**Программное обеспечение**

**«Graviton Secure BIOS Boot»**

**Руководство пользователя**

**Содержание**

Введение 3

Принятые сокращения и обозначения 4

1. Ограничение текущей версии 5

2. Логика работы модулей 6

2.1. Модуль Graviton LogOn 6

2.2. Модуль Graviton NFC/RFID 6

3. Организационные меры 7

4. Порядок настройки работы модулей 8

4.1. Модуль Graviton LogOn 8

4.2. Модуль Graviton NFC/RFID 10

5. Порядок аутентификации пользователя 12

5.1. Аутентификация с помощью ключа на USB-носителе 12

5.2. Аутентификация с помощью карты и NFC/RFID считывателя 12

6. Сброс настроек модулей 13

**Введение**

Настоящий документ предназначен для ознакомления пользователя с программным обеспечением «Graviton Secure BIOS Boot», информацией о его назначении, функциональных особенностях и работе.

Программное обеспечение «Graviton Secure BIOS Boot» – это программно-аппаратный комплекс авторизации пользователя по электронным ключам для запуска системы, российский модуль базовой системы ввода-вывода (BIOS), разработанный в соответствии со спецификацией UEFI для моноблоков, ноутбуков, компьютеров, серверов и программно-аппаратных комплексов «Гравитон».

Программное обеспечение поставляется комплектно в составе платформ «Гравитон».

Данное руководство ориентировано на пользователей, ознакомившихся с документаций на BIOS, обладающих опытом настройки и эксплуатации BIOS.

**Принятые сокращения и обозначения**

| *BIOS* | – | Basic Input/Output System, набор микропрограмм для работы с аппаратурой компьютера и подключенными к нему устройствами |
| --- | --- | --- |
| *Graviton USB Key* | – | USB-накопитель, хранящий пароль согласно спецификации шифрования Graviton |
| *NFC* | – | Near Field Communication, технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров |
| *RFID* | – | Radio Frequency IDentification, способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках |
| *UEFI* | – | Unified Extensible Firmware Interface, унифицированный расширяемый микропрограммный интерфейс между операционной системой и программным обеспечением, управляющим низко-уровневыми функциями оборудования |
| *USB* | – | Universal Serial Bus, последовательный интерфейс для подключения периферийных устройств к вычислительной технике |

1. **Ограничение текущей версии**

В текущей версии программного обеспечения имеются следующие ограничения:

поддерживаются только 64-битные сборки BIOS;

для работы с NFC/RFID поддерживается только считыватель типа PN532;

типы подключений PN532 ограничены последовательным портом;

аутентификация с использованием метода NFC/RFID доступна только через стандартные методы защиты BIOS;

с NFC/RFID меток считывается только серийный номер.

Модуль не защищает систему от непосредственного физического вмешательства. Все настройки модулей будут аннулированы при сбросе настроек BIOS Setup (например, через извлечение батарейки из материнской платы).

1. **Логика работы модулей**

Программное обеспечение «Graviton Secure BIOS Boot» имеет в своем составе два функциональных модуля:

Graviton LogOn (для аутентификации пользователя с помощью Graviton USB Key);

Graviton NFC/RFID (для аутентификации пользователя с помощью поднесения карты к считывателю).

* 1. **Модуль Graviton LogOn**

Во время одной из фаз загрузок встроенного программного обеспечения (DXE) проверяется наличие Graviton USB Key и корректность ключа, записанного на нем. В случае, если пароли, хранящиеся на Graviton USB Key и в системе, совпадают, то модуль позволяет продолжить загрузку в обычном режиме. В противном случае, загрузка будет прервана и не позволит войти ни в меню настройки BIOS Setup, ни в операционную систему. Вышеописанные действия актуальны только при включенном режиме модуля.

Также модуль предоставляет возможность сформировать и записать ключ для авторизации для USB-носителя(-ей) Graviton USB Key(s), используя меню BIOS Setup. Ключ записывается в специально зарезервированное место и не влияет на работу с USB-носителем. Таким образом, USB-носитель может быть использован по основному назначению. В большинстве случаев, даже форматирование диска не приводит к утрате записанного на него ключа, однако переразметка диска должна осуществляться с осторожностью, т.к. может привести к утрате ключей.

* 1. **Модуль Graviton NFC/RFID**

Модуль состоит из двух составных-взаимосвязанных частей:

драйвер NFCPassDxe, работающий с поддерживаемыми считывателями, и предоставляющий стандартный доступ к оборудованию считывателя. NFCPassDxe реализует поддержку интерфейса USB-Serial через переходник типа FTDI или собственного производства;

Текущая версия поддерживает только переходники собственного производства.

драйвер, реализующий логику считывателя, используя стандартный интерфейс, предоставленный первой частью модуля, и выводящий получаемую информацию на стандартный интерфейс ввода, имитирующий ввод с клавиатуры.

При поднесении карты к считывателю происходит чтение информации и передача данных через поток ввода с клавиатуры. Используя стандартные методы BIOS для ограничения доступа (пароли пользователя и администратора, пароли на вход в BIOS или загрузку системы) достигается необходимый функционал.

1. **Организационные меры**

Должны быть приняты организационные (организационно-технические) меры, исключающие неконтролируемый доступ посторонних лиц к устройствам пользователей в нерабочее время, а также в рабочее время при отсутствии пользователей.

Программное обеспечение выполняет свои функции защиты от доступа к системе при обеспечении защиты от несанкционированного доступа к корпусу устройства.

Пользователь обязан соблюдать следующие правила работы с носителем ключа:

не передавать носитель, находящийся в распоряжении пользователя, другим лицам, а также не оставлять его без присмотра. Попадание носителя в чужие руки несет опасность его компрометации;

беречь носитель от механических повреждений;

при утере носителя немедленно сообщить от этом администратору.

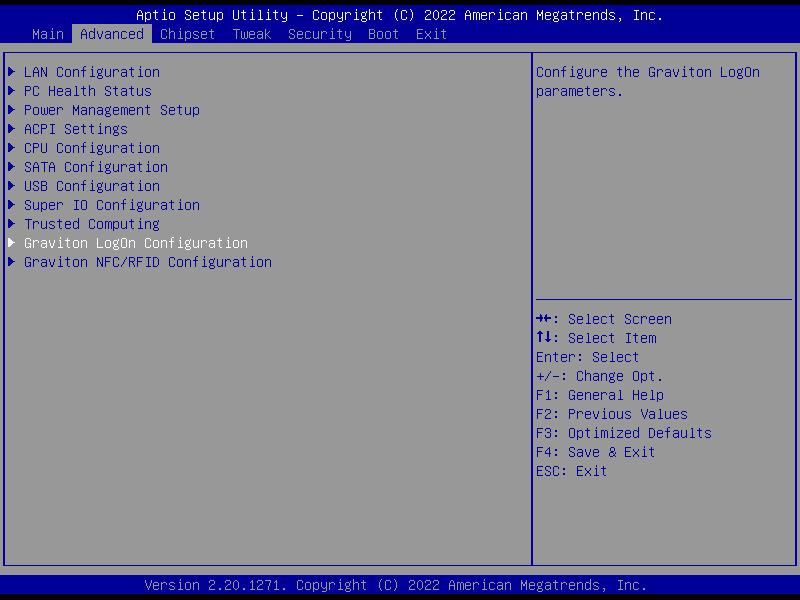
1. **Порядок настройки работы модулей**

Для перехода в меню активации модулей необходимо выполнить следующие действия:

при включении устройства нажать клавишу <F2> для входа в BIOS;

стрелками на клавиатуре перейти в меню «Advanced», где последними пунктами будут «Graviton LogOn Configuration» и «Graviton NFC/RFID Configuration», представленные на рисунке 1;

Внешний вид интерфейса BIOS, а также средства управления могут отличаться от приведённых в настоящем Руководстве, поскольку они зависят от версии BIOS.



* + - 1. – Меню «Advanced» в BIOS Setup

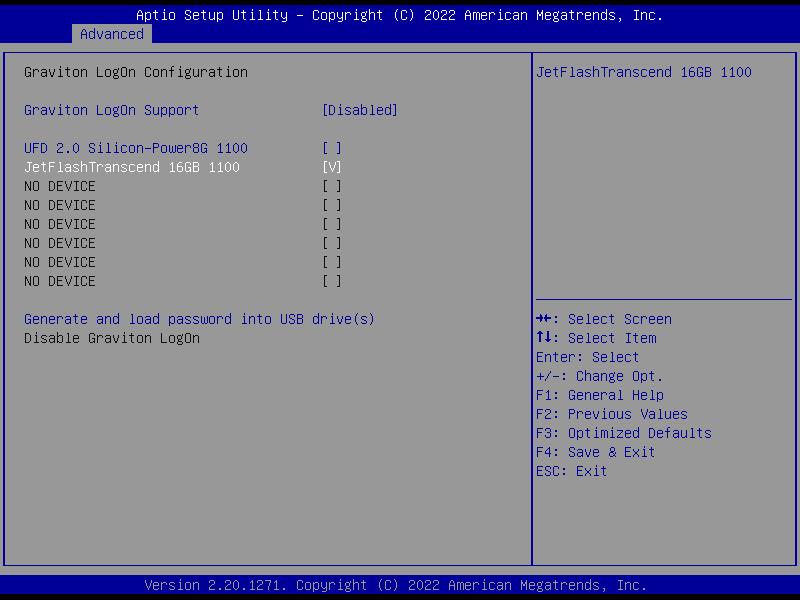
выбрать пункт требуемого модуля для перехода в меню его активации.

* 1. **Модуль Graviton LogOn**

Для активации модуля Graviton LogOn в меню «Graviton LogOn Configuration», представленном на рисунке 2, необходимо выбрать один или несколько USB-носителей, на которые будет загружен ключ. Выбор USB-носителей производится проставлением метки [V] напротив его названия.

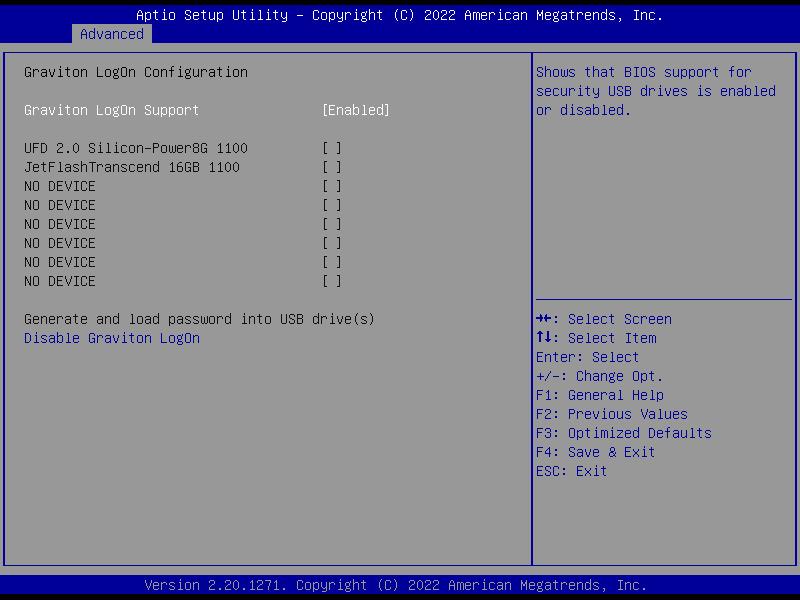
Для одного устройства доступно создание максимум восьми USB-носителей с ключом. Все ключи должны быть записаны одновременно.

Модуль автоматически распознает USB-носители, подключенные к системе, и выводит их названия на экран. Если USB-носитель был подключен к системе после входа в меню модуля, то необходимо вернуться в меню «Advanced» BIOS и снова зайти в меню модуля.



* + - 1. – Меню «Graviton LogOn Configuration» с выбранным USB-носителем

После выбора хотя бы одного USB-носителя в меню станет доступен пункт «Generate and load password into USB drive(s)». При выборе этого пункта происходит генерация ключа и загрузка его на USB-носитель. Статус модуля поменяется на «Enabled». Внешний вид меню «Graviton LogOn Configuration» после активации модуля представлен на рисунке 3.



* + - 1. – Меню «Graviton LogOn Configuration» после активации модуля

После активации модуля необходимо сохранить настройки и выйти из BIOS. С этого момента модуль включен, а выбранные USB-носители выполняют функцию Graviton USB Key.

Для деактивации модуля Graviton LogOn необходимо снова войти в меню «Graviton LogOn Configuration» и выбрать пункт «Disable Graviton LogOn». Статус модуля поменяется на «Disabled», а ключ удалится с USB-носителей. После сохранения настроек система продолжит работу в штатном режиме.

Если требуется создать еще Graviton USB Key, необходимо подключить все USB-носители, имеющие ключ и новые, деактивировать модуль Graviton LogOn, после чего вновь провести процедуру активации модуля.

* 1. **Модуль Graviton NFC/RFID**

Для активации модуля Graviton NFC/RFID необходимо выполнить следующие действия:

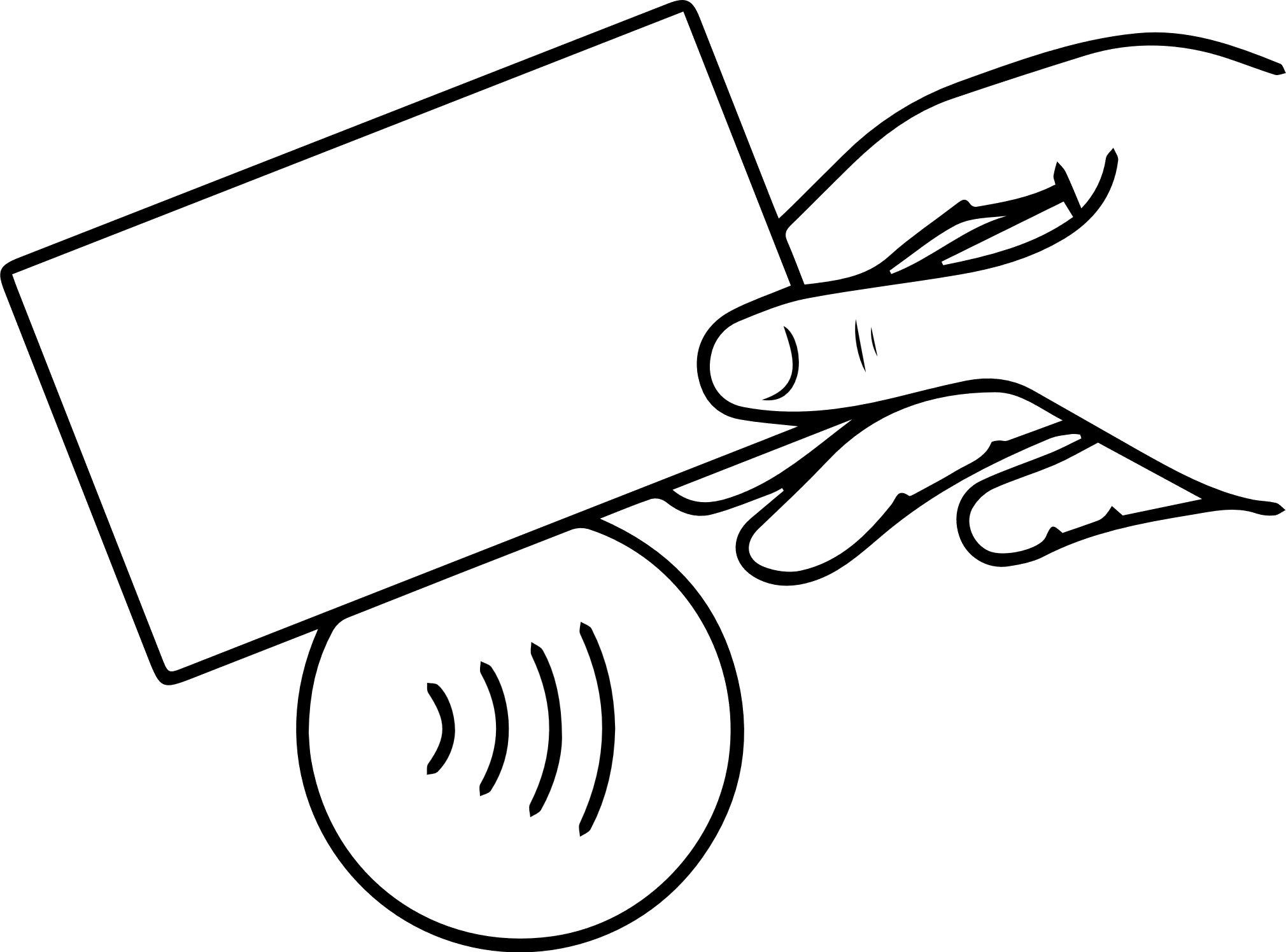
в меню «Graviton NFC/RFID Configuration» изменить статус модуля на «Enabled». Внешний вид меню «Graviton NFC/RFID Configuration» после активации модуля представлен на рисунке 4;



* + - 1. – Меню «Graviton NFC/RFID Configuration» после активации модуля

сохранить настройки и выйти из BIOS, а после перезагрузки системы снова вернуться в BIOS;

после активации модуля необходимо в BIOS в разделе «Security» установить пароль прикладыванием карты к считывателю, нажать клавишу <Enter>. Процесс прикладывания карты к считывателю изображен на рисунке 5;



* + - 1. – Процесс прикладывания карты к считывателю

повторно приложить карту к считывателю для подтверждения пароля, нажать клавишу <Enter>;

Прикладывать карту необходимо однократным кратким действием.

сохранить настройки BIOS и перезапустить систему выключением и повторным включением устройства.

При перезапуске средствами операционной системы настройки могут не примениться.

Для деактивации модуля Graviton NFC/RFID необходимо выполнить действия в следующем порядке:

перед деактивацией модуля необходимо в BIOS в разделе «Security» отключить пароль. Пароль отключается нажатием клавиши <Enter> без ввода пароля и прикладывания карты к считывателю;

в меню «Graviton NFC/RFID Configuration» изменить статус модуля на «Disable»;

сохранить настройки и выйти из BIOS.

После сохранения настроек система продолжит работу в штатном режиме.

1. **Порядок аутентификации пользователя**

После установки пароля и/или записи ключей при включении устройства дальнейшая загрузка будет продолжаться только после аутентификации пользователя предъявлением электронного ключа на носителе.

* 1. **Аутентификация с помощью ключа на USB-носителе**

Для аутентификации необходимо подключить USB-носитель с ключом к   
USB-порту устройства перед его включением.

При попытке включения устройства без предоставления ключа система автоматически выключится.

После аутентификации и загрузки операционной системы USB-носитель можно извлечь. Отсутствие USB-носителя не влияет на работу операционной системы.

* 1. **Аутентификация с помощью карты и NFC/RFID считывателя**

Для аутентификации пользователя при включении устройства необходимо ввести пароль.

При запросе устройством пароля необходимо приложить карту к считывателю однократным кратким действием (см. рисунок 5) и нажать клавишу <Enter>. После система успешно загрузится.

1. **Сброс настроек модулей**

**Внимание!**

**В случае утери носителей ключа или отключении модуля Graviton NFC/RFID без удаления пароля BIOS доступ к устройству будет заблокирован.**

При возникновении подобных ситуаций необходимо вмешательство системного администратора для сброса настроек BIOS до заводских согласно эксплуатационной документации на материнскую плату устройства.

После сброса настроек необходимо вновь установить требуемые параметры в BIOS и настроить модули при необходимости.