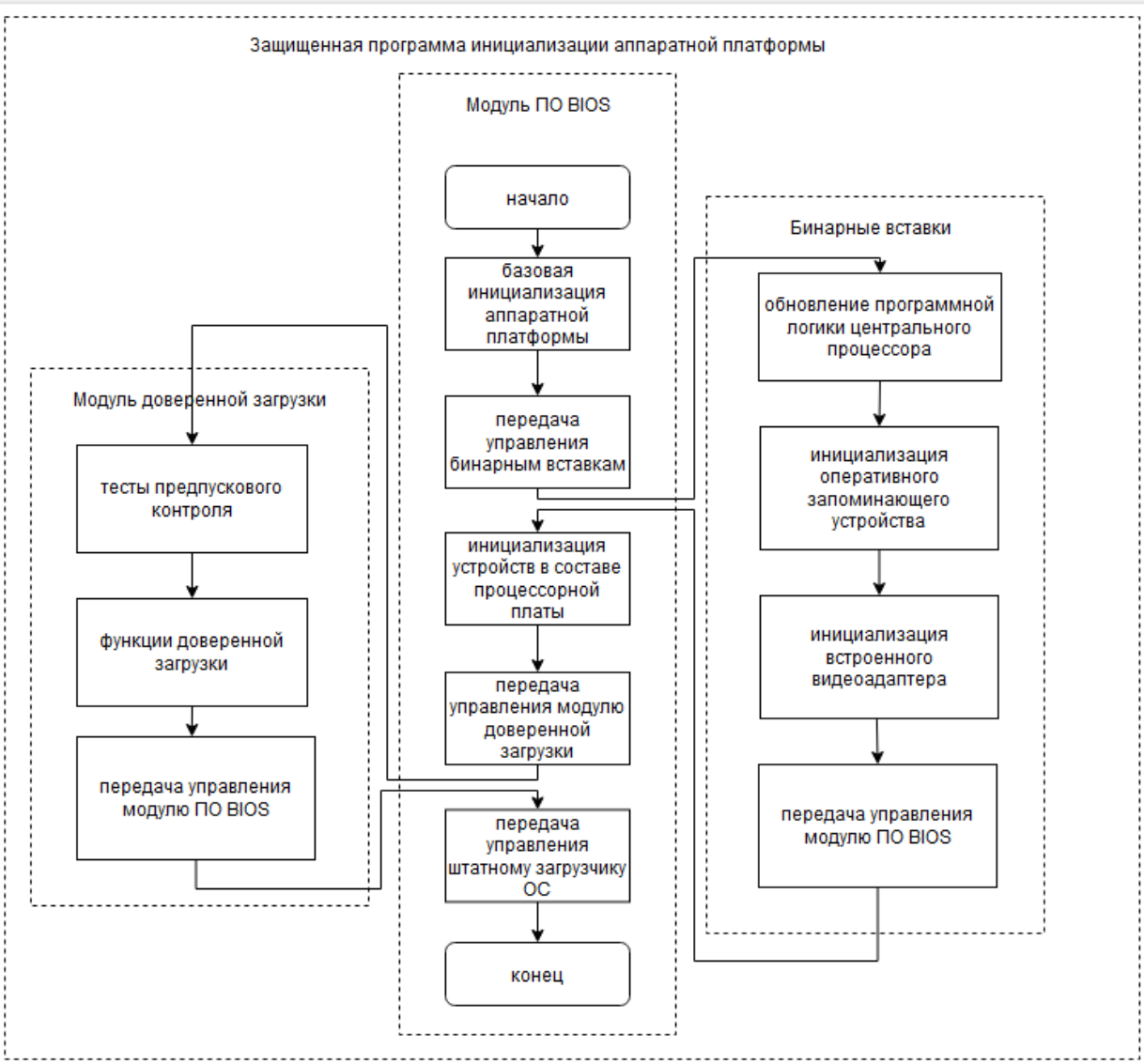


Рисунок 1 – Обобщенный алгоритм выполнения защищенной программы инициализации аппаратной платформы

Защищенная программа инициализации аппаратной платформы в процессе разработки будет тестироваться на процессорной плате Intel Minnowboard. При написании ПО требуется учитывать, что в дальнейшем программа должна быть с минимальными затратами портирована на плату Fastwel CPC1311.

2.1 Разработка модуля ПО BIOS

Модуль ПО BIOS – программное обеспечение, результатом компиляции которого является бинарная прошивка, предназначенная для записи в специальный накопитель на материнской плате и выполняющая инициализацию аппаратного обеспечения ЭВМ для его последующего использования операционной системой [6].

Разработка модуля ПО BIOS будет выполняться с использованием ПО проекта «Coreboot» - проекта с открытым исходным кодом, предназначенного для сборки ПО BIOS различных аппаратных платформ [7]. На текущий момент существуют готовые реализации и наборы настроек для систем на базе x86-архитектуры, ARM, MIPS, SPARC. ПО состоит преимущественно из исходного кода, который можно проанализировать на наличие недекларированных возможностей или потенциальных уязвимостей, что значительно повышает доверие к нему при анализе ПО регулирующими органами [8].

Аналогом проекта «Coreboot» является проект «Tianocore» на базе системы сборки «EDK II», поддерживаемый фирмой-производителем системной логики Intel. Однако, данный проект содержит большое число бинарных вставок и сборочных утилит без исходного кода, необходимых для сборки итогового образа ПО BIOS. В случае проведения сертификационных испытаний и работ, направленных на получение разрешения об использовании ПО BIOS в машинах, обрабатывающих информацию с содержанием государственной тайны, это приведет к необходимости дизассемблирования бинарных вставок с последующим восстановлением алгоритмов их работы. Процедура дизассемблирования является наиболее трудоемкой и дорогой при анализе ПО, из-за чего эффективность использования системы сборки «EDK II» для сборки защищенной программы инициализации аппаратной платформы ниже, чем использование проекта «Coreboot» [7].

Другим аналогом является проект «SlimBootloader», также поддерживаемый фирмой-производителем системной логики Intel. Данный проект состоит преимущественно из исходного кода и сравним по этому показателю с проектом «Coreboot». Отрицательным показателем проекта является небольшое количество поддерживаемых им аппаратных платформ: поддержка старых платформ отсутствует, кроме того не поддерживаются платформы не на базе системной логики фирмы Intel. Таким образом, наработки, полученные при работе с проектом «SlimBootloader», не получится использовать при необходимости портировать защищенную программу инициализации аппаратной платформы на платы фирмы AMD или для работы с аппаратной платформой на базе ARM-процессоров.

2.2.1 Модуль процессорной платы

Модуль материнской платы – набор программного кода и конфигурационных файлов, которые могут быть применены только при инициализации конкретной материнской платы.

Состав разработанного модуля процессорной платы:

1. Конфигурационные файлы, в которых указываются модули платформы Coreboot (программной платформы, с использованием которой разработан ПО BIOS) для их использования в процессе построения модуля BIOS. Для платы Fastwel CPC1311 было указано подключение кода soc/Intel BayTrail, предназначенного для инициализации чипсета аппаратной платформы Intel BayTrail;

2. Модуль конфигурации, который выполняет считывание массива настроек ПО BIOS из энергонезависимой памяти на раннем этапе инициализации платформы. По результатам анализа считанного массива настроек другими модулями ПО BIOS принимаются решения о внесении изменений в порядок инициализации процессорной платы

(включение/отключение отдельных устройств, пропуск отдельных стадий инициализации). Структура с настройками может быть размещена в памяти NVRAM (данная память присутствует на всех материнских и процессорных платах) или в памяти FRAM (накопитель с памятью данного типа размещен на плате Fastwel CPC1311);

3. Дерево устройство devicetree.cb, которое описывается перечень реализованных аппаратных устройств в составе материнской платы и размещенных на шине PCI, их адреса и соответствующие им номера аппаратных прерываний. При составлении дерева устройств для платы Fastwel CPC1311 использовалась официальная документация производителя материнской платы и утилита lspci ОС Linux;

4. Файлы ACPI, которые будут использованы операционной системой для управления энергопотреблением аппаратных устройств в составе материнской платы. Файлы ACPI были получены с помощью утилит пакета acpica-tools, запуск которых был выполнен из-под ОС Linux на материнской плате Fastwel CPC1311 со штатным BIOS.

5. Функции обратного вызова с кодом, специфичным для конкретной материнской платы. Данные функции будут вызваны платформой Coreboot на различных стадиях процесса выполнения доверенного загрузчика. Функции обратного вызова содержат код инициализации последовательного порта для включения отладочной консоли.

Полученный модуль материнской платы был размещен в директории src/mainboard/fastwel_cpc1311 для его использования в процессе компиляции доверенного загрузчика операционной системы.

2.2.2 Модуль графического интерфейса

Модуль графического интерфейса – набор функций, посредством

которых выполняется вывод символьной графики на экран пользователя до загрузки ОС.

Модуль графического интерфейса представлен в виде библиотеки с набором программных функций, посредством которых осуществляется управление отображаемым на экран изображением. Функции являются обертками над рядом ассемблерных инструкций, которые используют в своей работе прерывание INT 010h.

Реализованные в библиотеке программные функции можно разделить на две группы:

1. Отображение отдельных элементов (нумерованный список, маркированный список, поле ввода пароля и др.);

2. Манипуляции над изображением на экране (очистка экрана, переключение на другую вкладку графического интерфейса, манипуляция цветом символов и курсором и др).

Графический интерфейс, разработанный с использованием вышеописанной библиотеки, содержит следующие окна:

1. Окно авторизации пользователя представлено отдельным графическим элементом с полем для ввода пароля с установленным в нем курсором. Вводимый пользователем пароль не отображается на экране, вместо него поле заполняется специальными символами «*»;

2. Меню настроек содержит большое число графических элементов, таких как «список», «кнопка», «радиокнопка», «флаговая кнопка». Меню настроек не статично: пункты меню описываются содержимым структуры, которая размещена в энергонезависимой памяти и может быть легко изменено при необходимости доработки меню и внесения новых пунктов;

3. Меню настройки даты и времени, где пользователь может увидеть текущие значения даты и времени и изменить их с помощью манипулятора «клавиатура».

Разработанный графический интерфейс отображает информацию о процессе инициализации процессорной платы и выполнения функций доверенной, а также предоставляет возможности по конфигурации защищенной программы инициализации аппаратной платформы.

2.2.3 Модуль локализации

Модуль локализации позволяет сменить язык, сообщения на котором выводятся на экран пользователю. Поддержка русского языка в доверенном загрузчике необходима для его успешного распространения на отечественном рынке.

При выполнении стандартной BIOS используется набор символов, которые загружены в знакогенератор любой системы по умолчанию. Набор состоит из 256 символов и соответствует кодировке ASCII. Данная кодировка включает в себя набор символов, соответствующих буквам английского алфавита в обоих регистрах. Представление символа в знакогенераторе занимает 1 байт, каждый бит которого – состояние «закрашен/не закрашен» пикселя в составе символа.

Для поддержки смены языка была разработана функция, выполняющая подмену содержимого знакогенератора собственной таблицей символов с помощью аппаратного прерывания. Таблица символов генерируется разработанным скриптом на языке Golang, который анализирует таблицу символов Unifont (доступна в открытом доступе и содержит битовое представление символов из таблицы Unicode) и составляет из неё новую таблицу с рядом запрошенных символов. Полученная таблица формируется в

виде массива char[], который включается в состав исходного кода доверенного загрузчика и размещается в знакогенераторе.

Реализованная схема локализации используется для вывода русских символов на экран пользователя, но может быть использована и для добавления других языков (французский, испанский, итальянский и др.).

Весь текст, выводимый на экран пользователя, представлен в виде набор статичных фраз. Для каждого языка генерируется массив с переводами этих фраз. Смена языка, используемого в графическом интерфейсе, означает смену массива с переводами фраз.

Также в модуле локализация реализована функция записи в знакогенератор оригинального массива данных. ПО установленных в системе устройств или ПО загрузчиков операционных систем также может выводить на экран символьный текст и ожидает, что в знакогенераторе установлена стандартная таблица ASCII. Поэтому после завершения отображения графического интерфейса требуется вернуть в знакогенератор его содержимое по умолчанию.

2.2 Модуль доверенной загрузки

Модуль доверенной загрузки реализует функции доверенной загрузки защищенной программы инициализации аппаратной платформы. Результатом выполнения данного модуля является решение о запрете или продолжении инициализации аппаратной платформы.

Модуль доверенной загрузке не компилируется в отдельную программу или бинарную вставку в составе защищенной программы, а выполнен в виде логического программного модуля.

Список реализованных функций доверенной загрузки:

1. Аутентификация пользователя;

2. Контроль носителя, выбранного источником для загрузки операционной системы;

3. Тесты предпускового контроля.

2.2.1 Аутентификация пользователя

Аутентификация пользователя – процесс подтверждения соответствия пользователя некоторой личности на основе предъявляемых данных.

Аутентификация пользователя в качестве функции доверенной загрузки несет цель запретить пользователю, не обладающих достаточными правами, или потенциальному злоумышленнику вносить изменения в конфигурацию защищенной программы инициализации аппаратной платформы.

Защищенная программа инициализации аппаратной платформы не позволяет создавать новых пользователей.

Подразумевается, что существует два пользователя:

1. «Пользователь», эксплуатирующий ПЭВМ. Не имеет прав на настройку ПО BIOS и защищенной программы;
2. «Администратор», сопровождающий эксплуатацию ПЭВМ. Имеет права на настройку ПО BIOS и защищенной программы.

Аутентификация выполняется при попытке зайти в меню настройки защищенной программы инициализации аппаратной платформы. Пользователь должен ввести в окно ввода пароля комбинацию из 8 символов, хэш-сумма которой будет сравнена с хэш-суммой эталонного пароля, хранящейся в FRAM. В один сеанс загрузки системы пользователь может совершить три попытки аутентификации, после чего плату потребуется перезагрузить. В качестве хэш-функции используется CRC32.

В текущей реализации пользователь может выполнять перезагрузку платы и попытки аутентификации произвольное число раз, однако по требованиям эксплуатации конкретного комплекса логика функции аутентификации может быть изменена (к примеру, блокировка загрузки даже после перезагрузки платы до совершения «Администратором» вскрытия контролируемого устройства и сброса энергонезависимой памяти).

Загрузка системы в текущей версии программы разрешается неавторизованному пользователю: в случае корректного прохождения тестов предпускового контроля и наличия подключенного загрузочного носителя выполняется передача управления загрузчику ОС. Однако по требованию данная функция может быть доработана для требования обязательного ввода пароля от пользователя АРМ для загрузки ОС.

2.2.2 Контроль носителя, выбранного источником загрузки ОС

Контроль носителя – процесс подтверждения соответствия носителя, установленного в системе, выбранному ранее носителю.

Функция доверенной загрузки предназначена для предотвращения загрузки ОС с незарегистрированного носителя, который мог быть подключен злоумышленником к контролируемой системе.

Список подключенных носителей отображается в меню настроек защищенной программы инициализации аппаратной платформы, где пользователь «Администратор» может выбрать носитель «источником загрузки ОС». При этом в энергонезависимую память сохраняется информация о порте, к которому подключен носитель, и хэш-сумма названия носителя.

При последующих загрузках системы данная информация будет использована доверенным загрузчиком для прекращения загрузки системы и запрета передачи управления загрузчику ОС в следующих случаях:

1. К указанному порту не подключен носитель информации;
2. К указанному порту подключен носитель информации с другим идентификатором.

Передача управления штатному загрузчику ОС, установленному на указанном носителе, осуществляется с помощью прерывания. Если передача управления закончилась с ошибкой, на экран выводится текст с сообщением об ошибке и дальнейшая загрузка системы запрещается.

2.2.3 Тесты предпускового контроля

Тесты предпускового контроля – ряд процедур, по результату которых можно установить о корректности инициализации базовых аппаратных ресурсов системы и возможности дальнейшей загрузки ОС.

В состав тестов предпускового контроля входят:

1 Тестирование центрального процессора. В рамках данного теста выполняется проверка корректности установки флагов в процессе работы ЦП, корректности выполнения условных и безусловных переходов. Реализовано в виде набора ассемблерных процедур, которые в процессе своей работы выполняют арифметико-логические операции, устанавливающие флаги центрального процессора в конкретные значения. В случае, если ожидаемое значение флагов центрального процессора не сходится с полученным по факту значением, тест считается непройденным и дальнейшая загрузка системы запрещается;

2 Тестирование оперативного запоминающего устройства. В рамках данного теста выполняется проверка корректности операций чтения и записи

в оперативную память. Реализовано в виде функции, заполняющей регионы оперативной памяти конкретным значением. После выполняется процедура чтения значения из регионов оперативной памяти. Если в результате выполнения операции чтения было получение значение, отличное от записанного в область памяти, тест считается непройденным и дальнейшая загрузка системы запрещается;

3 Контроль целостности доверенного загрузчика. Реализован посредством расчета контрольной суммы по алгоритму CRC 32 на неизменяемые области прошивки загрузчика, содержащие исполняемый код. Каждая секция прошивки имеет заголовок, содержащий описывающую ее информацию (название, размер секции и др.). В процессе контроля целостности производится поиск местоположения бинарных секций из списка неизменяемых бинарных секций в составе прошивки и рассчитывается их контрольная сумма. Полученная сумма сравнивается с эталонной контрольной суммой, записанной непосредственно в бинарный образ защищенной программы инициализации аппаратной платформы

Процесс выполнения тестов предпускового контроля сопровождается выводом на экран текста о статусе выполнения тестов. В случае отрицательного результата выполнения одного из тестов загрузка платформы немедленно прекращается до перезагрузки процессорной платы.

2.3 Бинарные вставки

Бинарные вставки – бинарные файлы от производителей системной логики аппаратной платформы, выполняющие инициализацию отдельных аппаратных устройств системы.

Алгоритмы работы бинарных вставок являются «закрытыми» и не описаны в открытом доступе, поэтому без проведения полного дизассемблирования с последующим анализом алгоритма работы бинарных

вставок и разработки их аналога в исходном коде удаление бинарных вставок из состава защищенной программы инициализации аппаратной платформы невозможно.

В состав прошивки защищенной программы были включены следующие бинарные вставки:

1 Обновление микрокода центрального процессора. Микрокод ЦП – программная реализация инструкций центрального процессора. Бинарная вставка обновления микрокода позволяет заменить оригинальную программную реализацию собственной, указанной в бинарной вставке, что может быть использовано с целью внедрения уязвимостей непосредственно в алгоритм работы центрального процессора. Бинарная вставка поставляется в зашифрованном виде, ключ располагается во внутренней памяти центрального процессора. Таким образом, дизассемблирование с целью изучения содержимого бинарной вставки невозможно без предварительной дешифрации;

2 Бинарная вставка встроенного видеоадаптера. Содержит исполняемый код x86, выполняющий инициализацию встроенного графического адаптера, а также реализующий видео-сервисы BIOS;

3 Intel FSP. Выполняет инициализацию оперативного запоминающего устройства, установленного на процессорной плате. Бинарная вставка выполнена в формате UEFI и разделена на ряд отдельных исполняемых модулей, управление которым передается на различных этапах инициализации системы.

Вышеуказанные бинарные вставки включены в состав прошивки защищенной программы инициализации аппаратной платформы, контроль их целостности выполняется на этапе исполнения тестов предпускового контроля.

3 Тестирование защищенной программы инициализации аппаратной платформы

Процесс разработки сопровождался проведением тестирования и отладки защищенной программы инициализации аппаратной платформы с целью подтверждения корректности функционирования ее алгоритмов.

3.1 Процесс отладки

Отладка разработанной программы проводилась с помощью эмулятора аппаратных устройств QEMU x86. Решение обусловлено необходимостью при отладке на настоящей процессорной плате в постоянно развернутом отладочном стенде и в большом количестве операций перезаписи содержимого SPI-носителя, что может привести к исчерпанию ресурса перезаписи и выхода его из строя.

В эмуляторе была описана конфигурация процессорной платы Intel Minnowboard:

1 Аппаратная платформа: Intel BayTrail;

2 Центральный процессор: Intel Atom E3846;

3 Объем оперативной памяти: 4 Гбайт;

4 Набор предоставляемых интерфейсов.

В качестве загружаемой операционной системы был выбран образ ОС Ubuntu Linux 18.04. Данная ОС содержит ряд утилит, позволяющих узнать набор обнаруженных аппаратных ресурсов системы и их состояние, что полезно при отладке.

Изображение с исполняемой защищенной программой инициализации аппаратной платформы в эмуляторе QEMU x86 представлен ниже ().

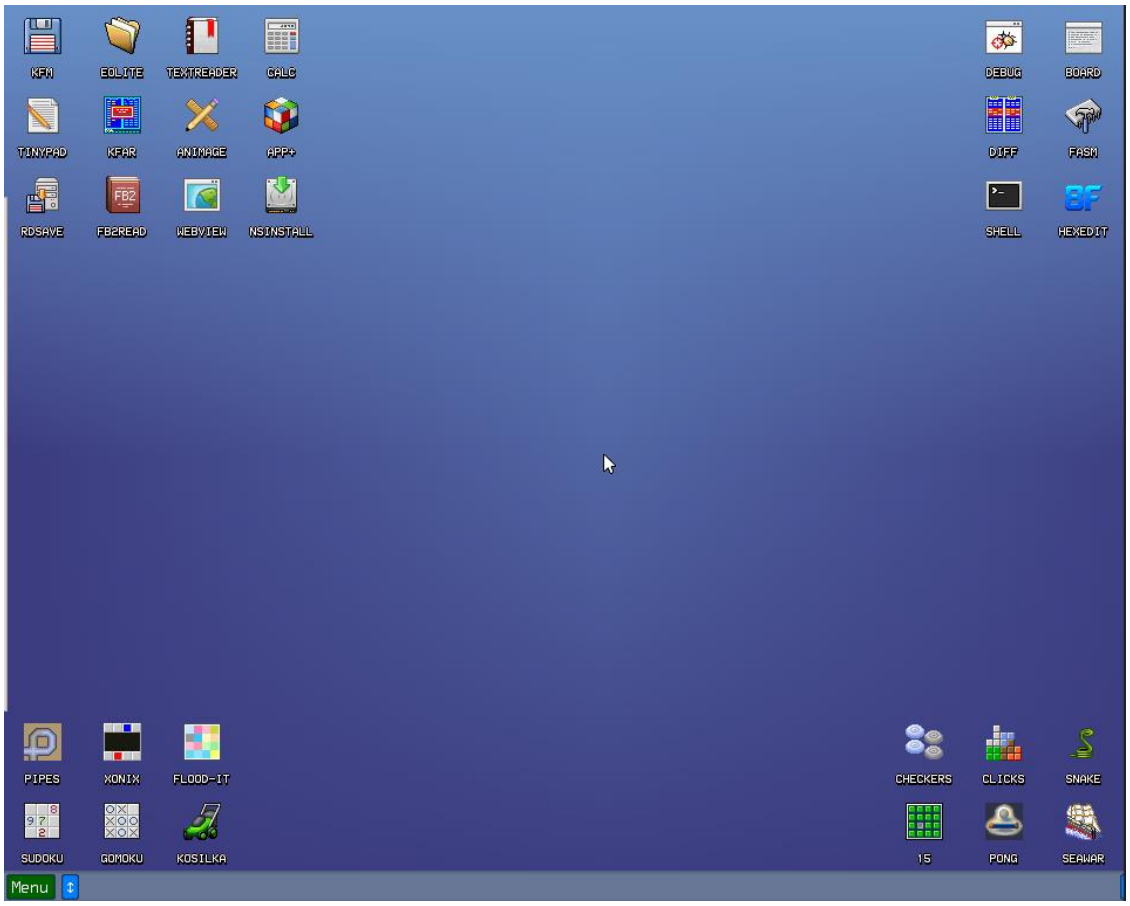


Рисунок 2 – Окно отладчика QEMU x86 с запущенной программой

Отладка в эмуляторе QEMU x86 позволила протестировать графический интерфейс и тесты предпускового контроля без запуска разработанной программы на реальной аппаратуре. Тестирование корректности инициализации подключенных в систему внешних аппаратных устройств проводилось с использованием процессорной платы.

3.2 Процесс тестирования

Тестирование защищенной программы инициализации аппаратной платформы проводилось с использованием процессорной платы Intel Minnowboard. Прошивка программы записана в носитель типа SPI на процессорной плате и заместила оригинальный образ ПО BIOS. Для

перезаписи содержимого носителя типа SPI использовался программатор Dediprog SF100.

В процесс тестирования вошли следующие проверки:

1 Тестирование предоставляемых процессорной платой интерфейсов. Были проведены проверки корректности работы установленных на плате интерфейсов: USB, mSATA, COM, mPCI-e. Тестирование проводилось посредством подключения к процессорной плате поддерживающих данные интерфейсы устройств и их детектирование в операционной системе. Тестирование завершено с положительным результатом;

2 Тестирование оперативной памяти с использованием утилиты Memtest86. Загрузочный образ утилиты размещен на USB-накопитель, который был подключен к процессорной плате и выбран в качестве источника загрузки операционной системы.

3 Тестирование функций доверенной загрузки. Тестирование проводилось посредством внесения изменений в бинарную прошивку защищенной программы инициализации аппаратной платформы, а также попыток войти в меню конфигурации ПО BIOS после введения некорректного пароля. Установлено, что после внесения изменений в прошивку на этапе выполнения тестов предпускового контроля выполняется остановка дальнейшей загрузки системы, в том числе не выполняется передача управления загрузчику ОС. В меню конфигурации ПО BIOS войти с некорректным паролем также не удалось.

По результатам проведения вышеуказанных тестов сделан вывод о корректности работы защищенной программы инициализации аппаратной платформы.

4 Руководство пользователя

В данном разделе будут рассмотрены вопросы инсталляции и эксплуатации защищенной программы инициализации аппаратной платформы.

4.1 Инсталляция

Инсталляция защищенной программы инициализации аппаратной платформы выполняется с помощью специализированного устройства: программатора.

Защищенная программа инициализации аппаратной платформы должна быть размещена в носителе из состава материнской (процессорной) плате, в котором по умолчанию размещен штатный образ ПО BIOS. Как правило, для этих целей на платах размещают носители типа SPI Flash размером 8/16/32 Мбайт. Однако, в редких случаях на плате могут быть носители другого типа (к примеру, носитель на шине LPC). В таком случае потребуется использовать соответствующий программатор.

Рассмотрим наиболее распространенный случай, в котором ПО BIOS размещен в носителе SPI Flash. При этом существуют следующие типы размещения носителей:

1. Носитель SPI Flash съемный. На процессорной плате находится сокет, в который может быть помещен SPI Flash-носитель (Рисунок 3). В таком случае требуется отключить процессорную плату от питания и извлечь носитель из сокета. Выходы программатора требуется соединить с соответствующими ножками носителя, после чего выполнить его перезапись. По завершению записи программы необходимо отсоединить программатор от SPI Flash-носителя и установить носитель в сокет.

Рисунок 3 – SPI Flash-носитель в специальном сокете

2. Носитель SPI Flash напаянный (Рисунок 4). Выходы программатора должны быть подключены к ножкам SPI Flash-носителя без его отсоединения от процессорной платы, процедура перезаписи содержимого носителя аналогична процедуре, выполняемой при перезаписи содержимого съемного носителя. Рекомендуется изучить документацию на предмет наличия на плате специальных выходов, соединенных с ножками микросхемы. В таком случае, программатор может быть подключен к данным выходам – это уменьшит шанс повредить напаянный носитель.

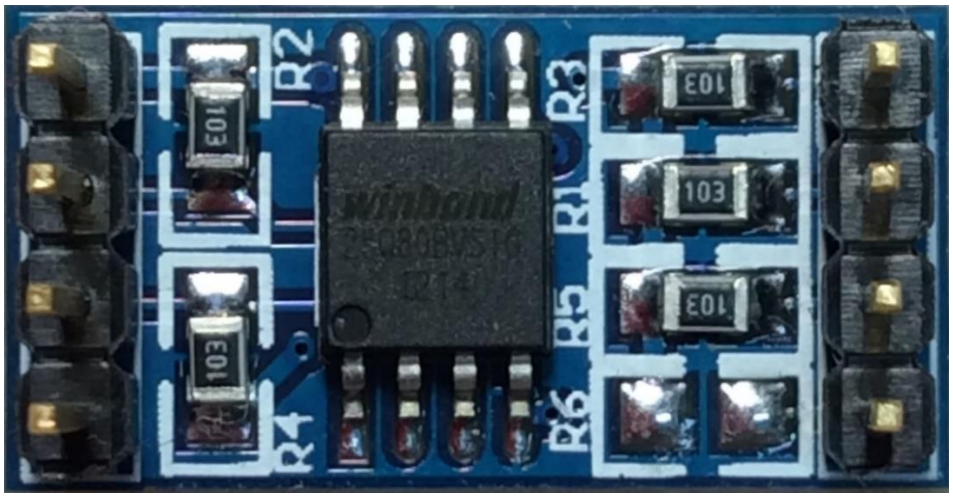


Рисунок 4 – SPI Flash-носитель припаян к плате

После завершения процедуры записи программы и отсоединения программатора от SPI Flash-носителя может быть подано питание на процессорную плату.

4.2 Эксплуатация

Для начала эксплуатации подайте сигнал включения ЭВМ. Вы увидите текст, содержащий информацию о процессорной плате в составе ЭВМ и версии прошивки защищенной программы инициализации аппаратной платформы (Рисунок 5).

Рисунок 5 –Экран "Информация о системе"

Процесс выполнения тестов предпускового контроля сопровождается выводом информации о статусе выполнения тестов (Рисунок 6). Тесты необходимы для проверки, что инициализация платформы завершена корректно и ЭВМ может эксплуатироваться пользователем.

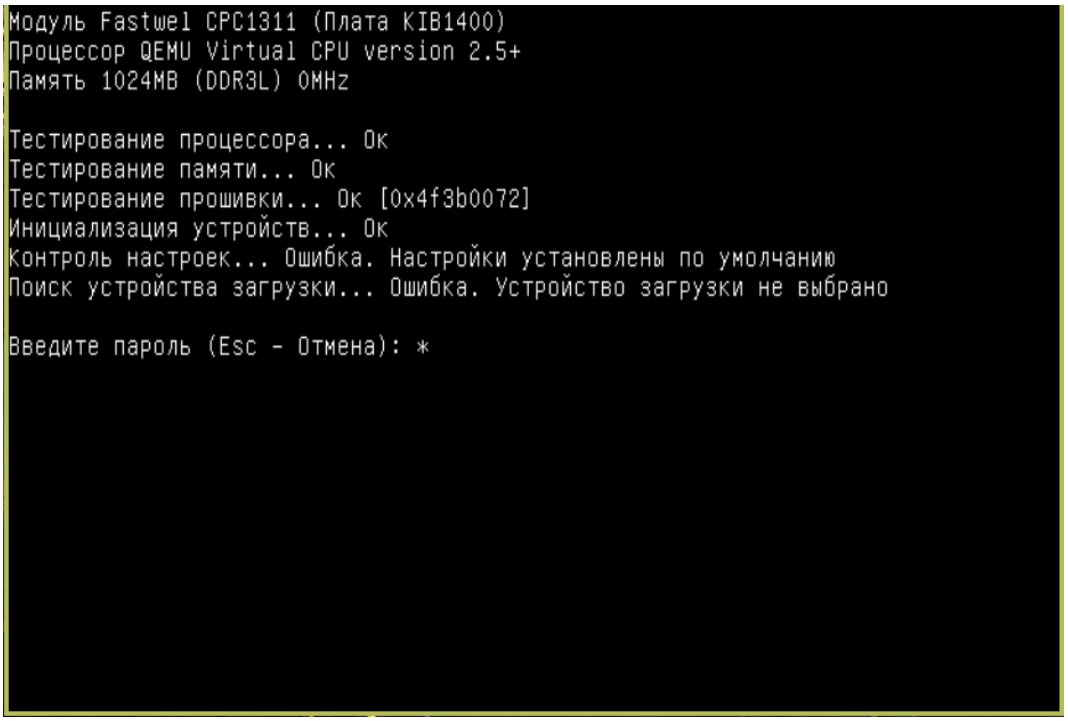


Рисунок 6 – Экран "Информация о выполнении тестов предпускового контроля"

После завершения тестов будет выведена информация о носителе информации, с которого будет завершена загрузка ОС (Рисунок 7).

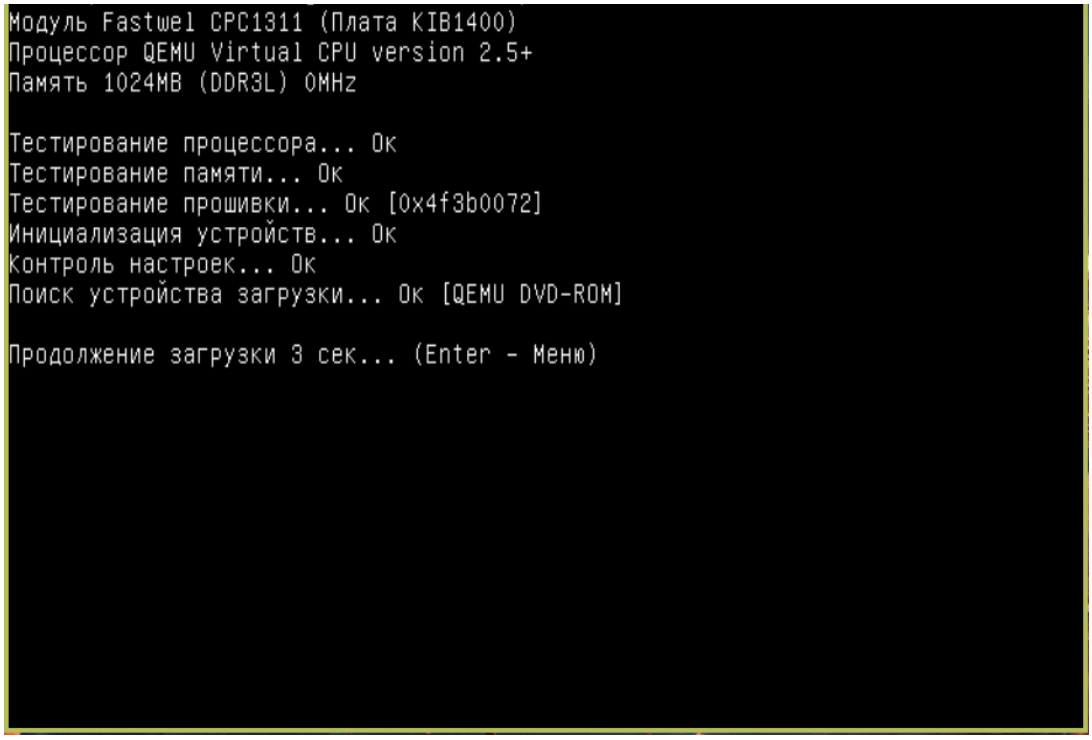


Рисунок 7 – Экран "Информация о выбранном носителе"

В случае, если выбранный носитель не обнаружен будет выведен соответствующий текст об ошибке и дальнейшая загрузка системы будет запрещена (Рисунок 8).

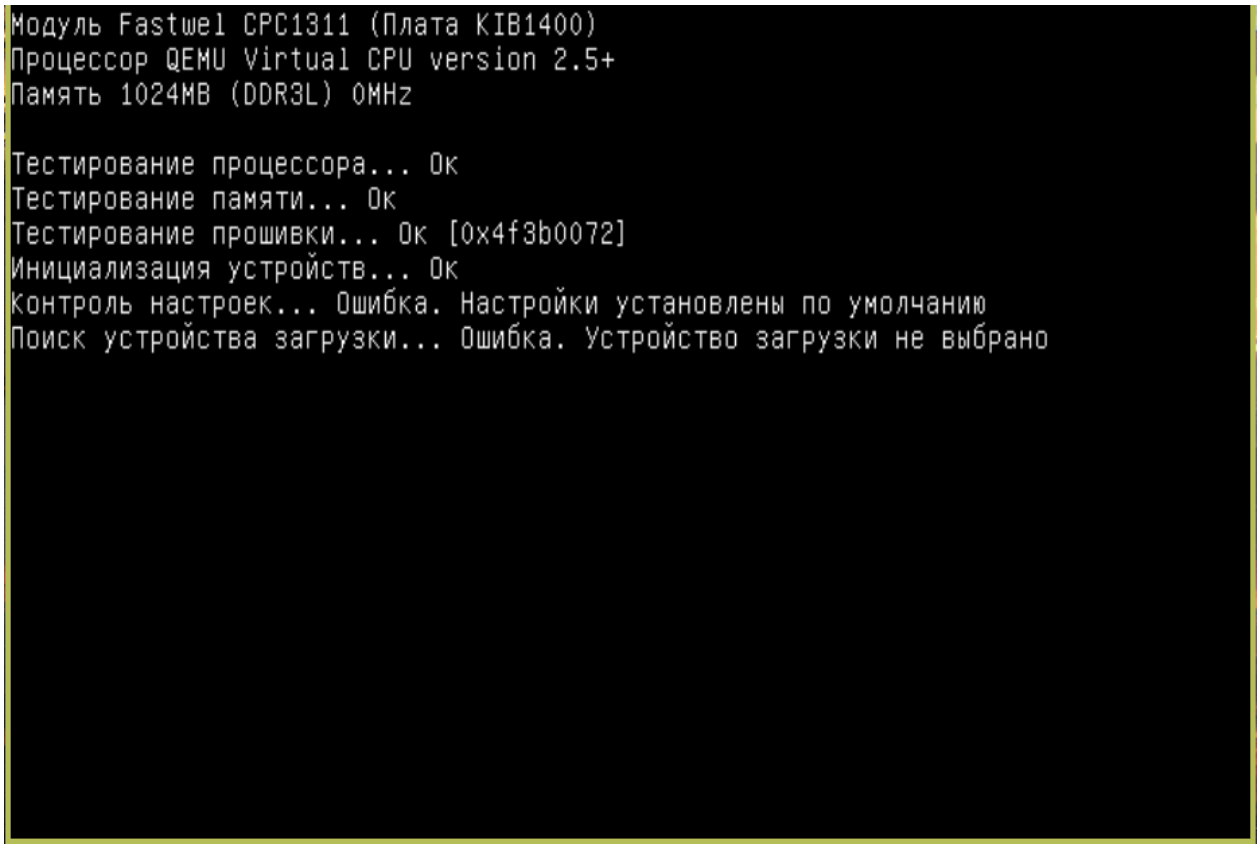


Рисунок 8 – Экран "Загрузка ОС запрещена"

Пользователь может нажать клавишу «ENTER» для входа в конфигурационное меню ПО BIOS. При этом будет выведено окно для ввода пароля пользователя (Рисунок 9). Вводимые символы заменяются на символ «звёздочка» при отображении на экране, чтобы не показывать вводимый пользователь пароль.

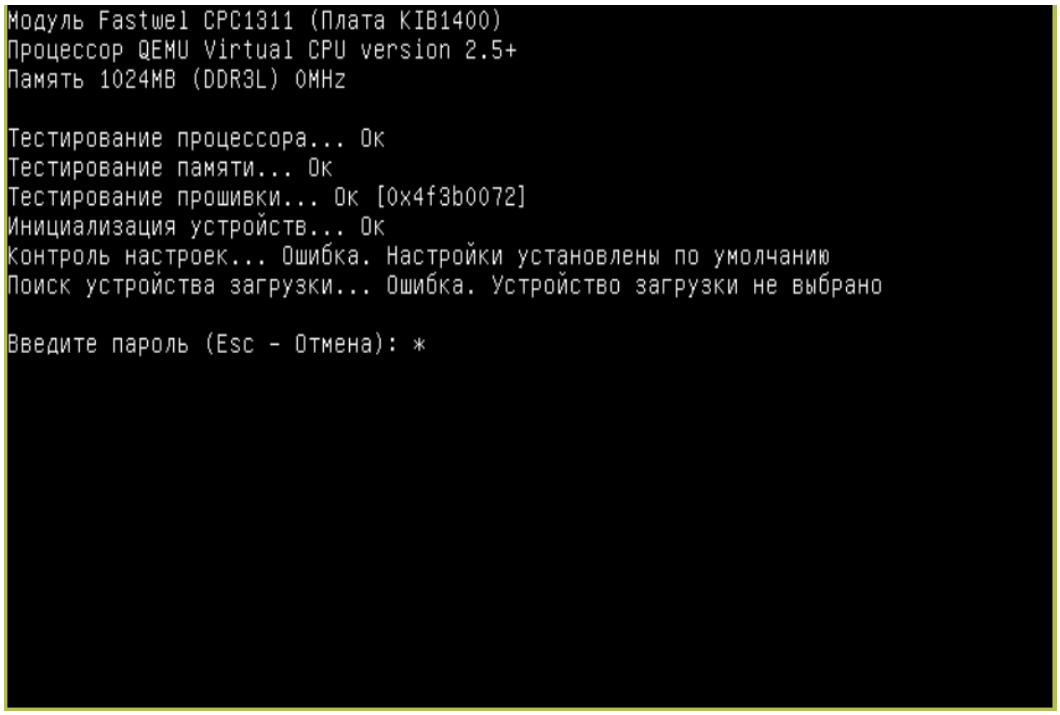


Рисунок 9 – Окно "Аутентификация пользователя"

В меню конфигурации ПО BIOS пользователь клавишами «стрелка» может выбрать пункт меню для изменения конкретных настроек (Рисунок 10).

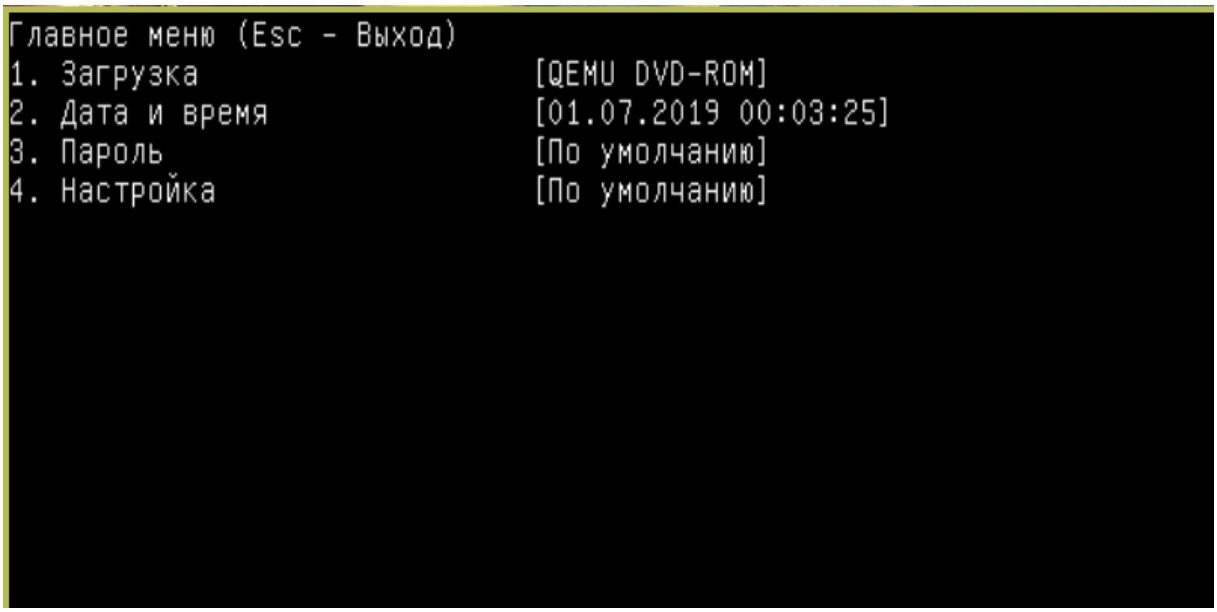


Рисунок 10 – Окно "Конфигурация ПО BIOS"

«Источник загрузки ОС» позволяет пользователю изменить носитель информации, который будет использован как источник для загрузки ОС по умолчанию (Рисунок 11).

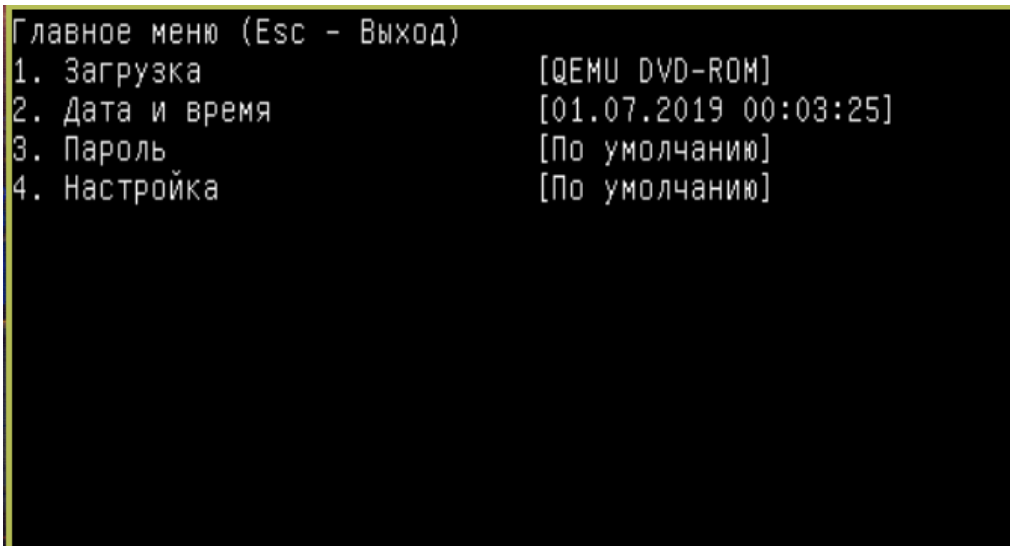


Рисунок 11 – Окно "Источник загрузки ОС"

«Смена пароля» позволяет пользователю изменить текущий пароль «Администратора» (Рисунок 12). Изменение вступит в силу немедленно после выполнения операции.

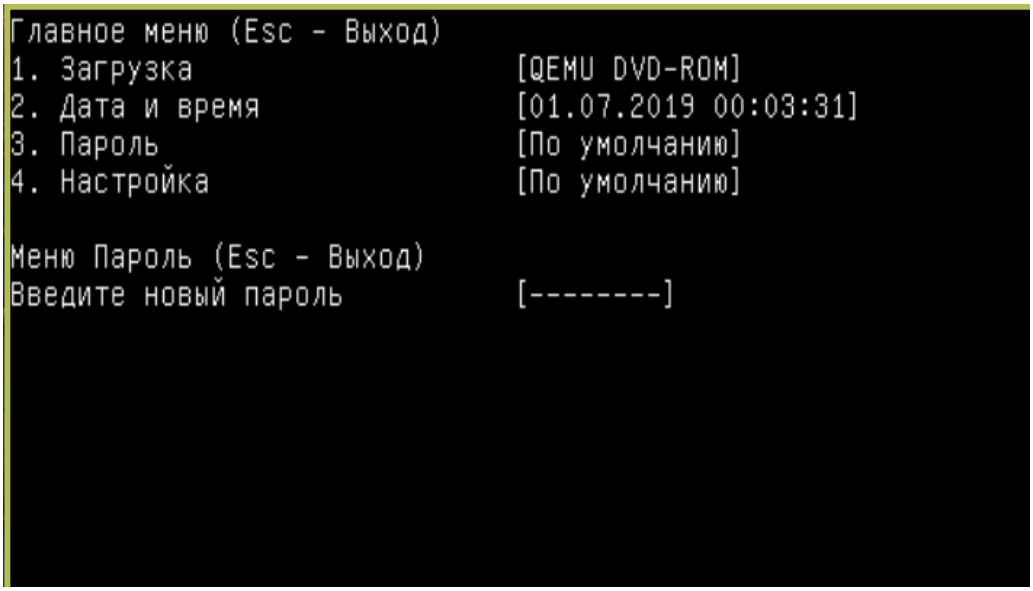


Рисунок 12 – Окно "Смена пароля"

«Дата и время» позволяет изменить текущие дату и время, отображаемые при инициализации системы и в ОС (Рисунок 13).

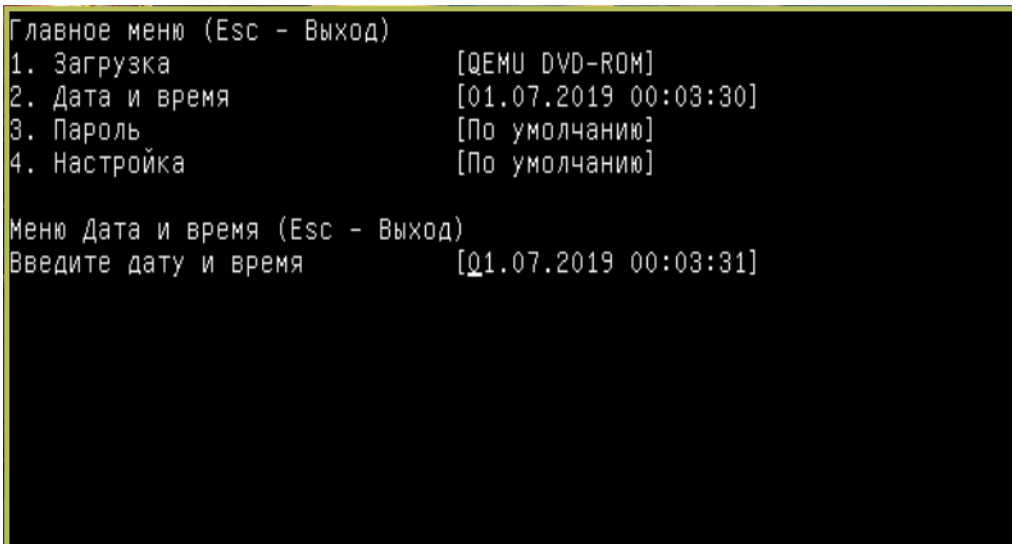


Рисунок 13 – Окно "Дата и время"

«Настройки системы» позволяет изменить настройки инициализации системы (Рисунок 14). Изменение настроек выполняется с помощью нажатий на клавиши стрелочного ввода или цифры, соответствующей номеру настройки. После внесения изменений в настройки будет выполнена перезагрузка системы для выполнения инициализации процессорной платы с использованием новых настроек.

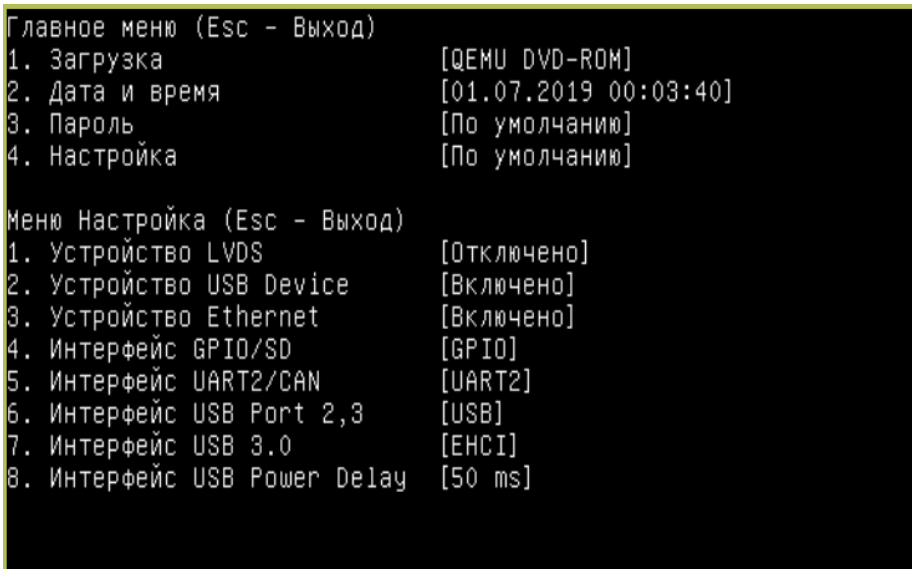


Рисунок 14 – Окно "Настройки системы"

Выход из данного меню выполняется с помощью нажатия на клавишу «ESC».

Передача управления штатному загрузчику ОС выполняется с выводом сопровождающего текста (Рисунок 15).

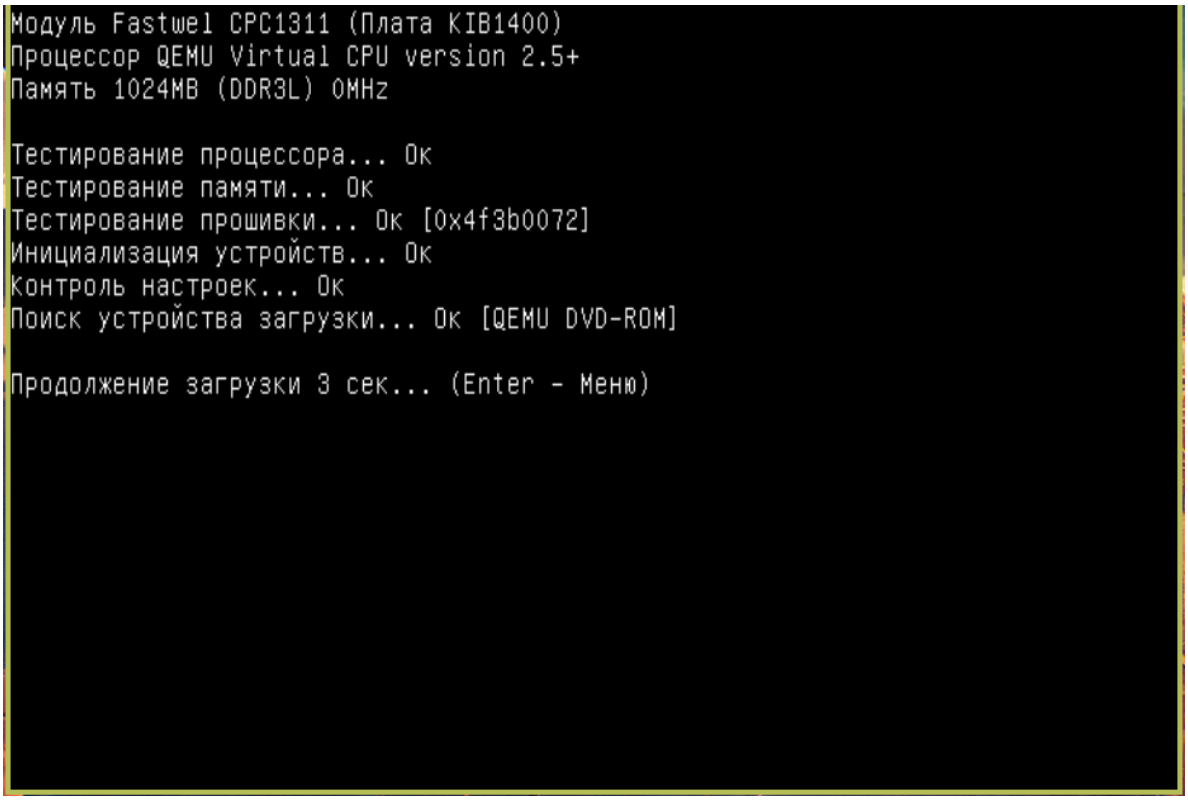


Рисунок 15 – Графический интерфейс перед передачей управления загрузчику ОС

После этого выполняется передача управления штатному загрузчику операционной системы.

ЗАКЛЮЧЕНИЕ

Результатом магистерской диссертации является программа, выполняющая инициализацию процессорной платы на базе аппаратной платформы Intel Baytrail и выполняющая функции доверенной загрузки, такие как аутентификация пользователя, контроль исполняемого образа ПО BIOS и тестирование базовых аппаратных ресурсов системы.

Программа выполнена в исходном коде и содержит только необходимый бинарный код (284 Кбайт по сравнению с 8 Мбайт в оригинальном ПО BIOS). Процессорная плата Intel Minnowboard, инициализация которая выполняется разработанной программой, является аналогом платы Fastwel CPC1311 российского производства с имеющейся у производителя документацией на ее схемотехнику. Таким образом, разработанная программа может быть доработана и исполняться на плате российского производства, что потенциально повышает доверие регулирующего органа к изделиям на основе платы с защищенной программой инициализации аппаратной платформы.

В процессе выполнения магистерской диссертации были опубликованы научные статьи на тематику разработки защищенной программы инициализации аппаратной платформы и перспективы замещения ПО BIOS в процессорных и материнских платах отечественного производства.

Имеющийся исходный код может быть предоставлен в испытательную лабораторию для проведения его сертификации по требования регулирующих органов и получения заключения о возможности использования защищенной программы инициализации аппаратной платформы в составе изделий, обрабатывающих информацию с содержанием государственной тайны.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. *Боровиков А.Ю., Новиков К.Б., Маслов О.А.* (2019) Описание подхода программной реализации модуля доверенной загрузки операционной системы // Наукоемкие технологии в космических исследованиях Земли. №1. С.43-48.

2. *Новиков К.Б., Боровиков А.Ю.* (2018) Рассмотрение возможности программной реализации модуля доверенной загрузки операционной системы // Новые информационные технологии и системы, С.32-34.

3. *Боровиков А.Ю., Новиков К.Б., Маслов О.А.* (2019) Принципы реализации программного модуля доверенной загрузки // Современные технологии автоматизации. №3. С.60-63.

4. *Лыдин С.С.* (2016) О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS // Вопросы защиты информации. №3. С.45-50.

5. *Хрусталев О.А.* (2017) Аппаратно-программный модуль доверенной загрузки // Аллея науки. №10. С.800-804.

6. *Чепанова Е.Г.* (2014) Формирование критериев сравнения модулей доверенной загрузки // Вопросы защиты информации. №4. С.60-63.

7. Coreboot Developer Manual. [Электронный ресурс]. – Электрон.дан. – URL: https://www.coreboot.org/Developer_Manual – 03.02.2018 г.

8. *Счастный Д.Ю.* (2017) Перспективы развития средств доверенной загрузки. Взгляд разработчика // Вопросы защиты информации. №3. С27-28.

9. *Чекин Р.Н.* (2010) Современные угрозы безопасности обработки информации со стороны встроенного программного обеспечения BIOS // Доклады ТУСУРа. №1. С.54-55.

ПРИЛОЖЕНИЕ А
ЛИСТИНГИ ПРОГРАММЫ

Приложение А.1

Файл mainboard.c

Приложение А.2

Файл generate_locales.go

Приложение А.3

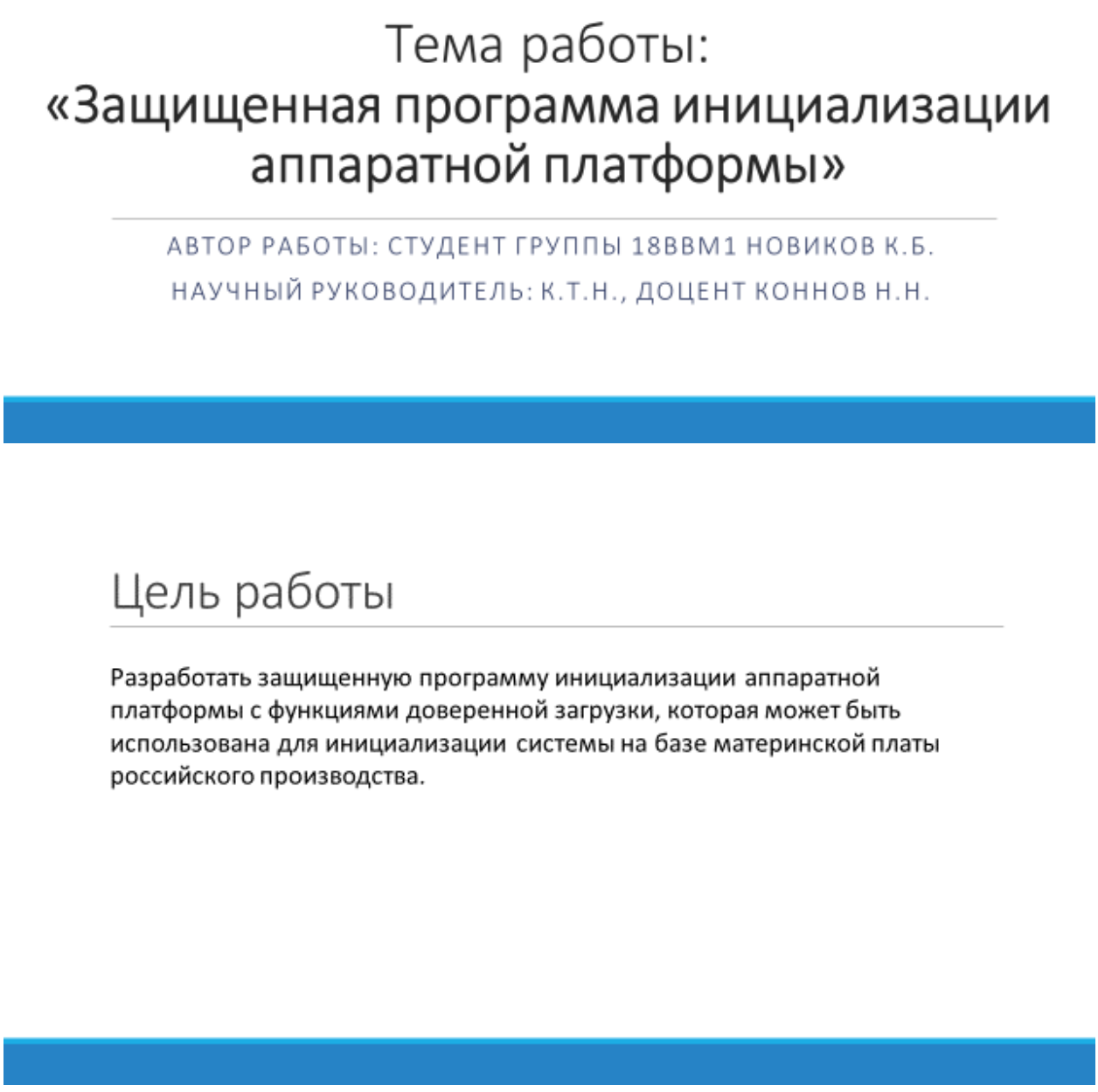
Файл codeLanguage.go

Приложение А.4

Файл graphics.c

ПРИЛОЖЕНИЕ В

ПРЕЗЕНТАЦИЯ



Доверенная загрузка

- Инициализация аппаратной платформы
- Передача управления штатному загрузчику ОС
- Функции доверенной загрузки:
  - Аутентификация пользователя
  - Журналирование процесса инициализации
  - Контроль целостности ПО BIOS
  - Контроль состава аппаратного обеспечения
  - Контроль состава подключенных носителей информации

«Соболь»

«Максим-М1»

«Центурион»

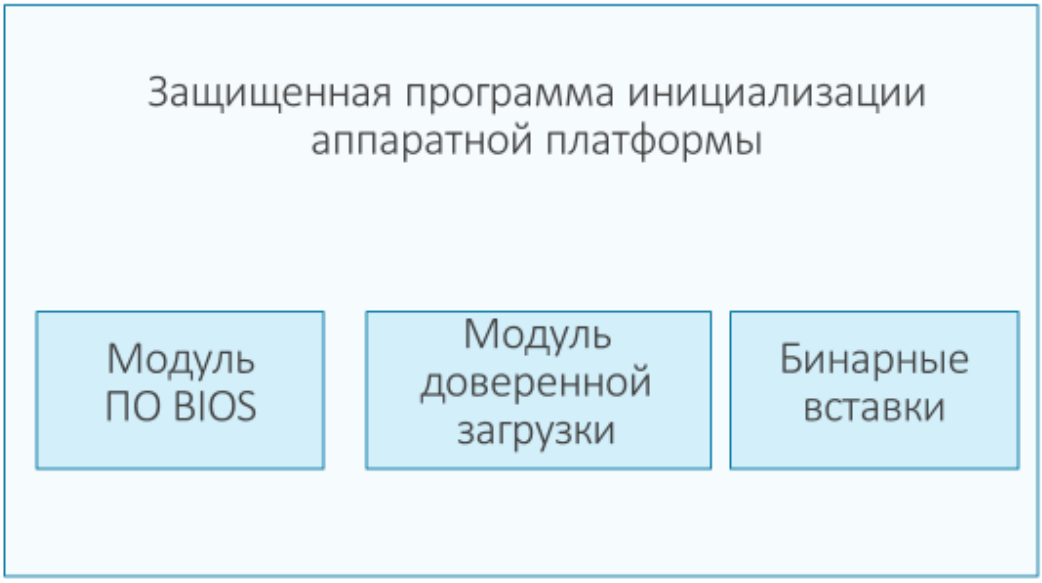
Преимущества программной реализации

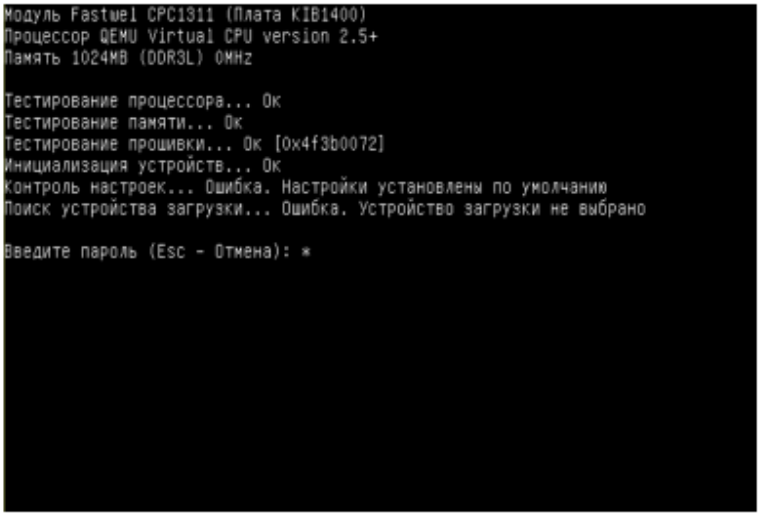
- Начало работы после включения ЭВМ
- Наличие исходного кода
  - Возможность доработки программы
  - Возможность провести анализ кода на предмет наличия уязвимостей
- Независимость от аппаратной составляющей при встраивании

Российская плата Fastwel CPC1311

Характеристики

- Процессор Intel Atom E38xx с тактовой частотой до 1,91 ГГц
- Оперативная память DDR3L до 4 Гбайт с поддержкой ECC
- eMMC Flash диск: 8 Гбайт
- Видеоконтроллер с интерфейсом LVDS/eDP (разрешение до 2560x1600 пикселей)
- Разъем COM-Express COM.0 Type 10 (1xGbEthernet, 5xUSB 2.0, 1xUSB 3.0, 2xSATA II, 3xPCIe x1, CAN 2.0 B)
- Потребляемая мощность от 12 Вт
- Температурный диапазон эксплуатации -40...+ 85°C


Защищенная программа инициализации аппаратной платформы
Модуль ПО BIOS
Модуль доверенной загрузки
Бинарные вставки


Модуль Fastwel CPC1311 (Плата KIB1400)
Процессор QEMU Virtual CPU version 2.5+
Память 1024MB (DDR3L) 0MHz
Тестирование процессора... Ok
Тестирование памяти... Ok
Тестирование прошивки... Ok [0x4f3b0072]
Инициализация устройств... Ok
Контроль настроек... Ошибка. Настройки установлены по умолчанию
Поиск устройства загрузки... Ошибка. Устройство загрузки не выбрано
Введите пароль (Esc - Отмена): *

Результаты работы

- Разработана защищенная программа инициализация аппаратной платформы, выполняющая доверенную загрузку ОС на плате российского производства Fastwel CPC1311
- Опубликованы четыре научные статьи в российских журналах по данной тематике, в том числе научная статья ВАК.

Спасибо за внимание