ВСТРОЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «БАЗОВАЯ СИСТЕМА ВВОДА-ВЫВОДА «СТАРТ-621AS» ДЛЯ ПЛАТЫ AQC621AS

ДОКУМЕНТАЦИЯ, СОДЕРЖАЩАЯ ИНФОРМАЦИЮ, НЕОБХОДИМУЮ ДЛЯ ЭКСПЛУАТАЦИИ ЭКЗЕМПЛЯРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРЕДОСТАВЛЕННОГО ДЛЯ ПРОВЕДЕНИЯ ЭКСПЕРТНОЙ ПРОВЕРКИ

на 26 листах

2024 год

СОДЕРЖАНИЕ

1 Список сокращений и обозначений

ПО	Программное обеспечение.
ПЗУ	Постоянное запоминающее устройство.
СВТ	Средства вычислительной техники на базе системной платы AQC621AS.
UEFI (Unified Extensible Firmware Interface)	Спецификация, определяющая программный интерфейс между ОС и прошивкой платформы.
Коды состояния (Status Codes)	Значения данных, используемые для предоставления диагностической информации о процессе загрузки.
Прогресс-коды (Progress Codes)	Коды состояний, которые указывают на успешный переход к следующему этапу инициализации.
Коды контрольных точек	Значения данных размером 1 байт.
Звуковой код	Серия коротких звуковых сигналов.
POST	Power-On Self-Test – тест подачи электропитания.
BIOS	Basic Input/Output System, базовая система ввода-вывода.
Фаза BDS (Boot Device Selection)	Настройка системы, пользовательского интерфейса перед загрузкой операционной системы и выбором источника загрузки.
Фаза DXE (Driver Execution Environment)	Инициализация основного оборудования.
Фаза PEI (Pre-EFI Initialization)	Предварительная инициализация памяти.
Фаза SEC (Security)	Безопасность, начальная инициализация низкого уровня.
Инициализация AP (Application Processor)	Процесс загрузки и настройки микрокода на процессоре, который отвечает за выполнение программ и обработку данных.
TFTP	Простой протокол передачи файлов, который используется для первоначальной загрузки бездисковых рабочих станций.

2 Общие сведения

Документ содержит информацию, необходимую для эксплуатации экземпляра программного обеспечения «Базовая система ввода-вывода «Старт621AS» (далее – ПО «Старт621AS»). ПО «Старт621AS» предназначено для удаленного мониторинга и управления компьютерными системами. ПО «Старт621AS» разработана для облегчения процесса начального запуска вычислительной техники и предназначена для инициализации и запуска основных устройств вычислительной техники и ее компонентов. ПО «Старт621AS» обеспечивает передачу управления операционной системе в соответствии с предварительно заданными настройками.

ПО «Старт621AS» использует технические средства, основанные на серверах разработки от ООО «ПК Аквариус», выполненные на базе системной платы AQC621AS.

3 Назначение программы

ПО «Старт-621AS» является полноценной собственной разработкой производственной компании ООО «Производственная компания «Аквариус». Разработка является системной программой низкого уровня, хранящейся в постоянном запоминающем устройстве (ПЗУ) на системной плате, и предоставляет пользователю возможность полного управления системой при загрузке. ПО «Старт-621AS» 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.

ПО «Старт-621AS» предоставляет расширенные функциональные возможности UEFI (Unified Extensible Firmware Interface), унифицированного расширяемого интерфейса микропрограмм для программного обеспечения низкого уровня, которое запускается автоматически при старте компьютера перед загрузкой операционной системы.

Основа платформы ПО «Старт-621AS» разработана в соответствии со спецификацией UEFI для решения проблемы переносимости встроенного программного обеспечения и расширяемости на будущие платформы, расширения используемых драйверов, средств разработки, утилит поддержки и предзагрузочных приложений.

В процессе эксплуатации ПО конечный пользователь использует его, как готовое, автономно работающее и не требующее вмешательства ПО. Взаимодействие с ПО доступно оператору. Возможности взаимодействия и сервисного доступа к ПО описаны в Руководстве оператора, приведенном в Приложении 1 данного документа.

4 Состав модулей и автоматизируемых функций

ПО «Старт621AS» представляет собой систему инициализации, запуска и управления вычислительной техникой и ее компонентами. Функциональная структура ПО «Старт621AS» представлена на рисунке 1. ПО «Старт621AS» состоит из двух основных компонентов, организованных на двух уровнях подпрограмм.

Первый уровень обеспечивает инициализацию системы в процессе проверки основных параметров, таких как работа тактовых генераторов, уровни напряжения и температуры. На этом уровне происходит определение возможности работы системы и активация следующего уровня - Boot Block. На первом этапе системная плата не проявляет "признаков жизни".

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

ПО «Старт621AS» осуществляет:

- Инициализацию и запуск вычислительной техники и ее компонентов.
- Передачу управления операционной системе в соответствии с заданными настройками.
- Имеет поддержку языка высокого уровня C и языка низкого уровня Asm.
- Функционирует без операционной системы.

ПО «Старт621AS» представляет собой системную программу низкого уровня, хранящуюся в постоянном запоминающем устройстве (ПЗУ) и обеспечивает полное управление системой при загрузке. Включает в себя драйверы, приложения и экранные формы для настройки параметров работы системы.

Основной особенностью ПО «Старт621AS» является использование расширенных функциональных возможностей UEFI, что позволяет обеспечить более эффективную и унифицированную работу системы. UEFI обладает рядом преимуществ, включая поддержку больших жестких дисков, быструю загрузку, безопасность, интерфейс и поддержку мыши, а также возможность удаленной настройки и отладки.

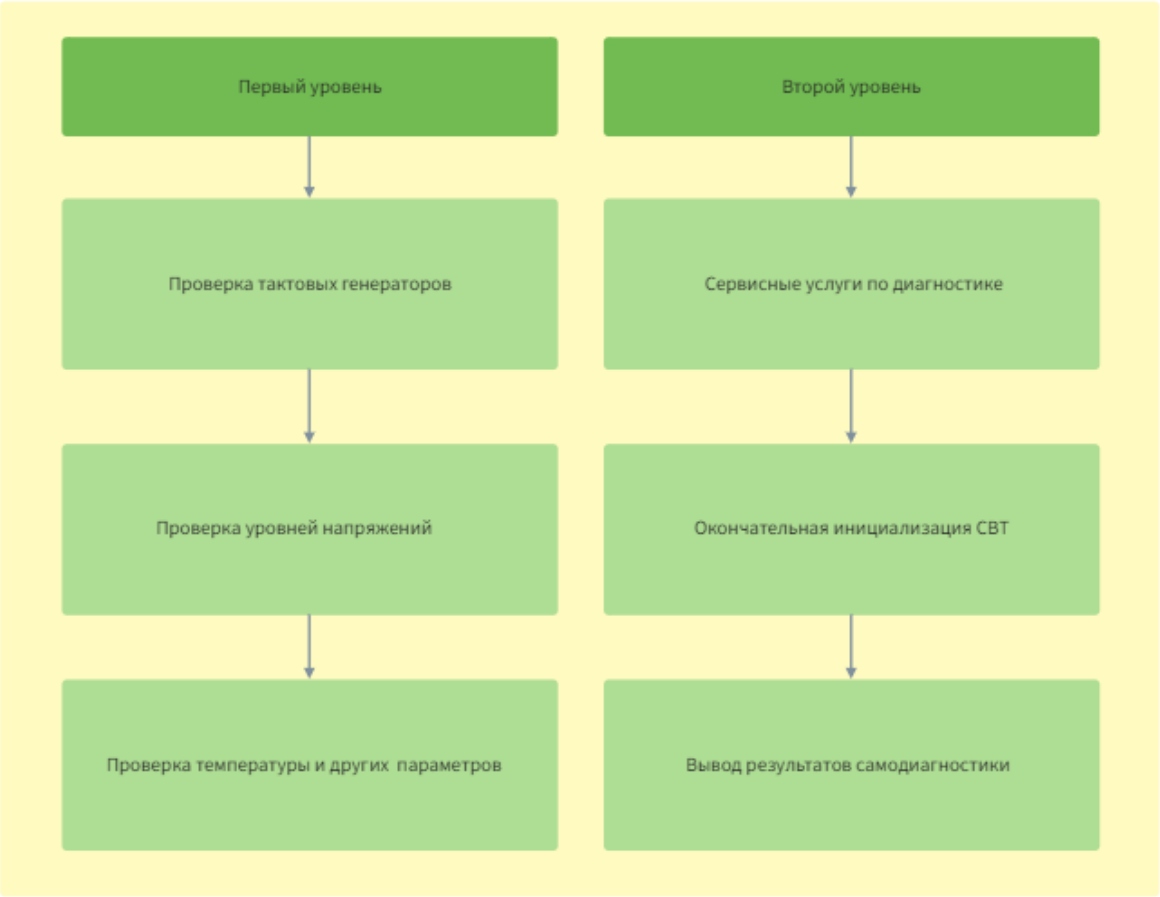

Рисунок 1 – Функциональная структура ПО «Старт621AS»

5 Подготовка к работе

Компиляция исходного кода ПО «Старт621AS» производится на серверах.

5.1 Техническое обеспечение Системы

ПО «Старт-621AS» устанавливается на серверы производства ООО «ПК Аквариус», выполненные на базе системной платы AQC621AS.

Для функционирования программы дополнительного программного обеспечения не требуется.

6 Описание работы

6.1 Установка и настройка ПО «Старт621AS»

6.1.1 «Главная» вкладка меню («Main»)

После входа загружается «Главная» вкладка меню на рисунке 2, на которой представлена информация о версии ПО «Старт-621AS», платформе, общей памяти, также представлены возможности выбора языка системы, определения системной даты и времени.

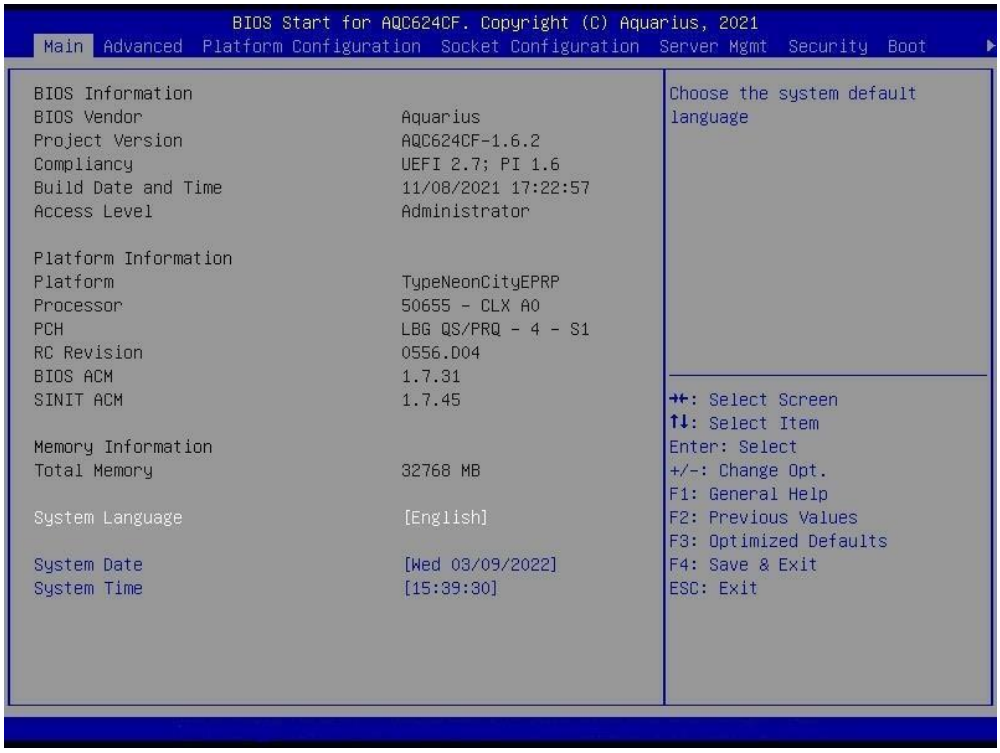

Рисунок 2 – «Главная» вкладка меню («Main»)

6.1.2 Запуск ПО «Старт-621AS»

Для входа в программу необходимо выполните следующие ниже действия:

- обеспечить питание системной платы;
- нажать клавишу <Delete> при появлении строки:
  - «Press DEL or F2 to enter Setup»;
  - «нажмите DEL или F2 для входа в Setup».

После нажатия клавиши <Delete> на экране появится главное меню (Main Menu) ПО «Старт-621AS», из которого возможно попасть в другие меню, например, меню набора микросхем (Chipset Menu), меню питания (Power Menu) и т.п.

6.1.3 Навигация в ПО «Старт-621AS»

Для навигации в меню необходимо использовать клавиши управления согласно таблице 1.

Таблица 1 Клавиши управления

Клавиша	Действие
← →	Перемещает курсор влево или вправо для выбора экрана.
↑ ↓	Перемещает курсор вверх или вниз по списку для выбора пункта раздела меню.
Enter	Позволяет открыть подменю или выбрать команду.
+/-	Смена опции.
F1	Общая помощь.
F7	Предыдущее значение.
F9	Оптимальные настройки по умолчанию.
F10	Сохранение и выход.
Esc	Выход из текущего раздела.

В качестве подсказки и для облегчения навигации краткое описание функций, настраиваемых при выборе раздела или пункта меню, будет отображаться на правом верхнем поле выбранной вкладки.

6.1.4 Вкладка «Расширенное меню» («Advanced»)

Для настройки в соответствии с предпочтениями пользователя дополнительных опций конфигурации сервера, дистанционного управления консолью, а также для конфигурации портов USB, сетевой конфигурации, аутентификации, конфигурации оперативной памяти служит вкладка «Расширенное меню» («Advanced») на рисунке 3 – следующая вкладка меню ПО «Старт-621AS».

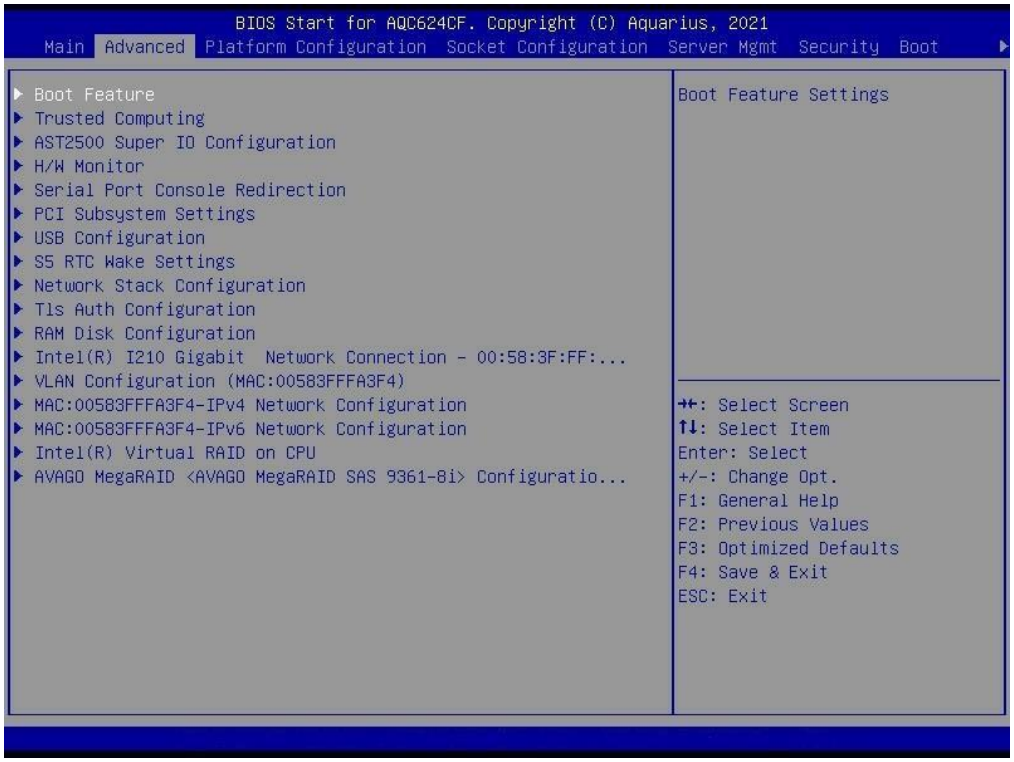

Рисунок 3 – Вкладка «Расширенное меню» («Advanced»)

6.1.5 Вкладка «Конфигурация платформы» («Platform Configuration»)

Вкладка отвечает за настройку дополнительных конфигураций платформы.

Установка некорректных значений параметров этой вкладки вызывает сбой всей системы.

Внешний вид вкладки «Конфигурация платформы» представлен на рисунке 4.

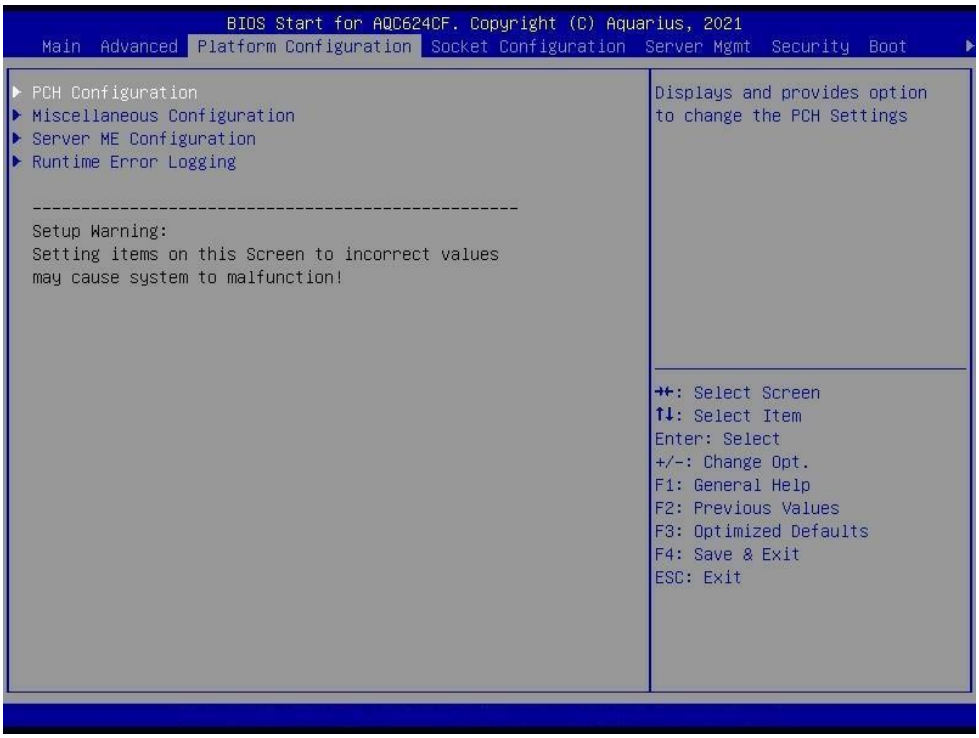

Рисунок 4 – Вкладка «Конфигурация платформы» («Platform Configuration»)

6.1.6 Вкладка «Конфигурация сокета» («Socket Configuration»)

Для настройки и конфигурации центрального процессора сервера и его окружения служит вкладка «Конфигурация сокета» («Socket Configuration»).

Установка некорректных значений параметров в этой вкладке вызывает сбой всей системы.

Внешний вид вкладки «Конфигурация сокета» представлен на рисунке 5.

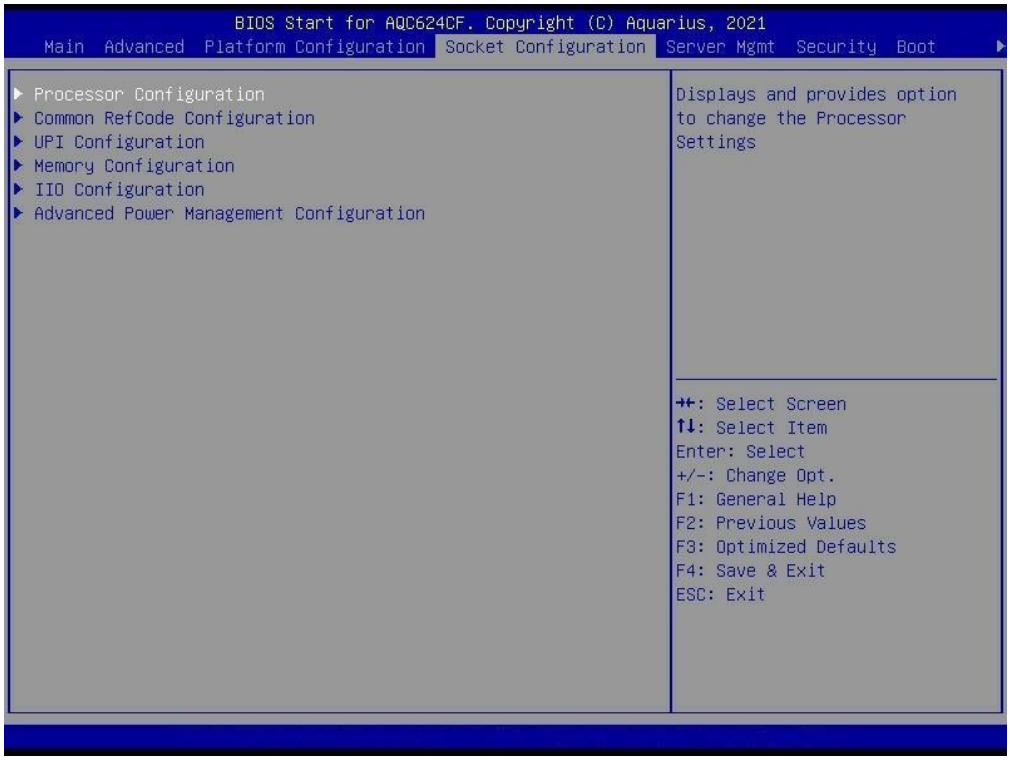

Рисунок 5 – Вкладка «Конфигурация сокета» («Socket Configuration»)

6.1.7 Вкладка «Управление серверами» («Server Mgmt»)

Вкладка «Управление серверами» служит для мониторинга и обслуживания серверов в сети с целью обеспечения максимальной производительности. Помимо этого, вкладка включает управление оборудованием, программным обеспечением, безопасностью и резервным копированием, а также настройки и обновления.

Внешний вид вкладки «Управление серверами» представлен на рисунке 6.

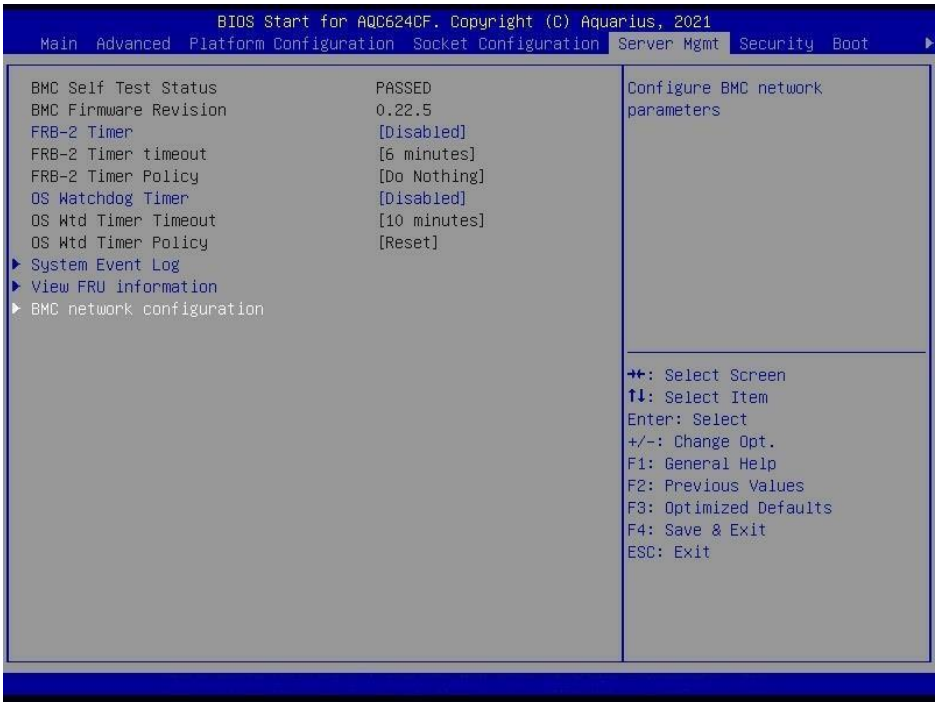

Рисунок 6 – Вкладка «Управление серверами» («Server Mgmt»)

6.1.8 Вкладка «Журнал событий» («Event Logs»)

Вкладка необходима для настройки и просмотра журнала событий. Установка некорректных значений параметров в этой вкладке вызывает сбой всей системы.

Внешний вид вкладки «Управление серверами» представлен на рисунке 7.

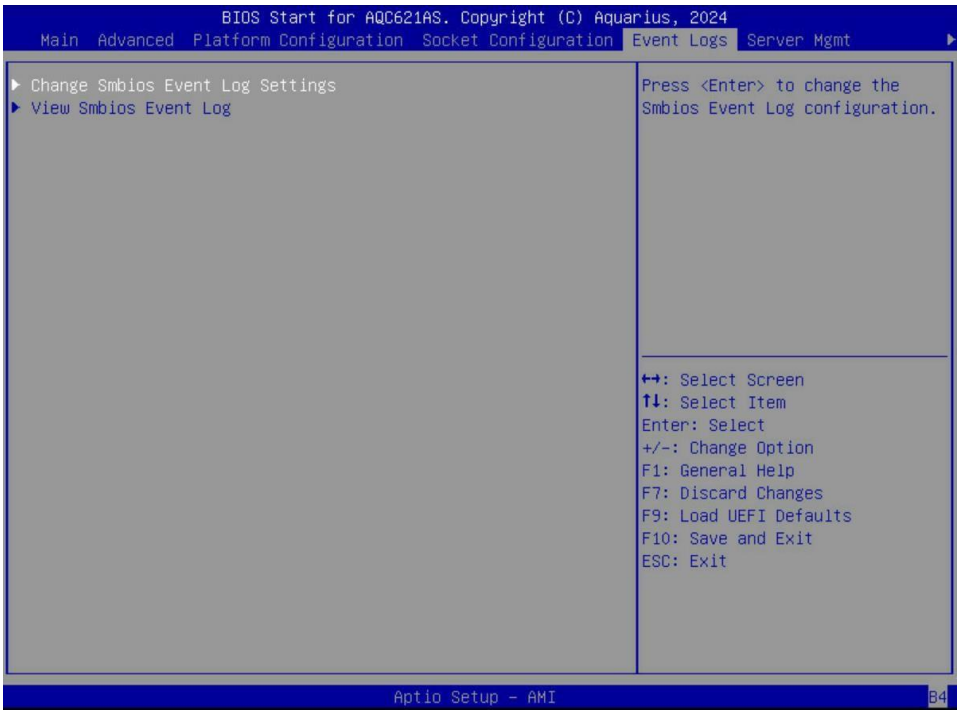

Рисунок 7 – Вкладка «Журнал событий» («Event Logs»)

6.1.9 Вкладка «Безопасность» («Security»)

Для определения способов корректной установки паролей администратора и пользователей в меню ПО «Старт-621AS» служит вкладка Безопасность (Security).

Если в системе установлен только пароль администратора, то он лишь ограничивает доступ к программе установки Setup и запрашивается только при входе в Setup.

Если в системе установлен только пароль пользователя, то его необходимо ввести для загрузки или входа в программу установки Setup. В программе установки пользователь будет иметь права администратора.

Внешний вид вкладки «Безопасность» представлен на рисунке 8.

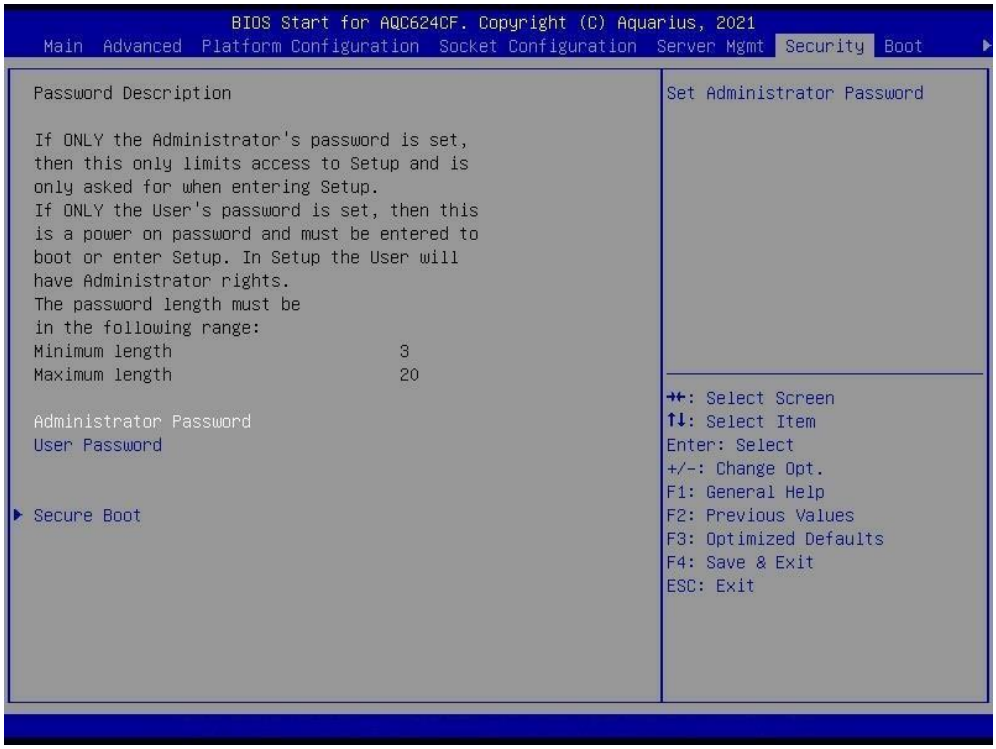

Рисунок 8 – Вкладка «Безопасность» («Security»)

6.1.10 Вкладка «Загрузка» («Boot»)

Вкладка «Загрузка» определяет последовательность приоритетов для всех устройств начальной загрузки операционной системы из доступных USBустройств. Порядок приоритета загрузки – это порядок, в котором компьютер начинает искать операционную систему на доступных устройствах.

Внешний вид вкладки «Загрузка» представлен на рисунке 9.

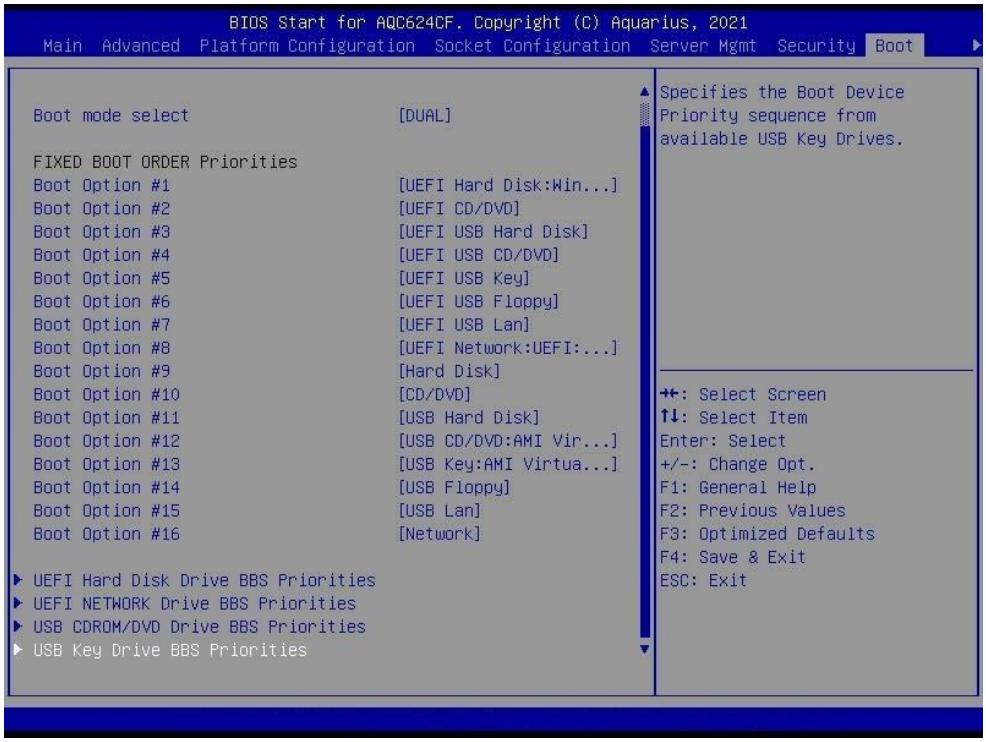

Рисунок 9 – Вкладка «Загрузка» («Boot»)

6.1.11 Вкладка «Сохранение и Выход» («Save & Exit»)

Вкладка «Сохранение и Выход» отвечает за управление сделанными изменениями: сохранение, отмену, возврат к прежним настройкам или к настройкам по умолчанию, а также за выход из меню.

Внешний вид вкладки «Сохранение и Выход» представлен на рисунке 10.

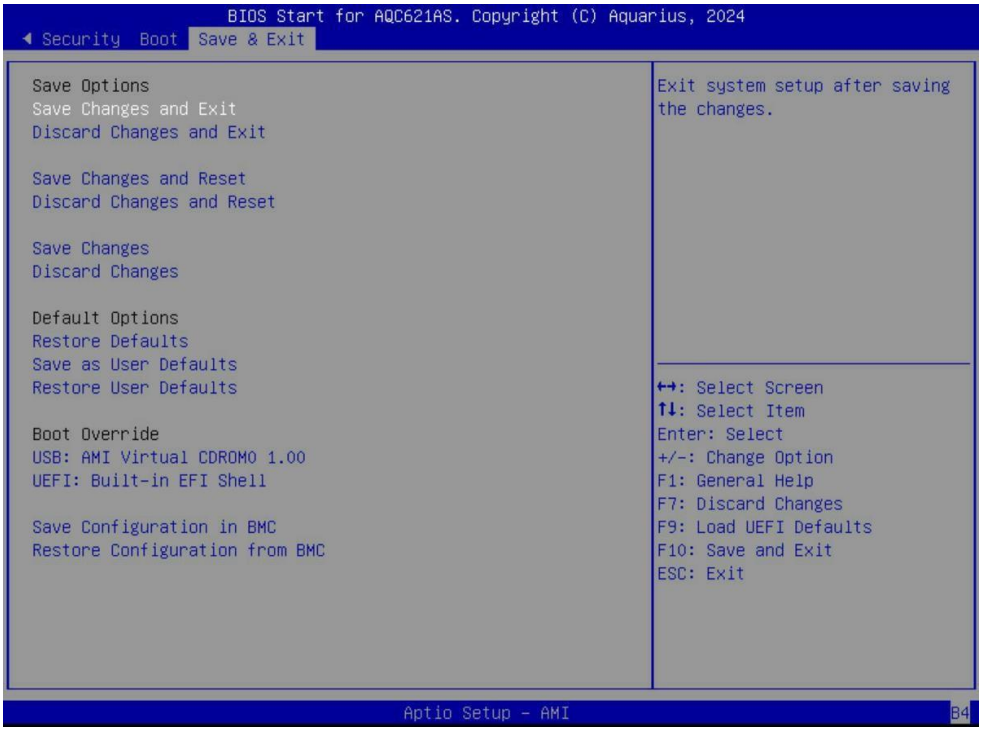

Рисунок 10 – Вкладка «Сохранение и Выход» («Save & Exit»)

6.2 Установка обновлений

Установка обновлений ПО «Старт621AS» производится силами Заказчика.

6.3 Штатное функционирование

ПО «Старт621AS» функционирует при его запуске на ПК. Все функции программы доступны после ее запуска.

В качестве используемых технических средств ПО «Старт621AS» могут выступают сервисные процессоры, встроенные на материнской плате AQC621AB производства компании «Aquarius». Загрузка ПО «Старт621AS» осуществляется автоматически при подаче дежурного питания на сервисный процессор.

Встраиваемое и общесистемное ПО «Старт621AS» функционирует на ЭВМ, имеющей состав и характеристики не ниже указанных в таблице 2.

Таблица 2. Состав и технические характеристики ЭВМ для функционирования ПО

Состав	**Технические характеристики**
Электронно-вычислительная машина (ЭВМ)	Средства вычислительной техники на базе системной платы AQC621AS

Для функционирования ПО «Старт621AS» дополнительного программного обеспечения не требуется. Если в системном программном обеспечении БСВВ Старт621AS невозможно найти необходимое меню, то целесообразно обратиться к руководству по эксплуатации сервера, системной платы или на сайт производителя

6.4 Запуск ПО «Старт621AS»

Для входа в программу необходимо выполните следующие ниже действия.

1) Обеспечить питание системной платы.
2) Нажать клавишу при появлении строки:
   - Press DEL or F2 to enter Setup
   - Нажмите DEL или F2 для входа в Setup

После нажатия клавиши на экране появится главное меню (Main Menu) БСВВ Старт621AS, из которого возможно попасть в другие меню, например, меню набора микросхем (Chipset Menu), меню питания (Power Menu) и т.п.

В большинстве случаев для вызова экрана загрузки используется клавиша DEL. В некоторых случаях используются другие клавиши, например,<F1>, <F2> и т.д. Пользователь может нажать клавишу во время загрузки, чтобы переключиться с загрузочного экрана для просмотра сообщений нажатия клавиши

6.5 Резервное копирование и восстановление данных

Для ПО «Старт621AS» не предусмотрено резервное копирование данных.

6.6 Проведение диагностики ПО «Старт621AS»

Для диагностики и решения возникших вопросов пользователю необходимо обращаться в службу поддержки производителя ПО «Старт621AS».

7 Аварийные ситуации

Информацию об аварийных ситуациях Исполнитель получает от пользователей. Для разрешения возникших в процессе эксплуатации вопросов, консультации и сообщения о неисправности пользователь может обратиться в службу поддержки.

В качестве средства предоставления диагностической информации о процессе загрузки POST и средства устранения неполадок, связанных с зависанием системы во время процедуры загрузки, системная плата имеет встроенный индикатор POST-кода на задней части системной платы (за разъемом VGA).

При запуске каждой процедуры на светодиодном индикаторе диагностики POST-кода на задней стороне системной платы отображается заданный номер кода POST.

Ядро процессора можно настроить для отправки кодов состояния в различные источники. Два наиболее часто используемых типов кодов состояния – коды контрольных точек и звуковые коды.

Контрольные точки обычно выводятся на порт ввода-вывода 80h, но ядро процессора также можно настроить для отправки контрольных точек в различные источники.

Звуковые коды, как правило, представляют собой коды ошибок, которые не возникают во время обычной загрузки. Каждая цифра в коде представлена последовательностью звуковых сигналов, число которых равно цифре.

Загрузка POST характеризуется несколькими фазами, которые обусловливают различные контрольные точки и звуковые сигналы описания кода загрузки:

- Security (SEC);
- Pre-EFI Initialization (PEI);
- Driver Execution Environment (DXE); − Boot Device Selection (BDS).

Большинство ошибок, обнаруженных в процессе выполнения POST, определяются с помощью кодов ошибок POST. Эти коды представляют собой характерные ошибки, предупреждения или информацию. Коды ошибок POST могут отображаться на экране дисплея и всегда заносятся в журнал системных событий System Event Log (SEL). Зарегистрированные события доступны приложениям управления системой, включая удаленное и автономное Out of Band (OOB).

Существуют исключительные случаи ранней инициализации, когда системные ресурсы не инициализируются должным образом для обработки отчетов по кодам ошибок POST. Эти случаи являются, главным образом, фатальными ошибками, возникающими в результате

инициализации процессоров и памяти, и о них сообщается диагностическим светодиодным дисплеем с остановкой системы.

Каждому коду ошибки присваивается тип ошибки, определяющий действие BIOS при обнаружении ошибки. Типы ошибок включают второстепенные, основные и неустранимые. Действие BIOS для каждого из них определяется следующим образом:

− второстепенные (Minor): сообщение об ошибке может отображаться на экране или в диспетчере ошибок BIOS setup, и код ошибки POST регистрируется в SEL. Система продолжает загрузку в ошибочном состоянии. Пользователь может заменить ошибочный блок. Параметр «POST Error Pause» в программе BIOS setup не влияет на эту ошибку;

− основные (Major): на экран диспетчера ошибок выводится сообщение об ошибке, и она регистрируется в SEL. Если включена опция BIOS setup «Post Error Pause», то для продолжения загрузки системы требуется вмешательство оператора. Если опция BIOS setup «POST Error Pause» отключена, то система продолжает загружаться.;

− неустранимые (Fatal): если система не может загрузиться, то функция POST останавливается и отображается следующее сообщение: «Обнаружена неустранимая ошибка. Система не будет загружаться, пока ошибка не будет устранена. Нажмите < F2 > для ввода настроек».

В таблице 2 представлен стандартные поддерживаемые коды диагностики и ошибок для каждой фазы загрузки.

Таблица 2 Стандартные коды для каждой фазы загрузки

Код состояния	Описание состояния и действие, которое необходимо предпринять по сообщениям об ошибке
Фаза SEC	
0x00	Не используется
Коды Progress Codes	
0x01	Включите питание. Обнаружение типа сброса type detection (soft/hard)
0x02	Инициализация AP перед загрузкой микрокода
0x03	Инициализация северного моста North Bridge перед загрузкой микрокода
0x04	Инициализация южного моста South Bridge перед загрузкой микрокода
0x05	Инициализация OEM перед загрузкой микрокода
0x06	Загрузка микрокода
0x07	Инициализация AP после загрузки микрокода
0x08	Инициализация северного моста North Bridge после загрузки микрокода
0x09	Инициализация южного моста South Bridge после загрузки микрокода
0x0A	Инициализация OEM после загрузки микрокода
0x0B	Инициализация кэша
0x0C–0x0D	Зарезервировано для будущих кодов ошибок АКВАРИУС SEC
0x0E	Микрокод не найден

0x0F	Микрокод не загружен
Фаза PEI	
0x10	Ядро PEI запущено
0x11	Предварительная инициализация памяти процессора CPU запущена
0x12	Предварительная инициализация памяти процессора CPU (характерная для модуля CPU)
0x13	Предварительная инициализация памяти процессора CPU (характерная для модуля CPU)
0x14	Предварительная инициализация памяти процессора CPU (характерная для модуля CPU)
0x15	Предварительная инициализация памяти северного моста North Bridge запущена
0x16	Предварительная инициализация памяти северного моста North Bridge (характерная для модуля North Bridge)
0x17	Предварительная инициализация памяти северного моста North Bridge (характерная для модуля North Bridge)
0x18	Предварительная инициализация памяти северного моста North Bridge (характерная для модуля North Bridge)
0x19	Предварительная инициализация памяти южного моста South Bridge запущена
0x1A	Предварительная инициализация памяти южного моста South Bridge (характерная для модуля South Bridge)
0x1B	Предварительная инициализация памяти южного моста South Bridge (характерная для модуля South Bridge)
0x1C	Предварительная инициализация памяти южного моста South Bridge (характерная для модуля South Bridge)
0x1D – 0x2A	Коды предварительной инициализации OEM-памяти
0x2B	Инициализация памяти. Считывание данных SPD (Serial Presence Detect)
0x2C	Инициализация памяти. Обнаружение присутствия памяти

0x2D	Инициализация памяти. Программирование таймингов памяти
0x2E	Инициализация памяти. Конфигурация памяти
0x2F	Инициализация памяти (другое)
0x30	Зарезервировано для ASL (см. раздел «Коды состояния ASL» ниже)
0x31	Память установлена
0x32	Запущена инициализация процессора после ввода памяти (CPU postmemory инициализация)
0x33	CPU post-memory инициализация. Инициализация кэша
0x34	CPU post-memory инициализация. Инициализация прикладных процессоров Application Processor(s) (AP)
0x35	CPU post-memory инициализация. Выбор процессора загрузки Boot Strap Processor (BSP)
0x36	CPU post-memory инициализация. Инициализация режима управления системой System Management Mode (SMM)
0x37	Запущена инициализация северного моста North Bridge после ввода памяти (Post-Memory North Bridge инициализация)

0x38	Post-Memory North Bridge инициализация (характерная для North Bridge модуля)
0x39	Post-Memory North Bridge инициализация (характерная для North Bridge модуля)
0x3A	Post-Memory North Bridge инициализация (характерная для North Bridge модуля)
0x3B	Запущена инициализация южного моста South Bridge после ввода памяти (Post-Memory South Bridge инициализация)
0x3C	Post-Memory South Bridge инициализация (характерная для South Bridge модуля)
0x3D	Post-Memory South Bridge инициализация (характерная для South Bridge модуля)
0x3E	Post-Memory South Bridge инициализация (характерная для South Bridge модуля)
0x3F-0x4E	Коды инициализации после ввода OEM-памяти
0x4F	Процедура DXE IPL запущена
Коды ошибок PEI Error Codes	
0x50	Ошибка инициализации памяти. Недопустимый тип памяти или несовместимая скорость памяти
0x51	Ошибка инициализации памяти. Сбой чтения SPD
0x52	Ошибка инициализации памяти. Неверный размер памяти или модули памяти не совпадают
0x53	Ошибка инициализации памяти. Полезная память не обнаружена
0x54	Неизвестная ошибка инициализации памяти
0x55	Память не установлена
0x56	Недопустимый тип процессора CPU или скорость процессора CPU
0x57	Несоответствие процессора CPU
0x58	Не удалось выполнить самопроверку процессора CPU или возможная ошибка кэша процессора
0x59	Микрокоды процессора CPU не найдены или обновление микрокодов не выполнено
0x5A	Внутренняя ошибка процессора CPU
0x5B	Переустановка PPI невозможна
0x5C	Отказ самотестирования BMC фазы PEI

0x5C-0x5F	Зарезервировано под коды будущих ошибок АКВАРИУС
Коды состояний S3 Resume Progress Codes	
0xE0	S3 Resume запускается (S3 Resume PPI вызывается DXE IPL)
0xE1	Выполнение сценария загрузки S3 Boot Script
0xE2	Видеорепост
0xE3	Вызов программы пробуждения OS S3 Wake vector
0xE4-0xE7	Зарезервировано по коды будущих состояний АКВАРИУС
Коды состояний S3 Resume Error Codes	
0xE8	Процесс S3 Resume не выполнен
0xE9	S3 Resume PPI не найден
0xEA	Ошибка сценария загрузки S3 Resume Boot Script
0xEB	Ошибка программы пробуждения S3 OS Wake

0xEC-0xEF	Зарезервировано под коды будущих ошибок АКВАРИУС
Коды состояний восстановления Recovery Progress Codes	
0xF0	Состояние восстановления, инициируемое микропрограммным обеспечением (Auto recovery – автоматическое восстановление)
0xF1	Состояние восстановления, инициируемое пользователем (Forced recovery – принудительное восстановление)
0xF2	Процесс восстановления Recovery process запущен
0xF3	Образ микропрограммы автоматического восстановления Recovery firmware найден
0xF4	Образ микропрограммы автоматического восстановления Recovery firmware загружен
0xF5-0xF7	Зарезервировано под коды будущих состояний АКВАРИУС
Коды ошибок восстановления Recovery Error Codes	
0xF8	Процесс Recovery PPI недоступен
0xF9	Программа восстановления Recovery capsule не найдена
0xFA	Недопустимая программа восстановления: Invalid recovery capsule
0xFB – 0xFF	Зарезервировано под коды будущих ошибок АКВАРИУС
Фаза DXE	
0x60	Ядро DXE Core запущено
0x61	Инициализация NVRAM
0x62	Инсталляция временных сервисов южного моста South Bridge Runtime Services
0x63	Запущена инициализация CPU DXE
0x64	Инициализация CPU DXE (характерная для модуля CPU)
0x65	Инициализация CPU DXE (характерная для модуля CPU)
0x66	Инициализация CPU DXE (характерная для модуля CPU)
0x67	Инициализация CPU DXE (характерная для модуля CPU)
0x68	Инициализация хост-моста PCI host bridge
0x69	Запущена инициализация North Bridge DXE (DXE северного моста)
0x6A	Запущена инициализация North Bridge DXE SMM
0x6B	Инициализация North Bridge (характерная для модуля северного моста North Bridge)
0x6C	Инициализация North Bridge (характерная для модуля северного моста North Bridge)
0x6D	Инициализация North Bridge (характерная для модуля северного моста North Bridge)

0x6E	Инициализация North Bridge (характерная для модуля северного моста North Bridge)
0x6F	Инициализация North Bridge (характерная для модуля северного моста North Bridge)
0x70	Запущена инициализация South Bridge DXE (DXE южного моста)
0x71	Запущена инициализация South Bridge DXE SMM
0x72	Инициализация устройств South Bridge
0x73	Инициализация South Bridge (характерная для модуля южного моста North Bridge)

0x74	Инициализация South Bridge (характерная для модуля южного моста North Bridge)
0x75	Инициализация South Bridge (характерная для модуля южного моста North Bridge)
0x76	Инициализация South Bridge (характерная для модуля южного моста North Bridge)
0x77	Инициализация South Bridge (характерная для модуля южного моста North Bridge)
0x78	Инициализация модуля ACPI
0x79	Инициализация CSM
0x7A – 0x7F	Зарезервировано под будущие коды АКВАРИУС DXE
0x80 – 0x8F	Коды инициализации OEM DXE
0x90	Фаза Boot Device Selection (BDS) запущена
0x91	Подключение драйвера запущено
0x92	Инициализация шины PCI Bus запущена
0x93	Инициализация контроллера горячей замены PCI Bus Hot Plug Controller
0x94	Перечисление шин PCI Bus
0x95	Запрос ресурсов PCI Bus
0x96	Назначение ресурсов PCI Bus
0x97	Подключение устройств вывода консоли
0x98	Подключение устройств ввода консоли
0x99	Супер-инициализация ввода/вывода (Super IO initialization)
0x9A	Инициализация USB запущена
0x9B	Переустановка USB
0x9C	Обнаружение USB
0x9D	Включение USB
0x9E – 0x9F	Зарезервировано под будущие коды АКВАРИУС
0xA0	Инициализация IDE запущена
0xA1	Переустановка IDE
0xA2	Обнаружение IDE
0xA3	Включение IDE
0xA4	Инициализация SCSI запущена
0xA5	Переустановка SCSI
0xA6	Обнаружение SCSI
0xA7	Включение SCSI
0xA8	Пароль проверки установки
0xA9	Старт установки
0xAA	Зарезервировано для ASL (см. раздел «Коды состояния ASL» ниже)

0xAB	Ожидание ввода установки Setup Input
0xAC	Зарезервировано для ASL (см. раздел «Коды состояния ASL» ниже)
0xAD	Событие Ready to Boot (готов к загрузке)

0xAE	Событие Legacy Boot (унаследованная загрузка)
0xAF	Событие Exit Boot Services (выход из служб загрузки)
0xB0	Начало времени выполнения Runtime Set Virtual Address MAP
0XB1	Конец времени выполнения Runtime Set Virtual Address MAP
0xB2	Унаследованный вариант инициализации ROM
0xB3	Переустановка системы
0xB4	Горячая установка USB
0xB5	Горячая установка PCI bus
0xB6	Очистка NVRAM
0xB7	Переустановка конфигурации (переустановка настроек NVRAM)
0xB8 – 0xBF	Зарезервировано под будущие коды АКВАРИУС
0xC0 – 0xCF	Коды инициализации OEM BDS
Коды ошибок DXE Error Codes	
0xD0	Ошибка инициализации процессора CPU
0xD1	Ошибка инициализации северного моста North Bridge
0xD2	Ошибка инициализации южного моста South Bridge
0xD3	Некоторые архитектурные протоколы недоступны
0xD4	Ошибка выделения ресурсов PCI. Недостаточно ресурсов
0xD5	Недостаточно места для унаследованной версии ROM
0xD6	Устройства вывода консоли не найдены
0xD7	Устройства ввода консоли не найдены
0xD8	Неверный пароль
0xD9	Ошибка загрузки Boot Option (возвращена ошибка LoadImage)
0xDA	Не удалось выполнить Boot Option (возвращена ошибка StartImage)
0xDB	Сбой обновления флэш-памяти
0xDC	Протокол переустановки Reset недоступен
0xDD	Отказ самотестирования BMC фазы DXE
Контрольные точки ACPI/ASL	
0x01	Система входит в спящий режим S1
0x02	Система входит в спящий режим S2

0x03	Система входит в спящий режим S3
0x04	Система входит в спящий режим S4
0x05	Система входит в спящий режим S5
0x10	Система выходит (просыпается) из спящего режима S1
0x20	Система выходит (просыпается) из спящего режима S2
0x30	Система выходит (просыпается) из спящего режима S3
0x40	Система выходит (просыпается) из спящего режима S4
0xAC	Система перешла в режим ACPI. Контроллер прерываний находится в режиме PIC
0xAA	Система перешла в режим ACPI. Контроллер прерываний находится в режиме APIC
OEM-зарезервированные диапазоны контрольных точек	
0x05	Инициализация OEM SEC перед загрузкой микрокода
0x0A	Инициализация OEM SEC после загрузки микрокода
0x1D – 0x2A	Коды инициализации памяти OEM post memory
0x3F – 0x4E	Коды инициализации памяти OEM PEI pre-memory
0x80 – 0x8F	Коды инициализации OEM DXE
0xC0 – 0xCF	Коды инициализации OEM BDS

8 Модернизация ПО «Старт621AS»

ООО «ПК «Аквариус» обеспечивает оценку и ревизию процессов разработки и поддержки ПО BIOS «Старт-621AS», документирование изменений.

Оценка и ревизия процессов выполняется ООО «ПК «Аквариус» при обеспечении контроля качества ПО BIOS «Старт-621AS» на основании обращений, направленных в службу технической поддержки ПО BIOS «Старт621AS».

Модернизация ПО BIOS «Старт-621AS» осуществляется путем загрузки обновленной версии образа диска на схему (перепрошивки) через интерфейс или через TFTP сервер.

Введение функциональных возможностей ПО BIOS «Старт-621AS» в дополнение к уж реализованных возможностям не предусмотрено.

Приложение 1

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ АКВАРИУС» (ООО «ПК АКВАРИУС»)

УТВЕРЖДЕН

RU.АМПР.11002-01 34 01-ЛУ

Программное обеспечение «Базовая система ввода-вывода «Старт621AS» (ПО «Старт621AS») для серверов

Руководство оператора

RU.АМПР.11002-01 34 01

Листов 50

2023

Литера

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

АННОТАЦИЯ

В соответствии с государственными стандартами Российской Федерации руководство оператора входит в состав комплекта эксплуатационной документации на программное обеспечение.

Поскольку перед оператором не ставятся прикладные задачи, которые он может решить с помощью программы тем или иным способом, в том или ином порядке, его работа заключается в выполнении отдельных операций, то есть конкретных последовательностей действий, приводящих к конкретному результату.

В руководстве содержится описания:

- назначения программного обеспечения (ПО) базовой системы ввода/вывода (БСВВ)* Старт621AS, где указываются общие сведения о ПО Старт621AS и область его применения;
- условий выполнения программы БСВВ Старт621AS, где указаны условия, необходимые для работы программного обеспечения;
- выполнения программы БСВВ Старт621AS с описанием последовательности действий оператора, описывающих выполнение его обязанностей, а также ожидаемая реакция программы на действия оператора;
- сообщения оператору с текстами сообщений, выдаваемых в ходе выполнения программы, а также действия оператора, если выполнение программы не соответствует стандартной ситуации.

---

* - аналог БСВВ - BIOS (Basic Input/Output System)

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Встраиваемое и общесистемное программное обеспечение «Базовая система ввода-вывода «Старт621AS» (ПО «Старт621AS») компании Аквариус - БСВВ или программа начального старта, является системной программой низкого уровня, хранящейся в постоянном запоминающем устройстве (ПЗУ) на системной плате, и предоставляет пользователю возможность полного управления системой при загрузке.

БСВВ Старт621AS 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. Среда БСВВ Старт621AS предоставляет расширенные функциональные возможности UEFI (Unified Extensible Firmware Interface), унифицированного расширяемого интерфейса микропрограмм для программного обеспечения низкого уровня, которое запускается автоматически при старте компьютера перед тем, как загрузится операционная система.

UEFI обладает многими преимуществами: поддерживает жесткие диски большего объема, быстрее грузится, более безопасно, обладает графическим интерфейсом и поддерживает мышь, позволяет проводить удаленную настройку и отладку. Программное обеспечение UEFI может храниться во флэш-памяти на системной плате, загружаться с жесткого диска или общего сетевого ресурса.

Основа платформы БСВВ Старт621AS специально разработана 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 предзагрузочных приложений.

ПО «Старт621AS» создано в 2020 г. и предназначено для обеспечения начального старта средств вычислительной техники.

Программное обеспечение «Базовая система ввода-вывода «Старт621AS» обеспечивает:

- инициализацию и запуск средств вычислительной техники и их компонентов;
- передачу управления операционной системе в соответствии с заданными настройками.

Язык высокого уровня С и язык низкого уровня (ассемблер) Asm являются языками программирования для БСВВ Старт621AS.

Программное обеспечение БСВВ Старт621AS функционирует без операционной системы.

ПО «Старт621AS» получило свое название 30.01.2023.

Ввиду быстрого изменения БСВВ Старт621AS внешний вид экранов меню БСВВ Старт621AS на представленных в Руководстве рисунках может отличаться от внешних видов экранов меню БСВВ Старт621AS Вашего компьютера.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Встраиваемое и общесистемное ПО «Базовая система ввода-вывода Старт 624» функционирует на ЭВМ, имеющей состав и характеристики не ниже указанных в таблице (Таблица 1).

Таблица 1. Состав и технические характеристики ЭВМ для функционирования ПО

Состав	Технические характеристики
Электронно-вычислительная машина (ЭВМ)	Средства вычислительной техники на базе системной платы AQC621AS

Программные средства, обеспечивающие выполнение программы

Для функционирования программы дополнительного программного обеспечения не требуется.

Если в системном программном обеспечении БСВВ Старт621AS невозможно найти необходимое меню, то целесообразно обратиться к руководству по эксплуатации сервера, системной платы или на сайт производителя.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Запуск БСВВ Старт621AS

Для входа в программу необходимо выполните следующие ниже действия.

- Обеспечить питание системной платы.
- Нажать клавишу <Delete> при появлении строки:
    - Press DEL or F2 to enter Setup
    - Нажмите DEL или F2 для входа в Setup

После нажатия клавиши <Delete> на экране появится главное меню (Main Menu) БСВВ Старт621AS, из которого возможно попасть в другие меню, например, меню набора микросхем (Chipset Menu), меню питания (Power Menu) и т.п.

Примечание - В большинстве случаев для вызова экрана загрузки используется клавиша <Delete>. В некоторых случаях используются другие клавиши, например <F1>, <F2> и т.д. Пользователь может нажать клавишу <TAB> во время загрузки, чтобы переключиться с загрузочного экрана для просмотра сообщений нажатия клавиши.

3.2. Главный раздел (Main) меню БСВВ Старт621AS

При входе в БСВВ Старт621AS автоматически загружается главный раздел меню (смотрите Рис. 1) Main, в котором представлена информация о версии БСВВ Старт621AS, ее платформе, общей памяти, а также представлены возможности выбора языка системы, определения системной даты и времени.

Главный (Main) раздел меню БСВВ Старт621AS

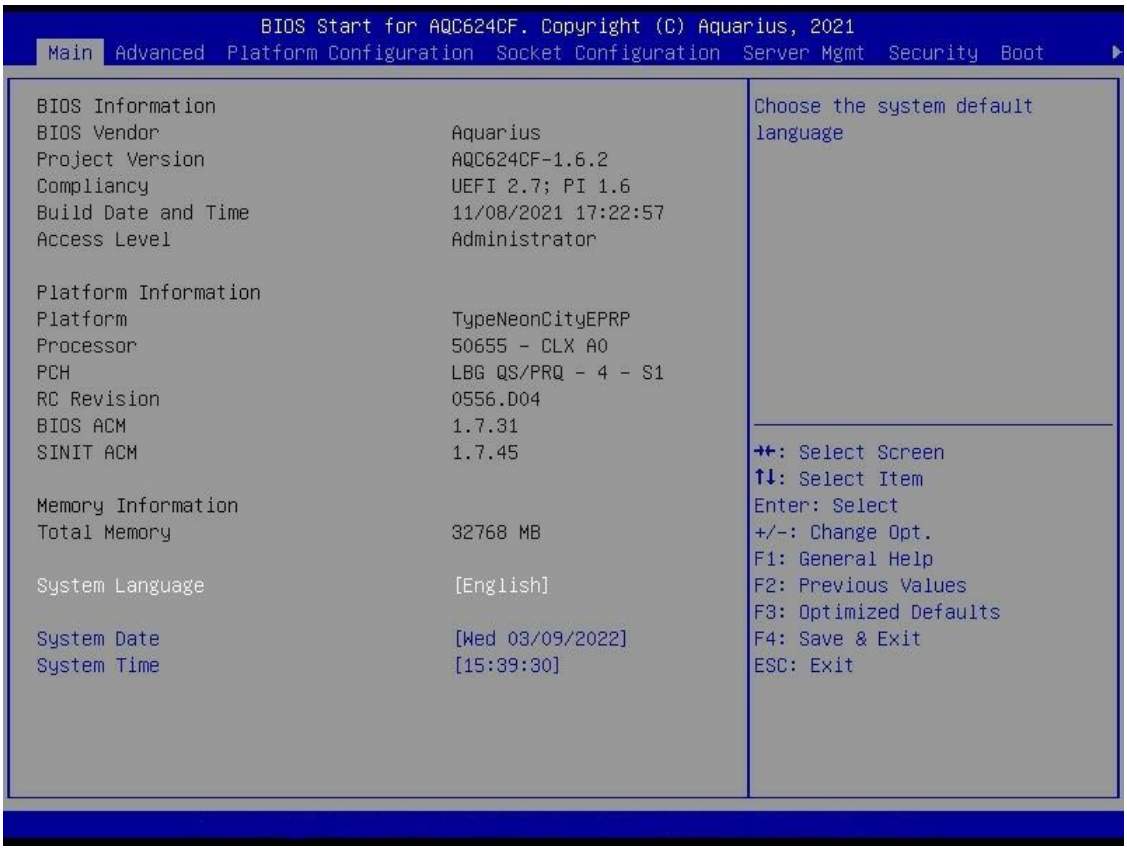

Рис. 1

Основные разделы

Основные разделы главного меню BIOS Старт смотрите в таблице ниже (Таблица 2).

Таблица 2. Основные разделы главного меню БСВВ Старт621AS

Наименование раздела	**Описание**
Информация о BIOS (BIOS Information)	
Производитель BIOS (BIOS Vendor)	Наименование компании-разработчика БСВВ Старт621AS (Аквариус)
Версия BIOS (Project Version)	Текущая версия БСВВ Старт621AS
Соответствие (Compliancy)	Спецификация версии UEFI
Дата и время сборки (Build Date and Time)	Дата (в формате ДД/ММ\ГГГГ) и время (в формате (ЧЧ:ММ:СС) сборки
Уровень доступа (Access Level)	Уровень доступа для текущей сессии (администратор)
Информация о платформе (Platform Information)	
Платформа (Platform)	Информация о платформе
Процессор (Processor)	Информация о процессоре
PCH	Информация о PCH (Platform Controller Hub)
RC Revision	Версия Release Candidate
BIOS ACM	Версия модуля BIOS ACM
SINIT ACM	Версия модуля SINIT ACM
Информация о памяти (Memory Information)	
Общая память (Total Memory)	Информация об общей памяти сервера (в МБ)
Язык системы (System Language)	Выбор языка
Системная дата (System Date)	Установка текущей даты (в формате ДД/ММ/ГГГГ)
Системное время (System Time)	Установка локального времени (в формате ЧЧ:ММ:СС)

Клавиши управления

Описание клавиш управления представлено ниже в таблице (Таблица 3).

Таблица 3. Клавиши управления

Символ	Значение
← →	Перемещает курсор влево или вправо для выбора экрана
↑ ↓	Перемещает курсор вверх или вниз по списку для выбора пункта раздела меню
Enter	Открыть подменю или выбрать команду
+/-	Смена опции
F1	Общая помощь
F2	Предыдущее значение
F3	Оптимальные настройки по умолчанию
F4	Сохранение и выход
Esc	Выход из текущего раздела

3.3. Вкладка Расширенное меню (Advanced) из меню БСВВ Старт621AS

Для настройки в соответствии с предпочтениями пользователя дополнительных опций конфигурации сервера, дистанционного управления консолью, а также для конфигурации портов USB, сетевой конфигурации, аутентификации, конфигурации оперативной памяти служит вкладка Расширенное меню (Advanced) – следующая вкладка меню БСВВ Старт621AS (Рис. 2).

Вкладка Расширенное меню (Advanced) в БСВВ Старт621AS

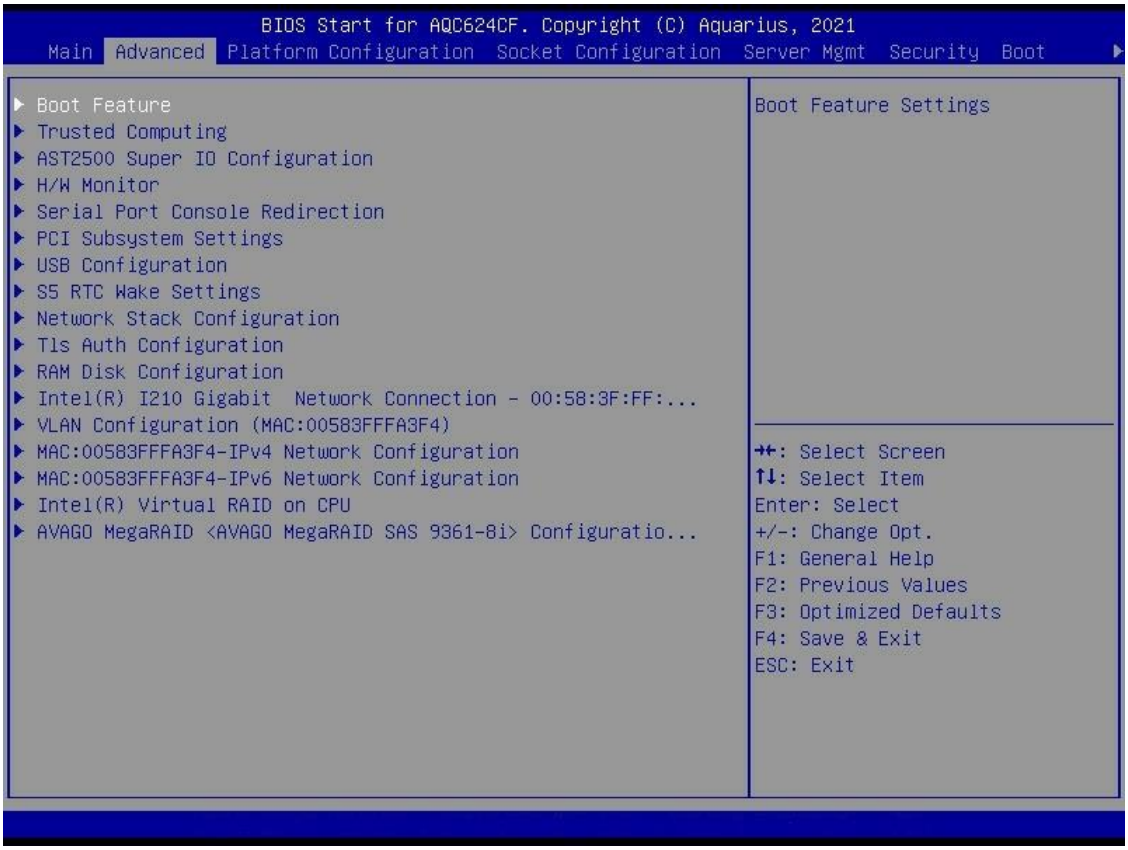

Рис. 2

Основные разделы вкладки Расширенное меню (Advanced) из меню БСВВ Старт621AS смотрите в таблице (Таблица 4).

Таблица 4. Разделы вкладки Расширенное меню (Advanced) из меню БСВВ Старт621AS

Наименование раздела	Описание
Функции загрузки Boot Feature	Настройка особенностей загрузки
Технология безопасности (Trusted Computing)	Настройка параметров безопасности
Конфигурация портов ввода-вывода (AST2500 Super IO Configuration)	Основные настройки последовательных портов ввода-вывода
Аппаратный мониторинг (H/W Monitor)	Основные настройки средств диагностики сервера Hardware Monitor
Порты перенаправления консоли (Serial Port Console Redirection)	Настройка портов перенаправления консоли для дистанционного управления
Настройка подсистемы PC (PCI Subsystem Settings)	Настройки шин расширения PCIe, PCIe, PCI-X, латентности, многопроцессорной графической конфигурации в соответствии с предпочтениями пользователя
Конфигурация портов USB (USB Configuration)	Настройка параметров включения/отключения (для защиты информации) шины USB
Настройки пробуждения системы (S5 RTC Wake Settings)	Включение/отключение пробуждения системы при возникновении аварийного сигнала. Если этот параметр включен, система пробуждается в течение ЧЧ:ММ:СС. По умолчанию параметр отключен
Конфигурация сетевого стека (Network Stack Configuration)	Настройка опций сетевого стека
Конфигурация параметров аутентификации (Tls Auth Configuration)	Настройка опций аутентификации в соответствии с сертификатом GUID. Если сертификат существует, список сертификатов отображается на экране. Если сертификат не существует, информация не отображается.
Конфигурация RAMDISK (RAM Disk Configuration)	Настройка параметров выделения части оперативной памяти для использования в качестве виртуального хранилища

Наименование раздела	Описание
Гигабитный сетевой адаптер Intel ® I210 (Intel ® I210 Gigabit Network Connection)	Настройка сетевого адаптера (при инициализации I210 выполняется проверка наличия внешней флэш-памяти; если она присутствует, запускается проверка актуальной цифровой подписи)
Конфигурация виртуальных локальных сетей (VLAN Configuration)	Настройка виртуальных локальных сетей
Конфигурация встроенной сетевой платы IPv4 (MAC:xxxxxxxxxxxx IPv4 Network Configuration)	Настройка встроенной сетевой платы IPv4
Конфигурация встроенной сетевой платы IPv6 (MAC: xxxxxxxxxxxx IPv6 Network Configuration)	Настройка встроенной сетевой платы IPv6
Настройка параметров для твердотельных накопителей NVMe (Intel ® Virtual RAID on CPU)	Настройка параметров для твердотельных накопителей NVMe, подключенных к процессору
Конфигурация контроллера AVAGO MegaRAID SAS 9361-8i (AVAGO MegaRAID SAS 9361-8i) Configuration	Настройка параметров RAID-контроллера (при его наличии)

3.4. Вкладка Конфигурация платформы (Platform Configuration) в меню БСВВ Старт621AS

Внешний вид экрана вкладки Конфигурация платформы (Platform Configuration) из меню БСВВ Старт621AS представлен на Рис. 3.

Установка некорректных значений параметров этой вкладки вызывает сбой всей системы.

Вкладка Конфигурация платформы (Platform Configuration) из меню БСВВ Старт621AS

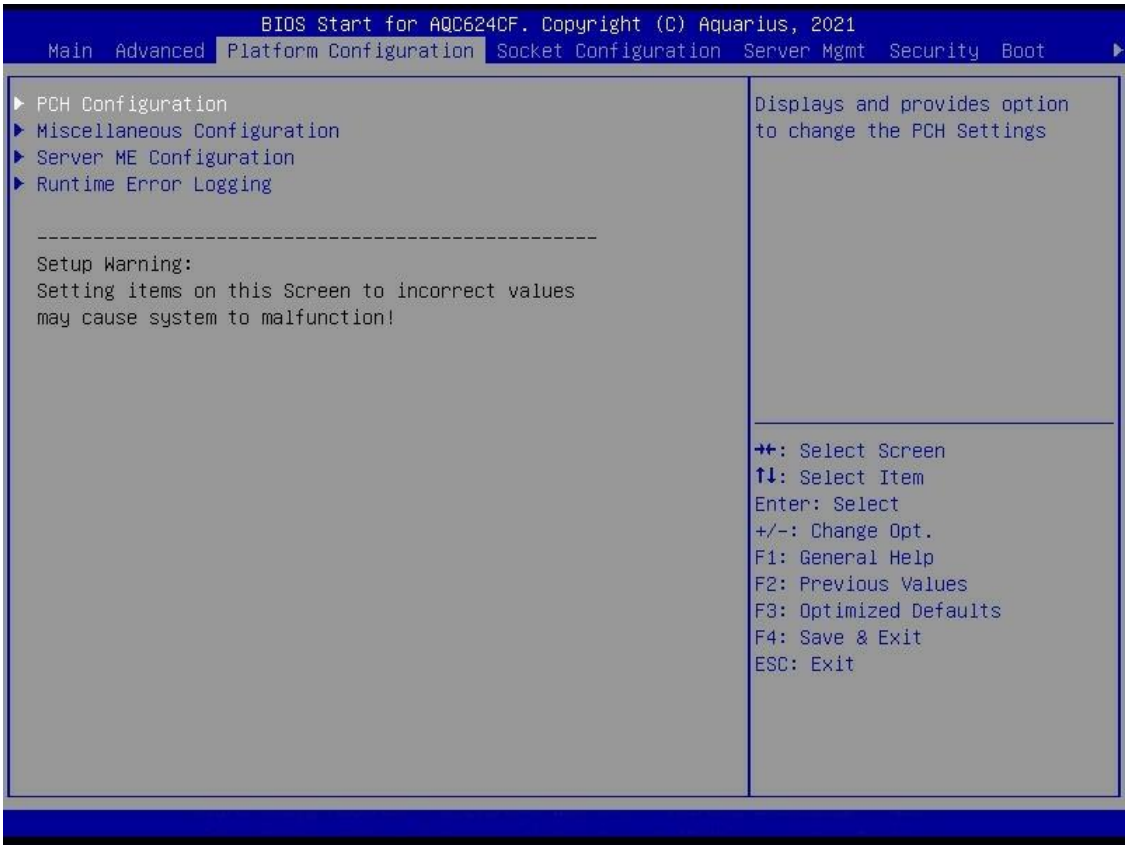

Рис. 3

Основные разделы вкладки Конфигурация платформы (Platform Configuration) из меню БСВВ Старт621AS смотрите в таблице ниже (Таблица 5).

Таблица 5. Разделы вкладки Конфигурация платформы (Platform Configuration) из меню БСВВ Старт621AS

Наименование раздела	Описание
Конфигурация параметров PCH (PCH Configuration)	Настройка параметров PCH (Platform Controller Hub), управляющих работой основных структур системной платы
Различные параметры (Miscellaneous Configuration)	Настройка нечасто использующихся параметров
Конфигурация встроенного программного обеспечения процессора (Server ME Configuration)	Конфигурация параметров встроенного программного обеспечения процессора (отображение информации о версии рабочего микропрограммного обеспечения, его текущем состоянии, его функциях, его кодах ошибки)
Журнал ошибок выполнения (Runtime Error Logging)	Настройка параметров журнала ошибок

3.5. Вкладка Конфигурация сокета (Socket Configuration) в меню БСВВ Старт621AS

Для настройки и конфигурации центрального процессора сервера и его окружения служит вкладка Конфигурация сокета (Socket Configuration) в меню БСВВ Старт621AS. Ее внешний вид представлен на Рис. 4 ниже.

Вкладка Конфигурация сокета (Socket Configuration) из меню БСВВ Старт621AS

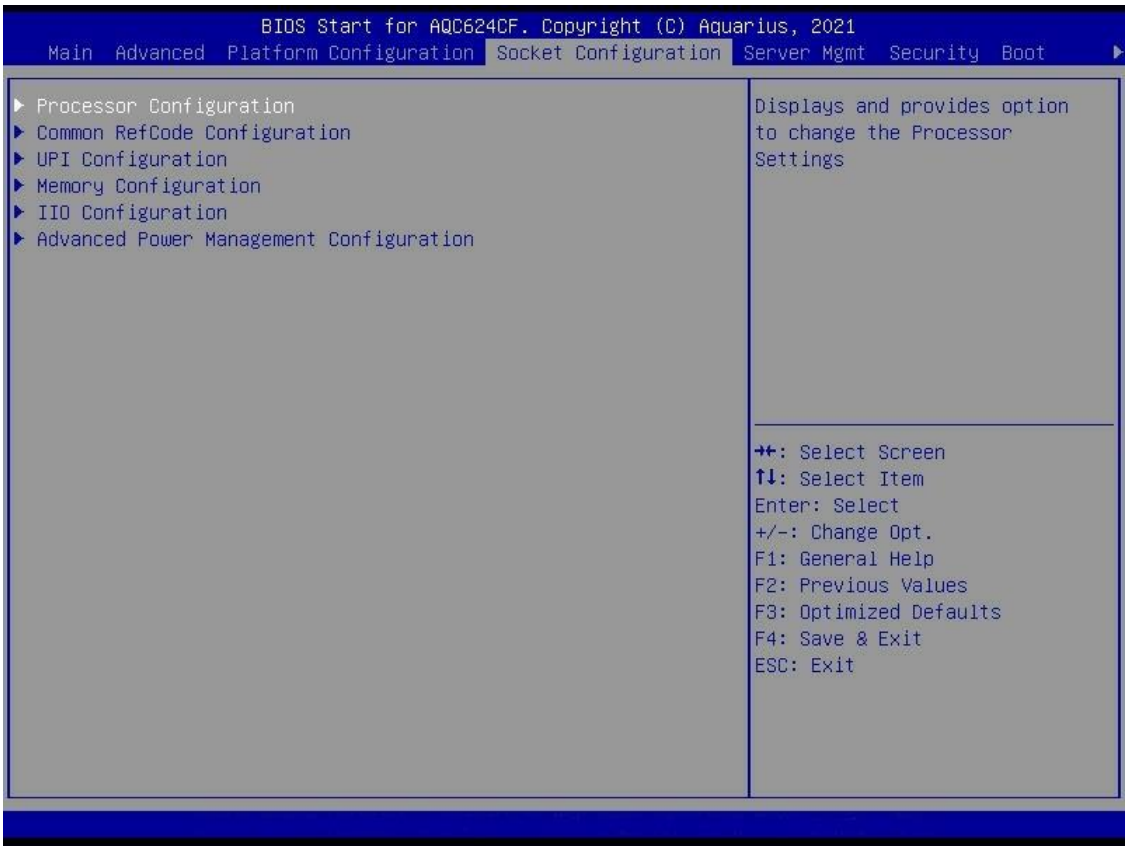

Рис. 4

Разделы вкладки Конфигурация сокета (Socket Configuration) из меню БСВВ Старт621AS смотрите в таблице ниже (Таблица 6).

Таблица 6. Разделы вкладки Конфигурация сокета (Socket Configuration) из меню БСВВ Старт621AS

Наименование раздела	Описание
Конфигурация процессора (Processor Configuration)	Настройка параметров конфигурации процессора
Конфигурация эталонного кода памяти (Common RefCode Configuration)	Определение параметров, отвечающих за общие настройки эталонного кода памяти MRC (Memory Reference Code).
Конфигурация параметров UPI (UPI Configuration)	Определение параметров, отвечающих за настройку UPI (Ultra Path Interconnect), шины, предназначенной для обеспечения взаимодействия между процессорами
Конфигурация памяти (Memory Configuration)	Настройка параметров, управляющих отображением количества настроек таймингов памяти
Конфигурация IIO (IIO Configuration)	Настройка портов PCIe, включая скорость их соединения и максимальный размер полезной нагрузки.
Advanced Power Management Configuration	Настройка включения/отключения поддержки APM (Advanced Power Management)

3.6. Вкладка Управление серверами (Server Mgmt) в меню БСВВ Старт621AS

Внешний вид экрана вкладки Управление серверами (Server Mgmt) из меню БСВВ Старт621AS представлен на Рис. 5. Вкладка служит для мониторинга и обслуживания серверов в сети с целью обеспечения максимальной производительности. Управление серверами также включает управление оборудованием, программным обеспечением, безопасностью и резервным копированием, а также настройки и обновления.

Вкладка Управление серверами (Server Mgmt) из меню БСВВ Старт621AS

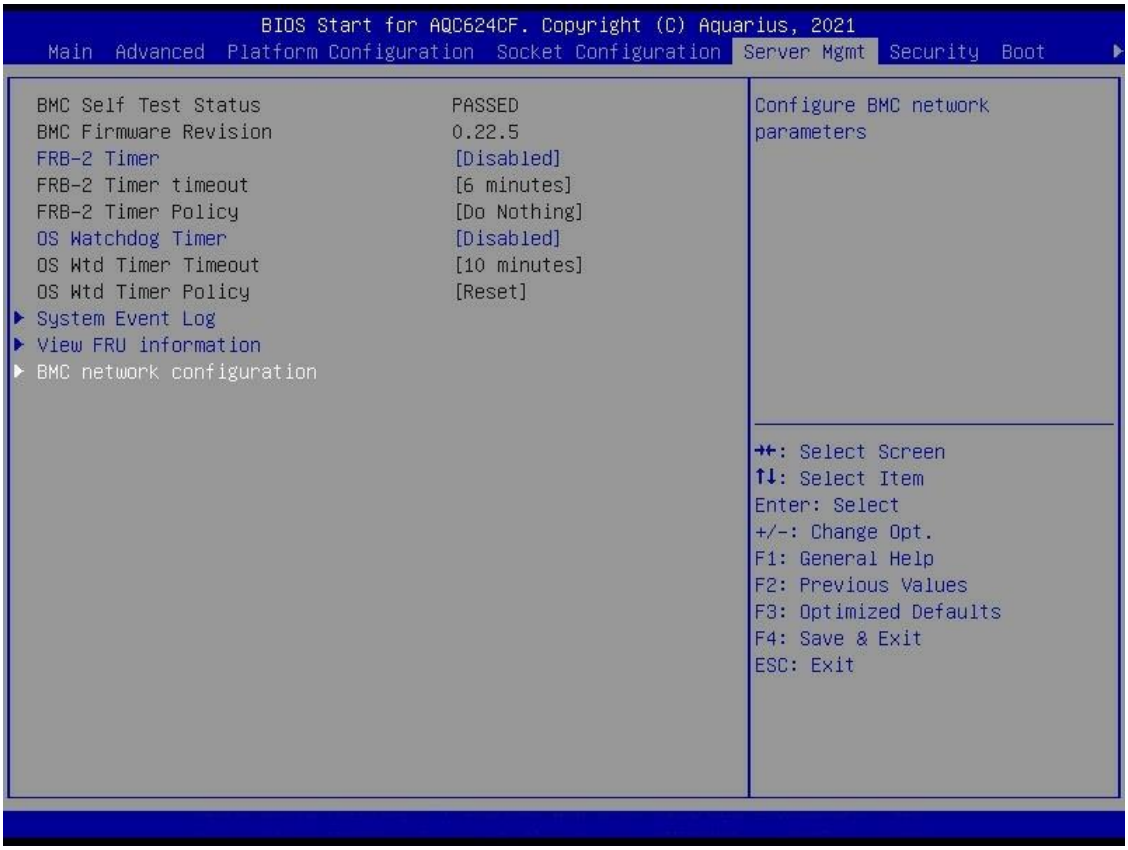

Рис. 5

Разделы вкладки Управление серверами (Server Mgmt) из меню БСВВ Старт621AS смотрите в таблице ниже (Таблица 7).

Таблица 7. Разделы вкладки Управление серверами (Server Mgmt) из меню БСВВ Старт621AS

Наименование раздела	Описание
BMC Self Test Status	Состояние диагностического теста BMC – Прошел/Не прошел (Passed/Failed)
Версия прошивки BMC (BMC Firmware Revision)	Версия программного обеспечения BMC
Второй контрольный таймер отказоустойчивой загрузки (FRB-2 Timer)	Состояние: включен/отключен (Enabled/Disabled)
Время ожидания второго таймера (FRB-2 Timer Timeout)	Время ожидания второго контрольного таймера FRB-2 отказоустойчивой загрузки (6 мин.). Второй контрольный таймер (FRB-2) контроллера BMC устанавливается приблизительно на 6 минут, чтобы дать системе время для выполнения процедуры POST.
Политика второго таймера FRB-2 Timer Policy	Политика второго контрольного таймера отказоустойчивой загрузки FRB-2 (из меню)
Сторожевой таймер операционной системы (OS Watchdog Timer)	Состояние: включен/отключен (Enabled/Disabled)
Время ожидания сторожевого таймера ОС (OS Wtd Timer Timeout)	Время ожидания сторожевого таймера операционной системы (10 мин.)
Политика сторожевого таймера ОС (OS Wtd Timer Policy)	Политика сторожевого таймера операционной системы (из меню)
Журнал системных событий (System Event Log)	Настройка журнала событий системы
Просмотр информации хранилища сменных устройств (View FRU Information)	Просмотр информации хранилища сменных устройств (Field Replaceable Unit)
Конфигурация сети BMC (BMC Network Configuration)	Настройка параметров сети BMC

3.7. Вкладка Безопасность (Security) в меню БСВВ Старт621AS

Для определения способов корректной установки паролей администратора и пользователей в меню БСВВ Старт621AS служит вкладка Безопасность (Security). Ее внешний вид с описанием паролей представлен на Рис. 6 ниже.

Если в системе установлен только пароль администратора, то он лишь ограничивает доступ к программе установки Setup и запрашивается только при входе в Setup.

Если в системе установлен только пароль пользователя, то его необходимо ввести для загрузки или входа в программу установки Setup. В программе установки пользователь будет иметь права администратора.

Вкладка Безопасность (Security) из меню БСВВ Старт621AS

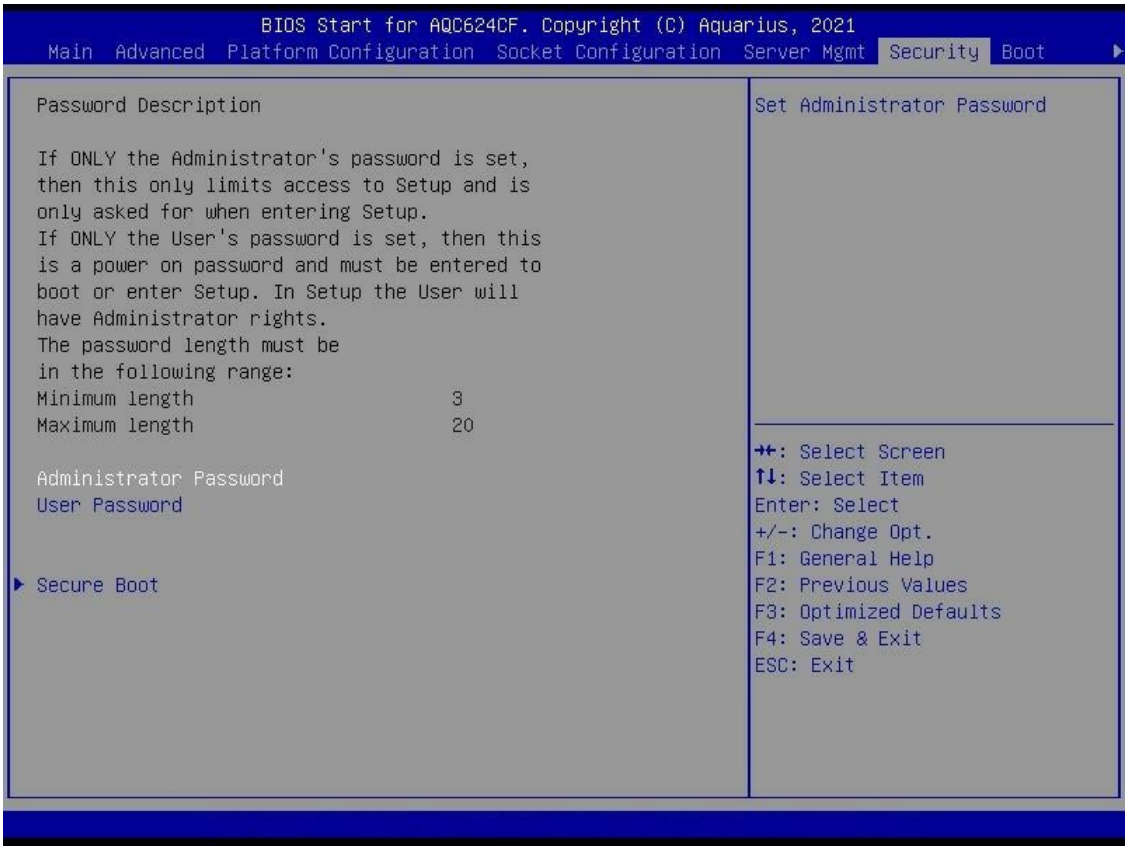

Рис. 6

Разделы вкладки Безопасность (Security) из меню БСВВ Старт621AS смотрите в таблице далее (Таблица 8).

Таблица 8. Разделы вкладки Безопасность (Security) из меню БСВВ Старт621AS

Наименование раздела	Описание
Пароль администратора (Administrator Password)	Установка пароля администратора
Пароль пользователя (User Password)	Установка пароля пользователя
Защищенная загрузка (Secure Boot)	Настройка параметров защищенной загрузки

3.8. Вкладка Загрузка (Boot) в меню БСВВ Старт621AS

Внешний вид экрана вкладки Выход из меню БСВВ Старт621AS представлен на Рис. 7. Вкладка определяет последовательность приоритетов для всех устройств начальной загрузки операционной системы из доступных USB-устройств. Порядок приоритета загрузки - это порядок, в котором компьютер начинает искать операционную систему на доступных устройствах.

Вкладка Загрузка (Boot) из меню БСВВ Старт621AS

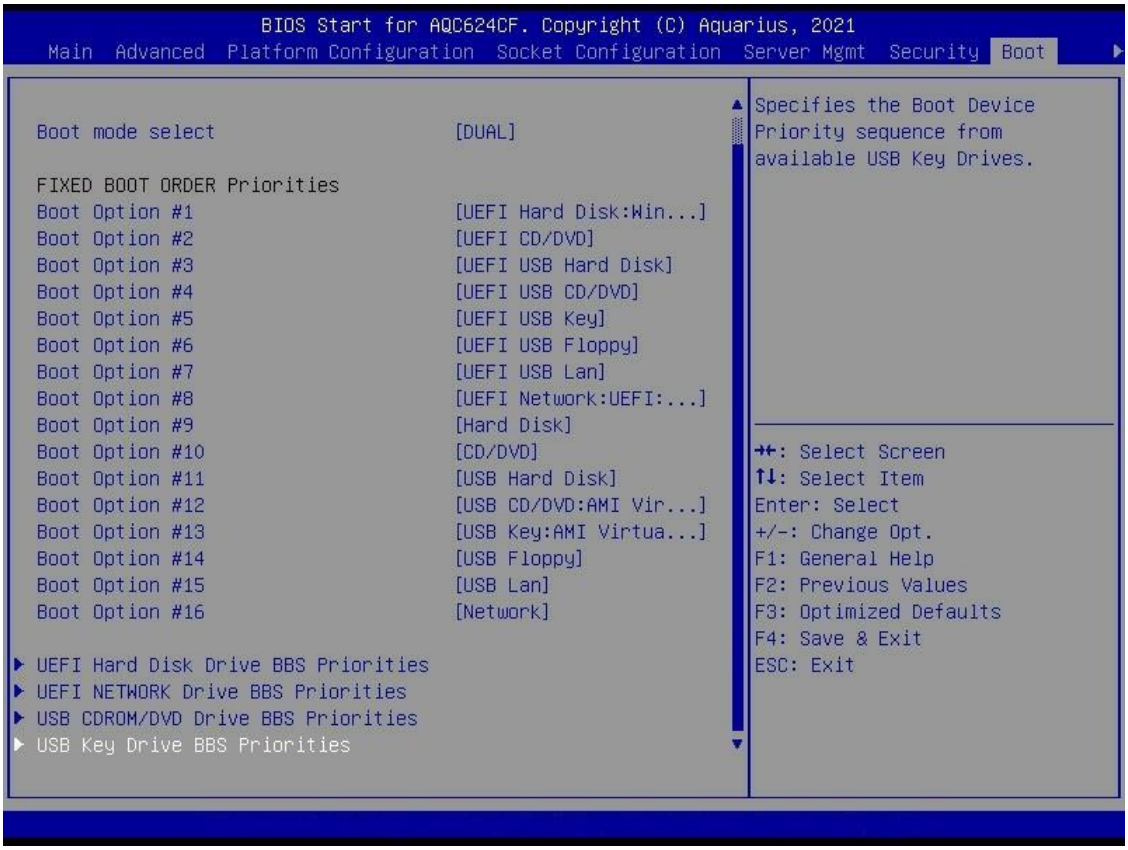

Рис. 7

Основные разделы вкладки Загрузка (Boot) из меню БСВВ Старт621AS смотрите в таблице далее (Таблица 9).

Таблица 9. Разделы вкладки Выход из меню БСВВ Старт621AS

Наименование раздела	Описание
Выбор режима загрузки (Boot Mode Select)	Двойной - [Dual]
Фиксированные приоритеты загрузки (Fixed Boot Order Priorities)	
Опция загрузки 1 (Boot Option #1)	[UEFI Hard Disk: Win…]
Опция загрузки 2 (Boot Option #2)	[UEFI CD/DVD]
Опция загрузки 3 (Boot Option #3)	[UEFI USB Hard Disk]
Опция загрузки 4 (Boot Option #4)	[UEFI USB CD/DVD]
Опция загрузки 5 (Boot Option #5)	[UEFI USB Key]
Опция загрузки 6 (Boot Option #6)	[UEFI USB Floppy]
Опция загрузки 7 (Boot Option #7)	[UEFI USB Lan]
Опция загрузки 8 (Boot Option #8)	[UEFI Network:UEFI:]
Опция загрузки 9 (Boot Option #9)	[Hard Disk]
Опция загрузки 10 (Boot Option #10)	[CD/DVD]
Опция загрузки 11 (Boot Option #11)	[USB Hard Disk]
Опция загрузки 12 (Boot Option #12)	[USB CD/DVD:AMI Vir…]
Опция загрузки 13 (Boot Option #13)	[USB Key:AMI Vir…]
Опция загрузки 14 (Boot Option #14)	[USB Floppy]
Опция загрузки 15 (Boot Option #15)	[USB Lan]
Опция загрузки 16 (Boot Option #16)	[Network]
Приоритеты загрузки жесткого диска из UEFI (UEFI Hard Disk Drive BBS Priorities)	Установка приоритета загрузки жестких дисков. Настройка содержится в UEFI.

Наименование раздела	Описание
Приоритеты загрузки сетевого диска из UEFI (UEFI Network Drive BBS Priorities)	Установка приоритета загрузки сетевого диска. Настройка содержится в UEFI.
Приоритеты загрузки привода CDROM/DVD из UEFI (UEFI CDROM/DVD Drive BBS Priorities)	Установка приоритетов загрузки привода CDROM/DVD. Настройка содержится в UEFI.
Приоритеты загрузки диска USB (USB Key Drive BBS Priorities)	Установка приоритетов загрузки диска USB.

4. СООБЩЕНИЯ ОПЕРАТОРУ

В качестве средства предоставления диагностической информации о процессе загрузки POST и средства устранения неполадок, связанных с зависанием системы во время процедуры загрузки, системная плата имеет встроенный индикатор POST-кода на задней части системной платы (за разъемом VGA).

При запуске каждой процедуры на светодиодном индикаторе диагностики POST-кода на задней стороне системной платы отображается заданный номер кода POST.

Коды состояния (Status Codes) – значения данных, используемые для предоставления диагностической информации о процессе загрузки. **Прогресс-коды (Progress Codes)** – коды состояний, которые указывают на успешный переход к следующему этапу инициализации. Коды ошибок указывают на наличие ошибок в процессе инициализации системы.

Ядро процессора можно настроить для отправки кодов состояния в различные источники. Два наиболее часто используемых типов кодов состояния – коды контрольных точек и звуковые коды.

Коды контрольных точек – значения данных размером 1 байт. Контрольные точки обычно выводятся на порт ввода-вывода 80h, но ядро процессора также можно настроить для отправки контрольных точек в различные источники.

Контрольные точки весьма полезны разработчикам программного обеспечения или техническим специалистам при отладке проблем, возникающих на серверном оборудовании во время процесса предварительной загрузки.

Звуковой код – серия коротких звуковых сигналов. Звуковые коды, как правило, представляют собой коды ошибок, которые не возникают во время обычной загрузки. Каждая цифра в коде представлена последовательностью звуковых сигналов, число которых равно цифре.

Звуковые сигналы не являются единственными звуками, генерируемыми в процессе загрузки. Некоторые микропрограммные компоненты могут использовать звуки для уведомления пользователя о других событиях, таких как обнаружение необходимости горячей замены устройства. Эти звуки обычно генерируются с использованием частоты, которая отличается от частоты звуковых кодов

Загрузка POST характеризуется несколькими фазами, которые обусловливают различные контрольные точки и звуковые сигналы описания кода загрузки:

- Security (SEC) – безопасность, начальная инициализация низкого уровня
- Pre-EFI Initialization (PEI) – предварительная инициализация памяти (аналог функционала bootblock из унаследованного BIOS),
- Driver Execution Environment (DXE) – инициализация основного оборудования (аналог функционала POST из унаследованного BIOS),
- Boot Device Selection (BDS) – настройка системы, пользовательского интерфейса перед загрузкой операционной системы и выбором источника загрузки (CD/DVD, HDD, USB, сеть, Shell и т.д.)

Во время зависания системы в процессе загрузки отображаемый код POST может использоваться для идентификации последней запущенной до возникновения ошибки процедуры POST, что помогает выявить возможную причину зависания.

Большинство ошибок, обнаруженных в процессе выполнения POST, определяются с помощью кодов ошибок POST. Эти коды представляют собой характерные ошибки, предупреждения или информацию. Коды ошибок POST могут отображаться на экране дисплея и всегда заносятся в журнал системных событий System Event Log (SEL). Зарегистрированные события доступны приложениям управления системой, включая удаленное и автономное Out of Band (OOB).

Существуют исключительные случаи ранней инициализации, когда системные ресурсы не инициализируются должным образом для обработки отчетов по кодам ошибок POST. Эти случаи являются, главным образом, фатальными ошибками, возникающими в результате инициализации процессоров и памяти, и о них сообщается диагностическим светодиодным дисплеем с остановкой системы.

В таблице, представленной ниже (Таблица 10) перечислены стандартные контрольные точки (поддерживаемые коды диагностики и ошибок POST для каждой фазы загрузки SEC, PEI, DXE, BDS).

Каждому коду ошибки присваивается тип ошибки, определяющий действие BIOS при обнаружении ошибки. Типы ошибок включают второстепенные, основные и неустранимые. Действие BIOS для каждого из них определяется следующим образом:

- второстепенные (Minor): сообщение об ошибке может отображаться на экране или в диспетчере ошибок BIOS setup, и код ошибки POST

регистрируется в SEL. Система продолжает загрузку в ошибочном состоянии. Пользователь может заменить ошибочный блок. Параметр «POST Error Pause» в программе BIOS setup не влияет на эту ошибку;

- основные (Major): на экран диспетчера ошибок выводится сообщение об ошибке, и она регистрируется в SEL. Если включена опция BIOS setup «Post Error Pause», то для продолжения загрузки системы требуется вмешательство оператора. Если опция BIOS setup «POST Error Pause» отключена, то система продолжает загружаться.

Замечание – для ошибки с кодом 0xD8 « Invalid password» система останавливается и после следующей перезагрузки отображает код ошибки на экране диспетчера ошибок.

- неустранимые (Fatal): если система не может загрузиться, то функция POST останавливается и отображается следующее сообщение:

«Обнаружена неустранимая ошибка. Система не будет загружаться, пока ошибка не будет устранена. Нажмите < F2 > для ввода настроек»

При нажатии клавиши <F2> на экране диспетчера ошибок появляется сообщение об ошибке, и в журнал системных событий (SEL) заносится сообщение об ошибке с кодом ошибки POST. Загрузка системы будет невозможна, пока ошибка не устранена. Неисправная компонента должна быть заменена. Параметр «POST Error Pause» из программы BIOS setup не влияет на эту ошибку.

Таблица 10. Стандартные контрольные точки

Фаза SEC

Код состояния Status Code (16-ричный)	**Описание**
0x00	Не используется
Коды Progress Codes	
0x01	Включите питание. Обнаружение типа сброса type detection (soft/hard).
0x02	Инициализация AP перед загрузкой микрокода
0x03	Инициализация северного моста North Bridge перед загрузкой микрокода
0x04	Инициализация южного моста South Bridge перед загрузкой микрокода
0x05	Инициализация OEM перед загрузкой микрокода
0x06	Загрузка микрокода
0x07	Инициализация AP после загрузки микрокода
0x08	Инициализация северного моста North Bridge после загрузки микрокода
0x09	Инициализация южного моста South Bridge после загрузки микрокода
0x0A	Инициализация OEM после загрузки микрокода

0x0B	Инициализация кэша
0x0C–0x0D	Зарезервировано для будущих кодов ошибок АКВАРИУС SEC
0x0E	Микрокод не найден
0x0F	Микрокод не загружен

Звуковые коды SEC BeepCodes
Нет

Фаза PEI

Код состояния Progress Code (16-ричный)	**Описание**
0x10	Ядро PEI запущено
0x11	Предварительная инициализация памяти процессора CPU запущена
0x12	Предварительная инициализация памяти процессора CPU (характерная для модуля CPU)
0x13	Предварительная инициализация памяти процессора CPU (характерная для модуля CPU)
0x14	Предварительная инициализация памяти процессора CPU (характерная для модуля CPU)
0x15	Предварительная инициализация памяти северного моста North Bridge запущена
0x16	Предварительная инициализация памяти северного моста North Bridge (характерная для модуля North Bridge)
0x17	Предварительная инициализация памяти северного моста North Bridge (характерная для модуля North Bridge)
0x18	Предварительная инициализация памяти северного моста North Bridge (характерная для модуля North Bridge)
0x19	Предварительная инициализация памяти южного моста South Bridge запущена
0x1A	Предварительная инициализация памяти южного моста South Bridge (характерная для модуля South Bridge)
0x1B	Предварительная инициализация памяти южного моста South Bridge (характерная для модуля South Bridge)
0x1C	Предварительная инициализация памяти южного моста South Bridge (характерная для модуля South Bridge)
0x1D – 0x2A	Коды предварительной инициализации OEM-памяти
0x2B	Инициализация памяти. Считывание данных SPD (Serial Presence Detect)
0x2C	Инициализация памяти. Обнаружение присутствия памяти.
0x2D	Инициализация памяти. Программирование таймингов памяти.
0x2E	Инициализация памяти. Конфигурация памяти.
0x2F	Инициализация памяти (другое).
0x30	Зарезервировано для ASL (см. раздел «Коды состояния ASL» ниже).
0x31	Память установлена.
0x32	Запущена инициализация процессора после ввода памяти (CPU post-memory инициализация).

0x33	CPU post-memory инициализация. Инициализация кэша.
0x34	CPU post-memory инициализация. Инициализация прикладных процессоров Application Processor(s) (AP)
0x35	CPU post-memory инициализация. Выбор процессора загрузки Boot Strap Processor (BSP)
0x36	CPU post-memory инициализация. Инициализация режима управления системой System Management Mode (SMM)
0x37	Запущена инициализация северного моста North Bridge после ввода памяти (Post-Memory North Bridge инициализация).
0x38	Post-Memory North Bridge инициализация (характерная для North Bridge модуля).
0x39	Post-Memory North Bridge инициализация (характерная для North Bridge модуля).
0x3A	Post-Memory North Bridge инициализация (характерная для North Bridge модуля).
0x3B	Запущена инициализация южного моста South Bridge после ввода памяти (Post-Memory South Bridge инициализация).
0x3C	Post-Memory South Bridge инициализация (характерная для South Bridge модуля).
0x3D	Post-Memory South Bridge инициализация (характерная для South Bridge модуля).
0x3E	Post-Memory South Bridge инициализация (характерная для South Bridge модуля).
0x3F-0x4E	Коды инициализации после ввода OEM-памяти.
0x4F	Процедура DXE IPL запущена
Коды ошибок PEI Error Codes	
0x50	Ошибка инициализации памяти. Недопустимый тип памяти или несовместимая скорость памяти.
0x51	Ошибка инициализации памяти. Сбой чтения SPD.
0x52	Ошибка инициализации памяти. Неверный размер памяти или модули памяти не совпадают.
0x53	Ошибка инициализации памяти. Полезная память не обнаружена.
0x54	Неизвестная ошибка инициализации памяти.
0x55	Память не установлена.
0x56	Недопустимый тип процессора CPU или скорость процессора CPU.
0x57	Несоответствие процессора CPU.
0x58	Не удалось выполнить самопроверку процессора CPU или возможная ошибка кэша процессора
0x59	Микрокоды процессора CPU не найдены или обновление микрокодов не выполнено
0x5A	Внутренняя ошибка процессора CPU.
0x5B	Переустановка PPI невозможна.
0x5C	Отказ самотестирования BMC фазы PEI.
0x5C-0x5F	Зарезервировано под коды будущих ошибок АКВАРИУС.
Коды состояний S3 Resume Progress Codes	
0xE0	S3 Resume запускается (S3 Resume PPI вызывается DXE IPL).
0xE1	Выполнение сценария загрузки S3 Boot Script,
0xE2	Видеорепост

0xE3	Вызов программы пробуждения OS S3 Wake vector.
0xE4-0xE7	Зарезервировано по коды будущих состояний АКВАРИУС.
Коды ошибок S3 Resume Error Codes	
0xE8	Процесс S3 Resume не выполнен.
0xE9	S3 Resume PPI не найден.
0xEA	Ошибка сценария загрузки S3 Resume Boot Script.
0xEB	Ошибка программы пробуждения S3 OS Wake
0xEC-0xEF	Зарезервировано под коды будущих ошибок АКВАРИУС.
Коды состояний восстановления Recovery Progress Codes	
0xF0	Состояние восстановления, инициируемое микропрограммным обеспечением (Auto recovery – автоматическое восстановление)
0xF1	Состояние восстановления, инициируемое пользователем (Forced recovery – принудительное восстановление)
0xF2	Процесс восстановления Recovery process запущен.
0xF3	Образ микропрограммы автоматического восстановления Recovery firmware найден
0xF4	Образ микропрограммы автоматического восстановления Recovery firmware загружен.
0xF5-0xF7	Зарезервировано под коды будущих состояний АКВАРИУС.
Коды ошибок восстановления Recovery Error Codes.	
0xF8	Процесс Recovery PPI недоступен.
0xF9	Программа восстановления Recovery capsule не найдена.
0xFA	Недопустимая программа восстановления: Invalid recovery capsule.
0xFB – 0xFF	Зарезервировано под коды будущих ошибок АКВАРИУС.

Звуковые коды PEI Beep Codes

№ кода	**Описание**
1	Память не установлена.
2	Восстановление Recovery запущено.
3	Как правило, для разработчиков: звуковой код генерируется, когда не найдены DXE IPL PPI или ядро DXE Core.
4	Сбой восстановления Recovery.
4	Сбой S3 Resume.
7	Как правило, для разработчиков: звуковой код генерируется, когда платформа не может быть переустановлена ввиду недоступности переустановки PPI.

Фаза DXE.

Код состояния Status Code (16-ричный)	**Описание**
0x60	Ядро DXE Core запущено.
0x61	Инициализация NVRAM.
0x62	Инсталляция временных сервисов южного моста South Bridge Runtime Services.

0x63	Запущена инициализация CPU DXE.
0x64	Инициализация CPU DXE (характерная для модуля CPU).
0x65	Инициализация CPU DXE (характерная для модуля CPU).
0x66	Инициализация CPU DXE (характерная для модуля CPU).
0x67	Инициализация CPU DXE (характерная для модуля CPU).
0x68	Инициализация хост-моста PCI host bridge.
0x69	Запущена инициализация North Bridge DXE (DXE северного моста).
0x6A	Запущена инициализация North Bridge DXE SMM.
0x6B	Инициализация North Bridge (характерная для модуля северного моста North Bridge).
0x6C	Инициализация North Bridge (характерная для модуля северного моста North Bridge).
0x6D	Инициализация North Bridge (характерная для модуля северного моста North Bridge).
0x6E	Инициализация North Bridge (характерная для модуля северного моста North Bridge).
0x6F	Инициализация North Bridge (характерная для модуля северного моста North Bridge).
0x70	Запущена инициализация South Bridge DXE (DXE южного моста).
0x71	Запущена инициализация South Bridge DXE SMM.
0x72	Инициализация устройств South Bridge.
0x73	Инициализация South Bridge (характерная для модуля южного моста North Bridge).
0x74	Инициализация South Bridge (характерная для модуля южного моста North Bridge).
0x75	Инициализация South Bridge (характерная для модуля южного моста North Bridge).
0x76	Инициализация South Bridge (характерная для модуля южного моста North Bridge).
0x77	Инициализация South Bridge (характерная для модуля южного моста North Bridge).
0x78	Инициализация модуля ACPI.
0x79	Инициализация CSM.
0x7A – 0x7F	Зарезервировано под будущие коды АКВАРИУС DXE.
0x80 – 0x8F	Коды инициализации OEM DXE.
0x90	Фаза Boot Device Selection (BDS) запущена.
0x91	Подключение драйвера запущено.
0x92	Инициализация шины PCI Bus запущена.
0x93	Инициализация контроллера горячей замены PCI Bus Hot Plug Controller.
0x94	Перечисление шин PCI Bus.
0x95	Запрос ресурсов PCI Bus.
0x96	Назначение ресурсов PCI Bus.
0x97	Подключение устройств вывода консоли.
0x98	Подключение устройств ввода консоли.
0x99	Супер-инициализация ввода/вывода (Super IO initialization).
0x9A	Инициализация USB запущена.
0x9B	Переустановка USB.
0x9C	Обнаружение USB.
0x9D	Включение USB.
0x9E – 0x9F	Зарезервировано под будущие коды АКВАРИУС.

0xA0	Инициализация IDE запущена.
0xA1	Переустановка IDE.
0xA2	Обнаружение IDE.
0xA3	Включение IDE.
0xA4	Инициализация SCSI запущена.
0xA5	Переустановка SCSI.
0xA6	Обнаружение SCSI.
0xA7	Включение SCSI.
0xA8	Пароль проверки установки.
0xA9	Старт установки.
0xAA	Зарезервировано для ASL (см. раздел «Коды состояния ASL» ниже)
0xAB	Ожидание ввода установки Setup Input.
0xAC	Зарезервировано для ASL (см. раздел «Коды состояния ASL» ниже)
0xAD	Событие Ready to Boot (готов к загрузке).
0xAE	Событие Legacy Boot (унаследованная загрузка).
0xAF	Событие Exit Boot Services (выход из служб загрузки).
0xB0	Начало времени выполнения Runtime Set Virtual Address MAP.
0XB1	Конец времени выполнения Runtime Set Virtual Address MAP.
0xB2	Унаследованный вариант инициализации ROM.
0xB3	Переустановка системы.
0xB4	Горячая установка USB.
0xB5	Горячая установка PCI bus.
0xB6	Очистка NVRAM.
0xB7	Переустановка конфигурации (переустановка настроек NVRAM).
0xB8 – 0xBF	Зарезервировано под будущие коды АКВАРИУС.
0xC0 – 0xCF	Коды инициализации OEM BDS.
Коды ошибок DXE Error Codes	
0xD0	Ошибка инициализации процессора CPU
0xD1	Ошибка инициализации северного моста North Bridge
0xD2	Ошибка инициализации южного моста South Bridge
0xD3	Некоторые архитектурные протоколы недоступны
0xD4	Ошибка выделения ресурсов PCI. Недостаточно ресурсов.
0xD5	Недостаточно места для унаследованной версии ROM.
0xD6	Устройства вывода консоли не найдены.
0xD7	Устройства ввода консоли не найдены.
0xD8	Неверный пароль.
0xD9	Ошибка загрузки Boot Option (возвращена ошибка LoadImage)
0xDA	Не удалось выполнить Boot Option (возвращена ошибка StartImage)
0xDB	Сбой обновления флэш-памяти.
0xDC	Протокол переустановки Reset недоступен.

0xDD	Отказ самотестирования BMC фазы DXE

Звуковые коды DXE.

№ кода	Описание
1	Неверный пароль.
4	Как правило, для разработчиков: звуковой код генерируется, когда некоторые архитектурные протоколы недоступны.
5	Устройства ввода или вывода консоли не найдены [1,2]
6	Сбой обновления флэш-памяти.
7	Как правило, для разработчиков: звуковой код генерируется, когда платформа не может быть переустановлена ввиду недоступности протоколов переустановки..
8	Требования к ресурсам PCI платформы не могут быть выполнены.

[1] *Замечание – последовательное перенаправление консоли считается устройством выхода консоли, если оно подключено.*

[2] *Замечание – последовательное перенаправление консоли считается устройством входа консоли, если оно подключено. Также в зависимости от конфигурации PS/2 драйвер может сообщить о наличии устройства входа консоли, если оно не подключено.*

Контрольные точки ACPI/ASL.

Код состояния Status Code (16-ричный)	Описание
0x01	Система входит в спящий режим S1.
0x02	Система входит в спящий режим S2.
0x03	Система входит в спящий режим S3.
0x04	Система входит в спящий режим S4.
0x05	Система входит в спящий режим S5.
0x10	Система выходит (просыпается) из спящего режима S1.
0x20	Система выходит (просыпается) из спящего режима S2.
0x30	Система выходит (просыпается) из спящего режима S3.
0x40	Система выходит (просыпается) из спящего режима S4.
0xAC	Система перешла в режим ACPI. Контроллер прерываний находится в режиме PIC.
0xAA	Система перешла в режим ACPI. Контроллер прерываний находится в режиме APIC.

OEM-зарезервированные диапазоны контрольных точек

Код состояния Status Code (16-ричный)	Описание
0x05	Инициализация OEM SEC перед загрузкой микрокода
0x0A	Инициализация OEM SEC после загрузки микрокода
0x1D – 0x2A	Коды инициализации памяти OEM post memory

0x3F – 0x4E	Коды инициализации памяти OEM PEI pre-memory
0x80 – 0x8F	Коды инициализации OEM DXE.
0xC0 – 0xCF	Коды инициализации OEM BDS.

ПЕРЕЧЕНЬ ТЕРМИНОВ

Чипсет — Набор микросхем

ACM — Authenticated Code Modules (ACM), модуль аутентифицированного кода: модули ACM создаются только корпорацией Intel и функционируют при наличии закрытого ключа, известного только Intel. Открытый ключ встраивается в аппаратные регистры набора микросхем, но выполняется только модуль с соответствующим закрытым ключом. Модули ACM вызываются микрокодом Intel и функционируют как расширения микрокода. Для серверной доверенной платформы Intel Trusted Execution Technology (Intel TXT) существует два модуля ACM:

- BIOS ACM
- SINIT ACM

ACPI — Advanced Configuration and Power Interface, стандарт (спецификация), определяющий способы программного управления электропитанием компонентов компьютера посредством встроенных средств операционной системы.

APM — Advanced Power Management, набор функций, позволяющий ПО управлять энергопотреблением устройств компьютера. Спецификация APM реализована на уровне БСВВ (BIOS), т.е. BIOS практически полностью управляет энергопотреблением и определяет состояния устройств компьютера.

BBS — BIOS Boot Specification, функция BIOS, которая создает, поддерживает и устанавливает приоритеты для всех устройств начальной загрузки программы IPL (Initial Program Load). Пока компьютер загружается, каждое устройство IPL проверяется на возможность загрузки.

BBS означает спецификацию загрузки BIOS, представляет собой стандартизированный процесс загрузки, который предписывает программе БСВВ (BIOS) идентифицировать и предоставлять приоритеты начальной программной загрузки IPL (Initial Program Load) устройств в компьютере, и позволяет выбрать конкретное загрузочное устройство для загрузки.

BIOS или БСВВ — Basic Input/Output System, базовая система ввода-вывода

BIOS ACM — BIOS ACM содержит несколько подфункций (вызовов), две из которых:

- Startup ACM при запуске вызывается микрокодом CPU при включении для запуска SRTM. Обычно выполняет загрузочный блок BIOS boot block или, как принято называть в UEFI, фазы SEC BIOS и PEI BIOS.
- Вызов Lock Config производится BIOS непосредственно перед выходом из выполненной Startup ACM части BIOS. При этом выполняется некие вычисления и блокируются некие регистры, для

предотвращения изменений критических параметров оборудования вредоносным ПО или микропрограммным обеспечением.

BMC — Baseboard Management Controller, контроллер управления системной платой, специализированный служебный процессор, который отслеживает физическое состояние компьютера, сетевого сервера или другого аппаратного устройства с помощью датчиков. Системный администратор связывается с BMC через независимое соединение.
BMC является частью интеллектуального интерфейса управления платформой (IPMI), обычно находится на системной плате или основной плате контролируемого устройства.

Boot Sequences — последовательность загрузки.

CMOS — энергонезависимая память БСВВ (BIOS) компьютера.

Cold Boot — холодная загрузка, если при запуске компьютер был выключенным, или холодным

COM-порт — последовательный порт (Communications Port), информация через который передаётся по одному биту, последовательно бит за битом.

CRTM — Core Root of Trust for Measurements, корень доверия ядра для измерений; первое, что выполняется при загрузке, иначе загрузочный блок BIOS измерит BIOS и отправит значение (хэш) в TPM в место, называемое регистром конфигураций платформы (PCR); 0 перед его выполнением.

CSM Legacy — CSM позволяет выполнять загрузку в устаревшем (Legacy) режиме БСВВ (BIOS) в системах UEFI. Модуль поддержки совместимости (CSM) является компонентом встроенного ПО UEFI, обеспечивающим совместимость с устаревшей BIOS путем эмуляции среды BIOS, что позволяет использовать устаревшие операционные системы и некоторые дополнительные ПЗУ, не поддерживающие UEFI.

DMA — Direct Memory Access, прямой доступ к памяти, особенность компьютерных систем, позволяющая некоторым аппаратным подсистемам получать доступ к основной системной памяти независимо от центрального процессора.

DMI — Desktop Management Interface, интерфейс управления настольными компьютерными системами. Служит для сбора информации о составе и работе компьютеров сети с целью накопления статистики или ведения базы данных по компьютерам в организации. Поддержка DMI может быть также встроена в системный БСВВ (BIOS), что облегчает для ОС отслеживание изменений в аппаратной конфигурации компьютера.

DMTF SMASH CLP — DMTF SMASH Command Line Protocol, дружественный пользователю командный протокол, разработанный рабочей группой Distributed Management Task Force (DMTF), поддерживающий простое и интуитивное управление серверами. SMASH CLP содержит спецификацию, определяющую пары запросов и ответов, которые передаются и принимаются в виде текстовых сообщений поверх какого-либо транспортного протокола.

Задача SMASH состоит в унификации взаимодействия с системами различных производителей.

DRAM — Dynamic Random Access Memory, тип компьютерной памяти, отличающийся использованием полупроводниковых материалов, энергозависимостью и возможностью доступа к данным, хранящимся в произвольных ячейках памяти. DRAM некорректно называют системной памятью, но она - память центрального процессора CPU, т.к. является основным накопителем рабочих данных и команд процессора. DRAM находится на небольших платах, вставляемых в системную (основную) плату устройства.

DRTM — Dynamic Root of Trust for Measurements, динамический корень доверия для измерения (с целью определения неавторизированного ПО).

Измерение целостности системы происходит во время работы системы. Реализация в Intel называется Trusted Execution Technology (TXT), тогда как AMD использует имя Secure Virtual Machine (SVM). Целью DRTM является создание доверенной среды. Технически DRTM создает безопасное/чистое состояние из ненадежного и далее сообщает (предоставляет) измерения - хэши в PCR на выполняемой части кода (или в измеренной запущенной среде – MLE, Measured Launched Environment). Как правило, MLE является операционной системой (ядро, пользовательское пространство и т.д.).

Технология Intel DRTM работает, вызывая набор новых команд CPU (SMX), предписывающих CPU и набору микросхем выполнять конкретный набор задач (GETSEC), обеспечивающих выполнение только специального кода, т.е. модуля аутентифицированного кода SINIT ACM. Эта часть включает в себя отключение всех ЦП, кроме одного, и блокирование/остановку всех текущих процессов, прерываний и операций ввода-вывода (через IOMMU, например, во избежание атак DMA). Затем все ЦП снова присоединяются в чистом состоянии (все, что выполнялось до этого, отбрасывается). В этот момент подпись этого специального кода (SINIT ACM) проверяется, и его значение (хэш-измерение) посылается в TPM в PCR 17. После этого выполнение передается в ACM, который затем измеряет MLE и посылает измерение в TPM в PCR 18. Затем выполнение передается в MLE.

EFI Shell — UEFI Shell, инструмент управления загрузкой вручную, принудительная загрузка.

Error Log — журнал ошибок; персонализированный документ, в котором перечислены ошибки и способы их исправления. При получении отзыва об ошибке создается запись в журнале ошибок, включающая ошибку и способы ее исправления.

FRB — Fault Resilient Booting, отказоустойчивая загрузка. В контроллере BMC используется отказоустойчивая загрузка (FRB) уровней 1, 2 и 3. Если установленный по умолчанию загрузочный процессор BSP (Boot Start Up Processor) не завершает загрузку, то FRB пытается загрузиться с использованием другого процессора.

- уровень FRB1 предназначен для восстановления работы при обнаружении ошибки автоматического тестирования загрузочного процессора (BIST) во время процедуры POST. Восстановление FRB полностью реализовано кодом BIOS;
- уровень FRB2 - загрузка при наличии ошибки с «эластичной» конфигурацией, выделяется из времени ожидания схемы обеспечения безопасности во время процесса POST (самотестирования после включения питания). Сторожевой таймер для уровня 2 FRB внедряется в модуль BMC;
- уровень FRB3 предназначен для восстановления работы в случае, несрабатывания контрольного таймера во время аппаратной перезагрузки или включения системы, что обеспечивает надлежащее функционирование оборудования на этом уровне FRB.

FRU — Field Replaceable Unit, хранилище сменных устройств, хранит данные о потенциально заменяемых устройствах, таких как идентификатор поставщика и производитель. Хранилище записей данных датчиков (SDR) сохраняет свойства отдельных датчиков, имеющихся на плате.

IDE/ATA — Advanced Technology Attachment или IDE (Integrated Drive Electronics), параллельный интерфейс подключения накопителей (гибких дисков, жёстких дисков и оптических дисководов) к компьютеру.

IOMMU — Input/Output Memory Management Unit, технология виртуализации ввода-вывода. Компании AMD и Intel выпустили свои спецификации IOMMU:

- AMD-Vi
- VT-d

Технология AMD-Vi, первое название IOMMU, где IOMMU - модуль управления памятью ввода/вывода, позволяющий гостевым виртуальным машинам напрямую использовать периферийные устройства, такие как Ethernet, графические карты и контроллеры жестких дисков, посредством прямого доступа к основной системной памяти (DMA-Direct Memory Access) и повторного отображения прерываний.

Технология Intel®Virtualization for Directed I/O (VT-d) включена в большинство (но не во все) процессоров Intel, начиная с двухъядерной архитектуры Core 2.

IPC — Inter-Process Communication, межпроцессное взаимодействие, обмен данными между потоками одного или разных процессов. Реализуется посредством механизмов, предоставляемых ядром ОС или процессом, использующим механизмы ОС, и реализующим новые возможности IPC. Может осуществляться как на одном компьютере, так и между несколькими компьютерами сети.

Из механизмов, предоставляемых ОС и используемых для IPC, можно выделить:

- механизмы обмена сообщениями;
- механизмы синхронизации;

- механизмы разделения памяти;
- механизмы удаленных вызовов (RPC).

Для оценки производительности различных механизмов IPC используют следующие параметры:

- пропускная способность (количество сообщений в единицу времени, которое ядро ОС или процесс способны обработать);
- задержки (время между отправкой сообщения одним потоком и его получением другим потоком).

IPC может также называться межпотоковым взаимодействием (Inter-Thread Communication) и межпрограммным взаимодействие (Inter-Application Communication).

IPMI — Platform Management Interface, интеллектуальный интерфейс управления платформой. Через IPMI можно удаленно подключиться к серверу и управлять его работой, а именно:

- проводить мониторинг физического состояния оборудования (проверять температуру отдельных составляющих системы, уровни напряжения, скорость вращения вентиляторов);
- восстанавливать работоспособность сервера в автоматическом или ручном режиме (удаленная перезагрузка системы, включение/выключение питания, загрузка ISO-образов и обновление программного обеспечения);
- управлять периферийными устройствами;
- вести журнал событий;
- хранить информацию об используемом оборудовании

GPT — таблица разделов GUID (GUID Partition Table), являющаяся стандартом для компоновки таблиц разделов физического компьютерного устройства хранения данных, такого как жесткий диск или твердотельный накопитель, использующих универсальные уникальные идентификаторы, также известные как глобальные уникальные идентификаторы (GUID). Являясь частью стандарта Unified Extensible Firmware Interface (UEFI, развитие PC BIOS), GPT, тем не менее, используется для некоторых систем BIOS, которые, из-за ограничений таблиц разделов Master Boot Record (MBR), используют 32 бита для логической блочной адресации (LBA) традиционных 512-байтовых дисковых секторов.

EFI использует GPT там, где BIOS использует MBR.

HBA — плата расширения, хост-адаптер шины, host bus adapter; также host channel adapter (HCA), хост-адаптер канала или просто host adapter; вид комплектующих: плата адаптера, устанавливаемая в компьютер и служащая для подключения накопителей (устройств хранения информации) или сети, имеющих в качестве интерфейса шинную организацию, отличную от имеющихся в компьютере изначально.

H/W Monitor — Hardware Monitor, комплекс программно-аппаратных средств диагностики, встроенный в системную плату компьютера, тесно связанный с БСВВ (BIOS).

Hardware Monitor позволяет измерить и вывести на экран монитора:

- величину питающих напряжений блока питания,
- величину напряжения питания ядра процессора,
- величину напряжения литиевого элемента,
- температуру процессора и, возможно, системной платы (или окружающего воздуха),
- величину оборотов вентилятора процессора (возможно, также других вентиляторов).

KVM/IP KVM over IP — Keyboard (клавиатура), Video (видео), Mouse (мышь); устройство, позволяющее передавать от сервера видеосигнал и ввод с мыши/клавиатуры по сети с использованием IP-протокола.

LPT-порт — Line Print Terminal, параллельный порт, порт принтера, международный стандарт параллельного интерфейса для подключения периферийных устройств компьютера.

MBR — Master Boot Record, главная загрузочная запись, код и данные, необходимые для последующей загрузки операционной системы и расположенные в первых физических секторах (чаще всего в самом первом) на жестком диске или другом устройстве хранения информации.

MBR содержит небольшой фрагмент исполняемого кода, таблицу разделов диска (Partition Table) и специальную сигнатуру.

Функция MBR — переход в тот раздел жесткого диска, с которого следует исполнять дальнейший код (загружать ОС). На стадии MBR происходит выбор раздела диска, загрузка кода операционной системы.

В процессе запуска компьютера после окончания начального теста POST (Power-On Self-Test) БСВВ (BIOS) загружает код MBR в оперативную память и передаёт управление находящемуся в MBR загрузочному коду

ME — Management Engine, автономная подсистема, встроенная почти во все чипсеты процессоров Intel с 2008 г. Она состоит из проприетарной прошивки, исполняемой отдельным микропроцессором. Т.к. чипсет всегда подключен к источнику тока (батарейке или другому источнику питания), эта подсистема продолжает работать даже при отключенном компьютере. ME необходима для обеспечения максимальной производительности. Сама прошивка не содержит информации для своего раскодирования. Компания AMD также встраивает в свои процессоры аналогичную систему AMD Secure Technology (ранее – Platform Security Processor), начиная с 2013 г.

MLE Measured Launched Environment, измеренная запущенная среда.

Как правило, MLE является операционной системой (ядро, пользовательское пространство и т.п.).

MRC — эталонный (референсный) код памяти; часть встроенного ПО системной платы на базе чипсета Intel, которая определяет, как в оперативной

памяти компьютера будут проходить процедуры записи и чтения информации с учетом эффектов любых модификаций, установленных пользователем или компьютерным оборудованием.

MRC отвечает за инициализацию памяти как часть постпроцесса (POST) после включения питания компьютера, при его загрузке. Физически MRC является частью BIOS (UEFI) системной платы на чипсете Intel.

OEM — Original Equipment Manufacturer, производитель оригинального оборудования. Здесь имеются ввиду ключи OEM, которые программируются на компьютере. Эти ключи встроенного продукта хранятся в памяти NVRAM BIOS/EFI на системной плате. Они позволяют пользователю переустановить операционную систему на этот компьютер любое количество раз.

PCH — Platform Controller Hub, элемент системной логики производства Intel, который управляет работой основных структур системной платы, выполняет роль южного моста (поскольку функции северного моста переместились в процессор).

PCH управляет определенными путями передачи данных и функциями поддержки, используемыми совместно с процессорами Intel. К ним относятся часы (системные часы), интерфейс гибкого дисплея (FDI – Flexible Display Interface) и интерфейс прямого мультимедиа (DMI – Direct Media Interface), хотя FDI используется только когда набор микросхем необходим для поддержки процессора со встроенной графикой.

PCI — Peripheral Component Interconnect, взаимосвязь периферийных компонентов, шина ввода/вывода для подключения периферийных устройств к системной плате компьютера.

Plug and Play — PnP, подключи и играй (работай); технология, предназначенная для быстрого определения и конфигурирования устройств в компьютере и других устройствах. В зависимости от аппаратного интерфейса и программной платформы (ОС, BIOS) процедура Plug and Play может производиться на этапе начальной загрузки системы или в режиме горячей замены.

PM — Power Management, управление электропитанием, позволяет экономить электроэнергию.

POST Power-On Self-Test – тест подачи электропитания.

PTT — Intel Platform Trust Technology, технология Intel PTT, платформа для хранения учетных данных и управления ключами, используемая в Windows 8, Windows®10 и Windows 11. Технология Intel PTT поддерживает BitLocker для шифрования жестких дисков и все требования Microsoft для встроенного программного обеспечения Trusted Platform Module (fTPM) 2.0.

PXE — Preboot Execution Environment, среда выполнения предзагрузки, которая запускает операционную систему с помощью сети.

RAID — Redundant Array of Independent Disks — массив независимых (с возможностью нахождения и исправления ошибок при записи, воспроизведении

и передаче данных) дисков; технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и/или производительности.

RAMDISK — технология для выделения части оперативной памяти с целью использования в качестве виртуального хранилища. Преимущество использования технологии: скорость оперативной памяти становится значительно быстрее.

RC —Release Candidate, версия потенциально готовая быть конечным продуктом, готовая к выпуску, если не появятся фатальные ошибки,
или версия на том этапе процесса разработки, когда она готова для оценки пользователями, пока проходит окончательное тестирование.

ROM — Read-Only-Memory, постоянное запоминающее устройство (ПЗУ), основная память компьютера.

SAS — Serial-Attached SCSI, последовательный компьютерный интерфейс для подключения различных устройств хранения данных.

Secure Boot— безопасная загрузка; протокол, являющийся частью спецификации UEFI, не является обязательным для реализации производителями.

Server Mgmt — управление серверами, процесс мониторинга и обслуживания серверов в сети для обеспечения максимальной производительности. Управление серверами также включает управление оборудованием, программным обеспечением, безопасностью и резервным копированием

SINIT ACM — модуль аутентифицированного кода.
Эта часть включает в себя отключение всех ЦП, кроме одного, и блокирование/остановку всех текущих процессов, прерываний и операций ввода/вывода (через IOMMU, например, во избежание атак DMA). Затем все ЦП снова присоединяются в чистом состоянии (все, что выполнялось до этого, отбрасывается). В такой момент подпись этого специального кода (SINIT ACM) проверяется, и его значение (хэш-измерение) посылается в TPM в PCR 17. После проверки и пересылки выполнение передается в ACM, который измеряет среду MLE (Measured Launched Environment) и посылает измерение в TPM в PCR 18. Наконец, выполнение передается в MLE.
Tboot - инструмент, созданный Intel для этого измерения целостности системы (DRTM) и являющийся альтернативой TrustedGrub (SRTM).

SLP или OEM:SLP — Original Equipment Manufacturer:System Locked Pre-Installation, ключи, предустановленные производителями компьютеров. Данные, включенные в BIOS (так называемая таблица SLIC 2.1), используются для проверки OEM:SLP-ключа. Для активации в том числе необходим файл сертификата производителя компьютеров. OEM:SLP-ключи устанавливаются на любую систему OEM:SLP независимо от бренда производителя. Для активации не требуется подключение к Интернету.

SMBIOS — System Management BIOS, системное управление BIOS, определяет структуру данных (метод доступа) в BIOS, позволяющую пользователю

или приложению сохранять и извлекать информацию, специфичную для данного компьютера.

SoL — Serial on LAN, последовательный порт по локальной сети, механизм, который позволяет перенаправлять ввод и вывод последовательного порта управляемой системы через IP.

В некоторых управляемых системах, особенно в системах блейд-серверов, последовательные порты на управляемых компьютерах обычно не подключаются к традиционному сокету последовательного порта.

SRTM — Static Root of Trust for Measurement, статический корень доверия для измерения (с целью определения неавторизированного ПО).

Функция безопасной загрузки Secure Boot UEFI использует доверенный платформенный модуль (TPM) для выполнения безопасных измерений каждой части встроенного (hardware) или программного (software) обеспечения в процессе ранней загрузки. Такой метод измерения этих UEFI-компонентов статической ранней загрузки называется статическим корнем доверия для измерения (SRTM).

SRTM выполняется при загрузке системы. Первое, что выполняется при загрузке, называется корнем доверия ядра для измерений (CRTM), иначе загрузочный блок BIOS измерит BIOS и отправит значение (хэш) в TPM в месте, называемом регистром конфигураций платформы (PCR), 0 перед его выполнением.

Затем BIOS измеряет следующую компоненту в цепочке загрузки и снова сохраняет значение в PCR доверенного платформенного модуля TPM. Этот процесс выполняется для каждого компонента в последовательности загрузки (дополнительная память PCI, загрузчик и т.д.)

Ввиду существования многочисленных моделей с различными версиями BIOS UEFI при запуске появляется большое количество измерений SRTM. Существует два метода, которые могут быть использованы для установления доверия - либо ведение списка известных «плохих» измерений SRTM (список блоков), либо список известных «хороших» измерений SRTM (список разрешений). Каждый вариант имеет свои недостатки:

- список известных «плохих» измерений SRTM позволяет при несанкционированном доступе изменить только 1 бит в компоненте, чтобы создать совершенно новый хэш SRTM. Это означает, что поток SRTM хрупок - незначительное изменение может аннулировать цепочку доверия;
- список известных «хороших» измерений SRTM требует корректного добавления каждого нового измерения комбинации BIOS/PC, что замедляет процесс. Кроме того, исправление ошибки для кода UEFI может занять также много времени при проектировании, построении, повторном тестировании, проверке и повторном развертывании.

SSH — Secure Shell, протокол сетевой связи, позволяющий двум компьютерам обмениваться данными (протокол передачи гипертекста, такого как веб-страницы)

Startup Screen — экран запуска.

SVGA — Super Video Graphics Array, спецификация (необязательное требование) к видеоадаптерам и тип современных видеоадаптеров, совместимых по графическим режимам с VGA, но дополнительно имеющих новые возможности:

- разрешение 800×600 точек и выше;
- количество цветов до 65536 и 16 млн. (24 бита на пиксель);
- увеличенные объемы видеопамяти от 1Мб и больше для поддержки новых графических режимов.

TBOOT — Trusted Boot**,** модуль предварительного ядра/VMM (prekernel/VMM module) с открытым исходным кодом, использующий технологию Intel (R)Trusted Execution Technology (Intel (R) TXT) для выполнения измеренного и проверенного запуска ядра или операционной системы VMM.

Thunderbolt—универсальный порт, который соединяет компьютер пользователя с любой другой док-станцией, дисплеем и устройством передачи данных при зарядке компьютера; все через один откидной, реверсивный кабель. Технология Thunderbolt совместима с продуктами USB 3 и USB4.

В режиме поддержки BIOS предварительно распределяет ресурсы, включая PCIe и ресурсы памяти, при использовании операционной системой для обработки добавления и удаления устройств Thunderbolt. Это гарантирует, что добавленные и удаленные устройства не окажут негативного влияния на производительность системы или работу пользователей.

TPM — Trusted Platform Module, доверенный платформенный модуль, выполняющий измерение целостности в системе и доверенные измерения каждой части встроенного аппаратного (hardware) или программного (software) обеспечения в процессе ранней загрузки.

Существуют 2 способа измерения целостности системы:

1. SRTM (Static Root of Trust for Measurements)
2. DRTM (Dynamic Root of Trust for Measurements).

Trusted Computing — это технология безопасности: специальная микросхема (чип) заботится чтобы программное обеспечение и компоненты компьютера были защищены от нелегальных манипуляций со стороны третьих лиц.

UEFI — Unified Extensible Firmware Interface, унифицированный расширяемый интерфейс микропрограмм, программное обеспечение низкого уровня, запускающееся при старте компьютера перед тем, как загрузится операционная система. UEFI – решение, поддерживающее жесткие диски большего объема, быстро грузится, более безопасно, обладает графическим интерфейсом, поддерживает мышь, позволяет проводить удаленную настройку и отладку. UEFI может храниться во флэш-памяти на

системной плате, загружаться с жесткого диска или общего сетевого ресурса. Разные компьютеры с UEFI будут иметь разные интерфейсы и функции.

UPI — Ultra Path Interconnect, шина, предназначенная для обеспечения взаимодействия между процессорами. Используется в серверных платформах на базе процессоров Intel.

Warm Boot — горячий запуск, процесс инициированный для перезагрузки системы нажатием клавиш Ctrl+Alt+Del.

Wtd Timer — Watchdog Timer, сторожевой таймер, контрольный таймер, аппаратно реализованная схема контроля над зависанием системы. Представляет собой таймер, который периодически сбрасывается контролируемой системой. Если сброса не произошло в течение какого-то интервала времени, происходит принудительная перезагрузка системы. В некоторых случаях сторожевой таймер может посылать системе сигнал на перезагрузку (мягкая перезагрузка), в других — перезагрузка происходит аппаратно (замыканием сигнального провода RST или т.п.). В большинстве случаев существуют специальные средства, позволяющие узнавать причину сброса: первый сброс при включении питания, аппаратный сброс кнопкой или сигналом, или это сработал сторожевой таймер. В некоторых процессорах сторожевой таймер вызывает не общий сброс, а прерывание.

Эмуляция (emulation) — комплекс программных, аппаратных средств, предназначенный для копирования (или эмулирования) функций одной вычислительной системы (гостя) на другую, вычислительную систему (хост) таким образом, чтобы эмулированные функции другой вычислительной системы соответствовали функциям оригинальной системы (гостя). Целью является максимально точное воспроизведение функций системы-гостя в отличие от разных форм компьютерного моделирования, в которых имитируется поведение некоторой абстрактной модели.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БСВВ – базовая система ввода-вывода, то же самое - BIOS (Basic Input/Output System)

ЕСКД – Единая система конструкторской документации

ЕСПД – Единая система программной документации

ЕСТД – Единая система технологической документации

КД – Конструкторская документация

ОЗУ – Оперативное запоминающее устройство

ОС – Операционная система

ПЗУ – Постоянное запоминающее устройство, память компьютера

ПО – Программное обеспечение

ЭВМ – Электронно-вычислительная машина

ЭД – Эксплуатационная документация

ARM – Advanced RISC Machines, архитектура процессора

DDR4 – Double-Data-Rate Four, четвертое поколение оперативной памяти

ECC – Error-Correcting Code Memory, память с коррекцией ошибок

HDMI – High Definition Multimedia Interface, интерфейс для мультимедиа высокой четкости

HDD – классический жёсткий диск, винчестер или HDD (Hard Disk Drive), привод жёстких дисков. Файлы в нём записываются на вращающихся магнитных дисках.

NVMe – Non-Volatile Memory Express, протокол доступа к твердотельным накопителям

OPAM – менеджер пакетов с открытым исходным кодом, редактируемый OCamlPro.

PCIe – Peripheral Component Interconnect Express, шина ввода/вывода для подключения периферийных устройств к системной плате

RAM Random Access Memory, оперативная память компьютера

SATA – Serial Advanced Technology Attachment, последовательный интерфейс обмена данными с накопителями информации

SCSI – Small Computer System Interface, набор стандартов для физического подключения и передачи данных между компьютерами и периферийными

устройствами. SCSI-стандарты определяют команды, протоколы и электрические и оптические интерфейсы. Разработан для объединения на одной шине различных по своему назначению устройств таких, как жёсткие диски, накопители на магнитооптических дисках, приводы CD, DVD, стримеры, сканеры, принтеры и т.д.

SDHC – Secure Digital High Capacity, формат карт памяти

SSD – Solid-State Drive, твердотельный накопитель

USB – Universal Serial Bus, последовательный интерфейс для подключения периферийных устройств к компьютеру

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

Обозначение документа	Наименование документа	Пункт
ГОСТ 8.417-2002	Государственная система обеспечения единства измерений. Единицы величин (с Поправками)	
ГОСТ 8.654-2016	Государственная система обеспечения единства измерений. Фотометрия. Термины и определения	
ГОСТ 15.016-2016	Система разработки и постановки продукции на производство. Техническое задание. Требования к содержанию и оформлению	
ГОСТ CISPR 24-2013	Совместимость технических средств электромагнитная. Оборудование информационных технологий. Устойчивость к электромагнитным помехам. Требования и методы испытаний (с Поправкой)	
ГОСТ 14192-96	Маркировка грузов (с Изменениями № 1, 2, 3)	
ГОСТ 14254-2015 (IEC 60529:2013)	Степени защиты, обеспечиваемые оболочками (Код IP) (Издание с Поправкой)	
ГОСТ 15150-69	Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды (с Изменениями № 1, 2, 3, 4, 5)	
ГОСТ 21552-84	Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение (с Изменениями № 1, 2, 3)	
ГОСТ 23216-78	Изделия электротехнические. Хранение, транспортирование, временная противокоррозионная защита, упаковка. Общие требования и методы испытаний (с Изменениями № 1, 2, 3)	
ГОСТ 28601.1-90	Система несущих конструкций серии 482,6 мм. Панели и стойки. Основные размеры	
ГОСТ 28601.2-90	Система несущих конструкций серии 482,6 мм. Шкафы и стоечные конструкции. Основные размеры	

Обозначение документа	Наименование документа	Пункт
ГОСТ 30631-99	ГОСТ 30631-99 Общие требования к машинам, приборам и другим техническим изделиям в части стойкости к механическим внешним воздействующим факторам при эксплуатации	
ГОСТ Р 8.563-2009	Государственная система обеспечения единства измерений (ГСИ). Методики (методы) измерений	
ГОСТ Р 8.568-2017	Государственная система обеспечения единства измерений. Аттестация испытательного оборудования. Основные положения	
ГОСТ Р 15.301-2016	Система разработки и постановки продукции на производство (СРПП). Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство	
ГОСТ Р ИСО 14021-2000	Этикетки и декларации экологические. Самодекларируемые экологические заявления (экологическая маркировка по типу II)	
ГОСТ 23945.0-80	Унификация изделий. Основные положения (с Изменением № 1)	
ГОСТ Р 51318.22-99 (СИСПР 22-97)	Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационных технологий. Нормы и методы испытаний (с Изменением № 1)	

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номер листов (страниц)				Всего листов (страниц) в докум.	Номер документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					