



Программа начального старта (UEFI) «Иртыш»

Руководство по установке

Листов 19

СОДЕРЖАНИЕ

1 Общие сведения.....	3
1.1 Способы установки программы.....	3
1.2 Типы материнских плат.....	3
2 Установка прошивки.....	4
2.1 Подготовка к работе и техника безопасности.....	4
2.2 Проверка прошивки.....	4
3 Установка с USB-накопителя.....	5
4 Установка с помощью программатора.....	9
4.1 Общие сведения.....	9
4.2 Подключение через зажим-прищепку (SOIC-8 CLIP).....	9
4.3 Запись прошивки через графическую программу IMSProg.....	12
4.4 Верификация соединения и создание резервной копии.....	13
4.5 Загрузка целевой прошивки.....	14
4.6 Запись образа.....	14
4.7 Завершение процедуры и аварийное восстановление.....	16
4.8 Признаки неудачной прошивки. Восстановление резервной копии.....	17
5 Запись прошивки через утилиту flashrom.....	18
Лист регистрации изменений.....	19

1 Общие сведения

1.1 Способы установки программы

Установка программы начального старта (UEFI) «Иртыш» возможна тремя способами:

- 1) установка с USB-накопителя;
- 2) установка с помощью программатора;
- 3) запись прошивки через утилиту flashrom.

1.2 Типы материнских плат

Типы материнских плат с установленными процессорами представлены в таблице 1.

Таблица 1 – Типы материнских плат с установленными процессорами

Плата	Процессор	Файл прошивки
AC612A0_V1.1	Иртыш C616	IrtyshC616_v1.fd
TD622E0_V1.2	Иртыш C632	IrtyshC632_v1.fd

Примечание – Название файла прошивки формируется следующим образом:

Irtysh – название процессора;

C616 – модель процессора;

v1 – версия прошивки.

2 Установка прошивки

2.1 Подготовка к работе и техника безопасности

Перед началом любых физических подключений серверное оборудование должно быть полностью обесточено.

Должна быть произведена проверка маркировки напряжения питания 3,3 В/5 В, а также ориентация SOIC-клипа.

Важно: Недостаточно просто выключить сервер программно. Необходимо физически отключить все кабели электропитания от блока питания. Это исключает подачу дежурного напряжения на материнскую плату, которое может привести к конфликту логических уровней на шине SPI или выходу из строя программатора либо чипа.

2.2 Проверка прошивки

Для проверки прошивки выполните следующие действия:

1. Произведите верификацию источника: убедитесь, что файл получен из официального репозитория производителя или от авторизованного поставщика. Использование файлов из сомнительных источников, таких как сторонние форумы или файлообменники, запрещено из-за риска компрометации встроенного программного обеспечения UEFI.

2. Рассчитайте хеш-сумму SHA-256 или по ГОСТ Р 34.11-2012 скачанного файла и сверьте её с эталонным значением, опубликованным производителем в документации к релизу. Запрещено загружать файл в программатор при несовпадении контрольных сумм.

3. Проверка совместимости: убедитесь, что версия прошивки в формате .fd или .bin точно соответствует модели и ревизии материнской платы, для чего проверьте маркировку на плате, тип и модель установленного процессора, а также текущую ревизию чипа SPI Flash.

4. Цифровая подпись: если файл прошивки снабжен цифровой подписью производителя, выполните проверку этой подписи средствами вашей рабочей станции, например с помощью openssl или штатных утилит ODM, перед открытием в программаторе.

3 Установка с USB-накопителя

Для установки с USB-накопителя выполните следующие действия:

1. Скопируйте файл прошивки «IrttyshC632_v1.fd» («IrttyshC616_v1.fd») на USB-накопитель.
2. Вставьте USB-накопитель в сервер.
3. При загрузке нажмите «F2» для входа в меню **Setup Utility**. При этом откроется окно (рисунок 1).

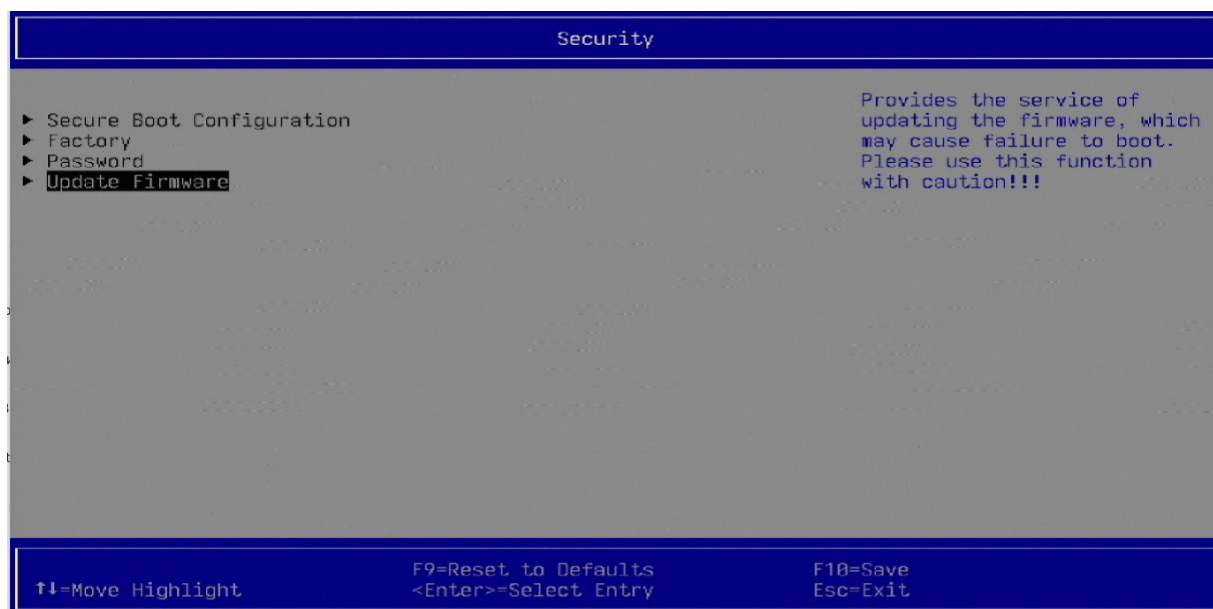


Рисунок 1 – Окно входа в Boot Manager

4. Выберите в меню **Setup Utility** раздел **Security** (рисунок 2).

Рисунок 2 – Раздел **Security**

5. В разделе **Security** выберите подраздел **Update Firmware** (рисунок 3).

Рисунок 3 – Подраздел **Update Firmware**

6. Далее выберите подключенное устройство (USB-накопитель) (рисунок 4).

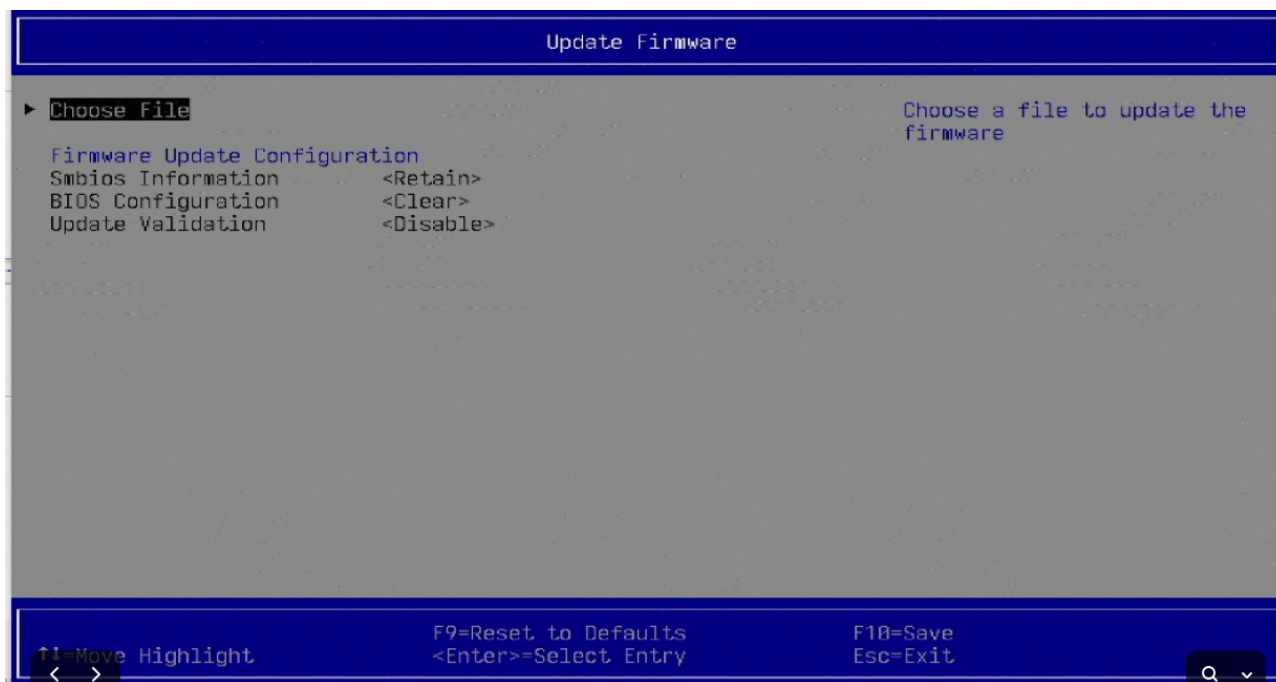


Рисунок 4 – Выбор подключенного устройства

7. Выберите файл прошивки на USB-накопителе и подтвердите запуск (рисунок 5).

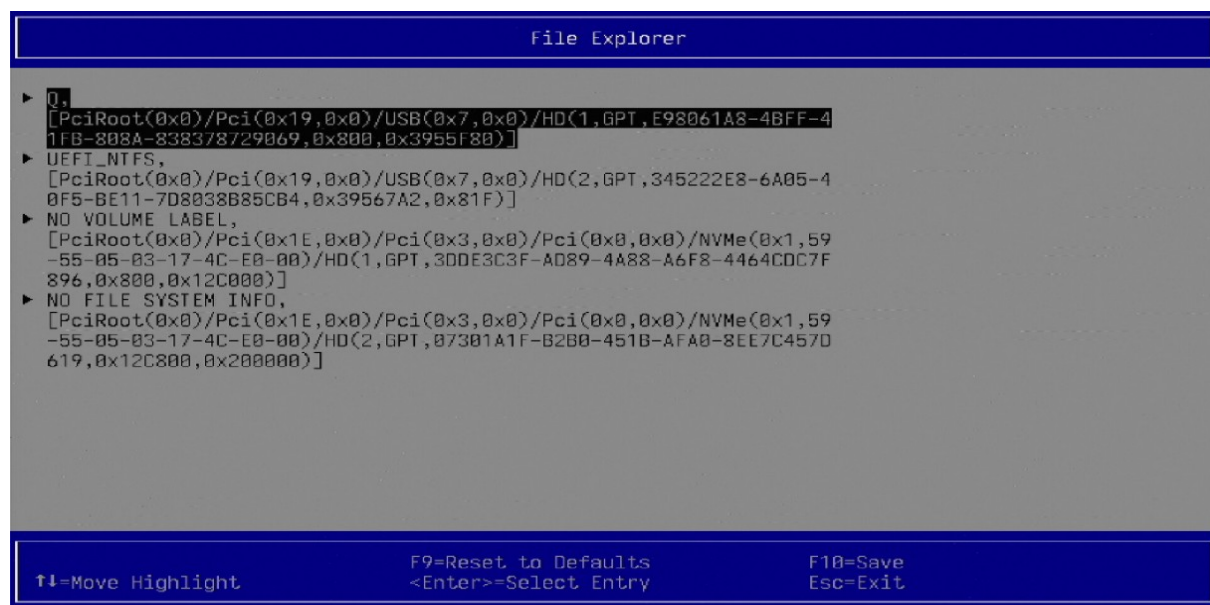


Рисунок 5 – Выбор файла прошивки

8. Дождитесь завершения процесса загрузки (100%).
9. Выберите «Yes» во всплывающем окне с вопросом о перезагрузке.
10. После завершения система автоматически перезагрузится.

4 Установка с помощью программатора

4.1 Общие сведения

4.1.1 Описана процедура обновления встроенного программного обеспечения микросхемы SPI Flash с использованием внешнего USB-программатора на базе микросхемы WCH CH341A.

4.1.2 Характеристики используемого программатора:

- базовая микросхема – WCH CH341A;
- тактовая частота – кварцевый резонатор 12 МГц;
- стабилизация напряжения – AMS1117-3.3;
- интерфейс подключения – USB (поддержка Windows, Linux, macOS);
- совместимость с ПО: CH341A Programmer, AsProgrammer, Flashrom, Colibri, NeoProgrammer, LibreSPI, SiberiaProg, IMSProg, SNANDer;
- поддерживаемые типы памяти – микросхемы EEPROM серии 24xx и SPI FLASH серии 25xx.

4.1.3 Комплект поставки

Комплект поставки включает (рисунок 6):

- 1 – USB программатор CH341A;
- 2 – зажим-прищепка (SOIC-8 Clip) с кабелем длиной 34 см;
- 3 – переходные колодки и адаптеры для различных корпусов чипов.

4.2 Подключение через зажим-прищепку (SOIC-8 CLIP)

4.2.1 Определение первого контакта на шлейфе

Осмотрите шлейф зажима. Проводник, соответствующий первому контакту, выделен цветом, обычно красным. Это ключ для правильной ориентации.

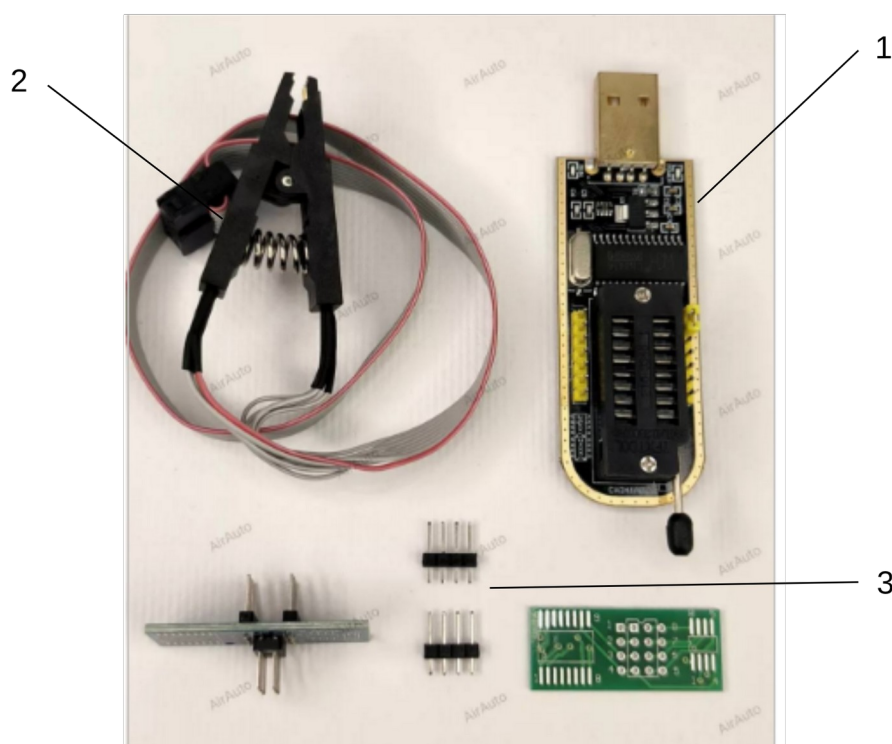


Рисунок 6 – Комплект поставки

4.2.2 Определение первого контакта на чипе

Найдите микросхему SPI Flash на материнской плате сервера. Она выполнена в корпусе стандарта SOIC-8. Ключом для определения первого вывода служит реперная точка, небольшое круглое углубление в пластике корпуса рядом с первым контактом (рисунок 7). На некоторых корпусах вместо точки может быть нанесена шелкография в виде полосы или фаски.

4.2.3 Фиксация адаптера

Совместите красный провод шлейфа «прищепки» с первым контактом микросхемы, ориентируясь на метку. Убедившись в отсутствии перекоса, зафиксируйте зажим на чипе. Контакты прищепки должны плотно прилегать к каждой из восьми ножек микросхемы.

4.2.4 Подключение к программатору

Подключите второй конец шлейфа к программатору, соблюдая соответствие контактов. Вывод с маркировкой «1» на разъеме программатора должен соединяться с красным проводом шлейфа (рисунок 8). Большинство

моделей программаторов и шлейфов используют стандартную распиновку, однако нарушение соответствия может привести к подаче питания на линии данных, что с высокой вероятностью вызовет повреждение чипа.



Рисунок 7 – Микросхема SPI Flash

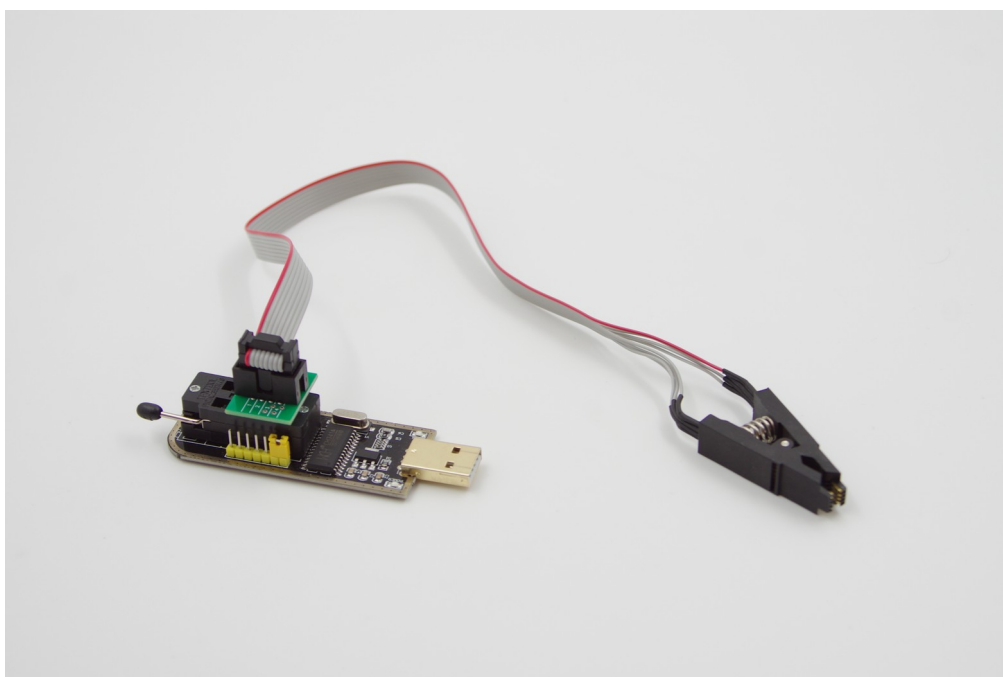


Рисунок 8 – Подключение к программатору

Примечание – Прямая пайка к контактным площадкам или использование стационарной колодки не требуется. Для подключения используется адаптер типа «прищепка» с набором подпружиненных игольчатых контактов.

4.3 Запись прошивки через графическую программу IMSProg

4.3.1 Подготовка подключения

Подключите программатор с уже зафиксированным на микросхеме адаптером к USB-порту ноутбука или персонального компьютера. Рекомендуется использовать порт USB 2.0, так как он обеспечивает наиболее стабильное напряжение питания и совместимость. Убедитесь, что операционная система корректно определила устройство. Запустите приложение IMSProg.

Примечание – Для взаимодействия с микросхемой используется свободно распространяемое ПО IMSProg (совместимое с ОС Linux).

4.3.2 Первичная настройка ПО

В интерфейсе программы выполните следующие действия:

1. Выберите тип программатора из выпадающего списка (CH341a или аналогичный, соответствующий вашей модели).

2. Выберите тип микросхемы. Для этого перейдите в ветку производителя, например Winbond, и укажите точную маркировку, указанную на корпусе чипа (например, W25Q128JV для объема 128 Мбит или W25Q256JV для 256 Мбит) (рисунок 9).

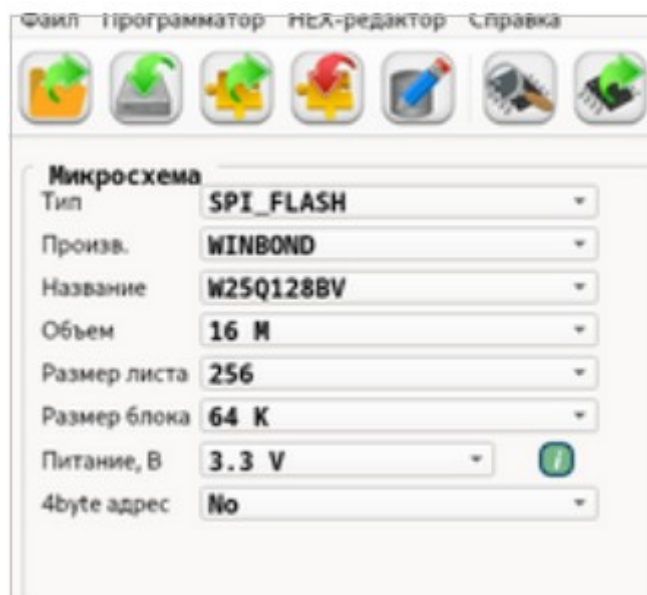


Рисунок 9 – Выбор типа микросхемы

4.4 Верификация соединения и создание резервной копии

Для верификации соединения выполните следующие действия:

1. Нажмите кнопку «Read» (Считать). При этом программа инициирует чтение всего дампа памяти микросхемы.

2. В случае отсутствия или нестабильного соединения программа выдаст ошибку, часто в виде значений FF FF FF или сообщения о несовпадении ID. В этом случае отключите USB, проверьте ориентацию зажима и при необходимости подожмите контакты. После успешного чтения данные в шестнадцатеричном представлении заполнят буфер программы (рисунок 10).

Важно: Независимо от того, является ли текущая прошивка рабочей или поврежденной, настоятельно рекомендуется **сохранить ее полный образ**. Содержимое может включать уникальные для данного экземпляра устройства данные, такие как MAC-адрес, серийный номер или настройки UEFI-переменных. Используйте меню «Файл», затем «Сохранить как», чтобы сохранить бинарный файл дампа с расширением .bin или .rom.

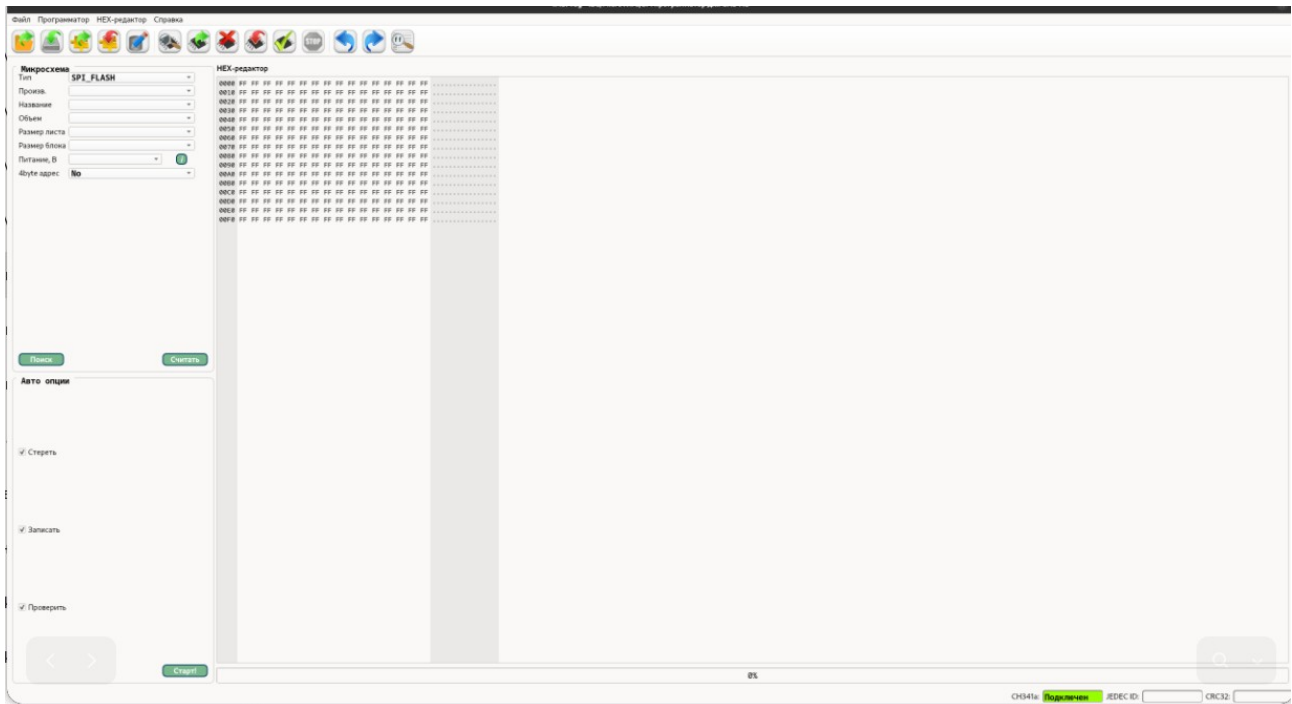


Рисунок 10 – Заполнение буфера программы

4.5 Загрузка целевой прошивки

Для загрузки целевой прошивки выполните следующие действия:

1. Загрузите целевой файл прошивки через меню «Файл», пункт «Открыть». Поддерживаются форматы .fd, .bin и .rom.
2. Проконтролируйте, чтобы размер загруженного файла точно соответствовал объему памяти микросхемы. Например, для 128-мегабитных чипов он должен составлять ровно 16 777 216 байт. В основном окне программы отобразится содержимое файла прошивки в виде HEX-таблицы (рисунок 11).

4.6 Запись образа

Запись образа может выполняться в автоматическом или ручном режиме.

В автоматическом режиме установите флажки напротив опций Erase (Стереть), Write (Записать) и Verify (Проверить), после чего нажмите кнопку

«Старт». Программа последовательно выполнит полное стирание чипа, запись страниц и побайтовую сверку.

В ручном режиме, который удобен для отладки, через выпадающее меню «Программатор» выполните операции вручную и строго последовательно.

Сначала выберите Erase для очистки всего массива памяти, при этом все ячейки примут значение 0xFF.

Затем выполните Write для записи данных из буфера программы в микросхему.

Процесс записи прошивки представлен на рисунке 12.

Запустите Verify для контрольного считывания и побайтового сравнения записанной информации с эталонным образом в буфере.

Любое расхождение, так называемый mismatch, сигнализирует о плохом контакте зажима или неисправности ячейки памяти.

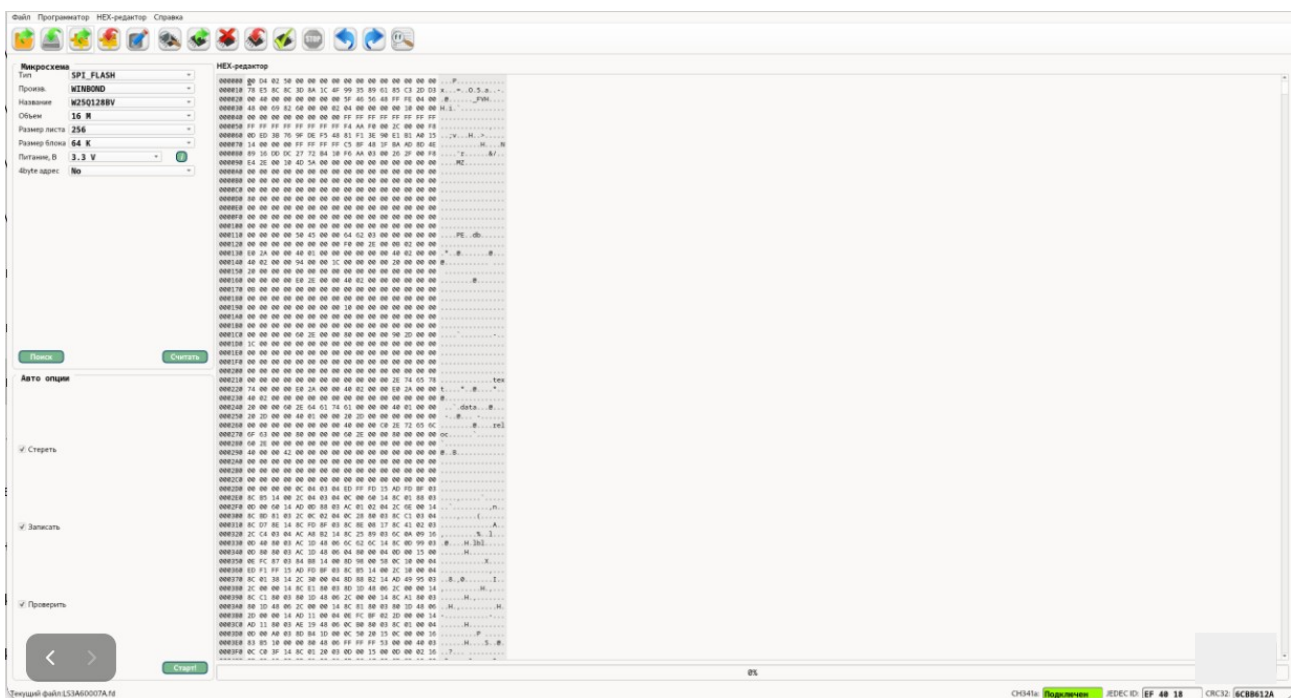


Рисунок 11 – Основное окно программы

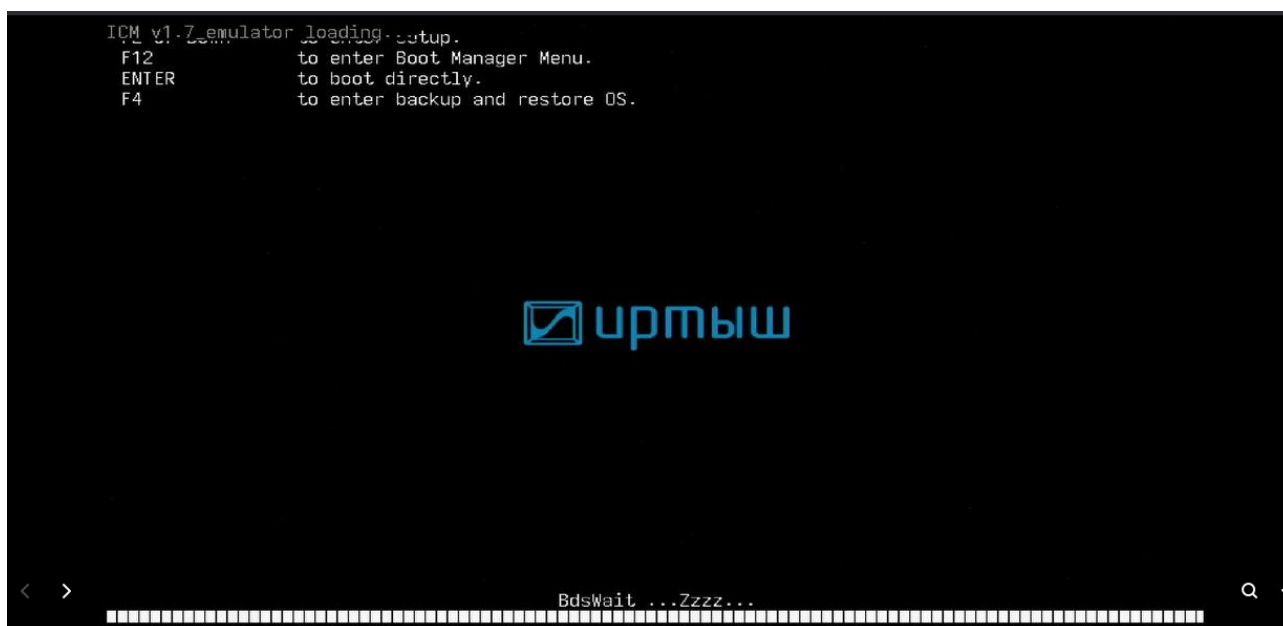


Рисунок 12 – Процесс записи прошивки

4.7 Завершение процедуры и аварийное восстановление

По завершении операции, при успешном прохождении верификации со статусом Verification successful или аналогичным сообщением, микропрограмма считается обновленной.

Для завершения процедуры выполните следующие действия:

1. Отключите программатор от USB-порта компьютера;
2. Аккуратно снимите зажим-прищепку с микросхемы.
3. Разместите микросхему в соответствующее гнездо на плате, подайте питание на сервер и выполните пробный запуск.
4. При успешной загрузке операционной системы или появлении логотипа POST процедура считается успешно завершенной.

4.8 Признаки неудачной прошивки. Восстановление резервной копии

В случае возникновения ошибок на этапе верификации, таких как статус Mismatch или ID mismatch, сбоя питания во время записи или некорректной

работы платы после установки прошивки, необходимо выполнить следующую процедуру аварийного восстановления.

Диагностика ошибки: если плата не стартует, нет изображения или не реагирует на питание, вероятно повреждена область загрузчика. Если программатор выдает ошибки при чтении или записи, проверьте физический контакт зажима или наличие короткого замыкания на дорожках платы.

Восстановление через программатор: обесточьте оборудование, физически отключив кабели питания, подключите программатор заново, строго соблюдая полярность. В интерфейсе IMSProg выберите файл ранее созданной резервной копии и выполните цикл стирания, записи и верифицирования.

Аппаратный режим восстановления: если программатор не опознает чип и все значения равны FF, проверьте наличие на материнской плате перемычек-джамперов или специальных контактов для режима Force Recovery, замыкание которых переводит SPI-флеш в режим программирования в обход процессора. Информация о таких перемычках указывается в техническом описании платы в документации OEM.

Критерии обращения в сервисный центр: если после трех попыток перезаписи с использованием резервной копии программатор по-прежнему выдает ошибки или чип не определяется с идентификатором FF FF FF, а также при физическом повреждении корпуса чипа или контактных площадок, запрещается продолжать самостоятельные попытки прошивки. Оборудование подлежит передаче в авторизованный сервисный центр для замены микросхемы SPI Flash.

5 Запись прошивки через утилиту flashrom

Для записи прошивки через утилиту flashrom (например, с использованием программатора CH341) выполните следующие действия:

1. Подключите программатор к USB-порту ноутбука или ПК с Linux.
2. Убедитесь, что программатор обнаружен:

```
lsusb | grep CH341
```

3. Выполните бэкап текущей прошивки:

```
sudo flashrom -p ch341a_spi -r backup_original.fd
```

4. Запишите новую прошивку:

```
sudo flashrom -p ch341a_spi -w IrtyshC632_v1.fd
```

5. Проверьте запись:

```
sudo flashrom -p ch341a_spi -v IrtyshC632_v1.fd
```

6. Запись прошивки завершена успешно.

Лист регистрации изменений

[illegible]