

УТВЕРЖДЕН

МКЕЮ.00559-01 32 01-ЛУ

Средство криптографической защиты информации

Мобильное защищенное автоматизированное рабочее место  
«Базовый доверенный модуль» версии 3 в исполнении 1  
СКЗИ МЗ АРМ «БДМ»

Руководство системного программиста

МКЕЮ.00559-01 32 01

Листов 33

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
5549				

2019

## Содержание

1.	Введение .....	4
1.1.	О СКЗИ МЗ АРМ «БДМ».....	4
1.1.1.	Назначение.....	4
1.1.2.	Область применения .....	4
1.1.3.	Характеристики.....	5
1.2.	О данном документе .....	8
1.2.1.	Как использовать данный документ .....	8
2.	Подготовка к использованию СКЗИ МЗ АРМ «БДМ» .....	10
2.1.	Минимальные системные требования .....	10
2.2.	Конфигурирование инсталляционного пакета СКЗИ МЗ АРМ «БДМ».....	10
2.2.1.	Создание образа доверенной среды .....	10
2.2.2.	Сбор начальных данных.....	10
2.2.3.	Подготовка всех компьютеров серии.....	11
3.	Авторизационный носитель администратора .....	12
4.	Авторизационный носитель пользователя .....	13
5.	Работа с инсталляционным носителем .....	14
5.1.	Установка СКЗИ МЗ АРМ «БДМ».....	14
5.2.	Удаление СКЗИ МЗ АРМ «БДМ» .....	15
5.3.	Дополнительные меры защиты СКЗИ МЗ АРМ «БДМ» .....	16
6.	Режим администрирования СКЗИ МЗ АРМ «БДМ».....	17
6.1.	Вход в графический интерфейс администрирования.....	17
6.2.	Целостность системы .....	19
6.2.1.	Восстановление работоспособности системы при нарушении целостности подконтрольных файлов.....	19
6.2.2.	Смена подконтрольных файлов ОС и их эталонных КС .....	19
6.2.3.	Смена файла, содержащего эталонные КС файлов Доверенной ОС .....	19
6.3.	Перешифрование.....	20
6.4.	Вход в UEFI Setup .....	20
6.5.	Работа с системой аудита.....	20
6.5.1.	Изменение настроек журнала аудита.....	21
6.5.2.	Сохранение журнала событий .....	21
7.	Система аудита.....	22
8.	Работа пользователя с СКЗИ МЗ АРМ «БДМ».....	23
8.1.	Краткий обзор работы в системе.....	23

8.2.	Запуск СКЗИ МЗ АРМ «БДМ».....	23
8.3.	Смена пароля пользователя .....	24
8.4.	Идентификация перешифрования .....	26
9.	Список ошибок при работе с СКЗИ МЗ АРМ «БДМ» .....	27
10.	Возможные неполадки и способы их устранения.....	30
	Перечень принятых терминов и сокращений.....	31
	Перечень ссылочных документов .....	32
	Лист регистрации изменений.....	33

# 1. ВВЕДЕНИЕ

## 1.1. О СКЗИ МЗ АРМ «БДМ»

### 1.1.1. Назначение

Изделие мобильное защищенное (МЗ) автоматизированное рабочее место (АРМ) «БДМ» версии 3 в исполнении 1 предназначено для доверенной загрузки операционной системы (ОС) и организации безопасного хранения персональных данных, конфиденциальной, служебной, коммерческой и другой информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на персональном компьютере (ПК) пользователя.

Доверенная загрузка ОС обеспечивается контролем целостности:

- ОС мобильного защищенного АРМ;
- СПО доверенной среды (ДС) мобильного защищенного АРМ.

Безопасное хранение данных и информации обеспечивается путем создания доверенного системного раздела жесткого диска, с установленной на нем Доверенной ОС, в котором информация хранится в зашифрованном виде.

Операции шифрования\расшифрования выполняются прозрачно для пользователя.

Для получения доступа к содержимому доверенного системного раздела пользователю необходимо пройти процедуру аутентификации по паролю (PIN-коду) и обладать необходимой ключевой информацией на отчуждаемом носителе.

### 1.1.2. Область применения

Этот документ описывает особенности, функциональные возможности, конфигурирование и применение СКЗИ МЗ АРМ «БДМ» для администратора безопасности. Большинству конечных пользователей не требуется уровень детализации, содержащийся в данном руководстве.

Изделие применяется в государственных информационных системах при использовании мобильных АРМ на базе современных ноутбуков, предназначено для организации безопасного хранения персональных данных, конфиденциальной, служебной, коммерческой и другой информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на ПК пользователя в соответствии с требованиями законодательства Российской Федерации и нормативными требованиями.

### 1.1.3. Характеристики

СКЗИ МЗ АРМ «БДМ», предназначено для обеспечения криптографической защиты обрабатываемых и хранимых данных по классу КС1, представляет собой программный комплекс, функционирующем на компьютере:

- выполненного на аппаратной платформе x64;
- выполненного на аппаратной платформе x64 с поддержкой набора инструкций AVX.

Спецификация аппаратной платформы приведена в подразделе 2.1 Минимальные системные требования.

СКЗИ МЗ АРМ «БДМ» включает в себя следующие программные модули:

- Модуль БДМ;
- Модуль инсталляции и удаления;
- Модуль шифрования/дешифрования;
- Модуль администрирования;
- Модуль нотификации.

#### 1.1.3.1. Инсталляция СКЗИ МЗ АРМ «БДМ»

Процедуру инсталляции выполняет пользователь с правами Администратора безопасности. Процедура инсталляции предшествует процедуре конфигурирования и формирования загрузочного USB флеш-носителя.

Для установки СКЗИ МЗ АРМ «БДМ» администратор загружается с серийного USB флеш-носителя и выполняет установочный скрипт TeInstall.exe.

#### 1.1.3.2. Блокирование и шифрование доступа к конфиденциальной информации

СКЗИ МЗ АРМ «БДМ» предоставляет следующие возможности по контролю целостности до загрузки ОС:

- контроль целостности программного комплекса СКЗИ МЗ АРМ «БДМ» по ГОСТ Р 34.11-2012;
- контроль целостности на основании процедур выработки и проверки значений хеш-функции ГОСТ Р 34.11-2012 заданных объектов доверенной ОС:
  - файлов ОС;
  - веток реестра ОС.

СКЗИ МЗ АРМ «БДМ» обеспечивает невозможность расшифровки данных зашифрованного раздела и загрузки СКЗИ МЗ АРМ «БДМ» в доверенную ОС в случае нарушения целостности аппаратно-программной платформы.

СКЗИ МЗ АРМ «БДМ» обеспечивает криптографическую защиту секторов доверенного раздела жесткого диска ПК шифрованием при записи и расшифрованием при чтении данных в режиме простой замены с зацеплением алгоритма ГОСТ Р 34.12-2015 (режим простой замены с зацеплением по ГОСТ Р 34.13-2015).

СКЗИ МЗ АРМ «БДМ» применяет алгоритм перемешивания байт сектора (перестановки) при шифровании и расшифровании секторов доверенного раздела жесткого диска ПК.

СКЗИ МЗ АРМ «БДМ» обеспечивает криптографическую защиту обрабатываемых и хранимых данных по классу КС 1, в соответствии с «Требования к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну», в зависимости от варианта комплектации.

СКЗИ МЗ АРМ «БДМ» обеспечивает перешифрование секторов доверенного раздела жесткого диска ПК при смене ключевой информации.

СКЗИ МЗ АРМ «БДМ» обеспечивает контроль корректности реализации выполняемых криптографических функций.

#### 1.1.3.3. Работа СКЗИ МЗ АРМ «БДМ»

СКЗИ МЗ АРМ «БДМ» предоставляет возможность работы с конфиденциальными сведениями (доверенная система):

- Загрузка ОС производится из доверенного (зашифрованного) системного раздела с контролем целостности аппаратно-программной платформы и с аутентификацией пользователя до загрузки ОС;
- Работа осуществляется с ОС, установленной на доверенном (зашифрованном) системном разделе.

#### 1.1.3.4. Аутентификация

СКЗИ МЗ АРМ «БДМ» обеспечивает аутентификацию пользователей ПО:

- аутентификацию пользователя до загрузки ОС;
- двухфакторную аутентификацию по паролю (PIN-коду) и отчуждаемому носителю информации «Рутокен ЭЦП 2.0»;

- авторизированному пользователю возможность осуществления замены собственной парольной информации (PIN-кода);
- невозможность расшифровки данных зашифрованного раздела и загрузки СКЗИ МЗ АРМ «БДМ» в доверенную ОС для неаутентифицированного субъекта.

Ключи выводятся из действия в следующих случаях:

- при плановой смене;
- при компрометации;
- при повреждении носителей.

Изделие СКЗИ МЗ АРМ «БДМ» обеспечивает сквозную авторизацию в домен при использовании в качестве ключевого носителя устройства «Рутокен ЭЦП 2.0».

#### 1.1.3.5. Управление ключевой и инсталляционной информацией и конфигурирование СКЗИ МЗ АРМ «БДМ»

Изделие СКЗИ МЗ АРМ «БДМ» обеспечивает:

- контроль подлинности СКЗИ МЗ АРМ «БДМ» перед инсталляцией;
- однозначную идентификацию целевой аппаратной платформы для установки СКЗИ, исключая возможность инсталляции на неидентифицированной аппаратной платформе;
- создание пользовательского авторизационного носителя на Рутокен ЭЦП 2.0 / JaCarta-2 ГОСТ.

#### 1.1.3.6. Инсталляция и восстановление

В СКЗИ МЗ АРМ «БДМ» предусмотрена процедура восстановления доступности зашифрованных конфиденциальных данных в случае полной или частичной утраты парольной информации пользователя, а также в случае неисправности аппаратной платформы ПК (за исключением аппаратных неисправностей собственно дискового накопителя).

В СКЗИ МЗ АРМ «БДМ» предусмотрена процедура восстановления целостности исполняемого кода СКЗИ МЗ АРМ «БДМ» и/или его конфигурационных данных в случае обнаружения нарушения их целостности.

СКЗИ МЗ АРМ «БДМ» обеспечивает:

- контроль подлинности СПО для инсталляции;

— однозначную идентификацию целевой аппаратной платформы для установки СКЗИ, исключая возможность инсталляции на неидентифицированной аппаратной платформе.

#### 1.1.3.7. Конфигурирование

Изделие СКЗИ МЗ АРМ «БДМ» обеспечивает:

- регистрацию и учет пользователей;
- смену ключевой информации СКЗИ МЗ АРМ «БДМ»;
- изменение эталонных значений параметров целостности аппаратно-программной платформы СКЗИ МЗ АРМ «БДМ»;
- изменение эталонных значений хеш-функции ГОСТ Р 34.11-2012 заданных объектов доверенной ОС.

## 1.2. О данном документе

Этот документ описывает особенности, функциональные возможности, конфигурирование и применение СКЗИ МЗ АРМ «БДМ» для системного администратора и администратора безопасности. Большинству конечных пользователей не требуется уровень детализации, содержащийся в данном руководстве.

### 1.2.1. Как использовать данный документ

Для того чтобы узнать, как подготовить к работе СКЗИ МЗ АРМ «БДМ», обратитесь к разделу 2 «Подготовка к использованию».

Для того чтобы узнать, как осуществлять выпуск и смену PIN-кода авторизационного носителя Администратора, обратитесь к разделу 3 «Авторизационный носитель администратора».

Для того чтобы узнать, как осуществлять выпуск и смену PIN-кода авторизационного носителя пользователя, обратитесь к разделу 4 «Авторизационный носитель пользователя».

Для того чтобы узнать, как осуществлять инсталляцию, деинсталляцию и восстановление системы, обратитесь к разделу 5 «Работа с инсталляционным носителем».

Для того чтобы узнать, как осуществлять администрирование СКЗИ МЗ АРМ «БДМ» в графическом интерфейсе, обратитесь к разделу 6 «Режим администрирования».

Для того чтобы узнать, как осуществляется логирование в системе, обратитесь к разделу 7 «Система аудита».



За информацией о том, как загрузить систему, сменить пароль пользователя и др. обратитесь к разделу 8 «Работа пользователя с .

За информацией по конфигурированию параметров СКЗИ МЗ АРМ «БДМ» обратитесь к разделу **Ошибка! Источник ссылки не найден. «Ошибка! Источник ссылки не найден.»**.

За информацией по конфигурированию параметров ключевых документов СКЗИ МЗ АРМ «БДМ» обратитесь к разделу **Ошибка! Источник ссылки не найден. «Ошибка! Источник ссылки не найден.»**.

За информацией о возможных ошибках СКЗИ МЗ АРМ «БДМ» при работе системы и их описание обратитесь к разделу 9 «Список ошибок при работе с ».

За информацией о возможных нарушениях СКЗИ МЗ АРМ «БДМ» при работе системы и способов их устранения обратитесь к разделу 10 «Возможные неполадки и способы их устранения».

## **2. ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ СКЗИ МЗ АРМ «БДМ»**

### **2.1. Минимальные системные требования**

СКЗИ МЗ АРМ «БДМ», предназначено для обеспечения криптографической защиты обрабатываемых и хранимых данных по классу КС 1, представляет собой программный комплекс, функционирующий на компьютере:

- выполненном на аппаратной платформе с 64-разрядным процессором или выполненном на аппаратной платформе с 64-разрядным процессором с поддержкой набора инструкций AVX;
- оснащенном системой ввода-вывода материнской платы, соответствующей спецификации UEFI 2.6, включая стандарт безопасности UEFI Secure Boot.
- укомплектованном лицензионной ОС типа Windows 10.
- укомплектованном авторизационным носителем пользователя Рутокен ЭЦП 2.0 / JaCarta-2 ГОСТ.
- укомплектованном авторизационным носителем администратора Рутокен ЭЦП Flash 2.0.

### **2.2. Конфигурирование инсталляционного пакета СКЗИ МЗ АРМ «БДМ»**

Создание инсталляционного носителя производится на СКЗИ «БДМ-АРМ-ФК» версия 3 МКЕЮ.00566 01 АО ЭЛВИС-ПЛЮС.

Ключевой носитель пользователя выпускается на СКЗИ «БДМ-АРМ-ФК» версия 3.

#### **2.2.1. Создание образа доверенной среды**

Для создания образа ДС необходимо снять образ требуемой ОС с установленными драйверами и дополнительным ПО для автоматического развертывания на всех компьютерах партии, в соответствии с п. 2.2.1 Руководства системного программиста для СКЗИ «БДМ-АРМ-ФК».

#### **2.2.2. Сбор начальных данных**

Для установки Мобильного защищенного (МЗ) автоматизированного рабочего места (АРМ) «БДМ» версия 3 Администратор безопасности должен подготовить серийный загрузочный отчуждаемый носитель, который будет использоваться для установки Продукта на все компьютеры данной партии.

### 2.2.3. Подготовка всех компьютеров серии

Для подготовки компьютера к серийной установке необходимо загрузиться в UEFI Setup и выполнить следующее:

- Сбросить UEFI Setup на компьютере из партии в заводские настройки.
- Выбрать раздел Security:
  - в пункте меню Password изменить параметр Supervisor Password нажав кнопку Enter и введя новый пароль и его подтверждение.



#### Внимание!

Пароль UEFI Setup необходимо запомнить.

После инсталляции версию UEFI Setup обновлять без предварительного тестирования разработчиков запрещено.

- в пункте меню Secure Boot изменить значение параметра Secure Boot на OFF.
  - в пункте меню Security для параметра Secure Chip поставить значение Disabled.
- Выбрать раздел Startup в пункте меню Boot и поставить первым в приоритет загрузки USB HDD.
- Сохранить изменения UEFI Setup.

### **3. АВТОРИЗАЦИОННЫЙ НОСИТЕЛЬ АДМИНИСТРАТОРА**

Авторизационный носитель администратора необходимо выпустить с помощью СКЗИ «БДМ-АРМ-ФК», подробнее о процедуре выпуска в документе МКЕЮ.00567-01 32 01 «Руководство системного программиста».

Авторизационный носитель администратора – отчуждаемый носителю информации смарт-карта «Рутокен ЭЦП 2.0 Flash» ЗАО «Актив-софт».

Смена PIN-кода авторизационного носителя администратора выполняется на СКЗИ «БДМ-АРМ-ФК».

В случае блокировки авторизационного носителя администратора необходимо обратиться к документации на СКЗИ КБДЖ.468244.044.1 Рутокен ЭЦП 2.0 Flash ЗАО «Актив-софт» для его разблокировки Администратором Рутокен или его форматирования.

## **4. АВТОРИЗАЦИОННЫЙ НОСИТЕЛЬ ПОЛЬЗОВАТЕЛЯ**

Авторизационный носитель пользователя необходимо выпустить с помощью СКЗИ «БДМ-АРМ-ФК», подробнее о процедуре выпуска в документе МКЕЮ.00567-01 32 01 «Руководство системного программиста».

Авторизационный носитель пользователя – отчуждаемый носитель информации смарт-карта Рутокен ЭЦП 2.0 / JaCarta-2 ГОСТ.

Смена PIN-кода авторизационного носителя пользователя выполняется пользователем на СКЗИ МЗ АРМ «БДМ».

В случае блокировки авторизационного носителя пользователя необходимо обратиться к документации на СКЗИ КБДЖ.468244.044.1 Рутокен ЭЦП 2.0 ЗАО «Актив-софт» для его разблокировки Администратором Рутокен или его форматирования.

## 5. РАБОТА С ИНСТАЛЛЯЦИОННЫМ НОСИТЕЛЕМ

### 5.1. Установка СКЗИ МЗ АРМ «БДМ»

Установка СКЗИ МЗ АРМ «БДМ» производится Администратором.

Администратор со сконфигурированным ранее инсталляционным носителем должен сделать следующее:

1. До установки СКЗИ МЗ АРМ «БДМ» должен быть проведен контроль целостности установочного носителя путём расчета контрольных сумм с помощью утилиты `crverify` и сверки с эталонным значением.
2. Загрузиться с инсталляционного носителя и выполнить в командной строке скрипт `TeInstall.exe`.



Изменить параметры системы возможно только с помощью СКЗИ «БДМ-АРМ-ФК», версия 3.



После запуска инсталлятора будет произведена проверка по папкам конфигураций для поиска свободного номера компьютера и присвоен первый незанятый номер конфигурации.

3. При запуске инсталлятора появится запись:

«Найден свободный номер в конфигурации серии: 1

Использовать этот номер для установки? (Y/N)»

4. Ввести [Y] в качестве ответа на вышеобозначенный запрос. Будет выбран номер компьютера для сохранения конфигурационных данных и выведен на экран. При серийной установке на первом компьютере из серии будет выбрана конфигурация [1].
5. При серийной установке на первом компьютере из серии ввести [Y] на запрос: «Серийные параметры не обнаружены. Запустить режим первоначального сохранения серийных параметров? (Y/N)». Будет отображен список доступных для инсталляции дисков.
6. При серийной установке на первом компьютере из серии ввести номер диска [номер диска] на запрос: «Укажите номер диска для подготовки:», после чего будет произведено отображение надписи «Подготовка диска [%введенный номер диска%]»

7. **Данный этап характеризует начало развертывания системы на всех компьютерах из серии.** Ввести [Y] на запрос: «Приступить к установке БДМ? (Y/N)».



**Внимание!**

В процессе инсталляции БДМ системная утилита Diskpart, входящая в состав среды установки WinPE, может некорректно осуществить операцию разметки диска и/или копирования файлов, в результате чего на экране появится сообщение «Скопировано файлов: 0», сигнализирующее о неправильном завершении операции копирования. Администратору необходимо прервать установку БДМ нажатием комбинации клавиш Ctrl+C, после чего повторно запустить процесс установки, с указанием номера компьютера в серии, который использовался при неудачно завершившейся процедуре установки.

8. **Данный этап характеризует начало развертывания системы на всех компьютерах из серии.** После выполнения всех этапов развертывания на экране появится сообщение: «Установка БДМ успешно завершена!».

Установка СКЗИ МЗ АРМ «БДМ» завершается после выполнения всех этапов развертывания.

После установки «СКЗИ МЗ АРМ «БДМ» на компьютер Администратору необходимо импортировать данные конфигурации на СКЗИ «БДМ-АРМ-ФК» и выпустить на нем авторизационный носитель пользователя для этого компьютера. Подробнее об осуществлении данной операции в документе МКЕЮ.00567-01 32 01 «Руководство системного программиста».



Если все компьютеры в серии уже установлены будет выдано предупреждение:

Все серии в использовании. Вы хотите ввести номер компьютера вручную? (Y/N)

где, [N] – выход из процедуры инсталляции, [Y] – необходимо ввести номер компьютера в серии.

При запуске режима инсталляции [Y] будет запущен режим переустановки системы. После ввода номера компьютера начнется инсталляция системы см. п. 6.



Запись авторизационного носителя пользователя необходимо произвести после установки СКЗИ МЗ АРМ «БДМ» после импортирования конфигурационных параметров на СКЗИ «БДМ-АРМ-ФК» подробнее в документе МКЕЮ.00567-01 32 01 «Руководство системного программиста».



При необходимости изменения серийных параметров следует создавать новую серию.

## 5.2. Удаление СКЗИ МЗ АРМ «БДМ»

Удаление СКЗИ МЗ АРМ «БДМ» осуществляется авторизованным пользователем – Администратором. Удаление осуществляется после авторизации Администратора и подтверждения валидности среды функционирования. Для удаления СКЗИ МЗ АРМ «БДМ»

необходим авторизационный носитель администратора и носитель для установки и удаления СКЗИ МЗ АРМ «БДМ». При запуске процедуры удаления происходит самотестирование СКЗИ МЗ АРМ «БДМ» и контроль целостности среды функционирования. Механизм, позволяющий отключить функцию контроля целостности при запуске, отсутствует.

После загрузки с носителя для инсталляции и удаления СКЗИ МЗ АРМ «БДМ» необходимо очистить и отформатировать диск.

### **5.3. Дополнительные меры защиты СКЗИ МЗ АРМ «БДМ»**

В качестве дополнительной меры защиты СКЗИ МЗ АРМ «БДМ» используется встроенный механизм UEFI Setup - UEFI Secure Boot. С включенной опцией Secure Boot перед загрузкой ОС осуществляется контроль подлинности/целостности программных модулей СКЗИ МЗ АРМ «БДМ» путем верификации подписи исполняемых файлов расширения UEFI (загрузчиков, DXE-драйверов и приложений UEFI Shell) RSA сертификатом, хранящемся в защищенной области NVRAM.

СКЗИ МЗ АРМ «БДМ» поставляется с включенной опцией Secure Boot и предустановленными в NVRAM ключами и сертификатами АО «ЭЛВИС-ПЛЮС» для проверки подписи программных файлов расширения UEFI БДМ, а также с сертификатом Microsoft для проверки подписи ПО Microsoft.

Все БДМ модули расширения UEFI поставляются подписанными.

Администратор должен контролировать состояние настройки Secure Boot в UEFI Setup.



## 6. РЕЖИМ АДМИНИСТРИРОВАНИЯ СКЗИ МЗ АРМ «БДМ»

Для работы в режиме администрирования после инсталляции Администратору необходимо авторизоваться с помощью авторизационного носителя.

### 6.1. Вход в графический интерфейс администрирования

Для входа в графический интерфейс администрирования (ГИА) необходимо выполнить действия:



1. Присоединить персональный идентификатор Пользователя к ПК.
2. Включить ПК с помощью кнопки Power.
3. На появившийся запрос  ввести PIN-код Пользователя
4. Ввести комбинацию клавиш <Ctrl>+<F4> либо <Ctrl>+<ELVIS> на экранной клавиатуре. После чего, в случае успешного прохождения авторизации пользователя появится окно с предложением подключить авторизационный носитель администратора (см. Рисунок 1).



Рисунок 1 – Запрос на подключение авторизационного носителя администратора

5. Извлечь Авторизационный носитель пользователя.
6. Присоединить персональный идентификатор Администратора к ПК.
7. На появившийся запрос  ввести PIN-код Администратора (см. Рисунок 2)

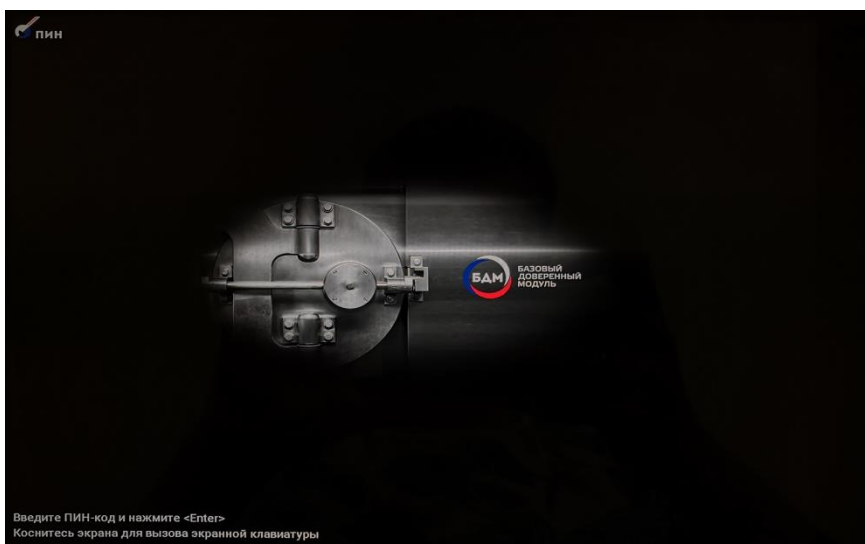


Рисунок 2 – Запрос на авторизацию Администратора

8. Произойдет отображение меню действий Администратора (см. Рисунок 3).

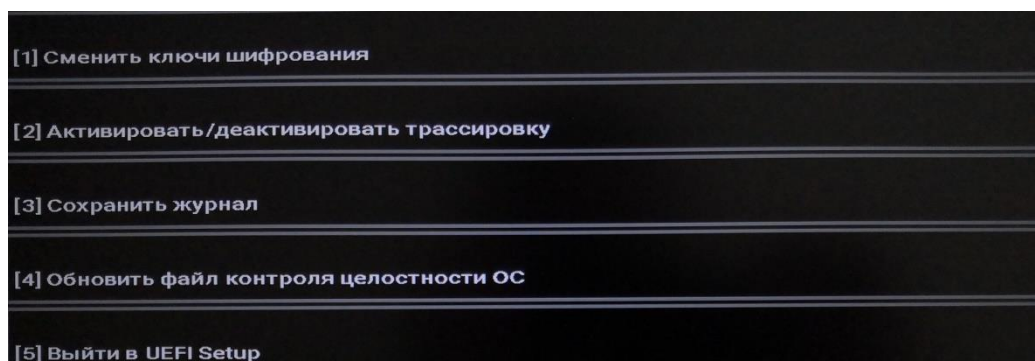


Рисунок 3 – Меню ГИА

После установки системы с помощью интерфейса Администратора можно выполнить следующие действия (см. Таблица 1).

Таблица 1 – Действия доступные в административном режиме

Действие	Описание
Сменить ключи шифрования	Запуск процедуры перешифрования всего жесткого диска. Выполняется в фоновом режиме после создания носителя данных перешифрования на СКЗИ «БДМ-АРМ-ФК» подробнее в документе МКЕЮ.00567-01 32 01 «Руководство системного программиста» и авторизации пользователя.
Активировать / деактивировать трассировку	Включить/Выключить отладочное журналирование событий
Сохранить журнал	Импортировать журнал работы СКЗИ МЗ АРМ «БДМ» на носитель Администратора
Обновить файл контроля целостности ОС	Обновление файла контроля целостности системы osintgrty.cfg. Данный файл поставляется в составе дистрибутива СКЗИ МЗ АРМ «БДМ» и содержит в себе

Действие	Описание
	контрольные суммы файлов СКЗИ МЗ АРМ «БДМ» (TeCrypto.sys, TeCrypto.inf, BdmAgent.exe, TeService.exe, а так же значение веток реестра, отвечающих за автозагрузку этих файлов).
Выйти в UEFI Setup	Осуществить вход в UEFI Setup, если до этого была нажата горячая клавиша входа в UEFI Setup.

Все действия с продуктом в описываемом интерфейсе осуществляются авторизованным пользователем – Администратором СКЗИ МЗ АРМ «БДМ».

## **6.2. Целостность системы**

### **6.2.1. Восстановление работоспособности системы при нарушении целостности подконтрольных файлов**

При обновлении системы возникает необходимость в смене эталонных КС подконтрольных файлов, описанных в конфигурационном файле osintgrty.cfg. При несовпадении контрольных сумм произойдет детектирование нарушения целостности после авторизации пользователя.

Для восстановления системы Администратору необходимо с помощью сторонних средств выполнить следующие действия:

- Обновить (при необходимости) подконтрольные файлы ОС, содержащиеся в файле контроля целостности системы;
- Обновить КС подконтрольных файлов ОС в интерфейсе Администратора.

### **6.2.2. Смена подконтрольных файлов ОС и их эталонных КС**

Изменение списка подконтрольных файлов и эталонных КС подконтрольных файлов, описанных в конфигурационном файле osintgrty.cfg выполняется Администратором при помощи СКЗИ «БДМ-АРМ-ФК», подробнее в документе МКЕЮ.00567-01 32 01 «Руководство системного программиста».

Для восстановления работоспособности системы при нарушении целостности системы Администратор должен изменить файл контроля целостности в административном режиме.

### **6.2.3. Смена файла, содержащего эталонные КС файлов Доверенной ОС**

Для восстановления работоспособности системы при нарушении целостности системы Администратор должен изменить файл контроля целостности в административном режиме.

Для изменения файла контроля целостности необходимо выполнить действия:

1. Убедиться в существовании на Авторизационном носителе Администратора файла КС, которым предполагается заменить текущий файл КС.
2. Войти в режим администрирования (см. подраздел 6.1).

3. Выбрать из предложенного списка пункт «Обновить файл контроля целостности ОС».
4. В случае успешного завершения процедуры замены будет выполнена проверка объектов целостности ОС и последующая загрузка в ОС.

### **6.3. Перешифрование**

Для автоматического перешифрования системы, администратору безопасности необходимо выпустить новые ключевые документы на «БДМ-АРМ-ФК» для этого необходимо обратиться к документу МКЕЮ.00567-01 32 01 Руководство системного программиста. СКЗИ «БДМ-АРМ-ФК».

Для запуска процедуры перешифрования необходимо:

- Убедиться в существовании на Авторизационном носителе Администратора новых ключевых документов.
- Войти в режим администрирования (см. подраздел 6.1).
- Выбрать пункт «Сменить ключи шифрования».
- На появившийся запрос присоединить Авторизационный носитель пользователя.
- Ввести PIN пользователя, дождаться сообщения об успешной смене ключей.
- Перезагрузить компьютер.

### **6.4. Вход в UEFI Setup**

СКЗИ МЗ АРМ «БДМ» блокирует вход в UEFI Setup для исключения загрузки нештатной операционной системы и изменения параметров конфигурации. Для входа в UEFI Setup необходимо воспользоваться интерфейсом Администратора.

Для однократного входа в UEFI Setup необходимо выполнить действия:

1. Ввести горячую клавишу для входа в **UEFI Setup на ПК**.
2. Войти в режим администрирования (см. подраздел 6.1).
3. В ГИА выбрать пункт **Выйти в UEFI Setup** .
4. Получить доступ к меню настроек UEFI Setup.

### **6.5. Работа с системой аудита**

В ГИА доступны следующие действие с системой аудита:

- Сохранить журнал.
- Активировать / деактивировать трассировку.

#### **6.5.1. Изменение настроек журнала аудита**

Для изменение уровня логирования необходимо выполнить действия:

1. Войти в режим администрирования (см. подраздел 6.1).
2. В меню ГИА выберите пункт Активировать / деактивировать трассировку.

#### **6.5.2. Сохранение журнала событий**

Сохранение журнала событий осуществляется на авторизационный носитель Администратора в фиксированный файл VDM.log (в корень раздела).

Чтобы экспортировать журнал событий, необходимо выполнить следующие действия:

1. Войти в режим администрирования (см. подраздел 6.1).
2. В меню ГИА выберите пункт Сохранить журнал.

## 7. СИСТЕМА АУДИТА

Система аудита работает на следующих этапах работы системы:

- логирование работы приложения teinstall.exe(логирование процесса инсталляции СКЗИ МЗ АРМ «БДМ»);
- логирование при работе СКЗИ МЗ АРМ «БДМ» (Администратора и Пользователя).

При инсталляции системы файл логирования сохраняется на административном носителе пользователя в папке bdm\teinstall.log.

После выбора номера компьютера из серии логирование осуществляется в файл install.log в папку с конфигурацией series\<номер конфигурации>\.

Журнал аудита при работе СКЗИ МЗ АРМ «БДМ» сохраняется на защищенном разделе диска. Журнал аудита доступен на чтение только Администратору в интерфейсе администратора. Журнал аудита возможно сохранить в интерфейсе администратора на съемный носитель информации.

Журналы аудита записываются в формате <дата : время><тэг><сообщение>, типы сообщений описаны в таблице (см. **Ошибка! Источник ссылки не найден.**).

Таблица 2 – Формат логирования

Тэг	Описание	Работа системы
[ERR]	ошибка	Ошибка, влияет на работоспособность системы, дальнейшие действия не возможны.
[INF]	информация	Информационное сообщение.
[WRN]	предупреждение	Предупреждение, не влияет на работоспособность системы, только при активированном режиме трассировки.
[SEC]	безопасность	Сообщения событий безопасности.
[DBG]	информация	Отладочные трассировки.

## 8. РАБОТА ПОЛЬЗОВАТЕЛЯ С СКЗИ МЗ АРМ «БДМ»

### 8.1. Краткий обзор работы в системе

Пользователи СКЗИ МЗ АРМ «БДМ» – сотрудники организации, использующие в работе ПК.

После установки инсталляционного пакета СКЗИ МЗ АРМ «БДМ» конечному пользователю не требуется выполнять каких-либо действий, кроме регламентированной ежегодной смены ключевой информации.

Ключ для входа в демилитаризованную зону сохранен на отчуждаемом носителе.

В СКЗИ МЗ АРМ «БДМ» реализована работа в качестве отчуждаемого носителя ключевой информации «Рутокен ЭЦП».

Пользователь может сменить PIN-код для входа в систему.

### 8.2. Запуск СКЗИ МЗ АРМ «БДМ»

Для запуска системы необходимо:




- Присоединить пользовательский отчуждаемый носитель с ключевой информацией к ПК;
- Включить компьютер с помощью кнопки Power;
  - На появившийся запрос  ввести PIN-код пользователя.
  - В случае ошибочного ввода PIN-кода, строка с символами очищается, а справа от нее появляется следующая пиктограмма:  

  - В случае ошибочного ввода PIN-кода после N-ой попытки появляется запись, сообщающая о блокировке ключевого носителя по причине превышения попыток ввода PIN-кода и невозможности дальнейшей загрузки СКЗИ МЗ АРМ «БДМ». Для разблокировки ключевого носителя необходимо обратиться к Администратору (см. **Ошибка! Источник ссылки не найден.**4).



Рисунок 4 - Блокировка ключевого носителя

### 8.3. Смена пароля пользователя

Для смены PIN-кода пользователя необходимо:

- Подключить съемный носитель с ключевой информацией;
- Включить питание СКЗИ МЗ АРМ «БДМ»;
- На поступивший запрос  ввести PIN-код пользователя (см. Рисунок 5);

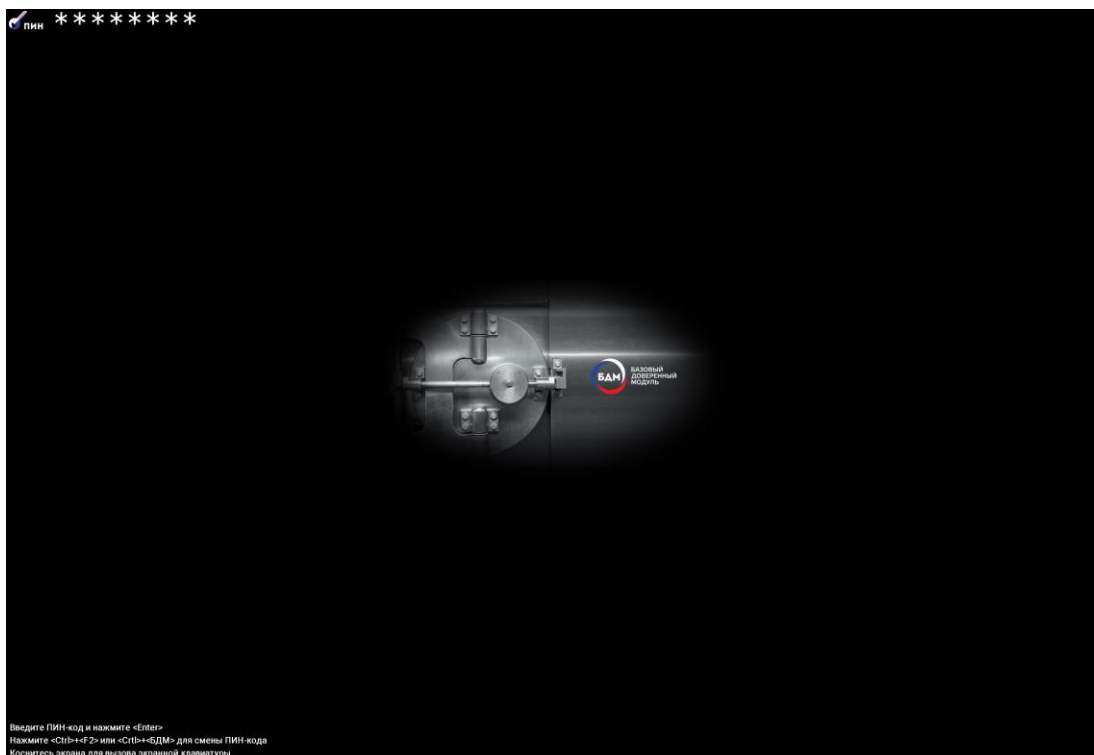


Рисунок 5 – Ввод текущего PIN-кода пользователя

- Ввести <Ctrl>+<F2> либо (<Ctrl>+<БДМ>) на экранной клавиатуре);
- Ввести новый PIN-код пользователя (см. Рисунок 6):



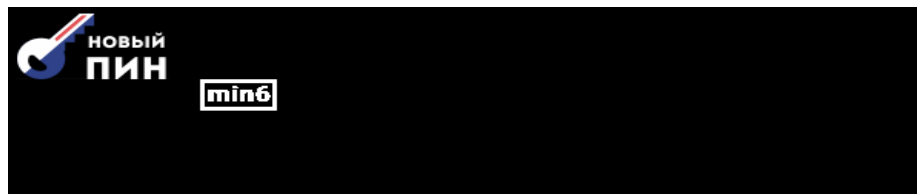


Рисунок 6 – Ввод нового PIN-кода пользователя



Примечание. В СКЗИ МЗ АРМ «БДМ» при смене парольной информации реализован контроль сложности пароля. Под строкой ввода пин-кода отображены иконки, символизирующие парольную политику, определенную на АРМ-ФК при выпуске установочного носителя:

**min6** - обязательная политика. Длина пин-кода должна превышать 6 символов;

**min6 123 abc** - длина пин-кода должна превышать 6 символов. Пин-код должен содержать цифры и символы в нижнем регистре;

**min6 123 abc ABC** - длина пин-кода должна превышать 6 символов. Пин-код должен содержать цифры и символы в обоих регистрах;

**min6 123 abc ABC #S%** - длина пин-кода должна превышать 6 символов.

Пин-код должен содержать цифры и символы в обоих регистрах и спец-символы;

Так же обязательной политикой является условие, что новый пин-код должен содержать больше половины новых символов.



Новый PIN-код следует вводить не спеша, последовательно, ожидая отображения каждого символа \*, вводимого на клавиатуре. По окончании ввода нового PIN-кода необходимо убедиться, что количество символов нового PIN-кода совпадает с количеством отображенных символов \*.

При выполнении всех условий парольной политики защита обратной связи (символы \*) будут отображаться зеленым цветом (см. **Ошибка! Источник ссылки не найден.**7). Система не отреагирует на нажатие клавиши Enter пока строка не будет окрашена в зеленый цвет, сигнализируя о том, что политика пин-кода соблюдена.



Рисунок 7 – Новый PIN-код пользователя удовлетворяет требованиям парольной политики

Если условия парольной политики не выполнены, символы \* будут отображаться красным цветом (см. **Ошибка! Источник ссылки не найден.**).



Рисунок 8 – Новый PIN-код пользователя не удовлетворяет требованиям парольной политики

– Подтвердить новый PIN-код пользователя (см. Рисунок 7):

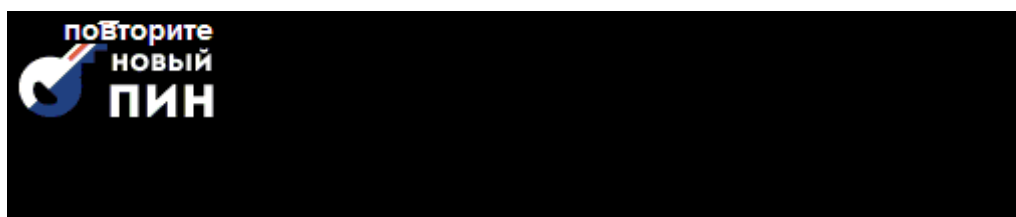


Рисунок 9 – Подтверждение нового PIN-кода пользователя

Пока пин-коды не будут совпадать – на экране будет отображаться соответствующая надпись и клавиша Enter будет заблокирована (Рисунок 10).



Рисунок 10 – Подтверждение нового PIN-кода пользователя

#### 8.4. Идентификация перешифрования

При сквозном перешифровании системы на панели инструментов отображается иконка о

статусе перешифрования   
БАЗОВЫЙ  
ДОВЕРЕННЫЙ  
МОДУЛЬ.

## 9. СПИСОК ОШИБОК ПРИ РАБОТЕ С СКЗИ МЗ АРМ «БДМ»

При обнаружении ошибок в ходе работы СКЗИ МЗ АРМ «БДМ» в журнал аудита выводятся следующие сообщения см. Таблица 3.

Таблица 3 – Сообщения журнала аудита

Сообщение об ошибке	Описание
<дата:время>< SEC > Начата работа системы логирования	Начата работа системы логирования
<дата:время>< SEC > Запущена процедура идентификации Администратора	Уведомление о начале процедуры идентификации текущего оператора в качестве Администратора в контексте текущей ДС.
<дата:время>< SEC >Администратор успешно идентифицирован	Уведомление об успешном завершении процедуры идентификации текущего оператора в качестве Администратора в контексте текущей ДС.
<дата:время>< SEC > Запущена процедура авторизации Администратора	Уведомление о начале процедуры обнаружения корректного ключевого носителя администратора среди всех вставленных в данный момент носителей.
<дата:время>< SEC > Неудачная попытка авторизации Администратора. Осталось <N попыток>	Предупреждение о неправильности введенных текущим оператором данных во время совершения процедуры авторизации Администратора
<дата:время>< SEC > Ключевой носитель Администратора заблокирован – превышено количество попыток ввода неверного пароля	Предупреждение о превышении количества ввода неправильных данных во время совершения процедуры авторизации Администратора
<дата:время>< SEC > Начата процедура смены ключей шифрования	Уведомление об инициализации администратором процедуры смены ключей
<дата:время>< SEC > Произошла ошибка активации/деактивации трассировки	Сообщение об ошибке, произошедшей при попытке активации администратором режима трассировки
<дата:время>< SEC > Начата процедура сохранения журнала	Уведомление об инициализации администратором процедуры сохранения журнала на ключевой носитель администратора
<дата:время>< SEC > Не удалось получить журнал событий	Сообщение об ошибке, произошедшей при инициализации администратором процедуры сохранения журнала
<дата:время>< SEC > Не удалось создать файл журнал событий на токене Администратора	Сообщение об ошибке, произошедшей при инициализации администратором процедуры сохранения журнала
<дата:время>< SEC > Не удалось сохранить журнал событий	Сообщение об ошибке, произошедшей при инициализации администратором процедуры сохранения журнала

Сообщение об ошибке	Описание
<дата:время>< SEC > Журнал событий успешно сохранен на токене Администратора	Уведомление об успешном завершении процедуры сохранения журнала на ключевой носитель администратора
<дата:время>< SEC > Не найден новый файл контроля целостности объектов ДС на токене администратора	Сообщение об ошибке, произошедшей во время выполнения процедуры обновления файла контроля целостности ОС
<дата:время>< SEC > Файл контроля целостности объектов ДС успешно обновлен	Уведомление об успешном завершении процедуры обновления файла контроля целостности ОС
<дата:время>< SEC > Файл контроля целостности объектов ДС пустой	Сообщение об ошибке, произошедшей во время выполнения процедуры обновления файла контроля целостности ОС
<дата:время>< SEC > Невозможно прочитать файл контроля целостности объектов ДС	Сообщение об ошибке, произошедшей во время выполнения процедуры обновления файла контроля целостности ОС
<дата:время>< SEC > Выход в UEFI Setup по запросу Администратора	Уведомление о выходе в UEFI Setup по запросу Администратора
<дата:время>< SEC > Нарушена целостность системы	Процедура самотестирования завершена с ошибкой
<дата:время>< SEC > Процедура самотестирования завершена успешно	Процедура самотестирования завершена успешно
<дата:время>< SEC > Нарушена целостность настроек системы	Не верный dev.bin
<дата:время>< SEC > Неудачная попытка идентификации Пользователя	Среди вставленных носителей не обнаружен ключевой носитель пользователя.
<дата:время>< SEC > Пользователь успешно идентифицирован	Уведомление об успешном завершении процедуры идентификации текущего оператора в качестве пользователя в контексте текущей ДС.
<дата:время>< SEC > Запущена процедура идентификации Пользователя	Уведомление о начале процедуры идентификации текущего оператора в качестве пользователя в контексте текущей ДС.
<дата:время>< SEC > Запущена процедура проверки целостности объектов доверенной ОС	Уведомление о запуске процедуры проверки целостности объектов контроля целостности.
<дата:время>< SEC > Процедура проверки целостности объектов доверенной ОС завершена успешно	Уведомление о завершении выполнения процедуры проверки целостности объектов контроля целостности
<дата:время>< SEC > Начата загрузка доверенной ОС	Уведомление о начале загрузки доверенной среды
<дата:время>< SEC > Пользователь успешно авторизован	Уведомление об успешном завершении процедуры проверки пароля, введенного текущим оператором системы, и предоставления ему прав Пользователя в

Сообщение об ошибке	Описание
	рамках текущей ДС.
<дата:время>< SEC > Администратор успешно авторизован	Уведомление об успешном завершении процедуры проверки пароля, введенного текущим оператором системы, и предоставления ему прав Администратора в рамках текущей ДС.
<дата:время>< SEC > Процедура смены ключей не была завершена	Уведомление о завершении процедуры смены ключей пользователя
<дата:время>< SEC > Смена ключей прошла успешно	Уведомление о смене ключей
<дата:время>< SEC > Запущена процедура авторизации Пользователя	Уведомление о начале процедуры авторизации текущего оператора системы (ввод пароля пользователя и его проверка)
<дата:время>< SEC > Неудачная попытка авторизации Пользователя. Осталось <N попыток>	Предупреждение о неправильности введенных текущим оператором данных во время совершения процедуры авторизации Пользователя
<дата:время>< SEC > Ключевой носитель Пользователя заблокирован – превышено количество попыток ввода неверного пароля	Предупреждение о превышении количества ввода неправильных данных во время совершения процедуры авторизации Пользователя
<дата:время>< SEC > Начата процедура смены PIN-кода Пользователя	Уведомление о запуске процедуры смены PIN-кода Пользователя
<дата:время>< SEC > Смена PIN-кода Пользователя завершилась с ошибкой	Предупреждение о неправильности введенных текущим оператором данных во время совершения процедуры смены PIN-кода
<дата:время>< SEC > Смена PIN-кода Пользователя завершилась успешно	Уведомление о смене пароля пользователя
<дата:время>< SEC > Запущена процедура проверки целостности объектов контроля целостности	Уведомление о запуске процедуры проверки целостности объектов контроля целостности.
<дата:время>< SEC > Процедура проверки целостности объектов контроля целостности завершена успешно	Уведомление о завершении выполнения процедуры проверки целостности объектов контроля целостности

## 10. ВОЗМОЖНЫЕ НЕПОЛАДКИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности и способы их устранения приведены в таблице (см. Таблица 4).

Таблица 4 – Возможные неисправности и способы их устранения

Возможные неполадки	Возможная причина	Решение
Система заблокирована		
Нарушена целостность ОС или объектов, поставленных на контроль	Обнаружено повреждение или несанкционированная замена поставленных на контроль объектов.	Необходимо устранить нарушения в поставленных на контроль объектах. В случае, если изменения были правомерны, выполнить пересчет КС
Нарушена целостность СКЗИ МЗ АРМ «БДМ»	Обнаружено повреждение или несанкционированная замена поставленных на контроль объектов.	Необходимо устранить нарушения в поставленных на контроль объектах. В случае, если изменения были правомерны, выполнить пересчет КС
Пользователь заблокирован		
Превышено допустимое количество неудачных попыток аутентификации	Попытка НСД или Пользователь забыл PIN-код.	Администратору необходимо разблокировать авторизационный носитель пользователя и изменить пароль.

**ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ**

Ниже приведен список русско- и англоязычных сокращений и отдельных специальных терминов, используемых в продукте.

UEFI	Unified Extensible Firmware Interface - интерфейс расширяемой прошивки
PC	Персональный компьютер
PIN	Personal Identification Number - личный опознавательный номер
TOS	Trusted Operation System
USB	Universal serial bus - универсальная последовательная шина
АРМ	Автоматизированное рабочее место
БДМ	Базовый доверенный модуль
ДС	Доверенная среда
МЗ	Мобильное защищенное
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СПО	Специальное программное обеспечение
ФК	Формирование ключей
НСД	Несанкционированный доступ
ОЗУ	Оперативное запоминающее устройство

**ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ**



