

УТВЕРЖДЕНО

BIOS REALINTECHPRO

Описание программы

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. и дата

г. Москва
2024

Содержание

1.	ОБЩИЕ СВЕДЕНИЯ.....	5
1.1.	НАИМЕНОВАНИЕ СИСТЕМЫ	5
1.2.	ПЕРЕЧЕНЬ ОРГАНИЗАЦИЙ, УЧАСТВУЮЩИХ В РАЗРАБОТКЕ СИСТЕМЫ..	5
1.3.	ИСПОЛЬЗУЕМЫЕ ЯЗЫКИ ПРОГРАММИРОВАНИЯ	5
1.4.	СРЕДА ФУНКЦИОНИРОВАНИЯ	5
2.	ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ ИЗДЕЛИЯ	6
2.1.	НАЗНАЧЕНИЕ ИЗДЕЛИЯ	6
2.2.	ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ	6
2.3.	ФУНКЦИОНАЛЬНЫЕ ОГРАНИЧЕНИЯ	7
3.	ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ.....	8
3.1.	ИНФОРМАЦИЯ О МОДУЛЯХ, СОСТАВЛЯЮЩИХ ИЗДЕЛИЕ.....	8
3.2.	СРЕДСТВА РАЗРАБОТКИ, ИСПОЛЬЗУЕМЫЕ ДЛЯ СБОРКИ ИЗДЕЛИЯ	10
3.3.	ФАЙЛЫ, СОСТАВЛЯЮЩИЕ ДИСТРИБУТИВ ИЗДЕЛИЯ.....	10
3.4.	ПРИМЕНЯЕМЫЕ МЕТОДЫ	11
3.5.	АЛГОРИТМ РАБОТЫ ПРОГРАММЫ	11
4.	ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА.....	14
5.	ВЫЗОВ И ЗАГРУЗКА	15
5.1.	УСТАНОВКА ПРОГРАММЫ.....	15
5.2.	ЗАПУСК ПРОГРАММЫ.....	17
6.	ВХОДНЫЕ ДАННЫЕ.....	18
7.	ВЫХОДНЫЕ ДАННЫЕ	19

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА.....	14
					5. ВЫЗОВ И ЗАГРУЗКА	15
Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	5.1. УСТАНОВКА ПРОГРАММЫ.....	15
					5.2. ЗАПУСК ПРОГРАММЫ.....	17
Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	6. ВХОДНЫЕ ДАННЫЕ.....	18
					7. ВЫХОДНЫЕ ДАННЫЕ	19

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Аббревиатура	Наименование
ЛУ	- Лист утверждения
ОС	- Операционная система
ПО	- Программное обеспечение
ACPI	- Advanced Configuration and Power Interface (Улучшенный интерфейс конфигурации и питания)
BDS	- Boot Device Select. Фаза поиска загрузчика операционной системы.
DXE	- Driver Execution Environment. Фаза инициализации устройств.
I2C	- Inter integrated circuit (Синхронная шина передачи данных)
NVM	- Non-Volatile Memory Host Controller Interface Specification (Интерфейс взаимодействия с постоянным запоминающим устройством)
PCIe	- Peripheral Component Interconnect Express (Интерфейс для соединения периферийных устройств)
PEI	- Pre EFI Initialization. Вторая фаза инициализации платформы
QEMU	- Программное обеспечение эмуляции и виртуализации.
SEC	- Security. Начальная фаза инициализации платформы.
SPI	- Serial Peripheral Interface (Последовательный интерфейс периферийных устройств)
UART	- Universal asynchronous receiver-transmitter (Универсальный асинхронный приемо-передатчик)
UEFI	- Unified Extensible Firmware Interface (Унифицированный расширяемый аппаратный интерфейс)
USB	- Universal Serial Bus (Универсальная последовательная шина)

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	PCle	- Peripheral Component Interconnect Express (Интерфейс для соединения периферийных устройств)
					PEI	- Pre EFI Initialization. Вторая фаза инициализации платформы
Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	QEMU	- Программное обеспечение эмуляции и виртуализации.
					SEC	- Security. Начальная фаза инициализации платформы.
Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	SPI	- Serial Peripheral Interface (Последовательный интерфейс периферийных устройств)
					UART	- Universal asynchronous receiver-transmitter (Универсальный асинхронный приемо-передатчик)
Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	UEFI	- Unified Extensible Firmware Interface (Унифицированный расширяемый аппаратный интерфейс)
					USB	- Universal Serial Bus (Универсальная последовательная шина)

1. ОБЩИЕ СВЕДЕНИЯ

1.1. НАИМЕНОВАНИЕ СИСТЕМЫ

Обозначение изделия: BIOS REALINTECHPRO.

Полное наименование системы: BIOS REALINTECHPRO.

1.2. ПЕРЕЧЕНЬ ОРГАНИЗАЦИЙ, УЧАСТВУЮЩИХ В РАЗРАБОТКЕ СИСТЕМЫ

Организация-разработчик: Общество с ограниченной ответственностью «ИНТЕХПРО» (ООО «ИНТЕХПРО»), 124575, г. Москва, вн.тер.г. муниципальный округ Силино, г. Зеленоград, К. 1003, помещ. 11Н

1.3. ИСПОЛЬЗУЕМЫЕ ЯЗЫКИ ПРОГРАММИРОВАНИЯ

При разработке изделия были использованы следующие языки программирования:

- Assembler;
- C/C++;
- Perl.

1.4. СРЕДА ФУНКЦИОНИРОВАНИЯ

Требования к программной среде функционирования отсутствуют.

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Из	Лист	№ докум.	Подп.	Дата					Лист
									5

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ ИЗДЕЛИЯ

2.1. НАЗНАЧЕНИЕ ИЗДЕЛИЯ

Изделие предназначено для начальной загрузки материнских плат REALINTECHPRO, передачи управления загрузчику установленной на него операционной системы и предоставления работающей операционной системе доступа к аппаратным ресурсам и подключенным периферийным устройствам.

2.2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

Изделие реализует следующие функциональные возможности:

- выполняет инициализацию материнской платы REALINTECHPRO
- после завершения работы передает управление загрузчику операционной системы
- поддерживает UEFI 2.8 и EDK 2
- поддерживает PI 1.7 и ACPI 6
- поддерживает определение и инициализацию устройств, подключенных через интерфейс PCI-E
- поддерживает определение и инициализацию устройств USB 1.x, 2.0, 3.0
- предоставляет графический интерфейс пользователя
- имеет возможность журналирования неполадок и ошибок, возникших во время работы
- поддерживает загрузку по протоколу NVMe
- предоставляет возможность выполнять обновление микропрограмм материнской платы REALINTECHPRO
- предоставляет возможность мониторинга производительности материнской платы REALINTECHPRO при загрузке
- имеет в своем составе программные средства для проверки целостности и безошибочной работы оперативной памяти
- имеет возможность самостоятельно восстанавливаться после неполадок
- предоставляет возможности для ручного восстановления, такие как:
 - а. восстановление с использованием интерфейса UART

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата					
Из	Лист	№ докум.	Подп.	Дата					
					Лист				
					6				

В. ВОССТАНОВЛЕНИЕ С ЖЕСТКОГО ДИСКА

- поддерживает процессоры Intel 12, 13, 14 поколений
- поддерживает работу с виртуальными процессорами с использованием QEMU
- предоставляет возможность автоматической миграции на UEFI
- имеет модульную архитектуру, что позволяет изменять функциональность по требованию.

Функциональные ограничения на применение данного изделия связаны с тем, что программное обеспечение рассчитано на работу на материнских платах REALINTECHPRO.

[illegible]

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

- | | | | | |
|--------------|--------------|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
| | | | | |

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

- | | | | | |
|--------------|--------------|--------------|--------------|--------------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
| | | | | |

- переключение в защищённый режим процессора с плоской памятью без подкачки;
- обновление микрокода;
- переход в режим использования кэша процессора в качестве временной RAM;
- передача управления в фазу PEI.

Фаза PEI подготавливает необходимое количество непрерывной оперативной памяти, достаточного для перехода в фазу DXE. При этом выполняются следующие шаги:

- перенос данных из ROM во временную оперативную память, размещённую в кэше процессора;
- запуск диспетчера модулей/драйверов, который выполняет модули в необходимом порядке, с учётом их зависимостей;
- инициализация базовых интерфейсов платформы;
- инициализация основной памяти и перенос в неё данных из временной памяти;
- если система находится в состоянии S3 Resume, то управление передаётся вектору восстановления операционной системы;
- если система не находилась в состоянии S3 Resume, то управление передаётся фазе DXE.

Фаза DXE обеспечивает выполнение окончательной инициализации всех устройств на основании информации, которая была передана из предыдущей фазы. После этого выполняется фаза поиска загрузчика операционной системы (BDS) на всех доступных носителях. В случае, если поиск загрузчика ОС завершился неудачей, то запускается оболочка UEFI или выводится сообщение о том, что ОС не найдена. В случае успешного обнаружения загрузчика, управление передаётся этому загрузчику.

Перед передачей управления операционной системе, программное обеспечение UEFI создаёт таблицы ACPI, в которых сохраняется конфигурация сервера, которая была обнаружена на этапе инициализации.

Инв. № подл.	Подл. и дата	Взам. инв. №	Инв. № дубл.	Подл. и дата	Лист
Из	Лист	№ докум.	Подп.	Дата	9

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

						Лист
						10
Из	Лист	№ докум.	Подп.	Дата		

контрольных сумм gostsum в операционной системе Astra Linux, указаны на компакт-диске с Изделием.

3.4.ПРИМЕНЯЕМЫЕ МЕТОДЫ

Изделие реализовано в соответствии со стандартом интерфейса между операционной системой и низкоуровневым управлением оборудованием UEFI (Unified Extensible Firmware Interface).

После подачи питания изделие выполняет начальное тестирование и настройку устройств процессорной платы и внешних относительно процессорной платы устройств, находящихся на шине PCI, а также подключенных по периферийным интерфейсам, например, USB и другим.

Изначально выполняется тестирование собственно модуля процессора. Далее проверяется целостность содержимого ПЗУ, в которое записано программное обеспечение. Затем поочередно запускаются входящие в состав изделия программы, выполняющие тестирование и инициализацию оборудования. Настраивается и включается на отображение видеоконтроллер. Определяется объем установленного в системе оперативного запоминающего устройства, выполняется его тестирование.

В соответствии с настройками, заданными в пункте Boot, поочередно перебираются указанные устройства, пытаясь осуществить запуск с них операционной системы.

Изделие предоставляет возможность пользователю выполнять настройки UEFI через меню BIOS SETUP, которое вызывается с помощью нажатия клавиши “Delete” в процессе выполнения программного обеспечения.

В процессе выполнения генерируются POST коды, которые позволяют выяснить какой этап инициализации выполняется. В случае ошибок, генерируются коды ошибок, на основании которых можно получить информацию о причинах, из-за которых не произошло успешного запуска загрузчика ОС.

3.5.АЛГОРИТМ РАБОТЫ ПРОГРАММЫ

Структурная схема программы представлена на Рисунке 1.

Инв. № подл	Подп. и дата		Инв. № дубл.		Взам. инв. №		Подп. и дата							Лист
														11
	Из	Лист	№ докум.		Подп.		Дата							

выполняется его тестирование. В соответствии с настройками, заданными в пункте Boot, поочередно перебираются указанные устройства, пытаюсь осуществить запуск с них операционной системы. Изделие предоставляет возможность пользователю выполнять настройки UEFI через меню BIOS SETUP, которое вызывается с помощью нажатия клавиши “Delete” в процессе выполнения программного обеспечения. В процессе выполнения генерируются POST коды, которые позволяют выяснить какой этап инициализации выполняется. В случае ошибок, генерируются коды ошибок, на основании которых можно получить информацию о причинах, из-за которых не произошло успешного запуска загрузчика ОС. 3.5.АЛГОРИТМ РАБОТЫ ПРОГРАММЫ Структурная схема программы представлена на Рисунке 1.													
--	--	--	--	--	--	--	--	--	--	--	--	--	--

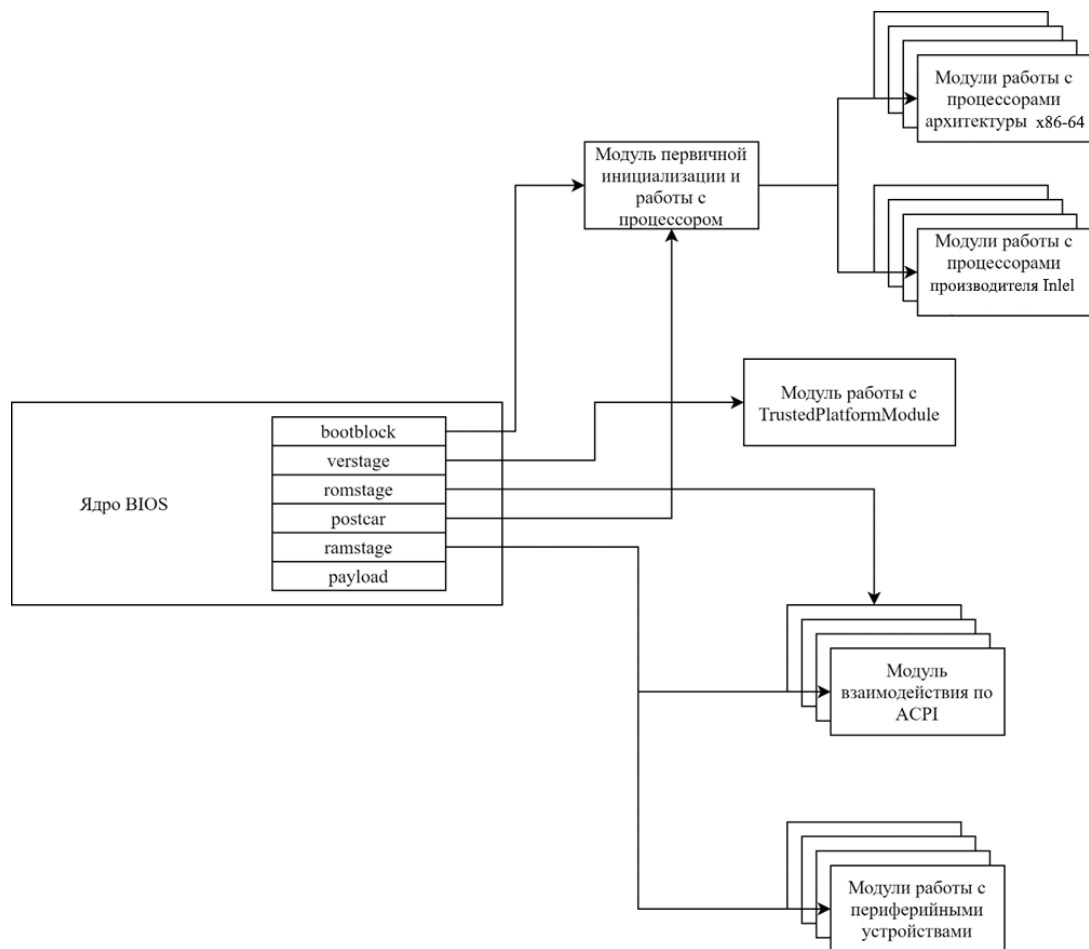


Рисунок 1 – Структурная схема программы

Общий алгоритм работы изделия можно разделить на несколько стадий, каждая из которых передает управление следующей.

Стадия bootblock является первой стадией, которая выполняется сразу после сброса CPU. Исходный код этой стадии написан на Assembler. Основная задача этой стадии – выполнить подготовку для работы в C окружении.

Основные задачи:

- инициализация кеша процессора для использования в качестве RAM
- установка указателя на стек
- инициализация памяти нулями
- обновление микропрограмм процессора
- инициализация системного таймера
- выполнение декомпрессии кода следующей стадии и его запуск

Стадия verstage - вторая стадия работы программного обеспечения. На этой стадии в память записывается программа, которая выполняет дешифровку и

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	Ис	Лист	№ докум.	Подп.	Дата	Лист
						12				

проверку кода последующих шагов на целостность. Код проверки далее будет выполняться при переходе к каждой следующей стадии. Эта стадия также позволяет убедиться, что код каждой стадии базовой системы ввода-вывода не изменился в процессе загрузки компьютера и все дальнейшие изменения могут быть возвращены в случае ошибки.

Стадия `romstage` инициализирует DRAM и выполняет подготовку к инициализации.

Стадия `postcar` выполняет частичный откат изменений шага `bootblock`. Из кеша процессора данные переносятся в уже инициализированную DRAM. После переноса данных происходит деинициализация кеша процессора и передача управления следующему шагу.

Предыдущие шаги выполнили базовую подготовку процессора и оперативной памяти для дальнейшей работы с периферийными устройствами. На стадии `ramstage` происходит обнаружение и инициализация периферийных устройств. Инициализируются:

- периферия на чипе (в случае наличия встроенных в процессор дополнительных модулей)
- PCI устройства
- TPM устройство (если его инициализация не была выполнена на стадии `verstage`)
- графические чипы (при их наличии).

После инициализации периферии составляется таблица обнаруженных и обработанных устройств для их использования ОС.

В качестве мер безопасности на этой стадии выставляется `read-only` флаг на область памяти, в которую помещен загрузчик ОС. Блокируются регистры процессора, связанные с безопасностью, а также блокируется SMM режим процессора. После этого управление передается загрузчику ОС или `payload`.

Стадия `payload` исполняет код, так называемой, «полезной нагрузки». Зачастую это загрузчик операционной системы, но в качестве `payload` может быть и программное обеспечение, которому не требуется наличие ОС.

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	Копировал Формат А4	Лист	13
Из	Лист	№ докум.	Подп.	Дата			

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

Минимальный состав технических средств:

- материнская плата REALINTECHPRO;
- Память оперативная 8 Гб
- Постоянное запоминающее устройство: 256 Гб

Выходные данные от программного обеспечения выводятся на подключаемый к материнской плате REALINTECHPRO внешний видеомонитор с интерфейсом VGA.

Инв. № подл	Подп. и дата				Взам. инв. №	Инв. № дубл.	Подп. и дата	
Из	Лист	№ докум.	Подп.	Дата				Лист
								14

5. ВЫЗОВ И ЗАГРУЗКА

5.1. УСТАНОВКА ПРОГРАММЫ

Установка экземпляра программного обеспечения BIOS REALINTECHPRO на флеш-память осуществляется по следующей инструкции.

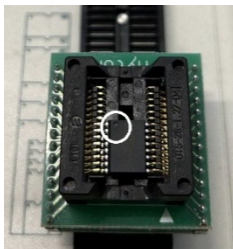
Установить утилиту для работы с программатором ChipProgUSB и на ПК под управлением ОС Windows, с которого будет осуществляться работа с программатором.

Включить программатор ChipProg-48.

Подключить к программатору ChipProg-48 адаптер для программирования микросхем DIP-SOIC 16/18/20/24/28 pin 300 mil.

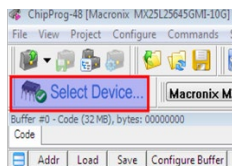


Установить в адаптер флеш-память согласно схеме, изображенной на программаторе (слева от адаптера), ключ должен быть слева вверху (см. рисунок ниже).



Запустить утилиту ChipProgUSB

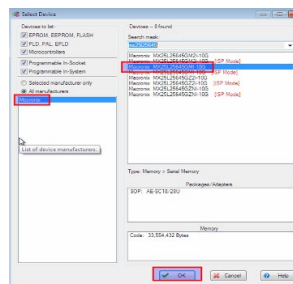
В левом верхнем углу интерфейса утилиты, как показано на рисунке снизу, нажать кнопку Select Device.



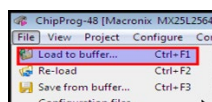
В открывшемся окне в списке слева найти производителя установленной в адаптер флеш-памяти, справа в списке найти наименование памяти, нажать кнопку ОК.

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

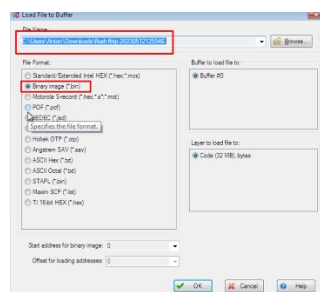
Из	Лист	№ докум.	Подп.	Дата	Лист
					15



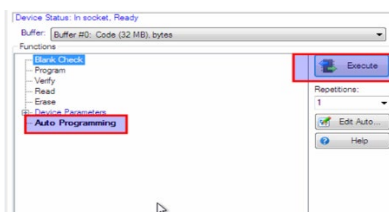
В левом верхнем углу экрана нажать кнопку File, далее выбрать Load to buffer.



В открывшемся окне в поле File format выбрать Binary image (*.bin) и нажать Browse, далее выбрать нужный файл прошивки для REALINTECHPRO, нажать открыть, затем нажать ОК.



Далее выбрать пункт Auto Programming и нажать кнопку Execute. Дождаться окончания записи образа на флеш память (должна загореться зеленая надпись READY справа сверху).



Изъять флеш-память из адаптера и установить в материнскую плату REALINTECHPRO.

Для обновления образа UEFI, хранящегося в Flash ROM предназначена утилита AFUWINx64. Обновление возможно как всего образа, так и отдельных компонентов. AFUWINx64 представляет собой утилиту, выполняемую в командной строке. Поддерживаются версии утилиты для следующих операционных систем:

- Microsoft® Windows® 10;
- Microsoft® Windows® 11;

Инв. № подл.	Подп. и дата
Взам. инв. №	Инв. № дубл.
Подп. и дата	
Инв. № подл.	

Из	Лист	№ докум.	Подп.	Дата	Лист
					16

Для обновления из под Linux используется утилита FPT

Данные утилиты осуществляют выполнение следующих операций:

- Сохранение в файле текущего образа UEFI;
- Получение ROM ID образа UEFI;
- Проверка образа UEFI;
- Отправка команд в UEFI;
- Запись блока ME в Flash ROM;
- Запись блока загрузки в Flash ROM;
- Запись блока NVRAM в Flash ROM;
- Запись блока программного обеспечения в Flash ROM;
- Запись блока дескриптора Flash ROM;
- Запись блоков программного обеспечения сетевых адаптеров в Flash ROM.

Также данные утилиты обладают дополнительными параметрами, позволяющими управлять процессом обновления программного обеспечения, расположенного на Flash ROM.

5.2.3 ЗАПУСК ПРОГРАММЫ

Вызов программного обеспечения выполняется автоматически центральным процессором материнской платы REALINTECHPRO при подаче питания. Для повторного старта программного обеспечения пользовательской программе следует выполнить переход по стартовому адресу ПО.

Инв. № подл	Подл. и дата	Взам. инв. №	Инв. № дубл.	Подл. и дата					
Из	Лист	№ докум.	Подп.	Дата					
					Лист				
					17				

6. ВХОДНЫЕ ДАННЫЕ

Входными данными для изделия являются конфигурационные параметры для работы системы ввода-вывода.

Дополнительным источником входных данных являются нажатия пользователем клавиш на клавиатуре. В случае, если в момент выполнения начального тестирования, пользователем была нажата клавиша «Delete», ПО запускает консольную программу конфигурирования настроек ПО, в которой пользователь может задать требуемые настройки.

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата						
Из	Лист	№ докум.	Подп.	Дата						
					Лист	18				

7. ВЫХОДНЫЕ ДАННЫЕ

Выходными данными изделия являются:

- служебные сообщения администратору в виде подсказок, или предупреждений в окне терминала CLI;
- данные о событиях, записываемые в соответствующие системные журналы и файлы.

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата						
Из	Лист	№ докум.	Подп.	Дата						
					Лист	19				

