

Средство доверенной загрузки
«SafeNode System Loader»

Руководство по установке на ОС Linux

Содержание

1 Требования к аппаратному и программному обеспечению ЭВМ.....	4
2 Подготовка изделия к установке	13
3 Установка изделия	14
4 Ошибки установки	26
5 Настройка изделия	33
6 Активация лицензии	39
7 Удаление изделия	43
8 Обновление изделия	45
Перечень сокращений	47

Введение

В настоящем руководстве приведены указания по установке средства доверенной загрузки «SafeNode System Loader» (далее по тексту – изделие).

Настоящее руководство предназначено для администратора безопасности (АБ), отвечающего за установку программного обеспечения на рабочих местах пользователей, настройку параметров изделия и управление учетными записями пользователей.

Перед началом эксплуатации изделия необходимо внимательно ознакомиться с данной инструкцией и руководством администратора на изделие.

Знаки, расположенные на полях руководства, указывают на примечания, различающиеся по степени важности.



Важная информация, информация предостерегающего характера.



Дополнительная информация, примеры.

1 Требования к аппаратному и программному обеспечению ЭВМ

Для установки изделия электронно-вычислительная машина (ЭВМ) должна иметь следующий минимальный состав технических и программных средств:

- материнская плата ЭВМ с процессором архитектуры Intel x86-64 класса Pentium и выше;
- тактовая частота процессора не ниже 500 МГц;
- BIOS ЭВМ должна соответствовать спецификации UEFI BIOS версии не ниже 2.0;
- требования к объему оперативного запоминающего устройства (оперативной памяти) определяются требованиями операционной системы (ОС), функционирующей в составе данной ЭВМ;
- устройство хранения данных (НЖМД) должно иметь не менее 200 Мбайт свободного места для установки и функционирования изделия;
- минимальное разрешение экрана видеодисплея ЭВМ должно составлять 800 x 600 пикселей.

! Требование к НЖМД: наличие раздела «EFI System Partition» (ESP) с разметкой GPT для возможности размещения модулей изделия.

1.1 Настройка UEFI BIOS ЭВМ

1.1.1 Перед началом установки изделия АБ требуется настроить параметры UEFI BIOS в соответствии с таблицей 1.

Таблица 1 – Значения настроек параметров EFI/UEFI BIOS

Пункт меню UEFI BIOS	Параметр	Значение
Режимы загрузки ОС	UEFI Boot	Enabled
	CSM (Compatibility Support Module)	Disabled
	Legacy Option ROM	Disabled
	Fast Boot	Disabled
	Secure Boot	Disabled
Дополнительно	Режим SATA ¹	AHCI

¹ Изменение значения параметра «Режим SATA» обязательно при эксплуатации изделия в составе некоторых ЭВМ (например, Acer Veriton N4660G)

Для этого АБ следует войти в меню настроек системы, нажав клавишу < F2 >, < F10 > или < Delete > (в зависимости от производителя UEFI BIOS) после включения ЭВМ.



Интерфейс меню настроек может изменяться в зависимости от производителя UEFI BIOS.

1.1.2 В открывшемся меню необходимо установить пароль администратора для предотвращения несанкционированного изменения настроек UEFI BIOS. В большинстве случаев установка пароля BIOS выполняется на главной странице меню **«Main»** или во вкладке **«Security»** (рисунки 1.1 – 1.3). Для некоторых ЭВМ необходимо дополнительно включить меню расширенной настройки **«Advanced Mode»** при помощи клавиши < F7 >².



Рисунок 1.1 – Вкладка **«Main»** UEFI BIOS материнской платы Asus

² Функциональная клавиша может отличаться от приведенного примера в зависимости от типа материнской платы

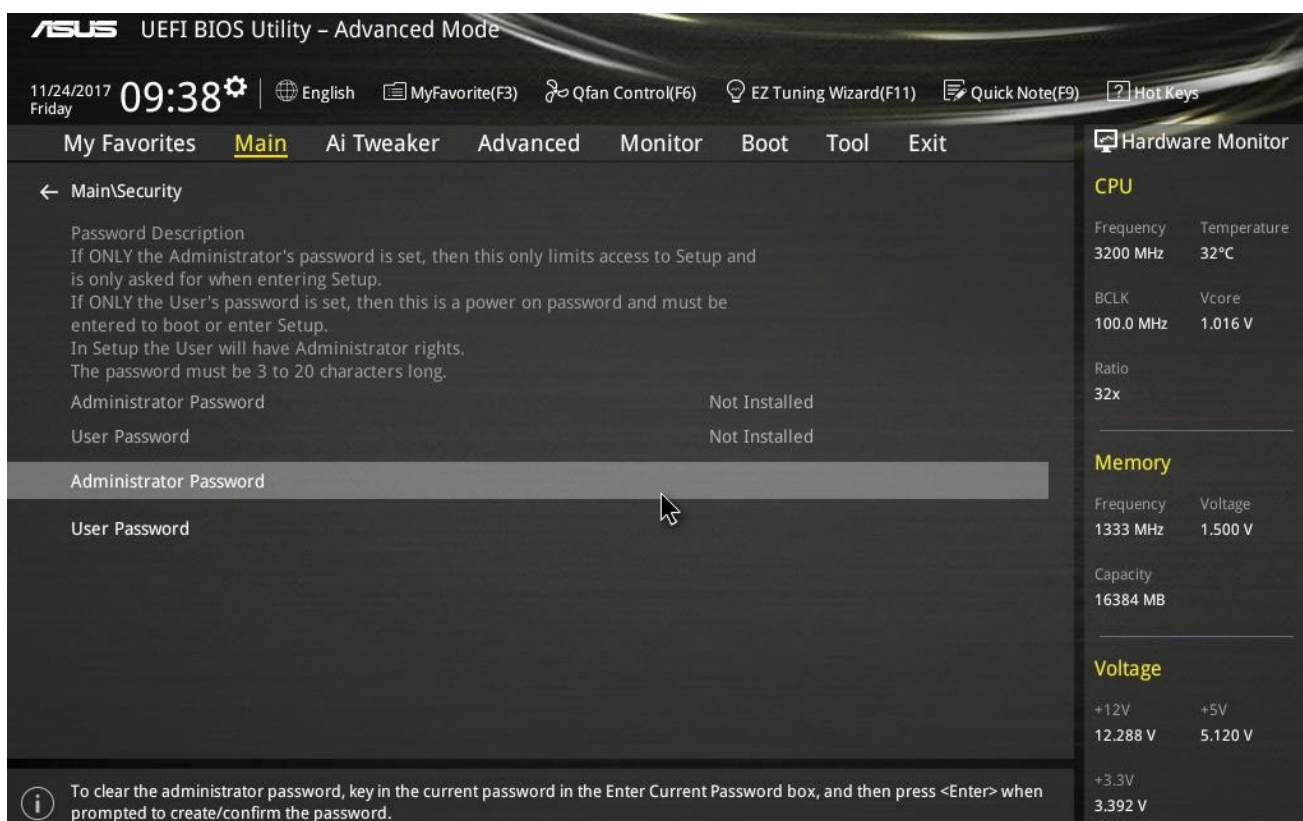


Рисунок 1.2 – Вкладка «Main\Security» UEFI BIOS материнской платы Asus

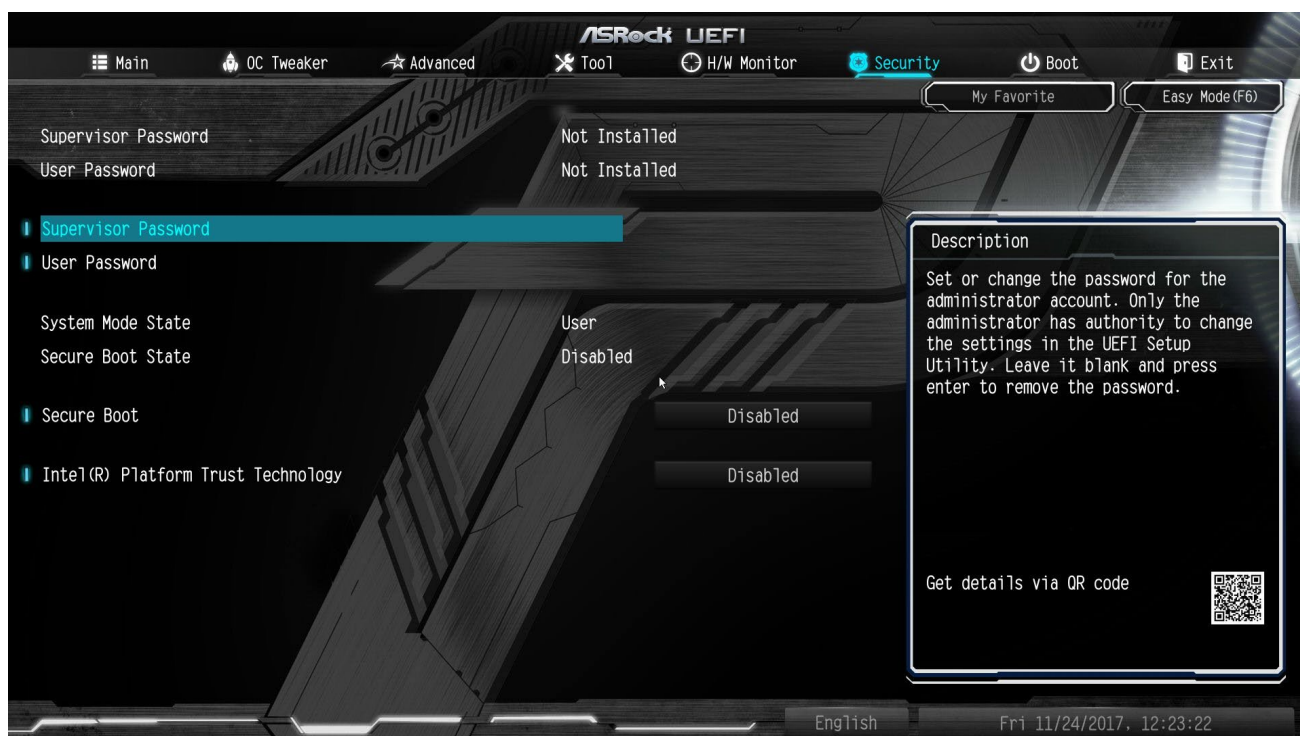


Рисунок 1.3 – Вкладка «Security» UEFI BIOS материнской платы ASRock

1.1.3 Далее следует выбрать пункт «**Administrator Password/Supervisor Password**» (рисунки 1.4 и 1.5) и в появившемся окне установить пароль для входа в UEFI BIOS.

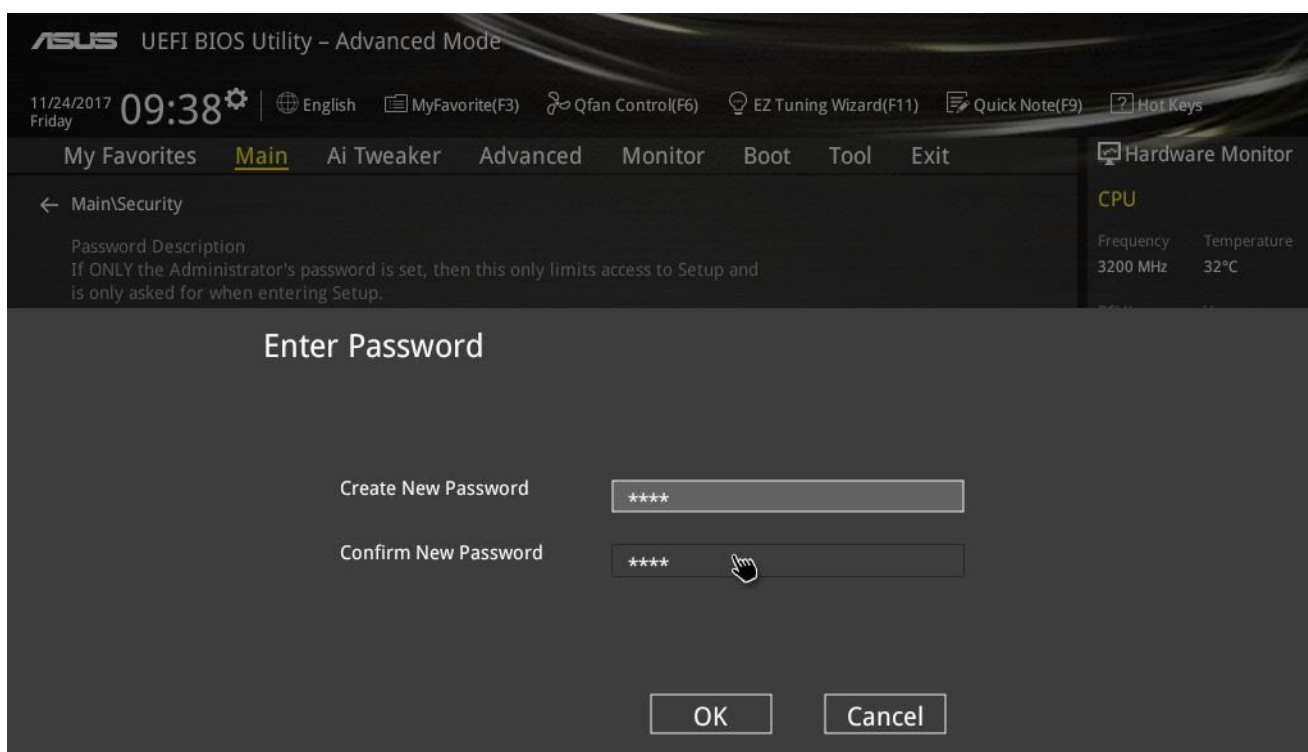


Рисунок 1.4 – Установка пароля UEFI BIOS материнской платы Asus

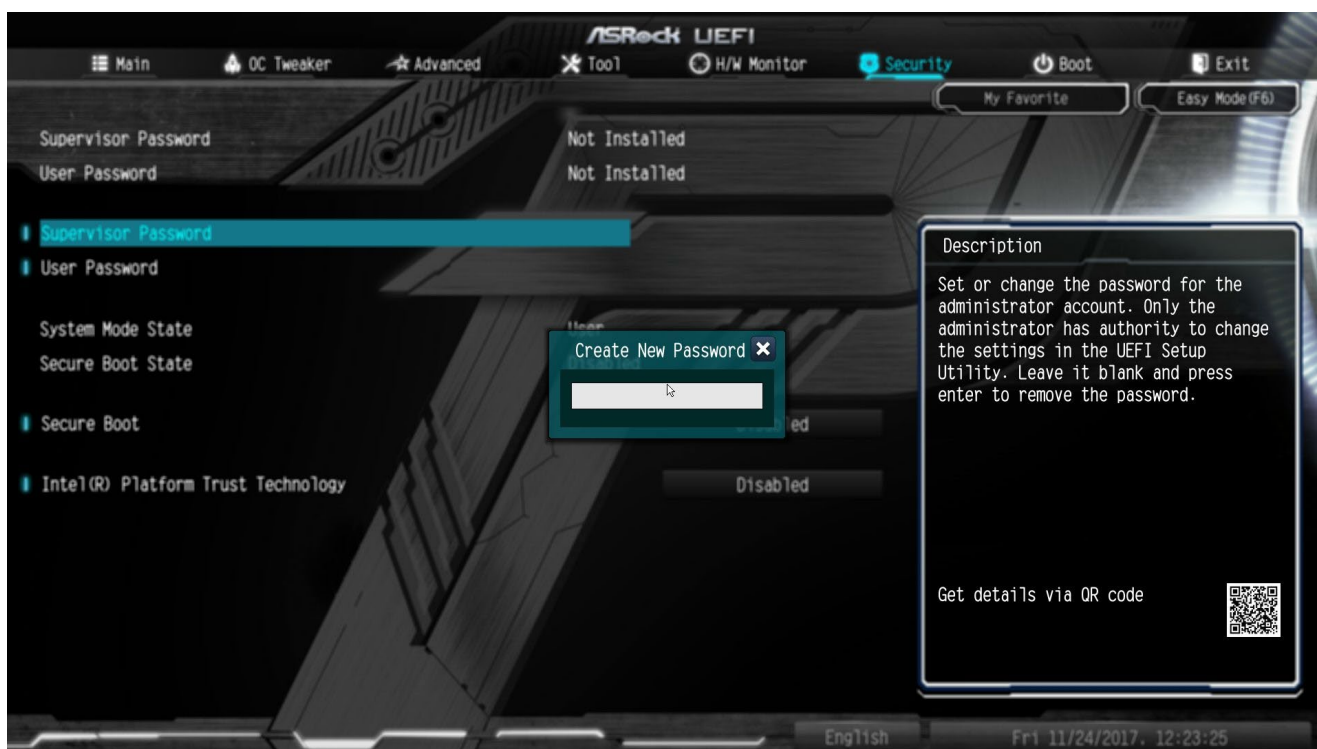


Рисунок 1.5 – Установка пароля UEFI BIOS материнской платы ASRock

1.1.4 В зависимости от интерфейса UEFI BIOS отключение параметра безопасной загрузки **«Secure Boot»** может быть выполнено во вкладке **«Security»** (рисунок 1.3).

1.1.5 После установки пароля необходимо отключить модуль поддержки совместимости CSM, а также режим поддержки загрузки **«Legacy Boot»**.

1.1.6 Для этого АБ следует перейти во вкладку **«Boot»**, а затем на вкладку «CSM» (рисунки 1.6 – 1.9).

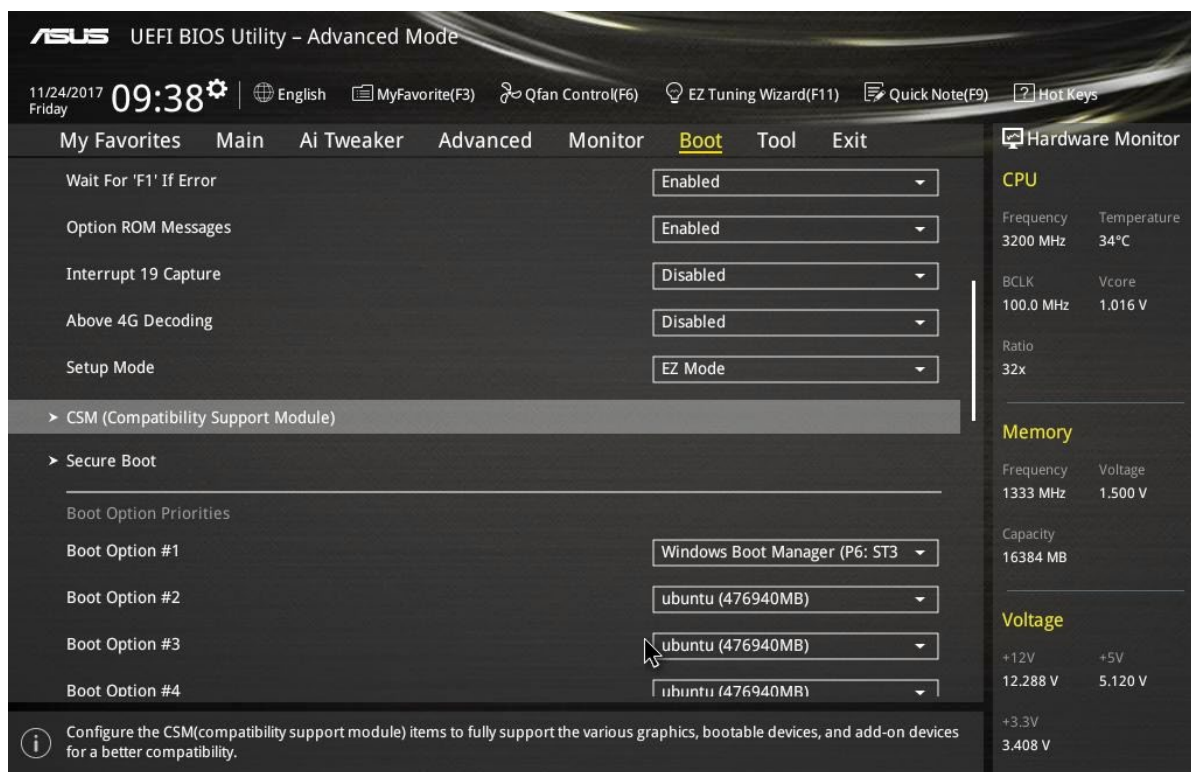


Рисунок 1.6 – Вкладка **«Boot»** UEFI BIOS материнской платы Asus



Рисунок 1.7 – Вкладка **«Boot»** UEFI BIOS материнской платы ASRock



Рисунок 1.8 – Вкладка «**CSM**» UEFI BIOS материнской платы Asus



Рисунок 1.9 – Вкладка «**CSM**» UEFI BIOS материнской платы ASRock

1.1.7 Во вкладке **«Boot»** необходимо установить параметру быстрой загрузки **«Fast Boot»** значение **«Disabled»** (рисунок 1.7).



У некоторых производителей управление параметром **«Secure Boot»** осуществляется во вкладке **«Boot»** (рисунок 1.6).

Данный параметр необходимо установить в значение **«Disabled»**.

1.1.8 Во вкладке CSM необходимо перевести работу модуля в режим **«Disabled»** (рисунки 1.10 – 1.11).

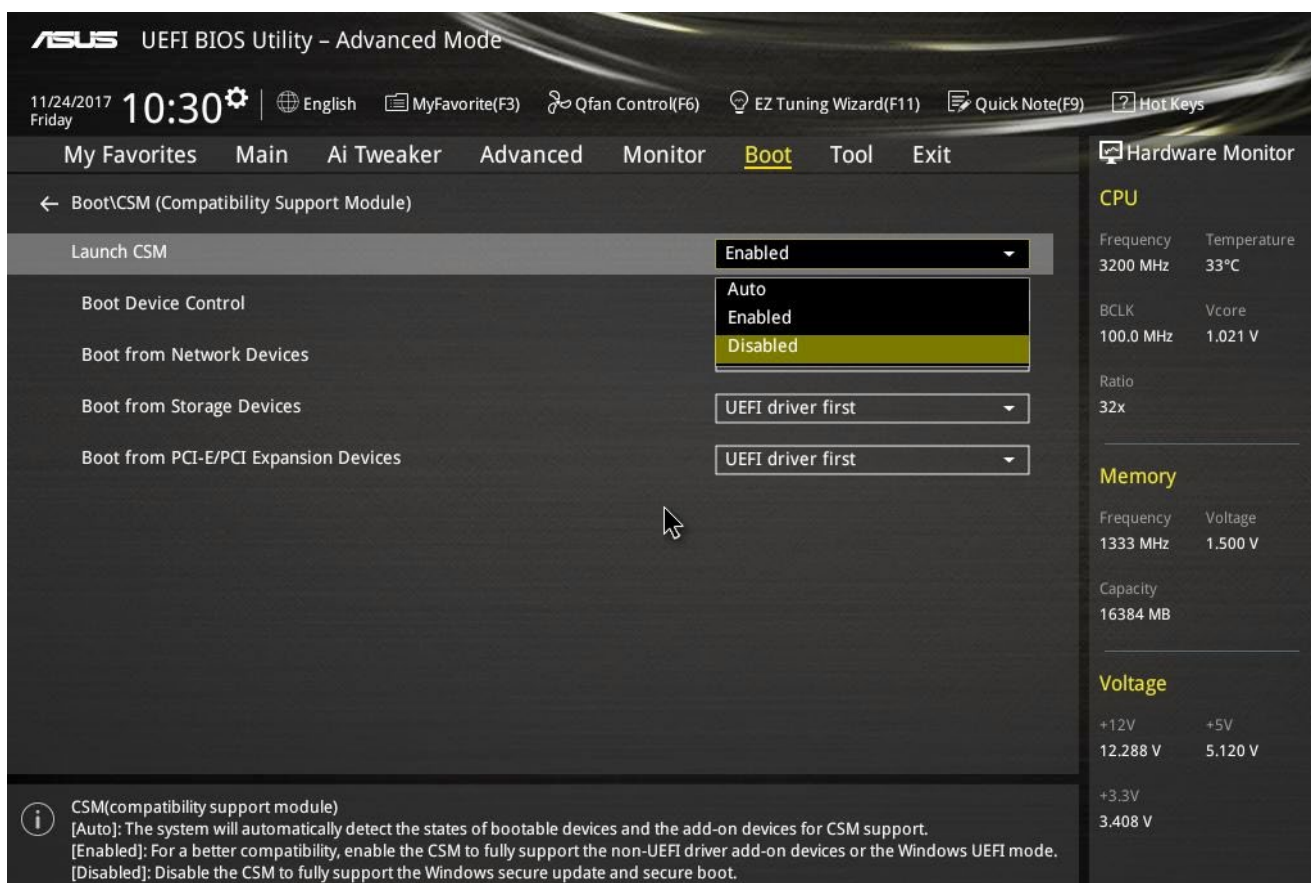


Рисунок 1.10 – Выключение параметра **«CSM»** UEFI BIOS материнской платы Asus



Рисунок 1.11 – Выключение параметра «CSM» UEFI BIOS материнской платы ASRock



Выключение параметра CSM и переключение платформы в полноценный UEFI режим загрузки требует наличия подписанных драйверов на PCI-E, M.2 и SATA Express SSD-носителях для возможности их работы в системе (рисунок 1.12).

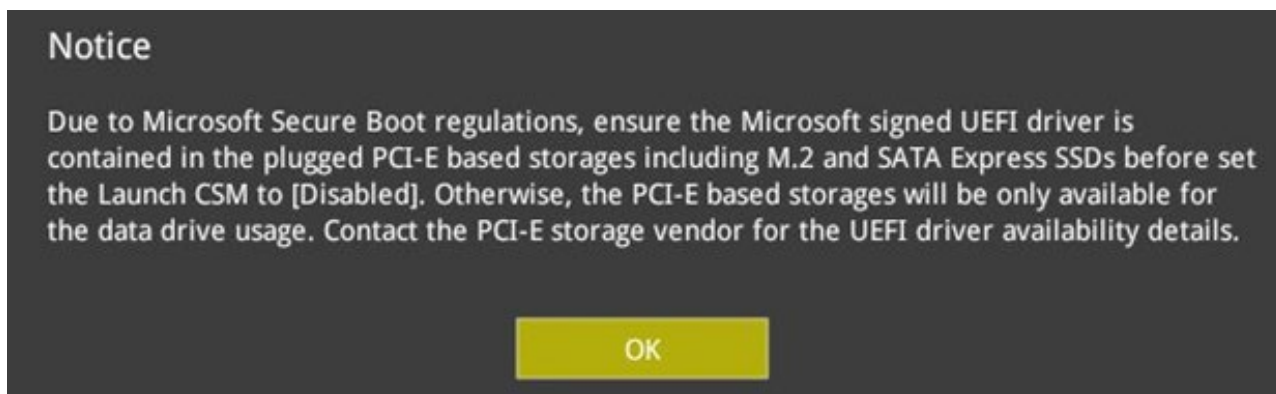


Рисунок 1.12 – Окно с предупреждением необходимости наличия UEFI драйверов для носителей на шине PCI-E

1.1.9 Современные версии UEFI автоматически выключают режим загрузки модулей Legacy при выключении параметра **«CSM»**. На более старых версиях BIOS может потребоваться принудительное выключение (рисунки 1.13 – 1.14).

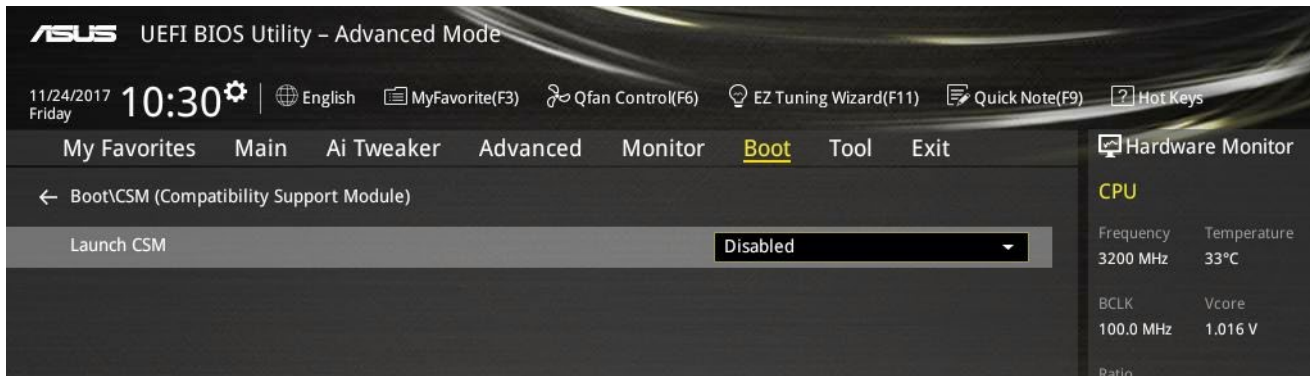


Рисунок 1.13 – Загрузка Legacy ОС отключена в UEFI BIOS Asus

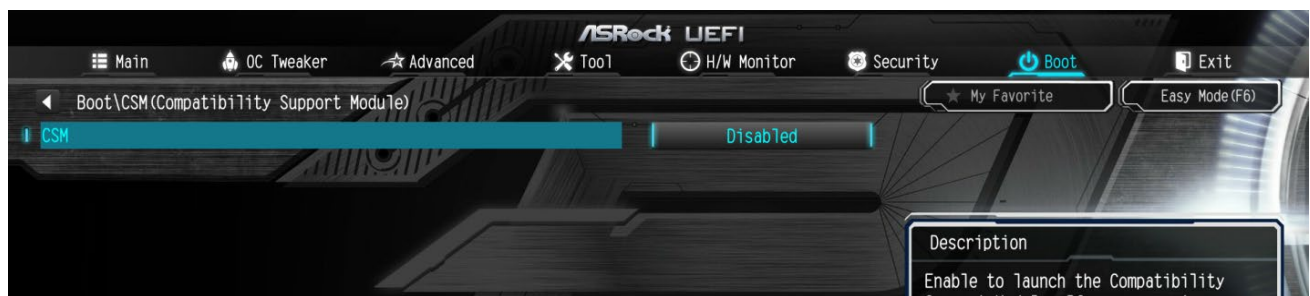


Рисунок 1.14 – Загрузка Legacy ОС отключена в UEFI BIOS ASRock

2 Подготовка изделия к установке

- 2.1 Скачать дистрибутив с ресурса <https://sftp.gaz-is.ru/>³
- 2.2 Перенести полученный дистрибутив на целевую ЭВМ для установки.



Меры безопасности при подготовке к использованию

Установка изделия должна осуществляться под руководством специально подготовленного персонала.

Некорректная установка изделия может привести к повреждению содержимого Flash-памяти UEFI BIOS ЭВМ, что потребует восстановления с использованием программатора.

При самостоятельной установке изделия на ЭВМ рекомендуется обязательная консультация с технической поддержкой ООО «Газинформсервис».

Контакты технической поддержки указаны на официальном сайте компании: <https://www.gaz-is.ru/>

³ Ссылка на скачивание будет отправлена в письме

3 Установка изделия

3.1 Общие требования к установке изделия

3.1.1 Перед установкой изделия необходимо произвести обязательные подготовительные действия в соответствии с разделом 2 документа и произвести обязательную настройку параметров UEFI BIOS в соответствии с разделом 1.

3.1.2 Установка модулей изделия и графической консоли осуществляется совместно в процессе инсталляции изделия.

3.1.3 Полный процесс установки изделия состоит из двух этапов.

1) Первый этап заключается в копировании модулей на ESP раздел НЖМД для последующей установки и перезаписи региона образа UEFI BIOS ЭВМ на модифицированный UEFI BIOS с добавленными модулями защиты изделия. Также осуществляется установка графической консоли изделия для работы из ОС Linux. Данный этап осуществляется в среде операционной системы.

2) На втором этапе осуществляется установка и перезапись региона образа UEFI BIOS ЭВМ на модифицированный UEFI BIOS с добавленными модулями защиты изделия. Данный этап осуществляется в среде UEFI ЭВМ.

Допускается установка изделия на ЭВМ, функционирующие под управлением следующих ОС семейства Linux:

- Astra Linux Special Edition 1.7 релиз «Смоленск» (производитель ООО «РусБИТех-Астра»);
- Альт 8 СП (производитель АО «ИВК»);
- РЕД ОС 7.3 «Муром» (производитель ООО «РЕД СОФТ»);
- Роса «Хром» (производитель АО «НТЦ ИТ РОСА»).



До завершения процесса установки изделия пользователям доступна загрузка ОС без настроенных механизмов защиты доверенной загрузки.

3.1.4 В случае возникновения ошибок при установке, необходимо перейти в директорию EFI, скопировать файл лога установки install.log и отправить его обратным письмом на адрес техподдержки support@gaz-is.ru. Также можно оформить заявку через официальный сайт компании <https://www.gaz-is.ru/poddergka/zajavka.html>

3.2 Установка изделия в ОС Astra Linux SE 1.7

3.2.1 Запустить консоль в ОС Astra Linux SE 1.7.

3.2.2 Для первого этапа установки выполнить следующую команду (рисунок 3.1):

```
sudo dpkg -i sns1.deb
```

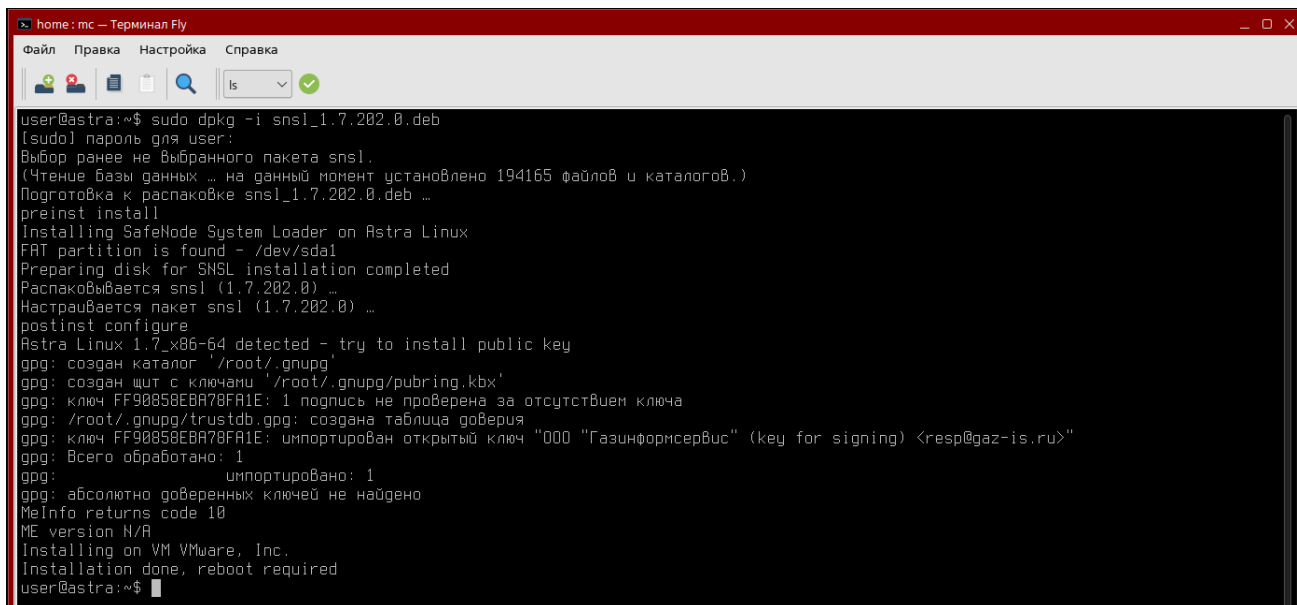


Рисунок 3.1 – Первый этап установки изделия

3.2.3 В случае успеха появится надпись:

```
Installation done, reboot required
```

3.2.4 На данном этапе на ESP разделе НЖМД будут сохранены модули изделия, графическая консоль будет скопирована по пути `/usr/share/sdz/bin/`

3.2.5 Если первый этап установки прошел корректно и при этом не возникло сбоев в процессе перезагрузки будет выведено сообщение (рисунок 3.2).

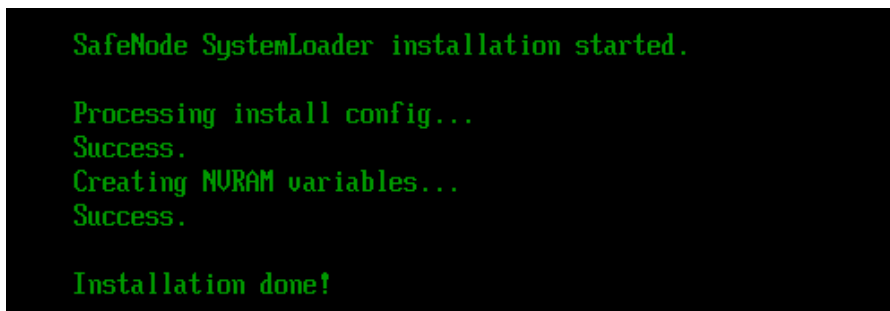

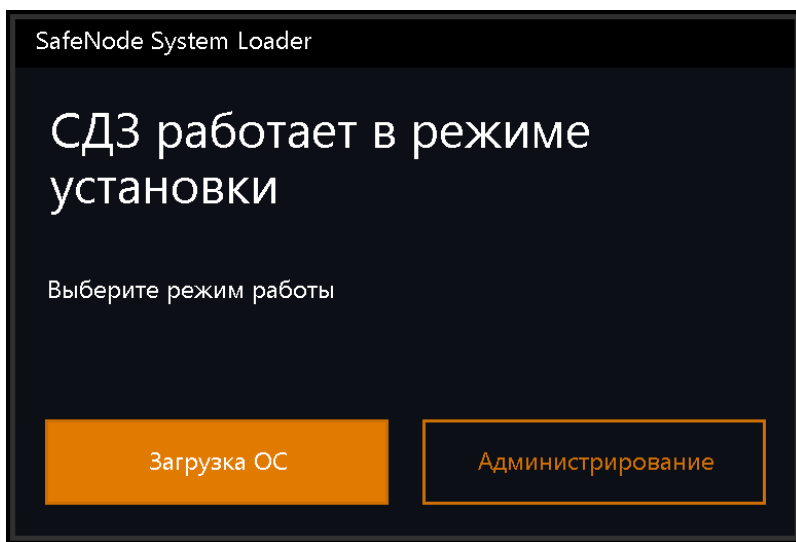


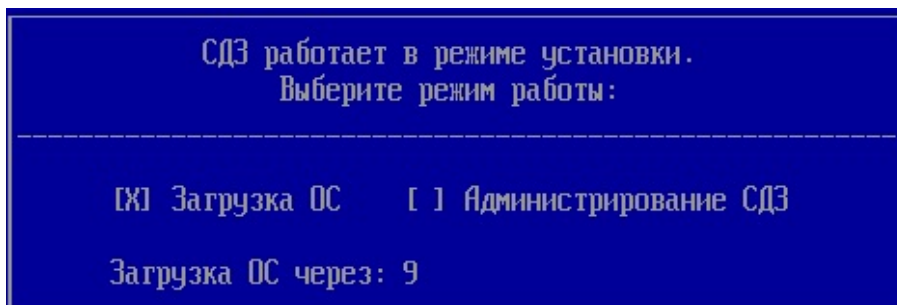
Рисунок 3.2 – Информационное сообщение

3.2.6 После перезагрузки ЭВМ появится информационное сообщение о работе изделия в режиме установки (рисунок 3.3).

 Стандартно загружается графический интерфейс консоли (рисунок 3.3 а) для переключения в псевдографическую консоль необходимо во время загрузки модулей ПО нажать клавишу «O» (рисунок 3.3 б).



а) Графический интерфейс



б) Псевдографический интерфейс

Рисунок 3.3 – Информационное сообщение о работе изделия в режиме установки

 **До завершения процесса установки изделия пользователям доступна загрузка ОС без настроенных механизмов защиты доверенной загрузки.**

3.2.7 Если установка изделия осуществляется при заранее активированном режиме **замкнутой программной среды**, далее необходимо принудительно обновить конфигурационный файл `/etc/digsig/digsig_initramfs.conf`. Для загрузки модулем `digsig_verif` ключей после их размещения, нужно от имени учетной записи администратора выполнить команду (рисунок 3.4):

```
sudo update-initramfs -u -k all
```

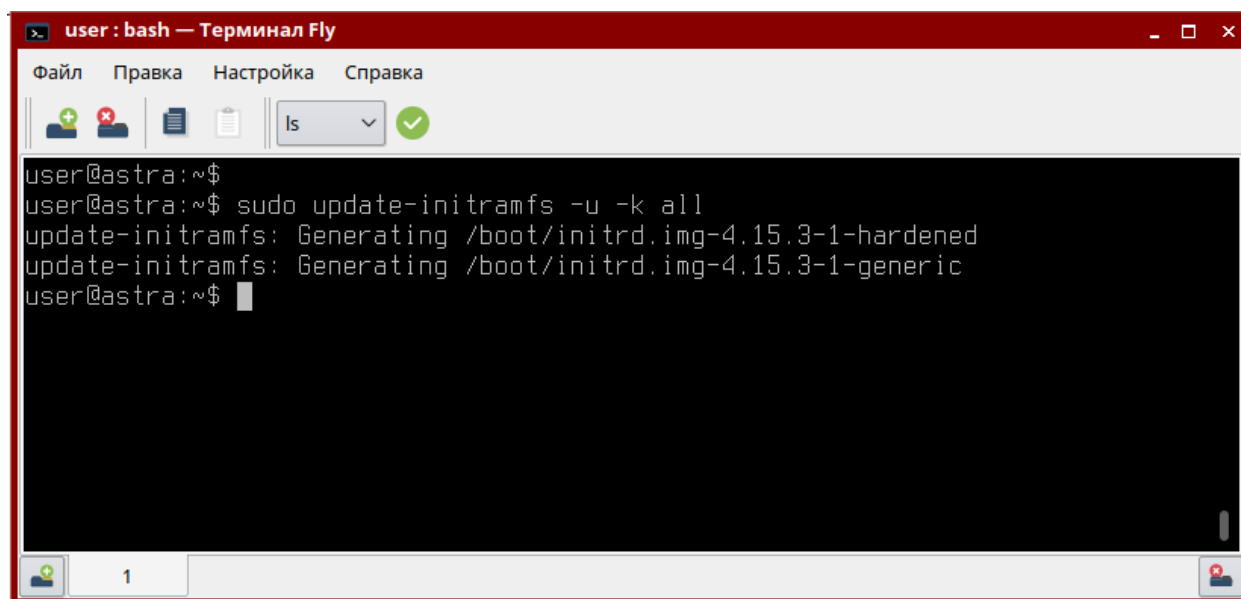


Рисунок 3.4 – Обновление конфигурационного файла



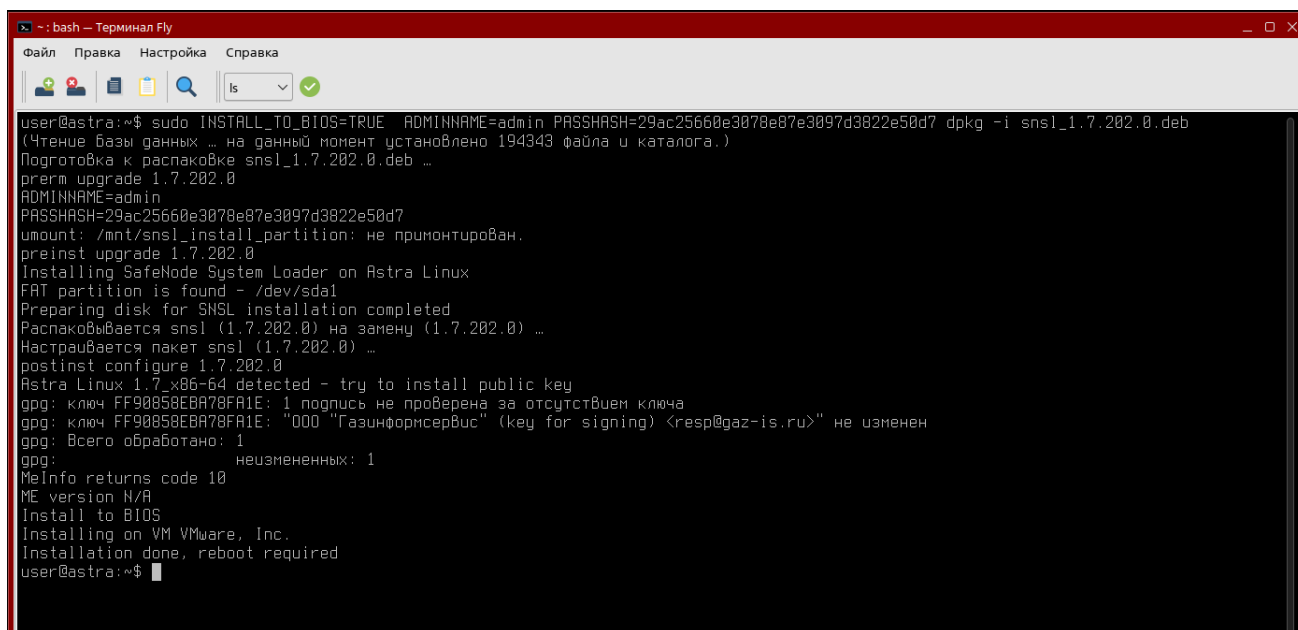
В случае, если режим замкнутой программной среды активируется в графическом режиме ОС после установки изделия на ЭВМ, конфигурационный файл **`/etc/digsig/digsig_initramfs.conf`** обновляется автоматически и дополнительных действий проводить не нужно. В режиме консоли включение замкнутой программной среды включает в себя принудительное требование обновления конфигурационного файла.

3.2.8 Для продолжения процесса установки необходимо загрузить операционную систему.

3.2.9 Для начала второго этапа установки необходимо указать команду на установку вместе с хеш-суммой пароля администратора (рисунок 3.5):

```
sudo INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29ac25660e30  
78e87e3097d3822e50d74 dpkg -i sns1.deb
```

⁴ хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512



```
user@astra:~$ sudo INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7 dpkg -i snsl_1.7.202.0.deb
(Чтение базы данных ... на данный момент установлено 194343 файла и каталога.)
Подготовка к распаковке snsl_1.7.202.0.deb ...
preinst upgrade 1.7.202.0
ADMINNAME=admin
PASSHASH=29ac25660e3078e87e3097d3822e50d7
umount: /mnt/snsl_install_partition: не примонтирован.
preinst upgrade 1.7.202.0
Installing SafeNode System Loader on Astra Linux
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
Распаковывается snsl (1.7.202.0) на замену (1.7.202.0) ...
Настраивается пакет snsl (1.7.202.0) ...
postinst configure 1.7.202.0
Astra Linux 1.7_x86-64 detected - try to install public key
gpg: ключ FF90858EBA78FA1E: 1 подпись не проверена за отсутствием ключа
gpg: ключ FF90858EBA78FA1E: "000 "Газинформсервис" (key for signing) <resp@gaz-is.ru>" не изменен
gpg: Всего обработано: 1
gpg: неизмененных: 1
MeInfo returns code 10
ME version N/A
Install to BIOS
Installing on VM VMware, Inc.
Installation done, reboot required
user@astra:~$
```

Рисунок 3.5 – Второй этап установки изделия

3.2.10 В процессе установки произойдет перезапись образа региона UEFI BIOS и во Flash-памяти будет расположен обновленный образ региона UEFI BIOS с добавленными модулями защиты изделия.

3.2.11 Эталонный регион образа UEFI BIOS будет сохранен на ESP раздел НЖМД.

Сохраненный регион образа UEFI BIOS необходим при удалении изделия, когда осуществляется обратная замена модифицированного образа UEFI BIOS на оригинальный образ.

3.2.12 После перезаписи региона UEFI BIOS осуществится автоматическая перезагрузка ЭВМ. Процесс установки завершен.

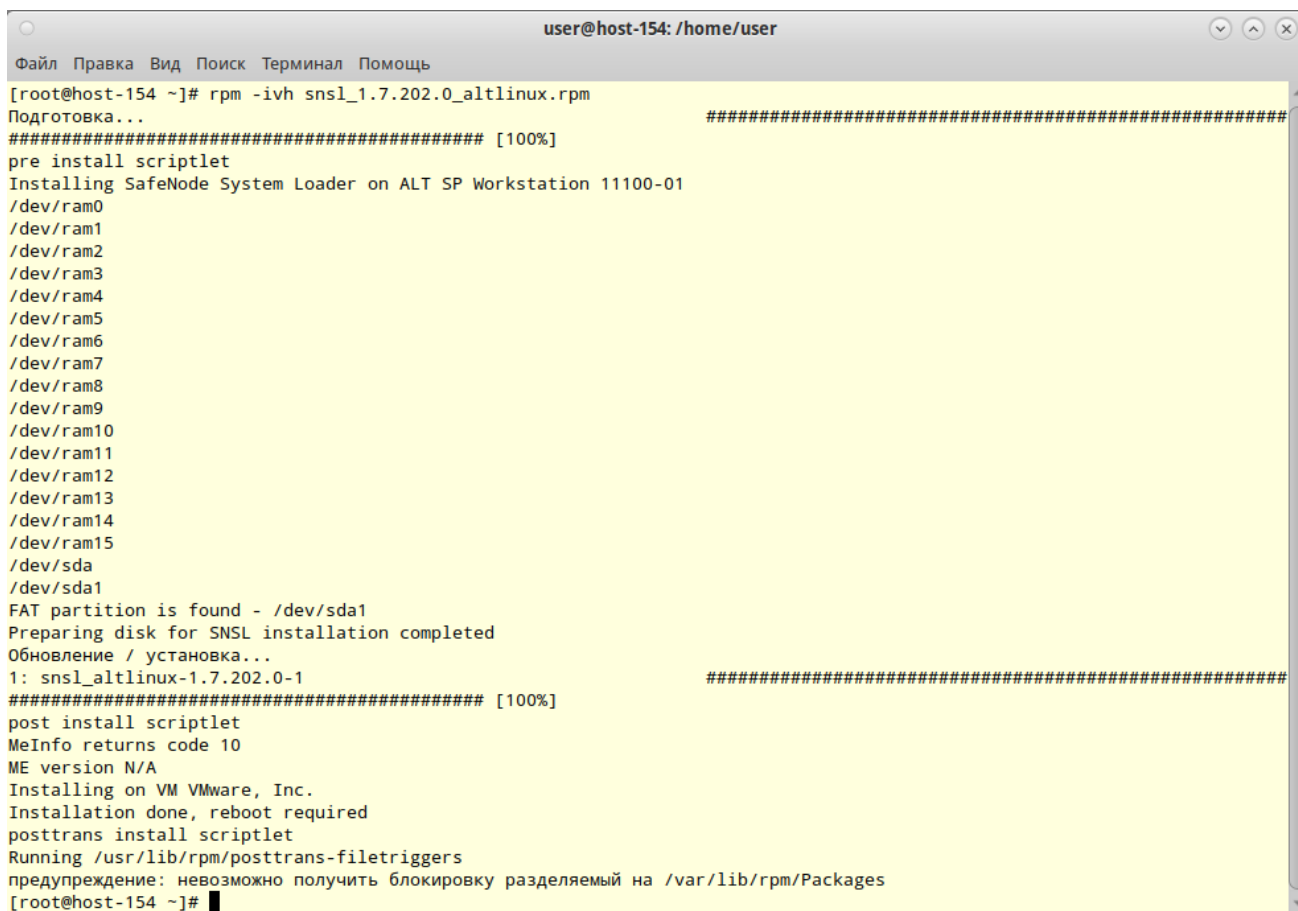
3.2.13 Если изделие было корректно установлено на ЭВМ и при этом не возникло сбоев в процессе установки, после перезагрузки ЭВМ появится информационное сообщение (рисунок 3.3).

3.3 Установка изделия на ОС Альт 8 СП

3.3.1 Запустить консоль ОС Альт 8 СП.

3.3.2 Для установки пакета выполнить следующую команду (рисунок 3.6).

```
sudo rpm -iv snsl_altlinux.rpm
```



```
user@host-154: /home/user
Файл Правка Вид Поиск Терминал Помощь
[root@host-154 ~]# rpm -ivh snsl_1.7.202.0_altlinux.rpm
Подготовка... #####
##### [100%]
pre install scriptlet
Installing SafeNode System Loader on ALT SP Workstation 11100-01
/dev/ram0
/dev/ram1
/dev/ram2
/dev/ram3
/dev/ram4
/dev/ram5
/dev/ram6
/dev/ram7
/dev/ram8
/dev/ram9
/dev/ram10
/dev/ram11
/dev/ram12
/dev/ram13
/dev/ram14
/dev/ram15
/dev/sda
/dev/sda1
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
Обновление / установка...
1: snsl_altlinux-1.7.202.0-1 #####
##### [100%]
post install scriptlet
MeInfo returns code 10
ME version N/A
Installing on VM VMware, Inc.
Installation done, reboot required
posttrans install scriptlet
Running /usr/lib/rpm/posttrans-filetriggers
предупреждение: невозможно получить блокировку разделяемый на /var/lib/rpm/Packages
[root@host-154 ~]#
```

Рисунок 3.6 – Первый этап установки изделия

3.3.3 В случае успеха появится надпись:

Installation done, reboot required

3.3.4 На данном этапе на ESP разделе НЖМД будут сохранены модули изделия и скопирована графическая консоль.

3.3.5 Если первый этап установки прошел корректно и при этом не возникло сбоев в процессе перезагрузки будет выведено сообщение (рисунок 3.2).

3.3.6 После перезагрузки ЭВМ появится информационное сообщение о работе изделия в режиме установки (рисунок 3.3).

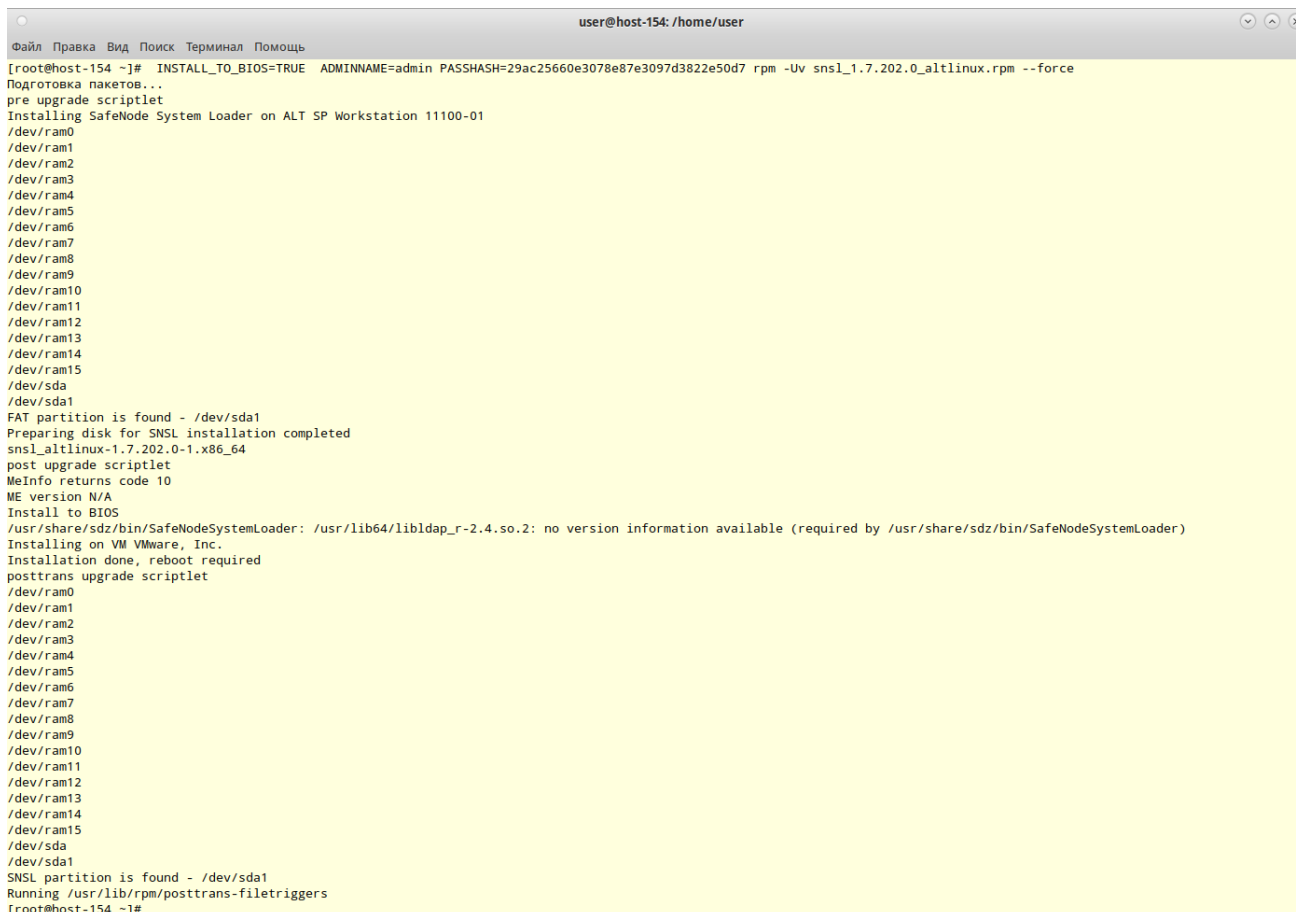


До завершения процесса установки изделия пользователям доступна загрузка ОС без настроенных механизмов защиты доверенной загрузки.

3.3.7 Для продолжения процесса установки необходимо загрузить операционную систему.

3.3.8 Для начала второго этапа установки необходимо указать команду на установку вместе с хеш-суммой пароля администратора (рисунок 3.7):

```
sudo INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d75 rpm -Uv sns1_altlinux.rpm --force
```



```
user@host-154: /home/user
[root@host-154 ~]# INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7 rpm -Uv sns1_1.7.202.0_altlinux.rpm --force
Подготовка пакетов...
pre upgrade scriptlet
Installing SafeNode System Loader on ALT SP Workstation 11100-01
/dev/ram0
/dev/ram1
/dev/ram2
/dev/ram3
/dev/ram4
/dev/ram5
/dev/ram6
/dev/ram7
/dev/ram8
/dev/ram9
/dev/ram10
/dev/ram11
/dev/ram12
/dev/ram13
/dev/ram14
/dev/ram15
/dev/sda
/dev/sda1
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
sns1_altlinux-1.7.202.0-1.x86_64
post upgrade scriptlet
MeInfo returns code 10
ME version N/A
Install to BIOS
/usr/share/sdz/bin/SafeNodeSystemLoader: /usr/lib64/libldap_r-2.4.so.2: no version information available (required by /usr/share/sdz/bin/SafeNodeSystemLoader)
Installing on VM VMware, Inc.
Installation done, reboot required
posttrans upgrade scriptlet
/dev/ram0
/dev/ram1
/dev/ram2
/dev/ram3
/dev/ram4
/dev/ram5
/dev/ram6
/dev/ram7
/dev/ram8
/dev/ram9
/dev/ram10
/dev/ram11
/dev/ram12
/dev/ram13
/dev/ram14
/dev/ram15
/dev/sda
/dev/sda1
SNSL partition is found - /dev/sda1
Running /usr/lib/rpm/posttrans-filetriggers
[root@host-154 ~]#
```

Рисунок 3.7 – Второй этап установки изделия

3.3.9 В процессе установки произойдет перезапись образа региона UEFI BIOS и во Flash-памяти будет расположен обновленный образ региона UEFI BIOS с добавленными модулями защиты изделия.

3.3.10 Эталонный регион образа UEFI BIOS будет сохранен на ESP раздел НЖМД.

Сохраненный регион образа UEFI BIOS необходим при удалении изделия, когда осуществляется обратная замена модифицированного образа UEFI BIOS на оригинальный образ.

3.3.11 После перезаписи региона UEFI BIOS осуществится автоматическая перезагрузка ЭВМ. Процесс установки завершен.

⁵ Хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512

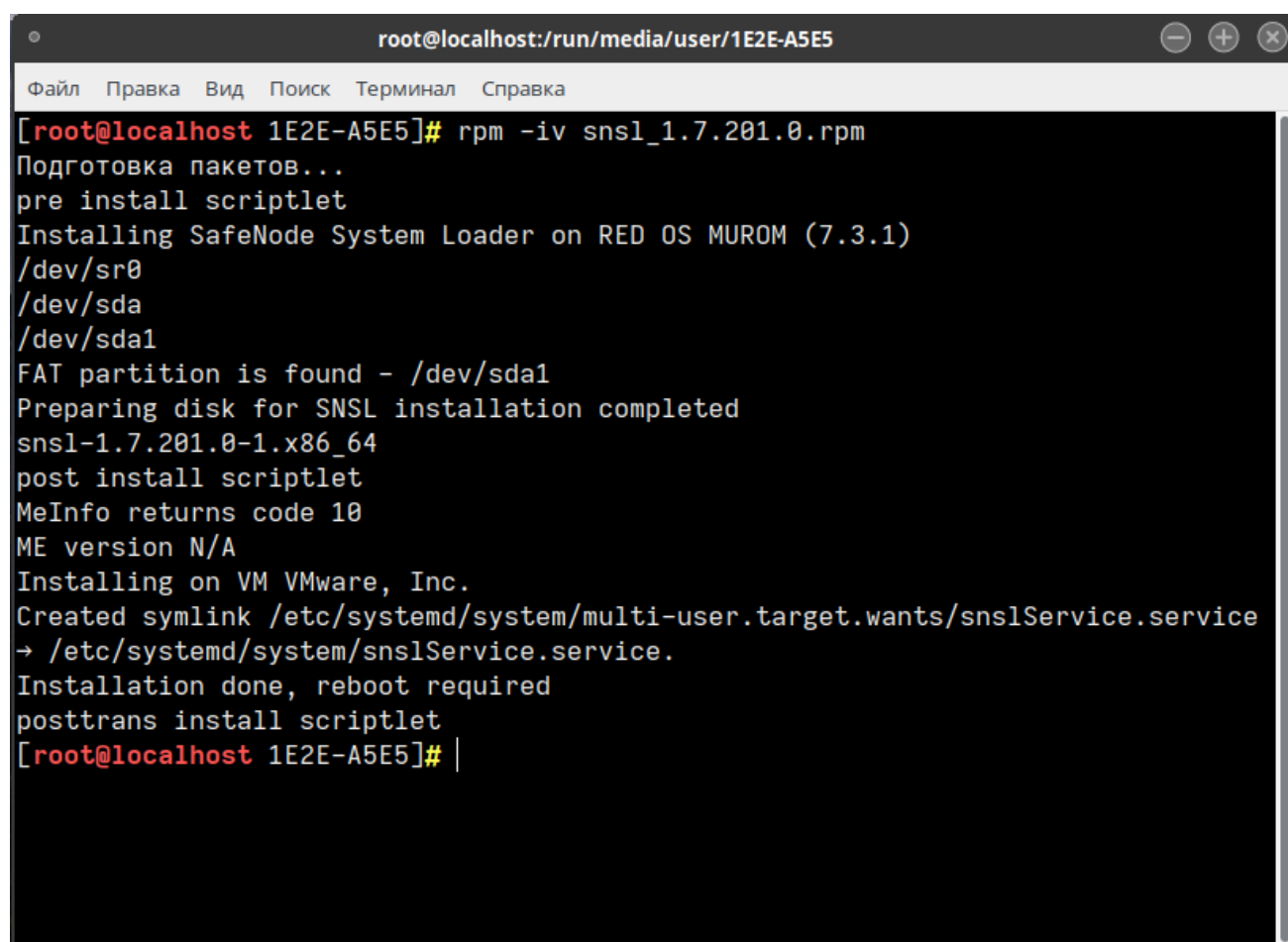
3.3.12 Если изделие было корректно установлено на ЭВМ и при этом не возникло сбоев в процессе установки, после перезагрузки ЭВМ появится информационное сообщение (рисунок 3.3).

3.4 Установка изделия на ОС РЕД ОС 7.3 Муром

3.4.1 Запустить консоль ОС РЕД ОС 7.3 Муром.

3.4.2 Для установки пакета выполнить следующую команду (рисунок 3.8).

```
sudo rpm -iv sns1.rpm
```



```
root@localhost:/run/media/user/1E2E-A5E5
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@localhost 1E2E-A5E5]# rpm -iv sns1_1.7.201.0.rpm
Подготовка пакетов...
pre install scriptlet
Installing SafeNode System Loader on RED OS MUROM (7.3.1)
/dev/sr0
/dev/sda
/dev/sda1
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
sns1-1.7.201.0-1.x86_64
post install scriptlet
MeInfo returns code 10
ME version N/A
Installing on VM VMware, Inc.
Created symlink /etc/systemd/system/multi-user.target.wants/sns1Service.service
→ /etc/systemd/system/sns1Service.service.
Installation done, reboot required
posttrans install scriptlet
[root@localhost 1E2E-A5E5]# |
```

Рисунок 3.8 – Первый этап установки изделия

3.4.3 В случае успеха появится надпись:

```
Installation done, reboot required
```

3.4.4 На данном этапе на ESP разделе НЖМД будут сохранены модули изделия и скопирована графическая консоль.

3.4.5 Если первый этап установки прошел корректно и при этом не возникло сбоев в процессе перезагрузки будет выведено сообщение (рисунок 3.2).

3.4.6 После перезагрузки ЭВМ появится информационное сообщение о работе изделия в режиме установки (рисунок 3.3).



До завершения процесса установки изделия пользователям доступна загрузка ОС без настроенных механизмов защиты доверенной загрузки.

3.4.7 Для продолжения процесса установки необходимо загрузить операционную систему.

3.4.8 Для начала второго этапа установки необходимо указать команду вместе с хеш-суммой пароля администратора (рисунок 3.9):

```
sudo env INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29ac2566  
0e3078e87e3097d3822e50d76 rpm -Uv <sns1>.rpm --force
```

```
root@localhost:/run/media/user/1E2E-A5E5
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@localhost 1E2E-A5E5]# env INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29
ac25660e3078e87e3097d3822e50d7 rpm -Uv sns1_1.7.201.0.rpm --force
Подготовка пакетов...
pre upgrade scriptlet
Installing SafeNode System Loader on RED OS MUROM (7.3.1)
/dev/sr0
/dev/sda
/dev/sda1
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
sns1-1.7.201.0-1.x86_64
post upgrade scriptlet
MeInfo returns code 10
ME version N/A
Install to BIOS
/usr/share/sdz/bin/SafeNodeSystemLoader: /lib64/libldap_r-2.4.so.2: no version i
nformation available (required by /usr/share/sdz/bin/SafeNodeSystemLoader)
Installing on VM VMware, Inc.
Installation done. reboot required
[root@localhost 1E2E-A5E5]# |
```

Рисунок 3.9 – Второй этап установки изделия

⁶ Хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512

3.4.9 В процессе установки произойдет перезапись образа региона UEFI BIOS и во Flash-памяти будет расположен обновленный образ региона UEFI BIOS с добавленными модулями защиты изделия.

3.4.10 Эталонный регион образа UEFI BIOS будет сохранен на ESP раздел НЖМД.

Сохраненный регион образа UEFI BIOS необходим при удалении изделия, когда осуществляется обратная замена модифицированного образа UEFI BIOS на оригинальный образ.

3.4.11 После перезаписи региона UEFI BIOS осуществится автоматическая перезагрузка ЭВМ. Процесс установки завершен.

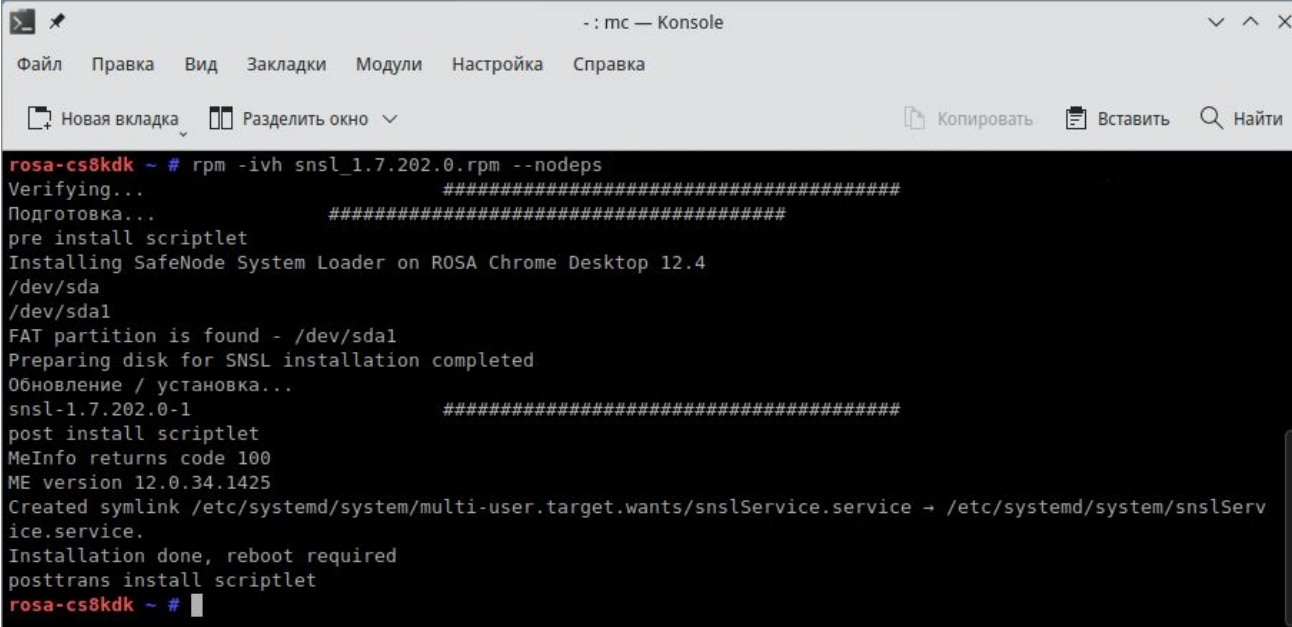
3.4.12 Если изделие было корректно установлено на ЭВМ и при этом не возникло сбоев в процессе установки, после перезагрузки ЭВМ появится информационное сообщение.

3.5 Установка изделия на ОС Роса «Хром»

3.5.1 Запустить консоль ОС Роса «Хром».

3.5.2 Для установки пакета выполнить следующую команду (рисунок 3.10).

```
sudo rpm -ivh sns1.rpm --nodeps
```



```
rosa-cs8kdk ~ # rpm -ivh sns1_1.7.202.0.rpm --nodeps
Verifying... #####
Подготовка... #####
pre install scriptlet
Installing SafeNode System Loader on ROSA Chrome Desktop 12.4
/dev/sda
/dev/sda1
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
Обновление / установка...
sns1-1.7.202.0-1 #####
post install scriptlet
MeInfo returns code 100
ME version 12.0.34.1425
Created symlink /etc/systemd/system/multi-user.target.wants/sns1Service.service -> /etc/systemd/system/sns1Service.service.
Installation done, reboot required
posttrans install scriptlet
rosa-cs8kdk ~ #
```

Рисунок 3.10 – Первый этап установки изделия

3.5.3 В случае успеха появится надпись:

```
Installation done, reboot required
```

3.5.4 На данном этапе на ESP разделе НЖМД будут сохранены модули изделия и скопирована графическая консоль.

3.5.5 Если первый этап установки прошел корректно и при этом не возникло сбоев в процессе перезагрузки будет выведено сообщение (рисунок 3.2).

3.5.6 После перезагрузки ЭВМ появится информационное сообщение о работе изделия в режиме установки (рисунок 3.3).



До завершения процесса установки изделия пользователям доступна загрузка ОС без настроенных механизмов защиты доверенной загрузки.

3.5.7 Для продолжения процесса установки необходимо загрузить операционную систему.

3.5.8 Для начала второго этапа установки необходимо указать команду вместе с хеш-суммой пароля администратора (рисунок 3.11):

```
sudo env INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29ac2566  
0e3078e87e3097d3822e50d77 rpm -Uv <sns1>.rpm --force --nodeps
```

```
bash — Konsole
Файл  Правка  Вид  Закладки  Модули  Настройка  Справка
Новая вкладка  Разделить окно  Копировать  Вставить  Найти

Добро пожаловать!
Для получения помощи введите в консоли: справка
user@rosa-cs8kdk ~ $ sudo -i
[sudo] пароль для user:
rosa-cs8kdk ~ # INSTALL_TO_BIOS=TRUE ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7 rpm -Uv sns1_1.7.202.0.rpm --force --nodeps
Verifying packages...
Подготовка пакетов...
pre upgrade scriptlet
Installing SafeNode System Loader on ROSA Chrome Desktop 12.4
/dev/sda
/dev/sda1
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
sns1-1.7.202.0-1.x86_64
post upgrade scriptlet
MeInfo returns code 100
ME version 12.0.34.1425
Install to BIOS
/usr/share/sdz/bin/SafeNodeSystemLoader: /usr/lib64/libldap_r-2.4.so.2: no version information available (required by /usr/share/sdz/bin/SafeNodeSystemLoader)
Installation done, reboot required
preun upgrade scriptlet
ADMINNAME=admin
PASSHASH=29ac25660e3078e87e3097d3822e50d7
sns1-1.7.202.0-1.x86_64
posttrans upgrade scriptlet
/dev/sda
/dev/sda1
SNSL partition is found - /dev/sda1
rosa-cs8kdk ~ #
```

Рисунок 3.11 – Второй этап установки изделия

⁷ Хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512

3.5.9 В процессе установки произойдет перезапись образа региона UEFI BIOS и во Flash-памяти будет расположен обновленный образ региона UEFI BIOS с добавленными модулями защиты изделия.

3.5.10 Эталонный регион образа UEFI BIOS будет сохранен на ESP раздел НЖМД.

Сохраненный регион образа UEFI BIOS необходим при удалении изделия, когда осуществляется обратная замена модифицированного образа UEFI BIOS на оригинальный образ.

3.5.11 После перезаписи региона UEFI BIOS осуществится автоматическая перезагрузка ЭВМ. Процесс установки завершен.

3.5.12 Если изделие было корректно установлено на ЭВМ и при этом не возникло сбоев в процессе установки, после перезагрузки ЭВМ появится информационное сообщение.

4 Ошибки установки

В случае появления ошибки в процессе второго этапа установки, дальнейшая установка возможна только при наличии аппаратного программатора.

Для установки изделия с использованием аппаратного программатора и специализированной утилиты для идентификации, чтения и записи flash-чипов понадобится дополнительная ЭВМ с ОС Linux.



Рекомендуется использовать следующие средства:

- программатор, подходящий для работы с flash-чипом BIOS, например, **CH341a_spi**;
- универсальная утилита **Flashrom**.

Описание процесса установки и удаления изделия приведено в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1» с использованием указанных средств.

После выключения ЭВМ, на которой произошла ошибка установки изделия, необходимо выполнить модификацию и запись модифицированного образа BIOS, воспользовавшись соответствующими скриптами⁸.



В случае успешного прохождения первого этапа установки инсталлятора, дополнительная установка NVRAM переменных не нужна.

⁸ Скрипты предоставляются производителем по запросу

4.1 Пример установки СДЗ на Lenovo ThinkCentre M79 (AMD)

Выполнить программную установку в два этапа на персональный компьютер **Lenovo ThinkCentre M79** (тип процессора – **AMD**) не представляется возможным, поэтому потребуется программатор и специализированная утилита.

Порядок установки:

- 1) Запустить инсталлятор для выполнения первого этапа установки (без самозащиты).
- 2) Перезагрузить компьютер, дождаться инициализации консоли СДЗ.



Второй этап установки невозможен из-за ограничений платформы. После перезагрузки консоль сохранит свою работу, и появится возможность записать модули самозащиты в прошивку вручную, через программатор.

- 3) Обесточить компьютер, снять образ с микросхемы, модифицировать его и залить обратно.



Выполнять скрипт записи NVRAM переменных не нужно!

4.1.1 Работа с программатором

Подробно работа с программатором модели «ch341a spi» в среде ОС Linux приведена в документе «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1», но есть небольшие отличия.

Сначала необходимо определить положение микросхемы с прошивкой, которая располагается рядом с SATA портами (на рисунке они красного цвета), и может быть скрыта переплетением кабелей (рисунки 4.1 и 4.2).



Рисунок 4.1 – Расположение микросхемы на примере открытого корпуса

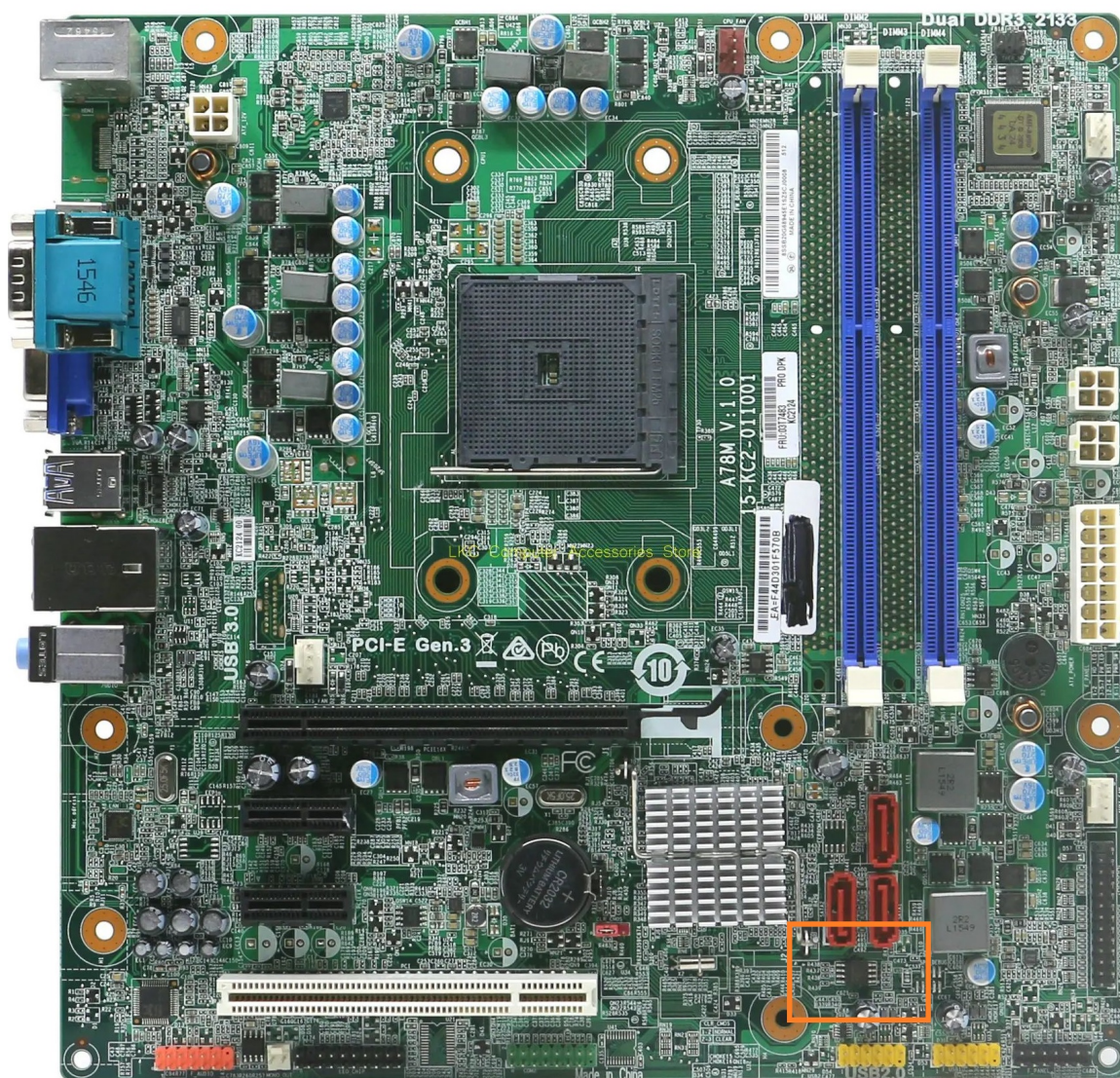


Рисунок 4.2 – Расположение микросхемы на примере фото материнской платы

Микросхема **MX25L6406E** на представленной плате (рисунок 4.3) имеет рабочее напряжение в 3 вольта, что не требует понижающего адаптера для программатора. **Но перед подключением рекомендуется проверить маркировку микросхемы на соответствие напряжению!**



Рисунок 4.3 – Маркировка микросхемы



Для корректного подключения к микросхеме может потребоваться отсоединение USB и SATA проводов от коннекторов для удобства работы.

Точка на корпусе показывает расположение первой ноги микросхемы, она же соответствует первому контакту на выводе программатора. Некоторые производители также маркируют первый контакт красным проводом на шлейфе (рисунок Рисунок 4.4).



Рисунок 4.4 – Пример подключения к микросхеме и расположение маркированного провода на шлейфе

После корректной установки клипсы на микросхему, следует выполнить проверку ее видимости программатором и утилитой. Для примера, команда в ОС Linux для утилиты flashrom:

```
sudo flashrom -p ch341a_spi
```

При корректной работе утилита определит микросхему и выдаст наименование. После можно приступить к чтению образа. Утилита может выдать запрос на принудительную идентификацию чипа и предложит варианты. Необходимо выбрать вариант с маркировкой микросхемы и ввести с параметром «-с», включая кавычки и все наименование между ними. Пример команды чтения:

```
sudo flashrom -p ch341a_spi -r bios.rom -c "MX25L6406E/MX25L6408E"
```

После чтения образа необходимо выполнить проверку на корректность считанного. Для большей надежности рекомендуется перед проверкой отключить и подключить заново клипсу на микросхему, это поможет выявить некорректность подключения к контактам в процессе чтения. Пример команды верификации образа:

```
sudo flashrom -p ch341a_spi -v bios.rom -c "MX25L6406E/MX25L6408E"
```

В случае успешной верификации, необходимо скопировать на USB-носитель и модифицировать с помощью скрипта **02_Modify** из среды EFI согласно инструкции, и залить обратно. Пример команды:

```
sudo flashrom -p ch341a_spi -w bios_mod.rom -c "MX25L6406E/MX25L6408E"
```

В процессе записи утилита сама проверит корректность залитого, после выдаст результат проверки. В случае успеха, необходимо вернуть компьютер в исходный вид и запустить. Условием работоспособности будет загрузка консоли СДЗ и перехват любых загрузок на носители в обход консоли.



Необходимо учитывать, что образ, снятый с одной платы, должен быть залит на эту же плату. Копирование одного образа на несколько плат имеет высокую вероятность повредить работоспособность их встроенного сетевого адаптера.

Для возможности оперативного восстановления работоспособности, рекомендуется сохранять снятые образы, и именовать их соответственно.

5 Настройка изделия

5.1 Для первоначальной настройки изделия необходимо выбрать пункт **«Администрирование СДЗ»** (рисунок 3.3) и дождаться появления окна аутентификации пользователя (рисунок 5.1).

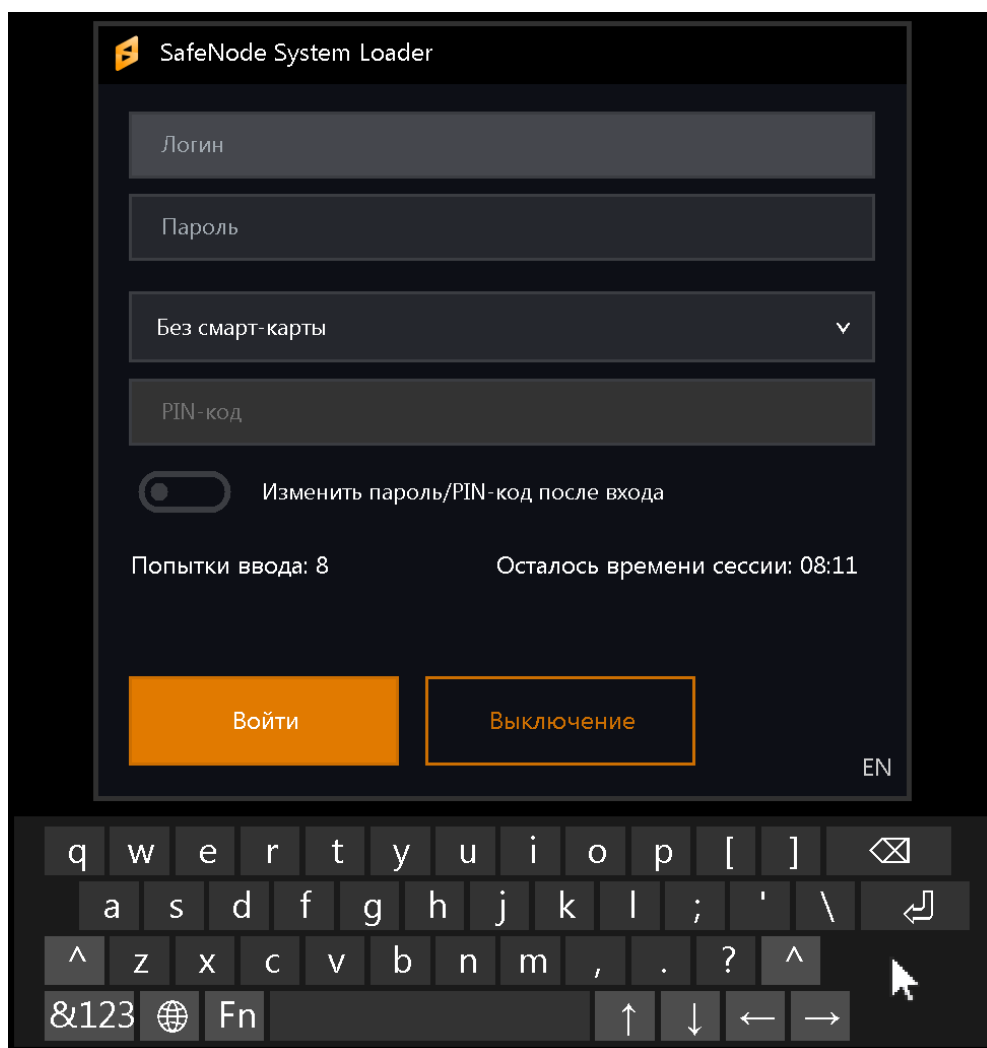


Рисунок 5.1 – Окно аутентификации пользователя

5.2 При первом входе АБ в окне с приглашением к идентификации и аутентификации пользователя (см. рис. 5.1) следует ввести имя пользователя **«admin»** и установленный по умолчанию пароль **«12345678»**.



В целях обеспечения безопасности после первого входа АБ осуществляется принудительная смена пароля, используемого по умолчанию.

При необходимости АБ также следует назначить АНП и PIN-код.

5.3 После успешной процедуры идентификации и аутентификации АБ появится информационное сообщение о необходимости смены аутентификационных данных АБ (рисунок 5.2).

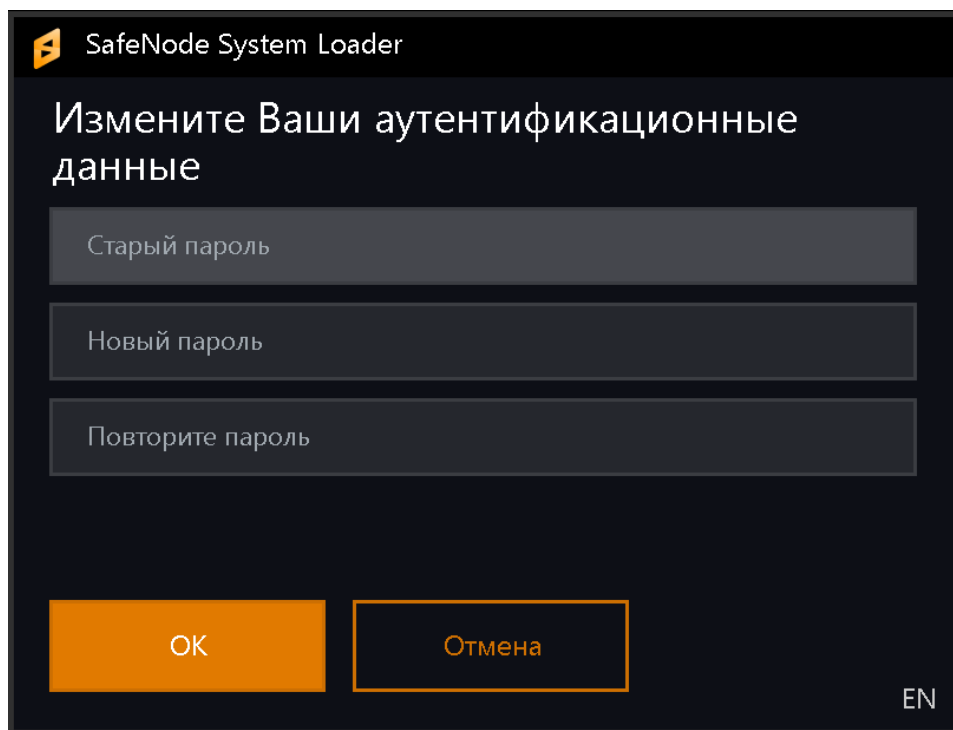



Рисунок 5.2 – Окно о необходимости смены аутентификационных данных АБ

5.4 Дальнейшие действия по принудительной смене аутентификационных данных администратора безопасности, конфигурированию параметров изделия указаны в документе «Средство доверенной загрузки «SafeNode System Loader» Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2».

5.5 Для завершения процесса установки и запрета загрузки ОС без процесса аутентификации пользователя, необходимо в **псевдографической консоли** выполнить переход: **Учетные записи пользователей** → **Редактирование**. Выбрать учетную запись **admin** из списка **Имя пользователя**. В появившемся диалоговом окне выбрать параметр **«Пароль восстановления»** и задать его (рисунок 5.3).

 Для обеспечения резервного копирования пароля восстановления, рекомендуется подключить мастер-ключ администратора.

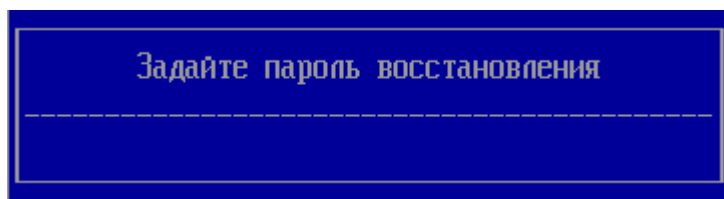


Рисунок 5.3 – Диалоговое окно «Ввода пароля восстановления»

5.6 Дальнейшие действия по завершению процесса, необходимо в **псевдографической консоли** выполнить переход: **Общие параметры** → **Основные настройки** (рисунок 5.4).

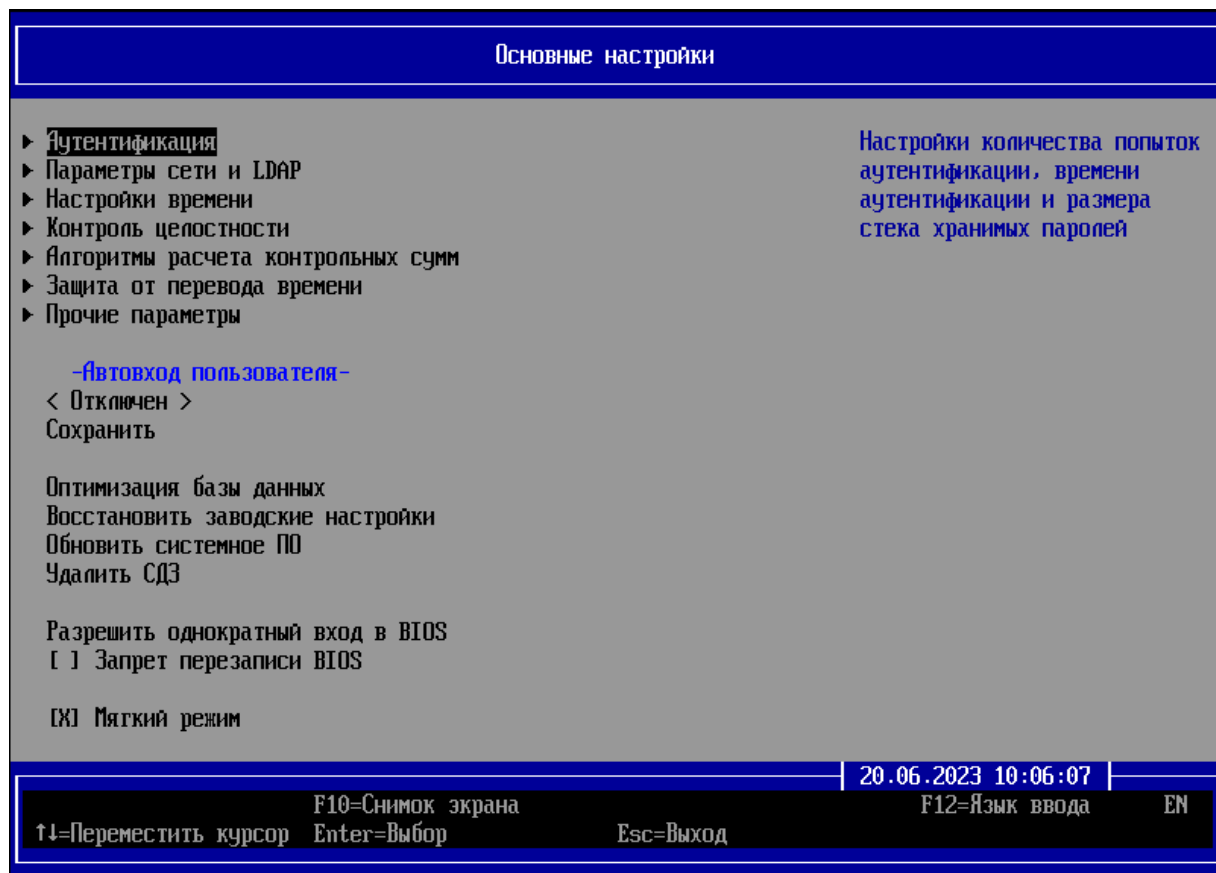


Рисунок 5.4 – Диалоговое окно «Основные настройки» псевдографической консоли

5.7 В появившемся диалоговом окне необходимо выбрать параметр **«Мягкий режим»** (рисунок 5.5).

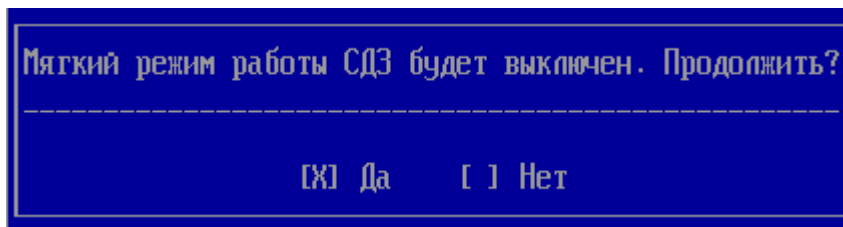


Рисунок 5.5 – Выбор параметра «Мягкий режим»

5.8 В диалоговом окне (см. рисунок 5.5) необходимо выбрать **«Да»**, при этом установка изделия завершена и изменения вступают в силу после перезагрузки ЭВМ (рисунок 5.6).

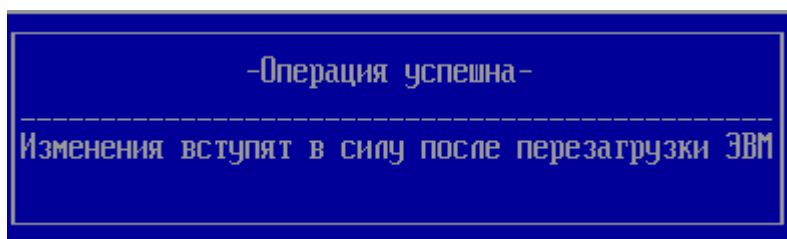


Рисунок 5.6 – Завершение установки СДЗ

5.9 Выйти из мягкого режима можно в **графической консоли СДЗ Linux (консоль АБ Linux)**, запускаемой по требованию АБ из среды ОС Linux, для этого необходимо загрузить ОС и выполнить команду (рисунок 5.7):

```
sudo /usr/share/sdz/bin/SafeNodeSystemLoader
```

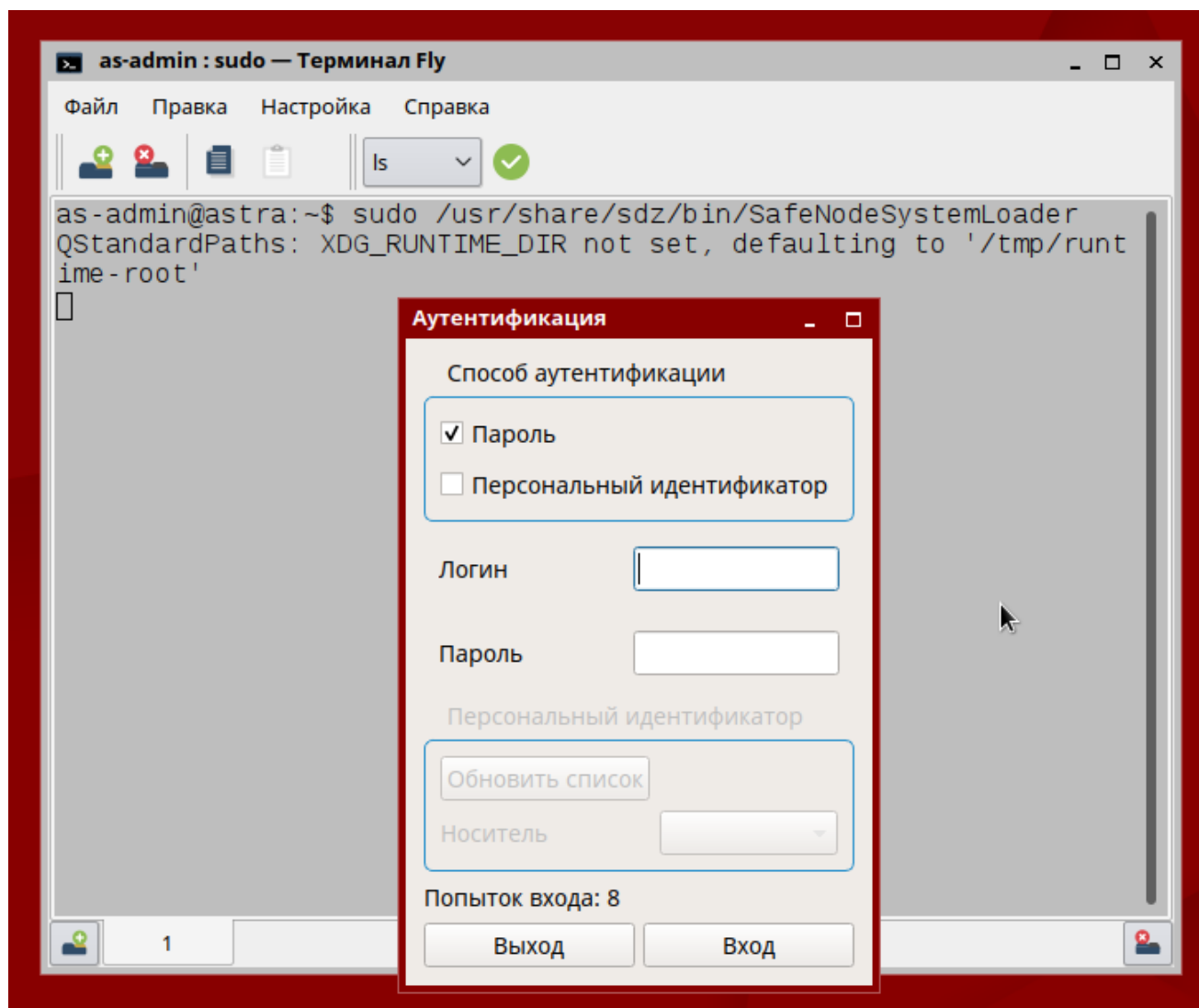


Рисунок 5.7 – Аутентификация в графической консоли СДЗ Linux

5.10 В окне аутентификации консоли АБ Linux необходимо ввести аутентификационные данные АБ, указанные при первичной настройке изделия в псевдографической консоли (рисунок 5.8).

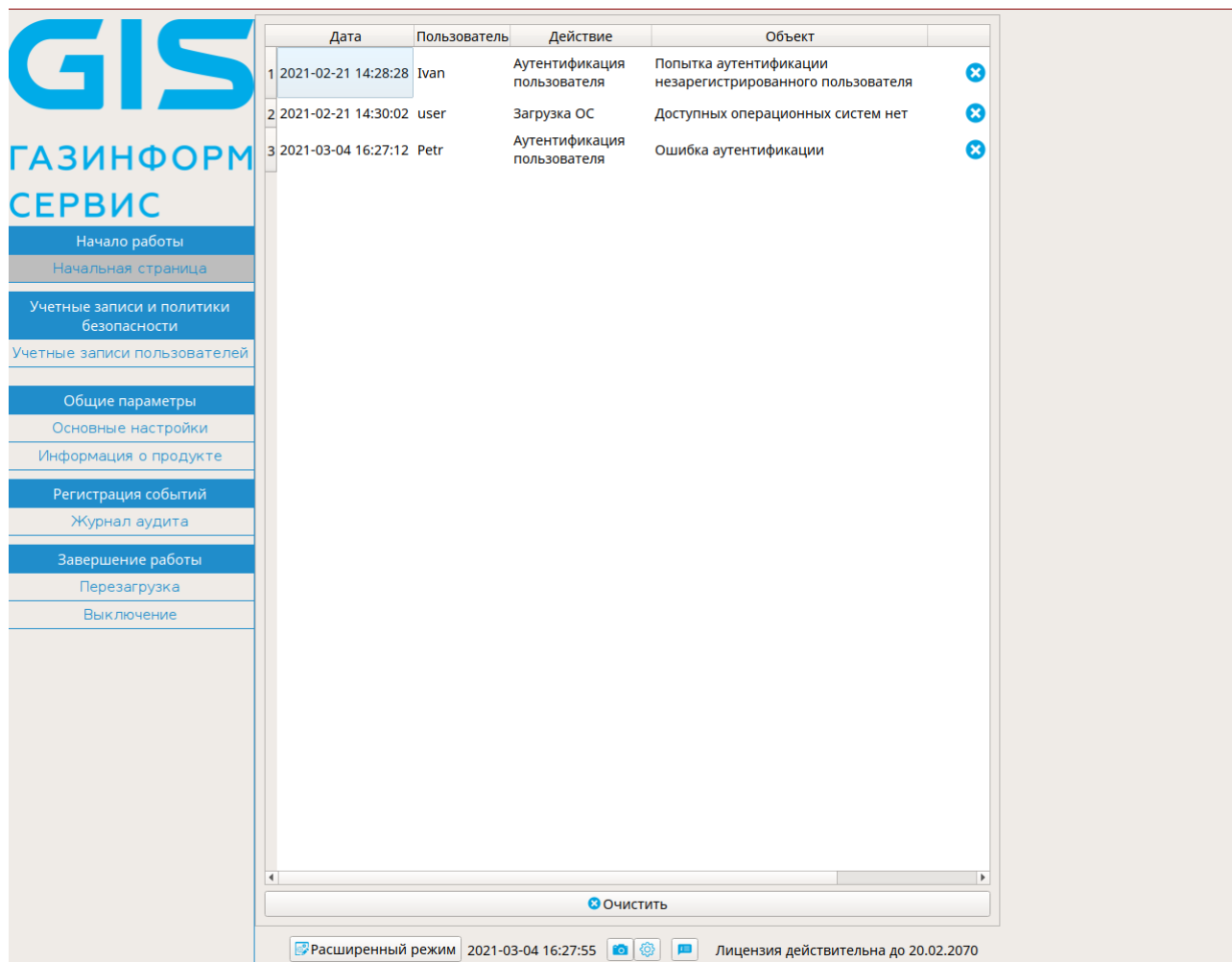
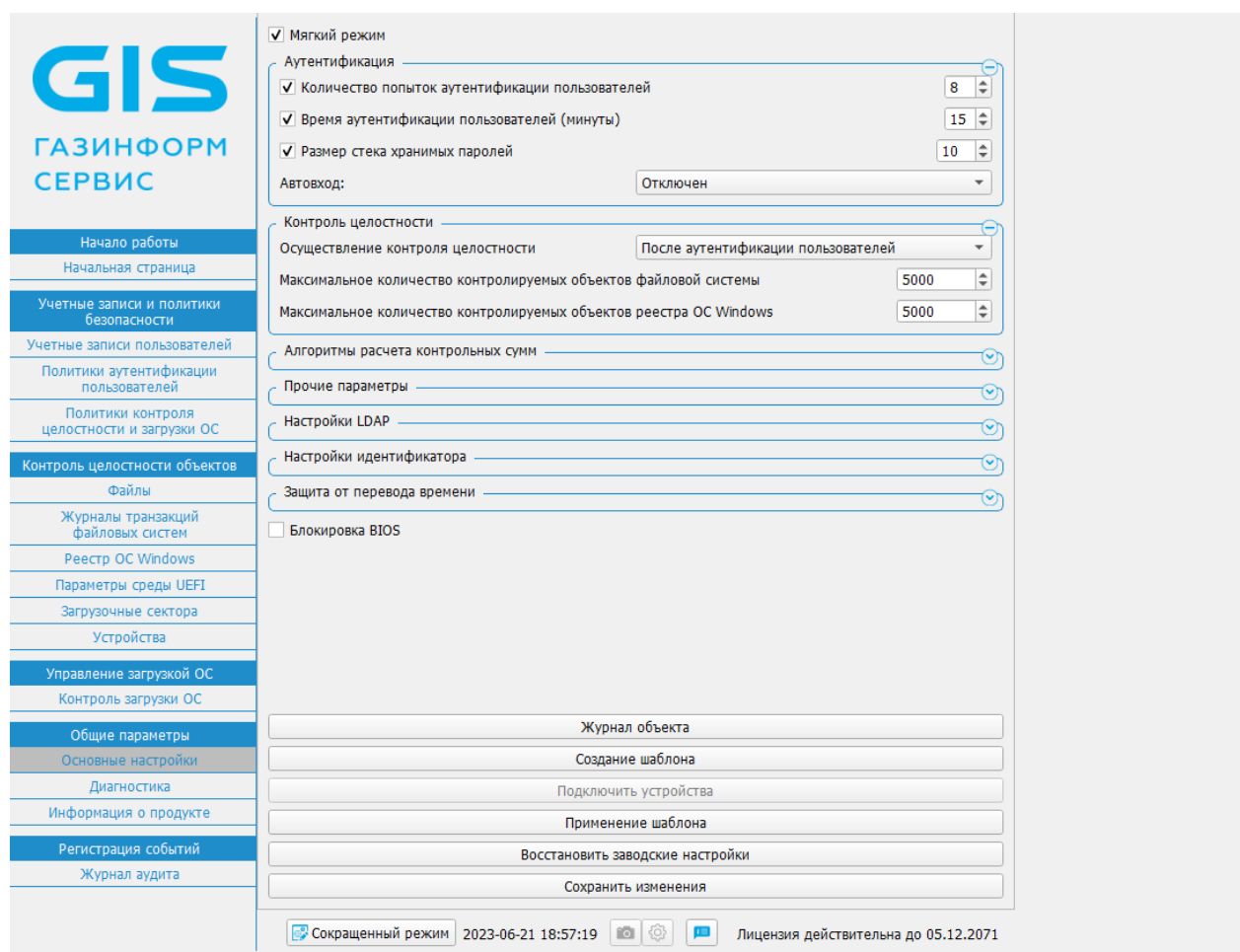


Рисунок 5.8 – Интерфейс консоли АБ в ОС Linux

5.11 В появившейся графической консоли необходимо установить расширенный режим отображения элементов интерфейса и выполнить переход **Общие параметры** → **Основные настройки** (рисунок 5.9).

Рисунок 5.9 – Содержимое окна «**Основные настройки**»

5.12 В верхней части окна расположено поле «**Мягкий режим**». Для выхода мягкого режима необходимо снять отметку напротив данного поля и сохранить изменения.

5.13 При первом выходе из мягкого режима необходимо сменить пароль восстановления, который будет использоваться для безопасного восстановления ПО в случае сбоев и отказов.



В целях обеспечения безопасности при первом выходе из мягкого режима осуществляется принудительная смена пароля восстановления, используемого по умолчанию.

5.14 Процесс смены пароля восстановления, в зависимости от консоли администратора, описан в соответствующих руководствах.

6 Активация лицензии



Активация изделия возможна на любом этапе установки изделия.

5.1. После установки изделия для разблокировки его полнофункциональной версии необходима активация лицензии. Активация изделия осуществляется после доверенной загрузки ОС пользователем. Для этого необходимо запустить приложение **SafeNodeSystemLoader**. Ярлык для данного приложения создается автоматически в основном меню операционной системы. Ниже приведен порядок онлайн активации лицензии.

5.2. После запуска приложения **SafeNodeSystemLoader** на экране ЭВМ появится диалоговое окно (рисунок 6.1).

SafeNodeSystemLoader

Благодарим за установку SafeNode System Loader.

Лицензия не действительна. Для работы в полнофункциональном режиме необходима активация лицензии.

XXXXXX-XXXXXX-XXXXXX-XXX

Ключ лицензии

example@domain.com

Электронная почта

Нет ключа лицензии? [Купить](#)

Ограниченный режим

Активация

Рисунок 6.1 – Окно активации продукта

5.3. В диалоговом окне следует ввести ключ лицензии из входящей в комплект поставки изделия лицензии и адрес электронной почты для получения ключа активации, при этом окно (см. рис. 6.1) примет вид (рисунок 6.2).

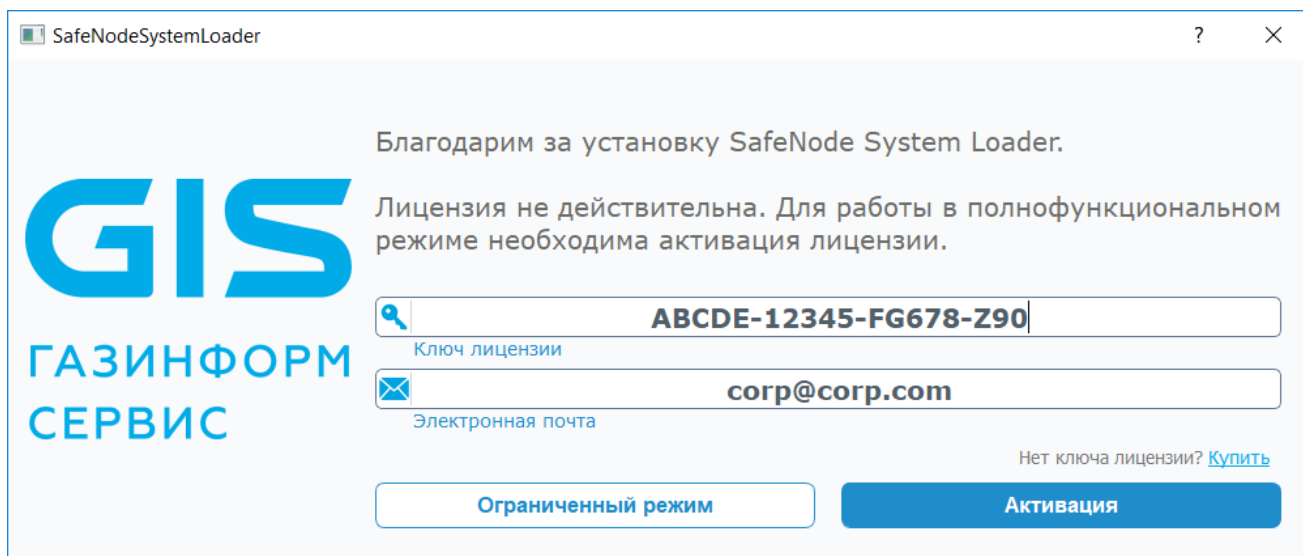


Рисунок 6.2 – Окно активации продукта

После нажатия кнопки «Активация» окно (см. рис. 6.2) примет вид (рисунок 6.3).

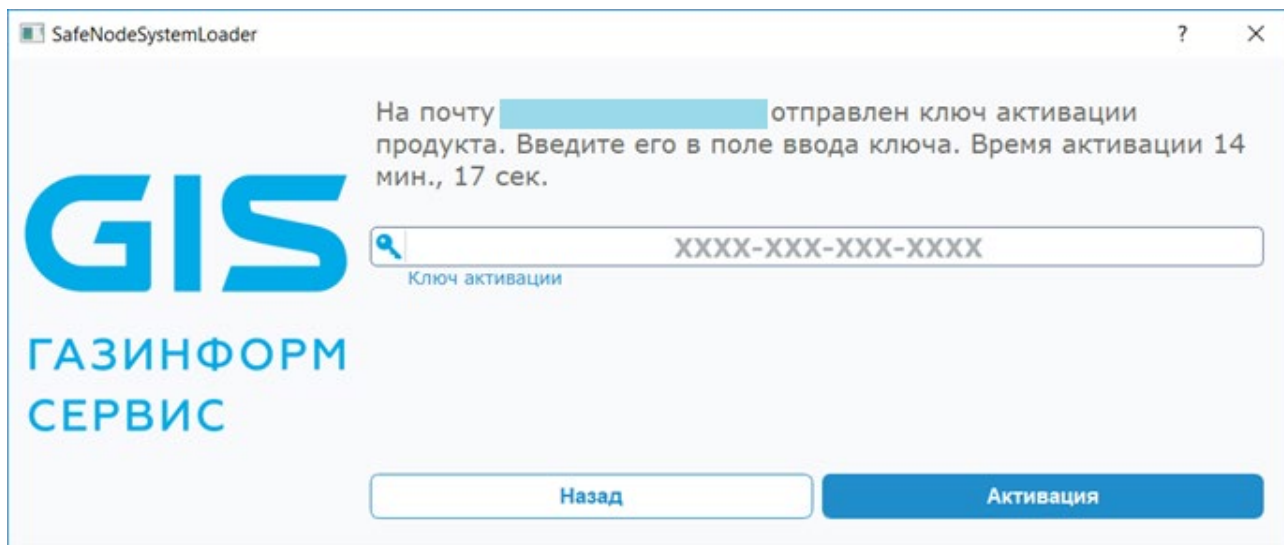


Рисунок 6.3 – Ввод ключа активации

5.4. На адрес электронной почты, указанной при активации лицензии (см. рис. 6.2), будет отправлено письмо с ключом активации (рисунок 6.4).

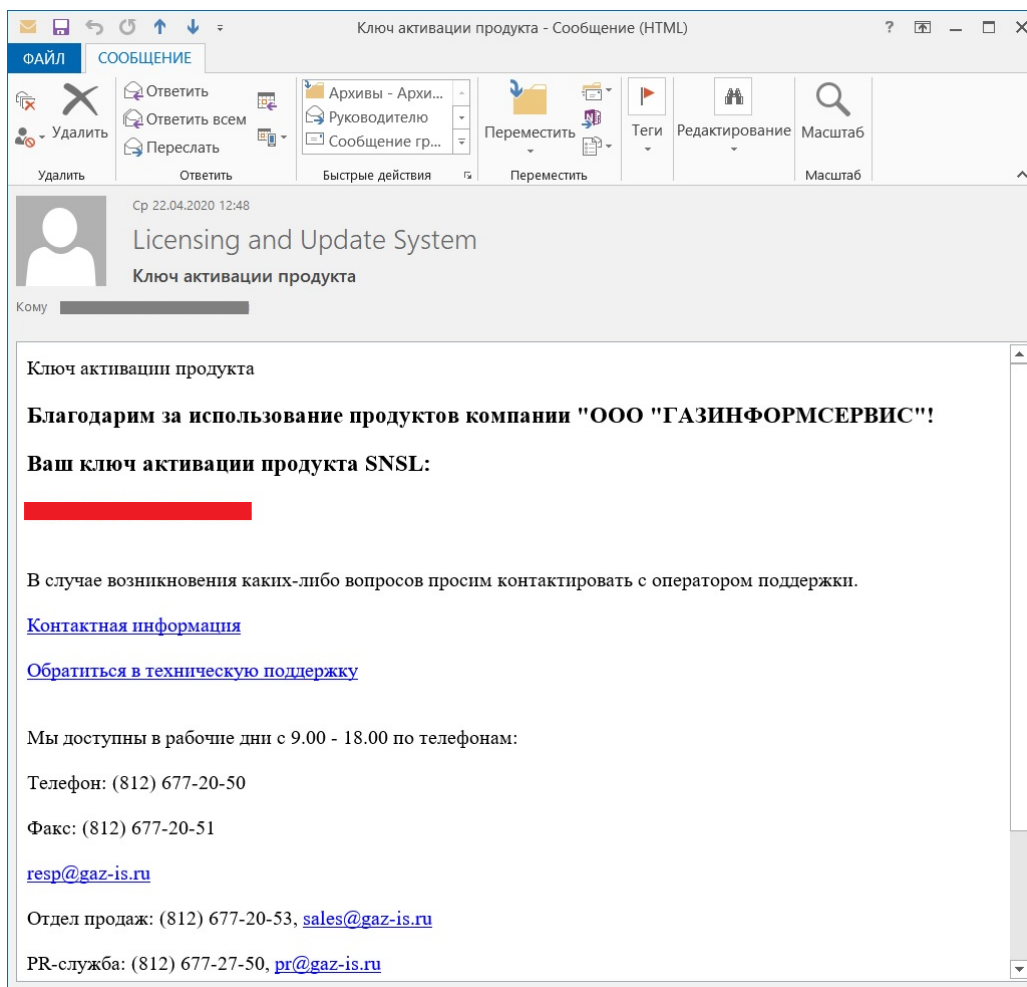


Рисунок 6.4 – Пример письма с ключом активации

5.5. В диалоговом окне (рисунок 6.5) следует указать полученный ключ активации (см. рис. 6.4) и нажать кнопку **«Активация»**

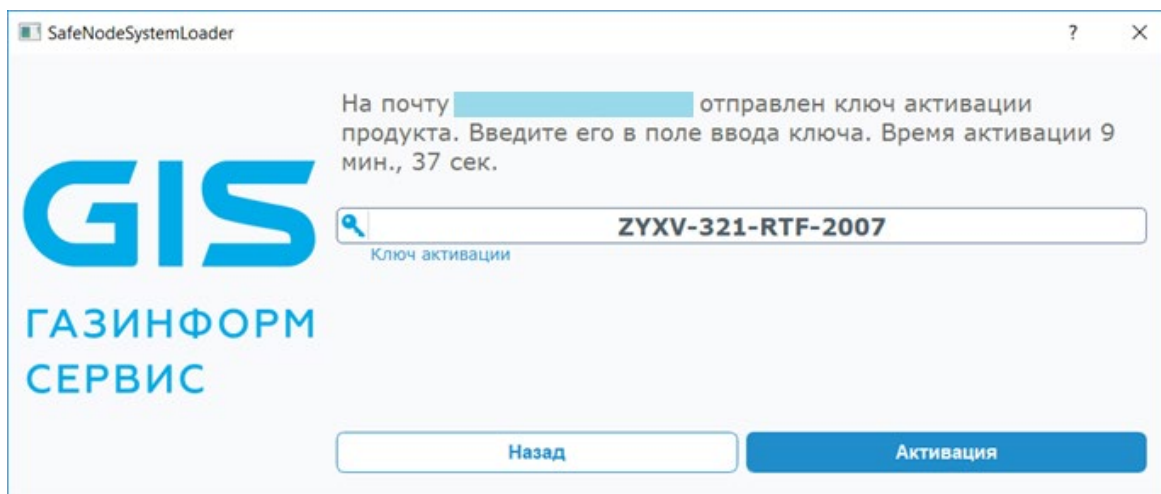


Рисунок 6.5 – Ввод ключа активации

5.6. После ввода ключа активации диалоговое окно (рисунок 5.5) примет вид (рисунок 6.6).

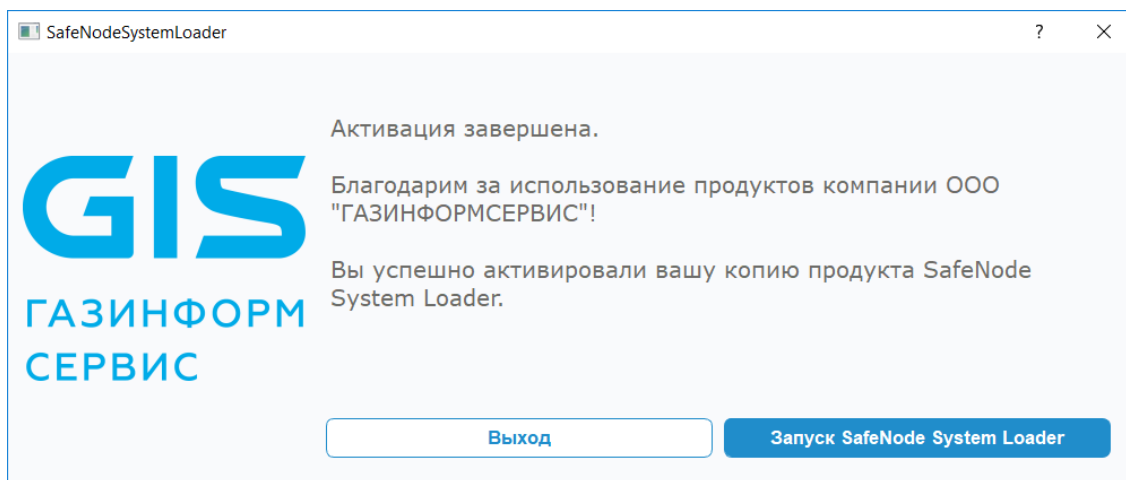


Рисунок 6.6 – Успешная активация лицензии

Нажатие кнопки «Запуск SafeNode System Loader» приведет к появлению на экране ЭВМ диалогового окна (рисунок 5.8).

5.7. На адрес электронной почты, указанной при активации лицензии (см. рис. 6.2), будет отправлено письмо с лицензионным ключом (рисунок 6.7).

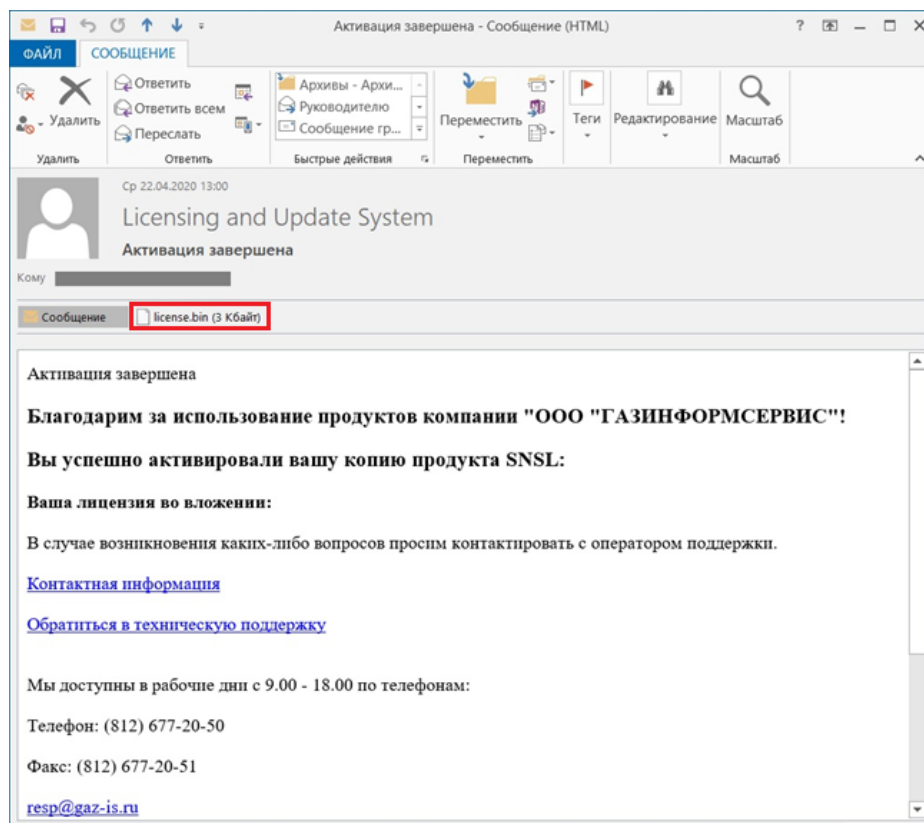


Рисунок 6.7 – Пример письма с лицензией

7 Удаление изделия



Удаление изделия возможно на любом этапе установки изделия.

7.1 Для удаления изделия из среды ОС Astra Linux SE необходимо запустить консоль и выполнить следующую команду (рисунок 7.1):

```
sudo ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7  
dpkg -r snsl
```

```
root@astra:/home/astra# ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7 dpkg -r snsl  
(Чтение базы данных ... на данный момент установлено 167296 файлов и каталогов.)  
Удаляется snsl (1.7.201.0) ...  
prerm remove  
ADMINNAME=admin  
PASSHASH=29ac25660e3078e87e3097d3822e50d7  
/dev/sr0  
/dev/sda  
/dev/sda1  
SNSL partition is found - /dev/sda1  
Uninstallation done, reboot required
```

Рисунок 7.1 – Удаление изделия из ОС Astra Linux SE 1.7



Удаление изделия из ОС осуществляется с передачей в dpkg аутентификационных данных администратора, где

PASSHASH=29ac25660e3078e87e3097d3822e50d7 – хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512

7.2 В случае успеха появится следующая надпись:

```
Uninstallation done, reboot required
```

7.3 После удаления изделия необходимо выполнить перезагрузку ЭВМ. Следующая загрузка ОС осуществиться в штатном режиме.



Для высчитывания хэш-суммы пароля рекомендуется использовать следующий скрипт, который необходимо сохранить с расширением sh:

```
#!/bin/bash
```

```
cat $1 | iconv -t UCS-2 -f UTF-8 | md5sum | cut -d" " -f1
```

Передать скрипту аргументом имя файла с паролем. Файл необходимо предварительно создать и вписать пароль вручную (перед сохранением,

убедитесь, что отсутствует перевод строки в конце созданного файла).

Получившийся хеш необходимо использовать для удаления изделия.

Запуск скрипта осуществляется с правами суперпользователя.

7.4 Для удаления установленного изделия из среды ОС Альт 8 СП необходимо запустить консоль и выполнить следующую команду (рисунок 7.2):

```
sudo env ADMINNAME=admin PASSHASH=21dcfb1487eb7469d922289a26b534d59 rpm -ev snsl
```

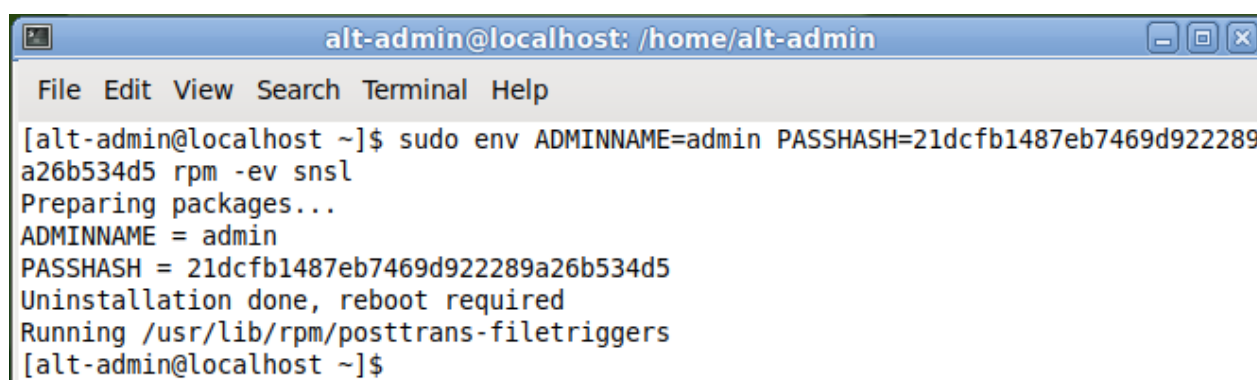


Рисунок 7.2 – Удаление изделия из ОС Альт 8 СП

7.5 После удаления изделия необходимо выполнить перезагрузку ЭВМ. Следующая загрузка ОС осуществиться в штатном режиме.

7.6 Если второй этап установки завершился с ошибками и дальнейшая установка выполнялась с использованием аппаратного программатора, то в команду удаления изделия из среды ОС Linux, необходимо добавить переменную FORCE=TRUE:

```
sudo env FORCE=TRUE ADMINNAME=admin PASSHASH=21dcfb1487eb7469d922289a26b534d5 rpm -ev snsl
```

Откат прошивки в исходное состояние при этом так же выполняется с использованием аппаратного программатора.

⁹ Хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512

8 Обновление изделия



Поддерживается обновление с версии 1.6 на версию 1.7. Для выполнения обновления необходимо, чтобы установка предыдущей версии была полностью завершена.

8.1 Для обновления установленного изделия из среды ОС Astra Linux SE 1.7 необходимо запустить консоль и выполнить следующую команду (рисунок 8.1):

```
sudo ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7  
dpkg -i snsl.deb
```

```
root@astra:/run/user/1000/media/by-id-usb-Kingston_DataTraveler_3.0_E0D55E6B646416817830178C-0:0-part1# ADMINNAME=admin PASS  
HASH=29ac25660e3078e87e3097d3822e50d7 dpkg -i snsl_1.7.201.0.deb  
(Чтение базы данных ... на данный момент установлен 167291 файл и каталог.)  
Подготовка к распаковке snsl_1.7.201.0.deb ...  
ADMINNAME=admin  
PASSHASH=29ac25660e3078e87e3097d3822e50d7  
prerm-upgrade  
preinst upgrade 1.6.405.0  
Installing SafeNode System Loader on Astra Linux  
FAT partition is found - /dev/sda1  
Preparing disk for SNSL installation completed  
Распаковывается snsl (1.7.201.0) на замену (1.6.405.0) ...  
Настраивается пакет snsl (1.7.201.0) ...  
postinst configure 1.6.405.0  
Astra Linux 1.7_x86_64 detected - try to install public key  
gpg: создан каталог '/root/.gnupg'  
gpg: создан щит с ключами '/root/.gnupg/pubring.kbx'  
gpg: key FF90858EBA78FA1E: 1 подпись не проверена за отсутствием ключа  
gpg: /root/.gnupg/trustdb.gpg: создана таблица доверия  
gpg: ключ FF90858EBA78FA1E: импортирован открытый ключ "000 "Газинформсервис" (key for signing) <resp@gaz-is.ru>"  
gpg: Всего обработано: 1  
gpg: импортировано: 1  
gpg: абсолютно доверенных ключей не найдено  
MeInfo returns code 10  
ME version N/A  
Installing on VM VMware, Inc.  
Installation done, reboot required
```

Рисунок 8.1 – Обновление изделия из ОС Astra Linux SE 1.7



Обновление изделия осуществляется с передачей в dpkg аутентификационных данных администратора, где:

PASSHASH=29ac25660e3078e87e3097d3822e50d7 – хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512

8.2 Процесс обновления аналогичен процессу установки, новая версия устанавливается поверх существующей.

8.3 В случае успеха появится следующая надпись:

```
Installation done, reboot required
```

8.4 После обновления изделия необходимо выполнить перезагрузку ЭВМ.



Обновление изделия не приводит к удалению информации из БД изделия.

8.5 Для обновления установленного изделия из среды ОС РЕД ОС 7.3 Муром необходимо запустить консоль и выполнить следующую команду (рисунок 8.2):

```
sudo env ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d710 rpm -Uvh sns1.rpm
```

```
root@localhost:run/media/user/1E2E-A5E5
[root@localhost 1E2E-A5E5]# env ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7 rpm -Uvh sns1_1.7.201.0.rpm
Подготовка... ##### [100%]
pre upgrade scriptlet
Installing SafeNode System Loader on RED OS MURUM (7.3.1)
/dev/sr0
/dev/sda
/dev/sda1
FAT partition is found - /dev/sda1
Preparing disk for SNSL installation completed
Обновление / установка... ##### [50%]
1:sns1-1.7.201.0-1
post upgrade scriptlet
MeInfo returns code 10
ME version N/A
/usr/share/sdz/bin/SafeNodeSystemLoader: /lib64/libldap_r-2.4.so.2: no version information available (required by /usr/share/sdz/bin/SafeNodeSystemLoader)
Installing on VM VMware, Inc.
Created symlink /etc/systemd/system/multi-user.target.wants/sns1Service.service -> /etc/systemd/system/sns1Service.service.
Installation done, reboot required
preun upgrade scriptlet
ADMINNAME = admin
PASSHASH = 29ac25660e3078e87e3097d3822e50d7
Очистка / удаление... ##### [100%]
2:sns1-1.6.405.0-1
posttrans upgrade scriptlet
/dev/sr0
/dev/sda
/dev/sda1
SNSL partition is found - /dev/sda1
/usr/share/sdz/bin/SafeNodeSystemLoader: /lib64/libldap_r-2.4.so.2: no version information available (required by /usr/share/sdz/bin/SafeNodeSystemLoader)
Update done - reboot required
[root@localhost 1E2E-A5E5]#
```

Рисунок 8.2 – Обновление изделия из ОС РЕД ОС 7.3 Муром

8.6 После обновления изделия необходимо выполнить перезагрузку ЭВМ.

¹⁰ Хеш-сумма пароля администратора, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD5, SHA1, SHA256, SHA384, SHA512

Перечень сокращений

BIOS	–	Basic Input Output System
CSM	–	Compatibility Support Module
ESP	–	EFI System Partition
GPT	–	GUID Partition Table
PCI-E	–	Peripheral Component Interconnect Express
PIN	–	Personal Identification Number
SATA	–	Serial ATA
SSD	–	Solid-State Drive
UEFI	–	Unified Extensible Firmware Interface
АБ	–	администратор безопасности
АНП	–	аутентификационный носитель пользователя
НЖМД	–	накопитель на жестких магнитных дисках
ОС	–	операционная система
ПО	–	программное обеспечение
СДЗ	–	средство доверенной загрузки
ЭВМ	–	электронно-вычислительная машина