ViPNet SafeBoot

Руководство администратора

infotecs

ФРКЕ.00180-02 32 01, версия 2.0.0.22

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, дом 1/23, строение 1

Тел: (495) 737-61-96 (горячая линия), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: (http://www.infotecs.ru)

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В данном документе описывается функциональное назначение и применение программного комплекса «Программный модуль доверенной загрузки ViPNet SafeBoot» ФРКЕ.00180-02 (далее — ViPNet SafeBoot), принципы работы и основные возможности, содержится информация, необходимая для настройки и использования ViPNet SafeBoot, а также приводится описание пользовательского интерфейса.

Для кого предназначен документ

Настоящее руководство предназначено для администраторов, отвечающих за безопасность, настройку и установку программного обеспечения на рабочих местах пользователей.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша + Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
Код	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О ViPNet SafeBoot

Областью применения ViPNet SafeBoot является построение автоматизированных систем, предназначенных для обработки информации ограниченного доступа, путем обеспечения доверенной загрузки операционной системы.

Назначение ViPNet SafeBoot

Программный комплекс ViPNet SafeBoot предназначен для идентификации и аутентификации пользователей, разграничения доступа на основе ролей, а также организации доверенной загрузки операционной системы.

ViPNet SafeBoot обеспечивает повышение уровня безопасности работы путем:

- Авторизации на уровне BIOS до загрузки основных компонентов операционной системы.
- Контроля целостности на уровне BIOS, защищаемых компонентов операционной системы и аппаратного обеспечения.
- Блокировки загрузки нештатной копии операционной системы.

Состав ViPNet SafeBoot

В состав ViPNet SafeBoot входят модули, реализующие:

- Доступ к базе данных конфигурации изделия.
- Чтение и запись конфигурационных параметров.
- Функции записи в журнал событий для всех компонентов системы.
- Контроль целостности параметров.
- Интерфейс аутентификации пользователя по электронному идентификатору, по паролю, по паролю и электронному идентификатору, по паролю на электронном идентификаторе, аутентификация пользователя, зарегистрированного на LDAP.

Системные требования

Требования к компьютеру, предназначенному для установки ViPNet SafeBoot:

- Процессор — x86-совместимый с поддержкой режима x86-64 (AMD64/Intel64), частота от 500 МГц.
- Системная плата — определяется исполнением ViPNet SafeBoot, совместимостью с используемым процессором. BIOS платы должен соответствовать спецификации UEFI версии: 2.3.1, 2.4, 2.5, 2.6, 2.7.

- Объем оперативной памяти — не менее 1 Гбайт.
- Жесткий диск — объем диска определяется требованиями установленной операционной системы (ОС).

Механизм защиты BIOS (в части защиты микросхемы BIOS от перезаписи) поддерживается для следующих поколений процессоров:

Семейство процессоров	Примечание
Intel SandyBridge	SandyBridge M/H (Client), SandyBridge E/EN/EP (Server)
Intel IvyBridge	IvyBridge M/H/Gladden (Client), IvyBridge E/EN/EP/EX (Server)
Intel Haswell	Haswell, Crystal Well, Haswell ULT, Haswell EP/EX
Intel Broadwell	Broadwell ULT, Broadwell H, Broadwell EP/EX, Broadwell DE
Intel Skylake	Skylake SP, Skylake ULT/ULX, Skylake DT/HALO
Intel Kabylake	Kabylake U/Y, Kabylake DT/HALO
Intel Coffeelake	CoffeeLake H/S, CoffeeLake U
Intel Cannonlake	CannonLake U/Y, CannonLake DT/HALO
Intel Rangeley	Atom C2000
Intel Baytrail	BayTrail I/M/D
Intel Braswell	Braswell N/J
Intel Apollolake	ApolloLake E/N/J
Intel Geminilake	GeminiLake N/J
Intel Whiskeylake	Whiskey Lake U/Y

Примечание. При использовании ПМДЗ ViPNet SafeBoot на платформах с другими чипсетами необходимо обеспечить невозможность перезаписи микросхемы BIOS другими средствами, если это не выполнено производителем платформы.

Комплект поставки

В комплект поставки ViPNet SafeBoot входит:

- Программный комплекс «Программный модуль доверенной загрузки ViPNet SafeBoot» ФРКЕ.00180-02.
- Формуляр ФРКЕ.00180-02 30 01 ФО.
- Документация в формате PDF, в том числе:
  - «ViPNet SafeBoot. Руководство администратора».
  - «ViPNet SafeBoot. Руководство пользователя».
  - «ViPNet SafeBoot. Руководство по установке».
  - Копия сертификата соответствия ФСТЭК России.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

8 (495) 737-6196,

8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения http://infotecs.ru/disclosure.php.

1

Общие сведения

Основные возможности ViPNet SafeBoot

Основные возможности ViPNet SafeBoot представлены в таблице ниже.

Функциональная возможность	Ссылка
Идентификация и аутентификация пользователей. Обеспечение идентификации и аутентификации зарегистрированных пользователей	Идентификация и аутентификация пользователей на стр. 15
Доверенная загрузка операционной системы. Обеспечение загрузки компонентов операционной системы только с определенных носителей, назначенных администратором, предоставление администратору возможности выбора режима загрузки ОС	Управление режимами загрузки операционной системы на стр. 77
Контроль целостности. Обеспечение целостности собственного программного обеспечения, образа BIOS и других компонентов	Контроль целостности на стр. 86
Управление учетными записями пользователей. Создание, редактирование и удаление учетных записей пользователей	Управление учетными записями пользователей на стр. 104
Управление настройками аутентификации. ViPNet SafeBoot позволяет задать настройки сессии аутентификации	Ограничение сессии аутентификации на стр. 56
Удаленное управление. Предоставляет функции удаленного управления ПК и настройками ViPNet SafeBoot	Удаленное управление на стр. 67
Управление сертификатами. Обеспечение загрузки корневых сертификатов и списка отзыва сертификатов	Управление сертификатами на стр. 141
Проверка и установка обновлений. Автоматический поиск файла обновления и установка обновлений посредством меню управления настройками	Обновление на стр. 29
Экспорт и импорт настроек ViPNet SafeBoot.	Экспорт настроек на стр. 59 Импорт настроек на стр. 75
Ведение журнала событий. Регистрация всех значимых событий безопасности и действий пользователя.	Управление журналом событий на стр. 171

Идентификация и аутентификация пользователей

Идентификация пользователей осуществляется по логину — имени пользователя, зарегистрированному в ViPNet SafeBoot.

В ViPNet SafeBoot пользователю может быть назначен один из следующих способов аутентификации:

- Пароль.
- Электронный идентификатор.
- Сочетание способов электронный идентификатор и пароль.
- Пароль на электронном идентификаторе.
- Пароль на LDAP.

Пароль может содержать от 4 до 32 символов для обычного пользователя и от 8 до 32 для администратора и аудитора.

Примечание. Срок действия пароля может быть ограничен.

Если администратор установил ограничение на срок действия пароля, то за 7 дней до истечения заданного периода будет выводиться соответствующе сообщение о необходимости смены пароля. Если по истечении семидневного периода пароль не будет изменен, то пользователь будет блокирован. При этом загрузка ОС блокирована не будет.

Электронный идентификатор представляет собой специальное USB-устройство, содержащее личный сертификат пользователя, а также закрытый ключ, соответствующий публичному ключу, содержащемуся в сертификате.

Форматы сертификата, используемые в ViPNet SafeBoot — X.509 (DER или PEM) и PKCS#7.

В ViPNet SafeBoot поддерживаются следующие электронные идентификаторы в формате USB-токенов: Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен Lite, JaCarta PKI, JaCarta-2 ГОСТ, JaCarta PKI/ГОСТ, JaCarta-2 PKI/ГОСТ, Guardant ID. Комбинированные идентификаторы JaCarta PKI/ГОСТ поддерживаются только в режиме PKI, работа с ними полностью аналогична JaCarta PKI. Комбинированные идентификаторы JaCarta-2 PKI/ГОСТ поддерживаются только в режиме ГОСТ, работа с ними полностью аналогична JaCarta-2 ГОСТ.

В случае использования электронных идентификаторов Рутокен Lite необходимо, чтобы ключ и сертификат были записаны на электронный идентификатор в виде контейнера, созданного при помощи криптопровайдера ViPNet CSP (см. Подготовка к работе электронных идентификаторов на

стр. 158). Информацию о ViPNet CSP можно получить на сайте https://infotecs.ru/product/vipnet-csp.html.

Для доступа к информации, содержащейся на электронном идентификаторе, требуется ввести PIN-код пользователя. Все операции по генерации ключей и запросов на выдачу сертификатов осуществляются при помощи ViPNet CSP (ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (256/512)).

Процедура идентификации и аутентификации приведена в разделе Запуск и завершение работы на стр. 41.

Роли пользователей

В ViPNet SafeBoot действуют следующие роли пользователей:

- Пользователь.
- Администратор.
- Аудитор.

На действия пользователей накладываются следующие ограничения:

- Пользователю после успешной аутентификации доступна загрузка операционной системы или возможность изменить свой пароль в режиме настройки ViPNet SafeBoot.
- Администратору предоставляется полный доступ ко всем пунктам меню режима настройки ViPNet SafeBoot, а также возможность загрузки операционной системы.
- Аудитору предоставляется доступ к просмотру и выгрузке журнала событий ViPNet SafeBoot, возможность менять свой пароль, возможность загрузки операционной системы.

Пользовательский интерфейс

В ViPNet SafeBoot, начиная с версии 2.0, предоставлена возможность выбора режима пользовательского интерфейса: текстовый (псевдографический) или графический. По своим функциям режимы пользовательского интерфейса полностью равнозначны. В данном руководстве приведена информация на примере графического режима.

Для переключения режимов пользовательского интерфейса при старте платформы необходимо нажать сочетание клавиш правый **Ctrl + g**. При этом, в зависимости от условий (профиля) установки продукта, может потребоваться перезагрузка системы.

Примеры пользовательского интерфейса в текстовом и графическом режиме приведены на рисунках ниже.

Рисунок 1. Аутентификация (текстовый режим пользовательского интерфейса)

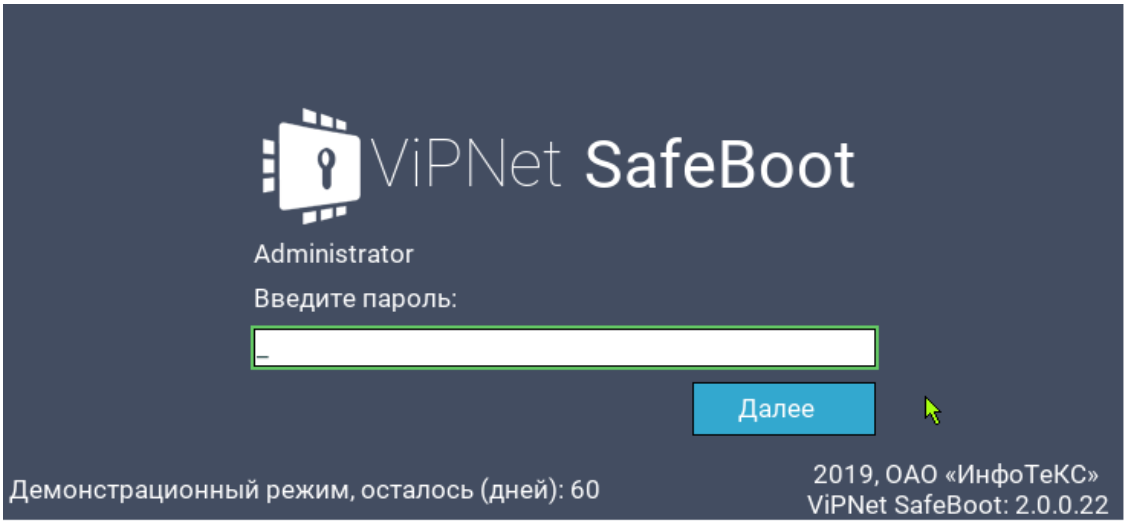


Рисунок 2. Аутентификация (графический режим пользовательского интерфейса)

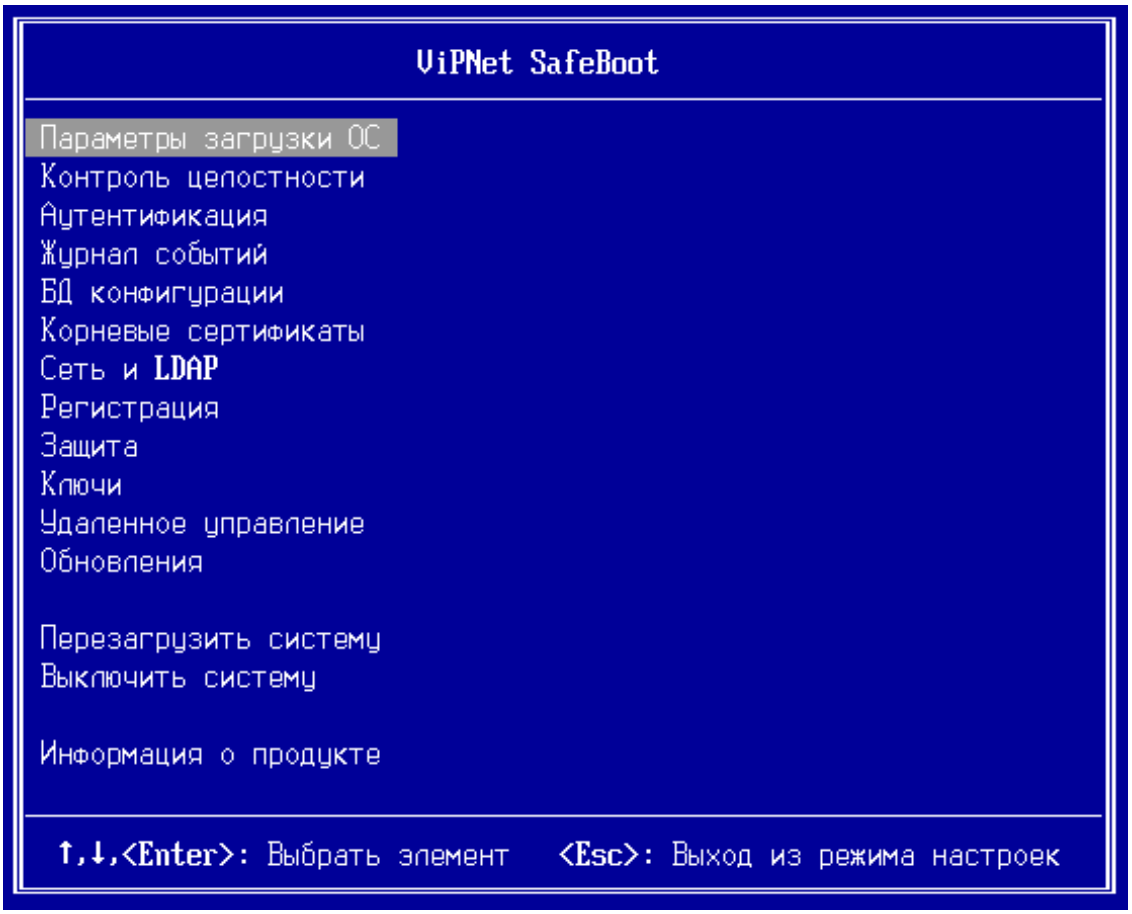


Рисунок 3. Меню режима настроек (текстовый режим пользовательского интерфейса)

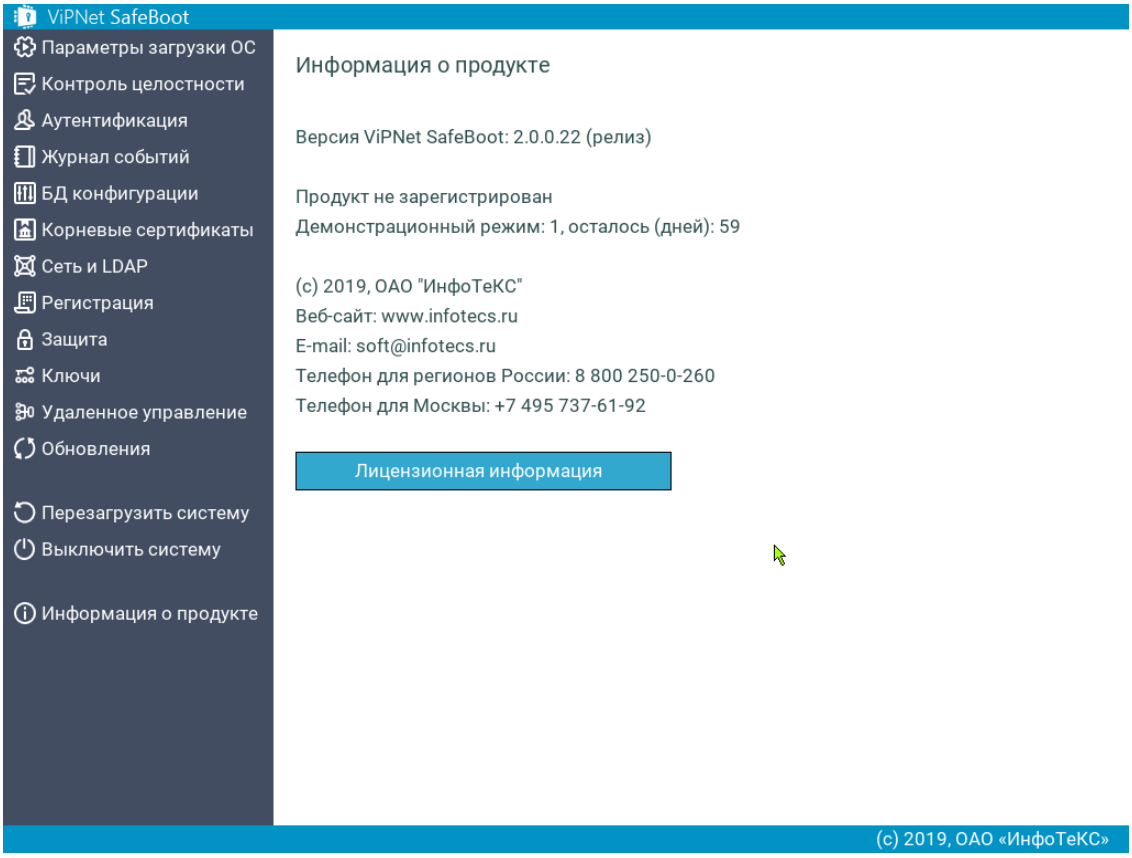


Рисунок 4. Меню режима настроек (графический режим пользовательского интерфейса)

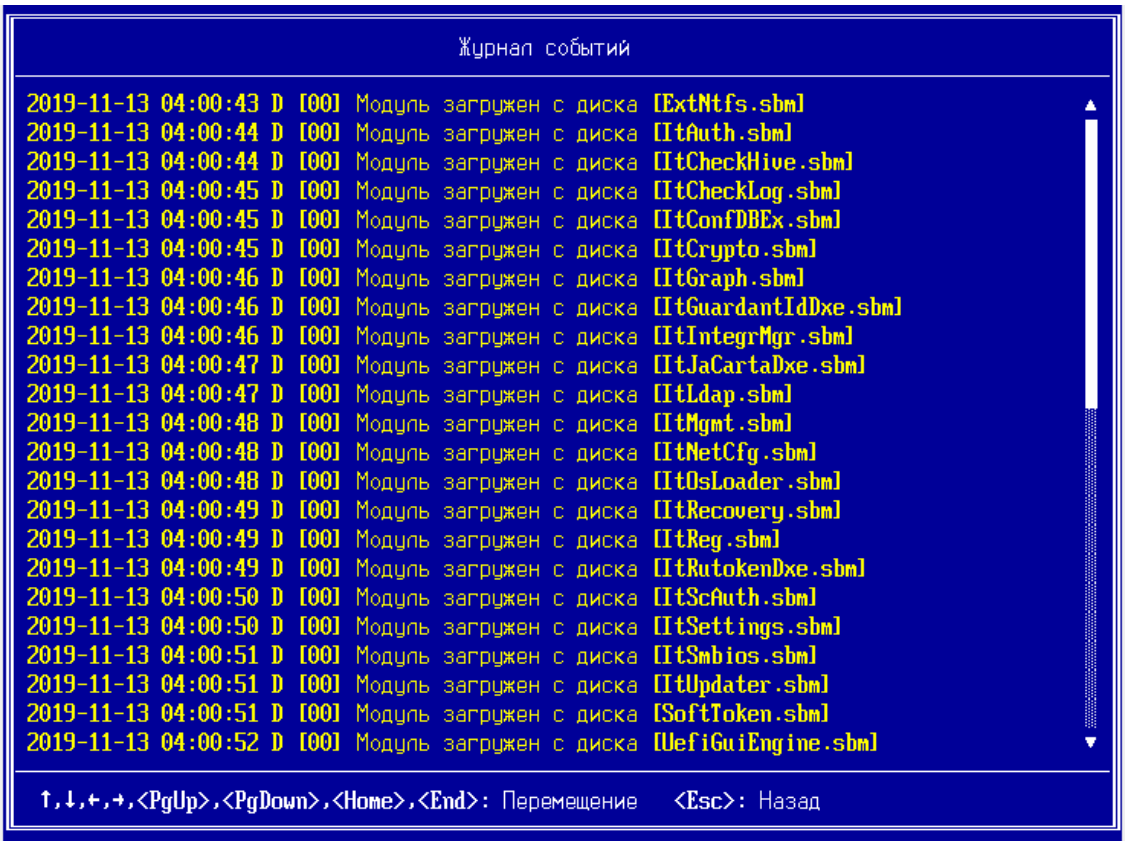


Рисунок 5. Журнал событий (текстовый режим пользовательского интерфейса)

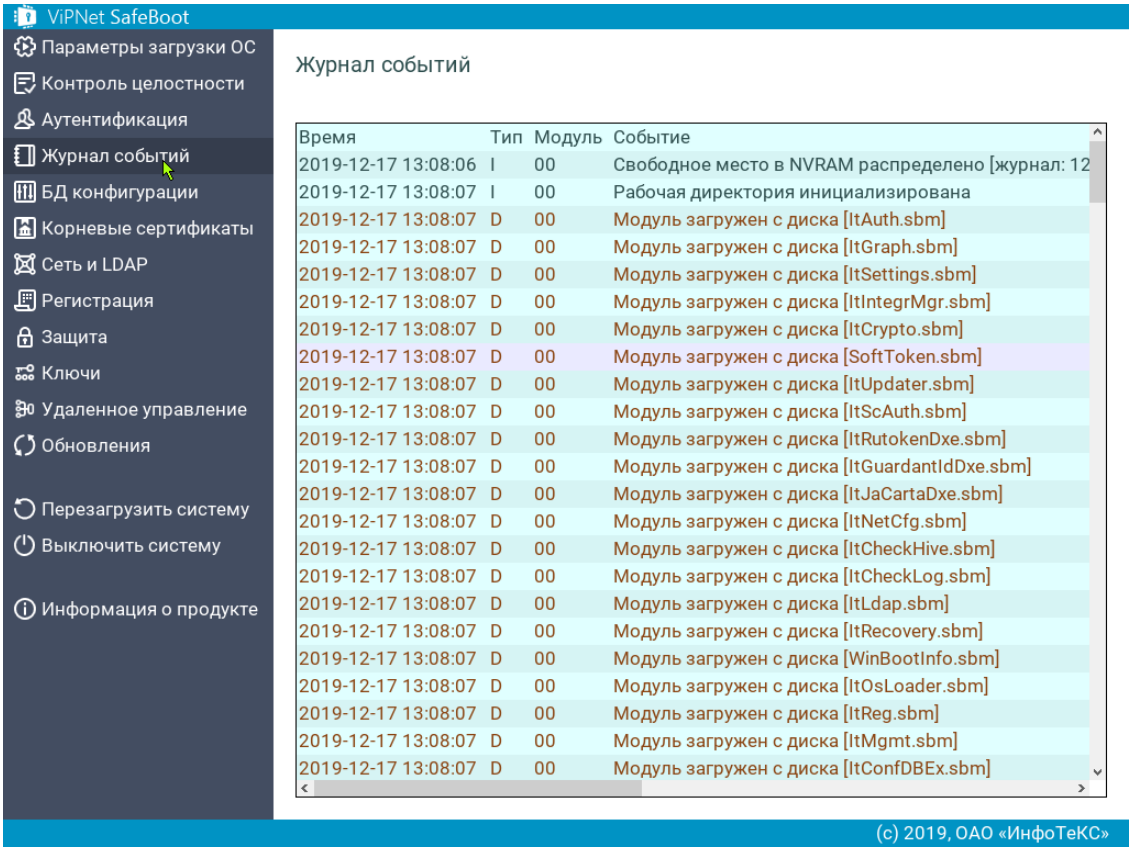


Рисунок 6. Журнал событий (графический пользовательский интерфейс)

2

Установка, регистрация, обновление и удаление ViPNet SafeBoot

Установка и удаление ViPNet SafeBoot

Программный комплекс ViPNet SafeBoot представляет собой фиксированный набор модулей. Установка ViPNet SafeBoot подразумевает встраивание его модулей в BIOS-регион, а также создание рабочего каталога на определенном разделе диска (для некоторых модулей допускается размещение в рабочем каталоге на диске). Встраивание модулей в образ BIOS и запись данного образа в память микросхемы может быть выполнена следующими способами:

- Запись образа ViPNet SafeBoot при помощи программатора.
- Установка образа ViPNet SafeBoot через механизм обновления BIOS платформы (может потребоваться подпись обновления).
- Установка образа ViPNet SafeBoot при помощи установочного дистрибутива ОАО «ИнфоТеКС». Процедура установки и удаления ViPNet SafeBoot приведена в руководстве по установке ФРКЕ.00180-02 90 19, входящем в комплект поставки.

Для предотвращения возможных проблем при установке ViPNet SafeBoot рекомендуется выполнять процедуру установки ViPNet SafeBoot после консультации со специалистами ОАО «ИнфоТеКС» (см. раздел Обратная связь на стр. 12).

Регистрация

После установки программного комплекса ViPNet SafeBoot в течение **60** дней необходимо пройти процедуру регистрации.

При первом включении ViPNet SafeBoot входит в демонстрационный режим, длящийся 60 дней. В данном режиме доступны все функции ViPNet SafeBoot. Количестве дней, оставшихся до окончания демонстрационного периода, указывает надпись, появляющаяся при включении в нижнем левом углу экрана: «**Демонстрационный режим, осталось (дней)**».

Если программный комплекс не будет зарегистрирован до окончания указанного срока, то ViPNet SafeBoot перейдет в режим ограниченной функциональности или будет выключен (зависит от режима установки продукта). В режиме ограниченной функциональности будут доступны только настройки загрузки ОС и Регистрация.

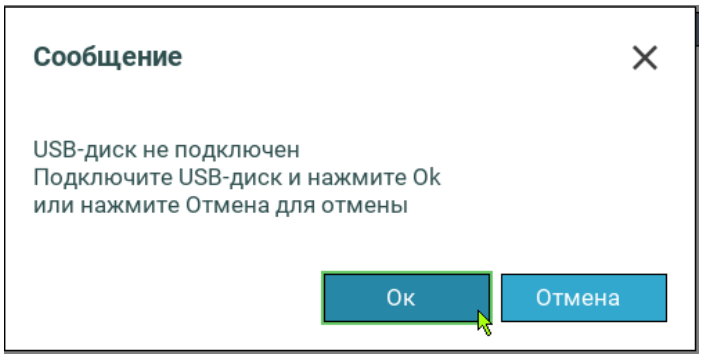
После прохождения регистрации функциональность ViPNet SafeBoot будет полностью восстановлена.

Перед регистрацией ViPNet SafeBoot подготовьте USB-диск, на котором должна быть создана директория **itregdata,** содержащая текстовый файл **serial_list.txt** со списком серийных номеров для регистрации программного продукта на нескольких ПК. Каждый серийный номер в файле **serial_list.txt** должен быть записан с новой строки. В некоторых случаях один серийный номер может использоваться для регистрации продукта на нескольких ПК. Подобный серийный номер должен быть записан в текстовый файл **itregdata\serial.txt**.

Для создания запроса на регистрацию ViPNet SafeBoot администратору необходимо обойти все регистрируемые ПК с подготовленным USB-диском. Выполните следующие действия:

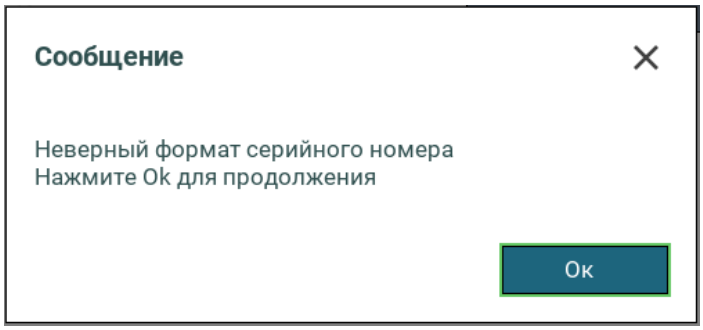
1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Регистрация**.
3. В открывшемся окне выберите пункт **Импортировать серийный номер**.

   Если USB-диск не был подключен, появится сообщение об ошибке:

   Подключите USB-диск и повторите импорт серийного номера.

Если серийный номер записан не в текстовом формате, то появится следующее сообщение об ошибке:



Нажмите **Ok** или **Enter**. Убедитесь, что серийный номер записан в текстовом формате в файле **itregdata\serial.txt,** и повторите импорт серийного номера.

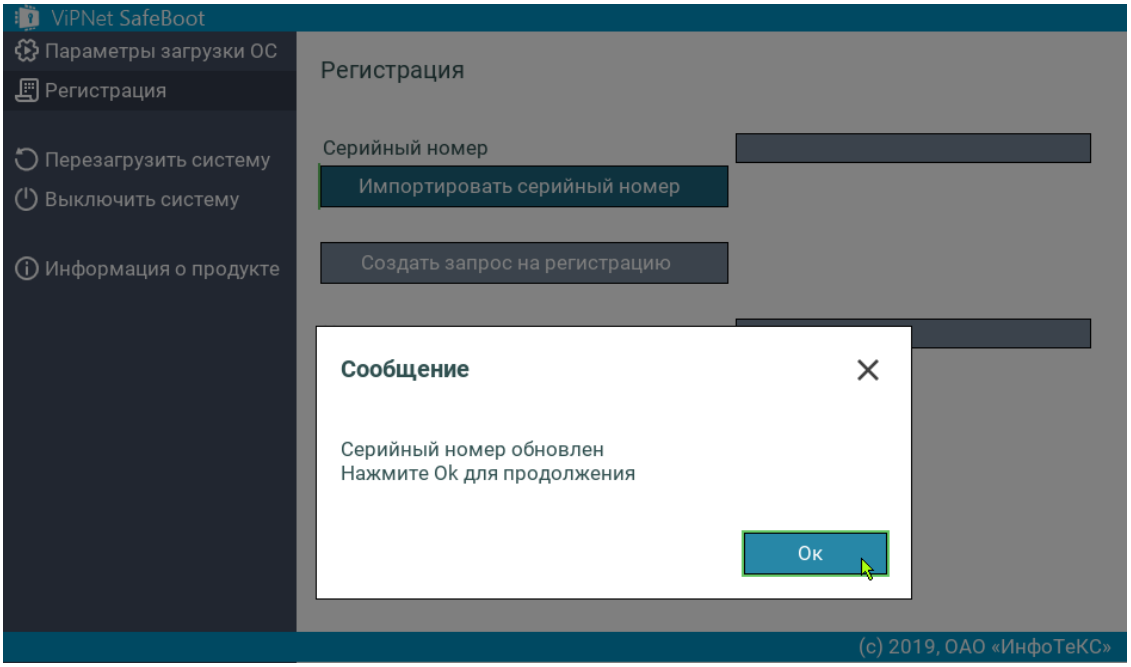


Рисунок 7. Импортирование серийного номера в графическом режиме

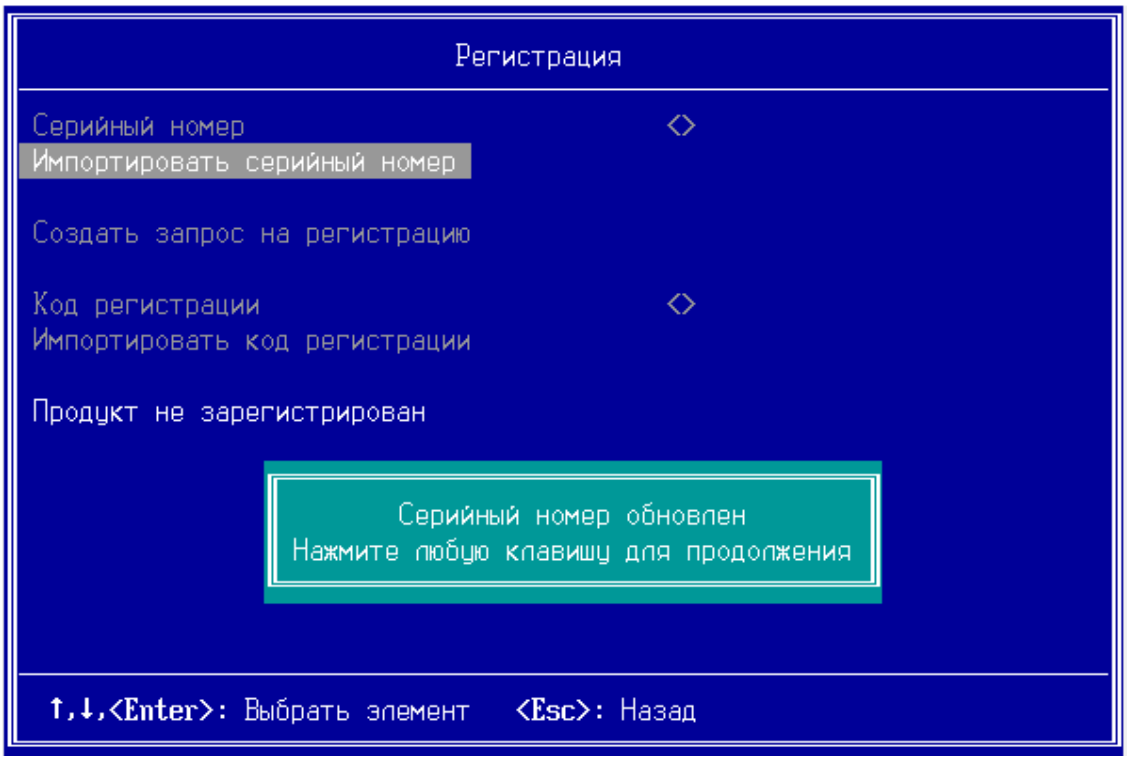


Рисунок 8. Импортирование серийного номера в текстовом режиме

Серийный номер из списка файла **serial_list.txt** будет зафиксирован в базе данных ViPNet SafeBoot и появится в соответствующей строке меню **Регистрация**.

4 Выберите пункт меню **Создать запрос на регистрацию**.

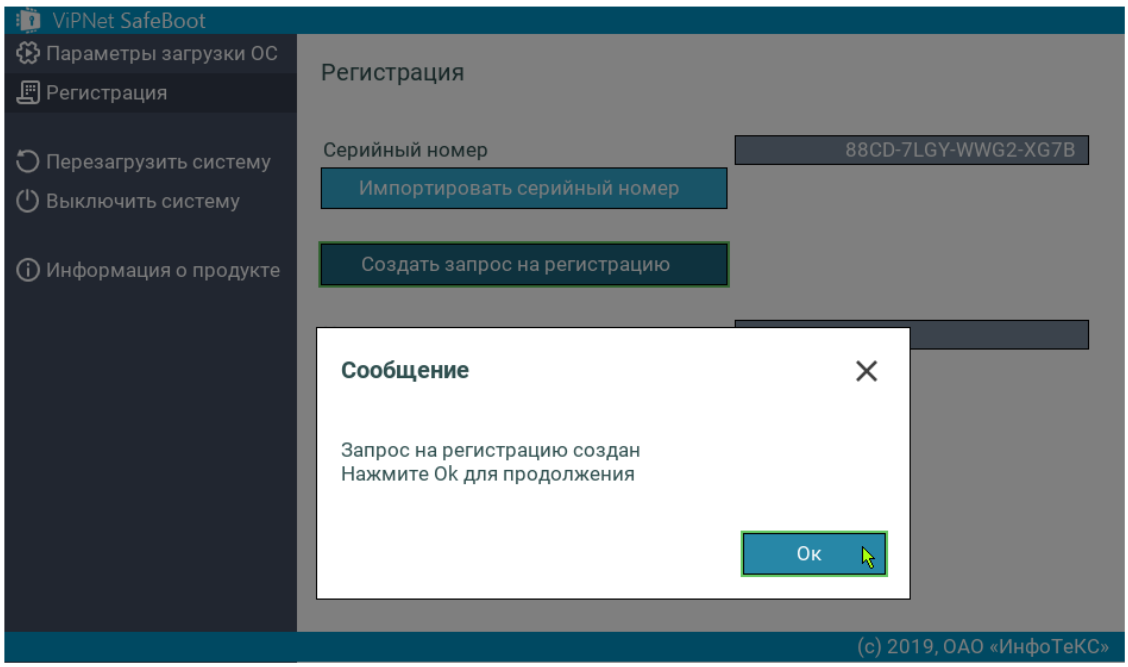


Рисунок 9. Создание запроса на регистрацию

В результате выполнения данной команды на USB-диске в директории **itregdata** будет создана директория с данными для запроса регистрации, на основе рассчитанного при первом запуске ViPNet SafeBoot уникального кода компьютера.

5 Повторите действия п.п. 1-3 для всех регистрируемых компьютеров.

При накоплении регистрационных данных от нескольких ПК, директория **itregdata** примет следующий вид:

```
itregdata\
          serial_list.txt
          <KK1>_<CH1>
          <KK2>_<CH2>
          ...
```

где **<KK1>_<CH1>, <KK2>_<CH2>** — директории, содержащие данные для запроса регистрации, **KK1** — код компьютера, **CH1** — серийный номер.

6 Подключите USB-диск с данными запроса регистрации к персональному компьютеру (ОС Windows 7 или выше) с доступом к интернету. Запустите скрипт запроса на регистрацию:

```
process_reg_reguests.bat <usb>:\itregdata
```

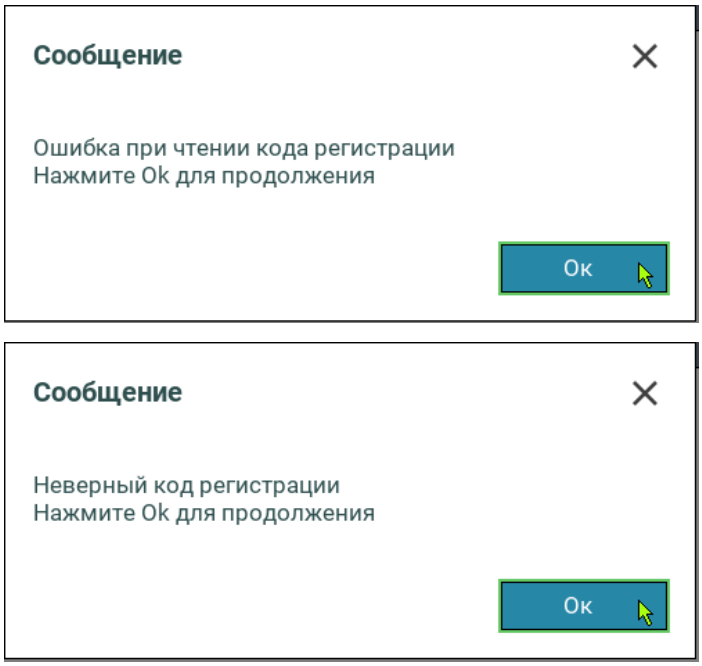
Ответ на запрос будет содержать коды регистрации, которые запишутся на USB-диск в директории, соответствующие коду компьютера, например, **itregdata\<KK1>_<CH1>**.

7 Подключите USB-диск с кодом регистрации к компьютеру с ViPNet SafeBoot, для которого проводится процедура регистрации.

8 В меню **Регистрация** выберите пункт **Импортировать код регистрации**.

Рисунок 10. Импортирование кода регистрации

В случае обнаружения некорректных данных регистрации на USB-диске, возможно появление следующих сообщений об ошибках:



Убедитесь, что подключенный USB-диск содержит данные регистрации, и повторите импорт кода регистрации.

После успешного импорта код регистрации отобразится в соответствующей строке меню.

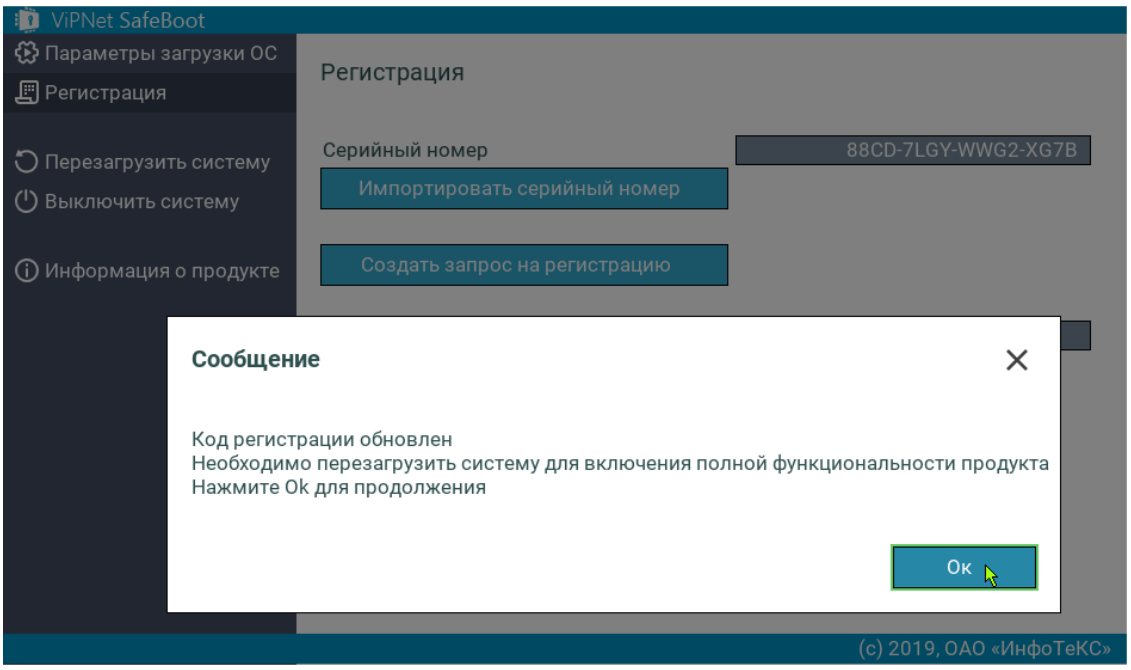


Рисунок 11. Успешное завершение регистрации

9 Нажмите **Ок** и выполните перезагрузку системы.

Обновление

Чтобы загрузить обновление ViPNet SafeBoot, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

Внимание! Во время обновления все настройки ViPNet SafeBoot будут удалены. Перед началом обновления рекомендуется выполнить сохранение настроек на USB-носителе (см. Экспорт настроек на стр. 73). После обновления рекомендуется выполнить импорт настроек (см. Импорт настроек на стр. 75)

---

2 Подключите USB-диск, содержащий файлы обновления.

3 В меню режима настроек выберите **Обновления**.

4 В открывшемся окне выберите **Проверить наличие обновлений**.

Начнется автоматический поиск файлов обновления.
В случае если USB-диск не подключен, появится соответствующее сообщение.

Вставьте USB-диск, содержащий файлы обновления, и нажмите любую клавишу для продолжения.
При отсутствии файлов обновлений, появится сообщение о том, что обновления не найдены. Нажмите любую клавишу для продолжения работы.

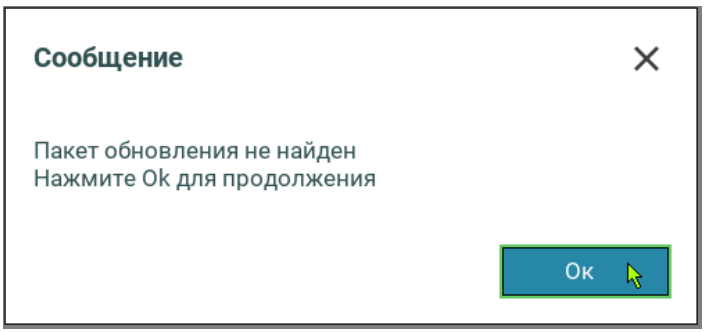


Рисунок 12. Сообщение в случае отсутствия файла обновления

Если USB-диск содержит устаревшую версию, то на экране появится соответствующее сообщение:

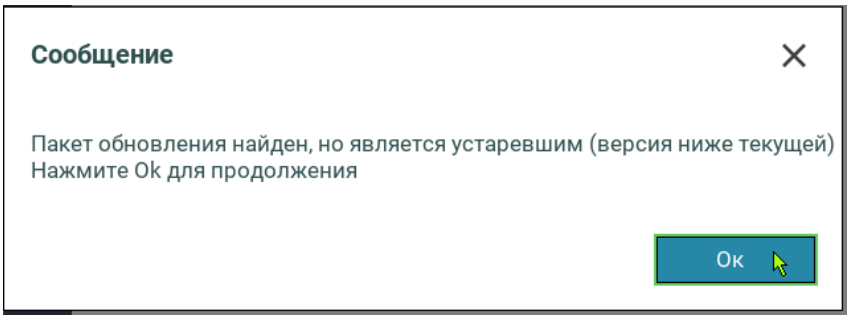


Рисунок 13. Сообщение об устаревшей версии обновления

Нажмите **Ок** или **Enter** для продолжения работы.

5 Если USB-диск содержит файл обновления, откроется окно с указанием версии обновления. В открывшемся окне выберите **Обновить ViPNet SafeBoot.**

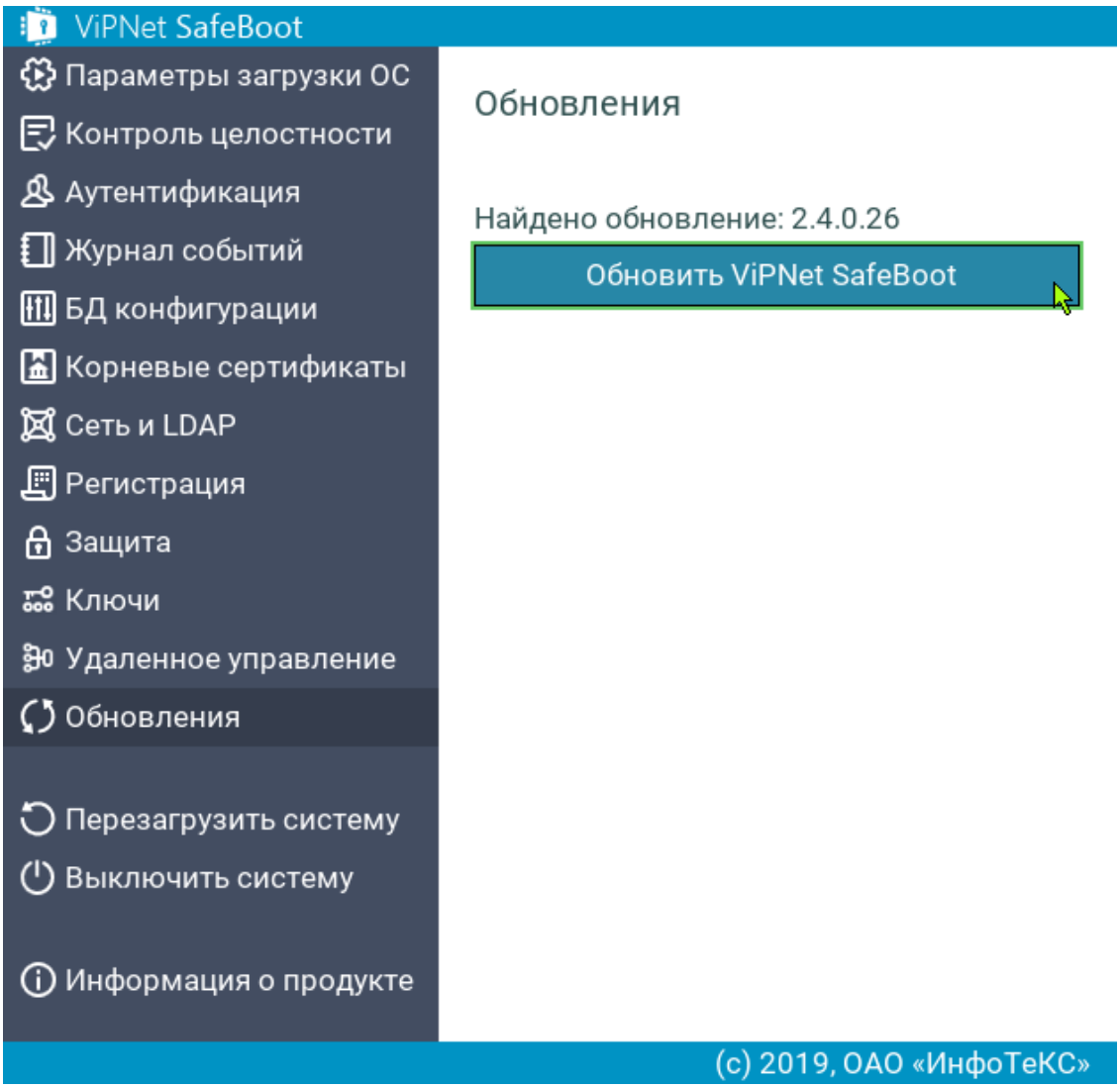


Рисунок 14. Выбор найденной версии обновления

6 Появится сообщение о подтверждении обновления. Нажмите **Ок**.

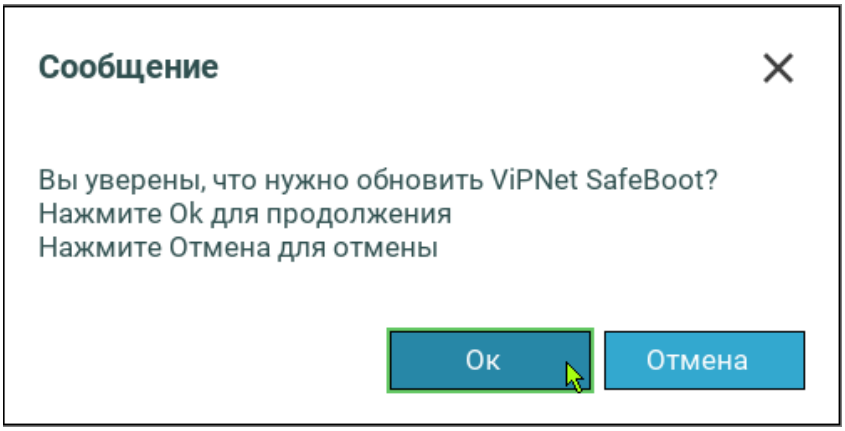


Рисунок 15. Подтверждение обновления

Внимание! Во время обновления не пытайтесь выключить питание или перезагрузить компьютер, это может вывести его из строя. При обновлении рекомендуется подключить компьютер к источнику бесперебойного питания.

7 Во время обновления на экране появятся сообщения о верификации и установке пакета обновления:

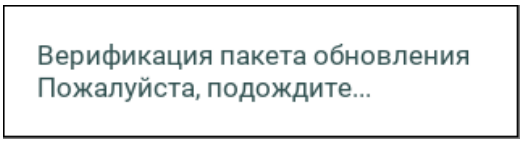


Рисунок 16. Сообщение о верификации пакета обновления

В случае ошибки при верификации пакета будет выдано сообщение:

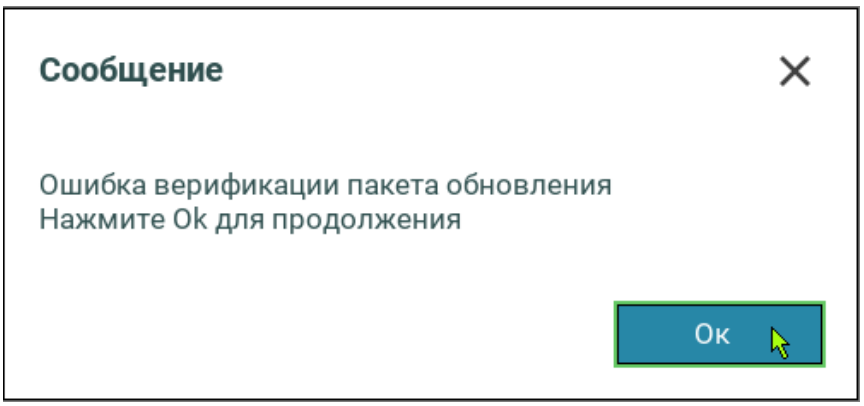


Рисунок 17. Сообщение об ошибке верификации пакета обновления

При обнаружении данной ошибки обратитесь в службу поддержки (см. Обратная связь на стр. 12).

8 В ходе установки обновления будет выдано следующее сообщение:

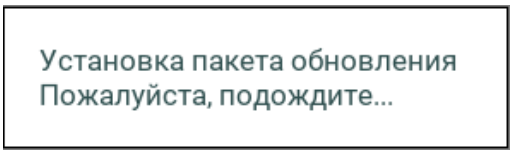


Рисунок 18. Сообщение об установке пакета обновления

Если будет обнаружено несколько разделов с рабочим каталогом «EFI\Infotecs» будет выдано сообщение:

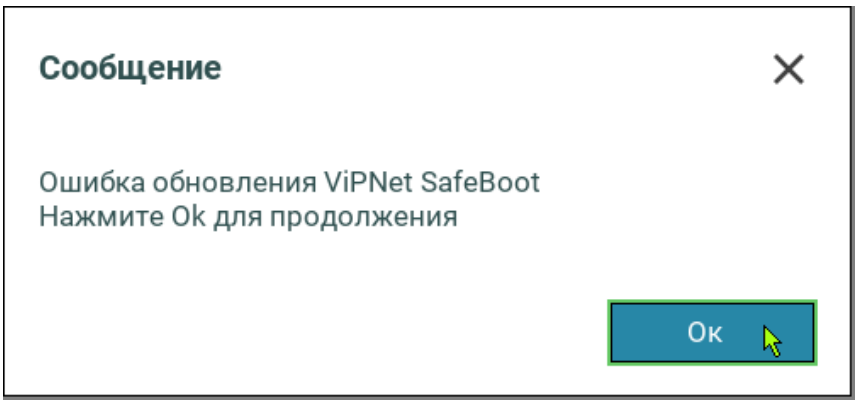


Рисунок 19. Сообщение об ошибке при установке обновления

9 В процессе обновления будет загружен UEFI Shell. По окончании установки пакета обновления будет выполнена перезагрузка. В журнале событий будет зарегистрирована запись о выполненном обновлении.

3

Начало работы

Первый запуск

Запуск ViPNet SafeBoot осуществляется автоматически при включении компьютера.

Запуск незарегистрированного программного комплекса ViPNet SafeBoot осуществляется в режиме, заданном администратором перед установкой ViPNet SafeBoot в флаговых файлах в директории **itinstallcfg** инсталлятора (см. документ «ViPNet SafeBoot. Руководство по установке»).

Первый запуск ViPNet SafeBoot должен выполняться с подключенным диском восстановления.

Режим неактивности

В данном режиме ViPNet SafeBoot находится в выключенном состоянии (все функции отключены, операционная система ПК загружается штатно, как будто ViPNet SafeBoot не установлен). Для включения ViPNet SafeBoot необходимо нажать сочетание клавиш **Ctrl + e** при старте платформы (с подключенным USB-диском восстановления). Работа ViPNet SafeBoot будет осуществляться в демонстрационном режиме 2.

Демонстрационный режим 1 (режим по умолчанию)

В данном режиме доступны все функции ViPNet SafeBoot до окончания **60** дневного периода. Если программный комплекс не будет зарегистрирован до окончания указанного срока, то ViPNet SafeBoot выключается. Для включения ViPNet SafeBoot необходимо нажать сочетание клавиш **Ctrl + e** при старте платформы (с подключенным USB-диском восстановления). Работа ViPNet SafeBoot будет осуществляться в режиме ограниченной функциональности, в котором будут доступны только настройки загрузки ОС и **Регистрация**. Порядок регистрации ViPNet SafeBoot приведен в разделе Регистрация на стр. 24.

Демонстрационный режим 2

В данном режиме доступны все функции ViPNet SafeBoot до окончания 60 дневного периода. Если программный комплекс не будет зарегистрирован до окончания указанного срока, то ViPNet SafeBoot перейдет в режим ограниченной функциональности, в котором будут доступны только настройки загрузки ОС и **Регистрация**. Порядок регистрации ViPNet SafeBoot приведен в разделе Регистрация на стр. 24.

Первый запуск ViPNet SafeBoot

При первом запуске рекомендуется настроить параметры загрузки операционной системы, изменить пароль администратора, а также создать диск восстановления пароля администратора (для восстановления или сброса пароля до значения при первом включении).

Порядок действий после включения ViPNet SafeBoot следующий:

1 При появлении приглашения ввести имя пользователя, введите логин **Administrator**.

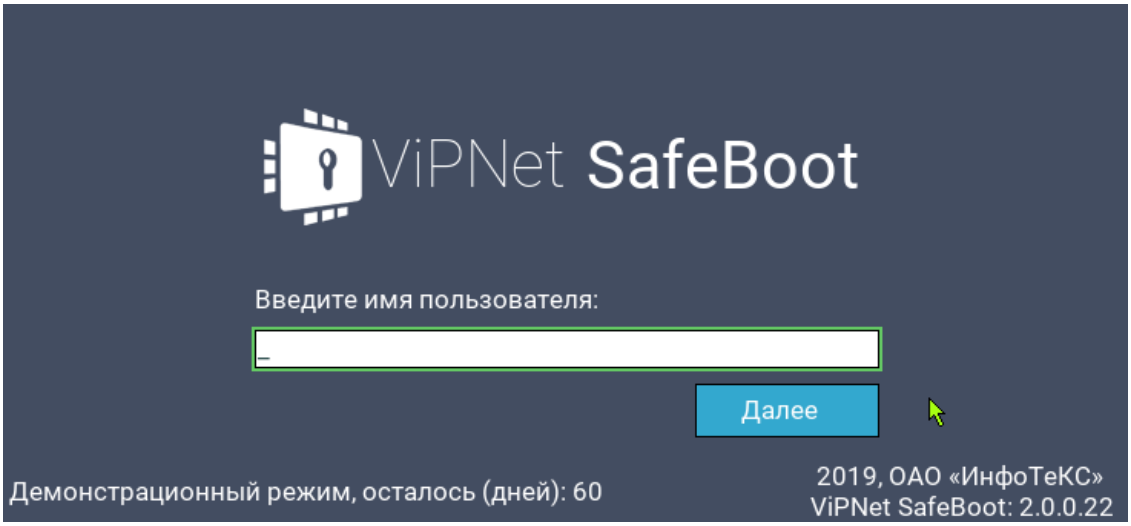


Рисунок 20. Начало аутентификации (ввод имени пользователя)

2 При появлении приглашения ввести пароль, введите пароль **12345678**.

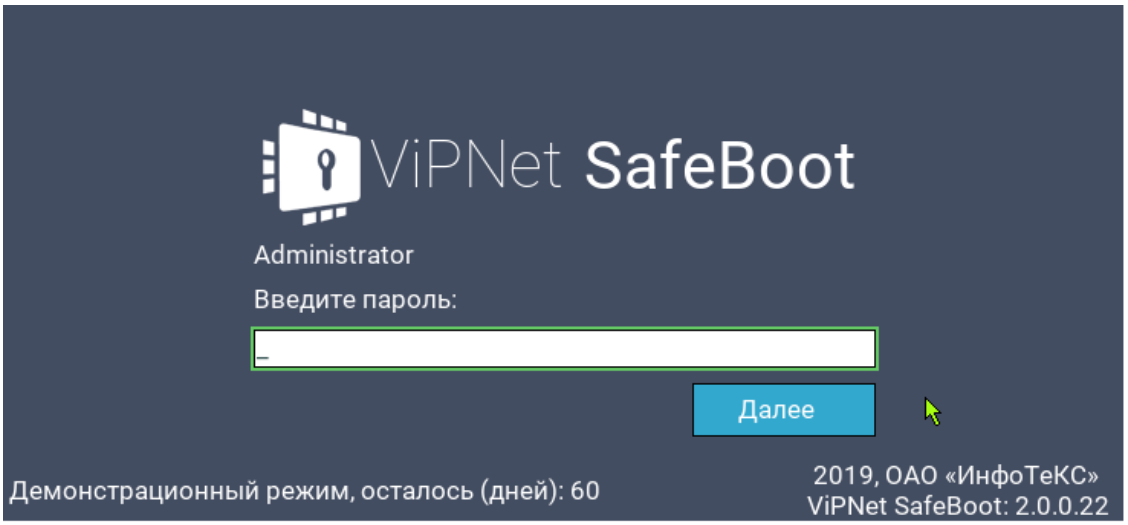


Рисунок 21. Приглашение ввести пароль

3 После успешной аутентификации будет выдано следующее сообщение:

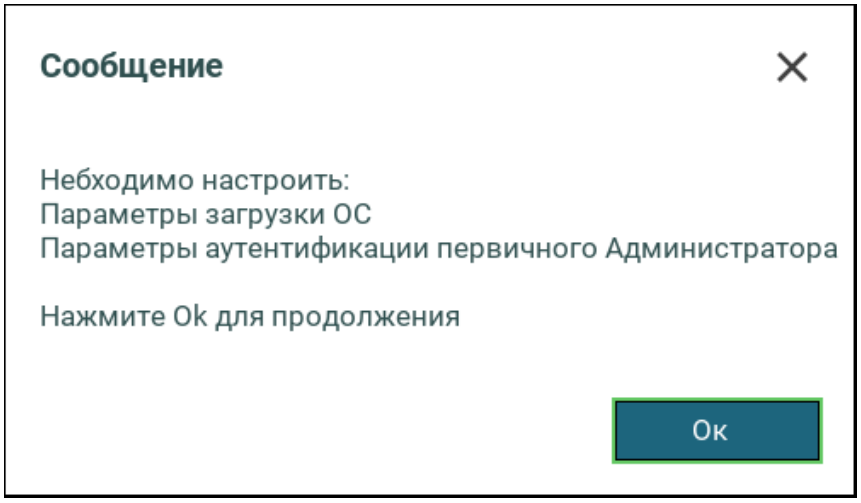
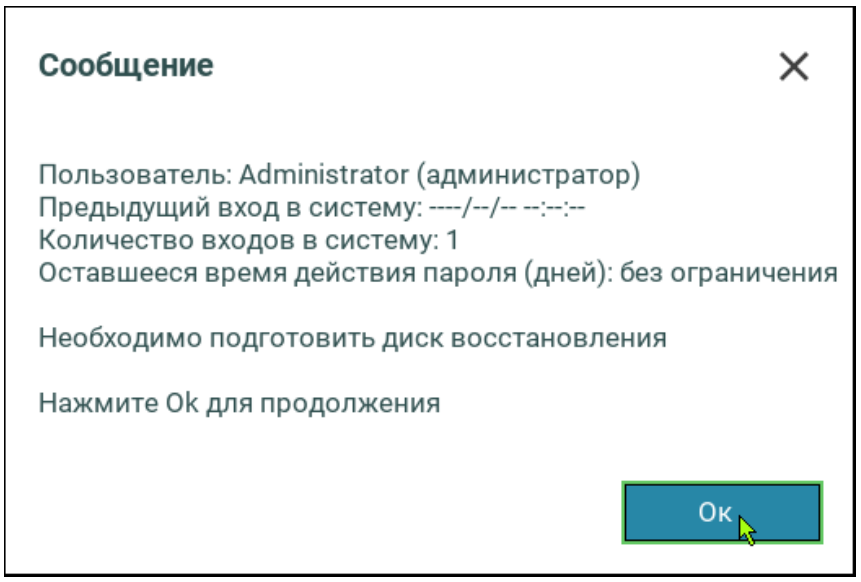


Рисунок 22. Сообщение о необходимых настройках при первом включении

4 Нажмите любую клавишу. Появится сообщение с информацией о предыдущем входе в систему, сроке действия пароля и необходимости подготовить диск восстановления:



Внимание! Диск восстановления рекомендуется создать сразу после изменения параметров аутентификации Администратора.

5 Нажмите любую клавишу. Откроется меню режима настроек ViPNet SafeBoot:

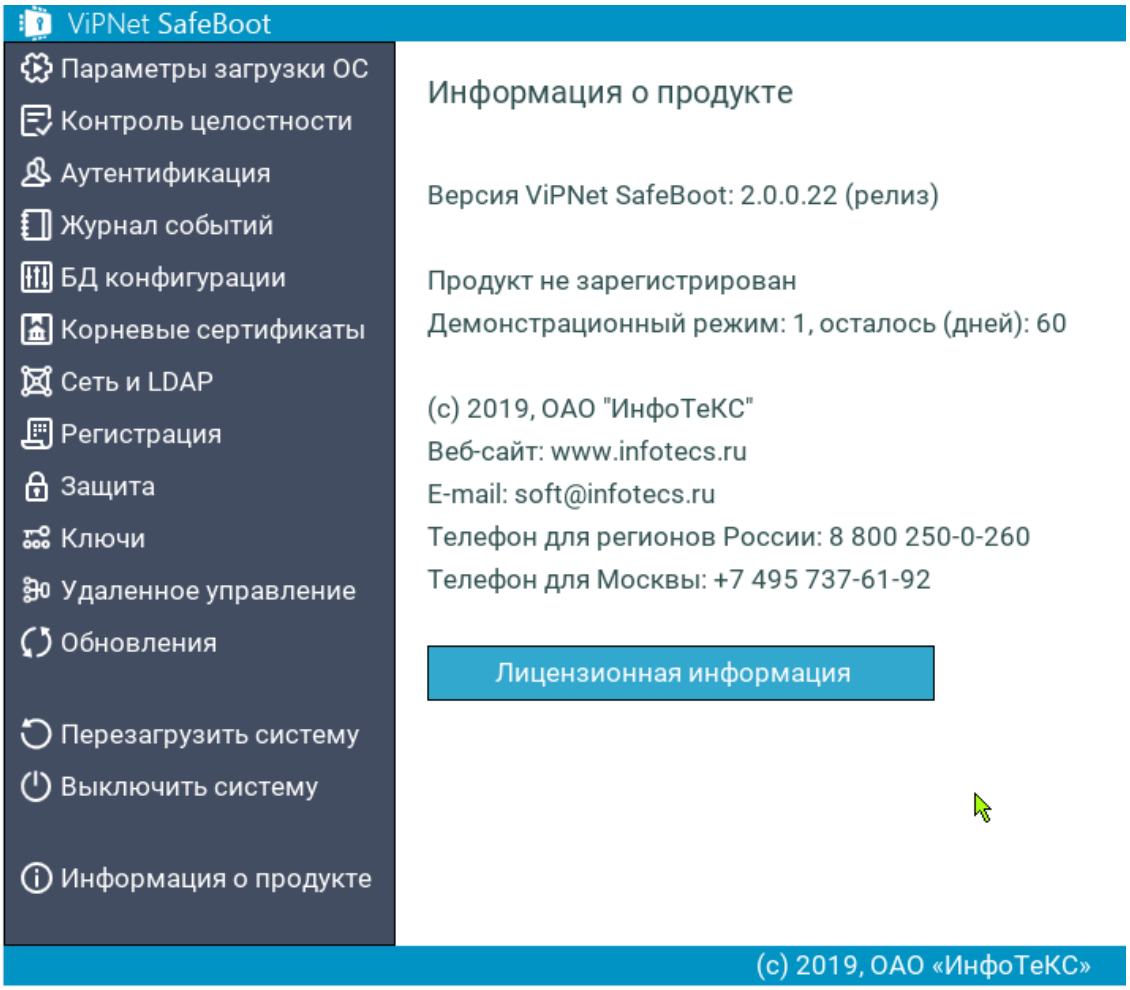


Рисунок 23. Меню режима настроек ViPNet SafeBoot

6 В меню режима настроек выберите пункт **Аутентификация**. В открывшемся окне выберите **Administrator** из списка текущих пользователей.

7 В окне **Настройки пользователя** выберите пункт **Изменить пароль**.

Совет. Рекомендуется установить сложный пароль, активировав опцию «Сложный пароль». Сложный пароль должен соответствовать следующим критериям:

- длина пароля не менее 8 символов;
- минимум один буквенный символ в верхнем регистре;
- минимум один буквенный символ в нижнем регистре;
- минимум один спецсимвол;
- минимум один цифровой символ.

Примечание. Спецсимволами считаются все печатные символы базовой таблицы ASCII (0-127), не являющиеся цифрами и буквами латинского алфавита:

	!	"	#	$	%	&	'	(	)	*
+	`	-	.	/	:	;	<	=	>	?
@	[	\	]	^	_	'	{	|	}	~

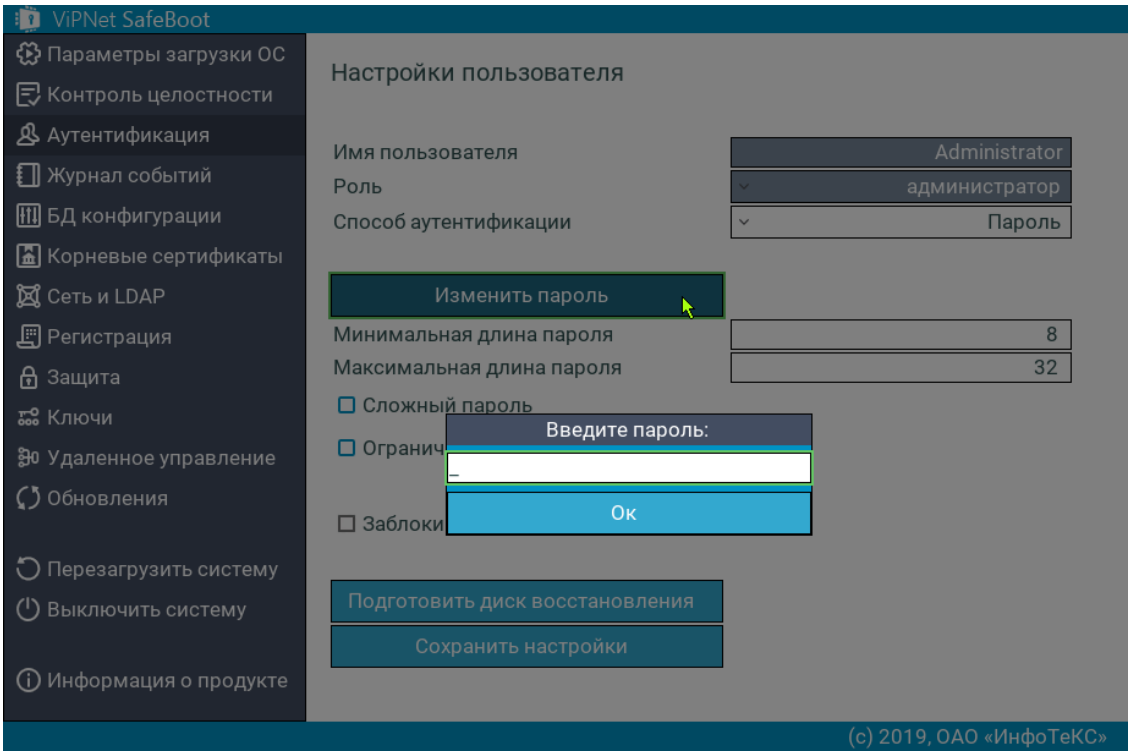


Рисунок 24. Меню настроек пользователя в графическом режиме

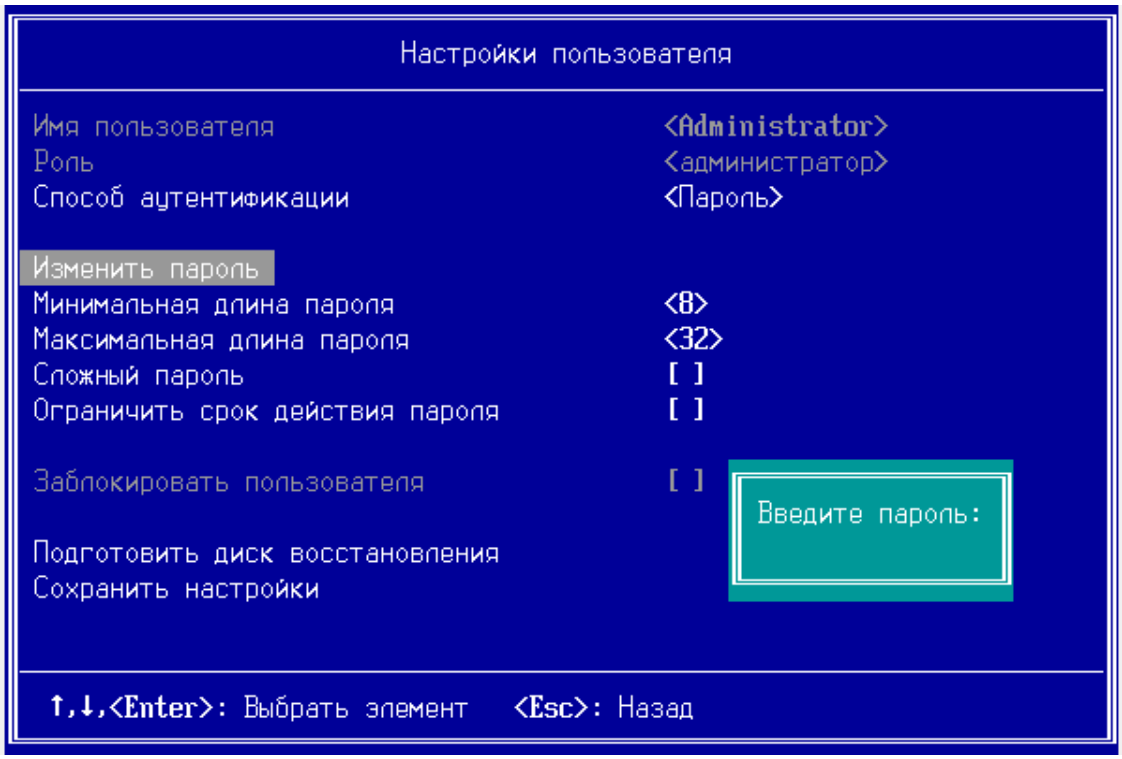
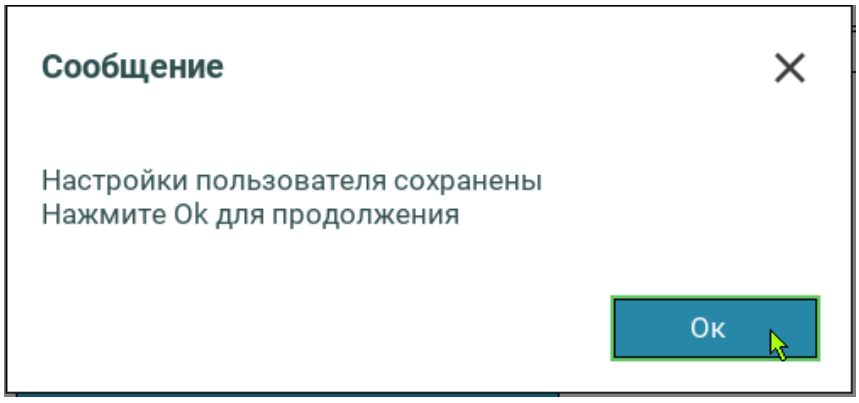


Рисунок 25. Меню настроек пользователя в текстовом режиме

Введите пароль, нажмите **Enter**. Затем повторите ввод пароля.

8 Сохраните настройки, выбрав пункт **Сохранить настройки**.

Дождитесь появления следующей надписи:



9 Нажмите **Ok** или **Enter**.

Примечание. Количество попыток ввода пароля при аутентификации ограничено. Администратор будет заблокирован при превышении количества неудачных попыток аутентификации. Для восстановления пароля администратора или сброса пароля до значения при первом включении рекомендуется создать диск восстановления (см. Создание диска восстановления на стр. 106).

---

10 Для выхода в основное меню нажмите **Esc**.

11 Установите параметры загрузки операционной системы (см. Управление режимами загрузки операционной системы на стр. 77).

Запуск и завершение работы

Запуск ViPNet SafeBoot осуществляется автоматически при включении компьютера до загрузки операционной системы.

Для начала загрузки операционной системы или входа в режим настройки ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51), необходимо выполнить процедуру идентификации и аутентификации.

Внимание! Ошибки при аутентификации могут привести к блокировке системы.

Пользователь, превысивший установленное администратором количество неудачных попыток аутентификации, блокируется.

Завершение работы ViPNet SafeBoot осуществляется при запуске операционной системы.

Аутентификация по паролю

Для выполнения аутентификации по паролю, выполните следующие действия:

1 При появлении приглашения ввести имя пользователя, введите логин и нажмите **Enter**.

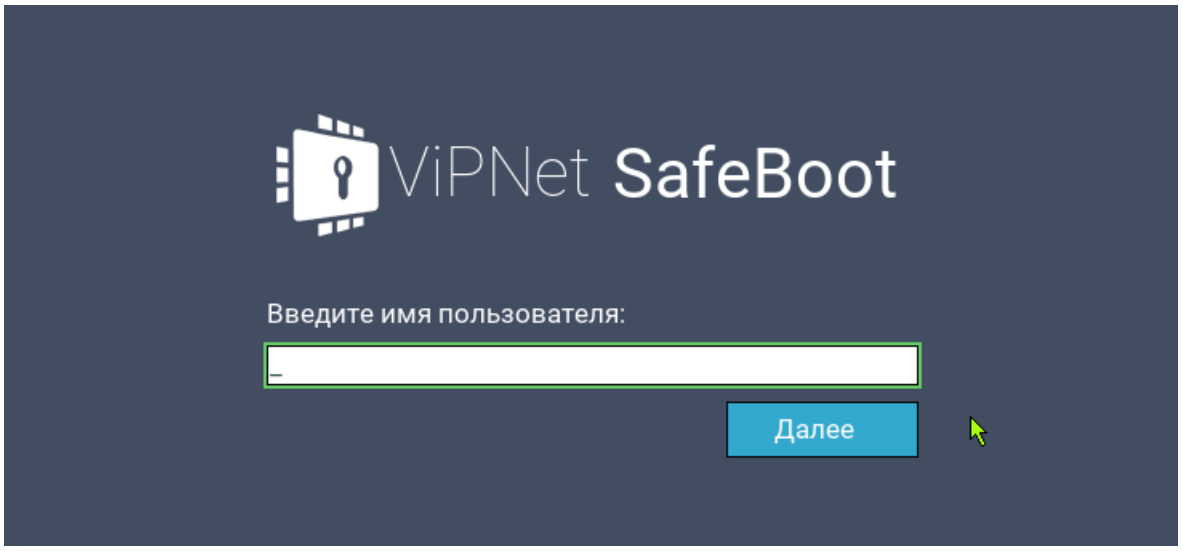


Рисунок 26. Начало аутентификации (ввод имени пользователя)

2 При появлении приглашения ввести пароль, введите пароль и нажмите **Enter**.

Рисунок 27. Приглашение ввести пароль

Аутентификация по электронному идентификатору

Для выполнения аутентификации по электронному идентификатору, выполните следующие действия:

1 Установите электронный идентификатор в USB-порт.

2 При появлении приглашения ввести имя пользователя, введите логин, выданный администратором, и нажмите **Enter**.

Рисунок 28. Начало аутентификации (ввод имени пользователя)

3 При появлении приглашения ввести PIN-код, введите PIN-код электронного идентификатора и нажмите **Enter**.

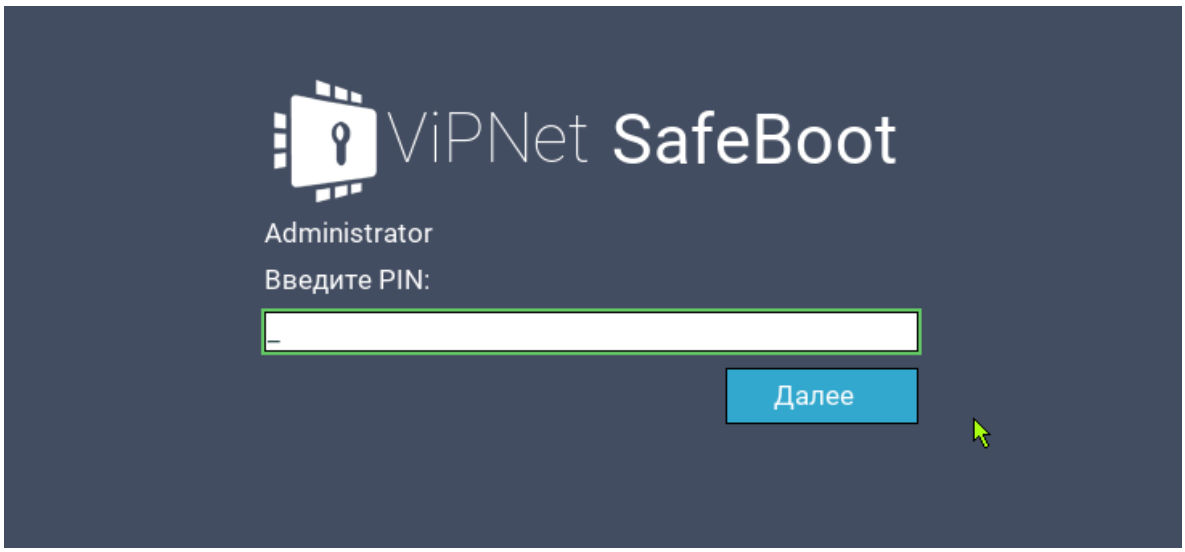
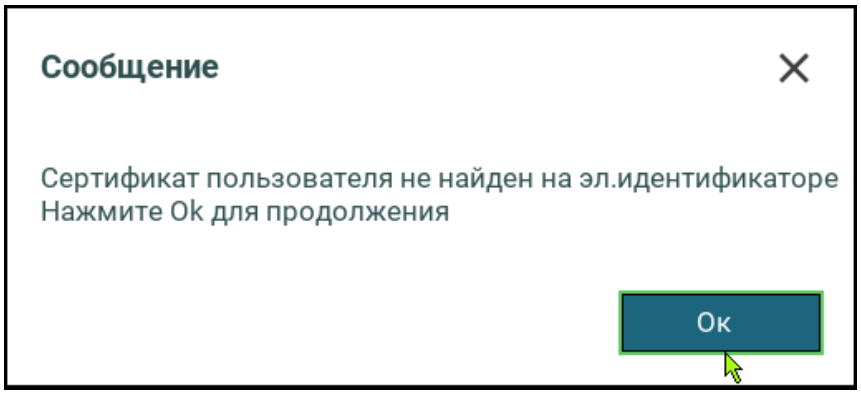


Рисунок 29. Приглашение ввести PIN-код

В случае отсутствия сертификата на электронном идентификаторе, появится сообщение об ошибке:



Нажмите **Ок** и повторите процедуру аутентификации с электронным идентификатором, содержащим сертификат для аутентификации.

Аутентификация по электронному идентификатору и паролю

Для выполнения аутентификации по электронному идентификатору и паролю, выполните следующие действия:

1 Установите электронный идентификатор в USB-порт.

2 При появлении приглашения ввести имя пользователя, введите логин, выданный администратором, и нажмите **Enter**.

Рисунок 30. Начало аутентификации (ввод имени пользователя)

3 При появлении приглашения ввести PIN-код, введите PIN-код электронного идентификатора и нажмите **Enter**.

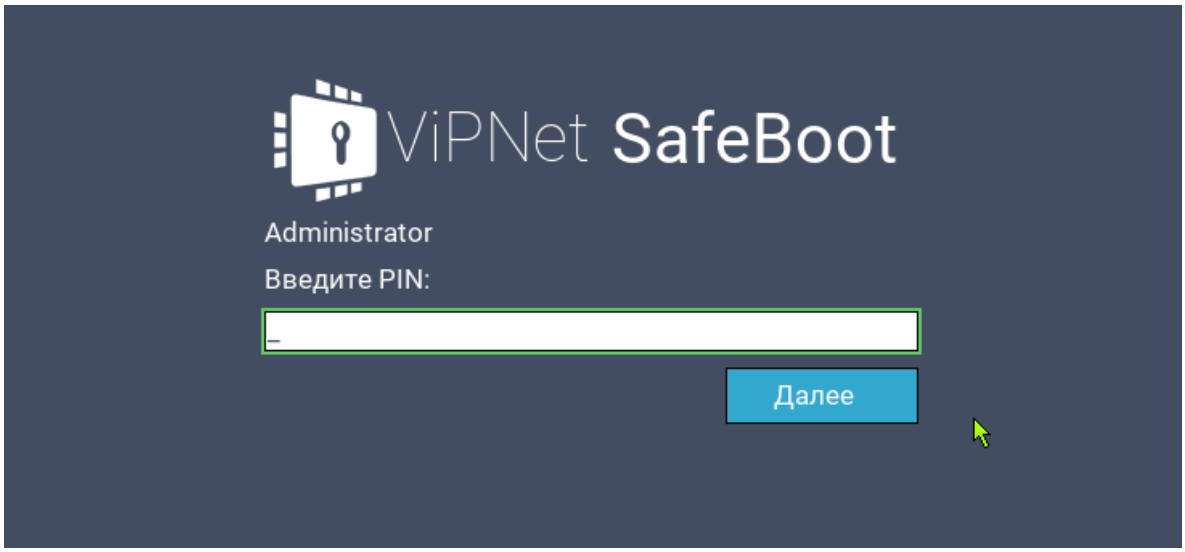


Рисунок 31. Приглашение ввести PIN-код

4 При появлении приглашения ввести пароль, введите пароль и нажмите **Enter**.

Рисунок 32. Приглашение ввести пароль

Аутентификация по паролю на электронном идентификаторе

Для выполнения аутентификации по паролю на электронном идентификаторе, выполните следующие действия:

1 Вставьте электронный идентификатор.

2 При появлении приглашения ввести имя пользователя, введите логин, выданный администратором, и нажмите **Enter**.

Рисунок 33. Начало аутентификации (ввод имени пользователя)

3 При появлении приглашения ввести PIN-код, введите PIN-код электронного идентификатора и нажмите **Enter**.

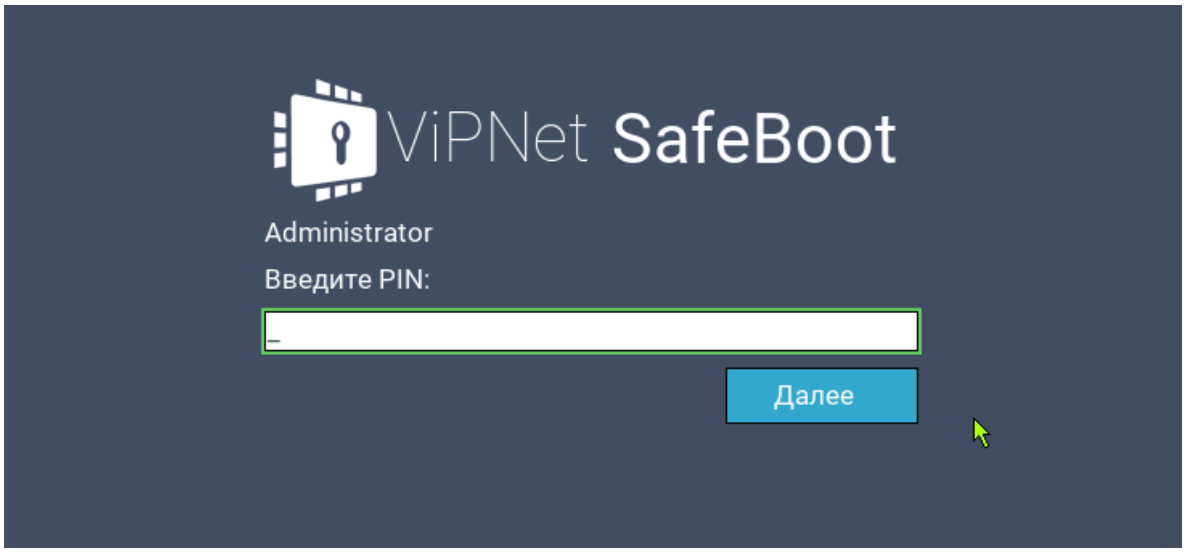
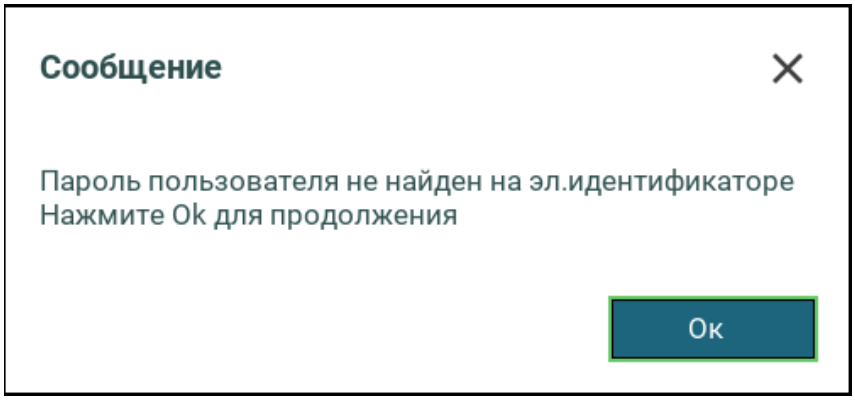


Рисунок 34. Приглашение ввести PIN-код

В случае отсутствия пароля на электронном идентификаторе, появится сообщение об ошибке:



Нажмите **Ок** для продолжения и повторите процедуру аутентификации с электронным идентификатором, содержащим пароль для аутентификации, или установите новый пароль на электронном идентификаторе в соответствии с рекомендациями раздела Добавление учетных записей пользователей с аутентификацией по электронному идентификатору на стр. 130.

Аутентификация пользователя, зарегистрированного на LDAP сервере

Для выполнения аутентификации пользователя, зарегистрированного на LDAP сервере, выполните следующие действия:

1 При появлении приглашения ввести имя пользователя, введите логин пользователя в следующем формате **<имя сервера>\<имя учетной записи пользователя>.** Имя сервера задается администратором в настройках (см. Добавление учетных записей пользователей с LDAP аутентификацией на стр. 134). Нажмите **Enter**.

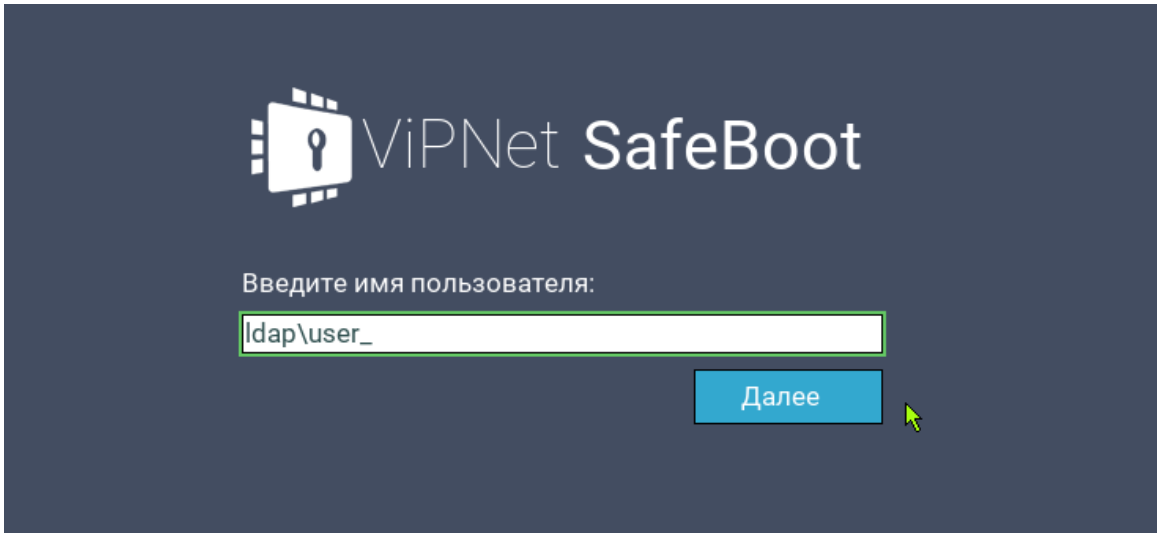


Рисунок 35. Начало аутентификации (ввод имени пользователя)

2 При появлении приглашения ввести пароль, введите пароль и нажмите **Enter**.

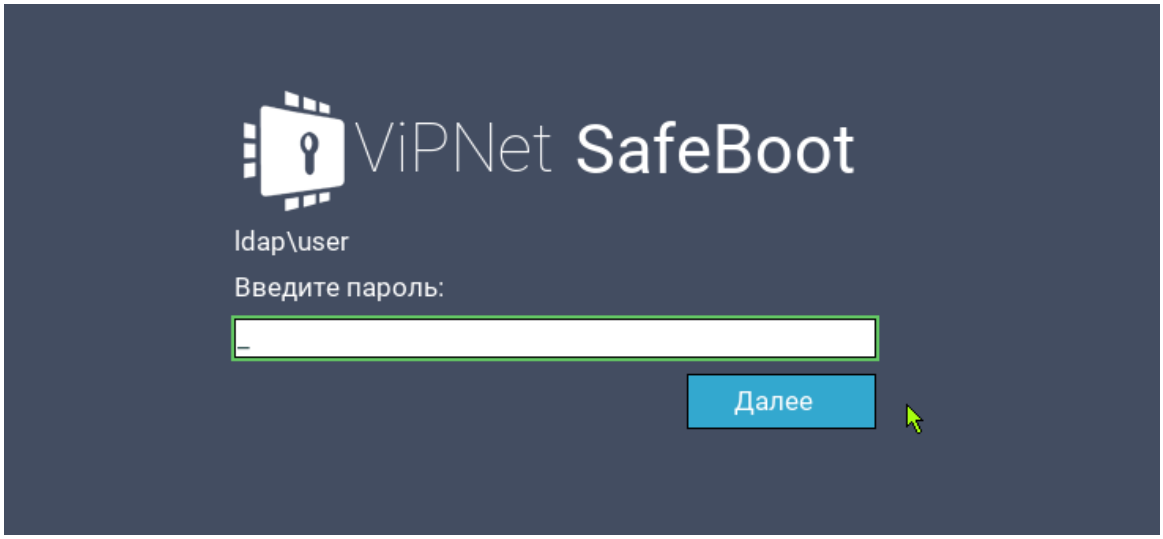


Рисунок 36. Приглашение ввести пароль

4

Режим настройки ViPNet SafeBoot

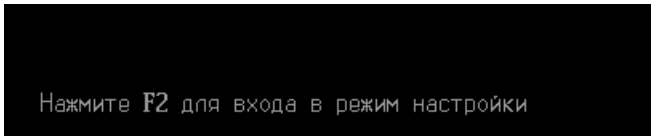
Вход в режим настройки ViPNet SafeBoot

В ViPNet SafeBoot полный доступ к функциям режима настройки имеет только Администратор. Аудитору предоставляется доступ только к управлению журналом событий и смене собственного пароля. Пользователю в режиме настройки ViPNet SafeBoot доступна только функция смены собственного пароля.

Чтобы войти в режим настройки, выполните следующие действия:

1. Включите или перезагрузите компьютер.
2. Выполните процедуру аутентификации (см. Запуск и завершение работы на стр. 41).

   После успешной аутентификации в нижней части экрана появится надпись:

   Внимание! Если не нажать клавишу **F2** в течение 3 секунд, то начнется загрузка операционной системы.

3. Нажмите клавишу **F2**.

   Откроется основное меню режима настроек ViPNet SafeBoot.

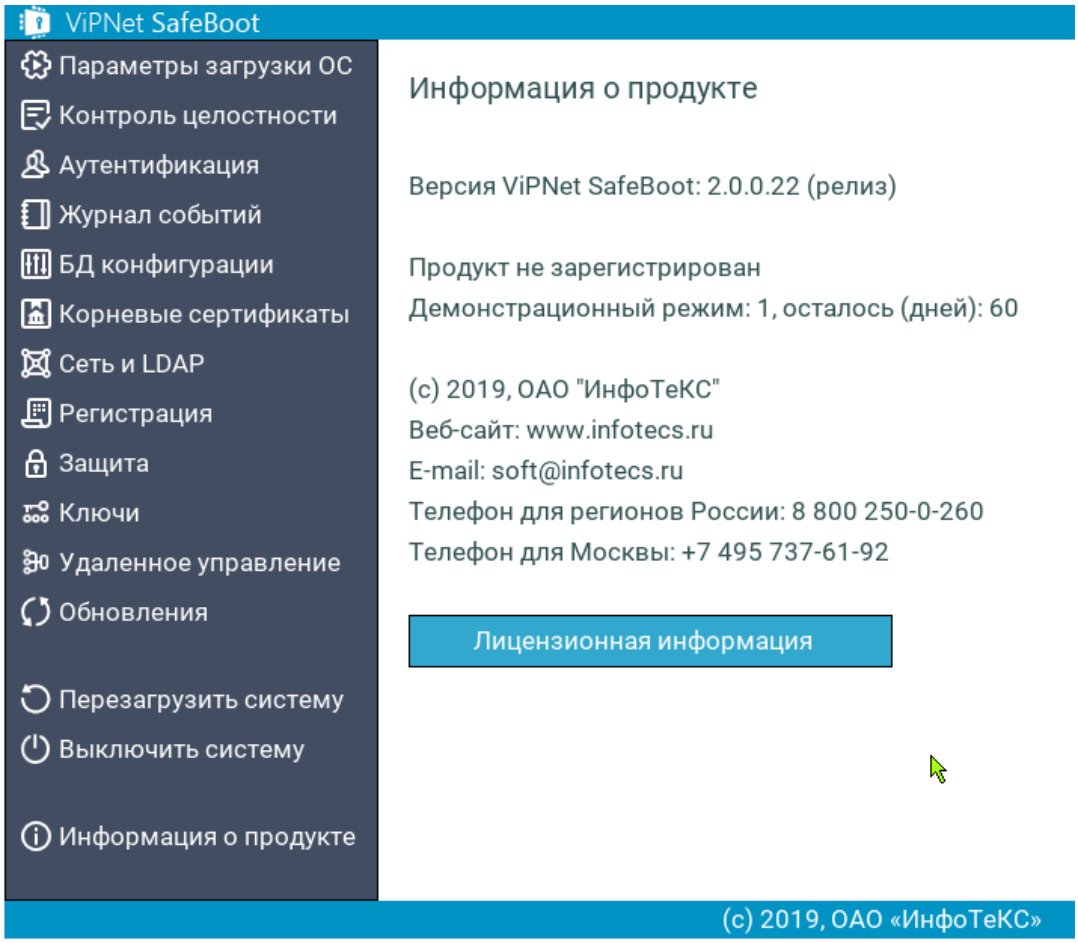


Рисунок 37. Вид меню режима настроек ViPNet SafeBoot для Администратора

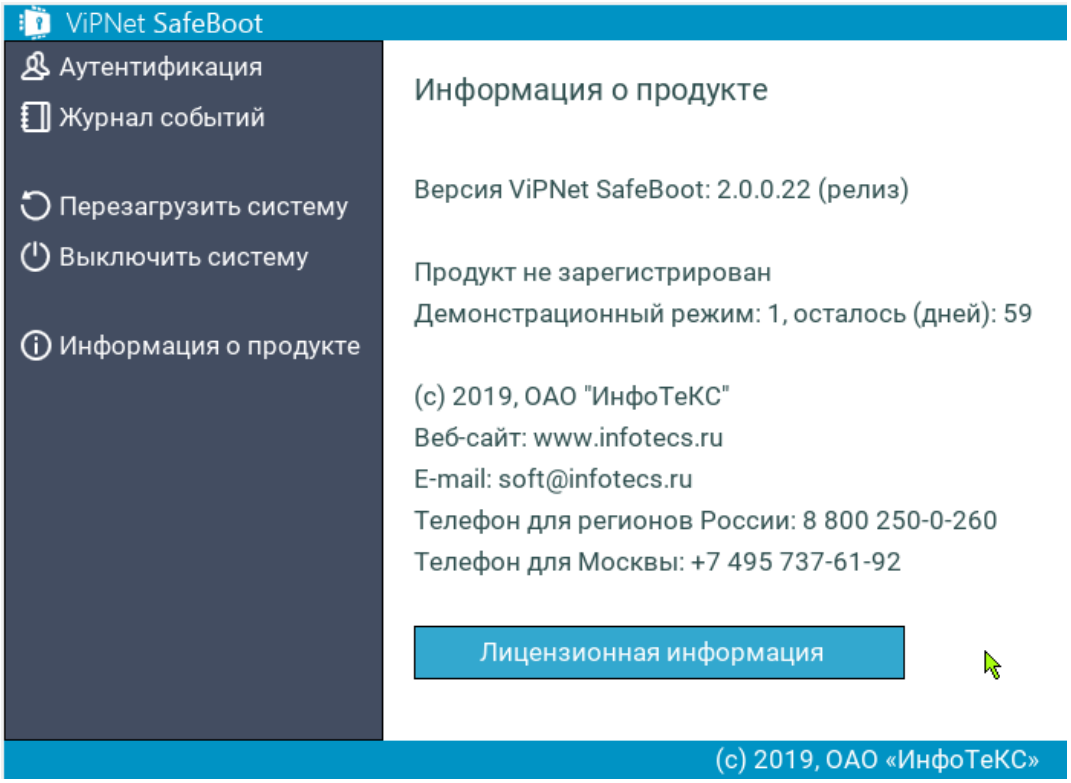


Рисунок 38. Вид меню режима настроек ViPNet SafeBoot для Аудитора

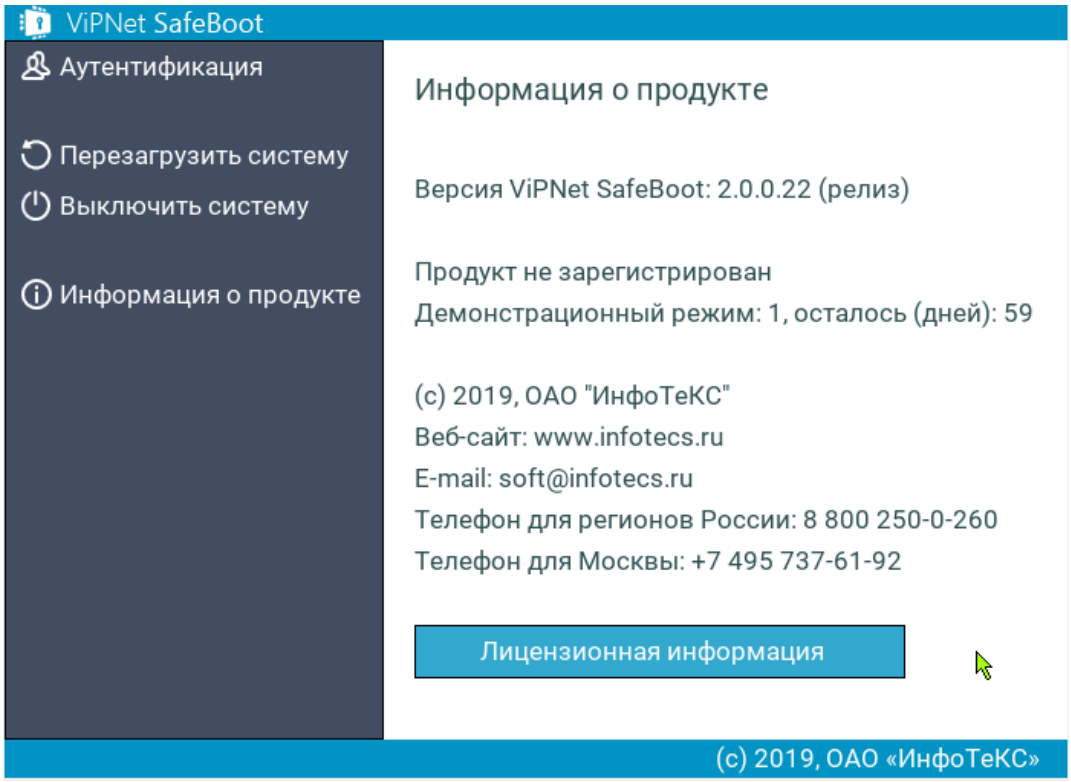


Рисунок 39. Вид меню режима настроек ViPNet SafeBoot для Пользователя

Интерфейс режима настройки

Интерфейс режима настройки представляет собой список функций для управления ViPNet SafeBoot. В графическом режиме переход к нужному пункту меню осуществляется клавишами и курсором мыши. В текстовом режиме перемещение по пунктам меню и выбор необходимого элемента осуществляется только клавишами клавиатуры:

- Стрелки вверх и вниз – перемещение вверх и вниз по пунктам меню.
- **Enter** – выбрать пункт.
- **Esc** – выход с текущей вкладки или из режима настройки, в случае нажатия Esc в основном меню.

Выбор элемента управления **Параметры загрузки ОС** позволяет:

- Задать режим загрузки ОС:
  - Legacy (режим совместимости) или UEFI.
- Выбрать загрузочное устройство (в режиме Legacy).
- Выбрать загрузочный раздел (ESP) и загрузчик операционной системы (в режиме UEFI).

Выбор элемента управления **Контроль целостности** позволяет:

- Выполнить автоопределение компонентов загрузки ОС для постановки на контроль;
- Выбрать контролируемые объекты:
  - Файлы на разделах диска.
  - CMOS, PCI, ACPI, SMBIOS, карта памяти.
  - Карта распределения памяти, модули UEFI.
  - Загрузочные сектора выбранного диска.
  - Параметры реестра Windows.
  - Журналы транзакций файловых систем NTFS, EXT3, EXT4.
- Выполнить принудительную проверку целостности контролируемых объектов.
- Выполнить перерасчет эталонов всех объектов, находящихся на контроле.

Выбор элемента управления **Аутентификация** позволяет выполнить настройки сессии аутентификации, просматривать, редактировать, удалять и создавать новые учетные записи пользователей, а также редактировать параметры учетной записи Администратора, создать диск восстановления пароля.

Выбор элемента управления **Журнал событий** позволяет просматривать и выгружать записи журнала событий, выбирать режим ведения записей в журнале и уровень регистрации событий.

Выбор элемента управления **БД конфигурации** позволяет:

- Выбрать режим ведения базы данных конфигурации: внутренний или внешний (на диске).
- Выбрать формат настроек при экспорте/импорте: бинарный или json.
- Экспортировать или импортировать настройки конфигурации.
- Сбросить настройки.
- Получить информацию о заполнении базы данных.

Выбор элемента управления **Корневые сертификаты** позволяет осуществить установку и удаление корневых сертификатов доверенного центра сертификации, а также установку, удаление и обновление списка отозванных сертификатов (CRL).

Выбор элемента управления **Сеть и LDAP** позволяет задать параметры сети и настроить аутентификацию пользователей на сервере LDAP.

Выбор элемента управления **Регистрация** позволяет зарегистрировать ViPNet SafeBoot.

Выбор элемента управления **Защита** позволяет:

- Установить защиту содержимого микросхемы BIOS от чтения и перезаписи из ОС.
- Разрешить эмуляцию NVRAM.
- Включить контроль программных SMI.
- Разрешить однократный вход в BIOS Setup.

Выбор элемента управления **Ключи** позволяет получить информацию об установленных сертификатах и ключах, изменить или удалить установленные сертификаты и ключи.

Выбор элемента управления **Удаленное управление** предоставляет пользователю функции удаленного управления настройками ViPNet SafeBoot.

Выбор элемента управления **Обновления** открывает меню для запуска автоматического поиска и установки файлов обновления с подключенного диска.

Выбор элемента управления **Перезагрузить систему** осуществляет немедленную перезагрузку системы.

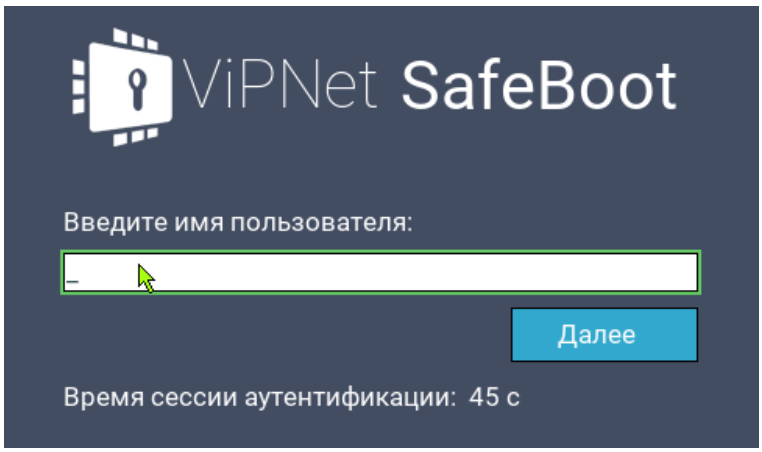
Выбор элемента управления **Выключить систему** осуществляет немедленное выключение системы.

Выбор элемента управления **Информация о продукте** открывает окно, содержащее информацию о версии и лицензии ViPNet SafeBoot.

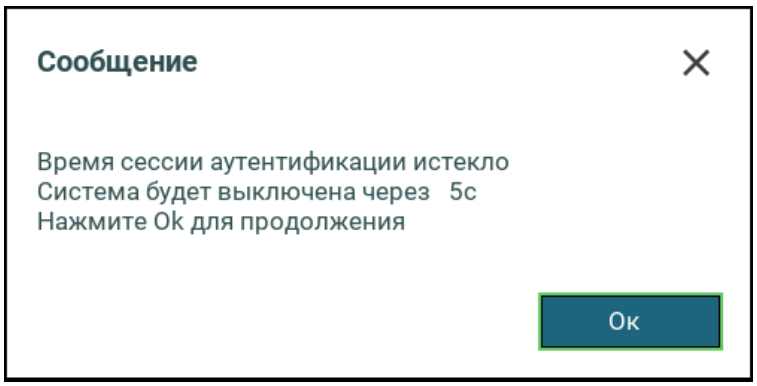
Ограничение сессии аутентификации

Опция «Ограничение сессии аутентификации» позволяет Администратору установить диапазон времени, в течении которого пользователь может пройти процедуру аутентификации. По окончании установленного Администратором времени на аутентификацию, система выключится.

Время до окончания сессии аутентификации отображается в строке **Время сессии аутентификации.** Отсчет времени ведется в обратном порядке.



Процедура аутентификации выполняется в установленном порядке (см. Запуск и завершение работы на стр. 41). Если пользователь не успеет ввести свои учетные данные до истечения установленного времени, появится следующее сообщение:



Включение и отключение опции «Ограничение сессии аутентификации» выполняется Администратором в режиме настройки ViPNet SafeBoot. По умолчанию эта опция отключена.

Чтобы ограничить время сессии аутентификации, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Аутентификация**.
3. В открывшемся окне установите флажок **Ограничение сессии аутентификации**.

Появится строка **Время сессии аутентификации**, содержащая значение **<60>** – время аутентификации по умолчанию.

4 В строке **Время сессии аутентификации** установите время из диапазона от 15 до 180 секунд.

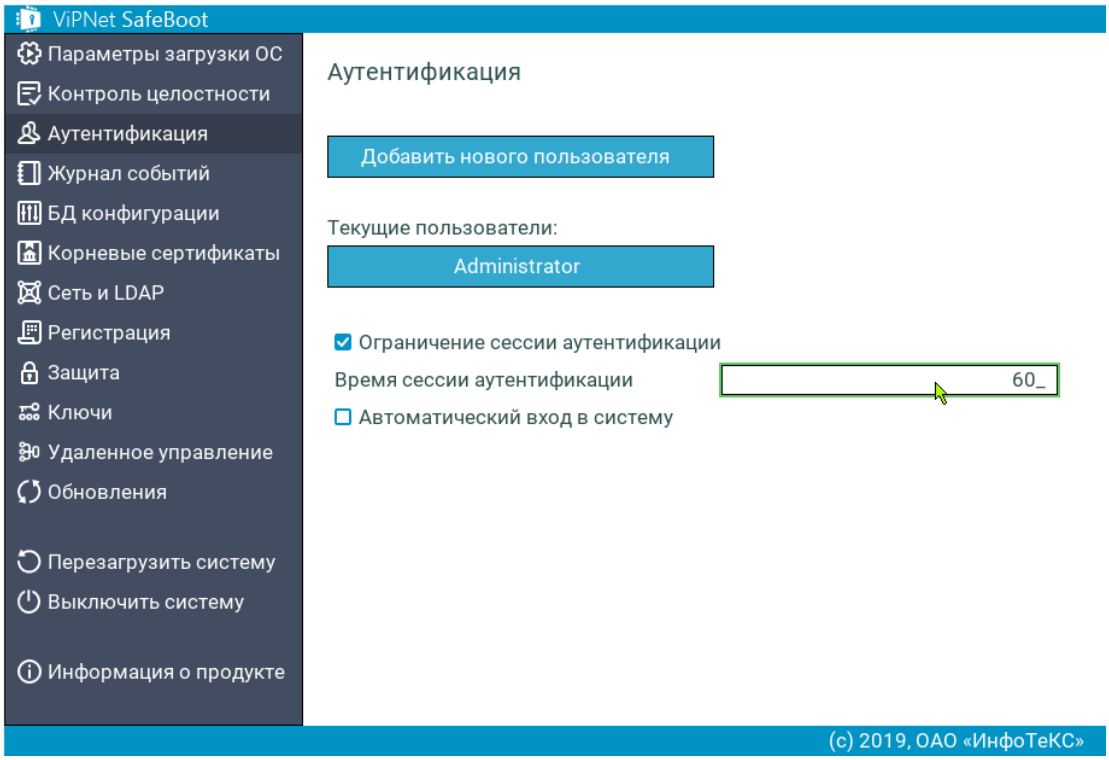


Рисунок 40. Ввод значения времени ограничения сессии аутентификации в графическом режиме

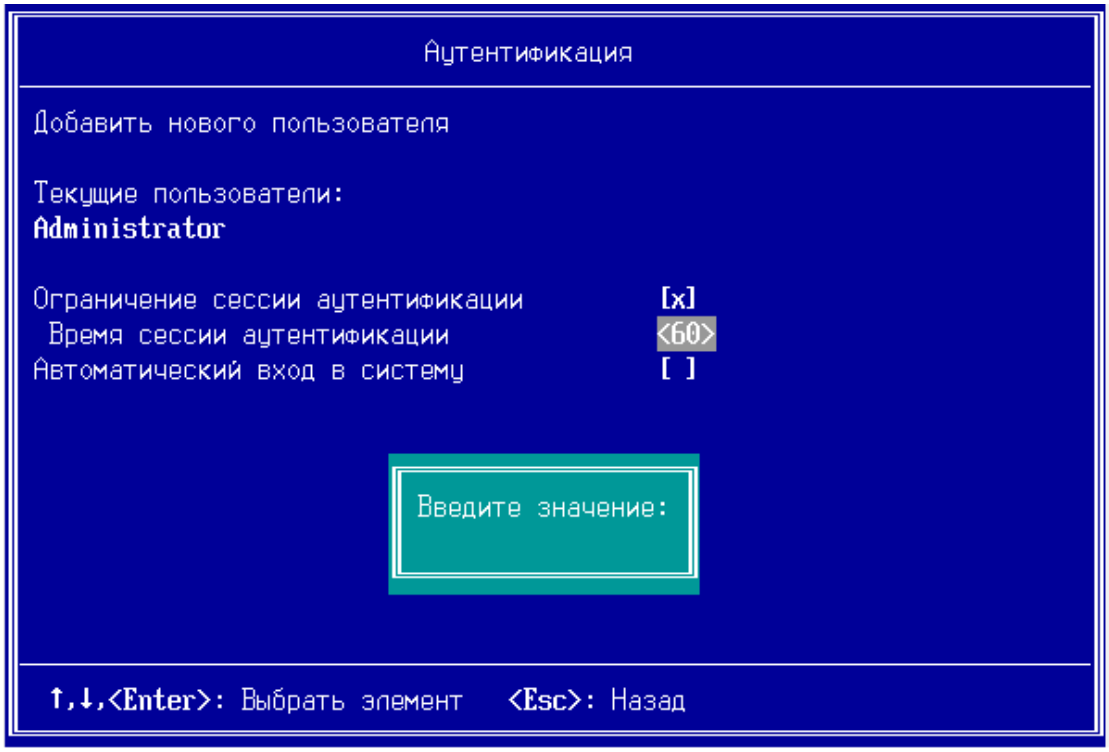


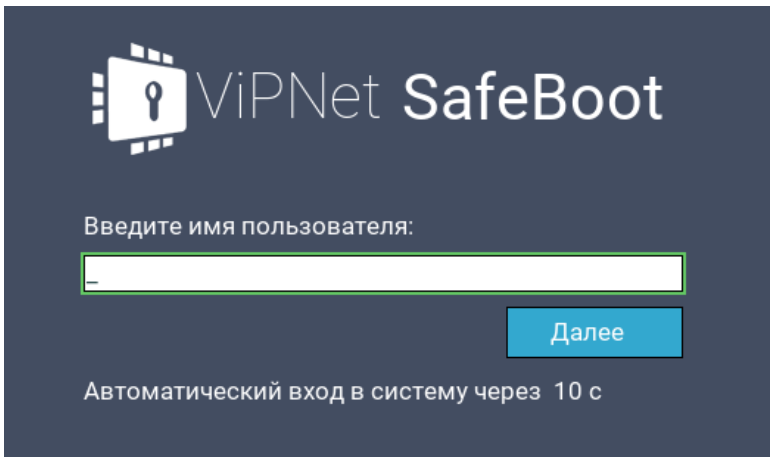
Рисунок 41. Ввод значения времени ограничения сессии аутентификации в текстовом режиме

5 Функция ограничения сессии аутентификации начнет действовать после перезагрузки.

Автоматический вход в систему

Настроенный автоматический вход в систему обеспечивает автоматическую загрузку операционной системы через установленный промежуток времени без аутентификации пользователя.

Время до автоматической загрузки операционной системы отображается в строке **Автоматический вход в систему через.** Отсчет времени ведется в обратном порядке.



Для остановки отсчета времени до автоматического входа, нажмите любую клавишу. Процедура аутентификации выполняется в установленном порядке (см. Запуск и завершение работы на стр. 41).

Настройка автоматического входа в систему выполняется Администратором в режиме настройки ViPNet SafeBoot.

Внимание! При включении флага «Автоматический вход в систему» необходимо предусмотреть организационные меры, ограничивающие доступ в помещение с таким ПМДЗ.

Для установки автоматического входа в систему выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Аутентификация**.
3. В открывшемся окне установите флажок **Автоматический вход в систему**.
4. В появившейся строке **Время до автоматического входа** установите нужное время, нажав **Enter**, или оставьте значение по умолчанию.

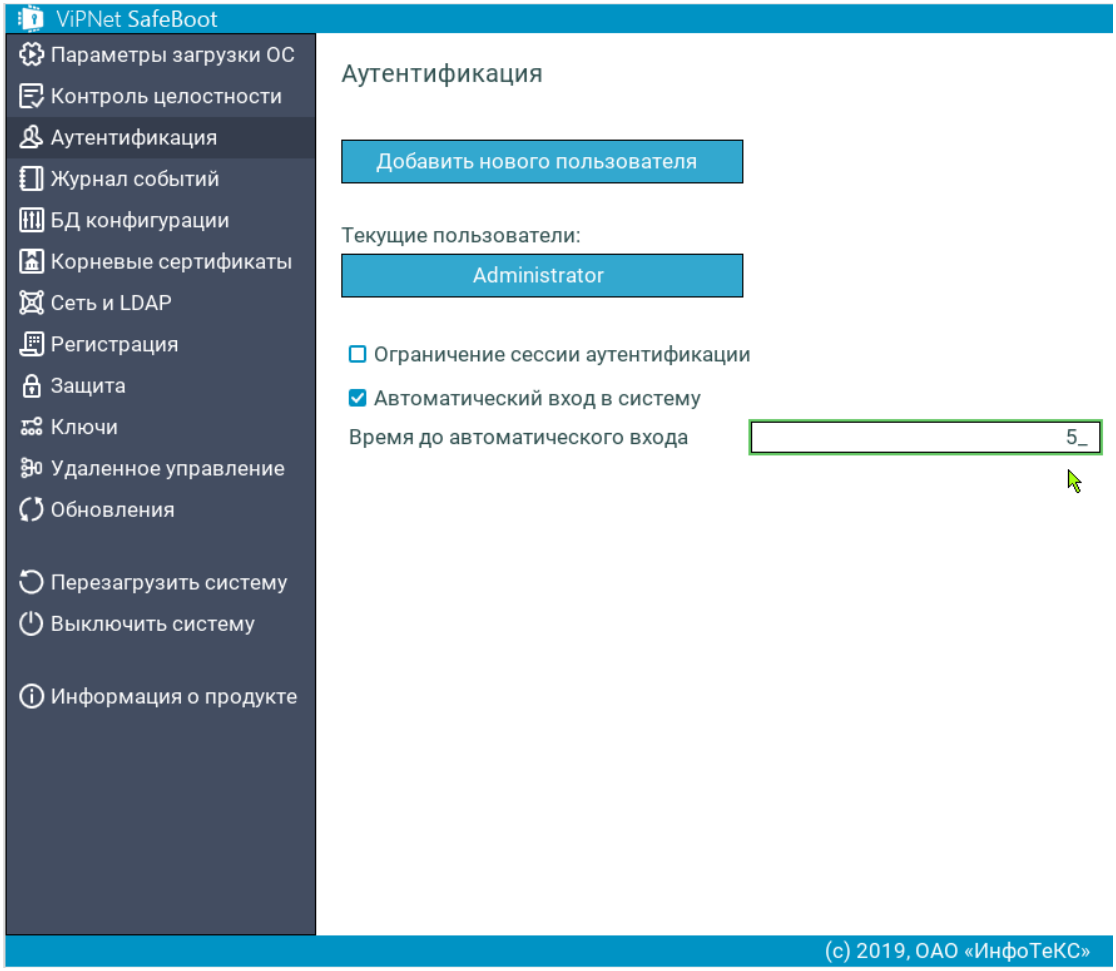


Рисунок 42. Ввод значения времени до автоматического входа в систему

5 Для выхода в основное меню нажмите **Esc**.

Эмуляция NVRAM

Эмуляция NVRAM — это подсистема эмуляции UEFI-переменных. При включенной подсистеме запись и чтение UEFI-переменных осуществляется во временную область памяти, в микросхему BIOS запись данных не производится, что позволяет предотвратить атаки на NVRAM платформы.

Включение эмуляции NVRAM может понадобиться при ошибках загрузки ОС, например, если включена защита BIOS, режим загрузки ОС — Legacy.

Чтобы установить функцию эмуляции NVRAM, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Защита**.
3. В открывшемся окне установите флажок **Эмуляция NVRAM**.

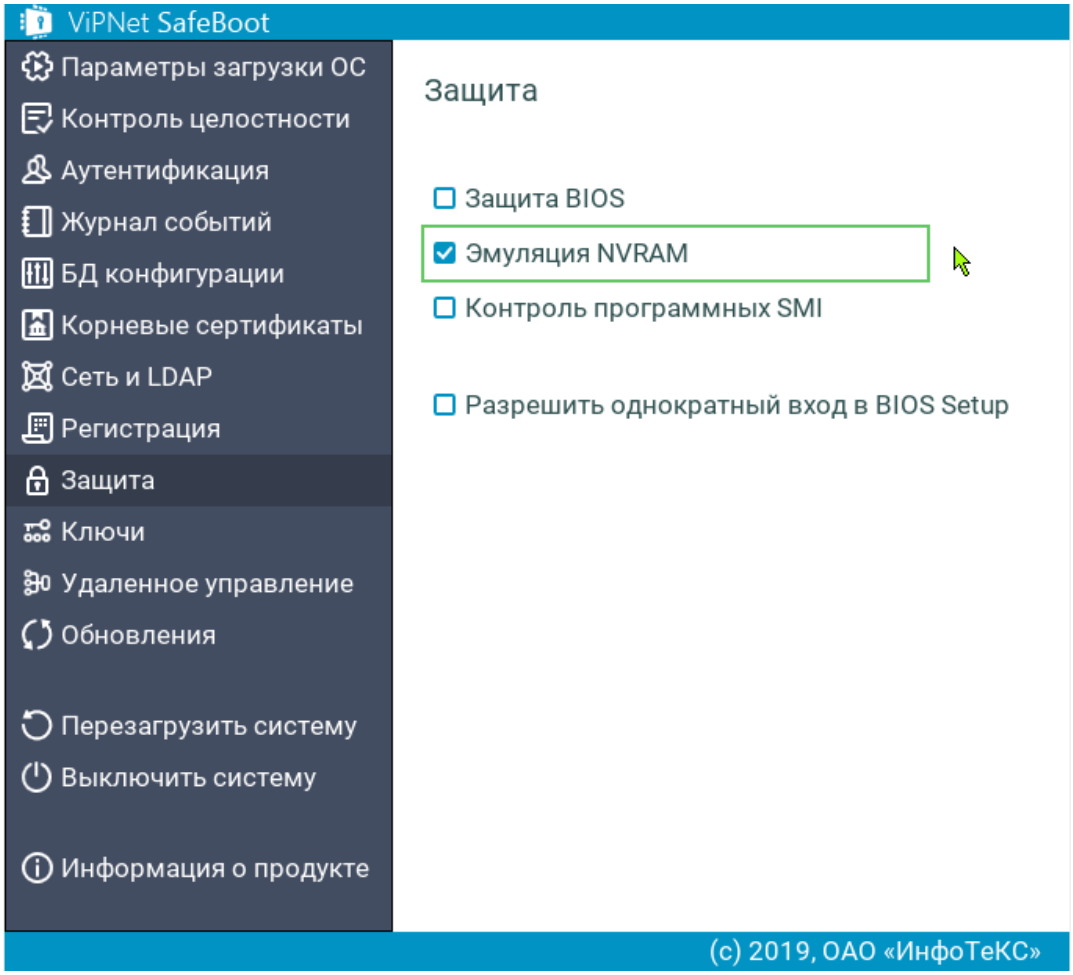


Рисунок 43. Включение функции эмуляции NVRAM в графическом режиме

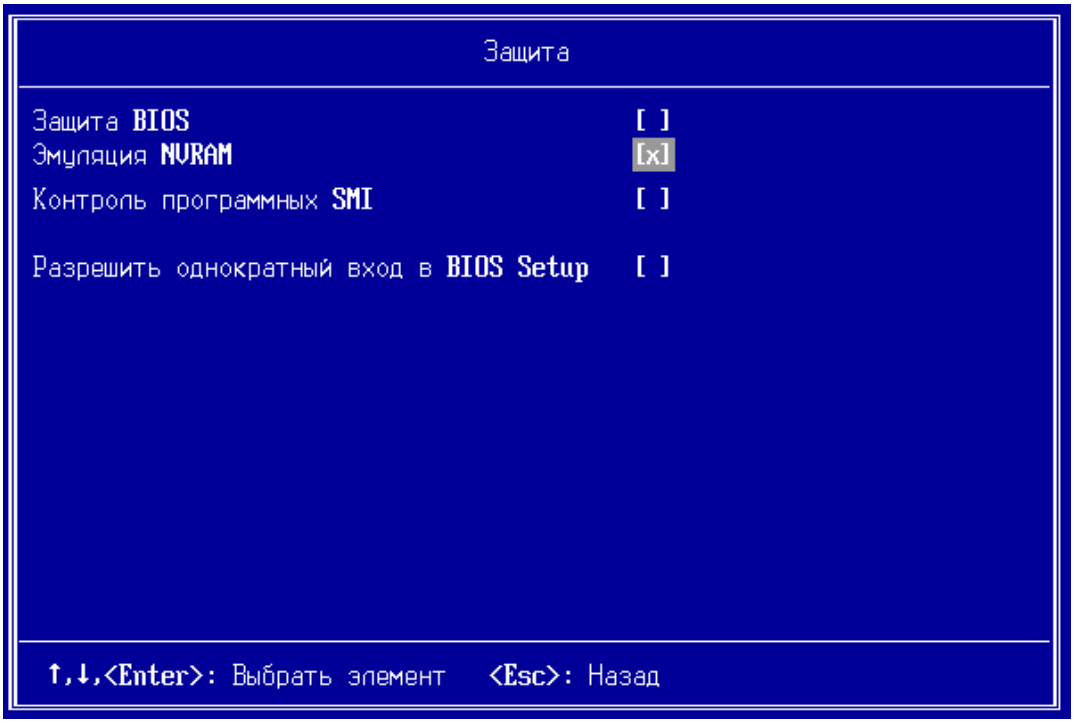


Рисунок 44. Включение функции эмуляции NVRAM в текстовом режиме

Защита BIOS

ViPNet SafeBoot обеспечивает защиту BIOS от перезаписи, чтения и от изменений EFI-переменных. В ПМДЗ предусмотрен дополнительный режим защиты при выходе из спящего режима.

Для систем с неподдерживаемым чипсетом защита не установится, на экране появится соответствующее сообщение.

Чтобы установить функцию защиты BIOS, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Защита**.
3. В открывшемся окне установите флажок **Защита BIOS**.

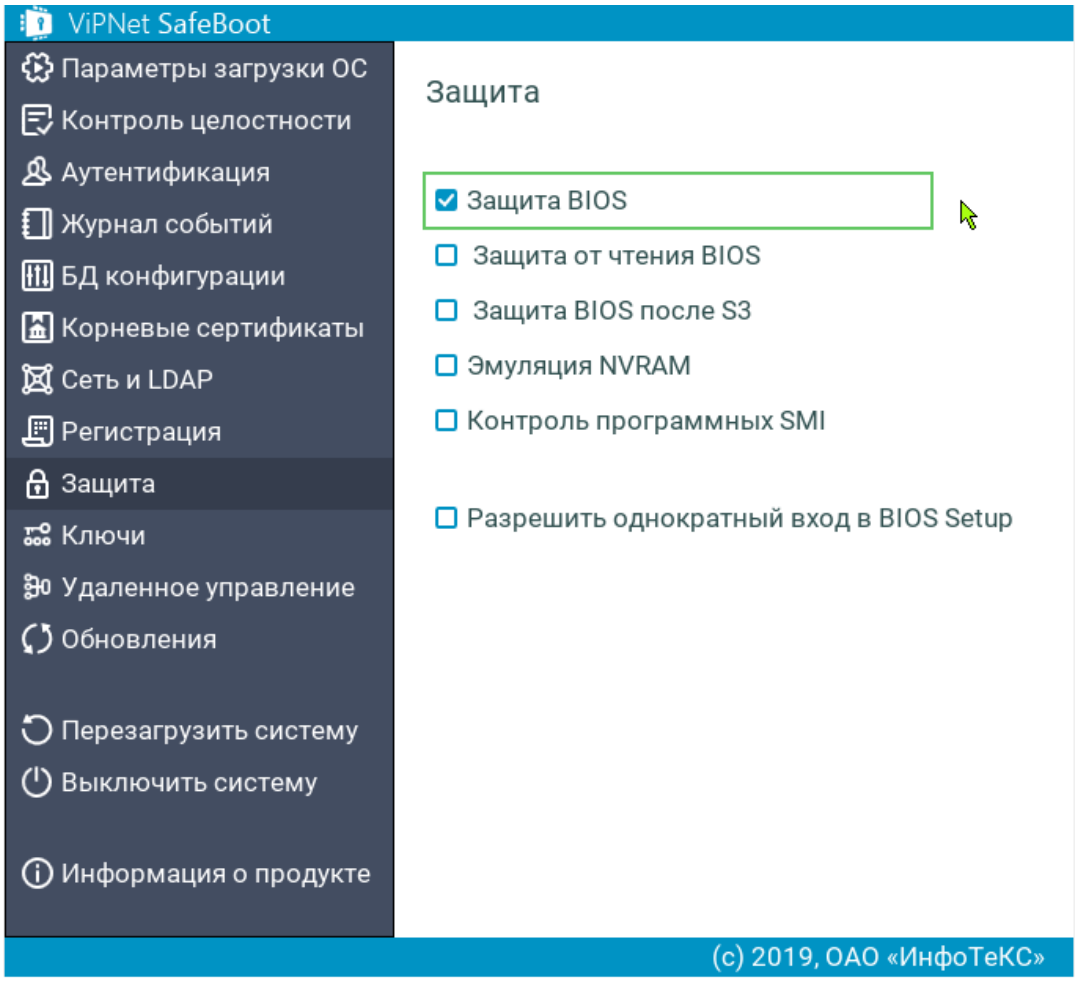


Рисунок 45. Включение функции защиты BIOS

4 Для включения функции защиты от чтения содержимого микросхемы BIOS, установите флажок **Защита от чтения BIOS**.

Примечание. Для применения функции защиты от чтения BIOS, необходимо, чтобы была включена эмуляция NVRAM (см. на стр. 61)

5 Для включения функции защиты BIOS при выходе из спящего режима, установите флажок **Защита BIOS после S3**.

Примечание. Чтобы функция защиты вступила в силу, понадобится перезагрузка системы.

Контроль программных SMI

ViPNet SafeBoot позволяет включать фильтрацию программных SMI и ограничивать функциональность, реализованную на основе программных SMI.

Чтобы установить функцию контроля программных SMI, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Защита**.
3. В открывшемся окне установите флажок **Контроль программных SMI**.

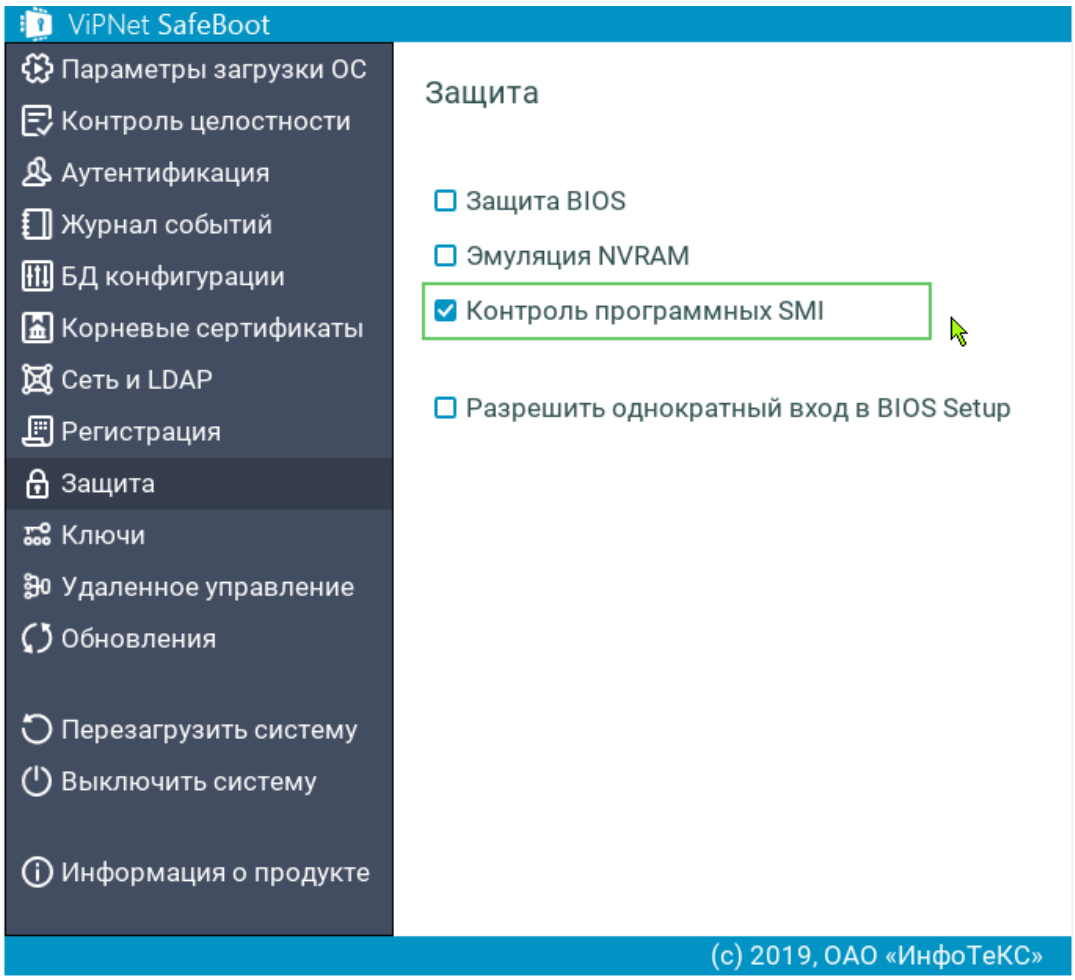


Рисунок 46. Включение функции контроля программных SMI

Вход в BIOS Setup

ViPNet SafeBoot блокирует вход в BIOS Setup для исключения загрузки нештатной операционной системы и изменения параметров конфигурации.

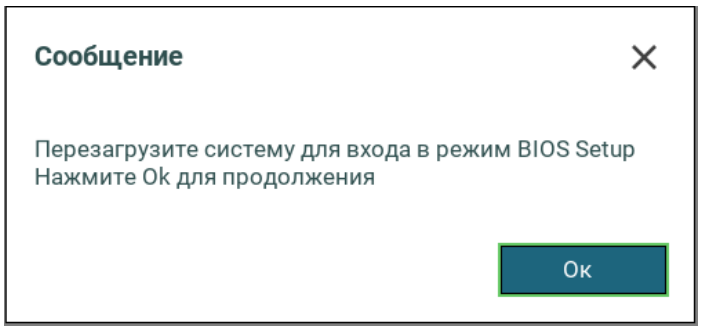
Для однократного входа в BIOS Setup выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Защита**.

3 В открывшемся окне установите флажок **Разрешить однократный вход в BIOS Setup**.

Появится сообщение о необходимости перезагрузить систему:



4 Нажмите **Ok** или **Enter** для выхода в основное меню режима настройки.

5 В меню режима настройки выберите **Перезагрузить систему**.

После перезагрузки будет доступно меню настроек BIOS.

Удаленное управление

ViPNet SafeBoot обеспечивает возможность удаленного управления путем изменения настроек и получения журнала продукта с помощью специализированного ПО уровня ОС. Непосредственное управление администратором группой СВТ с установленным ViPNet SafeBoot осуществляется централизовано из единой консоли управления.

Взаимодействие между ViPNet SafeBoot и специализированным ПО уровня ОС происходит с помощью запросов управления, формируемых специализированным ПО уровня ОС и обрабатываемых ViPNet SafeBoot.

Аутентификация запроса управления обеспечивается посредством его подписи **Сертификатом КЦ запросов управления**, предварительно установленным в настройках ViPNet SafeBoot (см. Изменение сертификатов и ключей на стр. 142). Запрос управления представляет собой файл с содержимым в виде списка файлов (БД и эталонов КЦ продукта) и зафиксированных контрольных сумм по ним, чем обеспечивается КЦ запроса управления.

В случае включения удаленного управления в настройках продукта:

1. В начале работы ViPNet SafeBoot – происходит проверка наличия запроса управления на диске (в директории EFI\Infotecs\mgmt), его аутентификация и КЦ, выполнение запроса управления (импорт БД и эталонов КЦ продукта), фиксирование результата выполнения запроса управления.
2. По завершении работы ViPNet SafeBoot – БД (в зашифрованном виде) и журнал продукта сохраняются на диск (в директорию EFI\Infotecs\mgmt), и в дальнейшем используются специализированным ПО уровня ОС.

Для включения функции удаленного управления выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Удаленное управление**.

   В открывшемся окне установите флажок **Разрешить удаленное управление**.

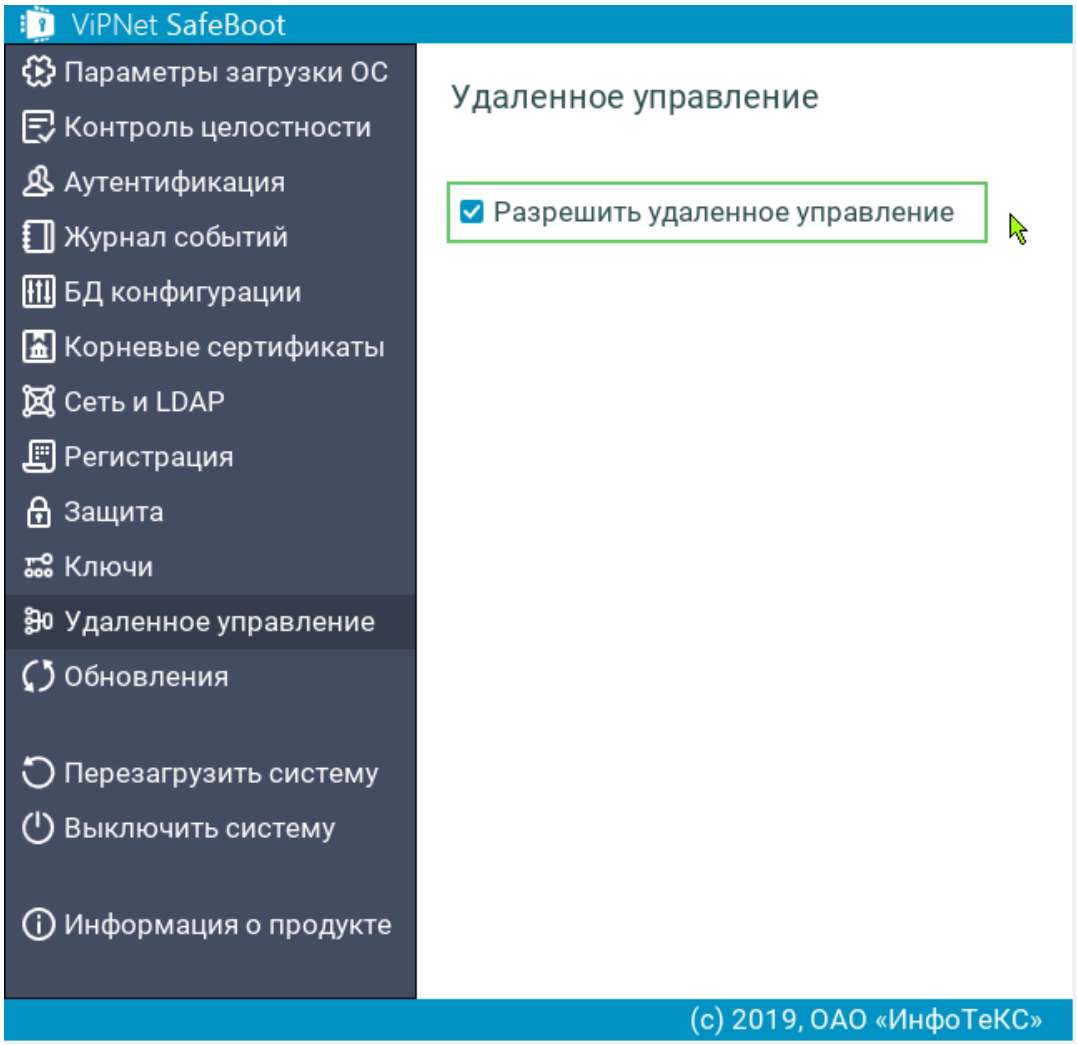


Рисунок 47. Включение функции удаленного управления

5

База данных конфигурации

Ведение базы данных конфигурации

Ведение базы данных конфигурации ViPNet SafeBoot по умолчанию осуществляется во внутренней памяти BIOS. В настройках **БД конфигурации** можно выбрать режим ведения базы данных конфигурации на внешнем диске.

Для выбора режима ведения базы данных конфигурации на внешнем диске, выполните следующие действия:

1. Войдите в режим настройки ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **БД конфигурации**.
3. В открывшемся окне выберите **Режим ведения БД конфигурации**.

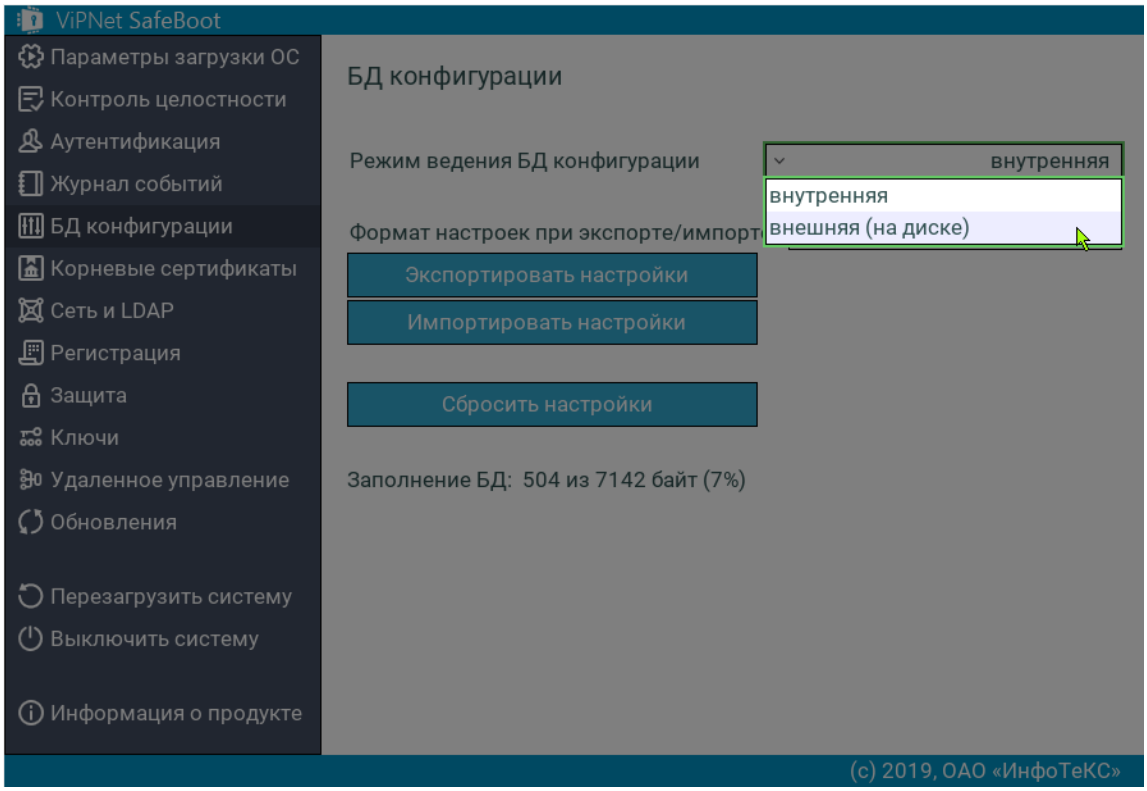


Рисунок 48. Выбор режима ведения БД конфигурации в графическом режиме

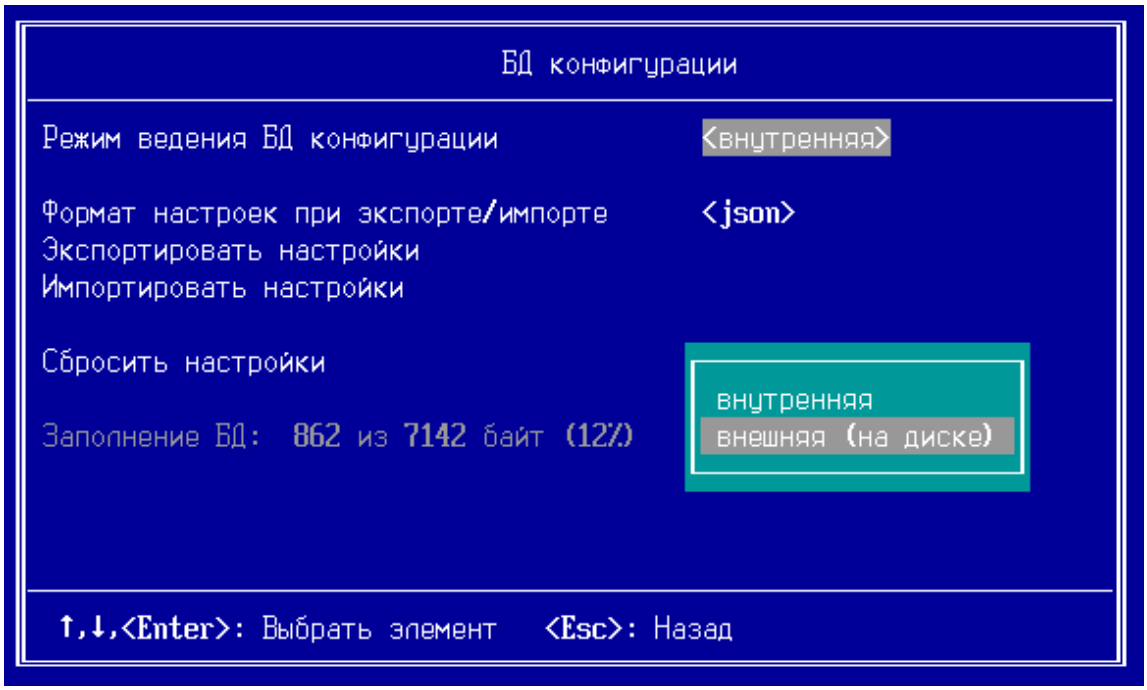


Рисунок 49. Выбор режима ведения БД конфигурации в текстовом режиме

Формат настроек при экспорте/импорте

Настройки базы данных конфигурации могут быть экспортированы и импортированы в следующих форматах:

- Json.
- Бинарный.

Для выбора формата настроек при экспорте/импорте, выполните следующие действия:

1 Войдите в режим настройки ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **БД конфигурации**.

3 В открывшемся окне выберите **Формат настроек при экспорте/импорте**.

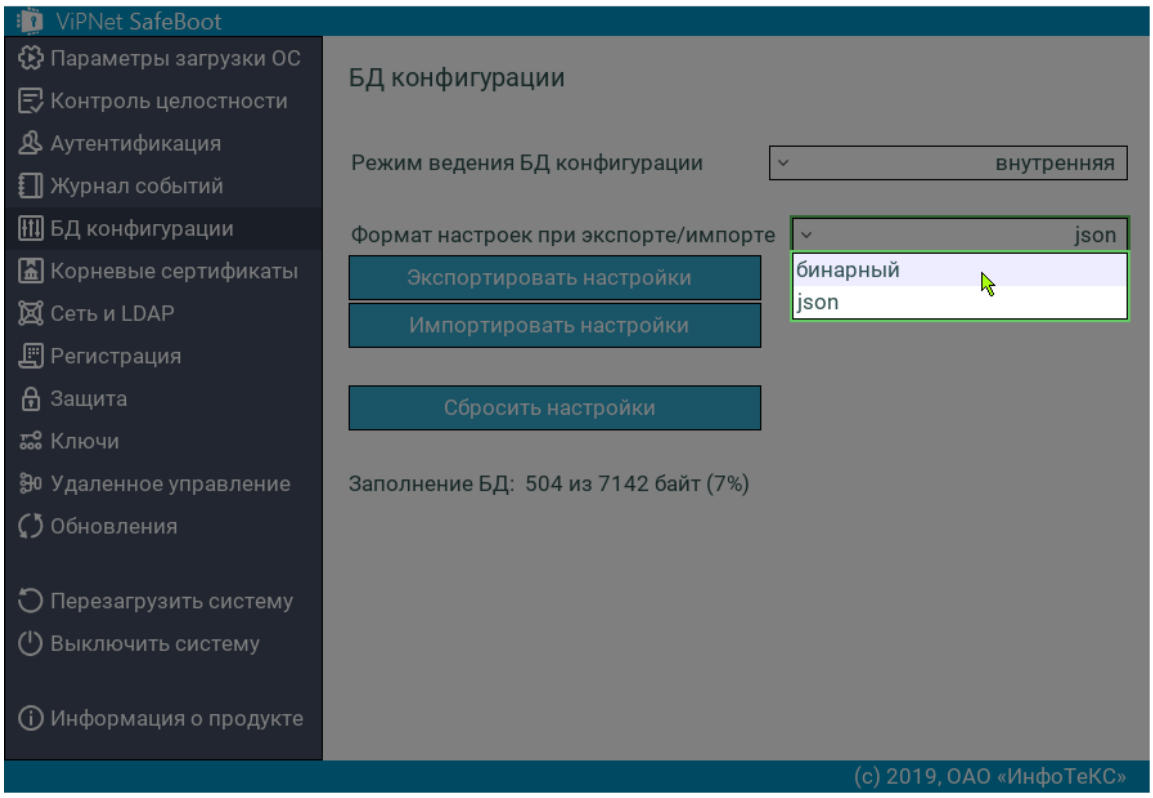


Рисунок 50. Выбор формата настроек при экспорте/импорте

Экспорт настроек

Экспорт настроек осуществляется на первый найденный USB-диск в фиксированный файл **itsbdb.bin** (в корень раздела), также на диске появляется файл с подписью **itsbdb.bin.sig**. Для формата json имена файлов будут **itsbdb.json** и **itsbdb.json.sig** соотвестенно.

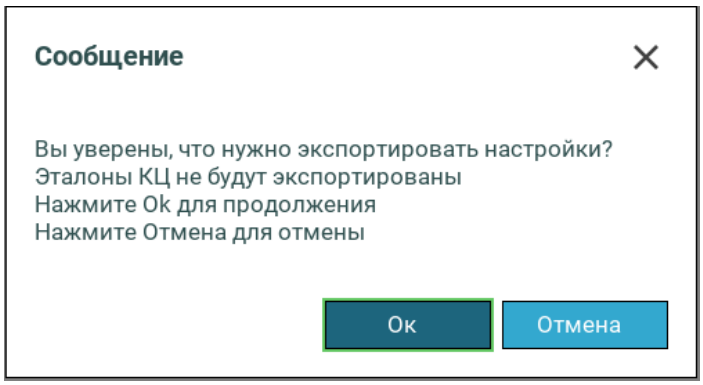
Экспортируются (и далее могут быть импортированы), в частности, следующие настройки:

- Общие настройки:
  - Параметры загрузки операционной системы.
  - Настройки процедуры входа в систему.
  - Значение режима защиты BIOS.
- Учетные записи пользователей и настройки аутентификации.
- Корневые сертификаты.

Чтобы экспортировать настройки, выполните следующие действия:

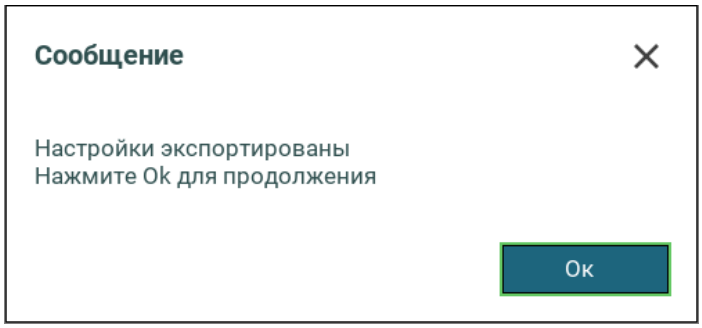
1. Вставьте USB-диск в соответствующий разъем.
2. Войдите в режим настройки ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
3. В меню режима настроек выберите **БД конфигурации**.
4. В открывшемся окне выберите **Экспортировать настройки**.

   Появится окно с предупреждением:



5 Нажмите **Ок**.

После завершения экспорта появится следующее сообщение:



Импорт настроек

Чтобы импортировать настройки, выполните следующие действия:

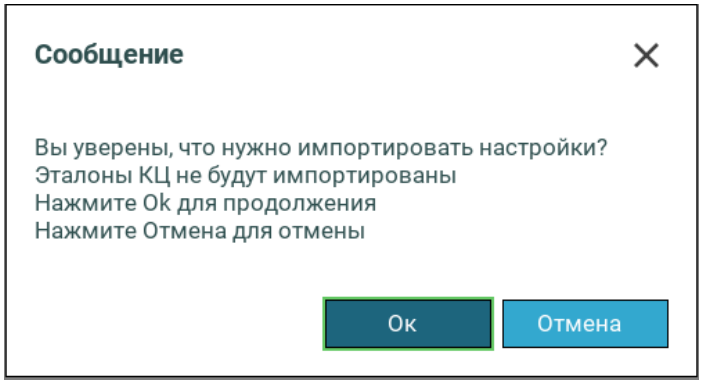
1 Вставьте USB-диск, содержащий файлы настроек **itsbdb.bin** и **itsbdb.bin.sig**, в соответствующий разъем. Если выбран формат настроек json, то имена файлов настроек должны быть **itsbdb.json** и **itsbdb.json.sig.**

2 Войдите в режим настройки ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

3 В меню режима настроек выберите **БД конфигурации**.

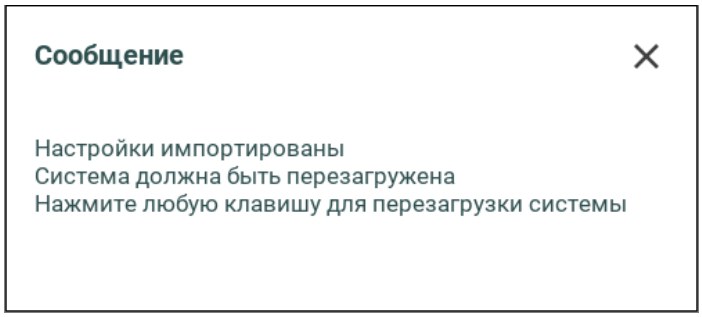
4 В открывшемся окне выберите **Импортировать настройки**.

Появится окно с предупреждением:



5 Нажмите **Ок**.

После успешного импорта настроек появится сообщение о необходимости перезагрузить систему.



6 Нажмите любую клавишу, система перезагрузится.

Сброс настроек

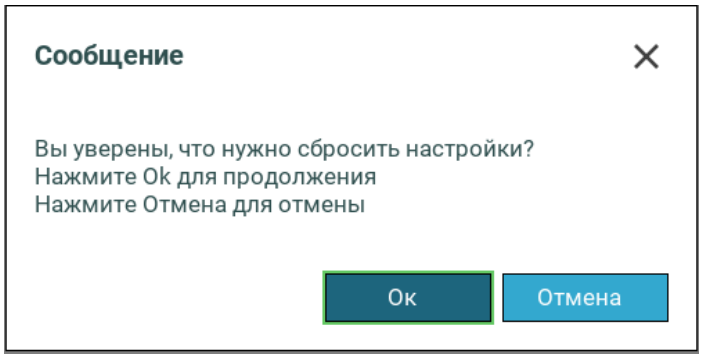
Чтобы сбросить настройки базы данных конфигурации, выполните следующие действия:

1 Войдите в режим настройки ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **БД конфигурации**.

3 В открывшемся окне выберите **Сбросить настройки**.

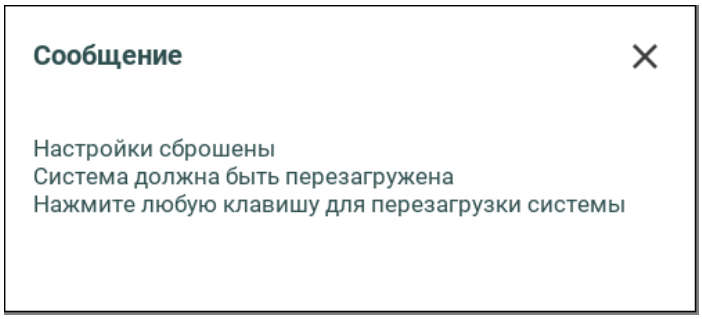
Появится окно с предупреждением:



Внимание! При сбросе настроек будут удалены все изменения, сделанные в меню Режима настроек, до первоначального состояния (при первом запуске).

4 Нажмите **Ок**.

Через некоторое время появится сообщение о необходимости перезагрузить систему.



5 Нажмите любую клавишу, система перезагрузится.

Управление режимами загрузки операционной системы

Режим загрузки операционной системы

ViPNet SafeBoot поддерживает следующие режимы загрузки ОС:

- Использование параметров загрузки BIOS.

  ViPNet SafeBoot использует порядок загрузки ОС, определенный в BIOS Setup.

- Legacy (режим совместимости).

  Данный режим подходит для загрузки практически всех ОС, включая Microsoft Windows XP и более ранних.

- UEFI.

  Режим UEFI подходит для загрузки современных ОС (начиная с Windows Vista) для процессоров с поддержкой x86-64 (AMD64/Intel64).

При выборе режима загрузки операционной системы необходимо руководствоваться документацией на используемую ОС.

Использование параметров загрузки BIOS

Для загрузки ОС с использованием параметров, определенных в BIOS Setup, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Параметры загрузки ОС**.

3 В открывшемся окне выберите **Использовать параметры загрузки BIOS** и нажмите **Enter**.

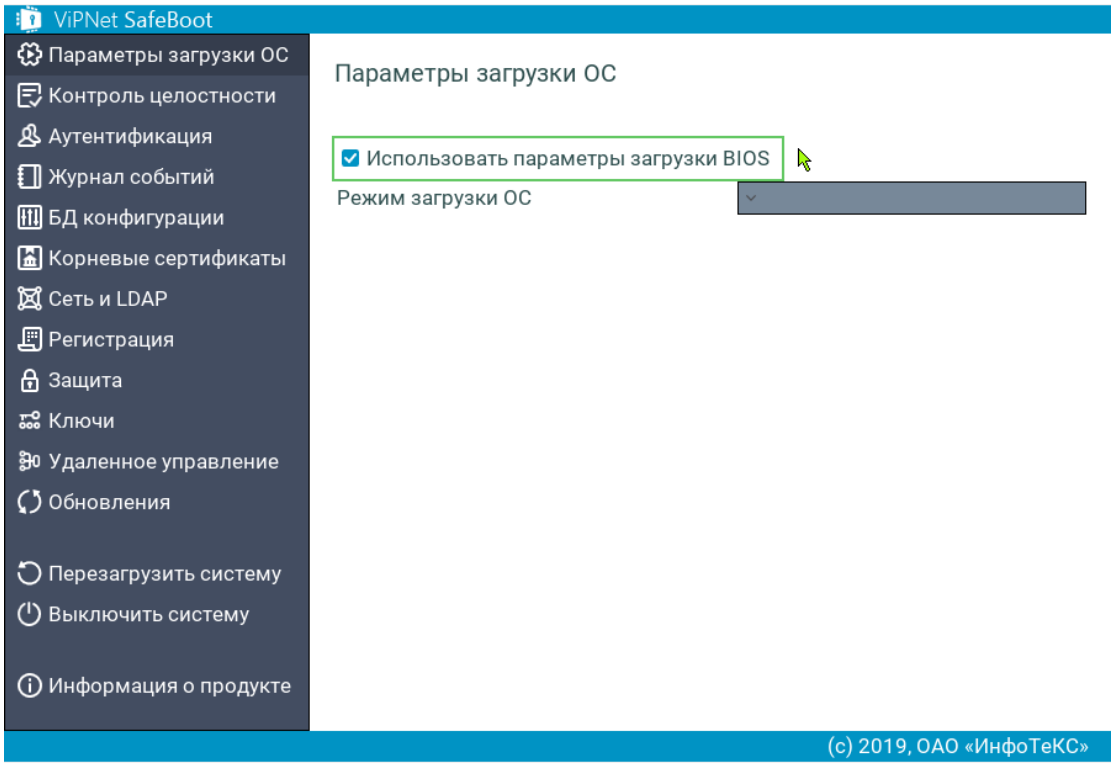
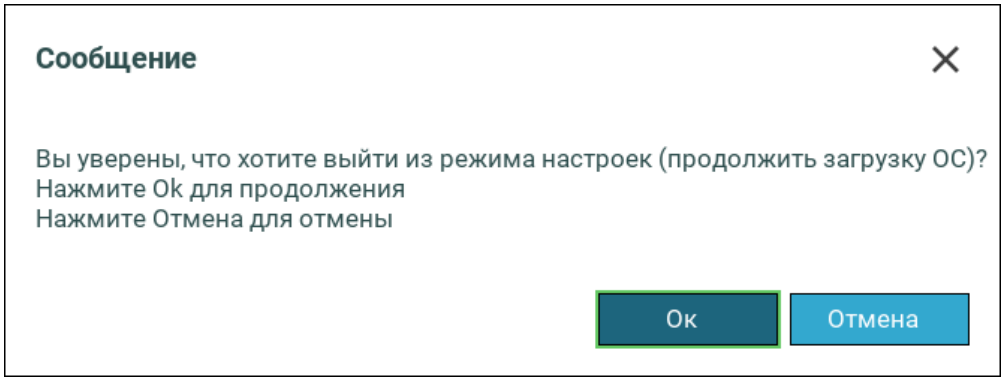


Рисунок 51. Выбор режима загрузки операционной системы

4 В основное меню режима настроек ViPNet SafeBoot нажмите **Esc** для выхода из режима настройки и начала загрузки операционной системы в выбранном режиме.

5 Появится окно со следующим сообщением:



Для начала загрузки ОС нажмите **Ок**.

Загрузка операционной системы в режиме совместимости

Для выбора загрузочного устройства в режиме совместимости (legacy), выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Параметры загрузки ОС**.

3 В открывшемся окне выберите **Режим загрузки ОС**.

4 В меню **Режим загрузки ОС** выберите из списка **legacy (режим совместимости)**.

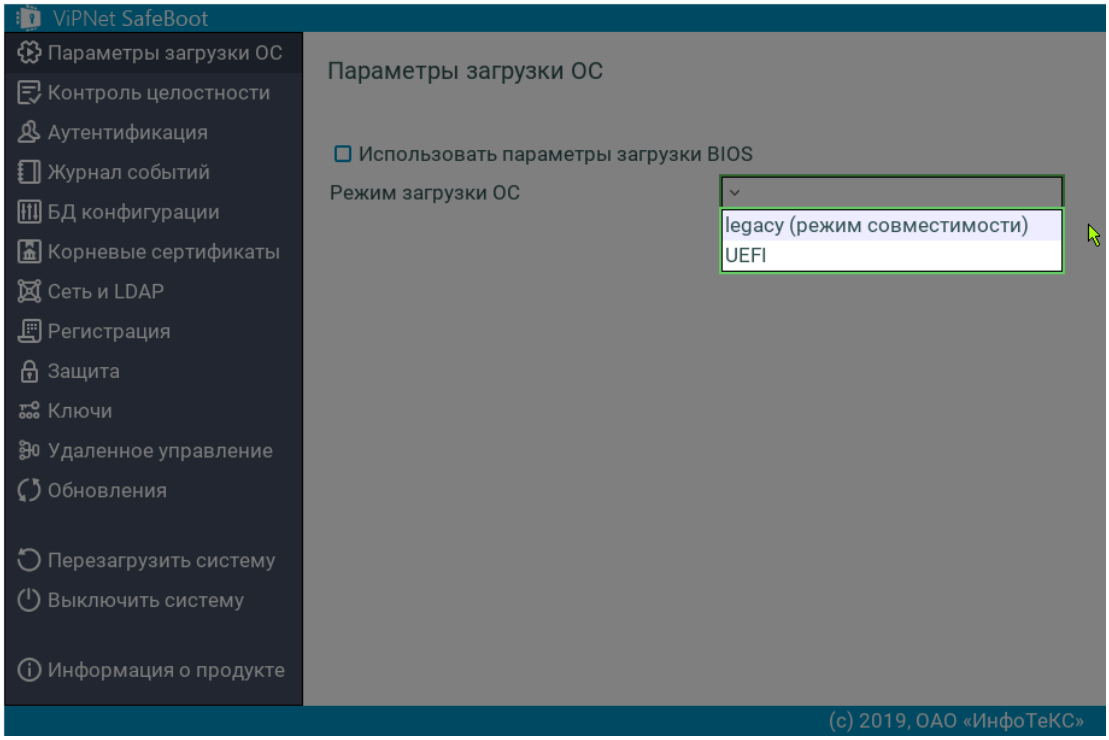


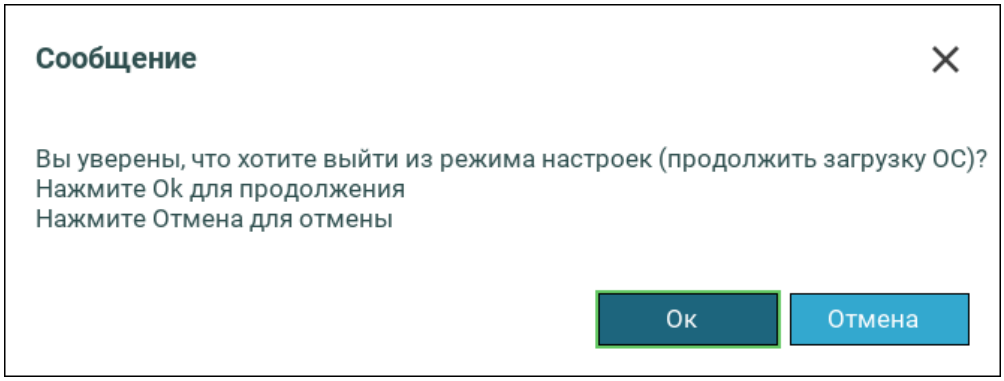
Рисунок 52. Меню выбора режима загрузки операционной системы — legacy (режима совместимости)

5 Выберите **Загрузочное устройство**.

Из списка выберите нужное загрузочное устройство.

6 В основном меню режима настроек ViPNet SafeBoot нажмите **Esc** для выхода из режима настройки и начала загрузки операционной системы в выбранном режиме.

7 При появлении следующего сообщения, нажмите **Ок** для начала загрузки ОС:



Загрузка операционной системы в режиме UEFI

Для выбора загрузочного устройства в режиме UEFI, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Параметры загрузки ОС**.

3 В открывшемся окне выберите **Режим загрузки ОС**.

4 В меню **Режим загрузки ОС** выберите из списка **UEFI**.

5 Выберите **Загрузочный раздел (ESP)**.

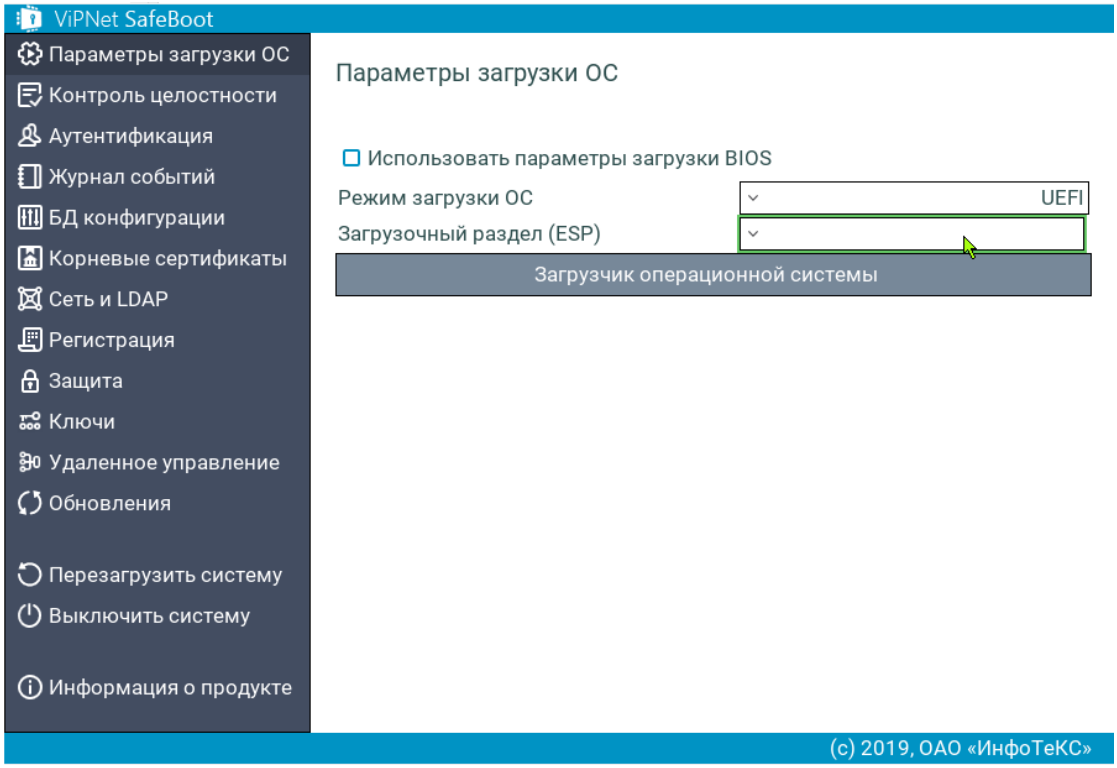


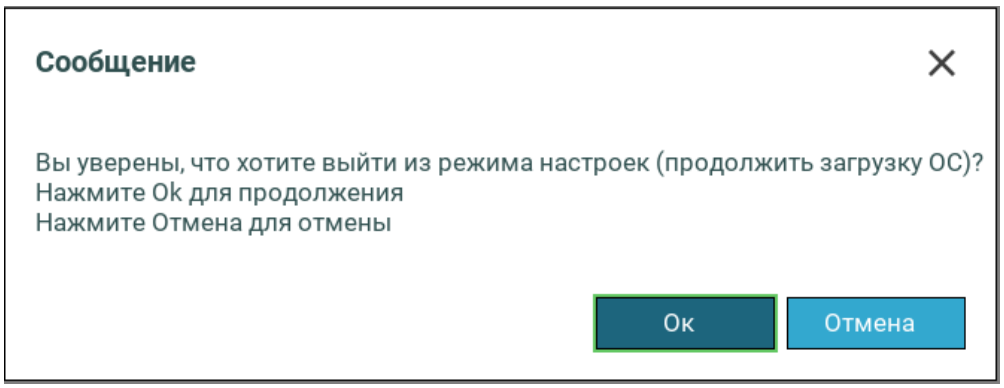
Рисунок 53. Выбор загрузочного раздела при выборе загрузки UEFI

Из открывшегося списка выберите нужный загрузочный раздел.

6 В пункте меню **Загрузчик операционной системы** выберите непосредственно файл загрузчика ОС.

7 В основном меню режима настроек ViPNet SafeBoot нажмите **Esc** для выхода из режима настройки и начала загрузки операционной системы в выбранном режиме.

8 При появлении следующего сообщения, нажмите **Ок** для начала загрузки ОС:



Временное отключение функциональности ViPNet SafeBoot

Для экстренных случаев предусмотрена загрузка операционной системы в режиме отключения функциональности ViPNet SafeBoot. Для выполнения загрузки операционной системы в таком режиме выполните следующие действия:

1. Подготовьте диск восстановления (см. Создание диска восстановления на стр. 106).
2. Подключите USB-диск, инициализированный как диск восстановления.
3. Для отключения функциональности ViPNet SafeBoot при загрузке нажмите сочетание клавиш **Правый Ctrl + x.**

В случае успеха, ViPNet SafeBoot будет временно отключен и осуществлена обычная процедура старта BIOS и загрузки операционной системы. При последующих загрузках компьютера без указанных выше действий, функциональность ViPNet SafeBoot полностью восстановится.

6

Контроль целостности

Контролируемые объекты

Выбор объектов для контроля целостности может быть выполнен автоматически при помощи функции автоопределения компонентов загрузки ОС или вручную.

ViPNet SafeBoot позволяет осуществлять контроль целостности следующих типов объектов:

- Файлы на файловых системах FAT32, NTFS, EXT2, EXT3 и EXT4;
- Содержимое энергонезависимой памяти CMOS;
- Ресурсы конфигурационного пространства PCI/PCIe;
- Таблицы ACPI;
- Таблицы SMBIOS;
- Карты распределения памяти;
- Образы BIOS;
- Загрузочные секторы на носителях информации;
- Реестр Windows;
- Завершенность транзакций в журналах файловых систем NTFS, EXT3 и EXT4.

Перед загрузкой ОС ViPNet SafeBoot осуществляет проверку поставленных на контроль Администратором объектов. В случае нарушения целостности загрузка ОС блокируется, в журнал заносится сообщение о данном событии.

Администратор имеет возможность провести принудительную проверку целостности всех контролируемых объектов (см. Принудительная проверка целостности на стр. 103), а также выполнить перерасчет эталонов (см. Перерасчет эталонных контрольных сумм на стр. 102).

Автоопределение компонентов загрузки ОС

При запуске функции автоопределения компонентов загрузки ОС выполняется сканирование ОС, в результате чего ее компоненты (файлы и ключи реестра) автоматически ставятся на контроль. Автоматическое построение списков контроля может быть выполнено только для ОС Windows 7 и далее. Для Linux и других ОС данная функция недоступна.

Чтобы запустить автоматическое построение списков контроля, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Контроль целостности**.
3. Выберите **Автоопределение компонентов загрузки ОС**.

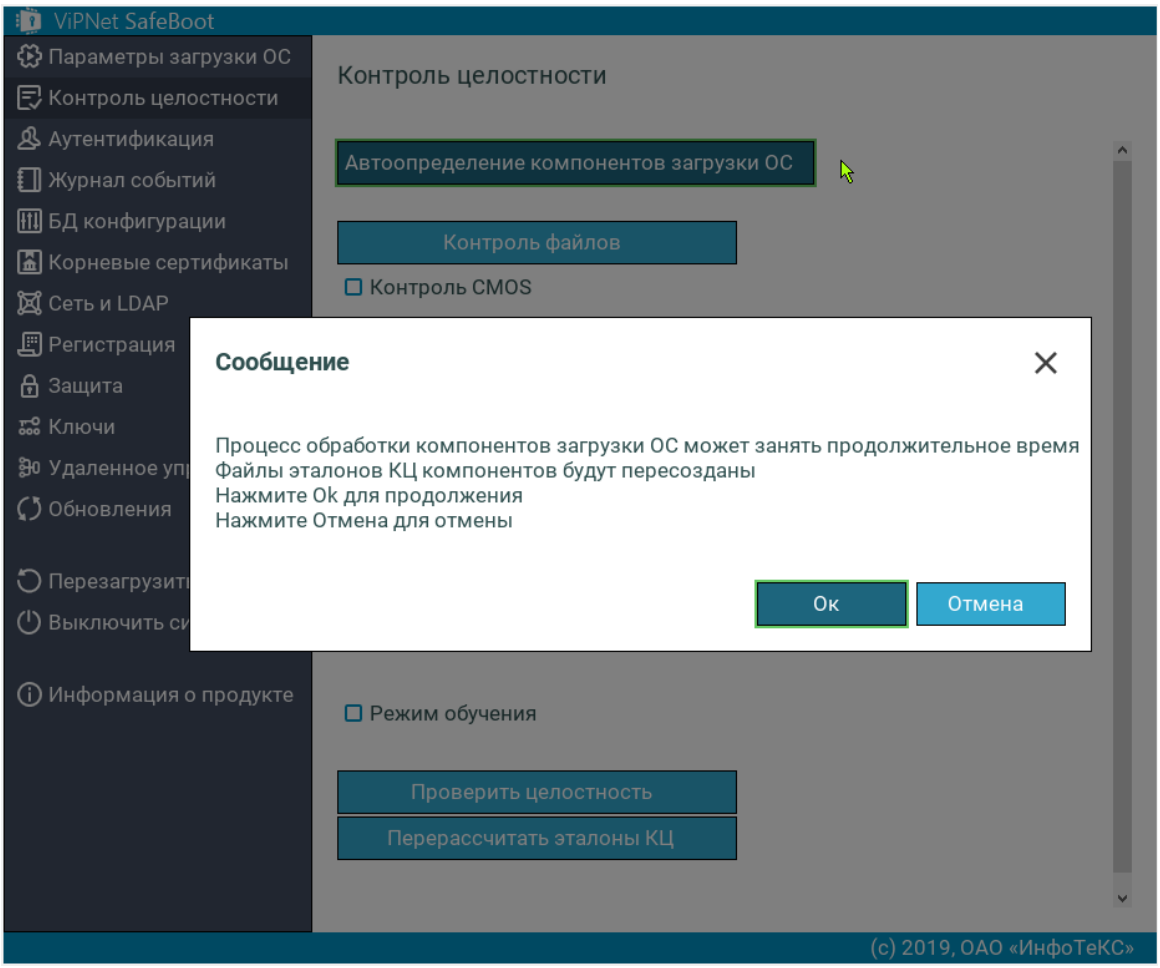
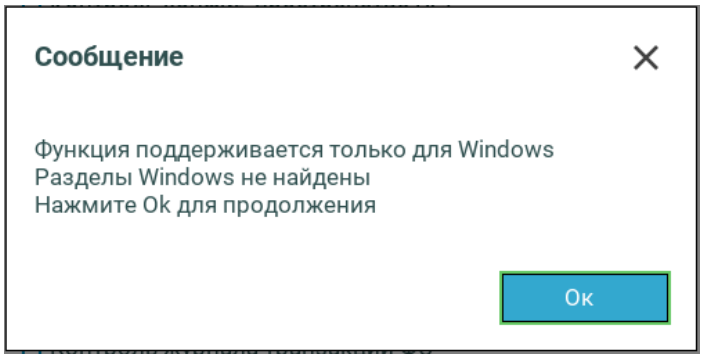


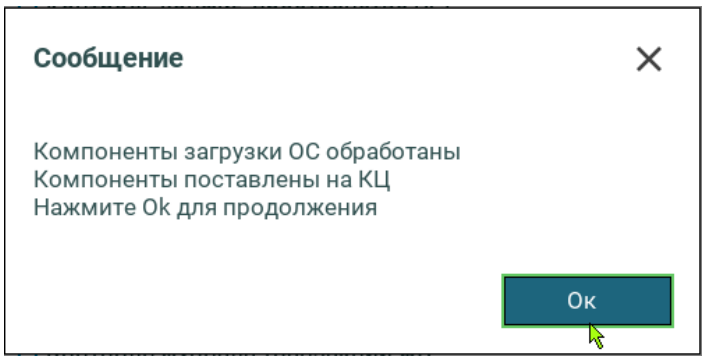
Рисунок 54. Меню Контроль целостности

4 Нажмите **Ок** для начала обработки компонентов загрузки ОС.

В случае если установлена ОС, отличная от Windows, появится следующее сообщение:



При успешном завершении обработки компонентов загрузки ОС появится следующее сообщение:



Нажмите **Ок** для продолжения.

Контроль разделов и файлов

Чтобы выбрать разделы и файлы, для которых будет проводиться контроль целостности, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Контроль целостности**.

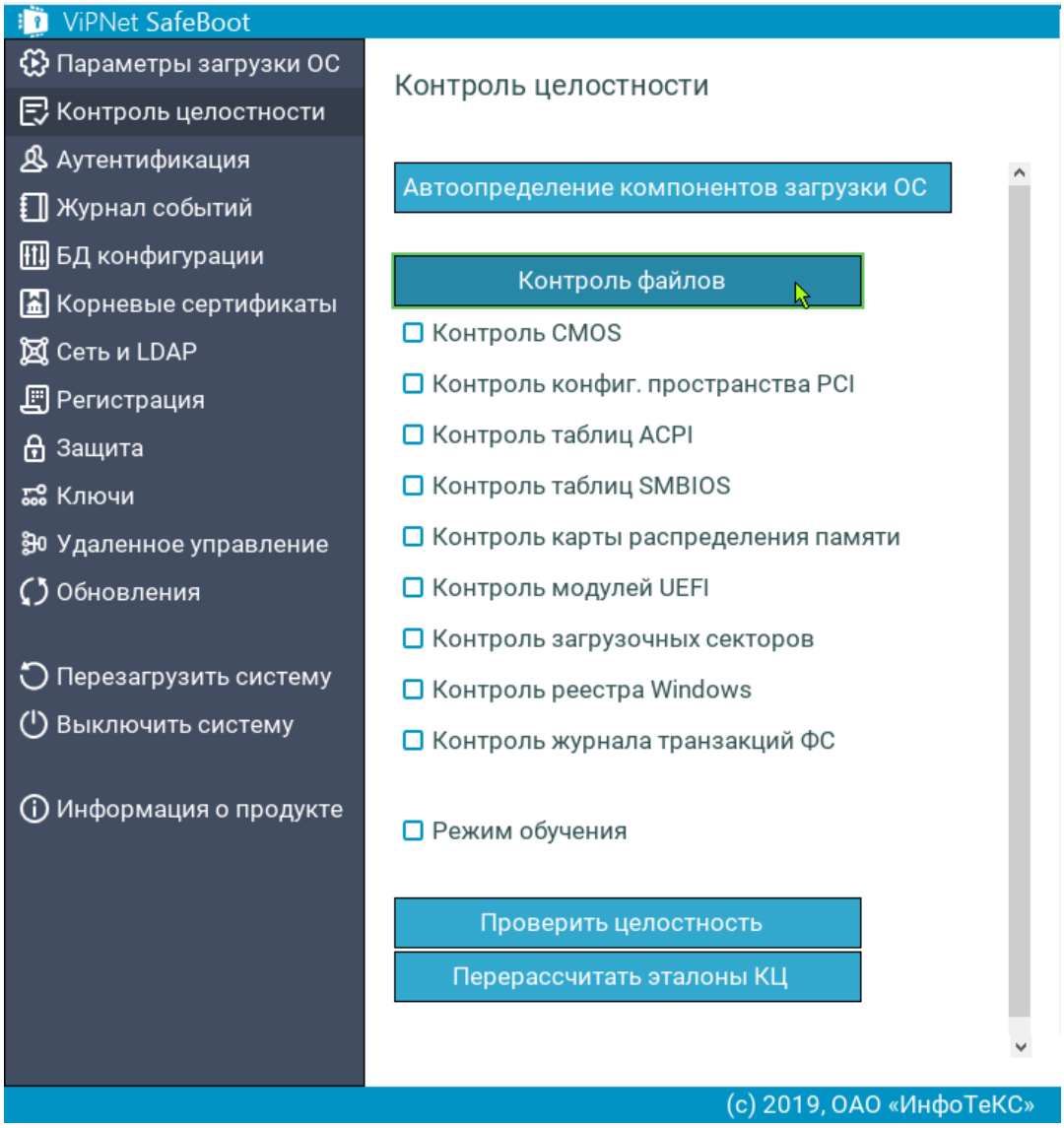


Рисунок 55. Меню Контроль целостности в графическом режиме

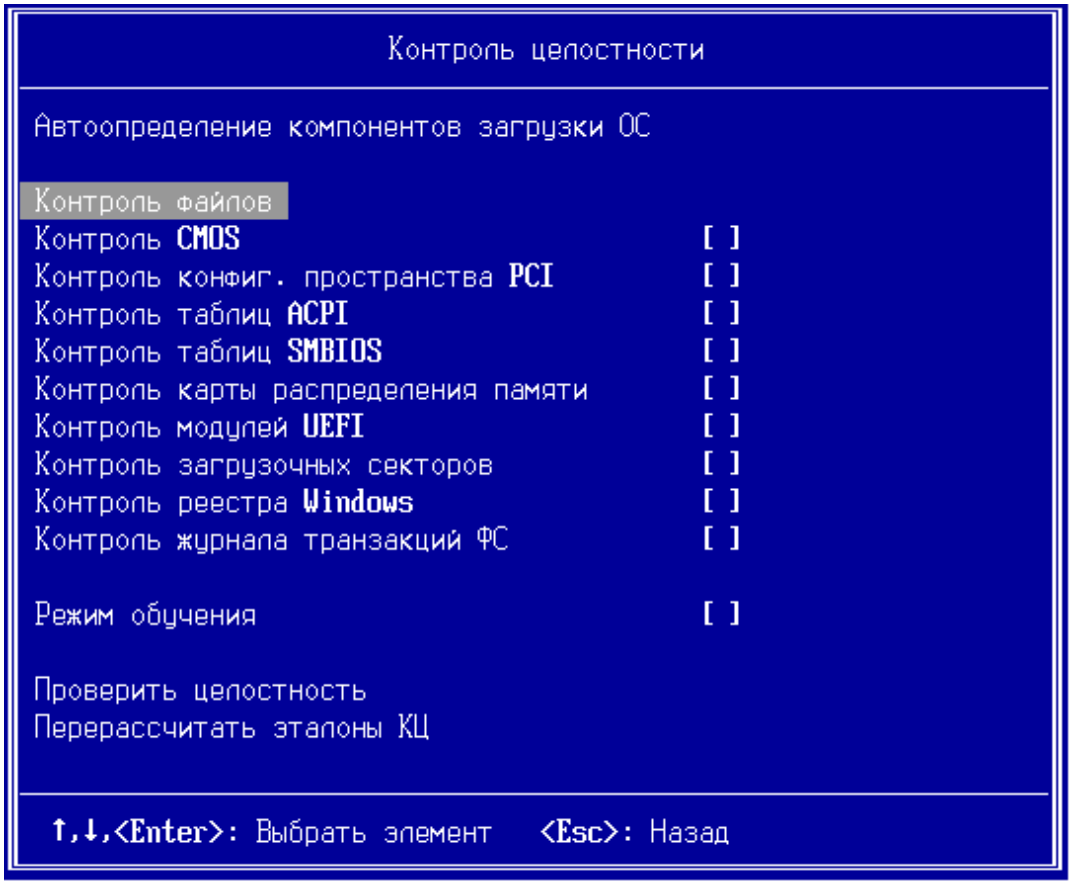


Рисунок 56. Меню Контроль целостности в текстовом режиме

3 Для добавления в список контроля целостности раздела, выберите пункт меню **Контроль файлов**.

4 Далее выберите **Добавить раздел**.

В открывшемся окне выберите из списка нужный раздел. После выполнения этой операции, раздел будет отображен в списке контролируемых разделов.

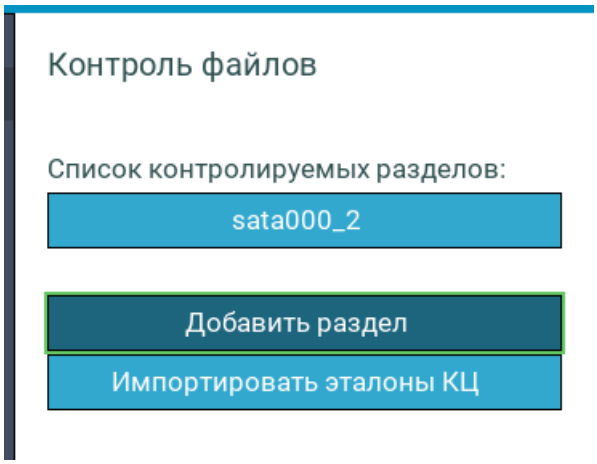


Рисунок 57. Меню контроля файлов

Внимание! Список контролируемых разделов ограничен 8 записями. Возможен одновременный контроль не более 8 разделов на всех подключенных устройствах.

5 Для операций контроля файлов выберите нужный раздел из пункта меню **Список контролируемых разделов**.

В отрывшемся окне (см. рис. 58) доступны следующие операции над файлами:

- **Список контролируемых файлов** – просмотр списка контролируемых файлов на разделе файловой системы и их контрольных сумм.
- **Импортировать эталоны КЦ раздела** – импорт файла эталонов контроля целостности раздела из указанного источника.
- **Добавить файл в список** – постановка файла на контроль.
- **Удалить файл из списка** – удаление файла из списка контролируемых.
- **Не контролировать раздел** – удаление раздела и всех файлов из списка контролируемых объектов. В последствии при выборе пункта меню «Обновить информацию о разделах», раздел будет включен в список контролируемых объектов.

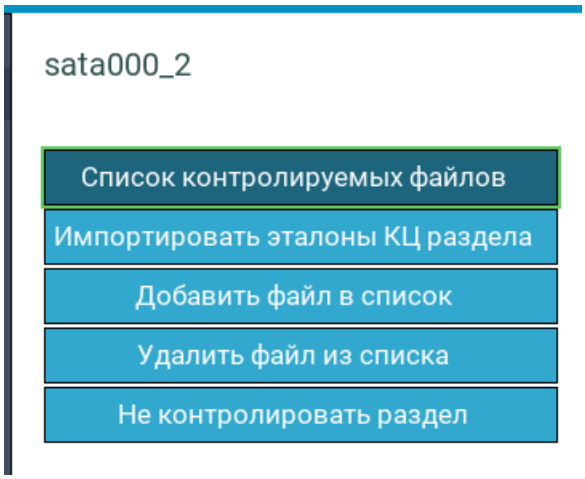


Рисунок 58. Операции контроля файлов

Для постановки на контроль файла, выполните следующие действия:

1 Выберите пункт **Добавить файл в список**.

2 В открывшемся окне выберите необходимый файл.

3 Для просмотра поставленных на контроль файлов выберите **Список контролируемых файлов**.

В открывшемся окне Администратор может просмотреть все контролируемые на разделе файлы и их контрольные суммы.

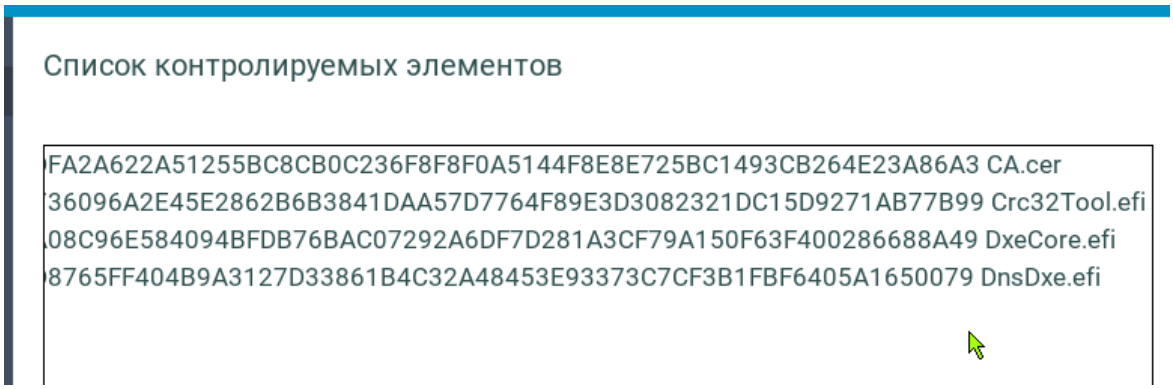


Рисунок 59. Список контролируемых файлов на разделе файловой системы

Для удаления файла из списка контролируемых объектов, выполните следующие действия:

1. Выберите пункт **Удалить файл из списка**.
2. В открывшемся окне выберите необходимый файл, нажав **Enter**.

Для импорта эталонов контроля целостности, выполните следующие действия:

1. Выберите пункт **Импортировать эталоны КЦ раздела**.
2. В открывшемся окне выберите раздел, где хранится файл эталона КЦ. Далее выберите нужный файл.

Для удаления всех файлов и раздела из списка контролируемых объектов выберите пункт **Не контролировать раздел**, при этом сами эталоны раздела не удаляются и могут быть повторно использованы.

Контроль состава аппаратных средств

Для контроля состава подключенных аппаратных средств, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Контроль целостности**.

3 В меню **Контроля целостности** выберите пункт **Контроль конфиг. пространства PCI**.

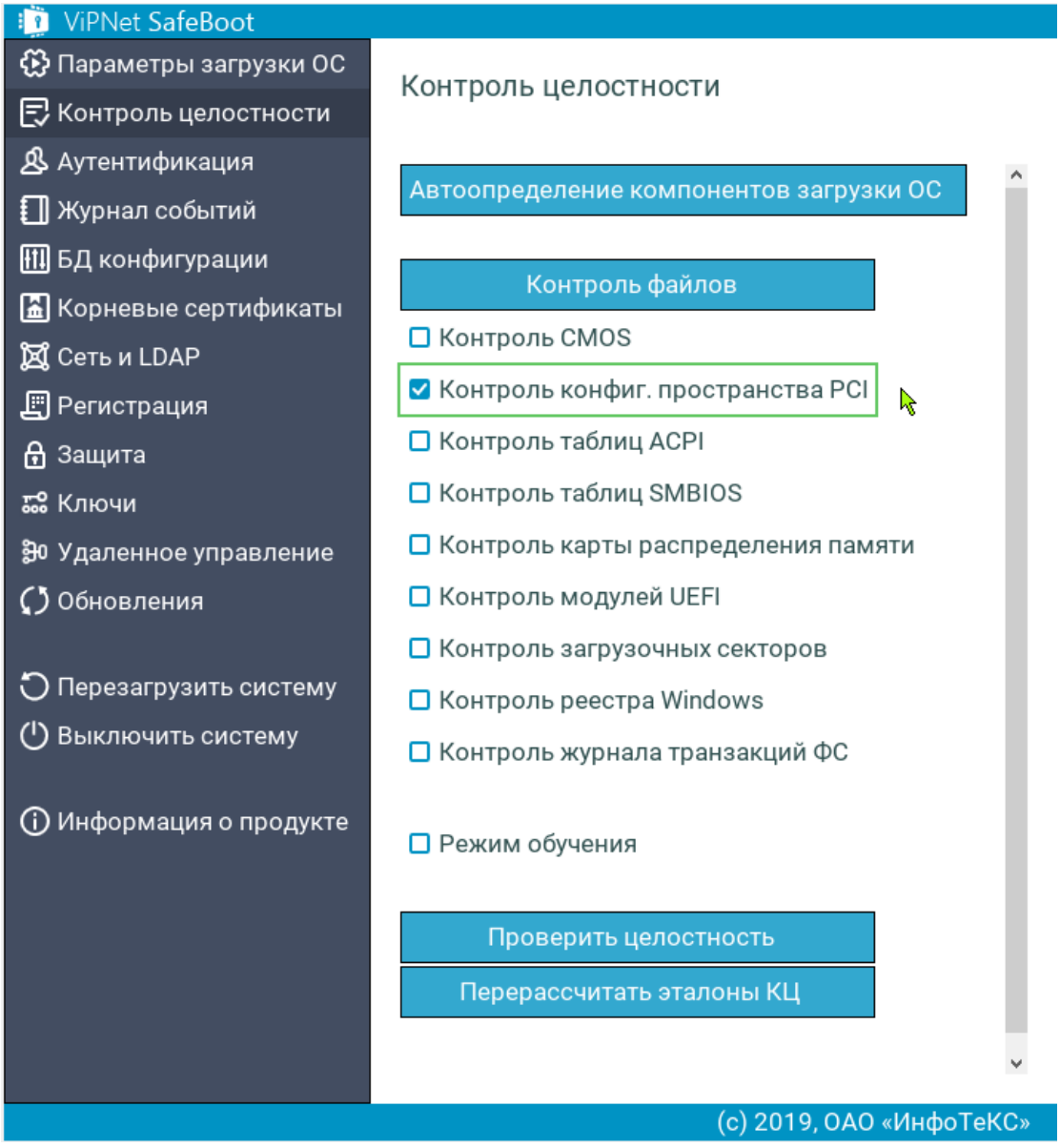


Рисунок 60. Расчет эталонов контрольных сумм состава аппаратных средств

Система выполнит расчет контрольных сумм состава подключенных аппаратных средств.

Примечание. При установленной опции **Контроль конфиг. пространства PCI**, после подключения или отключения PCI устройства, необходимо отключить, а затем включить опцию **Контроль конфиг. пространства PCI** и выполнить перерасчет эталонов.

Контроль реестра Windows

Для контроля реестра Windows, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Контроль целостности**.

3 В меню **Контроля целостности** нажмите **Enter** на пункте **Контроль реестра Windows**.

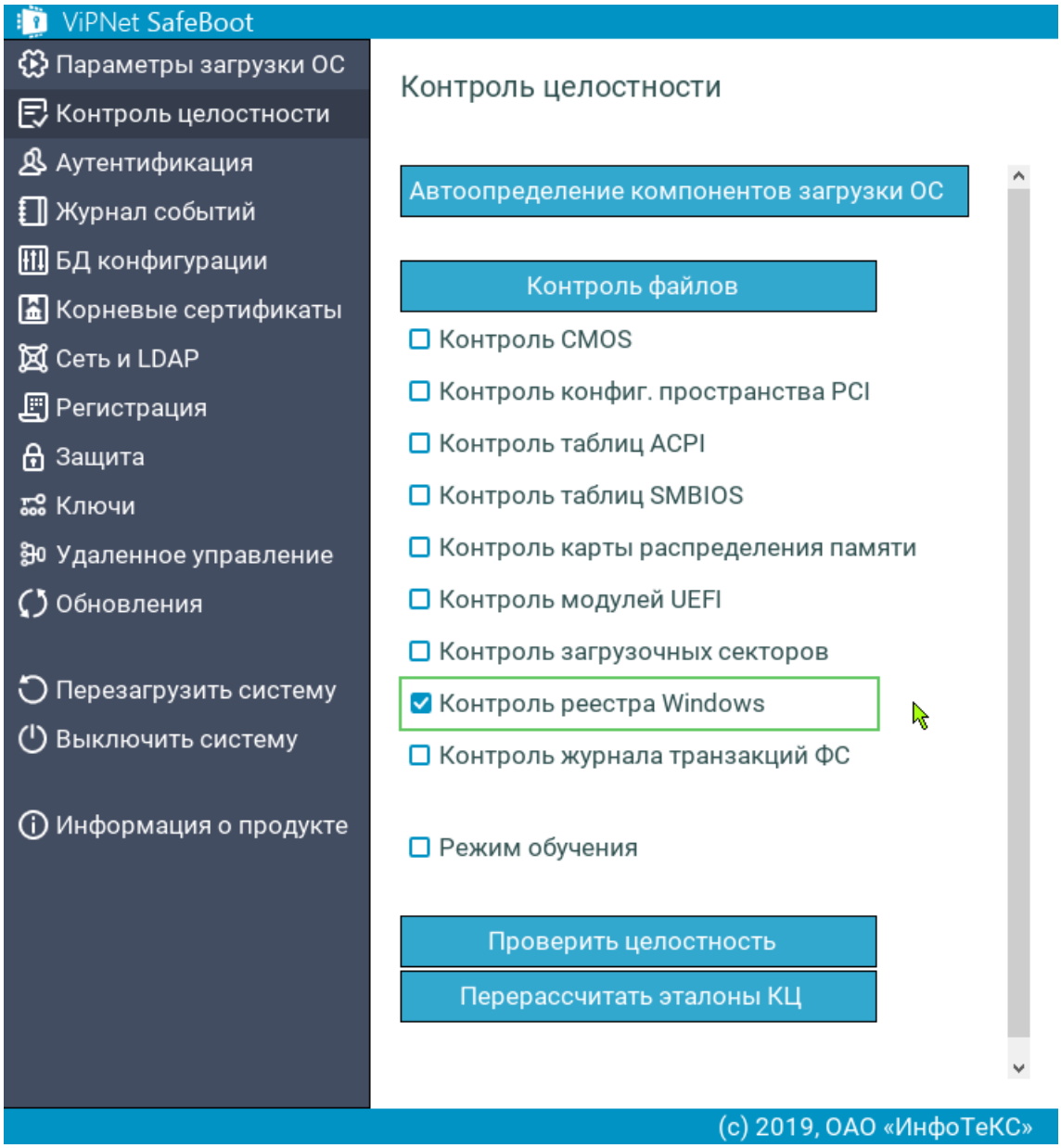


Рисунок 61. Выбор контроля реестра Windows

Откроется меню управления параметрами реестра Windows, содержащее следующие пункты:

- Импортировать эталоны КЦ реестра.
- Добавить параметр в список.
- Удалить параметр из списка.

4 Для добавления контролируемого параметра реестра Windows, выберите **Добавить параметр в список**. Откроется окно реестра Windows для выбора параметра.

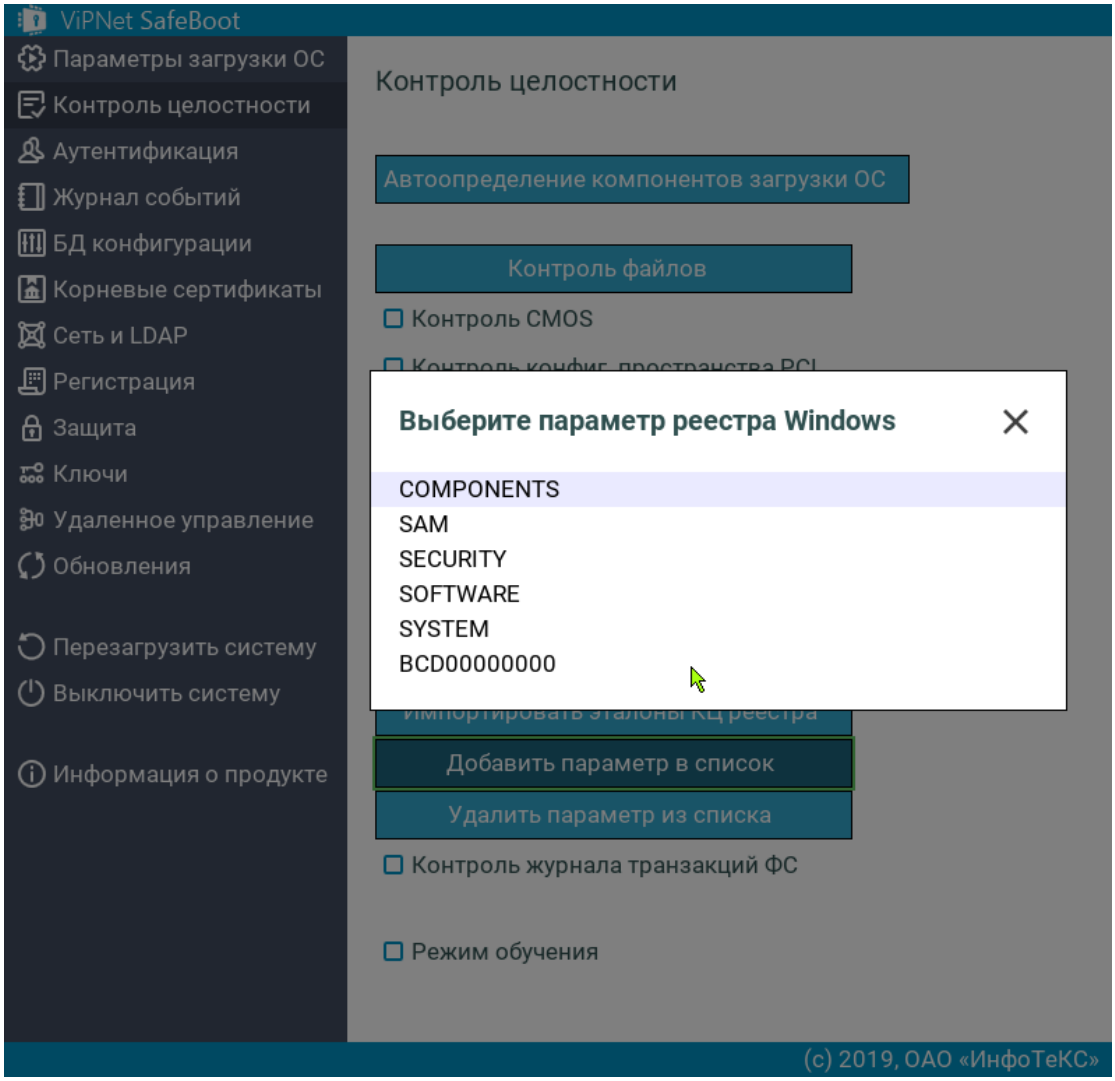


Рисунок 62. Выбор параметра реестра Windows

5 Выберите параметр реестра Windows, который нужно поставить на контроль.

6 Для удаления параметра реестра Windows из контролируемого списка выберите **Удалить параметр из списка**.

Откроется список контролируемых параметров реестра Windows.

7 Выберите параметр, который нужно удалить, и нажмите **Enter**.

8 Перед использованием эталонов при контроле реестра Windows, необходимо создать текстовый файл со списком контролируемых параметров реестра Windows в следующем формате:

0000000000000000000000000000000000000000000000000000000000000000 <имя параметра реестра Windows с полным путем>

```
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SnIcon
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnCloneVault\Start
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDacs\Group
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnEraser\Group
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Subsystems\SnLDB\Type
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Subsystems\SnPc\Type
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnCDFilter\Group
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDiskEnc\Start
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Subsystems\SnOptions\Type
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Type
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDiskEnc\Group
0000000000000000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDiskFilter\ImagePath
```

Рисунок 63. Пример файла эталонов для контроля параметров реестра Windows

9 Чтобы загрузить файл эталонов, вставьте USB-диск, содержащий файл эталонных значений, и выберите **Импортировать эталоны КЦ реестра**.

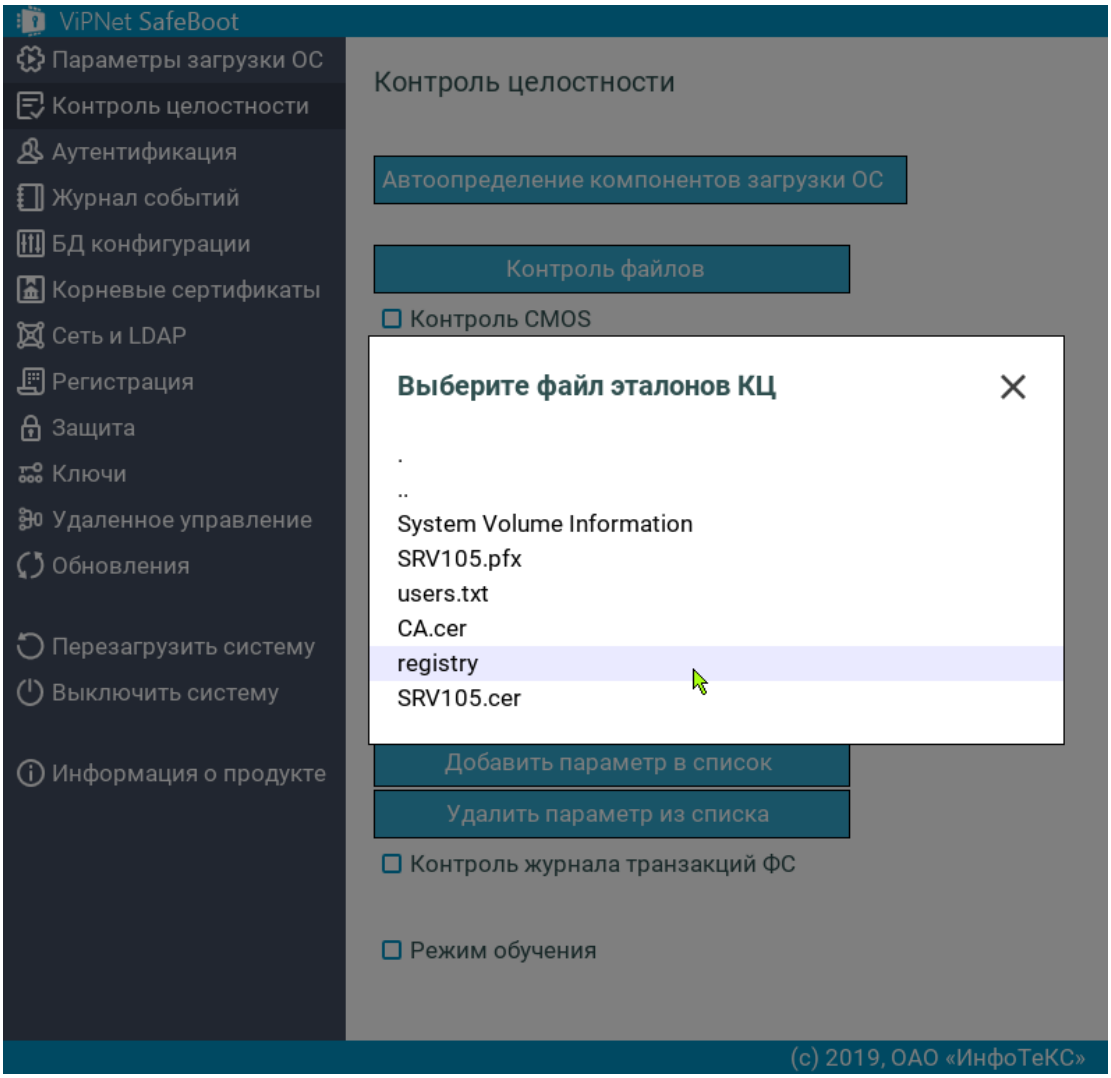
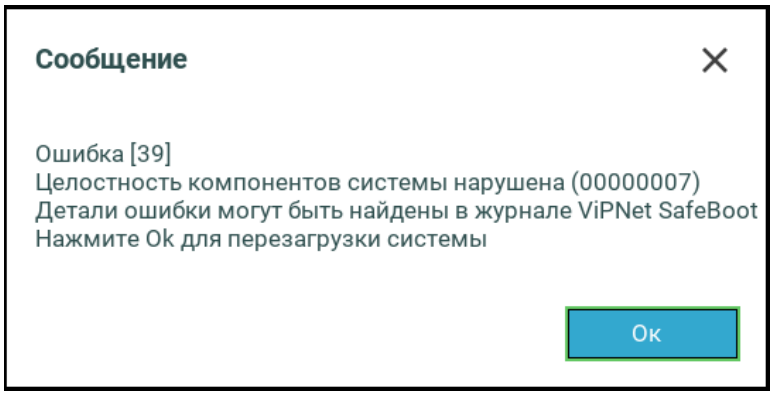


Рисунок 64. Выбор файла эталонов

Режим обучения

Включение опции **Режим обучения** используется для исключения из контроля целостности отдельных элементов компонентов, изменяемых при нормальном функционировании системы (например, при контроле CMOS). Элементы, не прошедшие проверку целостности, снимаются с контроля целостности, что позволяет «обучить» (адаптировать) систему контролировать определенный набор элементов.

При отключенной опции **Режим обучения**, в случае нарушения целостности одного или нескольких элементов из контролируемого списка, на экране появится сообщение об ошибке:



Загрузка операционной системы будет заблокирована. После перезагрузки системы в журнале событий ViPNet SafeBoot можно увидеть для каких элементов зафиксировано нарушение целостности.

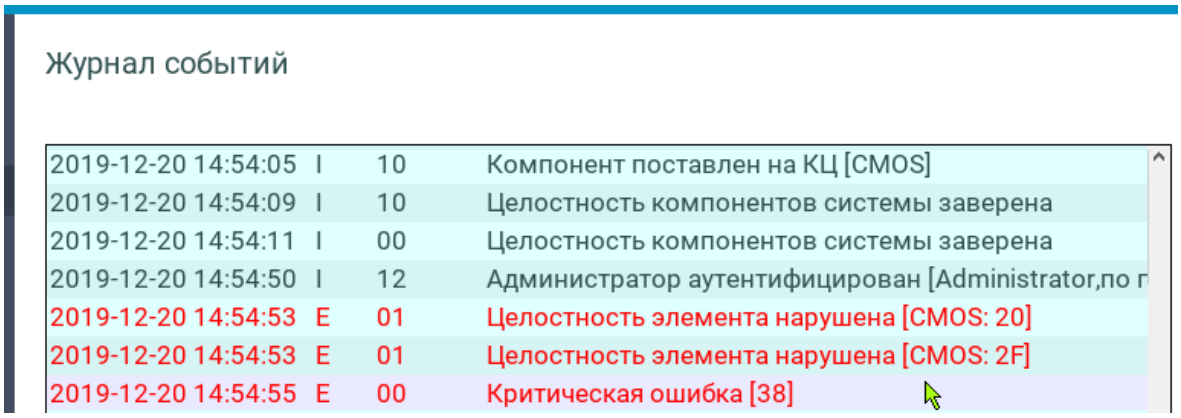


Рисунок 65. Записи в журнале событий о нарушении целостности

Для начала режима обучения выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Контроль целостности**.
3. В меню **Контроля целостности** выберите те компоненты, для которых должен быть выполнен контроль целостности (например, Контроль CMOS).

4 В меню **Контроля целостности** выберите пункт **Режим обучения**.

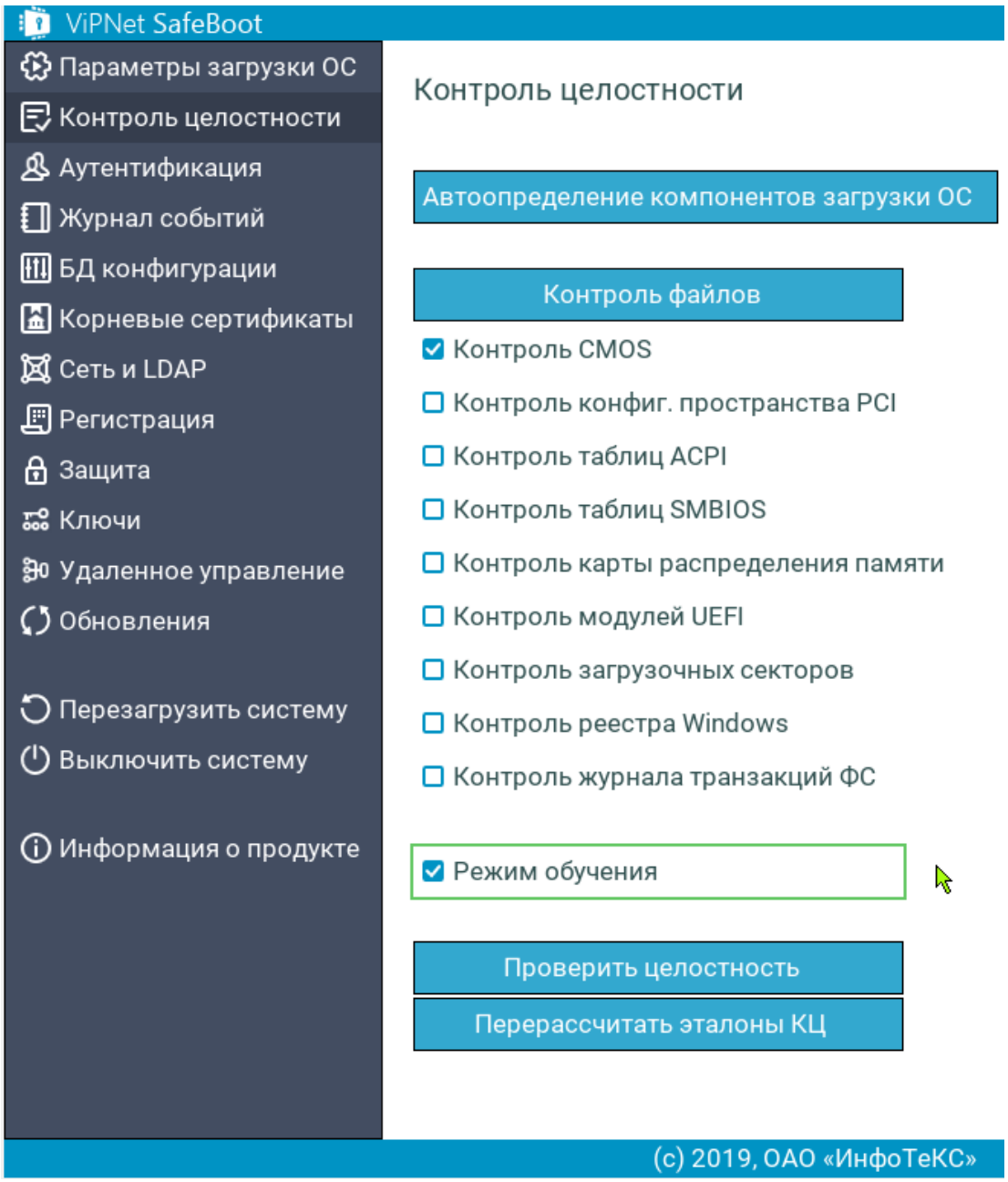


*Рисунок 66. Включение опции **Режим обучения***

При обнаружении нарушения целостности контролируемых элементов, на экране появится сообщение об ошибке контроля целостности. После перезагрузки системы в журнале событий ViPNet SafeBoot можно будет увидеть сообщение о снятых с контроля целостности элементах.

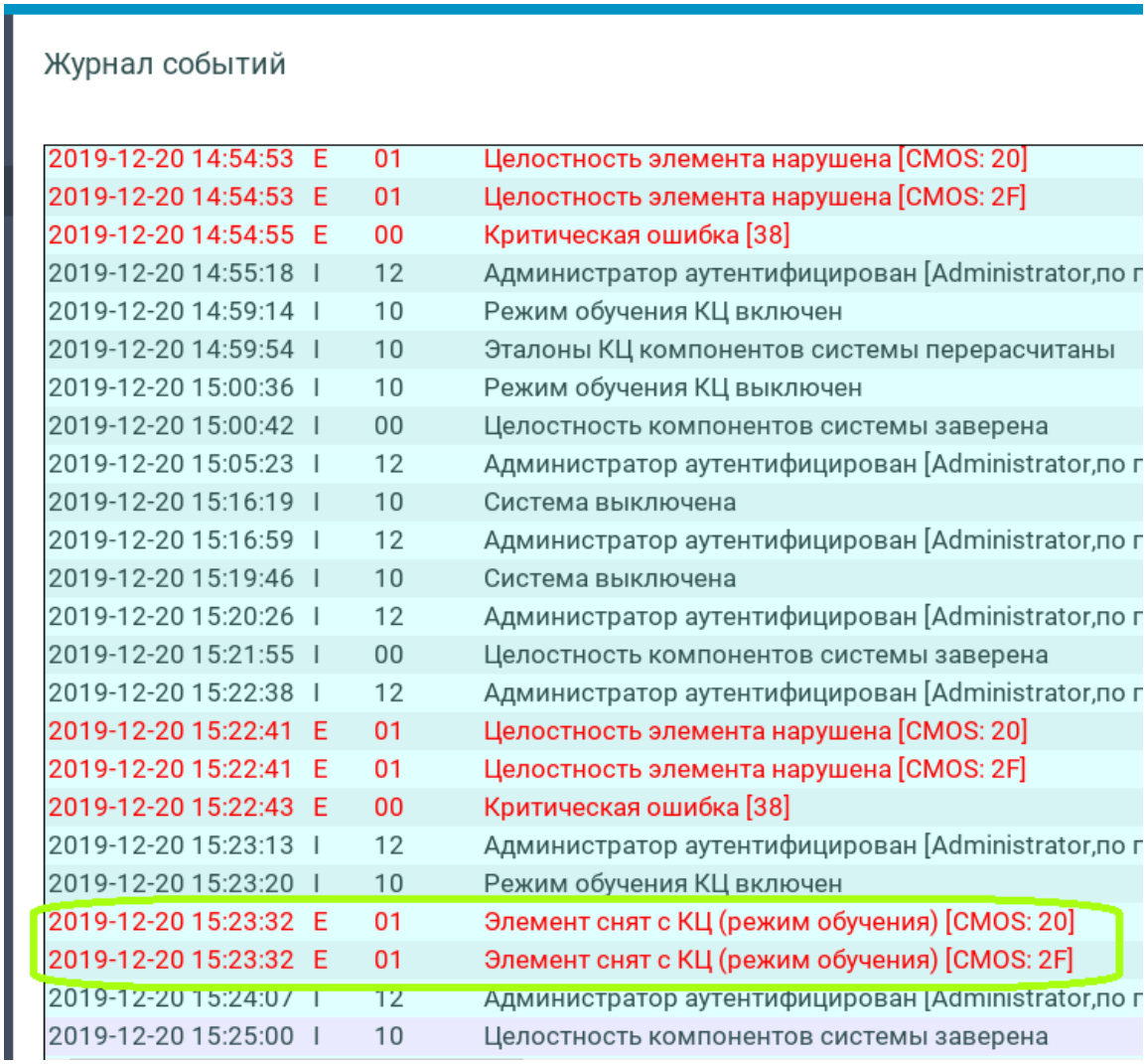


Рисунок 67. Записи в журнале событий о снятых с контроля целостности элементах

5 Рекомендуется выполнить несколько циклов перезагрузки/работы на персональном компьютере, чтобы с контроля целостности были сняты элементы, которые изменяет система.

6 После завершения адаптационного периода отключите опцию **Режим обучения**, нажав **Enter** на пункте **Режим обучения** в меню **Контроль целостности**.

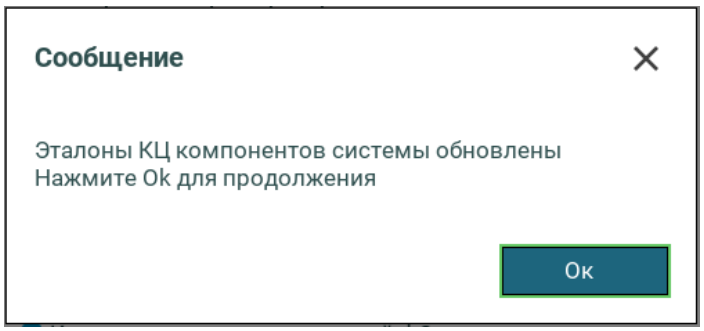
Примечание. Для того чтобы вновь поставить на контроль целостности элементы, снятые режимом обучения, следует в меню **Контроль целостности** снять с контроля компонент, измененный режимом обучения, а затем опять поставить его на контроль.

Перерасчет эталонных контрольных сумм

В случае штатного изменения контролируемых объектов, Администратору необходимо провести перерасчет эталонов контролируемых объектов.

Чтобы пересчитать эталонные контрольные суммы, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Контроль целостности**.
3. В открывшемся окне выберите **Перерассчитать эталоны КЦ**.
4. Дождитесь появления на экране сообщения:



Нажмите **Ok** или **Enter** для продолжения.

Принудительная проверка целостности

Администратор имеет возможность произвести принудительную проверку целостности из меню режима настроек без последующей загрузки операционной системы. Для этого выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

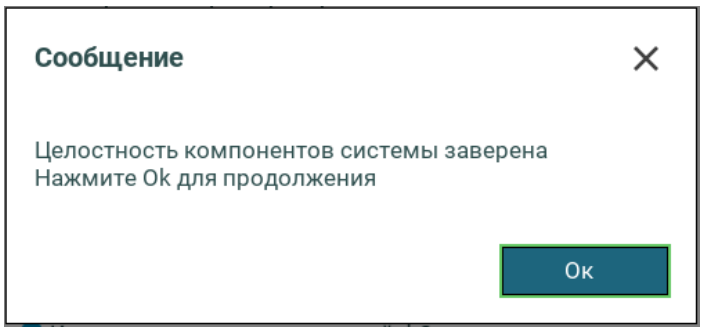
2 В меню режима настроек выберите **Контроль целостности**.

3 Добавьте, если необходимо, объекты для контроля.

4 Выберите **Проверить целостность**.

Контроль целостности будет выполнен для объектов, отмеченных флажками в окне **Контроль целостности**, и объектов из **Списка контролируемых разделов**.

После завершения проверки целостности появится следующее сообщение:



Нажмите **Ok** или **Enter** для продолжения.

7

Управление учетными записями пользователей

Учетные записи пользователей

ViPNet SafeBoot поддерживает несколько учетных записей для организации совместной работы с одним ПК нескольких пользователей. Каждой учетной записи могут назначаться следующие параметры:

- Имя учетной записи.
- Способ аутентификации.
- Роль пользователя.
- Аутентификационные данные.
- Дополнительные параметры, определяющие ограничение к качеству аутентификационных данных и их времени действия.

ViPNet SafeBoot поддерживает разграничение доступа пользователей к функциям режима настройки. Для этого введены три роли пользователей, которым помимо загрузки операционной системы даны следующие разрешения:

- Администратор. Разрешен доступ ко всем функциям режима настройки ViPNet SafeBoot.
- Аудитор. Разрешен доступ к журналу событий и смена пароля.
- Пользователь. Разрешена смена пароля.

Внимание!

Общее максимальное количество учетных записей — 32.

Создание диска восстановления

Диск восстановления может понадобиться Администратору при потере аутентификационных данных либо для временного отключения функциональности ViPNet SafeBoot (см. Временное отключение функциональности ViPNet SafeBoot на стр. 85). Процесс создания диска восстановления состоит в создании на USB-носителе уникального ключа восстановления.

Внимание! Храните диск восстановления в защищенном месте. Информация, записанная на нем, важна для обеспечения безопасности.

Чтобы подготовить диск восстановления пароля Администратора, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Аутентификация**.
3. В открывшемся окне выберите **Administrator**.

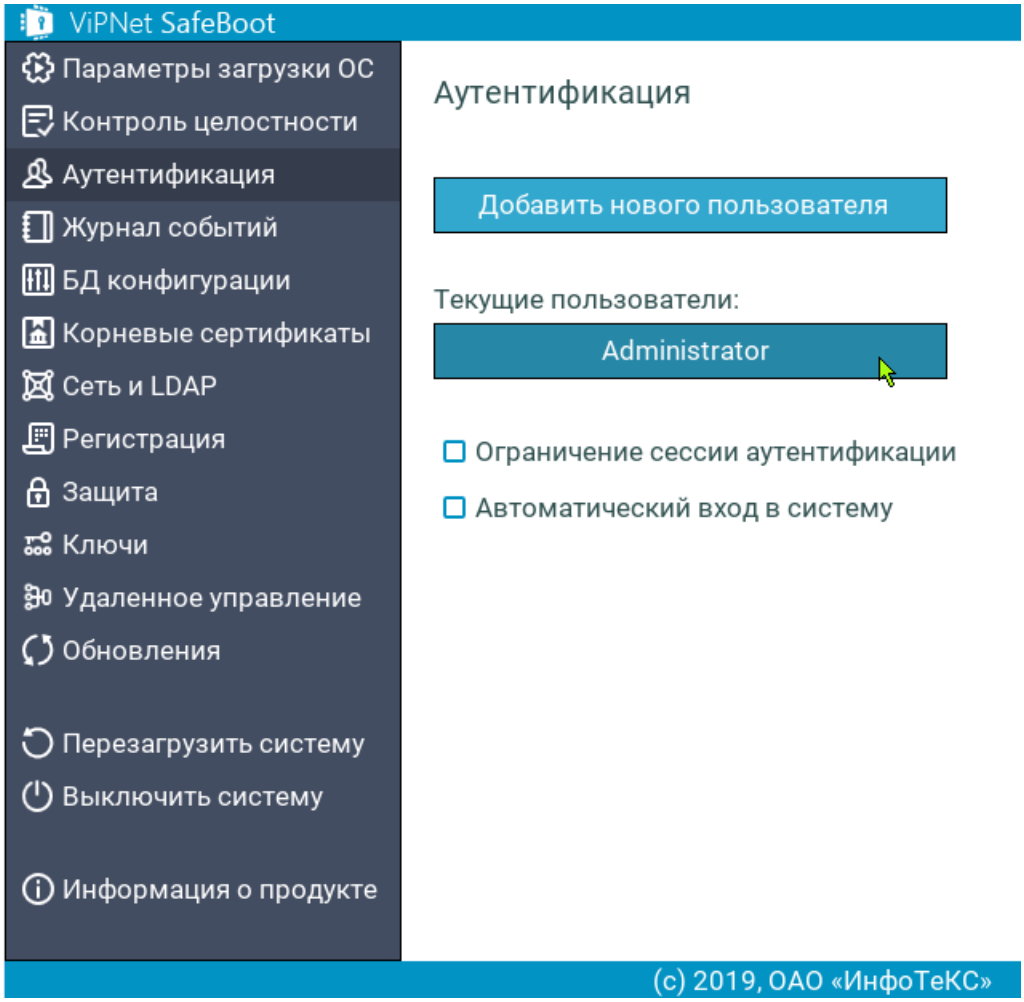
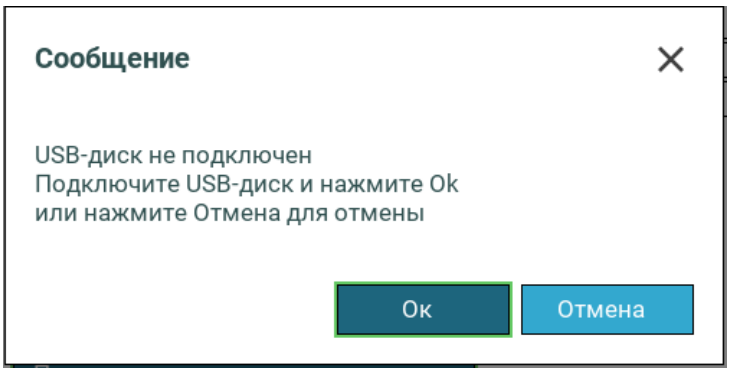


Рисунок 68. Выбор учетной записи Администратора

4 Подключите USB-диск.

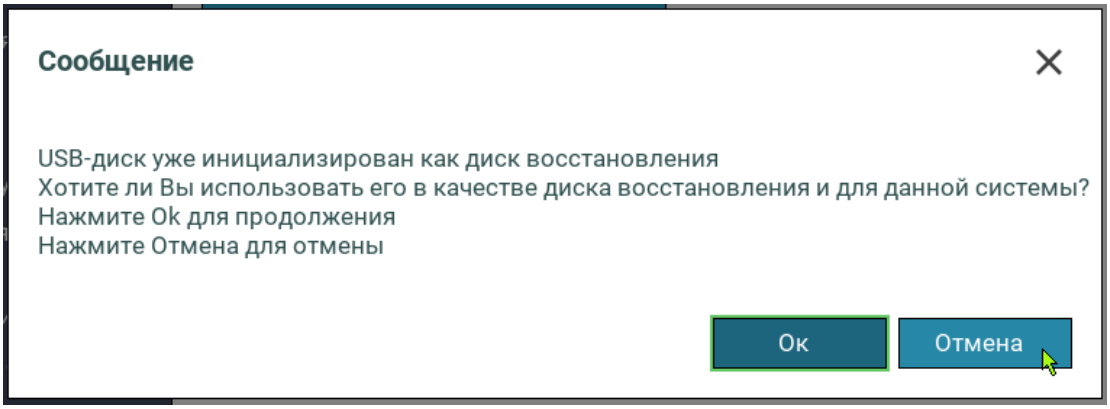
5 В окне **Настройки пользователя** выберите **Подготовить диск восстановления**.

- При отсутствии подключенного USB-диска появится следующее сообщение:



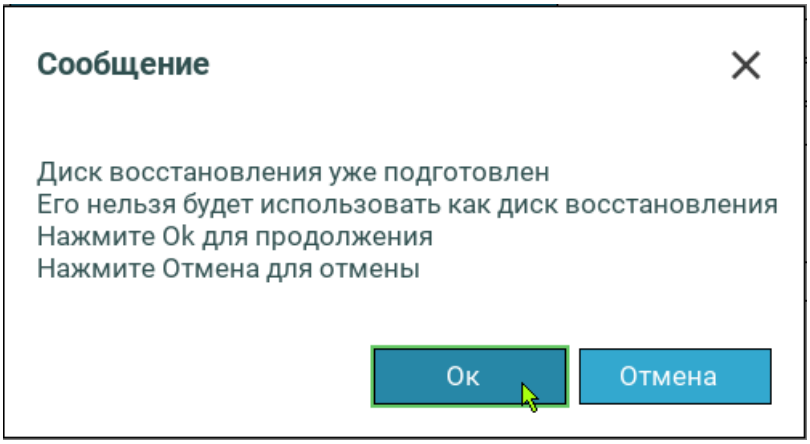
Подключите USB-диск и повторите подготовку диска восстановления.

- Если установленный USB-диск ранее уже был использован (инициализирован данными) для восстановления, появится следующее сообщение:



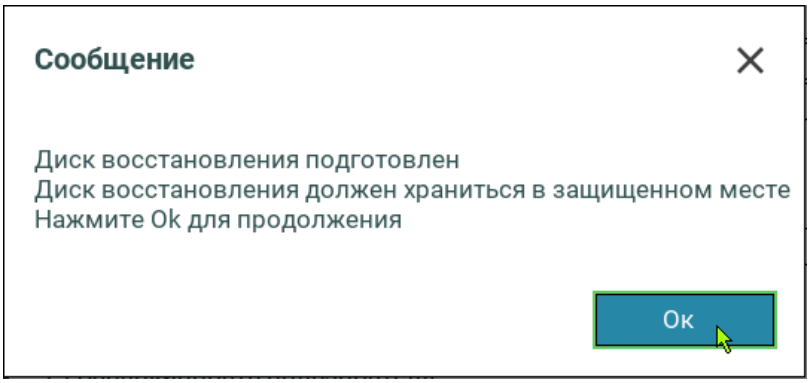
Нажмите **Ok** для продолжения или **Отмена**, если хотите использовать другой USB-диск.

- Если ранее уже создавался диск восстановления, то появится следующее сообщение:



Нажмите **Ok** для продолжения или **Отмена**, если хотите использовать другой USB-диск.

- После успешного создания диска восстановления появится следующее сообщение:



Нажмите **Ok** для продолжения и уберите созданный диск восстановления в защищенное место.

6 Для выхода в основное меню нажмите клавишу **Esc**.

Восстановление пароля администратора

Восстановление пароля Администратора возможно, только если ранее был создан диск восстановления (см. Создание диска восстановления на стр. 106).

Для восстановления пароля Администратора, выполните следующие действия:

1 Подключите USB-диск, инициализированный как диск восстановления.

2 Для входа в режим восстановления при загрузке нажмите сочетание клавиш **Правый Ctrl + r.**

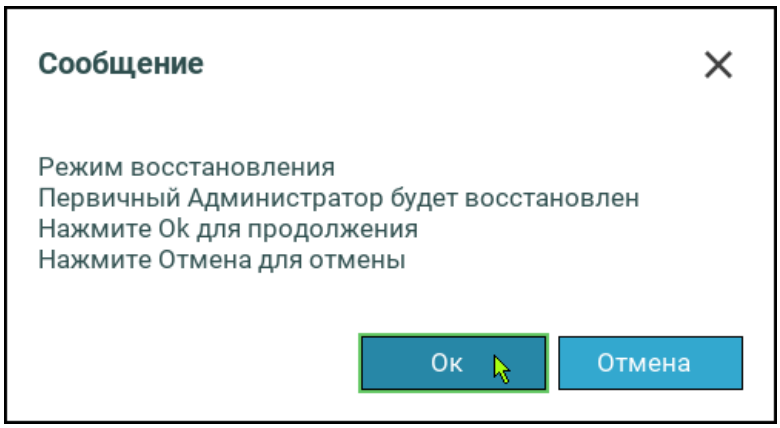
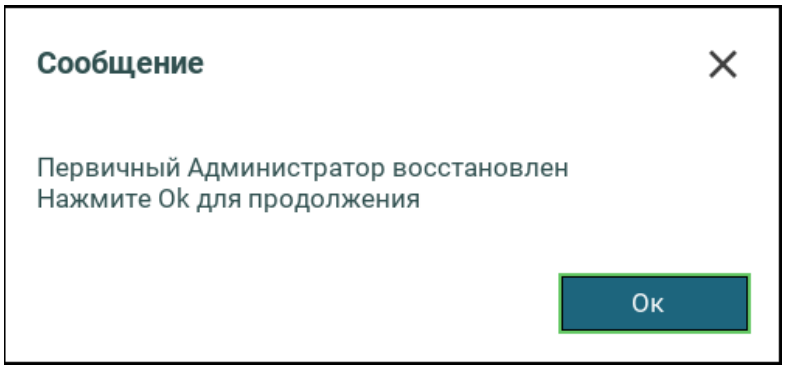


Рисунок 69. Вход в режим восстановления

Нажмите **Ок** или **Enter** для продолжения.

3 После завершения процедуры восстановления значение пароля Администратора будет сброшено до первоначального. На экране появится сообщение об успешном восстановлении:



4 Нажмите любую клавишу для продолжения.

На экране появится приглашение к авторизации. Порядок действий такой же, как при первом включении (см. Первый запуск на стр. 34).

- При появлении приглашения ввести имя пользователя, введите логин **Administrator**.
- При появлении приглашения ввести пароль, введите пароль **12345678**.

- В режиме настройки установите новый пароль Администратора.

Информация о восстановлении будет отражена в журнале событий.

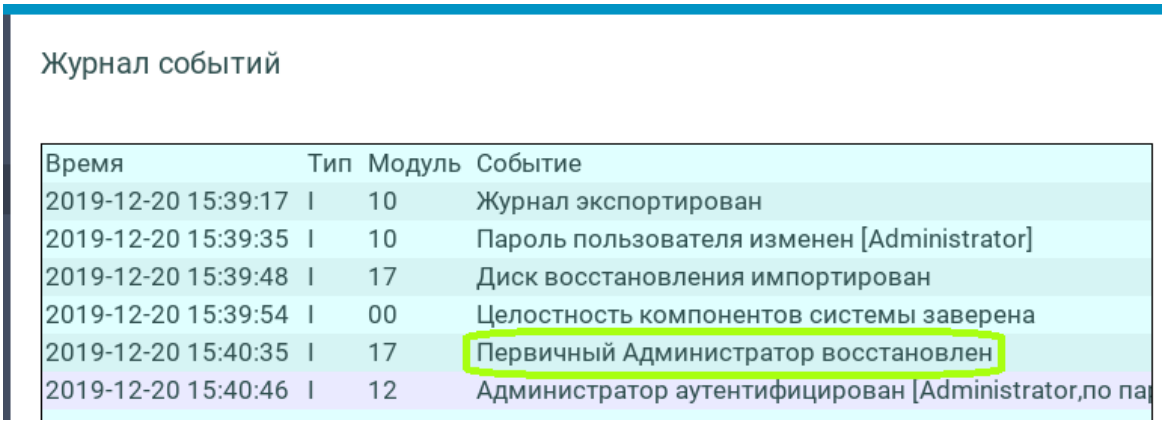


Рисунок 70. Записи журнала событий после восстановления пароля Администратора

Добавление учетных записей пользователей с аутентификацией по паролю

Чтобы добавить учетную запись пользователя, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Аутентификация**.

3 В открывшемся окне выберите **Добавить нового пользователя**.

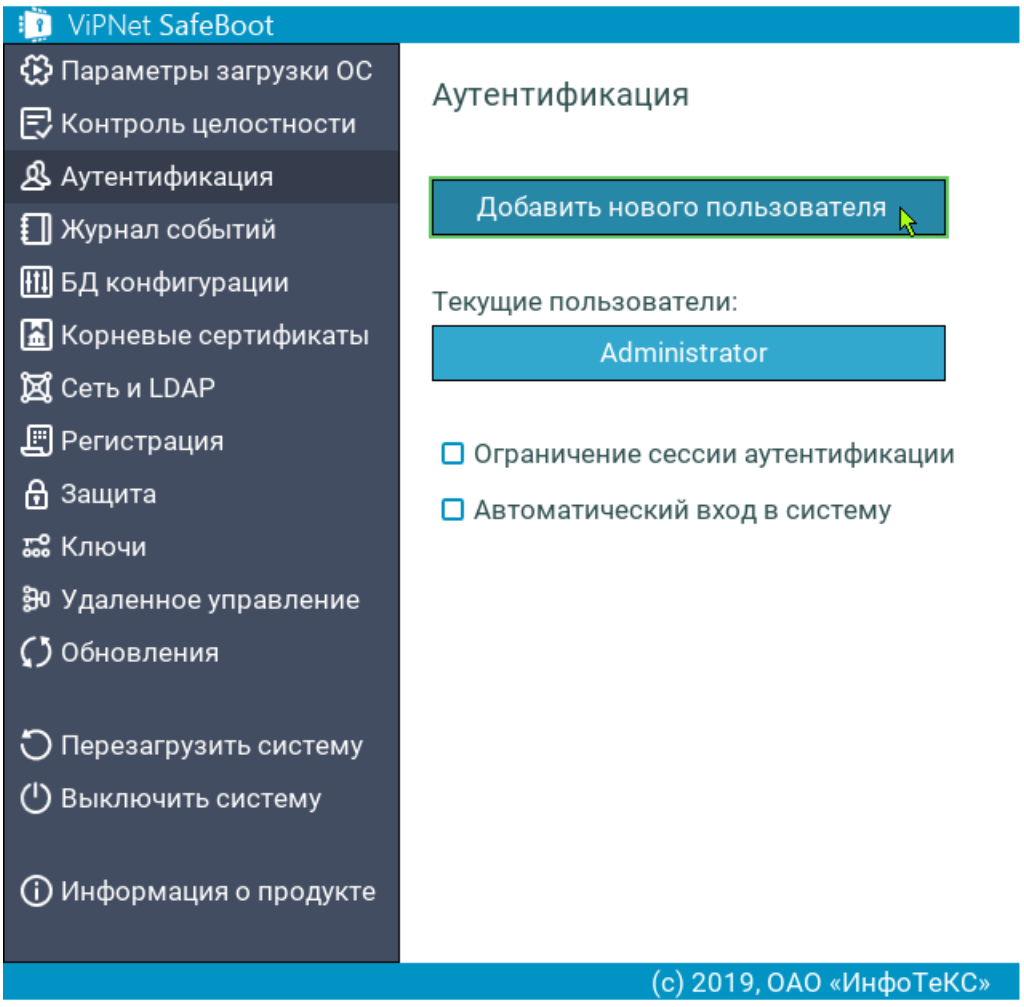


Рисунок 71. Добавление нового пользователя

4 В окне **Настройки пользователя** выберите поле пункта **Имя пользователя**.

Введите имя пользователя.

Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

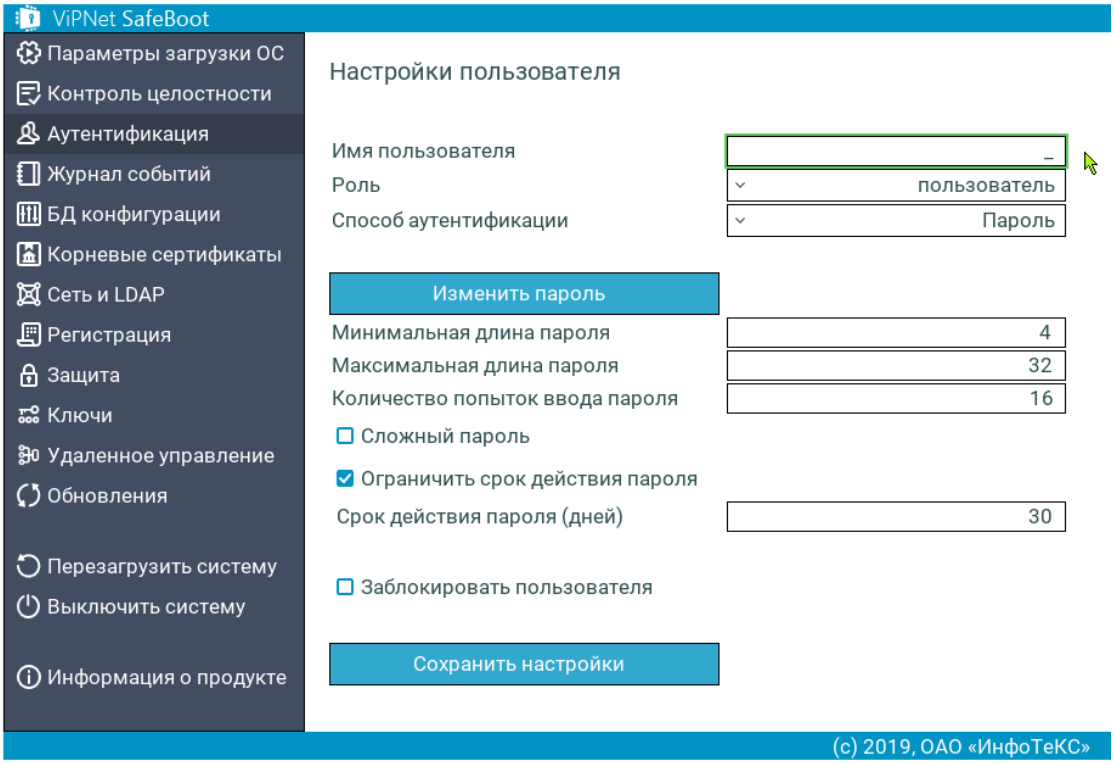


Рисунок 72. Приглашение ввести Имя пользователя в графическом режиме

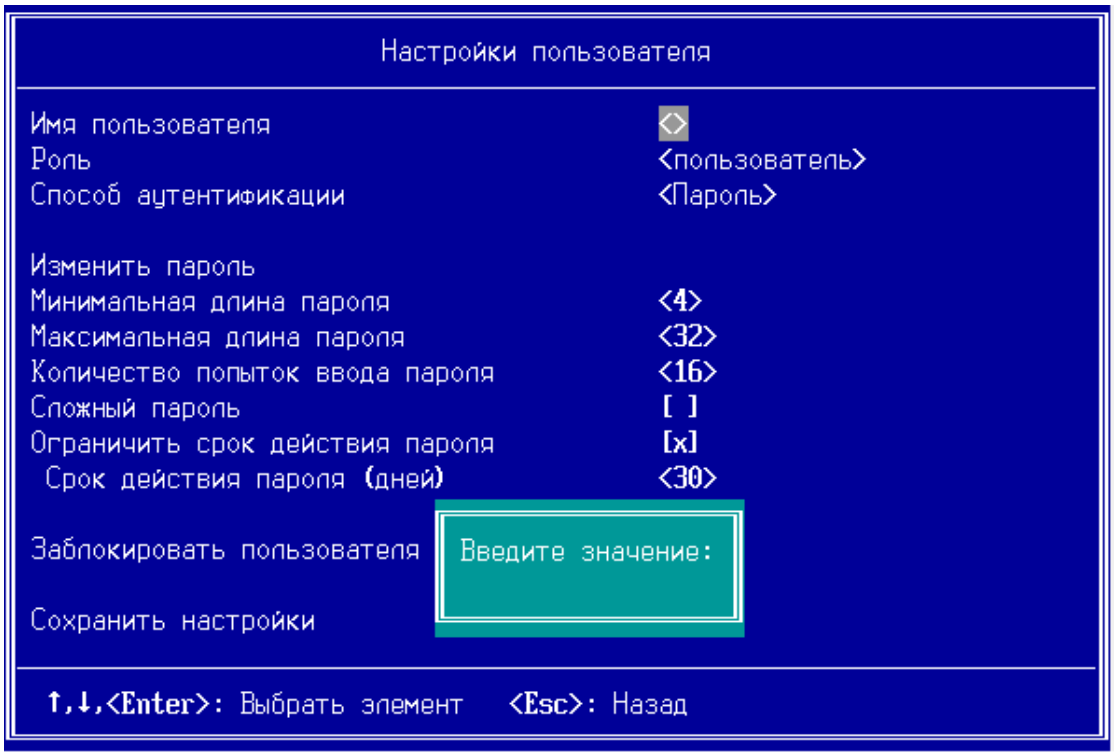
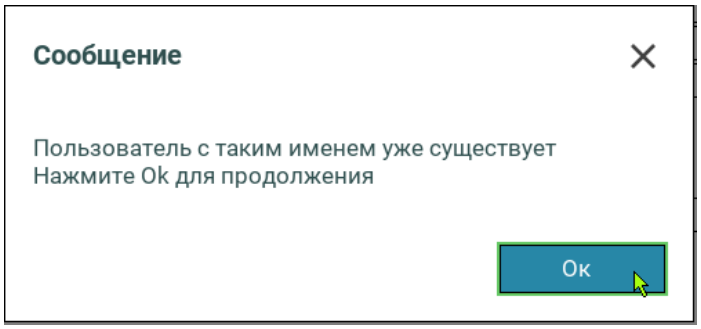
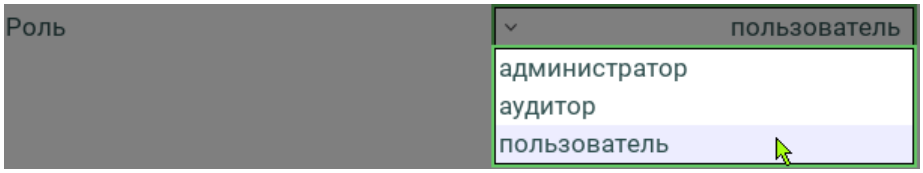


Рисунок 73. Приглашение ввести Имя пользователя в текстовом режиме

Если в ViPNet SafeBoot уже зарегистрирован пользователь с введенным именем, появится соответствующее сообщение.

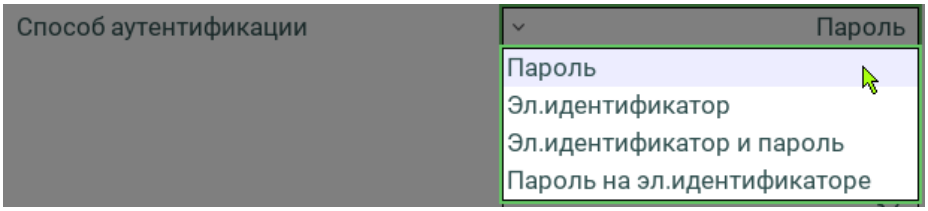


5 В пункте **Роль** в открывшемся списке выберите роль:



Внимание! Общее максимальное количество пользователей — 32.

6 В пункте **Способ аутентификации** в открывшемся списке выберите способ аутентификации **Пароль**:



7 Выберите пункт **Изменить пароль**.

Примечание. Ограничения, действующие при создании пароля для обычного пользователя:

- минимальная длина пароля — 4 символа;
- максимальная длина пароля — 32 символа.

Данные ограничения задаются администратором и могут отличаться от указанных.

Ограничения, действующие при создании пароля для администратора и аудитора:

- минимальная длина пароля — 8 символов;
- максимальная длина пароля — 32 символа.

Для использования более надежного пароля установите флажок **Сложный пароль**.

Примечание. Критерии, действующие при создании сложного пароля:

- длина пароля не менее 8 символов;
- минимум один буквенный символ в верхнем регистре;
- минимум один буквенный символ в нижнем регистре;
- минимум один спецсимвол;
- минимум один цифровой символ.

Для ограничения количества попыток ввода пароля выберите соответствующий пункт или оставьте значение по умолчанию.

Примечание. Пользователь превысивший установленное количество неудачных попыток ввода пароля блокируется. Для разблокировки учетной записи необходимо выполнить вход с учетной записью администратора.

---

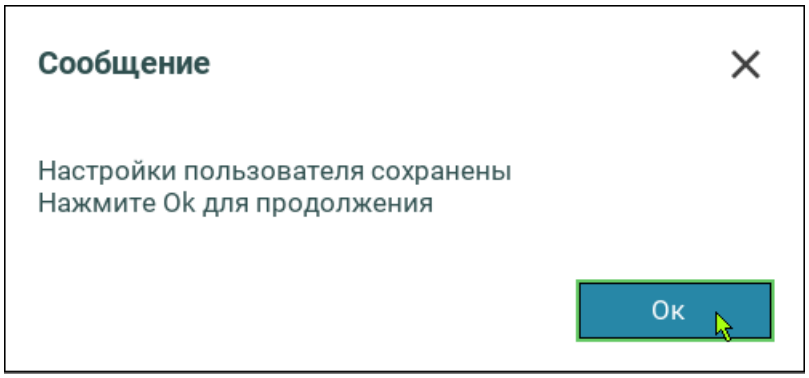
8 Измените настройки ограничения срока действия пароля или оставьте значение по умолчанию.

- Для изменения срока действия пароля оставьте флажок **Ограничить срок действия пароля**, выберите пункт **Срок действия пароля (дней)** и установите необходимое значение.

- Для отмены ограничения срока действия пароля снимите флажок **Ограничить срок действия пароля**.

Примечание. При установленном флажке **Ограничить срок действия пароля** по истечении периода действия пароля выводится соответствующее сообщение о необходимости смены пароля, пользователь блокируется до смены пароля.

9 Убедитесь, что все поля заполнены правильно, и выберите **Сохранить настройки**.



10 Нажмите **Ок**.

При успешной регистрации имя пользователя появится в списке **Текущие пользователи.**

Добавление учетных записей пользователей с аутентификацией по электронному идентификатору

Чтобы добавить учетную запись пользователя с аутентификацией по электронному идентификатору, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Аутентификация**.

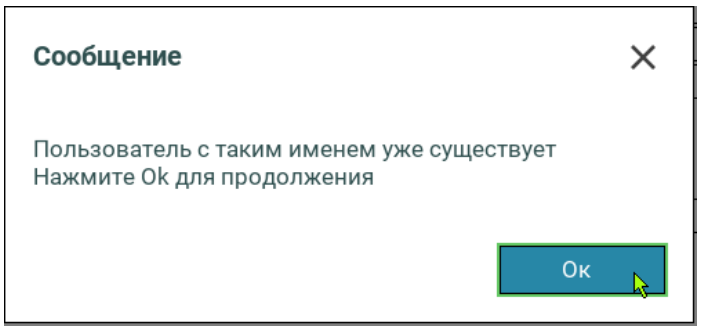
3 В открывшемся окне выберите **Добавить нового пользователя**.

4 В окне **Настройки пользователя** выберите **Имя пользователя**.

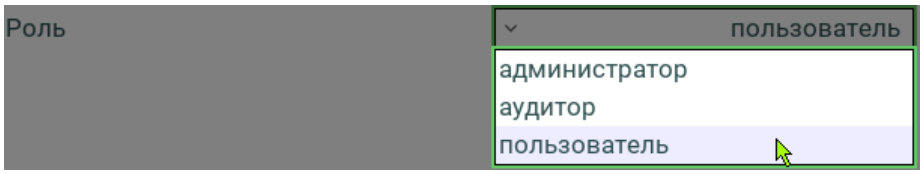
Введите имя пользователя.

Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

Если в ViPNet SafeBoot уже зарегистрирован пользователь с введенным именем, появится соответствующее сообщение.

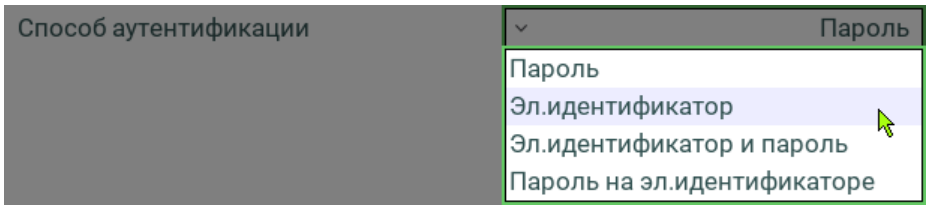


5 В пункте **Роль** в открывшемся списке выберите роль:



Внимание! Общее максимальное количество пользователей — 32.

6 В пункте **Способ аутентификации** в открывшемся списке выберите способ аутентификации **Эл. идентификатор**:



Меню **Настройки пользователя** примет следующий вид:

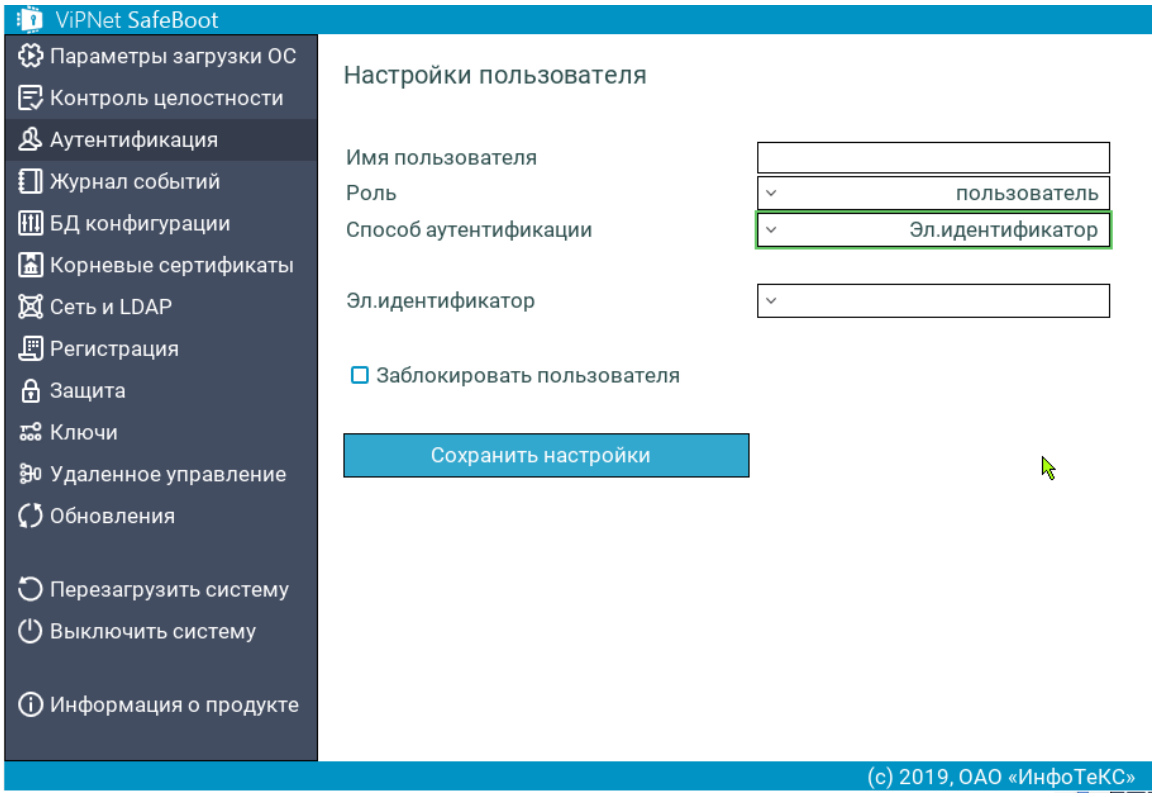


Рисунок 74. Меню Настройки пользователя при выбранном способе аутентификации «Электронный идентификатор»

Внимание! Перед созданием пользователей с аутентификацией по электронному идентификатору, необходимо установить корневые сертификаты (см. Установка корневого сертификата на стр. 150).

7 Настройки при использовании электронного идентификатора Guardant ID.

7.1 Выберите в пункте **Эл. идентификатор** Guardant ID.

Примечание. Перед инициализацией электронного идентификатора Guardant ID необходимо подготовить USB-диск, на котором должны быть сохранены ключевой контейнер, сформированный средствами ViPNet CSP, и сертификат (см. Подготовка к работе Guardant ID на стр. 159).

7.2 Выберите сертификат на электронном идентификаторе Guardant ID.

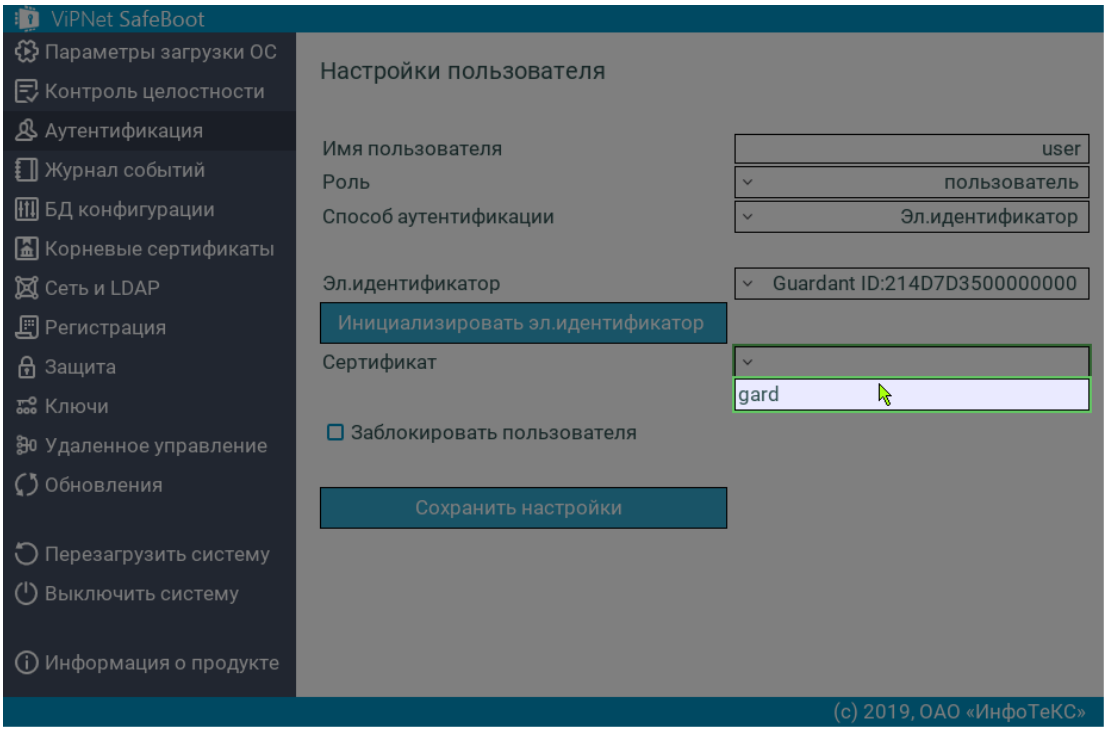


Рисунок 75. Выбор сертификата на электронном идентификаторе Guardant ID

7.3 После приглашения ввести PIN, введите текущий PIN-код для установленного Guardant ID.

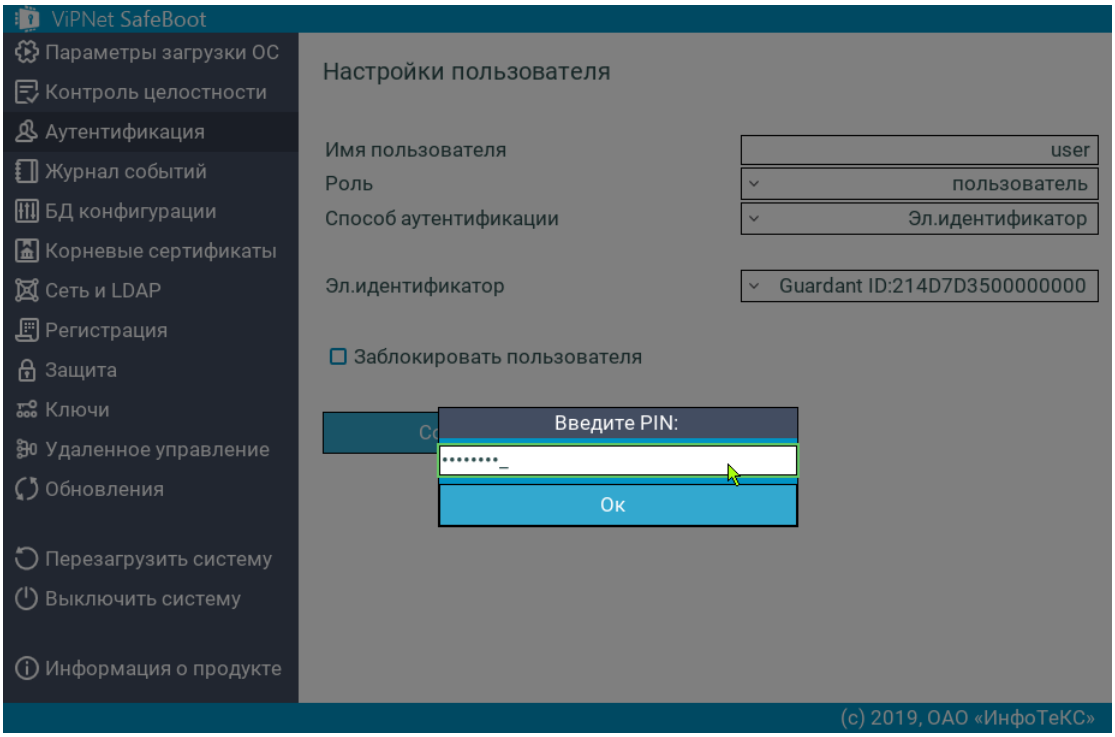


Рисунок 76. Приглашение ввести текущий PIN-код электронного идентификатора

При неправильно введенном PIN-коде появится соответствующее сообщение об ошибке.

7.4 Выберите пункт меню **Инициализировать идентификатор**, а затем из появившегося списка выберите сертификат пользователя, расположенный на заранее подготовленном USB-диске.

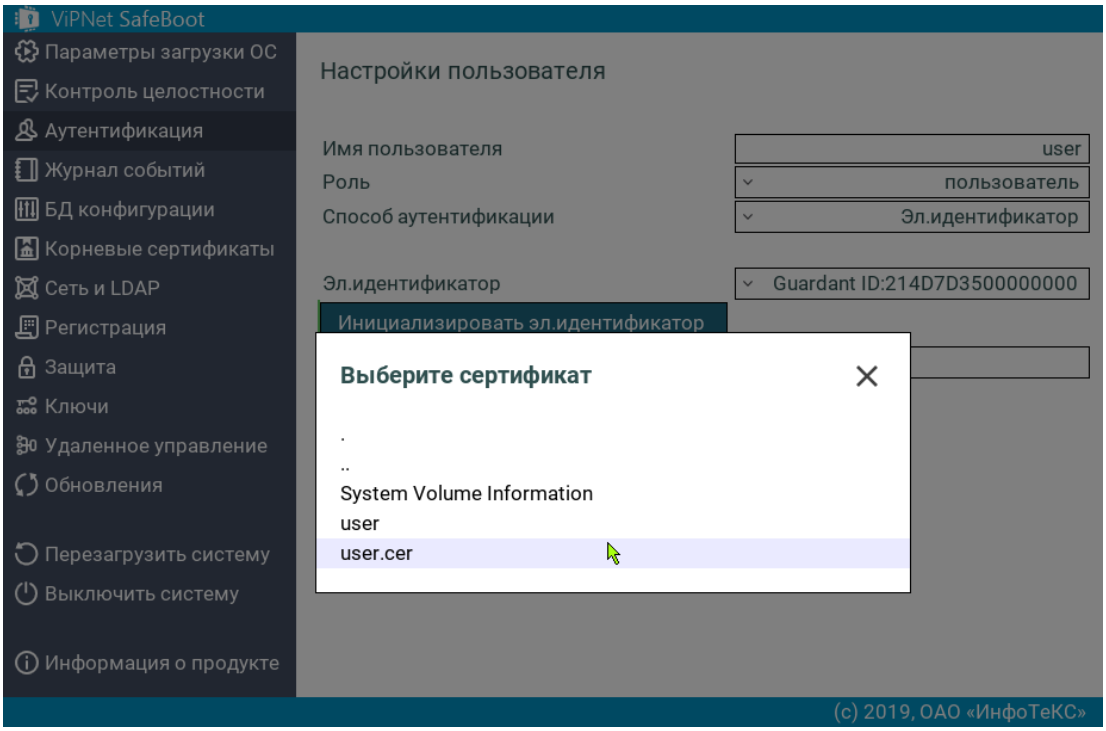


Рисунок 77. Выбор сертификата пользователя

7.5 Выберите ключевой контейнер, соответствующий сертификату.

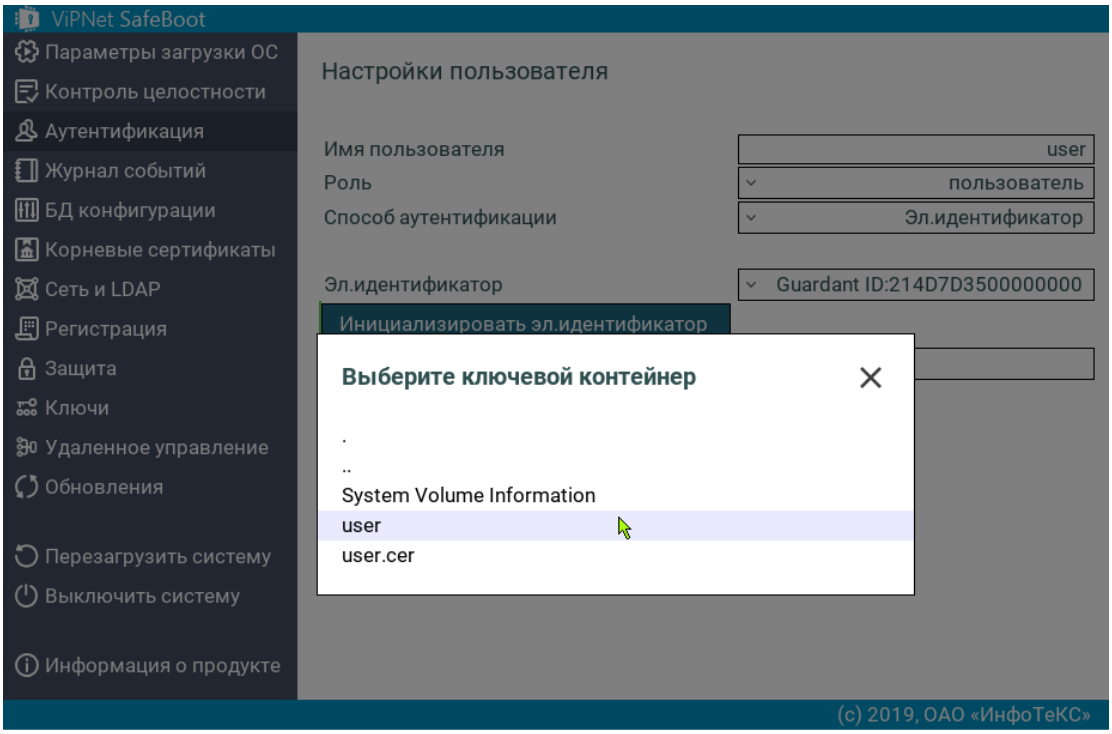
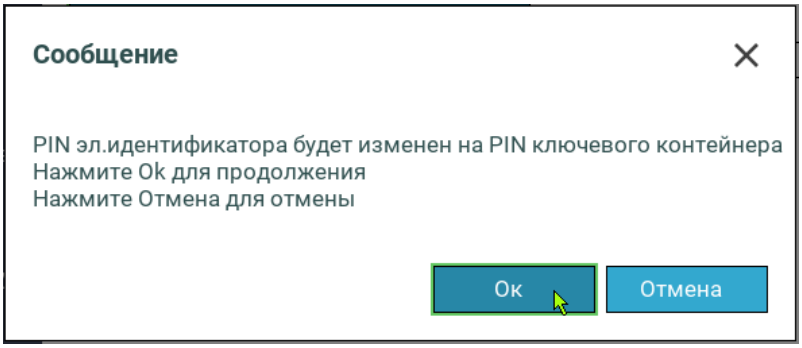


Рисунок 78. Выбор ключевого контейнера

7.6 После приглашения ввести PIN, введите PIN-код контейнера.

Появится сообщение о смене PIN-кода электронного идентификатора на соответствующий PIN-код контейнера:



В случае отказа (при нажатии на **Отмена**) электронный идентификатор не инициализируется.

7.7 Нажмите **Ок**. На экране появится сообщение об инициализации идентификатора:

Дождитесь сообщения об окончании инициализации.

7.8 Выберите сертификат пользователя, нажав на пункт меню **Сертификат пользователя**.

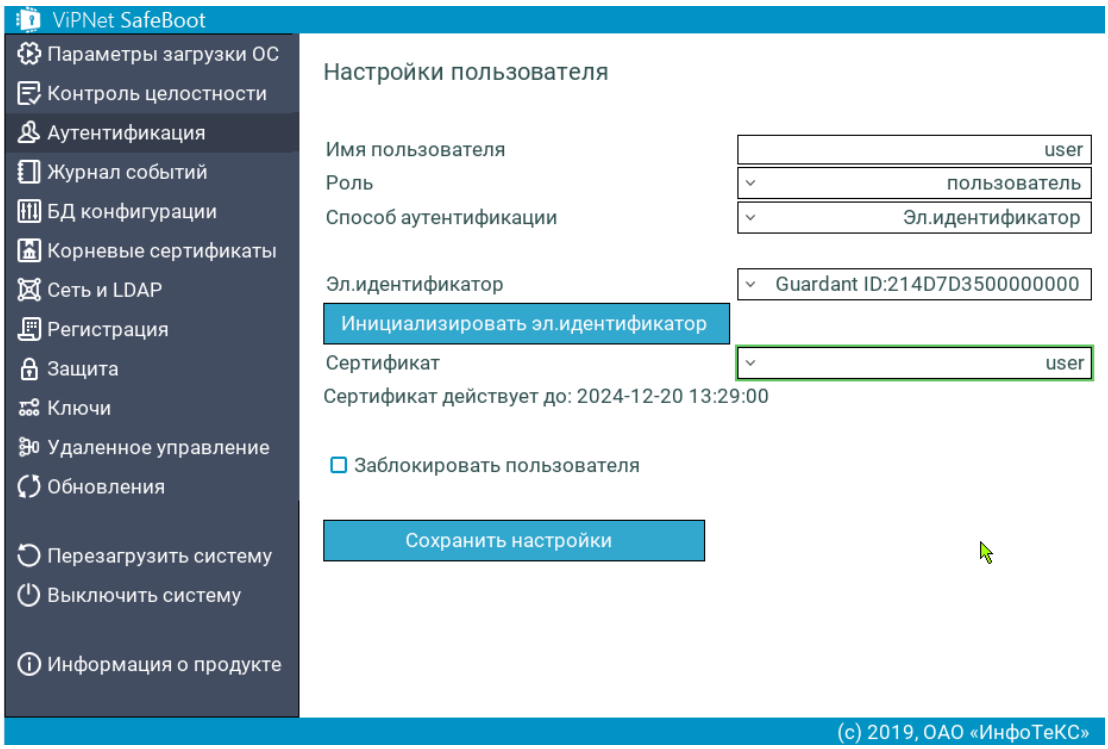


Рисунок 79. Выбор сертификата пользователя

7.9 Сохраните настройки.

8 Настройки при использовании электронных идентификаторов Рутокен ЭЦП, Рутокен Lite, JaCarta PKI

8.1 Выберите в пункте **Эл. идентификатор** Рутокен ЭЦП.

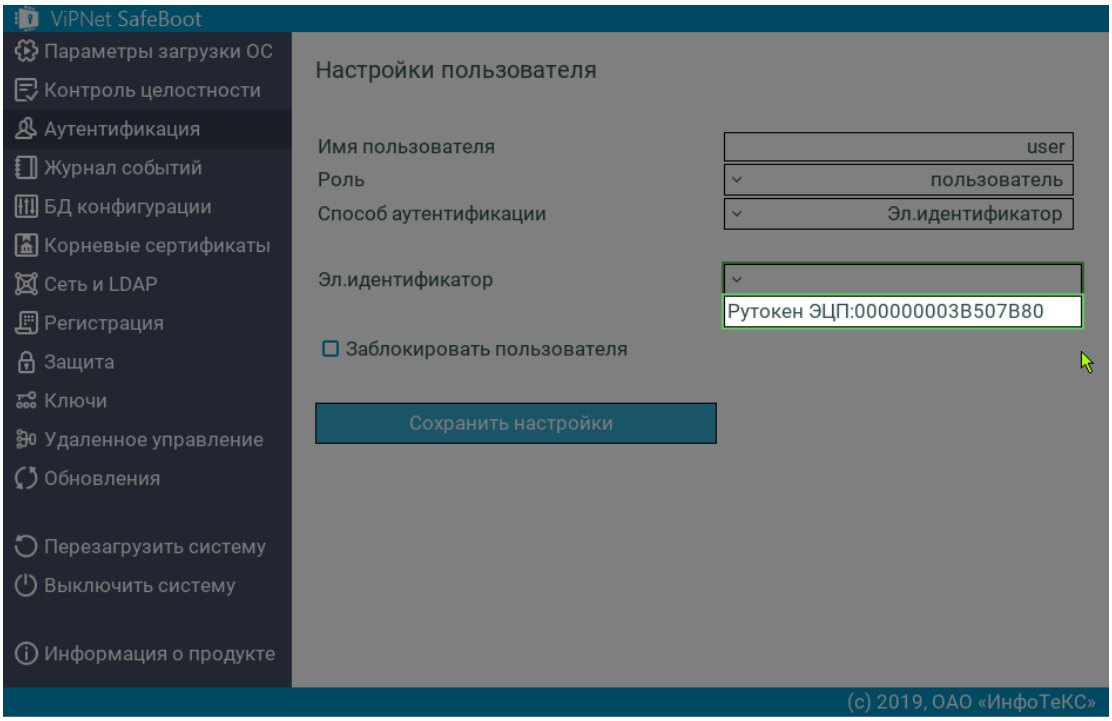
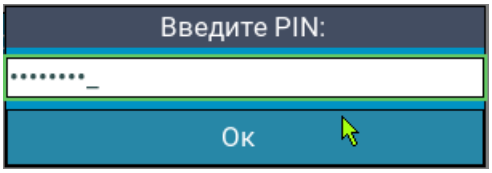


Рисунок 80. Выбор в качестве электронного идентификатора Рутокен ЭЦП

8.2 После приглашения ввести PIN, введите текущий PIN-код для установленного электронного идентификатора.



При неправильно введенном PIN-коде появится соответствующее сообщение об ошибке.

8.3 Выберите сертификат пользователя, нажав на пункт меню **Сертификат пользователя**.

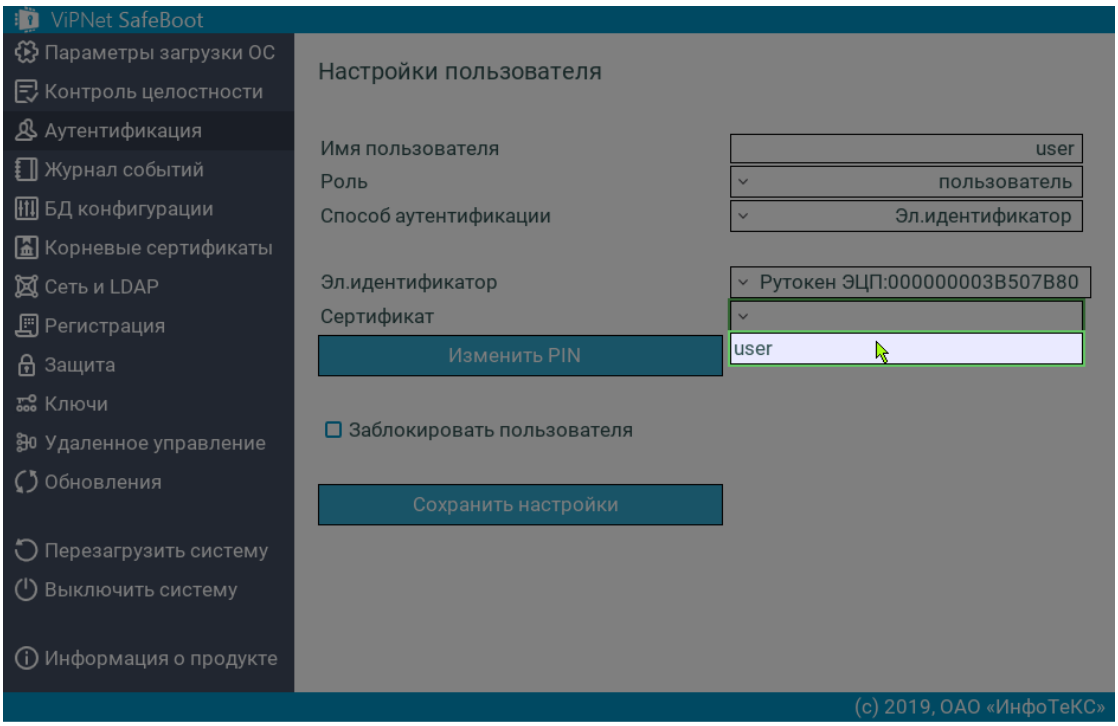
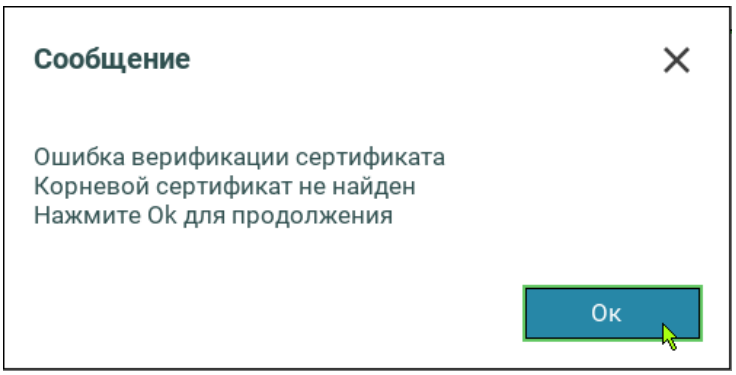
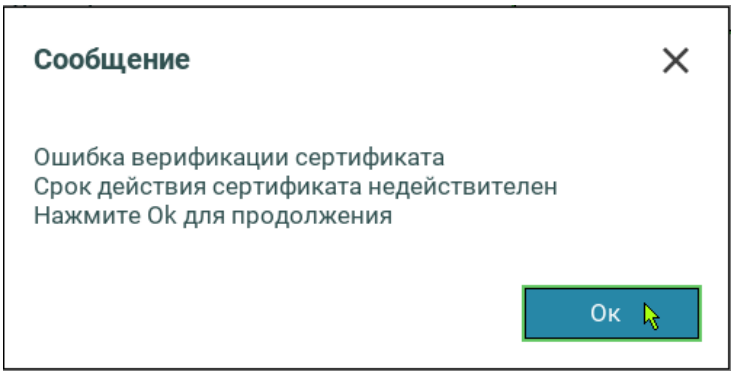


Рисунок 81. Выбор сертификата пользователя

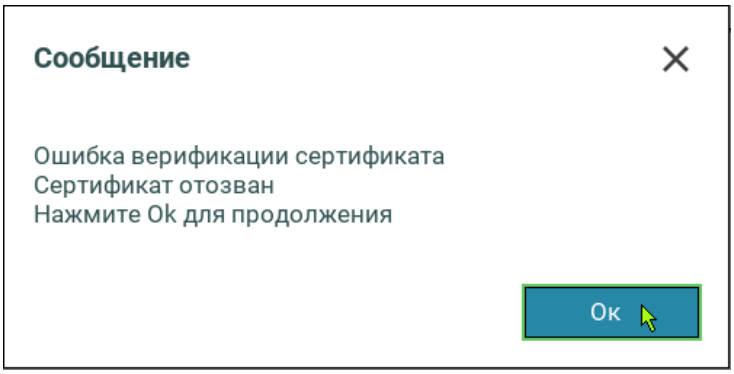
Если корневой сертификат отсутствует, появится сообщение об ошибке:



Если сертификат просрочен, появится следующее сообщение:



Если сертификат пользователя был внесен в список отозванных сертификатов (CRL), то появится следующее сообщение об ошибке:



При отсутствии ошибок назначенный сертификат появится в строке **Сертификат пользователя**:

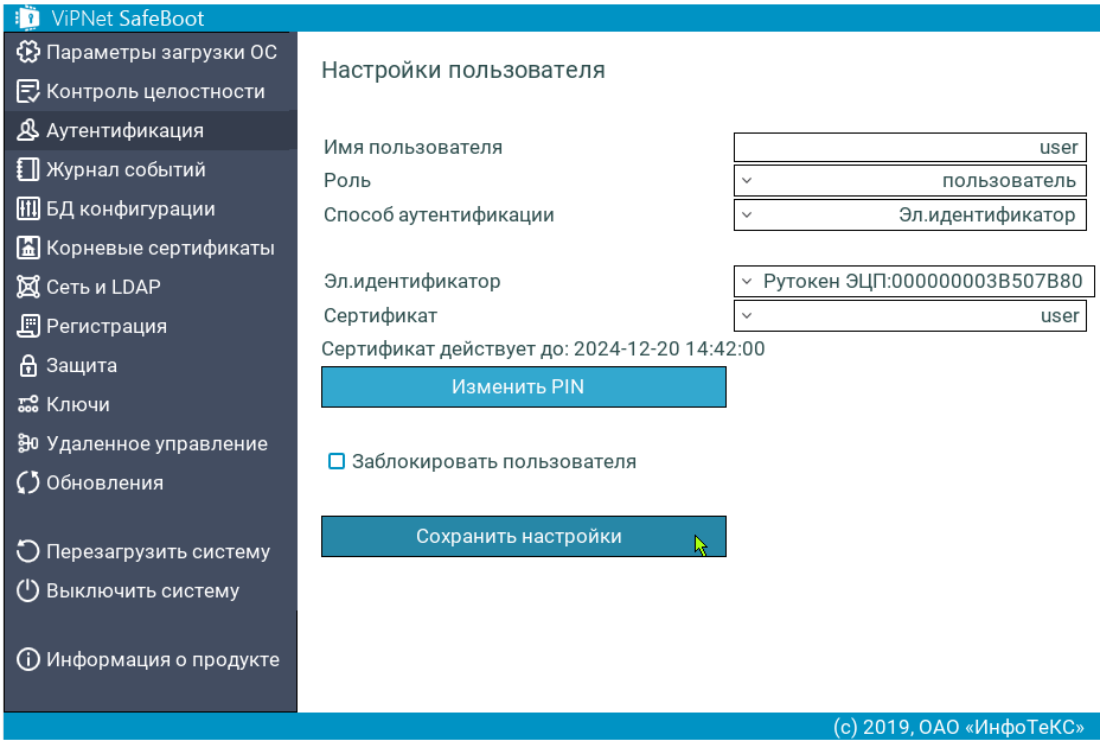
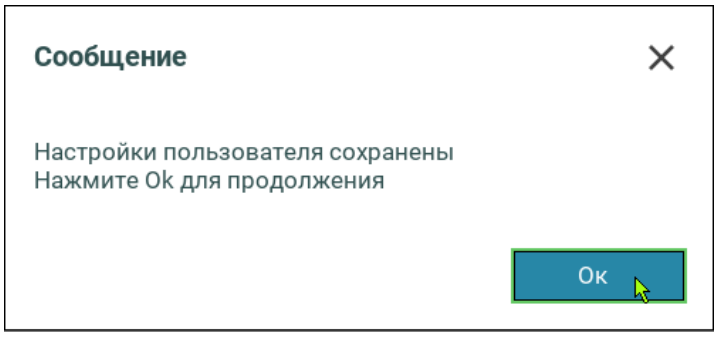


Рисунок 82. Вид меню настроек пользователя с установленным сертификатом

8.4 При необходимости измените PIN-код для установленного электронного идентификатора, выбрав соответствующий пункт меню.

9 Убедитесь, что все поля заполнены правильно, и выберите **Сохранить настройки**.



10 Нажмите **Ок**.

При успешной регистрации имя пользователя появится в списке **Текущие пользователи**.

Добавление учетных записей пользователей с аутентификацией по электронному идентификатору и паролю

Чтобы добавить учетную запись пользователя с аутентификацией по электронному идентификатору и паролю, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Аутентификация**.

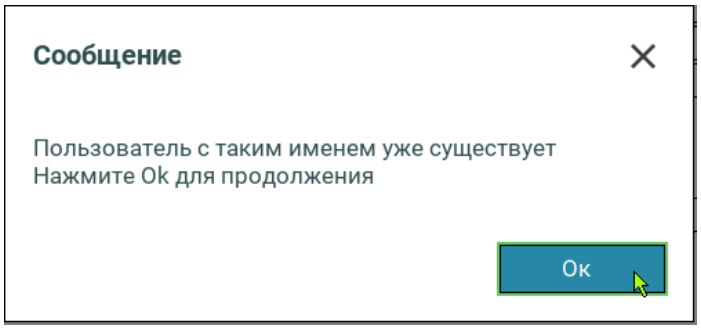
3 В открывшемся окне выберите **Добавить нового пользователя**.

4 В окне **Настройки пользователя** выберите **Имя пользователя**.

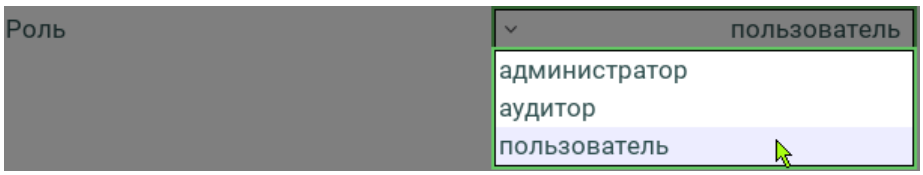
Введите имя пользователя.

Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

Если в ViPNet SafeBoot уже зарегистрирован пользователь с введенным именем, появится соответствующее сообщение.

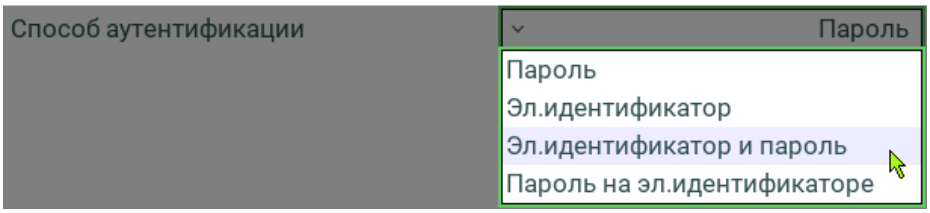


5 В пункте **Роль** в открывшемся списке выберите роль.



Внимание! Общее максимальное количество пользователей — 32.

В пункте **Способ аутентификации** в открывшемся списке выберите способ аутентификации **Эл. идентификатор и пароль**:



Меню **Настройки пользователя** примет следующий вид:

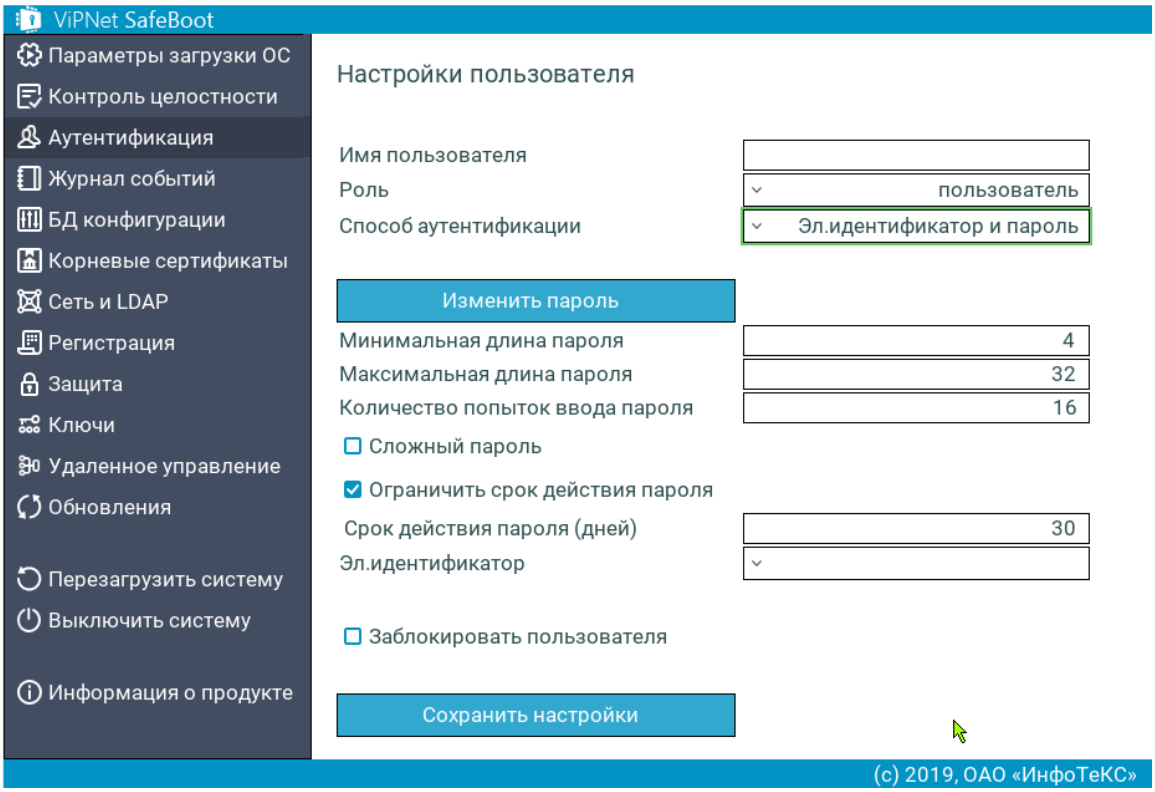


Рисунок 83. Меню Настройки пользователя при выбранном способе аутентификации «Электронный идентификатор и пароль»

6 Выберите пункт **Эл. идентификатор**.

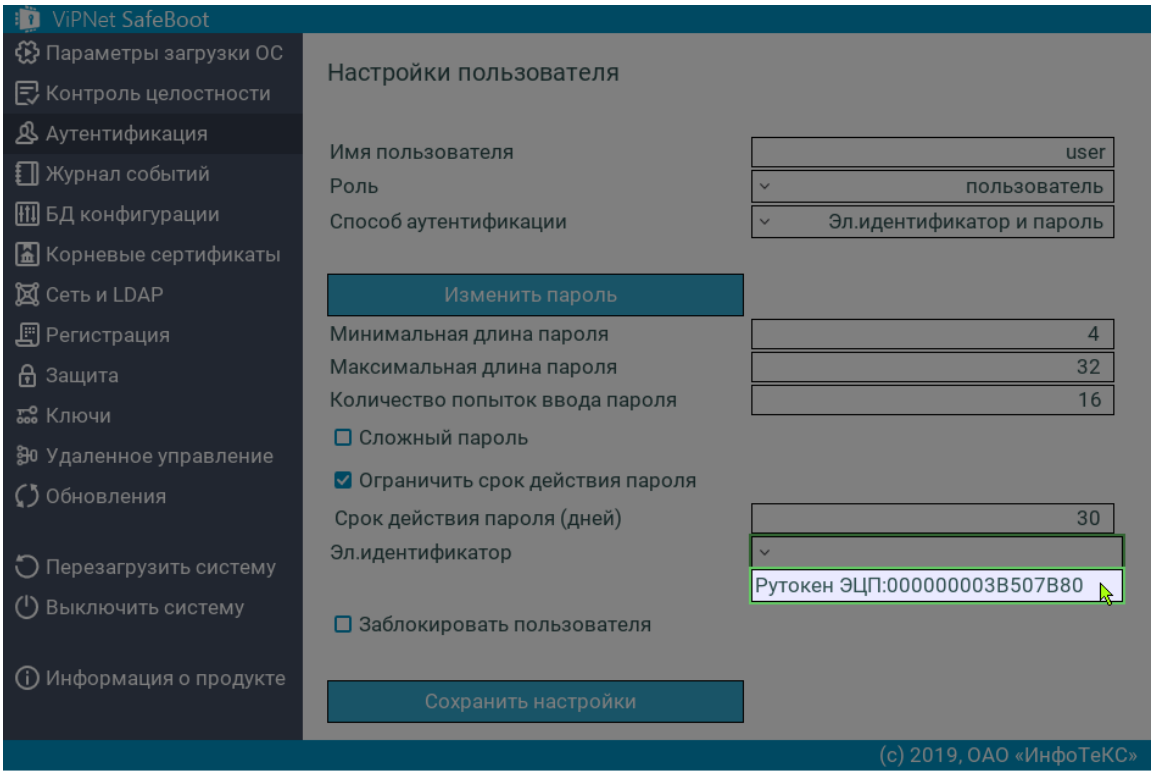
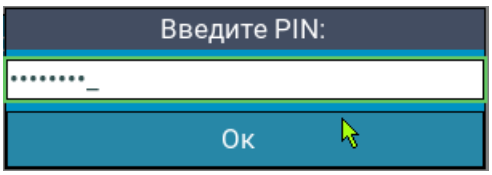


Рисунок 84. Выбор в качестве электронного идентификатора Рутокен ЭЦП

7 После приглашения ввести PIN, введите текущий PIN-код для установленного электронного идентификатора.



8 Выберите сертификат пользователя, нажав на пункт меню **Сертификат пользователя**.

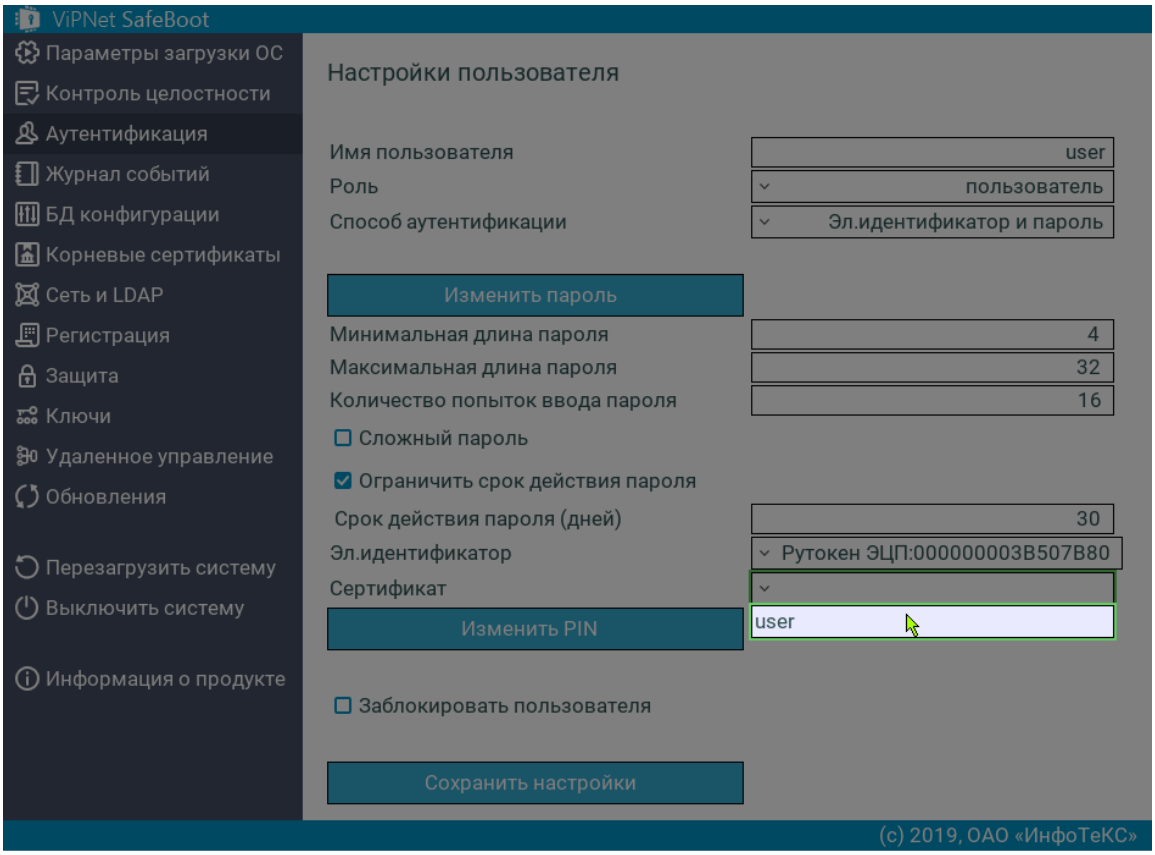
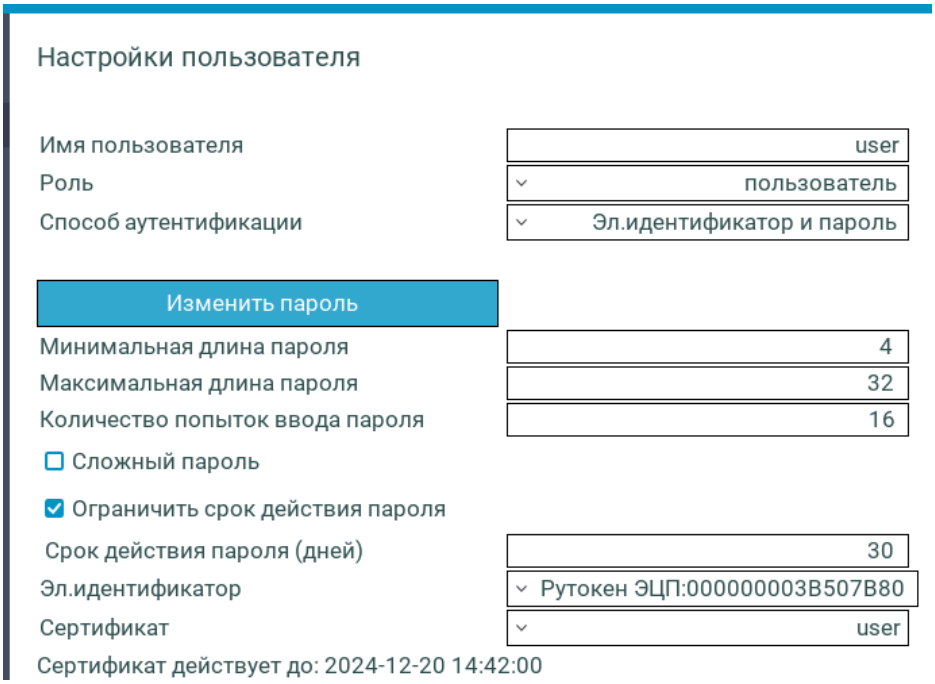


Рисунок 85. Выбор сертификата пользователя

При отсутствии ошибок, назначенный сертификат появится в строке **Сертификат пользователя**:



9 Выберите пункт **Изменить пароль**.

Примечание. Ограничения, действующие при создании пароля для обычного пользователя:

- минимальная длина пароля — 4 символа;
- максимальная длина пароля — 32 символа.

Данные ограничения задаются администратором и могут отличаться от указанных.

Ограничения, действующие при создании пароля для администратора и аудитора:

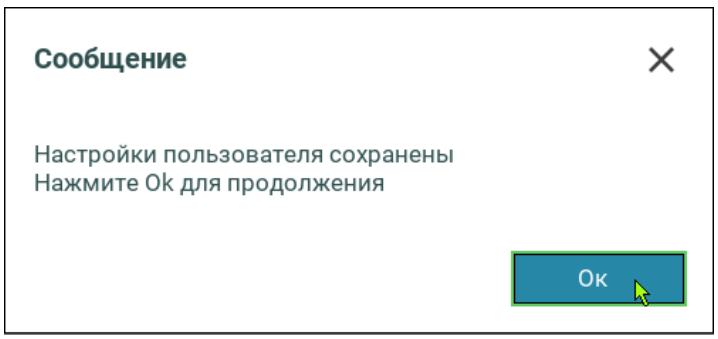
- минимальная длина пароля — 8 символов;
- максимальная длина пароля — 32 символа.

10 Для использования более надежного пароля установите флажок **Сложный пароль**.

Примечание. Критерии, действующие при создании сложного пароля:

- длина пароля не менее 8 символов;
- минимум один буквенный символ в верхнем регистре;
- минимум один буквенный символ в нижнем регистре;
- минимум один спецсимвол;
- минимум один цифровой символ.

11 Убедитесь, что все поля заполнены правильно, и выберите **Сохранить настройки**.



12 Нажмите **Ok**.

При успешной регистрации имя пользователя появится в списке **Текущие пользователи**.

Добавление учетных записей пользователей с аутентификацией по паролю на электронном идентификаторе

Чтобы добавить учетную запись пользователя с аутентификацией по паролю на электронном идентификаторе, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 В меню режима настроек выберите **Аутентификация**.

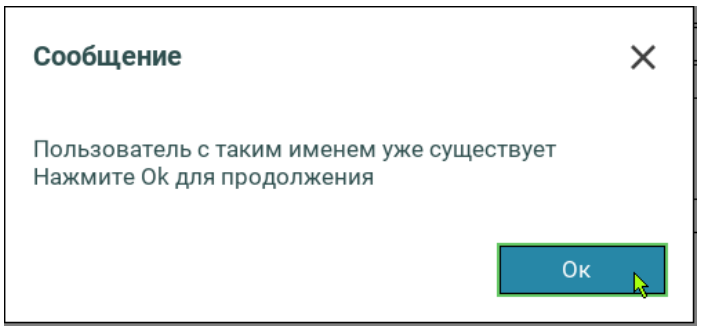
3 В открывшемся окне выберите **Добавить нового пользователя**.

4 В окне **Настройки пользователя** выберите **Имя пользователя**.

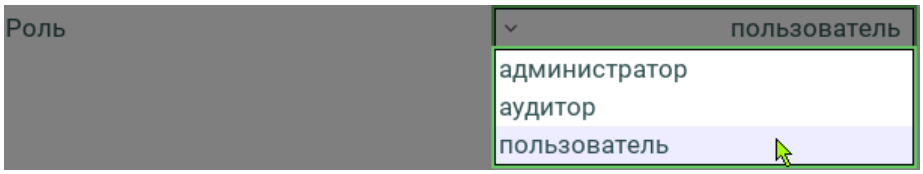
Введите имя пользователя.

Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

Если в ViPNet SafeBoot уже зарегистрирован пользователь с введенным именем, появится соответствующее сообщение.

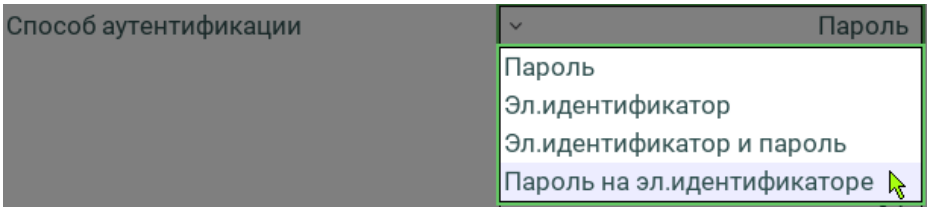


5 В пункте **Роль** в открывшемся списке выберите роль.



Внимание! Общее максимальное количество пользователей — 32.

В пункте **Способ аутентификации** в открывшемся списке выберите способ аутентификации **Пароль на эл. идентификаторе**:



6 Выберите пункт **Эл. идентификатор**.

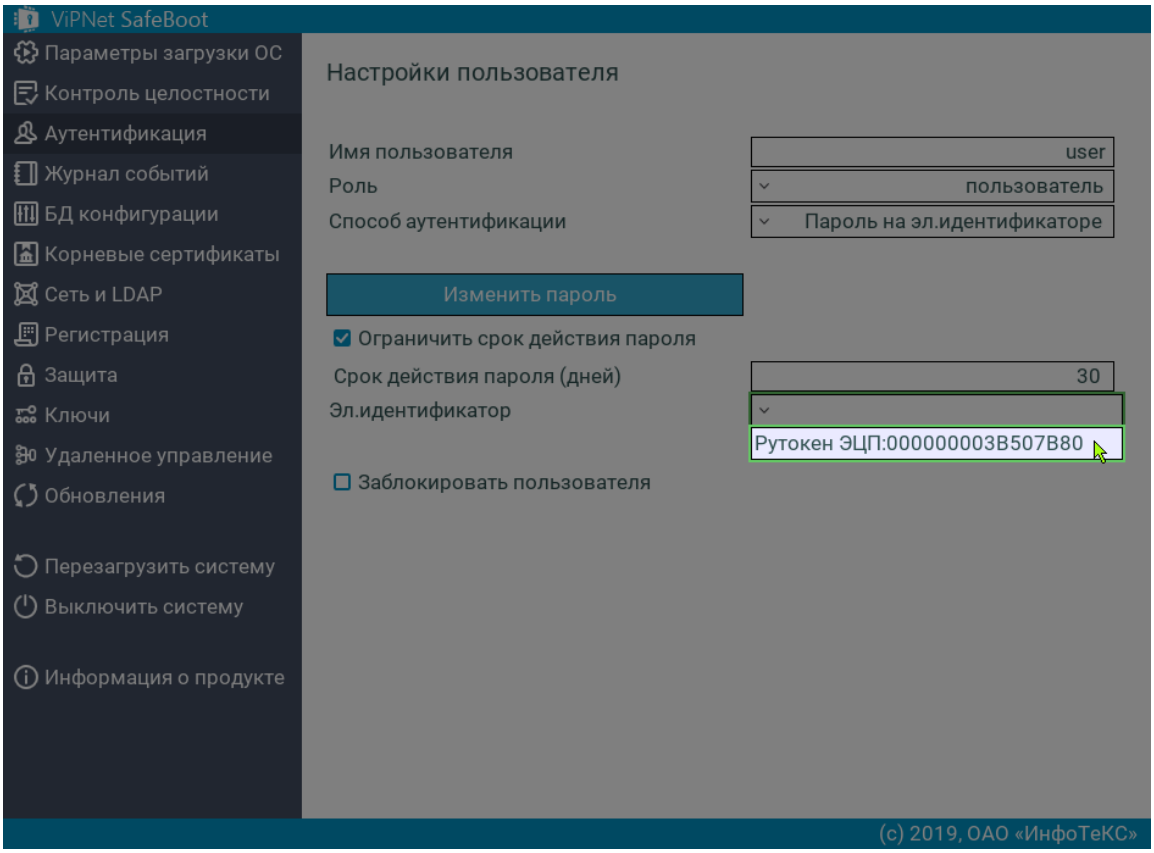
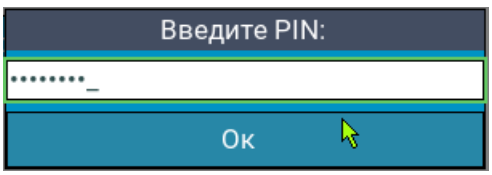


Рисунок 86. Выбор в качестве электронного идентификатора Рутокен ЭЦП

7 После приглашения ввести PIN, введите текущий PIN-код для установленного электронного идентификатора.



8 Выберите пункт **Изменить пароль**.

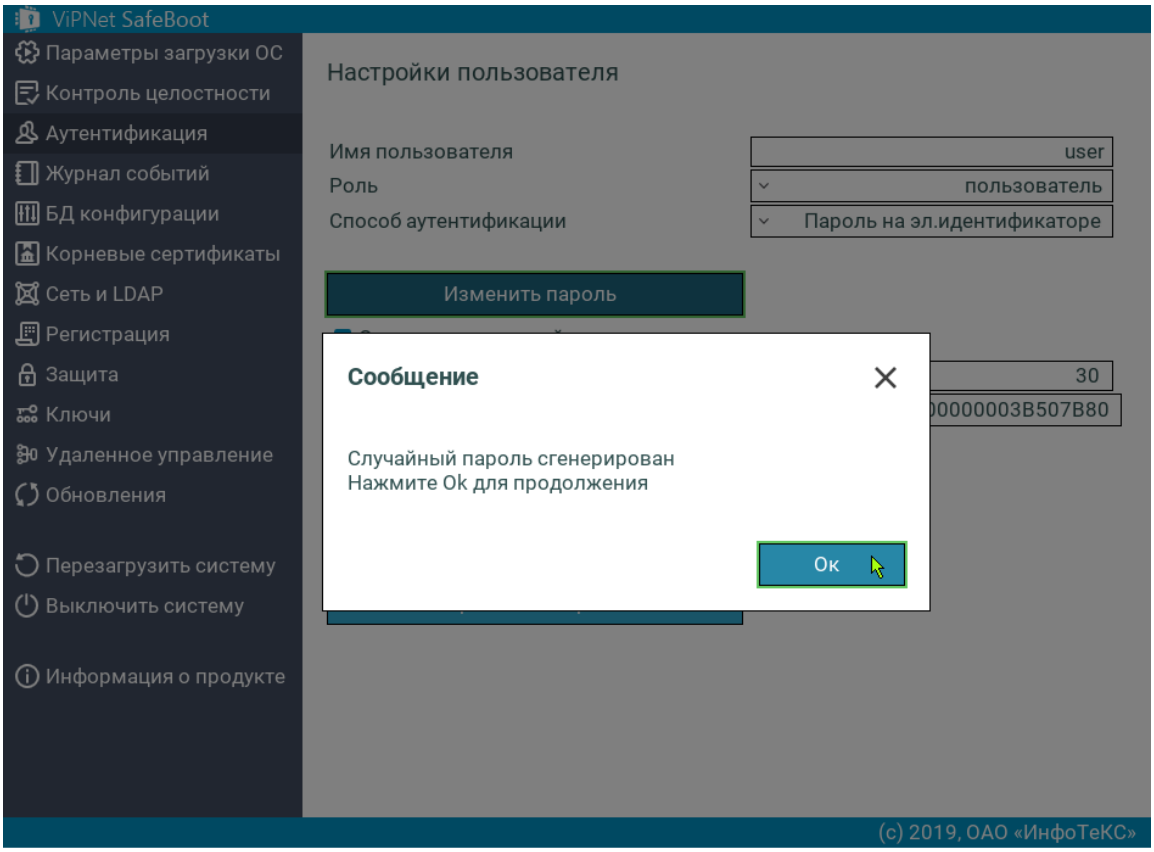
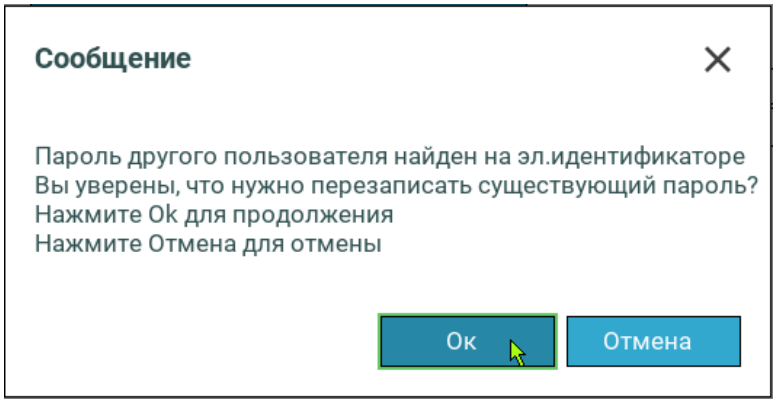


Рисунок 87. Генерация случайного пароля на электронном идентификаторе

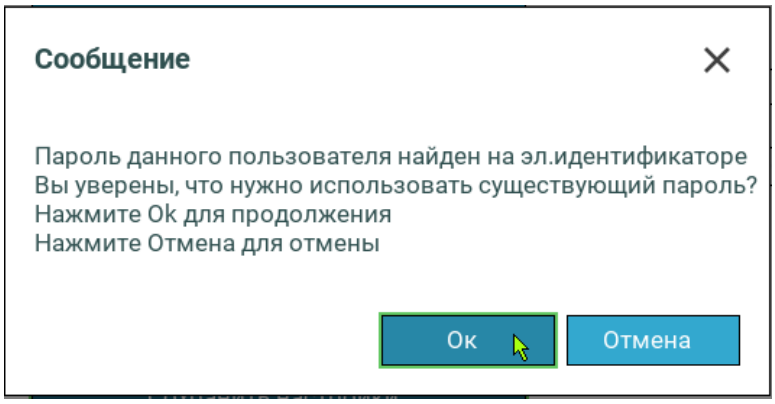
9 Дождитесь появления сообщения об окончании генерации и нажмите любую клавишу.

10 Убедитесь, что все поля заполнены правильно, и выберите **Сохранить настройки**.

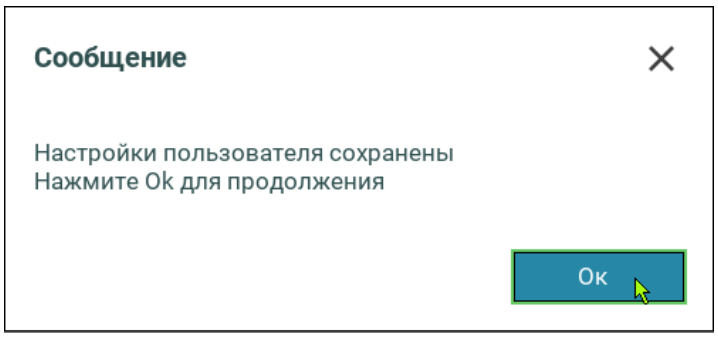
Если ранее на электронном идентификаторе уже был сгенерирован пароль для другого пользователя, то появится следующее сообщение:



Если на электронном идентификаторе уже есть пароль для текущего пользователя, то появится следующее сообщение:



Нажмите **Ок** для сохранения настроек.



11 Нажмите **Ок**.

При успешной регистрации имя пользователя появится в списке **Текущие пользователи**.

Добавление учетных записей пользователей с LDAP аутентификацией

ViPNet SafeBoot позволяет выполнять аутентификацию пользователей, осуществляемую непосредственно LDAP сервером. Администратору ViPNet SafeBoot предоставляется управление разрешениями путем установки списков разрешенных пользователей. Для доступа к этой функции требуется предварительно осуществить настройку сети и LDAP. Порядок выполнения настроек приведен в разделе Настройки сети и LDAP на стр. 161.

Редактирование учетных записей пользователей

Редактирование всех полей учетной записи доступно только Администратору. Пользователю и Аудитору доступен для изменения только свой пароль, остальные параметры своей учетной записи доступны лишь в режиме чтения.

Чтобы изменить параметры учетной записи пользователя, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Аутентификация**.
3. В открывшемся окне выберите из списка **Текущие пользователи** имя пользователя, данные которого необходимо изменить.
4. Выполните необходимые изменения.

Примечание. Полный доступ к настройкам пользователя с аутентификацией по электронному идентификатору предоставляется после ввода PIN-кода.

5. Убедитесь, что все поля заполнены правильно, и выберите **Сохранить настройки**.

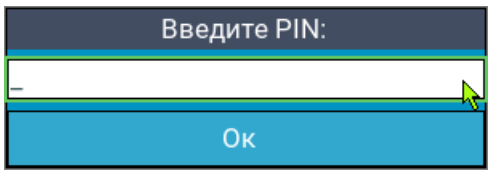
Редактирование учетной записи пользователя с аутентификацией по электронному идентификатору

Внешний вид настроек учетной записи пользователя с аутентификацией по электронному идентификатору будет меняться в зависимости от использования администратором электронного идентификатора и ввода PIN-кода при входе в учетную запись пользователя.

Для редактирования учетной записи пользователя с аутентификацией по электронному идентификатору, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. Подключите электронный идентификатор, назначенный пользователю.
3. В меню режима настроек выберите **Аутентификация**.
4. В меню **Текущие пользователи** выберите из списка имя пользователя, учетную запись которого нужно открыть.

   Появится сообщение о необходимости ввести PIN-код.

5. Введите PIN-код.

Меню настроек пользователя примет следующий вид:

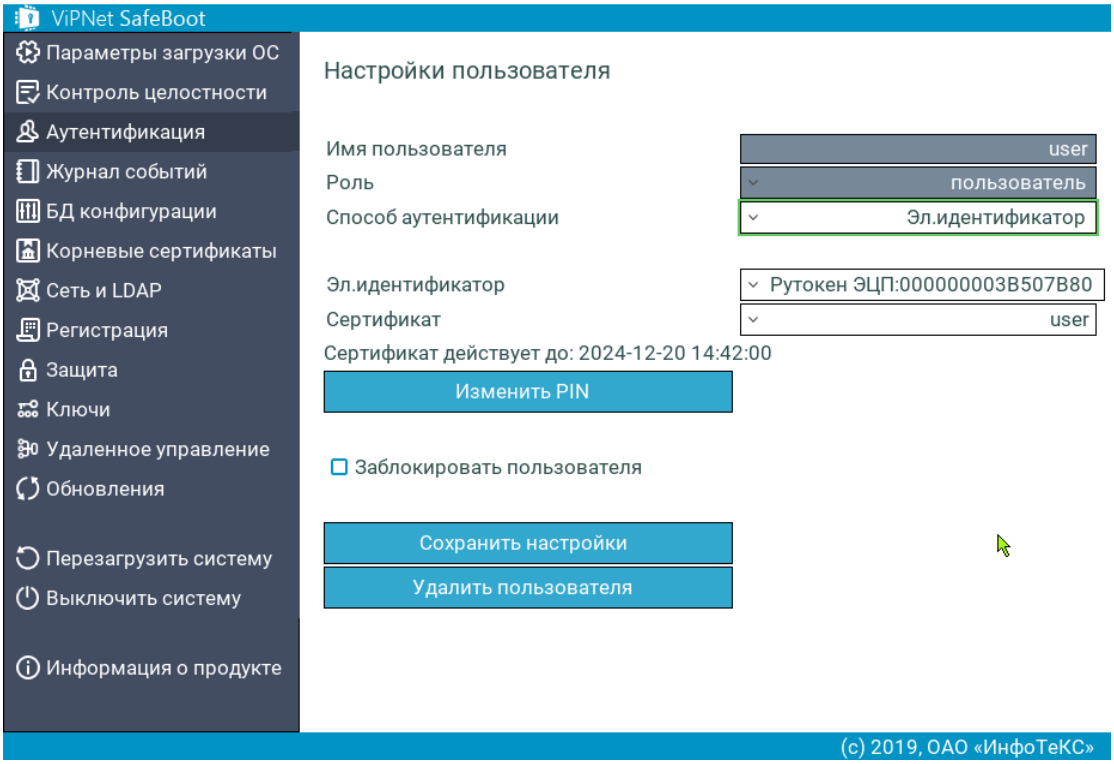


Рисунок 88. Вход в настройки пользователя с вводом PIN-кода

6 При входе в учетную запись пользователя без ввода PIN-кода (электронный идентификатор не подключен), изменение сертификата пользователя будет недоступно.

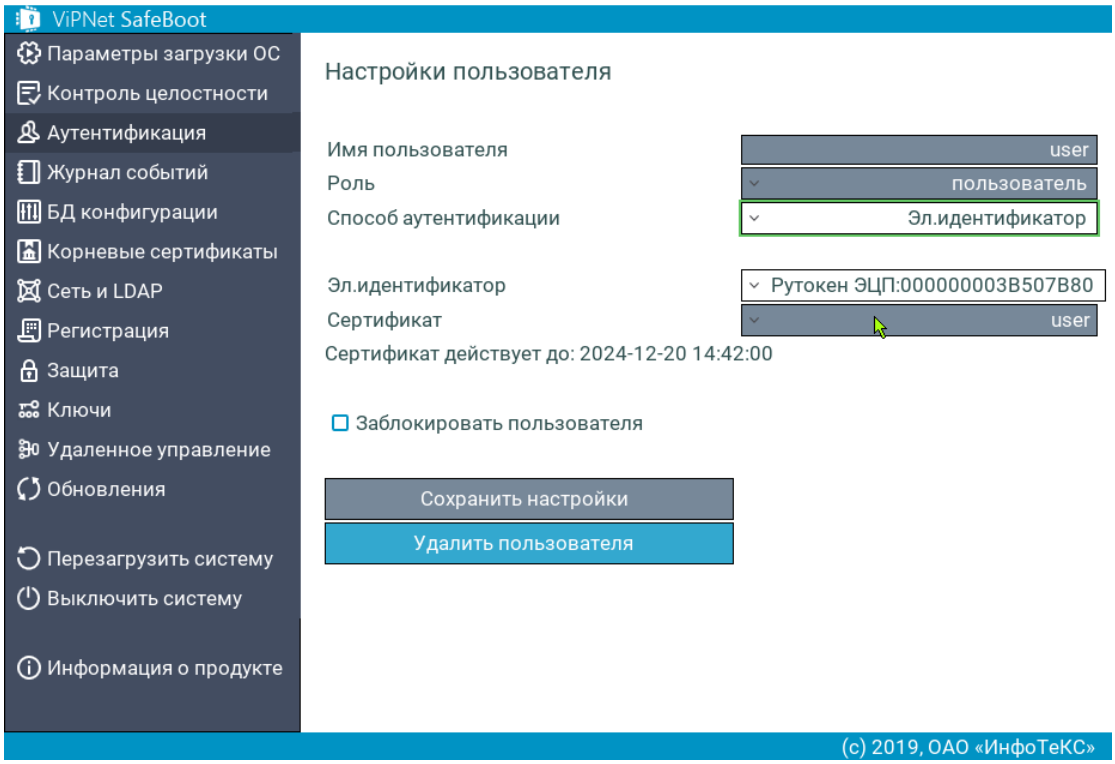


Рисунок 89. Вход в настройки пользователя без ввода PIN-кода (электронный идентификатор не подключен)

7 Сохраните выполненные изменения, выбрав **Сохранить настройки**.

Блокирование учетной записи пользователя

Чтобы заблокировать учетную запись пользователя, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Аутентификация**.
3. В открывшемся окне выберите из списка **Текущие пользователи** имя пользователя, учетную запись которого необходимо заблокировать.
4. В открывшемся окне **Настройки пользователя** установите флажок в пункте **Заблокировать пользователя**.
5. Выберите **Сохранить настройки**.

   Вход в систему пользователю данной учетной записи будет заблокирован.

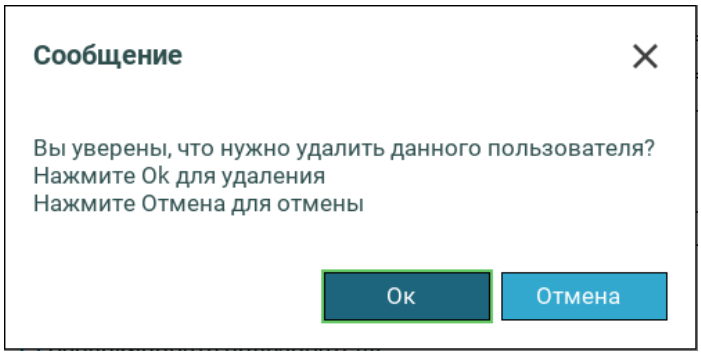
   Для разблокирования учетной записи пользователя необходимо снять флажок в пункте **Заблокировать пользователя** из меню **Настройки пользователя** и сохранить изменения.

Удаление учетных записей пользователей

Чтобы удалить учетную запись пользователя, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Аутентификация**.
3. В открывшемся окне выберите из списка **Текущие пользователи** имя пользователя, которого необходимо удалить.
4. В открывшемся окне **Настройки пользователя** выберите **Удалить пользователя**.

   Появится следующая надпись:

   После подтверждения учетная запись пользователя будет удалена.

8

Управление сертификатами

Изменение сертификатов и ключей

Перечень установленных в ViPNet SafeBoot сертификатов и ключей находится в пункте меню режима настроек **Ключи**. Меню **Ключи** позволяет изменить сертификат контроля целостности запросов управления, сертификат контроля целостности данных и ключ защиты данных. Измененные ранее сертификаты и ключ можно вернуть к установленным по умолчанию.

Сертификаты и ключи должны удовлетворять следующим правилам:

- алгоритм: ГОСТ Р 34.10-2012 256;
- параметры алгоритма: CryptoPro_A_ParamSet.

Чтобы изменить сертификат контроля целостности запросов управления, сертификат контроля целостности данных и ключ защиты данных, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).

2 Подключите USB-диск, содержащий файл сертификата.

3 В меню режима настроек выберите **Ключи**.

4 В открывшемся окне в подстроке **Сертификат КЦ запросов управления** выберите **Изменить сертификат**.

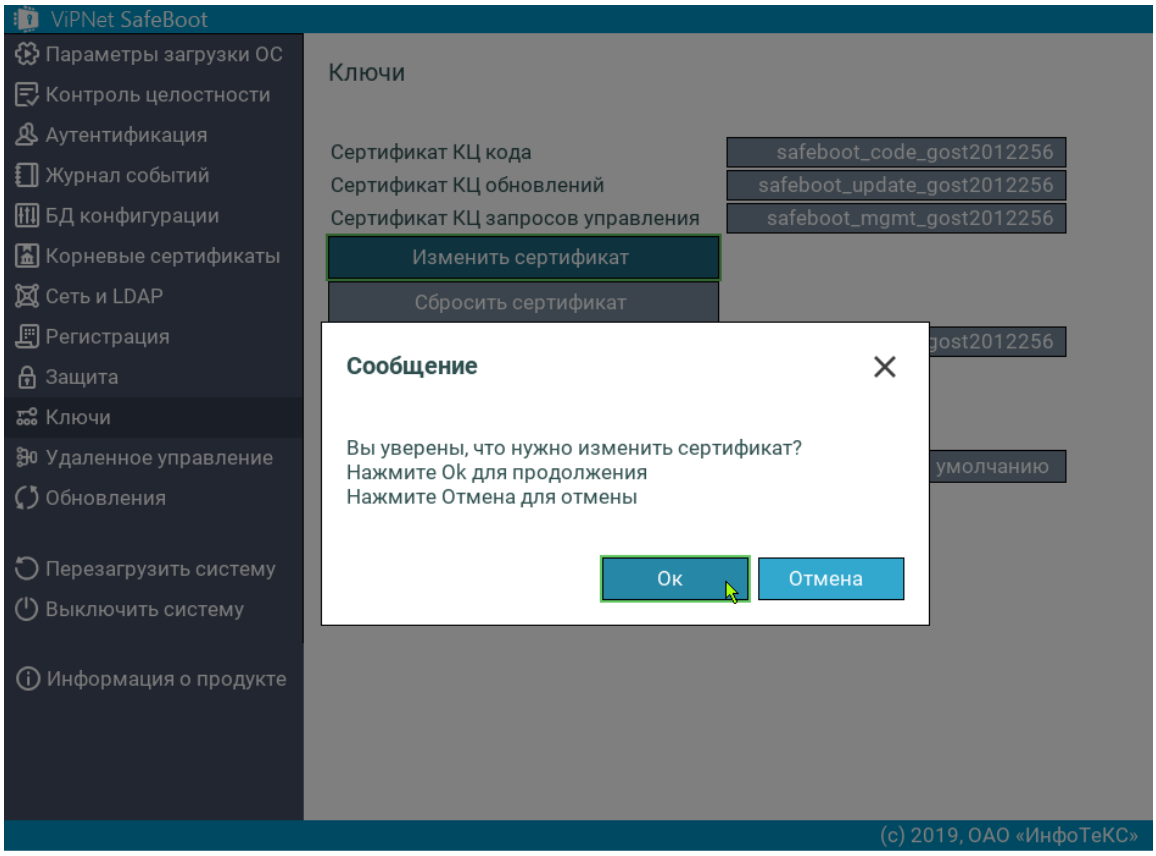


Рисунок 90. Изменение сертификата КЦ запросов управления в графическом режиме

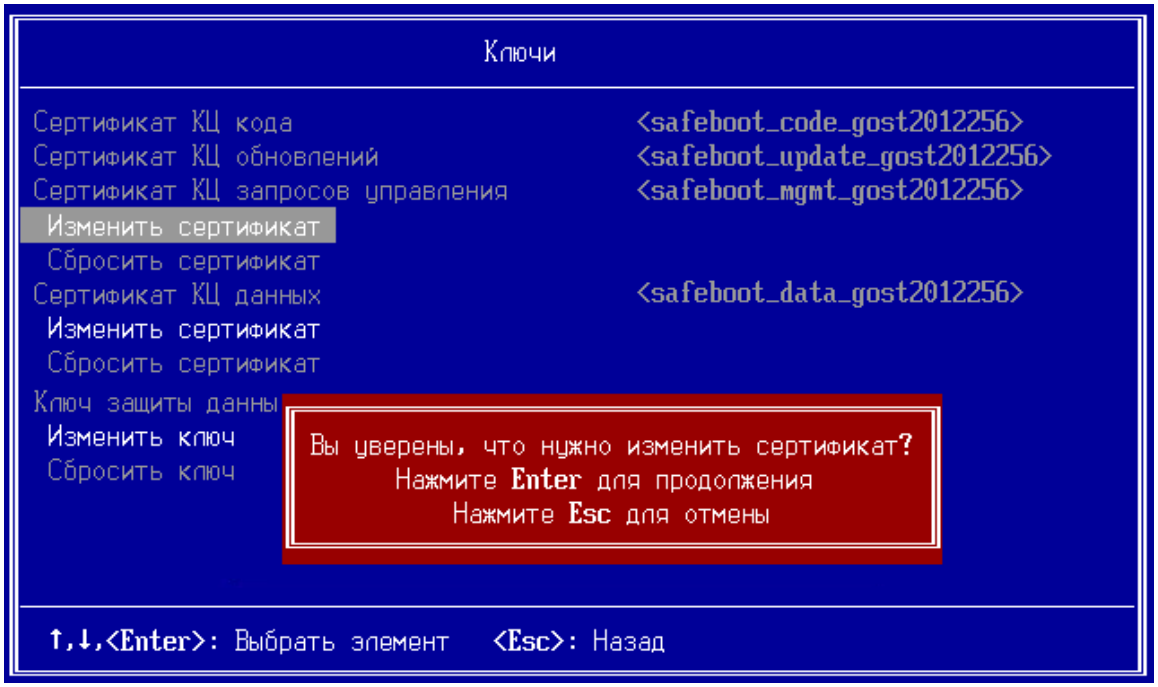


Рисунок 91. Изменение сертификата КЦ запросов управления в текстовом режиме

5 Нажмите **Ок** или **Enter** для продолжения.

В случае если USB-диск не подключен, появится соответствующее сообщение. Вставьте USB-диск, содержащий сертификат, и повторите попытку изменить сертификат.

6 В открывшемся списке выберите файл сертификата.

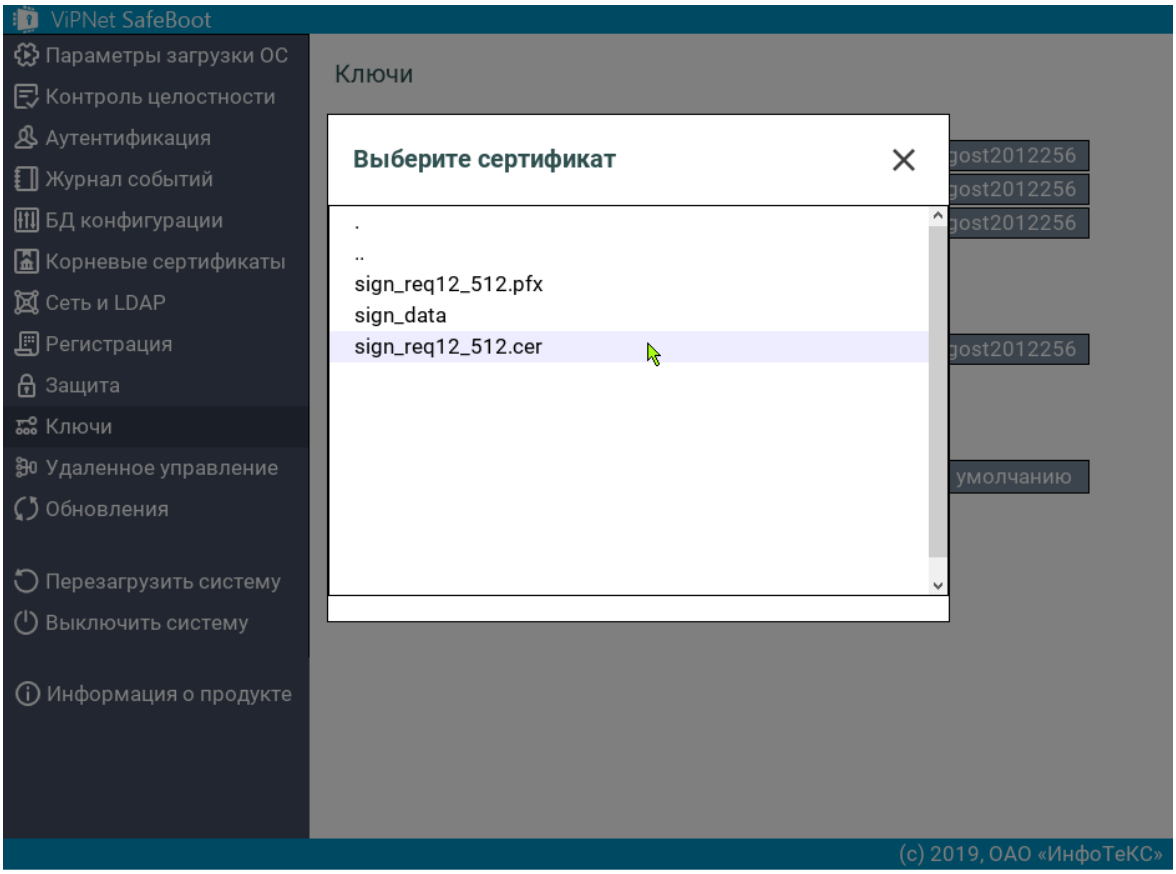


Рисунок 92. Выбор сертификата

Выбранный сертификат появится в строке **Сертификат КЦ запросов управления**.

7 Для изменения сертификата КЦ данных подключите USB-диск, содержащий необходимые файлы. Сертификат КЦ данных должен быть в формате контейнера ViPNet CSP.

8 В подстроке **Сертификат КЦ данных** выберите **Изменить сертификат**.

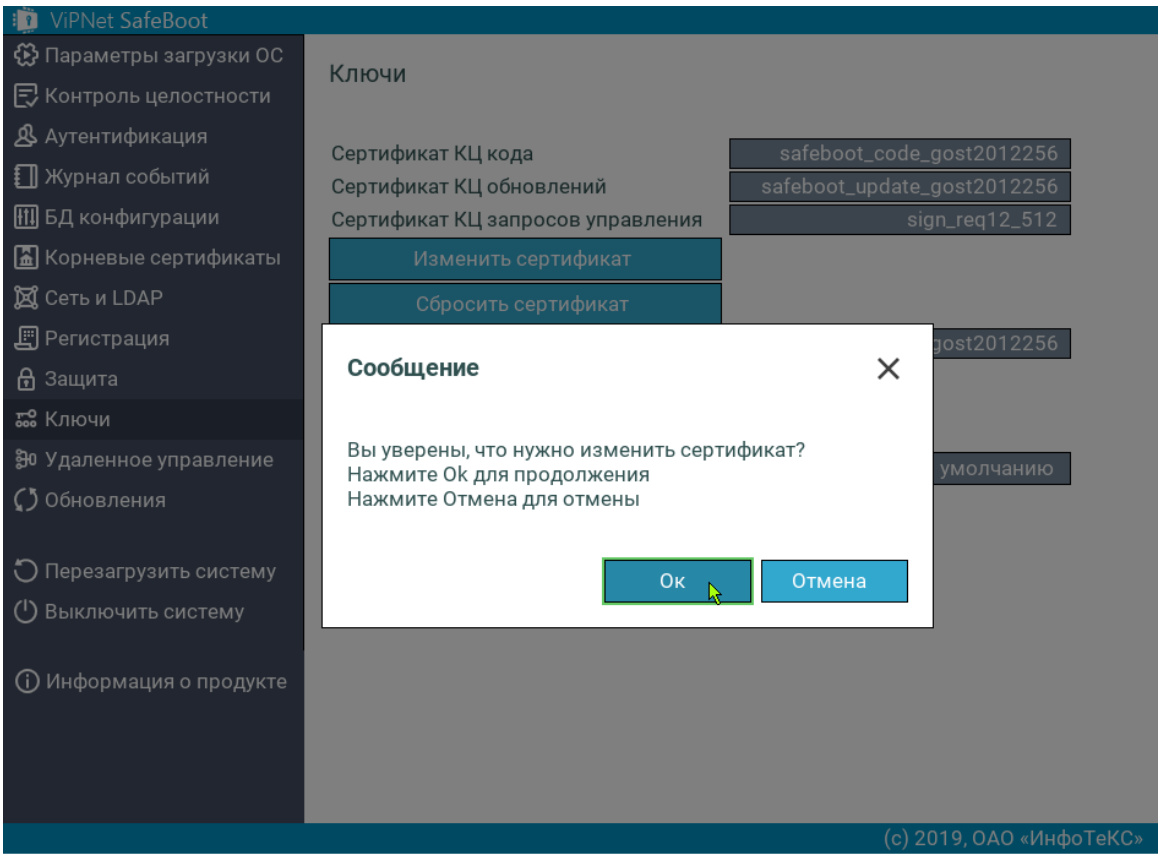


Рисунок 93. Изменение сертификата КЦ данных

9 Нажмите **Ок** для продолжения.

В случае если USB-диск не подключен, появится соответствующее сообщение. Вставьте USB-диск, содержащий сертификат, и повторите попытку изменить сертификат.

10 Выберите ключевой контейнер с сертификатом.

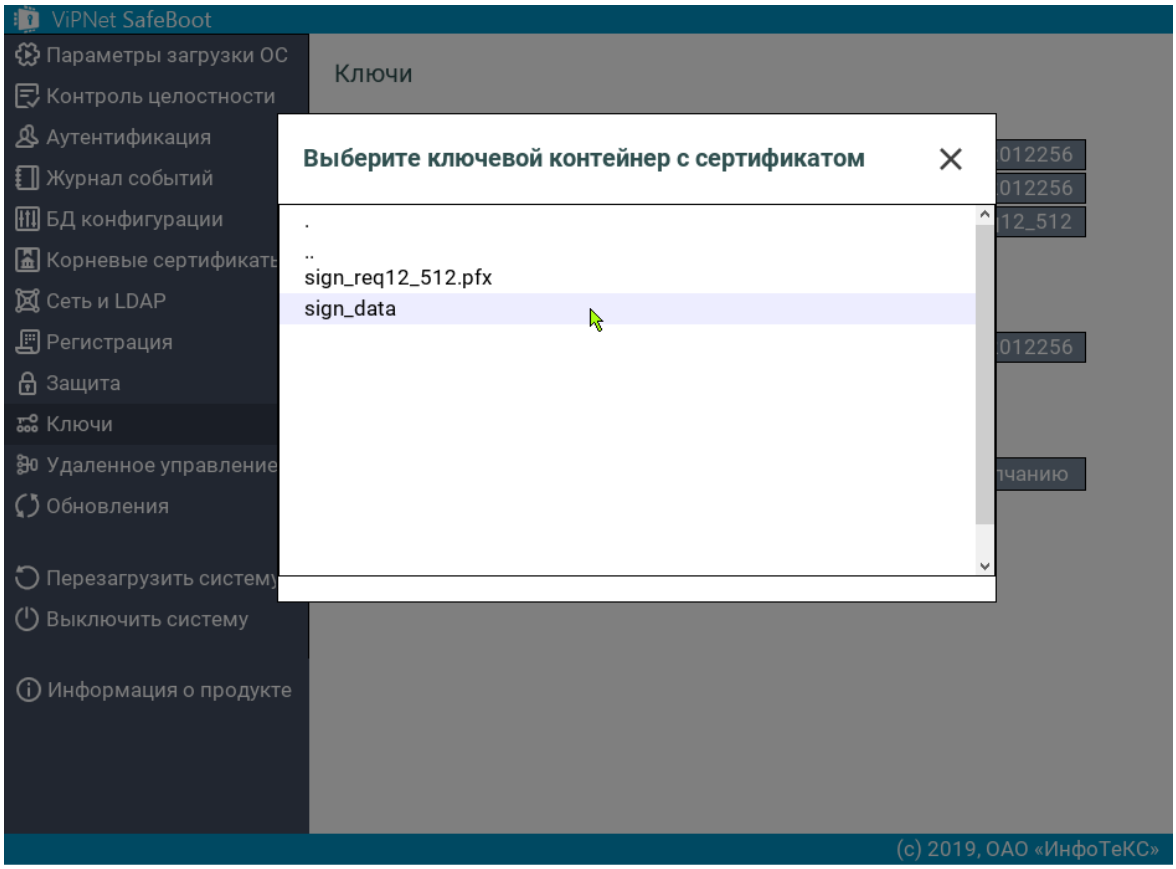
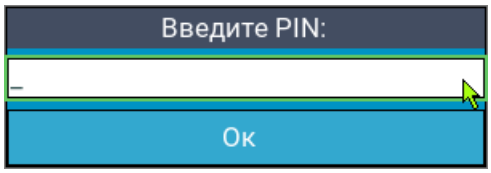


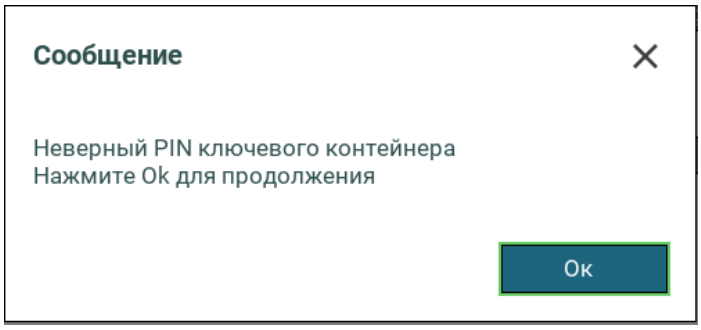
Рисунок 94. Выбор сертификата

В случае если файл ключевого контейнера был выбран неверно, появится соответствующее сообщение об ошибке. Убедитесь, что USB-диск содержит сертификат КЦ данных в формате контейнера ViPNet CSP, и повторите изменение сертификата.

11 Далее появится приглашение ввести PIN код.



Если PIN код был введен неверно, появится сообщение об ошибке:



Нажмите **Ok** для продолжения и повторите изменение сертификата с правильным PIN-кодом.

Если все действия выполнены правильно, то в строке **Сертификат КЦ данных** появится имя файла ключевого контейнера с сертификатом.

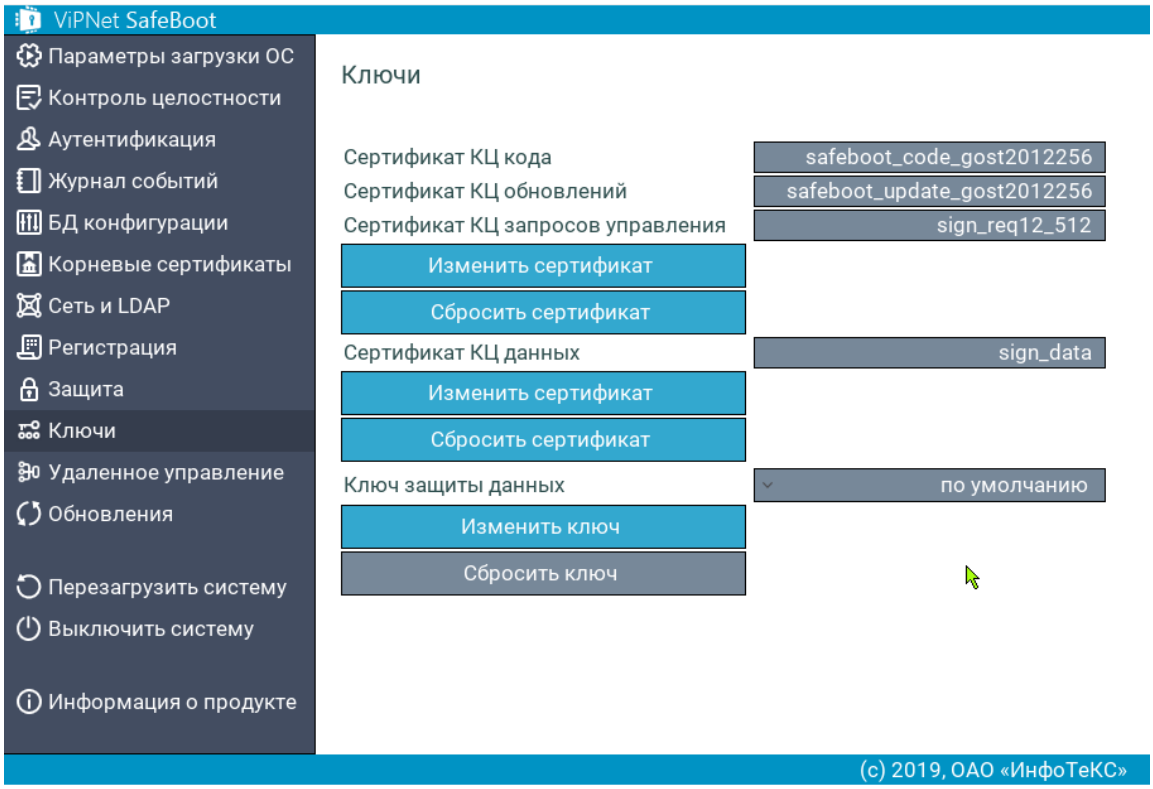


Рисунок 95. Меню с измененными сертификатами

12 Для изменения ключа защиты данных, в подстроке **Ключ защиты данных** выберите **Изменить ключ**.

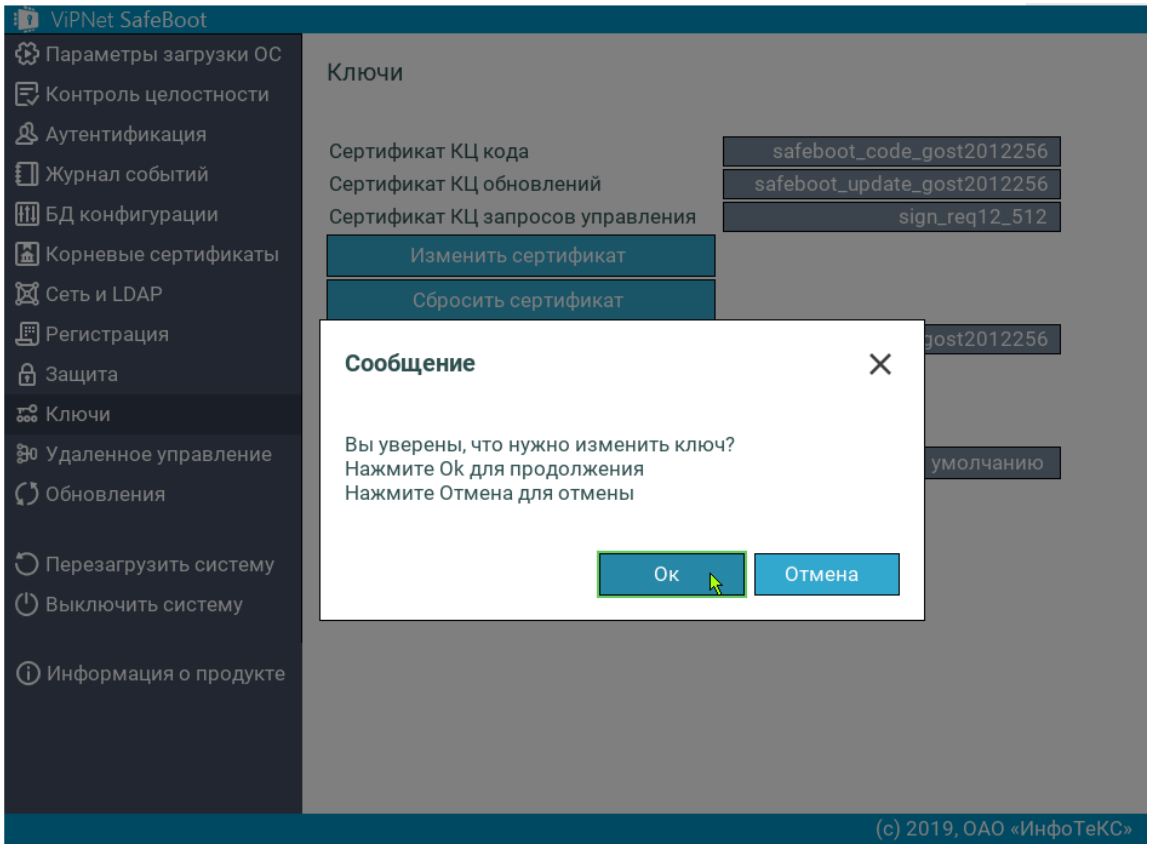
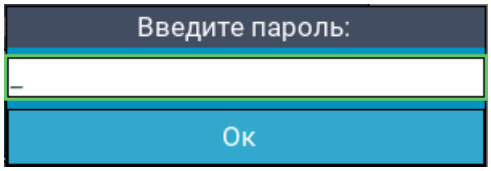


Рисунок 96. Изменение ключа защиты данных

13 Нажмите **Enter** для продолжения.

В появившемся окне введите пароль.



Затем повторите ввод пароля.

В строке **Ключ защиты данных** значение <по умолчанию> изменится на <изменен>.

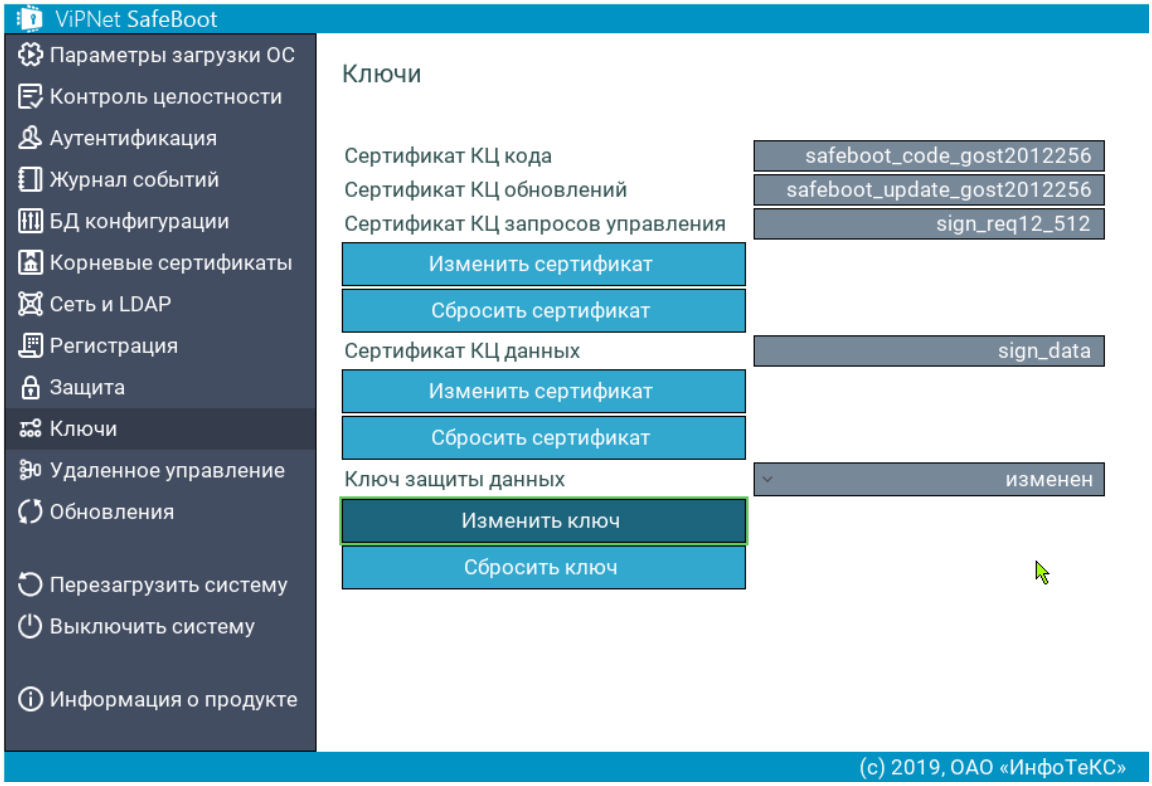


Рисунок 97. Меню с измененным ключом защиты данных

14 Чтобы вернуться к сертификатам или ключу, установленным по умолчанию, выберите подпункт **Сбросить сертификат** или **Сбросить ключ** в соответствующем пункте меню.

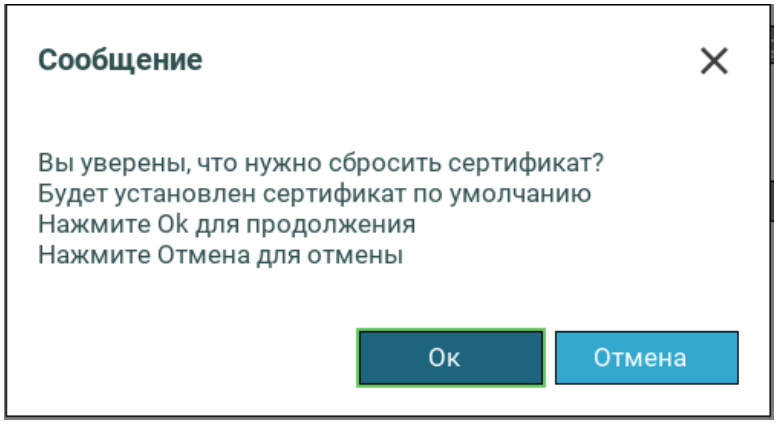


Рисунок 98. Удаление сертификата

15 Нажмите **Enter**. Будет установлен сертификат по умолчанию.

Корневой сертификат доверенного центра сертификации

Корневой сертификат доверенного центра сертификации — это сертификат, от имени которого выдаются сертификаты на предприятии, включая сертификат пользователя, а также сертификаты вышестоящих центров сертификации. Форматы сертификата, используемые в ViPNet SafeBoot — X.509 (DER или PEM) и PKCS#7. Корневые сертификаты используются в случае аутентификации пользователей по электронному идентификатору, а также для аутентификации по LDAP при использовании TLS. В случае если такой вид аутентификации не используется, установка корневых сертификатов не является необходимой. Для получения более подробной информации обратитесь к документации центра сертификации, используемого на вашем предприятии или в уполномоченную организацию, предоставляющую услуги центра сертификации.

Примечание. ViPNet SafeBoot поддерживает установку до четырех корневых сертификатов.

Установка корневого сертификата

Корневой сертификат доверенного центра сертификации — это сертификат пользователя, выданный от имени доверенного центра, а также сертификаты вышестоящих центров сертификации.

Чтобы установить корневой сертификат, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. Подключите USB-диск, содержащий файл сертификата, который необходимо установить.
3. В меню режима настроек выберите **Корневые сертификаты**.
4. В открывшемся окне выберите **Установить корневой сертификат**.
5. Из списка выберите файл сертификата.

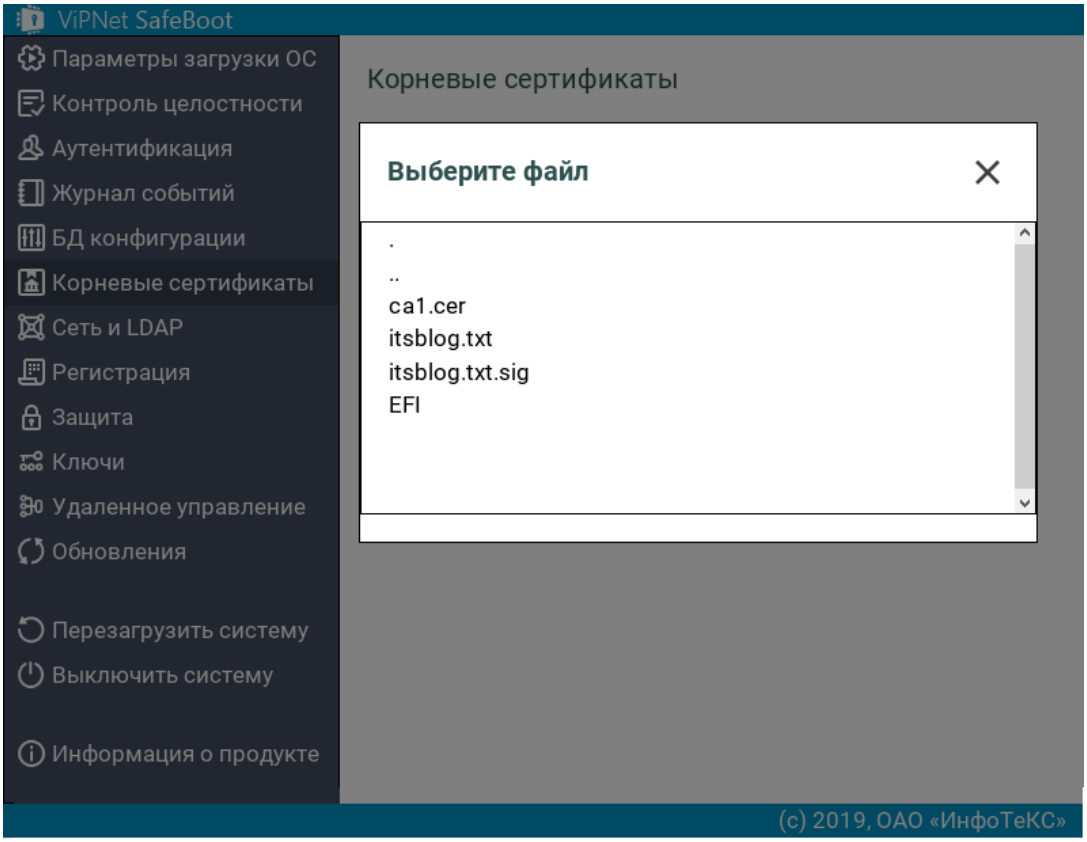


Рисунок 99. Выбор корневого сертификата

Выбранный сертификат появится в списке **Установленные корневые сертификаты**.

Экспорт корневого сертификата

Чтобы экспортировать корневой сертификат на USB-диск, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. Подключите USB-диск, на который собираетесь экспортировать сертификат.
3. В меню режима настроек выберите **Корневые сертификаты**.
4. В открывшемся окне выберите нужный сертификат из списка **Установленные корневые сертификаты**.
5. В открывшемся окне выберите **Экспортировать корневой сертификат**.

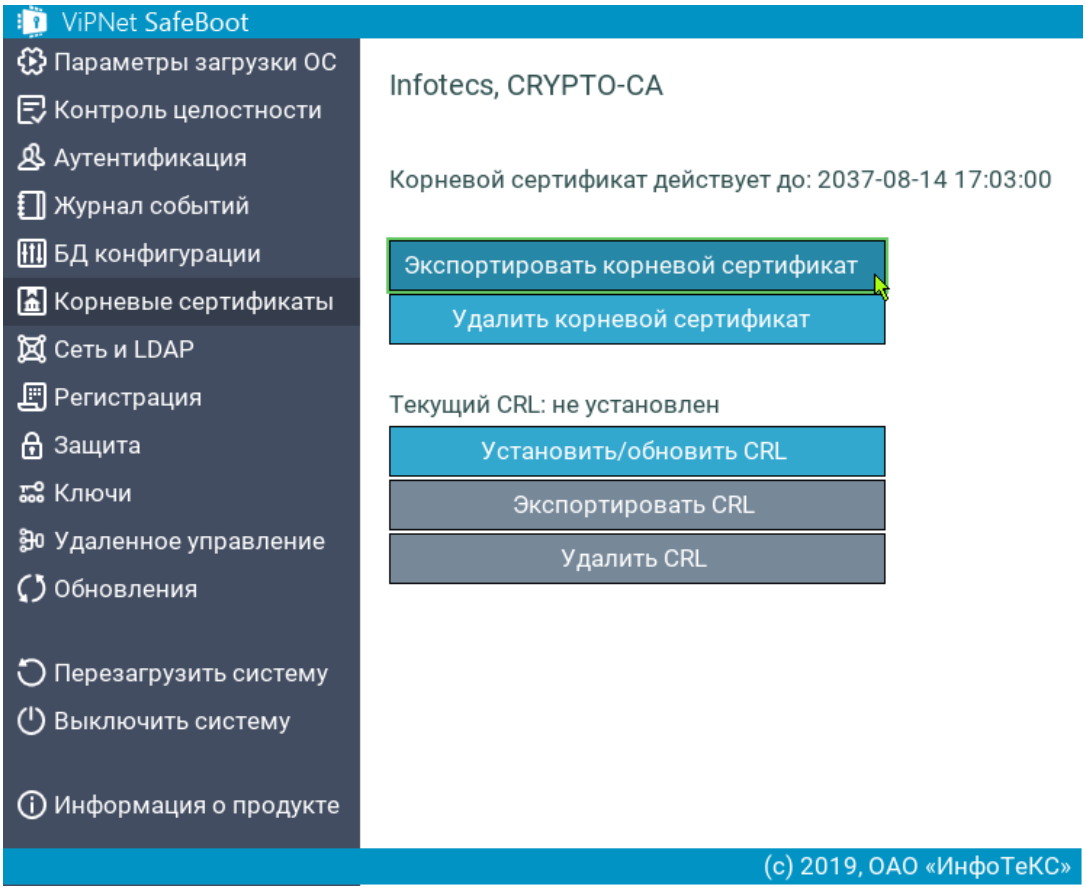
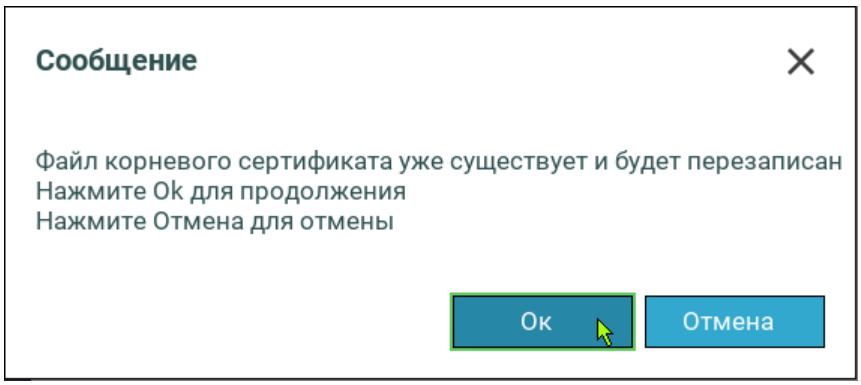


Рисунок 100. Экспорт корневого сертификата

6 Если на USB-диске будет обнаружен файл корневого сертификата **ca.crt**, то появится следующее сообщение:



Нажмите **Esc**, если собираетесь экспортировать корневой сертификат на другой USB-диск, или **Enter** для продолжения. Корневой сертификат экспортируется в файл **ca.crt** в корень USB-диска. На экране появится следующее сообщение о том, что корневой сертификат экспортирован.

Удаление корневого сертификата

Чтобы удалить корневой сертификат, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Корневые сертификаты**.
3. В открывшемся окне, из списка **Установленные корневые сертификаты** выберите нужный сертификат.
4. В открывшемся окне, выберите **Удалить корневой сертификат.**

   Выбранный сертификат будет удален из списка **Установленные корневые сертификаты**.

Операции со списком отозванных сертификатов (CRL)

Установка или обновление CRL

Чтобы установить или обновить CRL, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. Подключите USB-диск, содержащий файл CRL, который необходимо установить или обновить.
3. В меню режима настроек выберите **Корневые сертификаты**.
4. В открывшемся окне из списка **Установленные корневые сертификаты** выберите нужный сертификат.

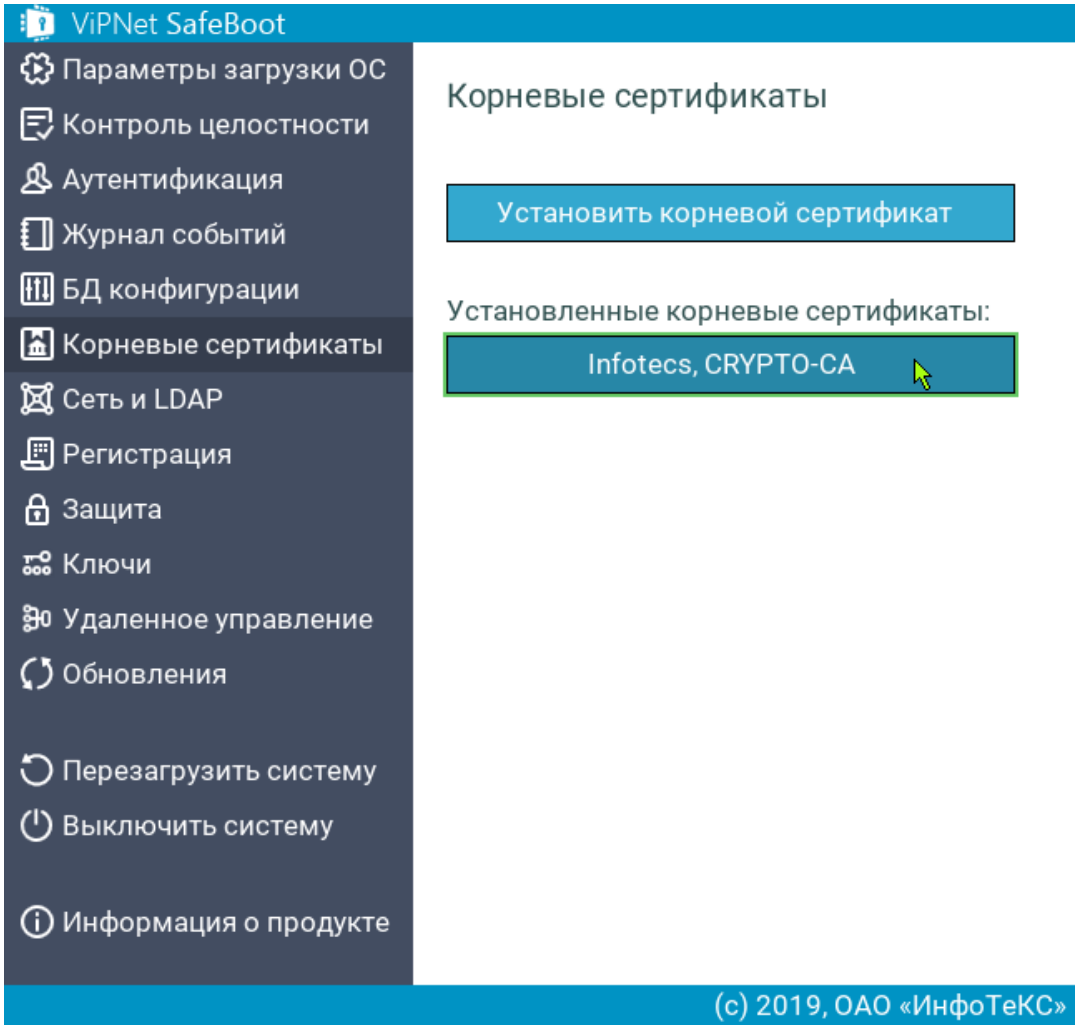


Рисунок 101. Выбор установленного сертификата

5 В открывшемся меню установленного сертификата выберите **Установить/обновить CRL**.

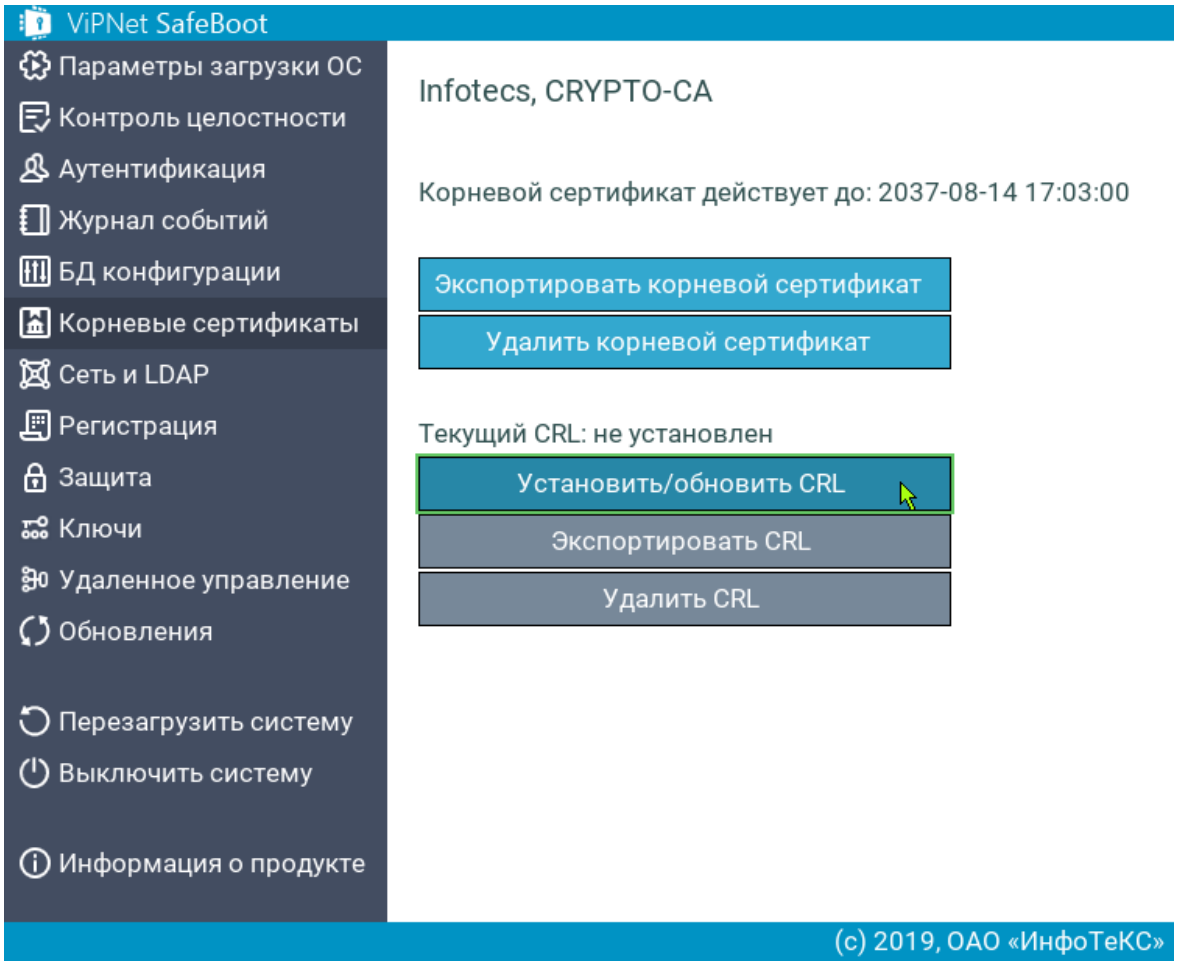
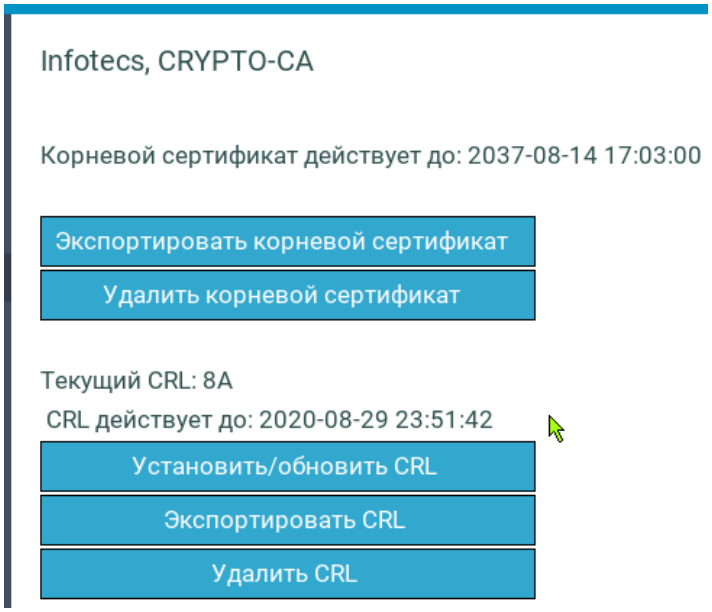


Рисунок 102. Установка или обновление файла CRL

6 Из открывшегося списка выберите файл **crl.crl**.

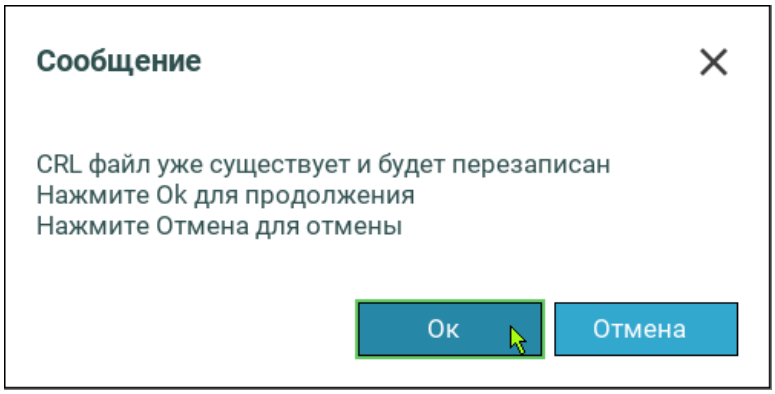
В поле **Текущий CRL** отобразится номер и срок действия выбранного CRL:



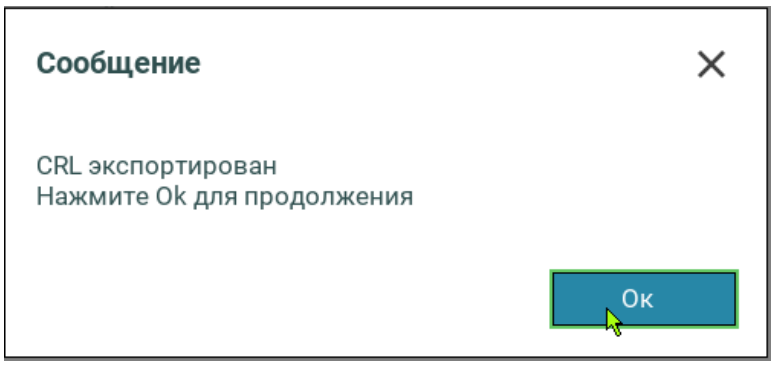
Экспорт CRL

Чтобы экспортировать CRL на USB-диск, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. Подключите USB-диск, на который необходимо собираетесь экспортировать CRL.
3. В меню режима настроек выберите **Корневые сертификаты**.
4. В открывшемся окне из списка **Установленные корневые сертификаты** выберите нужный сертификат.
5. В открывшемся меню установленного сертификата выберите **Экспортировать CRL**.
6. Если на USB-диске будет обнаружен файл **crl.crl**, то появится следующее сообщение:



Нажмите **Отмена**, если собираетесь экспортировать CRL на другой USB-диск, или **Ок** для продолжения. CRL экспортируется в файл **crl.crl** в корень USB-диска. На экране появится следующее сообщение:



Нажмите **Ок** для продолжения.

Удаление CRL

Чтобы удалить CRL, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Корневые сертификаты**.
3. В открывшемся окне из списка **Установленные корневые сертификаты** выберите нужный сертификат.
4. В открывшемся меню установленного сертификата выберите **Удалить CRL**.

   Выбранный CRL будет удален.

Подготовка к работе электронных идентификаторов

Подготовка к работе JaCarta

Для подготовки к работе электронного идентификатора JaCarta необходимо установить на технологический ПК ПО «Единый клиент JaCarta» производства компании «Аладдин». В случае использования комбинированных идентификаторов JaCarta PKI/ГОСТ может использоваться только режим PKI. В случае использования комбинированных идентификаторов JaCarta-2 PKI/ГОСТ может использоваться только режим ГОСТ. Идентификаторы JaCarta ГОСТ не поддерживаются.

Подготовка электронного идентификатора к работе заключается в его форматировании и записи на него ключевой информации и сертификата пользователя. Для этого выполните следующие действия:

- В ПО «Единый клиент JaCarta» произведите форматирование токена.
- В ПО «Единый клиент JaCarta» создайте запрос на сертификат.
- Получите сертификат передав запрос в удостоверяющий центр.
- В ПО «Единый клиент JaCarta» запишите полученный сертификат на электронный идентификатор.

Примечание. При импорте сертификата пользователя в ПО «Единый клиент JaCarta», необходимо убрать флажок в поле "Задать имя контейнера".

Для работы с ГОСТ сертификатами на JaCarta PKI потребуется дополнительно установить на технологический ПК ViPNet CSP, и выполнить следующие действия:

- При помощи утилиты «Создание запроса на сертификат» (входит в состав криптопровайдера ViPNet CSP) создать запрос на сертификат, указав носителем ключевой информации электронный идентификатор;
- Получить сертификат, передав запрос в удостоверяющий центр;
- В криптопровайдере ViPNet CSP записать полученный сертификат на электронный идентификатор.

В этом случае работа с сертификатами происходит без использования аппаратной криптографии на электронном идентификаторе.

Подготовка к работе Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен Lite

Для подготовки к работе электронного идентификатора типа Рутокен необходимо установить на технологический ПК следующее программное обеспечение:

- Комплект ПО «Драйверы Рутокен для Windows» производства компании «Актив».
- Криптопровайдер ViPNet CSP.

Подготовка электронного идентификатора к работе заключается в его форматировании и записи на него ключевой информации и сертификата пользователя. Для этого выполните следующие действия:

- При необходимости в ПО «Панель управления Рутокен» (входит в комплект «Драйверы Рутокен для Windows») произведите форматирование токена.
- При помощи утилиты «Создание запроса на сертификат» (входит в состав криптопровайдера ViPNet CSP) создайте запрос на сертификат, указав носителем ключевой информации электронный идентификатор.
- Получите сертификат передав запрос в удостоверяющий центр;
- В криптопровайдере ViPNet CSP запишите полученный сертификат на электронный идентификатор.

Для идентификаторов Рутокен ЭЦП и Рутокен ЭЦП 2.0 ключевой контейнер также может быть создан внешними средствами в формате pfx или p12 и записан на электронный идентификатор при помощи ПО «Панель управления Рутокен».

Подготовка к работе Guardant ID

Для подготовки к работе электронного идентификатора Guardant ID необходимо установить на технологический ПК криптопровайдер ViPNet CSP.

Подготовка электронного идентификатора к работе заключается в его форматировании и записи на него ключевой информации и сертификата пользователя. Для этого выполните следующие действия:

- При помощи утилиты «Создание запроса на сертификат» (входит в состав криптопровайдера ViPNet CSP) создайте запрос на сертификат, указав носителем ключевой информации корневой каталог на USB-носителе. Контейнер с ключевой информацией будет создан на USB-диске в каталоге \Infotecs\Containers.
- Получите сертификат передав запрос в удостоверяющий центр.
- Запишите полученный сертификат на USB-носитель.
- Инициализируйте электронный идентификатор записав на него контейнер с ключевой информацией и сертификат (см. Добавление учетных записей пользователей с аутентификацией по электронному идентификатору на стр. 117).

В данной версии ViPNet SafeBoot поддерживается только один сертификат на электронном идентификаторе Guardant ID.

9

Настройки сети и LDAP

Настройки сети

Раздел **Сеть и LDAP** позволяет установить параметры, используемые для подключения ViPNet SafeBoot к сети.

Для настройки сети выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите пункт **Сеть и LDAP**.
3. В открывшемся меню настроек сети выберите пункт **Сетевой интерфейс**.

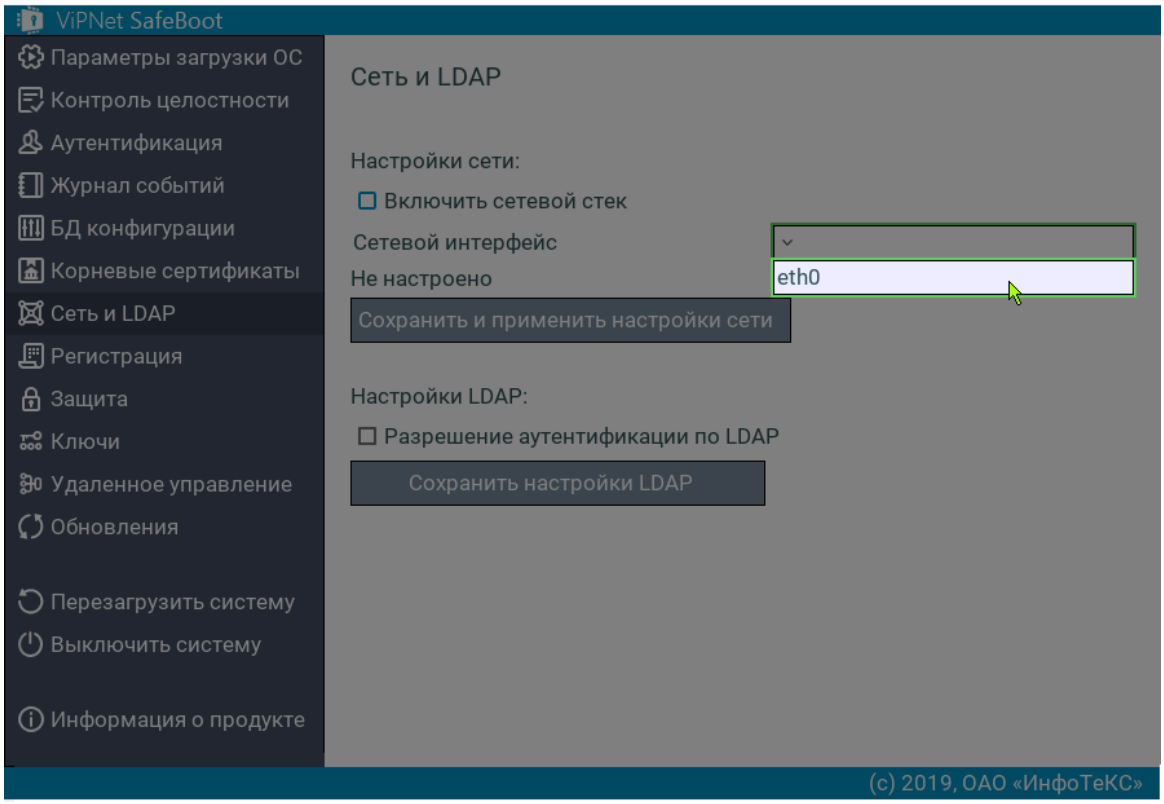


Рисунок 103. Выбор сетевого интерфейса в графическом режиме

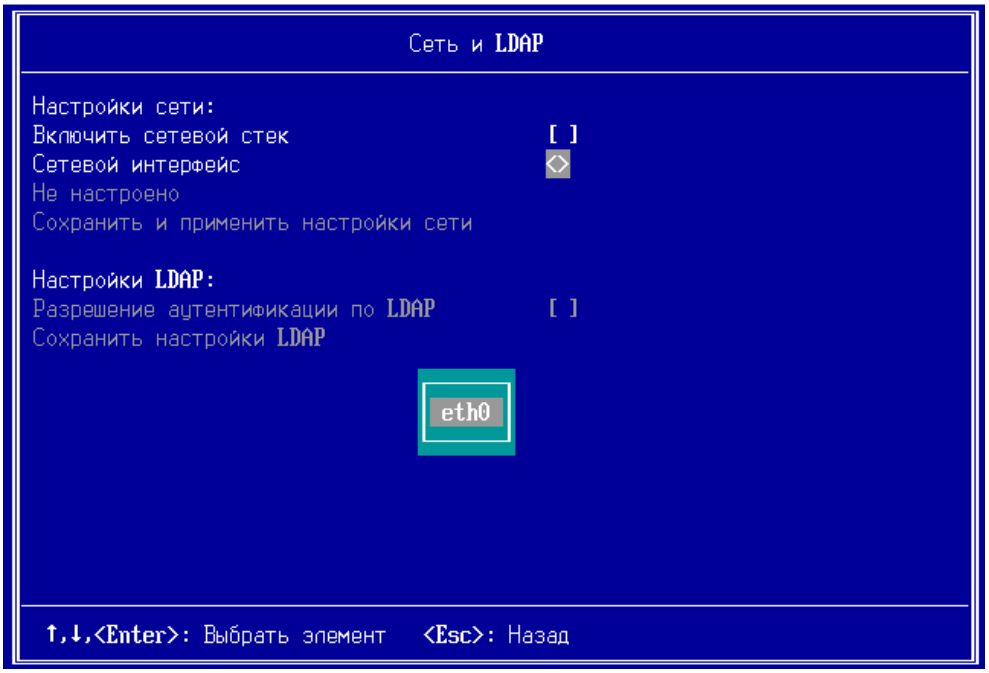


Рисунок 104. Выбор сетевого интерфейса в текстовом режиме

4 Выберите **Получение IP**: динамически (автоматическое назначение IP-адресов с использованием DHCP) или статически (ручной способ назначения IP-адресов).

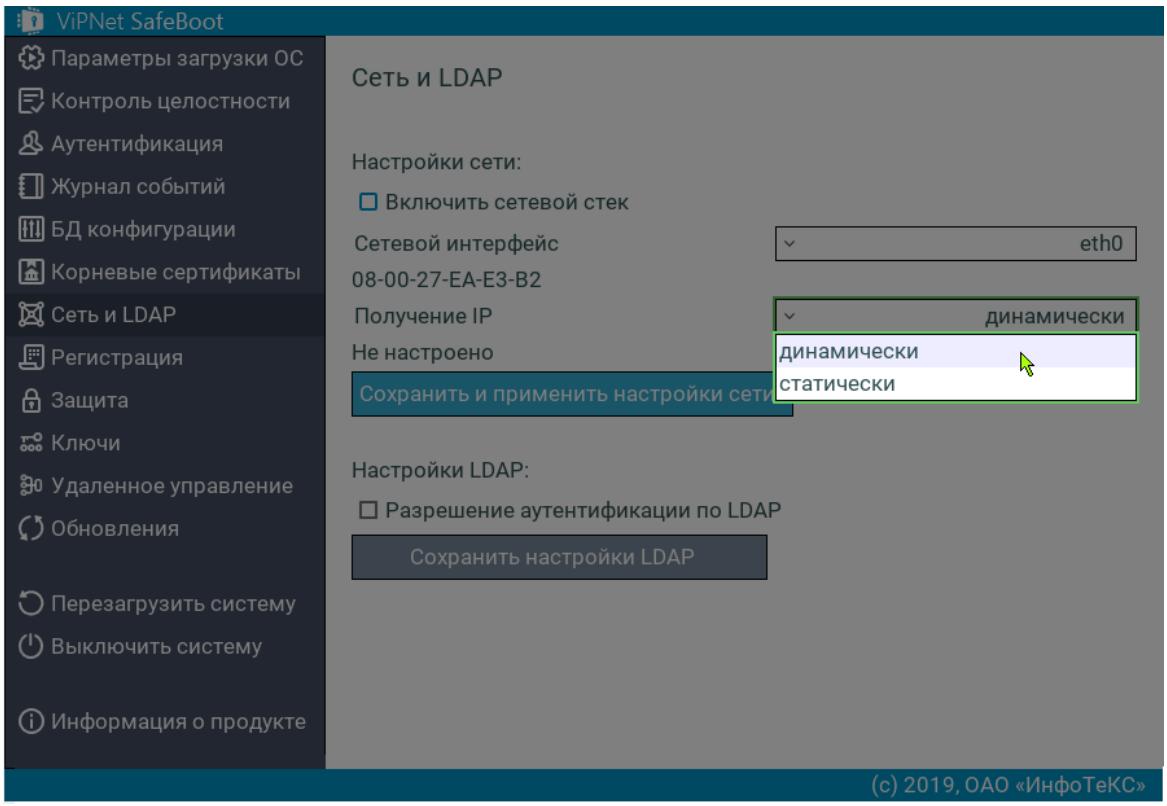


Рисунок 105. Выбор получения IP

5 Сохраните настройки сети, выбрав **Сохранить и применить настройки сети**.

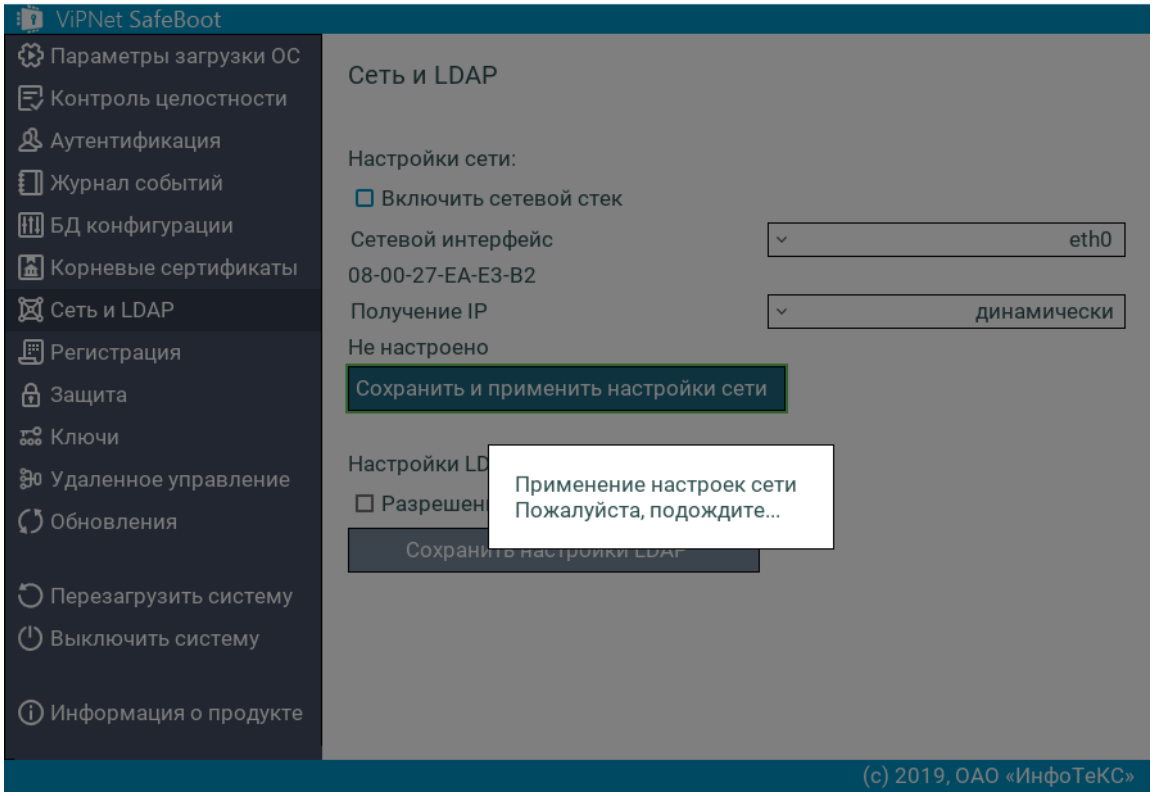
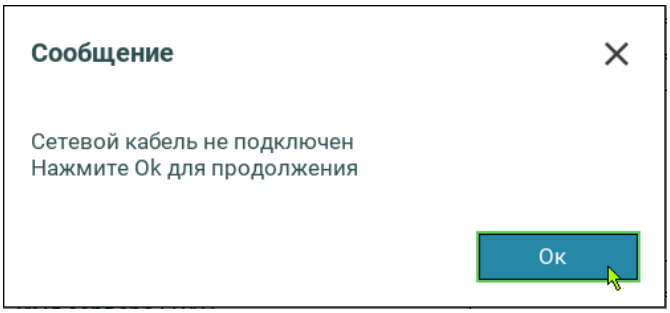


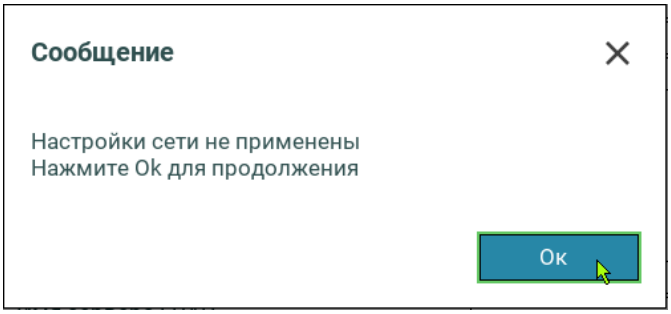
Рисунок 106. Применение заданных настроек сети

5.1 Если во время применения настроек сети сетевой кабель был не подключен, то появится следующее сообщение:



Нажмите **Ok** для продолжения, проверьте подключение сетевого кабеля и повторите команду **Сохранить и применить настройки сети**.

5.2 В случае ошибки, при конфигурации сетевого адаптера, появится следующее сообщение:



Нажмите любую клавишу для продолжения и установите настройки сети вручную, выбрав в поле **Получение IP** способ **<статически>**.

6 Дождитесь появления сообщения о сохранении настроек сети и нажмите **Ок** или **Enter** для продолжения.

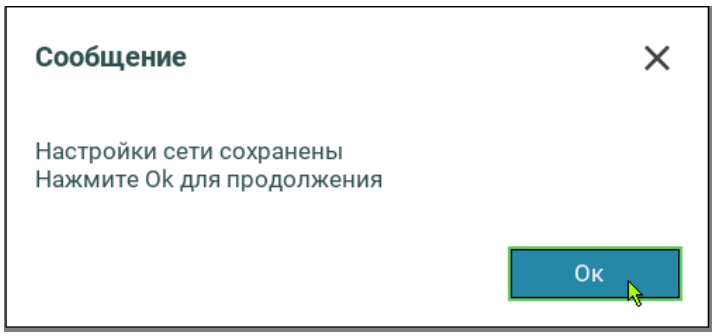


Рисунок 107. Успешное завершение сохранения настроек сети

Настройки подключения к LDAP серверу

Для настройки подключения к LDAP серверу выполните следующие действия:

1 Установите флажок в поле **Разрешение аутентификации по LDAP** и введите **IP сервера LDAP**.

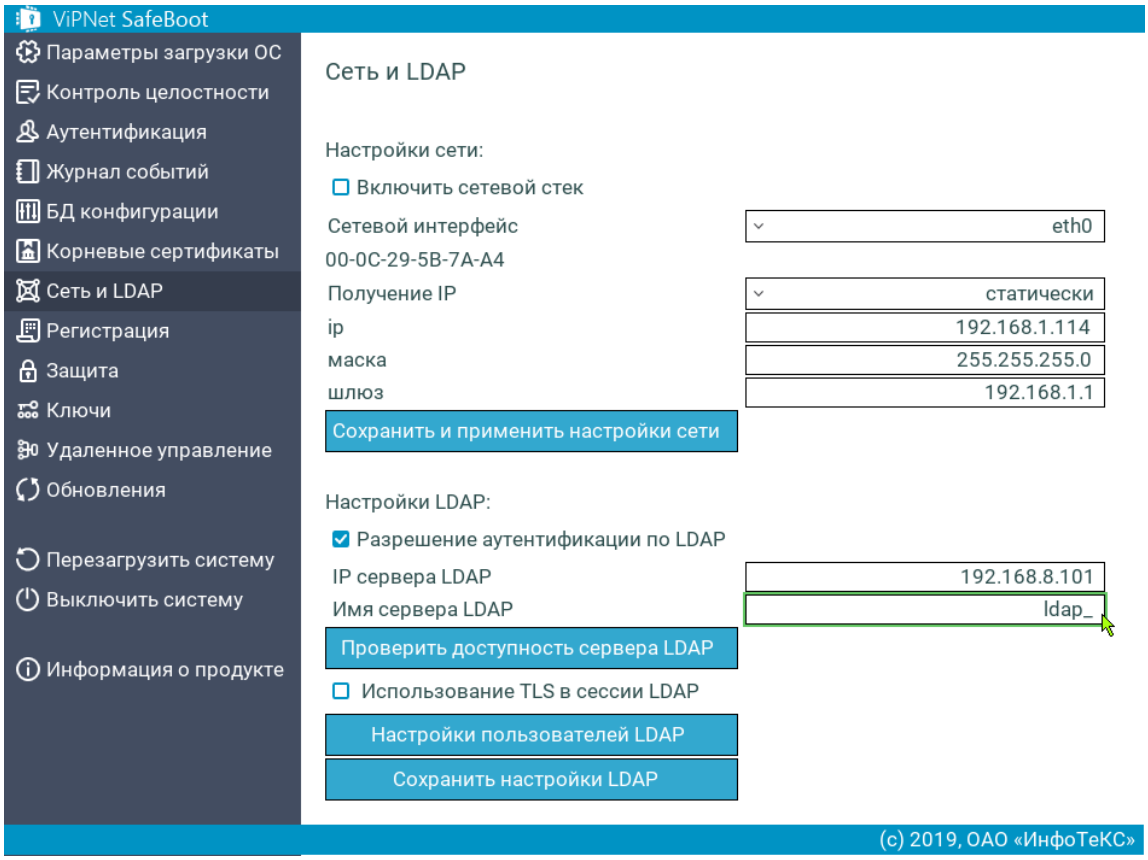


Рисунок 108. Установка настроек LDAP сервера

2 Задайте **Имя сервера LDAP**, которое впоследствии будет использоваться пользователем для аутентификации.

3 При необходимости проверки соединения с сервером LDAP, выберите **Проверить доступность сервера LDAP**.

После успешной проверки соединения с сервером LDAP появится соответствующее сообщение. Если соединение установить не удалось, то необходимо проверить настройки LDAP и повторить попытку проверки доступности сервера LDAP.

4 В настройках по умолчанию, установлен TLS для защиты соединения – флажок в поле **Использование TLS в сессии LDAP**. Для использования TLS предварительно необходимо установить корневой сертификат (см. Установка корневого сертификата на стр. 150).

Корневой сертификат LDAP должен быть импортирован только в DER кодировке.

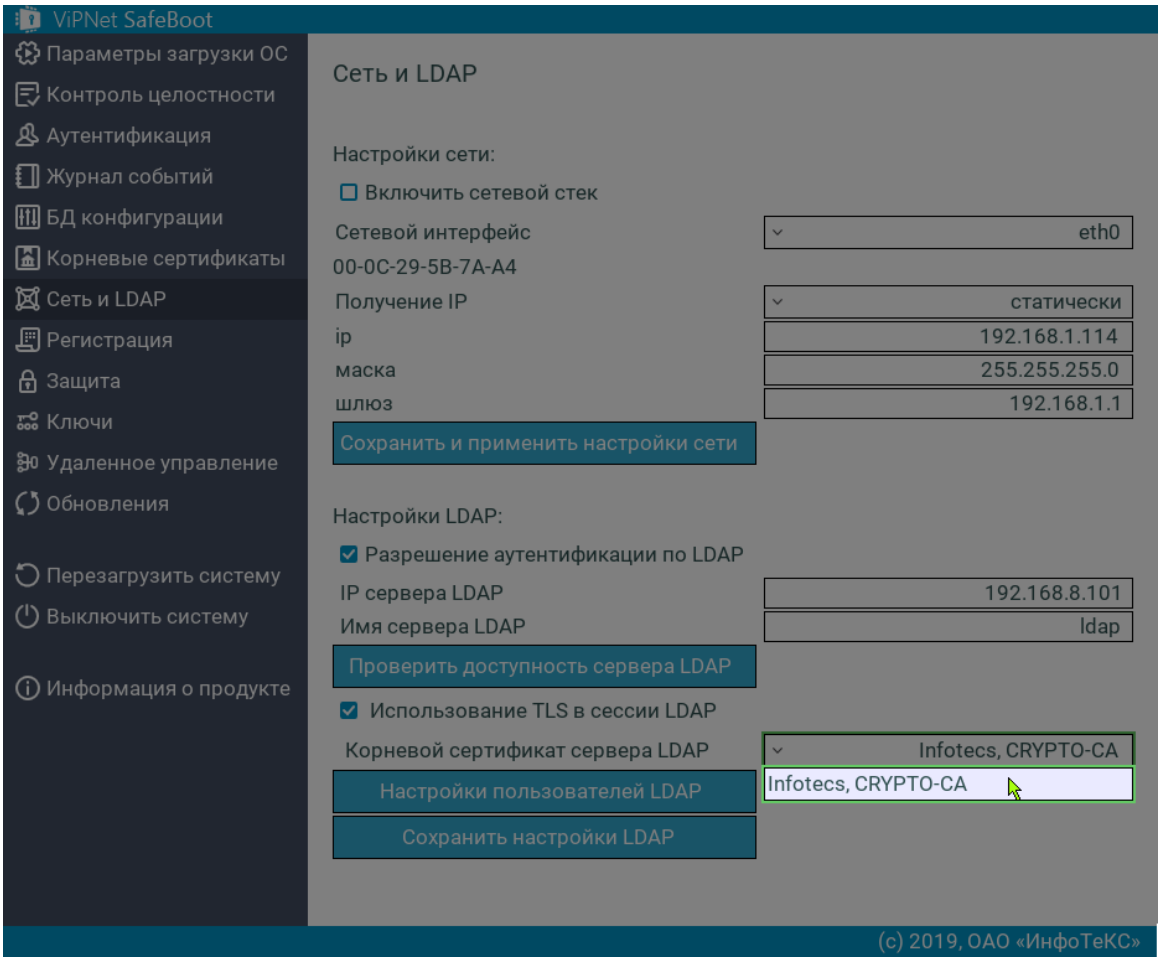


Рисунок 109. Выбор корневого сертификата при использовании TLS в сессии LDAP

5 Выберите **Настройки пользователей LDAP**. В открывшемся меню задайте суффикс DN, адресующий место хранения учетных записей пользователей.

Рисунок 110. Настройка пользователей LDAP

Примечание. Поле **Суффикс DN пользователей** используется для более удобного ввода имени пользователя при аутентификации по LDAP.

Если не указывать значение в данном поле, то при аутентификации по LDAP необходимо будет вводить полный DN пользователя, например: <ldap_server_name>/CN=User,CN=Users,CN=SafeBoot

---

Если для полного DN пользователя “CN=User,CN=Users,CN=SafeBoot” в качестве “Суффикса DN пользователей” указать значение “CN=Users,CN=SafeBoot”, тогда при вводе имени пользователя нужно будет вводить:

<ldap_server_name>/User

6 Импортируйте список разрешенных пользователей LDAP, выбрав **Импортировать список**. Список должен быть заранее подготовлен на USB носителе при помощи текстового редактора. Формат списка — текстовый файл в кодировке utf-8/cp1251, каждая строка которого представляет собой полный DN разрешенного пользователя (подробности формата DN можно найти в RFC 2253).

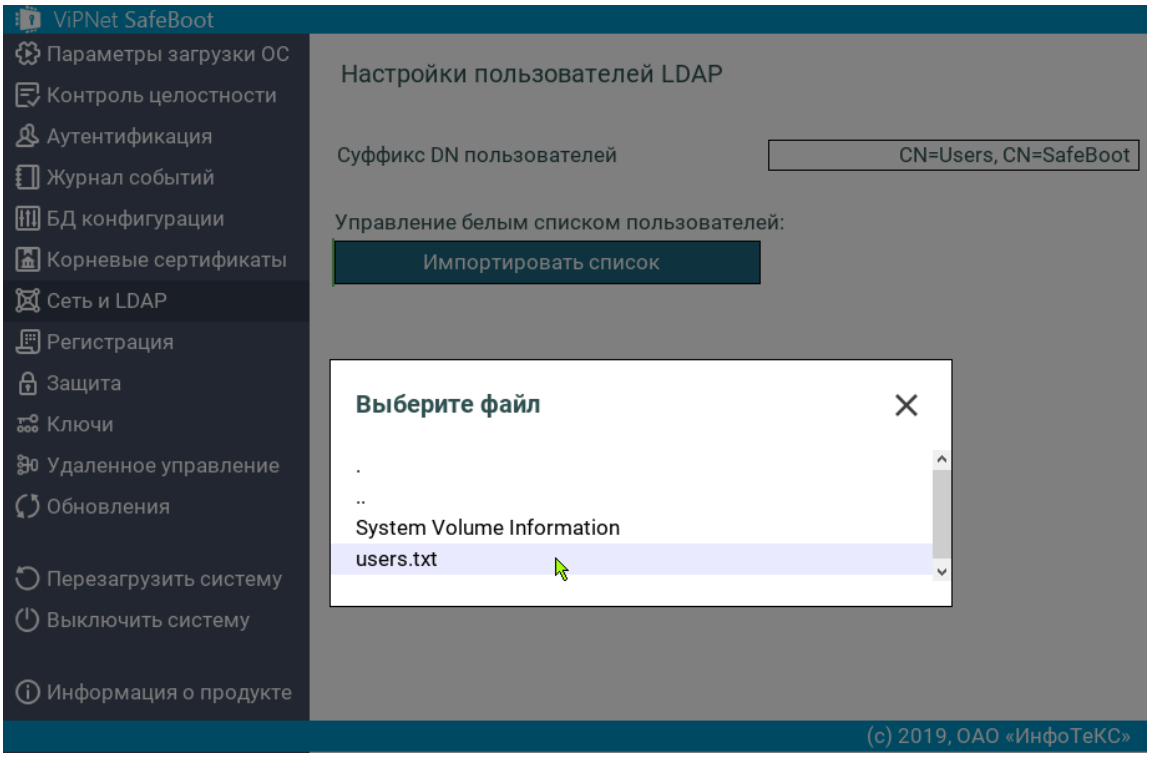


Рисунок 111. Выбор файла со списком разрешенных пользователей LDAP

6.1 После импортирования списка пользователей, в меню управления белым списком пользователя появляются элементы **Просмотреть список** и **Удалить список**.

6.2 Для просмотра списка пользователей выберите **Просмотреть список**.

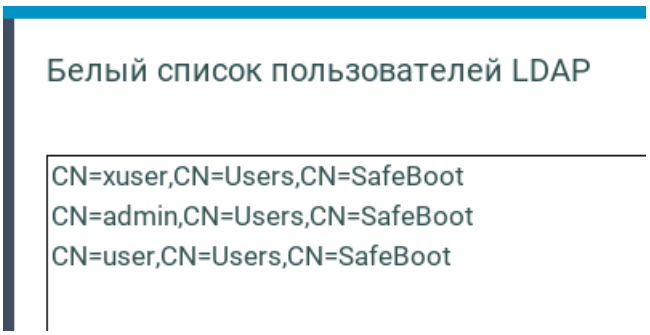


Рисунок 112. Просмотр списка пользователей LDAP

6.3 Для удаления списка пользователей LDAP выберите **Удалить список.**

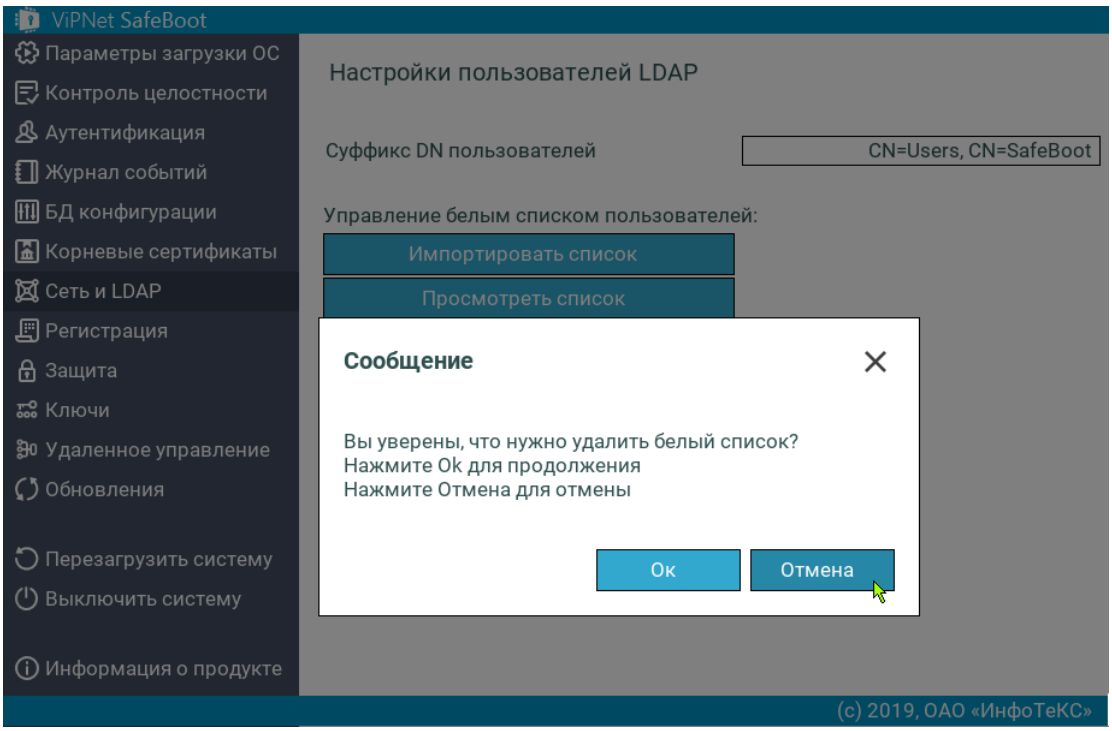
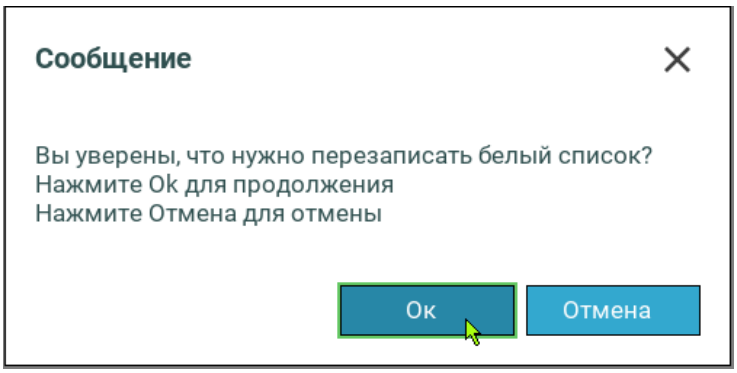


Рисунок 113. Удаление списка пользователей LDAP

6.4 При повторном выборе элемента меню **Импортировать список**, появится следующее сообщение:



В случае продолжения новый импортированный список заменит текущий.

7 Выйдите из меню настроек пользователей LDAP, нажав **Esc**.

8 Выберите **Сохранить настройки LDAP**.

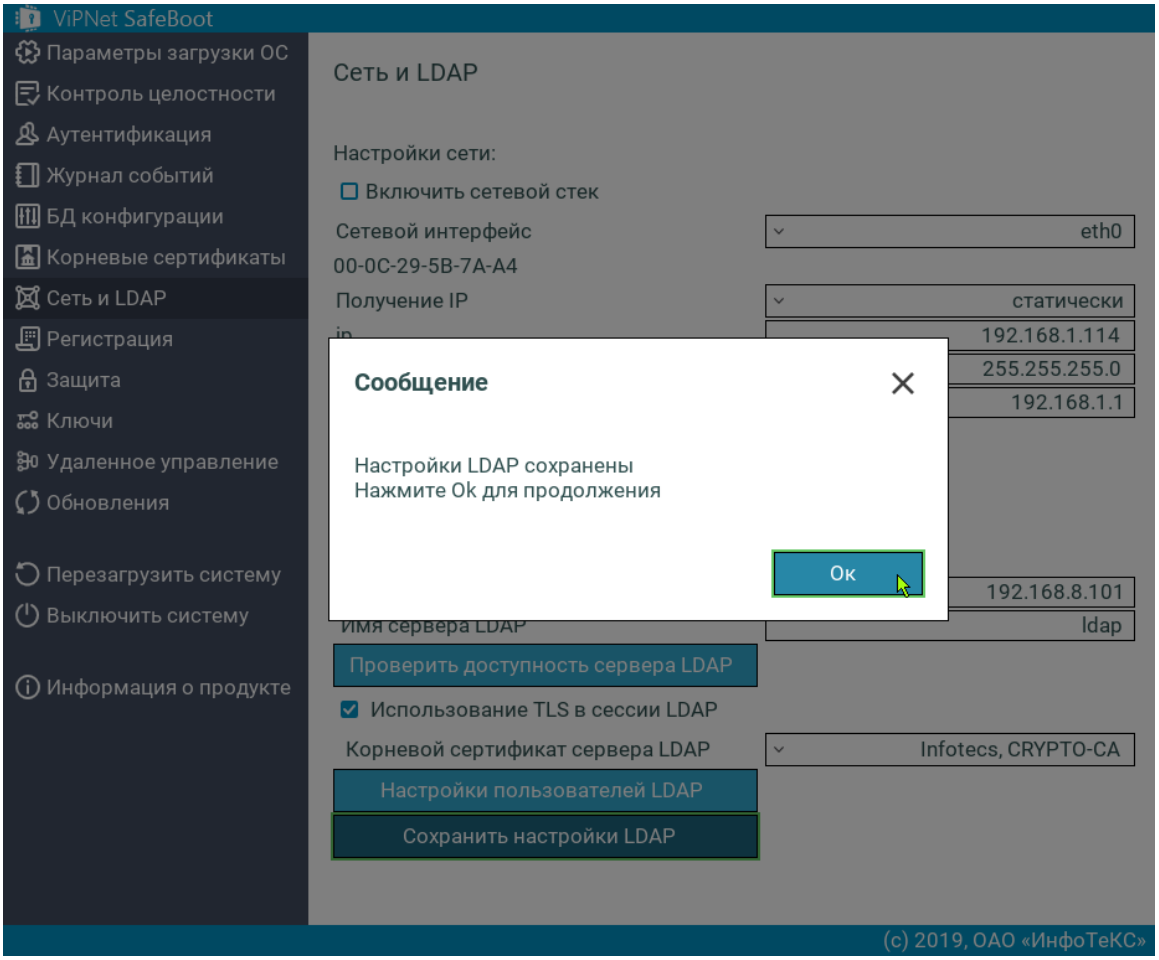


Рисунок 114. Сохранение настроек LDAP

9 Нажмите **Ok** или **Enter**.

10

Управление журналом событий

Настройки журнала событий

Настройки журнала событий включают:

- Режим ведения журнала:
  - внутренний, циклический;
  - внутренний, экспортируемый;
  - внешний (на диске).
- Уровень регистрации событий:
  - подробный;
  - основной.

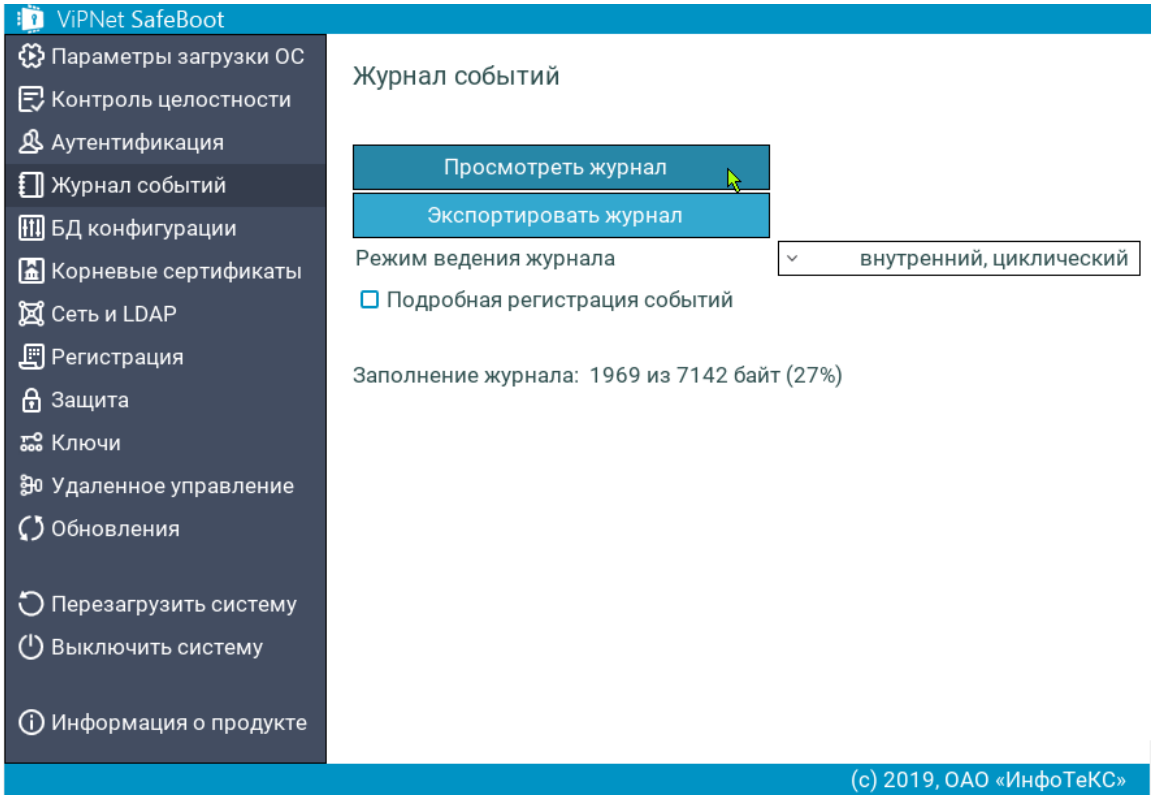


Рисунок 115. Меню управления настройками журнала событий

Режим ведения журнала «внутренний, циклический»

В режиме ведения журнала «**внутренний, циклический**»:

- Журнал хранится в NVRAM-памяти BIOS.

- События регистрируются циклически, то есть при переполнении журнала, новые записи событий записываются на место самых старых записей.
- При переключении режима на «**внешний (на диске)**», рекомендуется экспортировать журнал на USB диск.

Примечание. При переключении на режим «**внешний (на диске)**», появится уведомление о необходимости экспортировать журнал. Для продолжения нужно нажать **Enter**, для отмены — **Esc**.

Перед экспортом журнала подключите USB диск и нажмите **Enter**. В результате:

- текущий журнал будет выгружен из NVRAM на USB диск;
- режим ведения журнала будет переведен на «**внешний (на диске)**»;
- на локальном диске в каталоге **efi\infotecs\log** будет создан новый журнал, и все записи будут вестись в него.

В случае отказа от экспорта:

- текущий журнал сохраняется в NVRAM;
- режим ведения журнала будет переведен на «**внешний (на диске)**»;
- на локальном диске в каталоге **efi\infotecs\log** будет создан новый журнал, и все записи будут вестись в него.

Режим ведения журнала «внутренний, экспортируемый»

В режиме ведения журнала «**внутренний, экспортируемый**»:

- Журнал хранится в NVRAM-памяти BIOS.
- В случае если журнал заполнен более чем на 85%, при входе в систему выдается соответствующее предупреждение.
- При переполнении журнала вход в систему пользователей блокируется до тех пор, пока администратор не экспортирует записи журнала.
- При переключении режима на «**внешний (на диске)**» рекомендуется экспортировать журнал на USB-носитель (см. примечание выше).

Режим ведения журнала «внешний (на диске)»

В режиме ведения журнала «**внешний (на диске)**»:

- Журнал хранится на диске (EFI System Partition) в каталоге EFI\Infotecs\Log\.
- При переключении режима на другой, будет продолжен журнал, сохранившийся в NVRAM (в случае отказа от его экспорта).

Изменение настроек журнала событий

Чтобы изменить настройки журнала событий, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Журнал событий**.
3. Для изменения режима записи событий выберите **Режим ведения журнала**.

   В открывшемся списке выберите нужный режим.
4. Для изменения уровня регистрации событий установите или снимите флажок **Подробная регистрация событий**.

Просмотр журнала событий

Отображение записей журнала событий зависит от выбранного режима записи событий. В случае когда журнал событий ведется в режимах «**внутренний, циклический**» и «**внутренний, экспортируемый**», то при просмотре отображаются записи, хранимые в NVRAM. В случае если журнал ведется на диске, то отображаются записи журнала событий, хранимые на диске.

Чтобы просмотреть записи журнала событий, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. В меню режима настроек выберите **Журнал событий**.
3. В открывшемся окне выберите **Просмотреть журнал**.

Цвет шрифта при отображении каждой записи регистрируемых событий соответствуют следующим уровням:

- Красный — ошибка (error).
- Белый — обычная информация (info/audit).
- Желтый — детализированная информация (details).

Записи типа «детализированная информация» предназначены для передачи разработчикам в целях диагностики возможных проблем.

Экспорт записей журнала событий

Экспорт записей журнала событий осуществляется на первый найденный USB-носитель в фиксированный файл **itsblog.txt** (в корень раздела), также на диске появляется файл с подписью **itsblog.txt.sig**.

Чтобы экспортировать записи журнала событий, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 51).
2. Подключите USB-носитель.
3. В меню режима настроек выберите **Журнал событий**.
4. В открывшемся окне выберите **Экспортировать журнал**.

Примечания.

1. В режиме записи событий, когда журнал при переполнении переносится на диск, экспортирование журнала событий может выполнить только Администратор или Аудитор.
2. Если переполнение журнала происходит до процедуры аутентификации или в процессе работы пользователя (не Администратора и не Аудитора) – журнал блокируется, выдается сообщение о блокировке журнала на экран и во внутренний журнал, дальнейшие записи во внутренний журнал игнорируются, аутентификация Пользователей блокируется.
3. Если переполнение журнала происходит после аутентификации Пользователя – система блокируется. В данной ситуации журнал должен экспортироваться Администратором или Аудитором.

A

События, регистрируемые в ViPNet SafeBoot

№ п/п	Тип события	Текст сообщения
1	**детальный**	Старт ПМДЗ
2	**информация**	Система перезагружена
3	**информация**	Система выключена
4	**информация**	Вход в режим настроек BIOS заблокирован
5	**ошибка**	Неверное системное время
6	**информация**	Измененное системное время подтверждено Администратором
7	**ошибка**	Критическая ошибка
8	**информация**	Первичная БД конфигурации импортирована
9	**информация**	Режим ограниченного функционирования активирован
10	**информация**	Режим ограниченного функционирования заблокирован
11	**детальный**	Модуль верифицирован
12	**детальный**	Модуль выгружен
13	**ошибка**	Ошибка выгрузки модуля
14	**детальный**	Модуль загружен с диска
15	**ошибка**	Ошибка загрузки модуля с диска
16	**ошибка**	Ошибка формата модуля

№ п/п	Тип события	Текст сообщения
17	**ошибка**	Неверная подпись модуля
18	**детальный**	Модуль загружен из BIOS
19	**ошибка**	Ошибка инициализации модуля
20	**ошибка**	Рабочая директория не найдена
21	**информация**	Рабочая директория инициализирована
22	**информация**	Автоматический вход в систему
23	**информация**	Система выключена: превышено количество допустимых неверных попыток аутентификации
24	**информация**	Превышено количество допустимых неверных попыток аутентификации: загрузка ОС заблокирована
25	**информация**	Счетчик допустимых неверных попыток аутентификации сброшен: загрузка ОС разрешена
26	**ошибка**	Пользователь не существует
27	**ошибка**	Попытка аутентификации в неинициализированной/заблокированной системе (разрешен вход только Администратору)
28	**ошибка**	Неверный пароль пользователя
29	**ошибка**	Пароль пользователя заблокирован
30	**ошибка**	Срок действия пароля пользователя истек
31	**ошибка**	Неверный PIN эл.идентификатора пользователя
32	**ошибка**	Эл.идентификатор пользователя не подключен
33	**ошибка**	Сертификат пользователя не найден
34	**ошибка**	Ошибка протокола аутентификации на эл.идентификаторе
35	**ошибка**	Корневой сертификат не установлен
36	**ошибка**	Ошибка верификации сертификата пользователя
37	**ошибка**	Неверное имя или пароль пользователя LDAP
38	**ошибка**	Пользователь LDAP не включен в белый список
39	**информация**	Администратор аутентифицирован
40	**информация**	Аудитор аутентифицирован
41	**информация**	Пользователь аутентифицирован
42	**информация**	Пользователь LDAP аутентифицирован
43	**информация**	Пользователь LDAP аутентифицирован (из кэша)
44	**ошибка**	Попытка аутентификации заблокированным пользователем
45	**ошибка**	PIN эл.идентификатора пользователя заблокирован

№ п/п	Тип события	Текст сообщения
46	детальный	Нарушение БД конфигурации
47	детальный	Неподдерживаемая версия БД конфигурации
48	информация	Изменен режим ведения БД конфигурации
49	ошибка	БД конфигурации пересоздана
50	ошибка	БД конфигурации переполнена
51	информация	БД конфигурации устаревшей версии сконвертирована
52	информация	Журнал заполнен и заблокирован
53	ошибка	Журнал пересоздан
54	информация	Журнал экспортирован
55	ошибка	Ошибка при экспорте журнала
56	информация	Параметры загрузки должны быть настроены
57	информация	Режим загрузки ОС изменен
58	информация	Изменено устройство загрузки (legacy)
59	информация	Раздел ESP изменен
60	информация	EFI-загрузчик изменен
61	информация	Использование параметров загрузки BIOS включено
62	информация	Использование параметров загрузки BIOS выключено
63	информация	Раздел поставлен на КЦ
64	информация	Раздел снят с КЦ
65	информация	Элемент поставлен на КЦ
66	информация	Элемент снят с КЦ
67	информация	Компонент поставлен на КЦ
68	информация	Компонент снят с КЦ
69	информация	Изменен диск для контроля загрузочных секторов
70	информация	Контроль журнала транзакций ФС включен
71	информация	Контроль журнала транзакций ФС выключен
72	информация	Режим обучения КЦ включен
73	информация	Режим обучения КЦ выключен
74	информация	Эталоны КЦ компонентов системы перерасчитаны
75	информация	Эталоны КЦ компонента импортированы
76	детальный	Неверный формат подписи

№ п/п	Тип события	Текст сообщения
77	**детальный**	Неверная подпись
78	**информация**	Эталоны КЦ компонента сгенерированы автоматически
79	**ошибка**	Ошибка обработки компонентов загрузки ОС
80	**ошибка**	Ошибка при импорте эталонов КЦ
81	**детальный**	Целостность элемента заверена
82	**ошибка**	Целостность элемента нарушена
83	**детальный**	Элемент не найден
84	**ошибка**	Элемент снят с КЦ (режим обучения)
85	**ошибка**	Незарегистрированный элемент
86	**детальный**	Целостность компонента заверена
87	**детальный**	Целостность компонента нарушена
88	**ошибка**	Эталоны КЦ компонента не найдены
89	**ошибка**	Ошибка при верификации подписи эталонов компонента
90	**информация**	Целостность компонентов системы заверена
91	**ошибка**	Незарегистрированный элемент снят с КЦ (режим обучения)
92	**ошибка**	Эталоны КЦ компонента не соответствуют БД конфигурации
93	**информация**	Эталоны КЦ компонента перерасчитаны
94	**детальный**	Журнал транзакций ФС пуст
95	**информация**	Журнал транзакций ФС не пуст
96	**информация**	Добавлен пользователь
97	**информация**	Пользователь удален
98	**информация**	Изменен тип аутентификации пользователя
99	**информация**	Пароль пользователя изменен
100	**информация**	Настройки пароля пользователя изменены
101	**информация**	Пароль пользователя изменен Администратором
102	**информация**	Эл.идентификатор пользователя инициализирован
103	**информация**	Изменен PIN эл.идентификатора пользователя
104	**информация**	Изменен эл.идентификатор пользователя
105	**информация**	Изменен сертификат пользователя
106	**информация**	Пользователь заблокирован

№ п/п	Тип события	Текст сообщения
107	**информация**	Пользователь разблокирован
108	**информация**	Изменен режим журналирования
109	**информация**	Изменен уровень журналирования
110	**информация**	Корневой сертификат установлен
111	**информация**	Корневой сертификат удален
112	**информация**	CRL установлен/обновлен
113	**информация**	CRL удален
114	**ошибка**	Корневой сертификат уже установлен
115	**ошибка**	Корневой сертификат просрочен
116	**ошибка**	CRL просрочен
117	**ошибка**	Установлено максимальное количество корневых сертификатов
118	**ошибка**	Сертификат не является корневым сертификатом
119	**ошибка**	CRL не соответствует корневому сертификату
120	**информация**	Корневой сертификат экспортирован
121	**ошибка**	Ошибка при экспорте корневого сертификата
122	**информация**	CRL экспортирован
123	**ошибка**	Ошибка при экспорте CRL
124	**информация**	Вход в режим настроек BIOS разрешен
125	**информация**	Вход в режим настроек BIOS запрещен
126	**информация**	Защита BIOS включена
127	**информация**	Защита BIOS выключена
128	**информация**	Защита BIOS после S3 включена
129	**информация**	Защита BIOS после S3 выключена
130	**информация**	БД конфигурации экспортирована
131	**ошибка**	Ошибка при экспорте БД конфигурации
132	**информация**	БД конфигурации импортирована
133	**ошибка**	Ошибка при импорте БД конфигурации
134	**информация**	Ограничение сессии аутентификации включено
135	**информация**	Ограничение сессии аутентификации выключено
136	**информация**	Время сессии аутентификации изменено
137	**информация**	Автоматический вход в систему разрешен

№ п/п	Тип события	Текст сообщения
138	**информация**	Автоматический вход в систему запрещен
139	**информация**	Время до автоматического входа в систему изменено
140	**информация**	Защита от чтения BIOS включена
141	**информация**	Защита от чтения BIOS выключена
142	**информация**	Эмуляция NVRAM включена
143	**информация**	Эмуляция NVRAM выключена
144	**информация**	Контроль программных SMI включен
145	**информация**	Контроль программных SMI выключен
146	**детальный**	Информация о защите BIOS
147	**детальный**	Информация о защите BIOS после S3
148	**детальный**	Ошибка при работе с устройствами загрузки (legacy)
149	**ошибка**	EFI-загрузчик возвратил управление
150	**ошибка**	Найдено несколько разделов ESP
151	**ошибка**	Shell из пакета обновления не найден
152	**ошибка**	Ошибка верификации пакета обновления
153	**ошибка**	Неверная версия пакета обновления
154	**информация**	Установка обновления
155	**информация**	Обновление установлено
156	**информация**	Ошибка при установке обновления
157	**ошибка**	Пакет обновления не найден
158	**ошибка**	Найдено несколько пакетов обновлений
159	**информация**	Настройки сети изменились
160	**информация**	Настройки LDAP изменились
161	**детальный**	Протокол конфигурирования сети:
162	**детальный**	Статистика ping:
163	**ошибка**	Включение сетевого стека не поддерживается
164	**ошибка**	Сервер LDAP недоступен
165	**ошибка**	Корневой сертификат сервера LDAP не установлен
166	**информация**	Сетевой стек включен
167	**информация**	Сетевой стек выключен
168	**информация**	Белый список пользователей LDAP импортирован

№ п/п	Тип события	Текст сообщения
169	**информация**	Белый список пользователей LDAP удален
170	**детальный**	Ошибка данных пароля на эл.идентификаторе
171	**ошибка**	Пароль на эл.идентификаторе не найден
172	**ошибка**	Неверный пароль на эл.идентификаторе
173	**ошибка**	Неподдерживаемый формат пароля на эл.идентификаторе
174	**ошибка**	Неверные данные диска восстановления
175	**информация**	Диск восстановления подготовлен
176	**информация**	Диск восстановления импортирован
177	**информация**	Первичный Администратор восстановлен
178	**ошибка**	Неверные данные восстановления
179	**информация**	Свободное место в NVRAM распределено
180	**ошибка**	Продукт выключен
181	**информация**	Продукт работает в демо-режиме
182	**ошибка**	Демо-период использования продукта завершен
183	**информация**	Серийный номер изменен
184	**информация**	Запрос на регистрацию создан
185	**информация**	Код регистрации изменен
186	**детальный**	Идентификатор устройства сгенерирован
187	**ошибка**	Неверный код регистрации
188	**ошибка**	Код регистрации просрочен
189	**ошибка**	Неверный формат серийного номера
190	**ошибка**	Несовместимый серийный номер
191	**ошибка**	Серийный номер не найден на диске
192	**ошибка**	Код регистрации не найден на диске
193	**ошибка**	Код регистрации не установлен
194	**информация**	Продукт переведен в состояние 'не зарегистрирован'
195	**информация**	Удаленное управление включено
196	**информация**	Удаленное управление выключено
197	**ошибка**	Ошибка верификации запроса управления
198	**информация**	БД конфигурации импортирована в режиме управления

№ п/п	Тип события	Текст сообщения
199	**информация**	Эталоны импортированы в режиме управления
200	**детальный**	Журнал и БД конфигурации подготовлены для агента управления
201	**информация**	Корневые сертификаты и CRL импортированы в режиме управления
202	**ошибка**	Ошибка обработки запроса управления
203	**информация**	Сертификат КЦ данных изменен
204	**информация**	Сертификат КЦ данных сброшен
205	**информация**	Сертификат КЦ запросов управления изменен
206	**информация**	Сертификат КЦ запросов управления сброшен
207	**информация**	Ключ защиты данных изменен
208	**информация**	Ключ защиты данных сброшен
209	**информация**	Программное SMI заблокировано

B

Возможные неполадки и способы их устранения

Система заблокирована

Блокированию системы может привести одна из следующих причин:

- Нарушена целостность операционной системы или объектов, поставленных на контроль.
- Нарушена целостность состава аппаратных средств, поставленных на контроль.
- Журнал событий переполнен.

Нарушена целостность операционной системы или объектов, поставленных на контроль

Возможная причина: Обнаружено повреждение или несанкционированная замена поставленных на контроль объектов.

Решение: Необходимо устранить нарушения в поставленных на контроль объектах.

В случае если изменения были правомерны, следует снять и вновь поставить компоненты на контроль (см. Контроль целостности на стр. 86).

Нарушена целостность состава аппаратных средств, поставленных на контроль

Возможная причина: К компьютеру было подключено или отключено PCI-устройство при включенной в меню настройки ViPNet SafeBoot опции контроля аппаратных средств.

Решение: Необходимо проверить состав подключенных аппаратных средств, отключить неправомерно подключенное устройство или подключить необходимое.

В случае если PCI-устройство было подключено или отключено правомерно, необходимо пересчитать контрольные суммы или отключить опцию **Контроль конфиг. пространства PCI** (см. Контроль целостности на стр. 86).

Журнал событий переполнен

Возможная причина: В случае переполнения журнала событий загрузка операционной системы будет остановлена с сообщением о переполнении журнала.

Решение: Администратору или Аудитору необходимо экспортировать журнал событий или изменить режим ведения журнала на **«внутренний, циклический»** (см. Управление журналом событий на стр. 171).

Пользователь заблокирован

Основные причины блокировки пользователя:

- Превышено допустимое количество неудачных попыток аутентификации.
- Время действия пароля пользователя истекло.
- Сертификат пользователя просрочен или отозван.

Превышено допустимое количество неудачных попыток аутентификации

Возможная причина:

- Попытка несанкционированного доступа.
- Пользователь забыл свои учетные данные.

Решение: Администратору необходимо войти в меню управления учетными записями пользователей и изменить пароль или способ аутентификации заблокированного пользователя (см. Управление учетными записями пользователей на стр. 104).

Время действия пароля пользователя истекло

Возможная причина: В учетной записи пользователя установлена опция ограничения срока действия пароля.

Решение: При необходимости Администратору следует продлить срок действия пароля (см. Управление учетными записями пользователей на стр. 104).

Сертификат пользователя просрочен или отозван

Возможная причина: Срок действия сертификата на электронном идентификаторе истек, или сертификат попал в список отозванных.

Решение: Администратору следует проверить статус сертификата. При необходимости продлить срок действия сертификата.

Глоссарий

Администратор

Лицо, обладающее правом загрузки операционной системы, правом доступа в режим настройки ViPNet SafeBoot и отвечающее за настройку и обновление.

Аудитор

Лицо, обладающее правом загрузки операционной системы и ограниченным доступом в режиме настройки ViPNet SafeBoot (просмотр и экспорт записей журнала событий, смена собственного пароля).

Аутентификация

Процедура проверки подлинности предоставленных пользователем данных при идентификации.

Идентификация

Процедура проверки данных, предоставляемых пользователем, для определения его идентификатора и соответствующих прав в ViPNet SafeBoot.

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Отличительное имя (DN)

Distinguished Name (англ.) – отличительное имя. Каждая запись каталога LDAP, включая объекты пользователей, имеет уникальное отличительное имя, которое может быть представлено в текстовом виде. Подробности формата DN могут быть найдены в RFC 2253.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Спецсимвол

Любой печатный символ базовой таблицы ASCII (0-127), не являющийся цифрой и буквой латинского алфавита:

	!	"	#	$	%	&	'	(	)	*
+	`	-	.	/	:	;	<	=	>	?
@	[	\	]	^	_	′	{	|	}	~

Электронный идентификатор

Персональное устройство доступа к информационным ресурсам, предназначенное для безопасного хранения и использования паролей, цифровых сертификатов, ключей шифрования и электронной подписи.

LDAP

Облегченный протокол доступа к каталогам. Протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP.

SMI (System Management Interrupt)

Системное немаскируемое прерывание с наивысшим приоритетом в системе для ввода процессора в режим работы SMM.

SMM (System Management Mode)

Один из режимов работы процессора архитектуры x86 начиная с Intel 386SL. В этом режиме останавливается нормальная работа процессора (в том числе работа ОС и обработка всех других прерываний) и управление передается специальным программным обработчикам BIOS (обработчикам SMI), работающим с наивысшим приоритетом.