Тринити

РОССИЙСКИЙ ПРИЗВОДИТЕЛЬ ОБОРУДОВАНИЯ
ДЛЯ ПОСТРОЕНИЯ ИТ-ИНФРАСТРУКТУРЫ

ВСТРОЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ BIOS RU.ТВЛФ.00001-01

Описание функциональных характеристик программного обеспечения

на 17 листа

г. Москва
2025

Содержание

1. Перечень сокращений и обозначений

ОС	Операционная система
ПЗУ	Постоянное запоминающее устройство
ПК	Персональный компьютер
ПО	Программное обеспечение
СТП	Служба технической поддержки
ЭВМ	Электронно-вычислительная машина
API (Application Programming Interface)	Описание способов взаимодействия программного обеспечения с аппаратными и программными компонентами системы
BIOS (Basic Input/Output System)	Базовая система ввода-вывода
UEFI (Unified Extensible Firmware Interface)	Интерфейс между операционной системой и микропрограммами, управляющими оборудованием
Программатор	Аппаратно-программное устройство для чтения и записи информации в ПЗУ, флэш-память или внутреннюю память микроконтроллеров (МК)

2. Общие сведения

Документ содержит описание функциональных характеристик встроенного программного обеспечения BIOS RU.ТВЛФ.00001-01 (далее – ВПО).

ВПО предназначено для обеспечения взаимодействия между аппаратными и программными компонентами платы материнской Тринити ТВЛФ.469555.001 (далее – материнская плата) в составе серверов Тринити, построенных на базе процессоров Intel Xeon 3-го поколения. ВПО разработано для облегчения процесса начального запуска вычислительной техники и предназначена для инициализации и запуска основных устройств вычислительной техники и ее компонентов. ВПО обеспечивает передачу управления операционной системе в соответствии с предварительно заданными настройками.

ВПО использует технические средства платы материнской Тринити ТВЛФ.469555.001 производства АО «ТРИНИТИ СОЛЮШНС».

3. Назначение программного обеспечения

ВПО – программа начального запуска, является системной программой низкого уровня, хранящейся в микросхеме ПЗУ на материнской плате, и предоставляет пользователю возможность полного управления системой при загрузке.

ВПО состоит из ряда драйверов, приложений и экранных форм, с помощью которых можно настроить параметры работы системы в соответствии с требованиями пользователя или использовать параметры, заданные по умолчанию.

ВПО предоставляет расширенные функциональные возможности UEFI, унифицированного расширяемого интерфейса микропрограмм для ПО низкого уровня, которое запускается автоматически при старте сервера перед тем, как загрузится операционная система.

Функции ВПО:

- начальная инициализация серверной платформы;
- проверка работоспособности аппаратных компонентов;
- загрузка операционной системы.

ВПО разработано в соответствии со спецификацией UEFI для решения проблемы переносимости встроенного программного обеспечения и расширяемости на будущие платформы, расширения использования различных драйверов, средств разработки, утилит поддержки и загрузочных приложений.

Особенности ВПО:

- поддержка UEFI 2.8, PI 1.7;
- интеграция с Intel Boot Guard;
- Secure Flash для безопасного обновления;
- модульная архитектура.

4. Аппаратные и программные требования

Для корректной работы ВПО установлены следующие минимальные и рекомендуемые требования:

1) Аппаратные требования:

- Процессор:
  - минимальные: Intel Xeon 3-го поколения (Ice Lake);
  - рекомендуемые: процессоры последнего выпуска в семействе Xeon Ice Lake с расширенными возможностями для оптимальной производительности.
- Материнская плата:
  - ВПО предназначено для использования в материнской плате Тринити ТВЛФ.469555.001 производства АО «ТРИНИТИ СОЛЮШНС».
- Оперативная память и прочие компоненты:
  - минимальные: 16 Гб оперативной памяти;
  - рекомендуемые: 32 Гб и более.

2) Программные требования:

- Совместимость с операционными системами:
  - минимальные: поддержка основных операционных систем, оптимизированных для работы с UEFI, включая определённые версии Windows, Linux и другие ОС, соответствующие требованиям платформы;
  - рекомендуемые: последние версии операционных систем с актуальными обновлениями безопасности и драйверов, обеспечивающие стабильную работу и взаимодействие с BIOS.
- Дополнительное программное обеспечение:
  - для полного функционала системы может потребоваться установка специализированных драйверов и утилит;
  - рекомендуется регулярное обновление этих компонентов согласно рекомендациям производителя для обеспечения максимальной совместимости и безопасности.
- Для реализации удаленного доступа к ВПО необходимо следующее ПО сторонних разработчиков:

браузер для доступа через Web-интерфейс;

программа для доступа посредством командной строки по протоколу IPMI.

Для удаленного доступа к ВПО через IPMI/BMC необходимо обеспечить сетевой доступ к сервисному процессору материнской платы.

5. Цели и автоматизируемые функции

5.1. Цели ВПО

Основные цели применения ВПО:

1) Обеспечение начального старта системы

ВПО является системной программой низкого уровня, предназначенной для запуска компьютерной системы при ее включении. Его целью является корректная инициализация аппаратного обеспечения и подготовка системы к загрузке операционной системы.

2) Полное управление системой при загрузке

Пользователю предоставляется возможность управлять настройками системы во время ее загрузки. Это позволяет пользователям изменять параметры работы системы в соответствии с их требованиями или использовать предустановленные значения.

3) Расширение функциональных возможностей UEFI

ВПО предоставляет расширенные функциональные возможности UEFI, обеспечивая более гибкую и удобную настройку и управление системой при старте. Это включает в себя поддержку жестких дисков большего объема, улучшенную скорость загрузки, графический интерфейс с поддержкой мыши, а также возможность удаленной настройки и отладки.

5.2. Автоматизируемые функции ВПО

ВПО обеспечивает следующую автоматизацию:

1) Инициализация аппаратного обеспечения при запуске системы

При включении питания система запускается с выполнения процедуры самодиагностики (POST), в ходе которой проверяется работоспособность основных компонентов, таких как процессор, оперативная память, устройства хранения данных и другие периферийные устройства. Это позволяет гарантировать корректное и безопасное начало работы системы.

2) Обеспечение интерфейса между операционной системой и аппаратными компонентами

BIOS служит промежуточным звеном, создающим стандартизированный программный интерфейс (API) для взаимодействия операционной системы с аппаратными средствами. Данный интерфейс обеспечивает стабильное и эффективное управление ресурсами системы, способствуя повышению её производительности и надёжности.

3) Поддержка специфических функций, реализованных компанией АО «ТРИНИТИ СОЛЮШНС»

Помимо стандартного функционала AMI BIOS, система включает дополнительные возможности, адаптированные под уникальные требования предприятия. К таким функциям относятся расширенные механизмы безопасности, оптимизированные процедуры обновления, а также возможности тонкой настройки параметров системы для удовлетворения специфических задач и повышения общей эффективности работы.

4) Поддержка драйверов и средств разработки

ВПО обеспечивает поддержку различных драйверов и средств разработки, что позволяет расширять функциональность системы и использовать различное аппаратное обеспечение.

5) Загрузка операционной системы

После завершения инициализации аппаратного обеспечения и настройки параметров ВПО загружает операционную систему с жесткого диска или другого носителя данных.

6) Обеспечение безопасной загрузки

ВПО может обеспечивать безопасную загрузку системы, проверяя подлинность и целостность загрузочных компонентов для предотвращения атак и вредоносных вмешательств.

6. Функциональная структура ВПО

ВПО представляет собой систему инициализации, запуска и управления вычислительной техникой и ее компонентами. ВПО состоит из двух основных уровней.

Первый уровень обеспечивает безопасность и инициализацию оборудования. Он отвечает за инициализацию аппаратных компонентов системы (работа тактовых генераторов, уровни напряжения и температуры). На этом уровне происходит определение возможности работы системы и активация следующего уровня – Boot Block. На первом этапе материнская плата не работает полноценно.

Второй уровень предоставляет сервисные возможности по диагностике и, при необходимости, устранению неполадок. Здесь осуществляется окончательная инициализация системы и вывод результатов самодиагностики через звуковые сигналы, сообщения на экране или определенные коды.

ВПО выполняет действия по:

- инициализации и запуску вычислительной техники и ее компонентов;
- передаче управления операционной системе в соответствии с заданными настройками.

ВПО поддерживает язык высокого уровня C и язык низкого уровня Asm. Функционирует без операционной системы.

ВПО представляет собой системную программу низкого уровня, обеспечивающую начальный запуск оборудования сервера. Оно хранится в ПЗУ на материнской плате и обеспечивает пользователю полный контроль над системой в процессе ее загрузки.

Основные компоненты ВПО включают в себя:

- драйверы – обеспечивают взаимодействие с аппаратным обеспечением сервера, таким как процессор, память, ввод-вывод и другие устройства;
- приложения – предоставляют пользователю возможность настройки параметров работы системы в соответствии с требованиями или использования параметров по умолчанию;
- экранные формы – предоставляют графический интерфейс для управления системой и настройки её параметров.

ВПО использует расширенные функциональные возможности UEFI, которые обеспечивают:

- поддержку жестких дисков большего объема – UEFI поддерживает работу с жесткими дисками большего объема, что увеличивает гибкость системы;
- быструю загрузку – UEFI работает на более низком уровне, чем традиционный BIOS, поэтому загрузка системы происходит быстрее;
- высокий уровень безопасности – UEFI предоставляет дополнительные механизмы безопасности, такие, как проверка цифровых подписей, что делает процесс загрузки более безопасным;
- графический интерфейс и поддержку мыши – UEFI обеспечивает более удобный и интуитивно понятный интерфейс для пользователей, включая поддержку мыши;

- возможность удаленной настройки и отладки – позволяет проводить настройку и отладку системы удаленно, что особенно важно для серверных и удаленных систем;

- различные способы хранения – UEFI может храниться во флэш-памяти на материнской плате, на жестком диске или на общем сетевом ресурсе.

ВПО разработана с учетом спецификации UEFI, что обеспечивает переносимость встроенного программного обеспечения и расширяемость на будущие платформы. Это позволяет легко добавлять новые драйверы, средства разработки, утилиты поддержки и загрузочные приложения.

7. Функциональные задачи

ВПО выполняет следующие функциональные задачи:

- инициализация аппаратного обеспечения;
- обеспечение взаимодействия между ОС и аппаратными компонентами;
- управление параметрами системы;
- поддержка специфических функций;
- поддержка драйверов и средств разработки;
- загрузка ОС;
- обеспечение безопасной загрузки.

7.1. Инициализация аппаратного обеспечения

При включении питания система запускается с выполнения процедуры самодиагностики (POST), в ходе которой проверяется работоспособность основных компонентов, таких как процессор, оперативная память, устройства хранения данных и другие периферийные устройства. Это позволяет гарантировать корректное и безопасное начало работы системы.

7.2. Обеспечение взаимодействия между ОС и аппаратными компонентами

BIOS служит промежуточным звеном, создающим стандартизированный программный интерфейс (API) для взаимодействия операционной системы с аппаратными средствами. Данный интерфейс обеспечивает стабильное и эффективное управление ресурсами системы, способствуя повышению её производительности и надёжности.

7.3. Управление параметрами системы

ВПО предоставляет широкий набор настроек, позволяющих детально конфигурировать аппаратные компоненты системы. Пользователи могут изменять параметры загрузки энергосбережения, управлять режимами работы процессора и оперативной памяти, а также настраивать параметры периферийных устройств в соответствии с конкретными требованиями эксплуатации.

7.4. Поддержка специфических функций

ВПО адаптировано для работы с аппаратными особенностями платформы на базе процессоров Intel Xeon 3-го поколения (Ice Lake). Реализована поддержка специализированных функций, таких как оптимизация энергопотребления, интеграция с системами управления температурой и мониторинг состояния критичных компонентов, что позволяет обеспечить высокую производительность и надежность работы системы.

7.5. Поддержка драйверов и средств разработки

Автоматическое обнаружение и подключение необходимых драйверов для обеспечения совместимости с различным аппаратным обеспечением. Поддержка

средств разработки для расширения функциональности и адаптации системы к конкретным требованиям пользователя.

7.6. Загрузка ОС

Управление процессом загрузки операционной системы с жесткого диска, флэш-памяти или других носителей данных, обеспечивая стабильность и надежность загрузки.

7.7. Обеспечение безопасной загрузки

Для обеспечения защиты системы от несанкционированного доступа и возможных угроз внедрены современные механизмы безопасности. ВПО включает функции аутентификации, проверки целостности загрузочных компонентов и шифрования, что способствует предотвращению атак и повышению устойчивости системы к внешним воздействиям.

8. Функционал системы

ВПО обеспечивает широкий спектр возможностей, направленных на оптимизацию загрузки, настройки и управления аппаратными ресурсами системы. Подробное описание функциональных возможностей представлено ниже:

1) Процесс загрузки системы

При включении питания система инициирует последовательность загрузки, начиная с выполнения процедуры самодиагностики (POST). Этот этап включает проверку основных компонентов, таких как процессор, оперативная память, устройства хранения данных и периферийные устройства. После успешного прохождения POST, BIOS осуществляет выбор и запуск загрузочного устройства, передавая управление загрузчику операционной системы. Данный механизм обеспечивает стабильное и безопасное начало работы системы.

2) Настройки и параметры, доступные пользователю

ВПО предоставляет интуитивно понятный интерфейс для настройки различных параметров системы. Пользователи имеют возможность конфигурировать:

- приоритет загрузки и выбор загрузочного устройства;
- параметры работы процессора, оперативной памяти и графических адаптеров;
- конфигурацию периферийных интерфейсов, таких как USB, SATA, PCI Express;
- настройки безопасности, включая механизмы аутентификации и контроля доступа.

Такой набор настроек позволяет адаптировать работу системы под конкретные эксплуатационные задачи и требования к производительности.

3) Поддержка периферийных устройств и интерфейсов

Программное обеспечение обеспечивает совместимость с широким спектром периферийных устройств и интерфейсов. Это включает поддержку:

- стандартных интерфейсов подключения для внешних устройств (USB, SATA, PCI Express);
- специфических аппаратных функций платформы на базе Intel Xeon Ice Lake;
- дополнительных периферийных модулей, необходимых для специализированных задач предприятия.

Благодаря этому реализована полноценная интеграция аппаратных средств, что способствует повышению стабильности и производительности системы.

4) Механизмы обновления ВПО

Для поддержания актуальности и безопасности системы предусмотрено несколько методов обновления микропрограммы BIOS:

- через web-интерфейс BMC – обновление может проводиться дистанционно посредством web-интерфейса базового контроллера управления (BMC), что позволяет централизованно управлять обновлениями в серверных и корпоративных средах.
- через программатор – использование специализированного программатора позволяет выполнить прямое программирование BIOS-чипа. Данный метод полезен для

восстановления системы после возникновения сбоев или повреждений микропрограммы.

9. Режим функционирования ВПО

9.1. Подготовка к работе

9.1.1. Установка и настройка ВПО

1) Установка

Встроенное программное обеспечение BIOS RU.ТВЛФ.00001-01 записывается в энергонезависимую память материнской платы на этапе производства. Запись выполняется с использованием специального оборудования – программаторов SPI Flash.

На момент поставки серверной платформы ВПО уже установлено, а его базовые настройки соответствуют требованиям производителя. Пользователь не нуждается в дополнительной установке.

2) Первичный вход в настройки

При включении системы необходимо войти в меню настроек BIOS (обычно с помощью клавиши DEL, F2 или иной, указанной в руководстве).

3) Конфигурация параметров

При необходимости настроить основные параметры, включая порядок загрузки, режимы работы процессора и оперативной памяти, а также конфигурацию периферийных интерфейсов. Также следует убедиться, что выбран правильный режим работы UEFI.

4) Сохранение изменений

После завершения настройки необходимо сохранить все внесённые изменения и перезагрузить систему для применения новой конфигурации.

9.1.2. Проверка совместимости аппаратного обеспечения

1) Аппаратные компоненты

Проверить соответствие всех компонентов системы минимальным требованиям (процессор Intel Xeon 3-го поколения (Ice Lake), совместимая материнская плата, оперативная память и др.).

2) Тестирование через POST

Выполнить встроенную процедуру самодиагностики (POST) для выявления аппаратных сбоев и проверки корректности работы всех узлов.

3) Обновления

При наличии, установить актуальные версии прошивок и драйверов для компонентов системы.

9.1.3. Настройка параметров безопасности

1) Аутентификация и контроль доступа

Настроить механизмы аутентификации для предотвращения несанкционированного доступа к настройкам ВПО.

2) Проверка целостности

Включить функции проверки целостности загрузочных компонентов и настройте шифрование, если это предусмотрено конфигурацией ВПО.

3) Резервное копирование конфигураций

Рекомендуется создать резервную копию текущих настроек ВПО для быстрого восстановления в случае возникновения проблем.

9.2. Штатное функционирование

После подачи питания на сервер ВПО загружается автоматически и выполняет инициализацию системы.

Для обеспечения бесперебойной работы системы и своевременного устранения неполадок предлагаются следующие рекомендации:

1) Для консультаций по настройке, обновлению или устранению проблем с ВПП обращаться в техническую поддержку АО «ТРИНИТИ СОЛЮШНС»;

2) Рекомендуемые процедуры обновления ВПО:

- через web-интерфейс BMC – обновление может проводиться дистанционно посредством web-интерфейса базового контроллера управления (BMC), что позволяет централизованно управлять обновлениями в серверных и корпоративных средах.
- через программатор – использование специализированного программатора позволяет выполнить прямое программирование BIOS-чипа. Данный метод полезен для восстановления системы после возникновения сбоев или повреждений микропрограммы.

3) Рекомендации по устранению распространенных проблем

- проблемы с загрузкой системы – проверить правильность настроек загрузочного устройства и последовательность загрузки, а также убедиться в корректности установки всех аппаратных компонентов.
- диагностика аппаратных сбоев – использовать встроенную процедуру POST для выявления и устранения аппаратных неисправностей. При необходимости заменить неисправные компоненты.
- ошибки обновления ВПО – при возникновении проблем с обновлением микропрограммы восстановить предыдущую рабочую версию из резервной копии или обратиться в службу технической поддержки для получения подробных инструкций.

9.3. Численность, функции и квалификация персонала, работающего с ВПО

Количество пользователей программного обеспечения определяется текущими потребностями заказчика программного обеспечения.

Пользователи должны иметь базовые навыки работы с ОС Linux и Windows, навыки пользователя сети Интернет, а также изучить эксплуатационную документацию на ВПО.

Перечень задач, выполняемых пользователями:

- поддержание работоспособности ВПО и ОС;
- резервное копирование системы;
- конфигурирование пользователей и их учетных записей;
- конфигурирование политики безопасности;

- конфигурирование действий при восстановлении питания;
- обновление ВПО.