ViPNet SafeBoot

Руководство пользователя

infotecs

ФРКЕ.00180-02 34 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 приведены сведения о назначении программного комплекса «Программный модуль доверенной загрузки ViPNet SafeBoot» ФРКЕ.00180-01 (далее – ViPNet SafeBoot), условия и порядок работы, описание процедуры идентификации и аутентификации пользователя, а также перечень сообщений, выдаваемых пользователю в ходе работы с ViPNet SafeBoot, и описание действий, которые следует предпринять при появлении этих сообщений.

Для кого предназначен документ

Настоящее руководство предназначено для пользователей, на рабочих местах которых установлен программный комплекс ViPNet SafeBoot.

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.

Системные требования

Требования к компьютерам для установки ViPNet SafeBoot:

- Процессор — x86-совместимый с поддержкой режима x86-64 (AMD64/Intel64), частота от 500 МГц.
- Системная плата — определяется 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

Семейство процессоров	Примечание
Intel Kabylake	Kabylake ULT/ULX, Kabylake ULT/ULX, Kabylake DT/HALO, Kabylake DT/HALO
Intel Coffeelake	CoffeeLake H/S, CoffeeLake H/S, CoffeeLake H/S
Intel Cannonlake	CannonLake Ult/Ulx, 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

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. 11
Доверенная загрузка операционной системы. Обеспечение загрузки компонентов операционной системы только с определенных носителей, назначенных администратором, предоставление администратору возможности выбора режима загрузки ОС	Управление ViPNet SafeBoot на стр. 13
Контроль целостности. Обеспечение целостности собственного программного обеспечения, образа BIOS и других компонентов	Управление ViPNet SafeBoot на стр. 13
Управление учетными записями пользователей. Создание, редактирование и удаление учетных записей пользователей	Управление ViPNet SafeBoot на стр. 13
Управление настройками аутентификации. ViPNet SafeBoot позволяет задать настройки сессии аутентификации	Управление ViPNet SafeBoot на стр. 13
Удаленное управление. Предоставляет функции удаленного управления ПК и настройками ViPNet SafeBoot	Управление ViPNet SafeBoot на стр. 13
Управление сертификатами. Обеспечение загрузки корневых сертификатов и списка отзыва сертификатов	Управление ViPNet SafeBoot на стр. 13
Проверка и установка обновлений. Автоматический поиск файла обновления и установка обновлений посредством меню управления настройками	Управление ViPNet SafeBoot на стр. 13
Экспорт и импорт настроек ViPNet SafeBoot	Управление ViPNet SafeBoot на стр. 13
Ведение журнала событий. Регистрация всех значимых событий безопасности и действий пользователя.	Управление ViPNet SafeBoot на стр. 13

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.

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. 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 на стр. 19.

Внимание! Множественные ошибки при вводе PIN-кода могут привести к самоблокировке электронного идентификатора.

В этом случае требуется разблокировка средствами ПО поставляемого с электронным идентификатором.

Управление ViPNet SafeBoot

Управление ViPNet SafeBoot выполняется из режима настройки, доступ к которому имеет только пользователь с полномочиями администратора.

В режиме настройки ViPNet SafeBoot выполняются следующие функции:

- Управление параметрами загрузки операционной системы.
- Контроль целостности.
- Управление настройками аутентификации и учетными записями пользователей.
- Ведение и управление журналом событий.
- Экспорт и импорт настроек ViPNet SafeBoot.
- Управление сертификатами.
- Настройки сети и LDAP.
- Регистрация ViPNet SafeBoot.
- Проверка и установка обновлений.

Подробное описание работы в режиме настройки приведено в документе «Руководство администратора ViPNet SafeBoot».

Пользователю в режиме настройки ViPNet SafeBoot доступна только смена своего пароля.

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 режимах приведены на рисунках ниже.

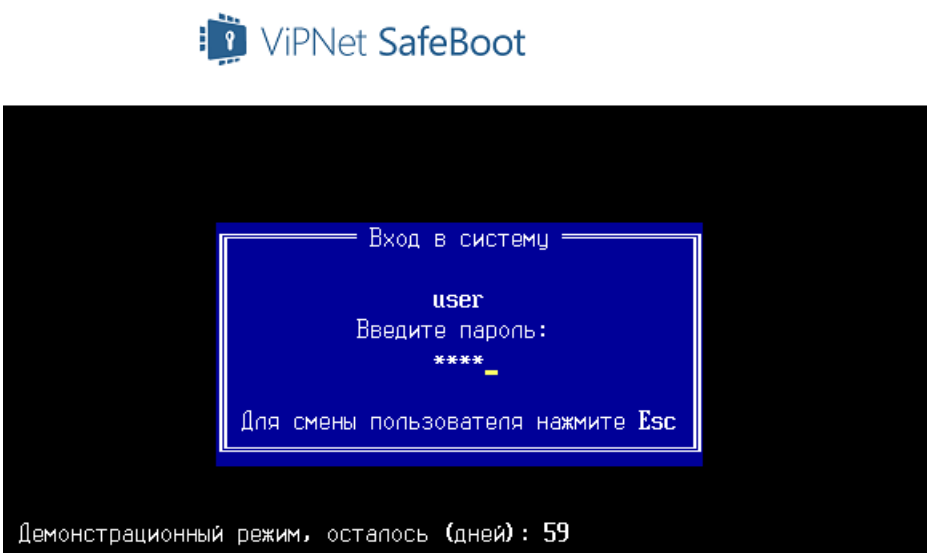


Рисунок 1. Аутентификация (текстовый режим пользовательского интерфейса)

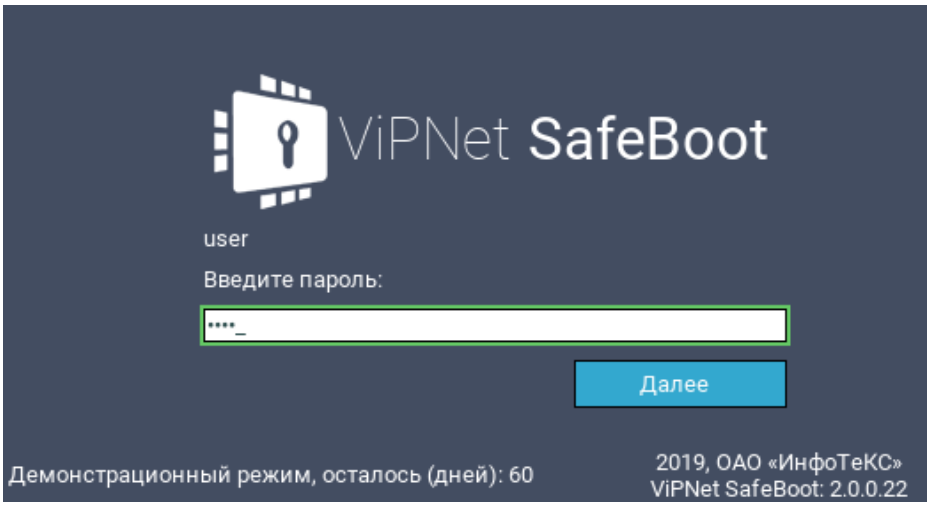


Рисунок 2. Аутентификация (графический режим пользовательского интерфейса)

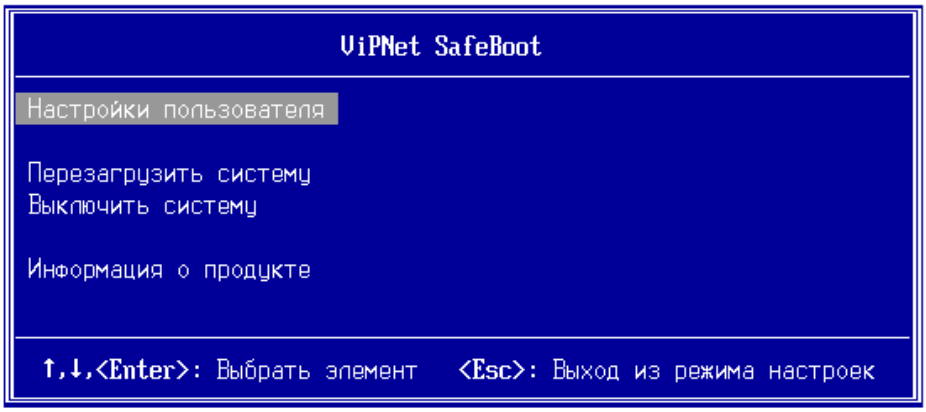


Рисунок 3. Меню режима настроек (текстовый режим пользовательского интерфейса)

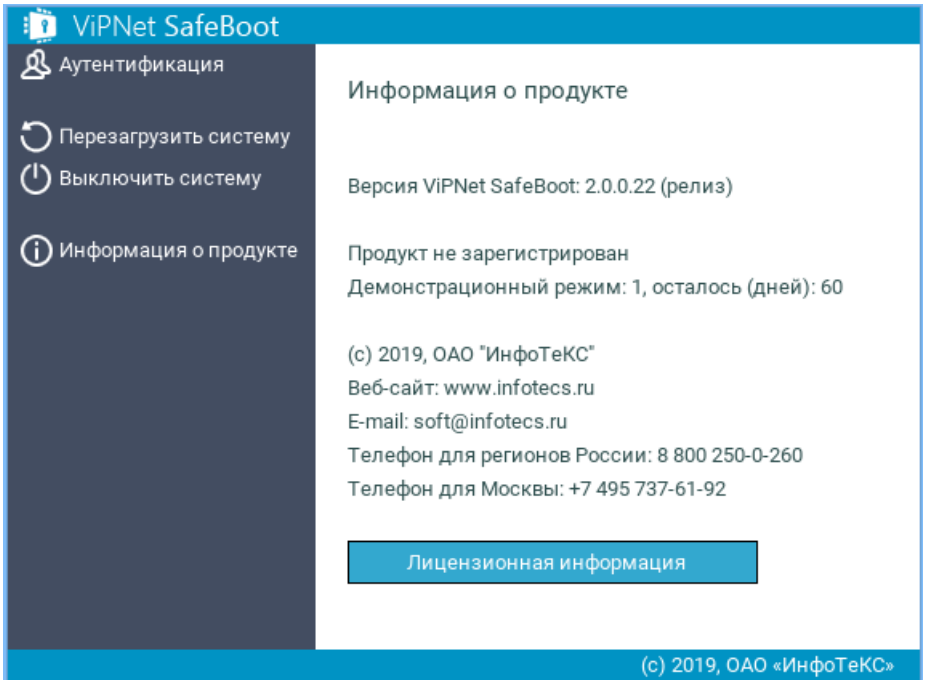


Рисунок 4. Меню режима настроек (графический режим пользовательского интерфейса)

2

Начало работы

Перед началом работы

Доступ к операционной системе получают только зарегистрированные в ViPNet SafeBoot пользователи.

Перед началом работы пользователю необходимо получить от системного администратора данные для аутентификации (учетные данные):

- Имя пользователя (логин).
- Пароль и/или электронный идентификатор и PIN-код.

Совет. Необходимо запомнить свои учетные данные или сохранить в недоступном для других людей месте.

В случае появления ошибок необходимо немедленно сообщить об этом системному администратору.

Запуск и завершение работы

Запуск ViPNet SafeBoot осуществляется автоматически при включении компьютера, на котором он установлен.

До начала загрузки операционной системы или входа в режим настройки ViPNet SafeBoot для смены пароля необходимо выполнить процедуру идентификации и аутентификации (см. Процедура идентификации и аутентификации на стр. 19).

Завершение работы ViPNet SafeBoot осуществляется при запуске операционной системы.

3

Процедура идентификации и аутентификации

Аутентификация по паролю

Для выполнения аутентификации по паролю, выполните следующие действия:

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

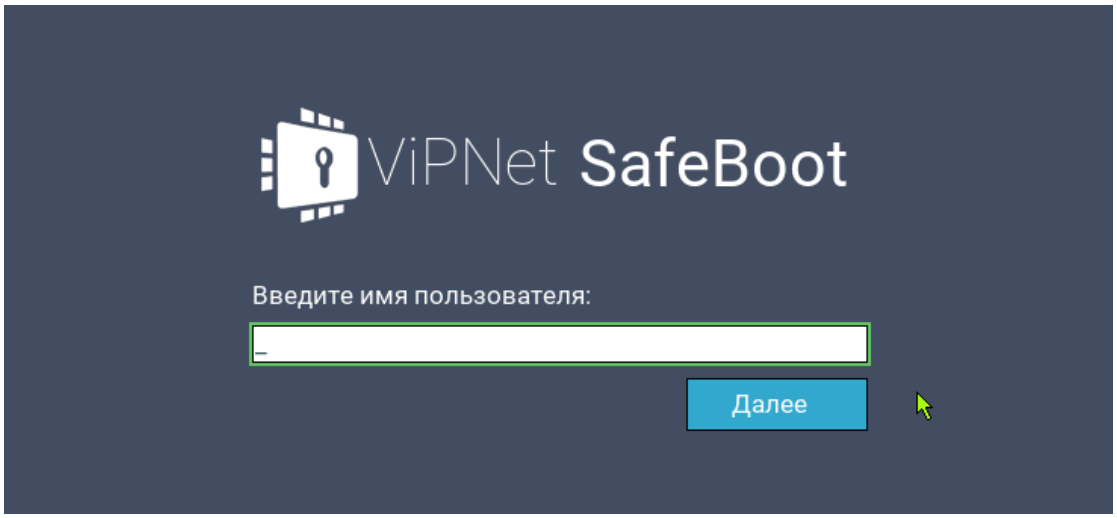


Рисунок 5. Начало аутентификации (ввод имени пользователя)

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

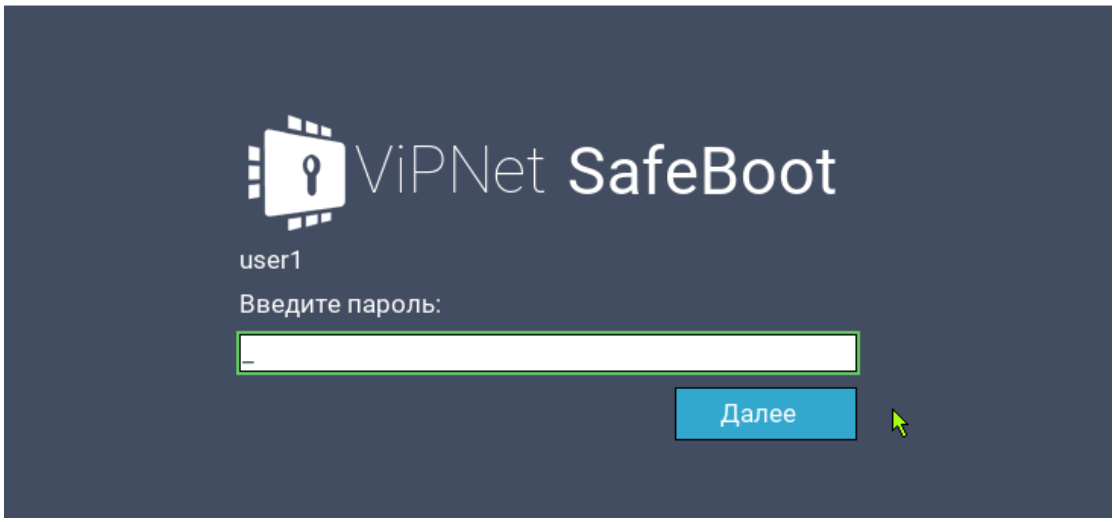


Рисунок 6. Приглашение ввести пароль

После успешной аутентификации и проверки контроля целостности выполняется загрузка операционной системы.

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**.

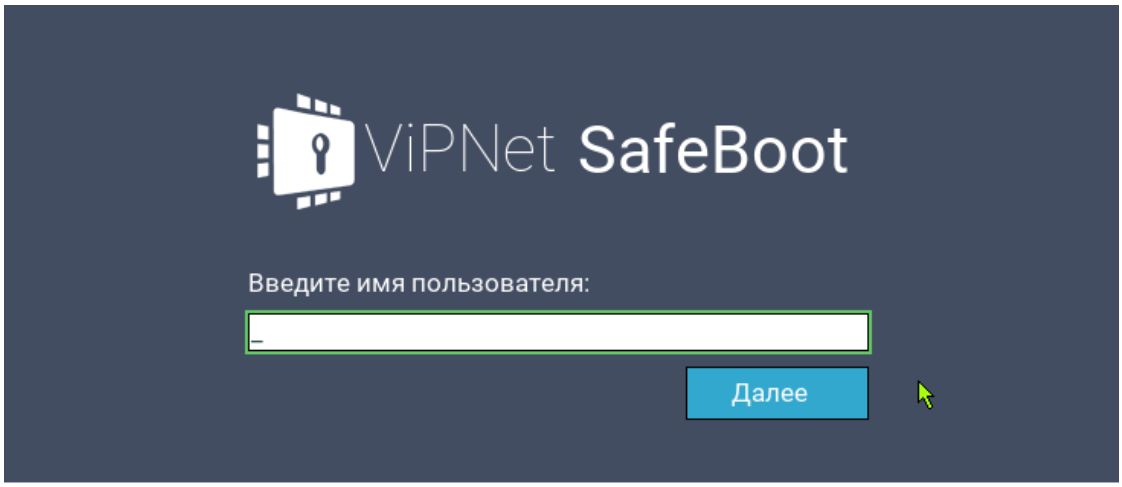


Рисунок 7. Начало аутентификации (ввод имени пользователя)

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

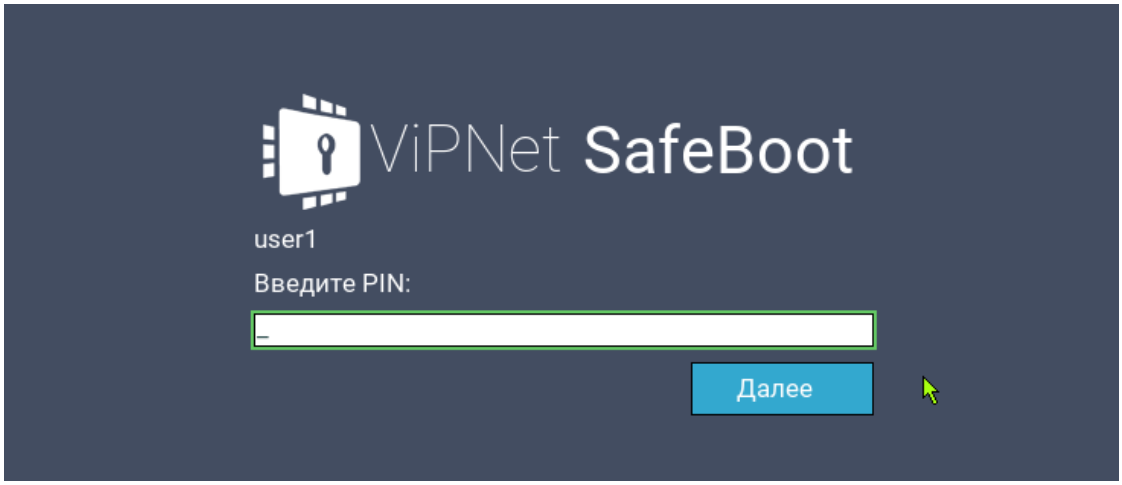


Рисунок 8. Приглашение ввести PIN-код

После успешной аутентификации и проверки контроля целостности выполняется загрузка операционной системы.

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**.

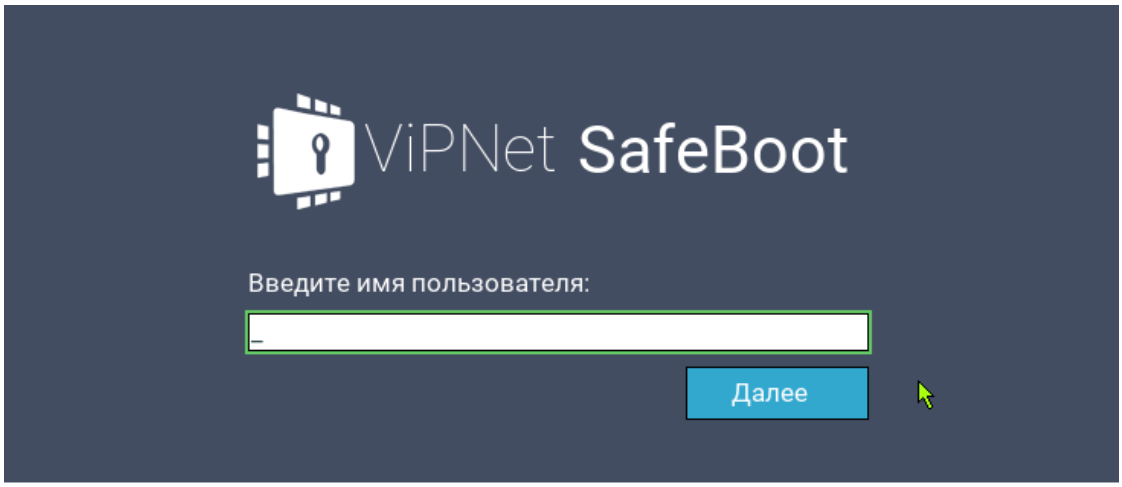


Рисунок 9. Начало аутентификации (ввод имени пользователя)

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

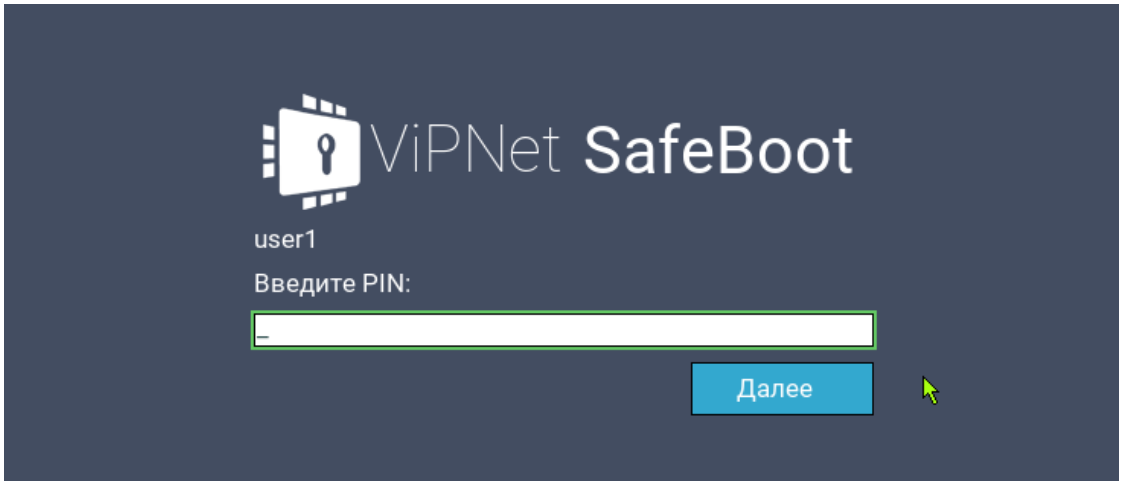


Рисунок 10. Приглашение ввести PIN-код

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

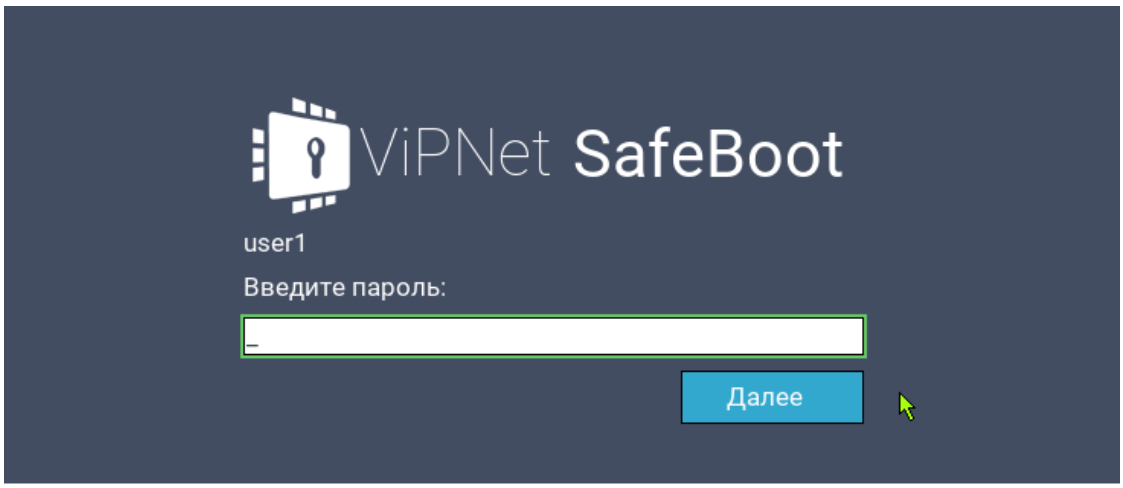


Рисунок 11. Приглашение ввести пароль

После успешной аутентификации и проверки контроля целостности выполняется загрузка операционной системы.

Аутентификация по паролю на электронном идентификаторе

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

1 Установите электронный идентификатор в USB-порт.

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

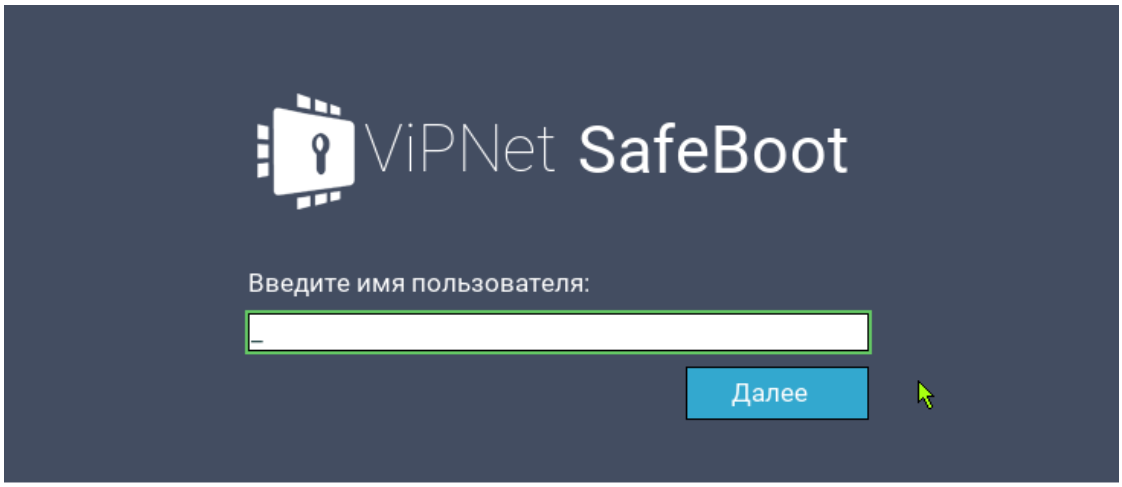


Рисунок 12. Начало аутентификации (ввод имени пользователя)

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

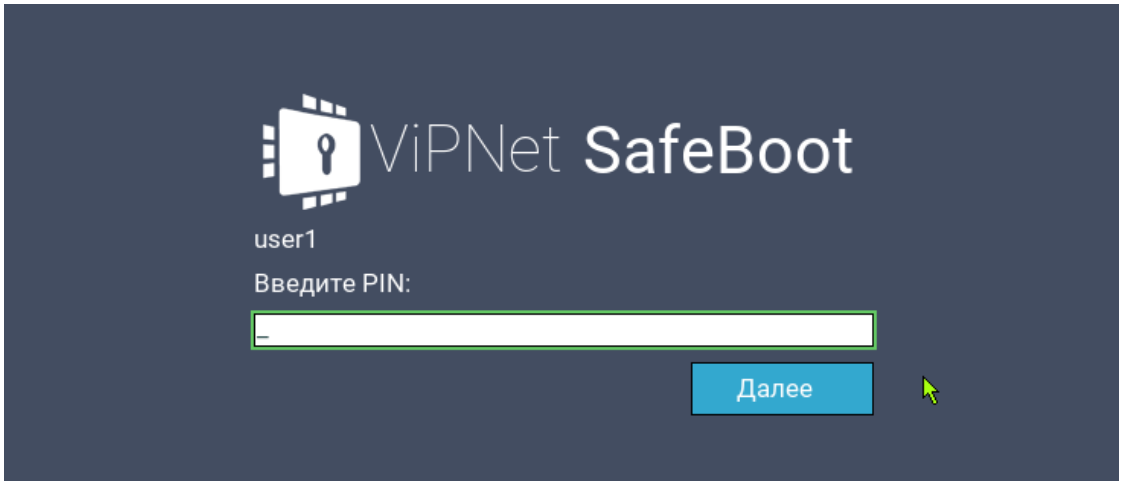


Рисунок 13. Приглашение ввести PIN-код

После успешной аутентификации и проверки контроля целостности выполняется загрузка операционной системы.

Аутентификация пользователя, зарегистрированного на LDAP

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

1 При появлении приглашения ввести имя пользователя, введите логин пользователя в следующем формате **<имя сервера>\<имя учетной записи пользователя>**. Нажмите **Enter**.

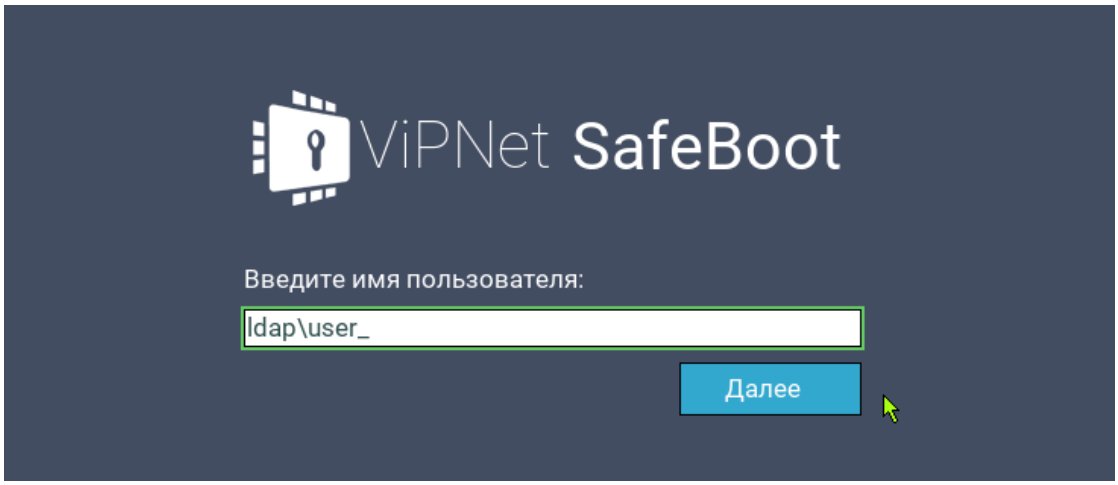


Рисунок 14. Начало аутентификации (ввод имени пользователя)

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

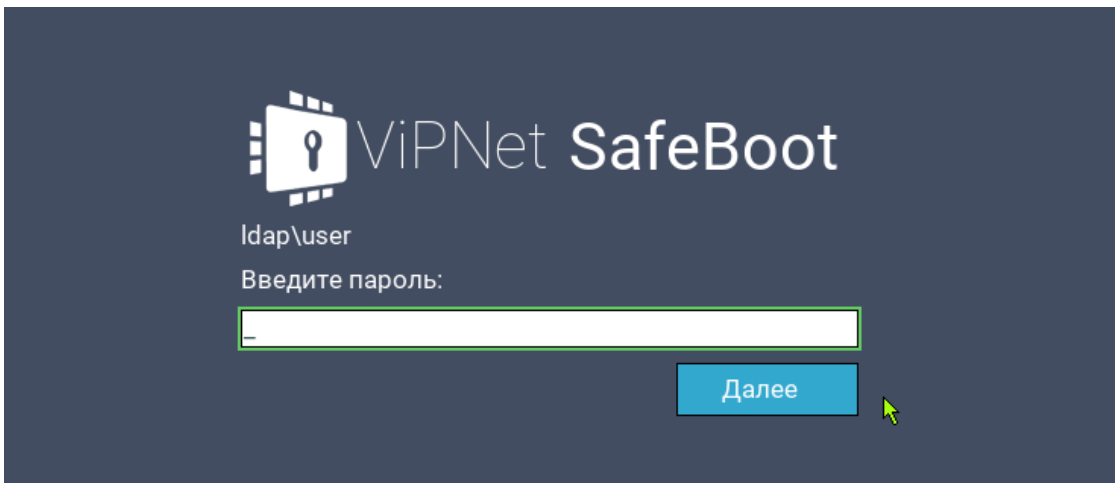


Рисунок 15. Приглашение ввести пароль

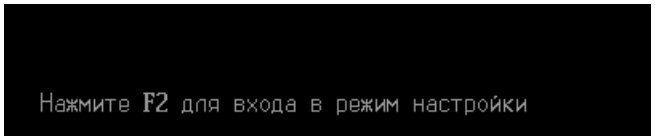
После успешной аутентификации и проверки контроля целостности выполняется загрузка операционной системы.

Смена пароля

Для смены пароля выполните следующие действия:

1 Выполните процедуру аутентификации (см. выше).

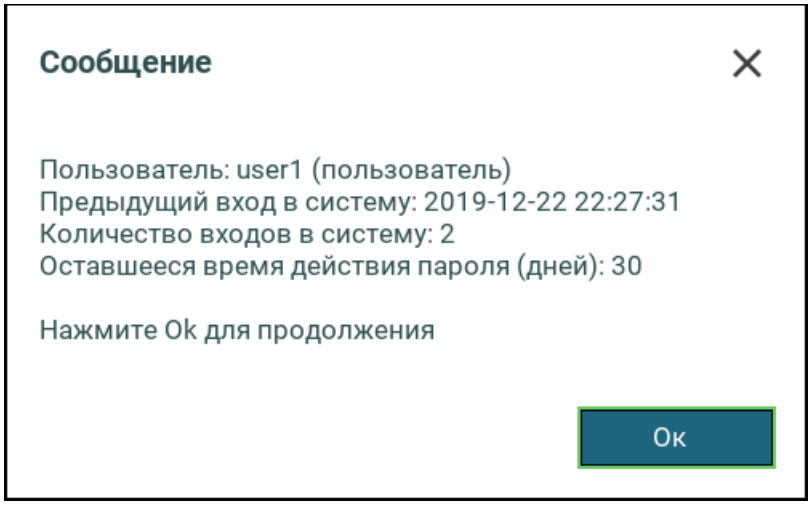
После успешной аутентификации в нижней части экрана появится надпись:



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

2 Нажмите клавишу **F2**.

Откроется окно с информацией о предыдущем входе в систему, количестве входов в систему и сроке действия пароля:



Нажмите любую клавишу. Откроется меню режима настроек ViPNet SafeBoot.

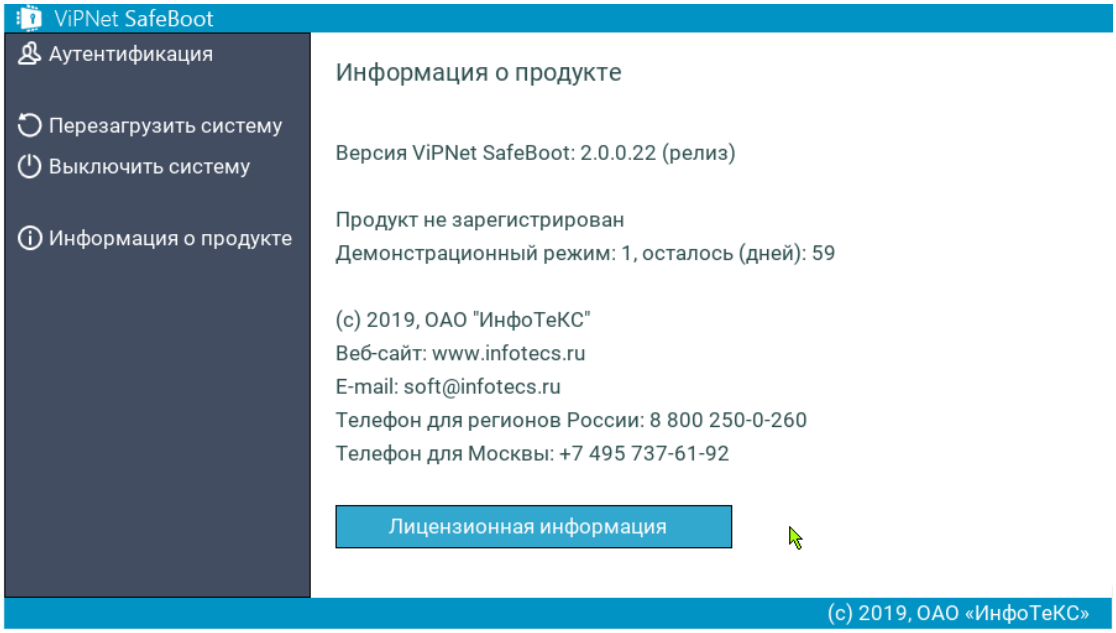


Рисунок 16. Меню режима настроек ViPNet SafeBoot

3 В графическом режиме выберите пункт **Аутентификация**, в текстовом режиме выберите **Настройки пользователя**.

4 В открывшемся меню настроек пользователя выберите **Изменить пароль**.

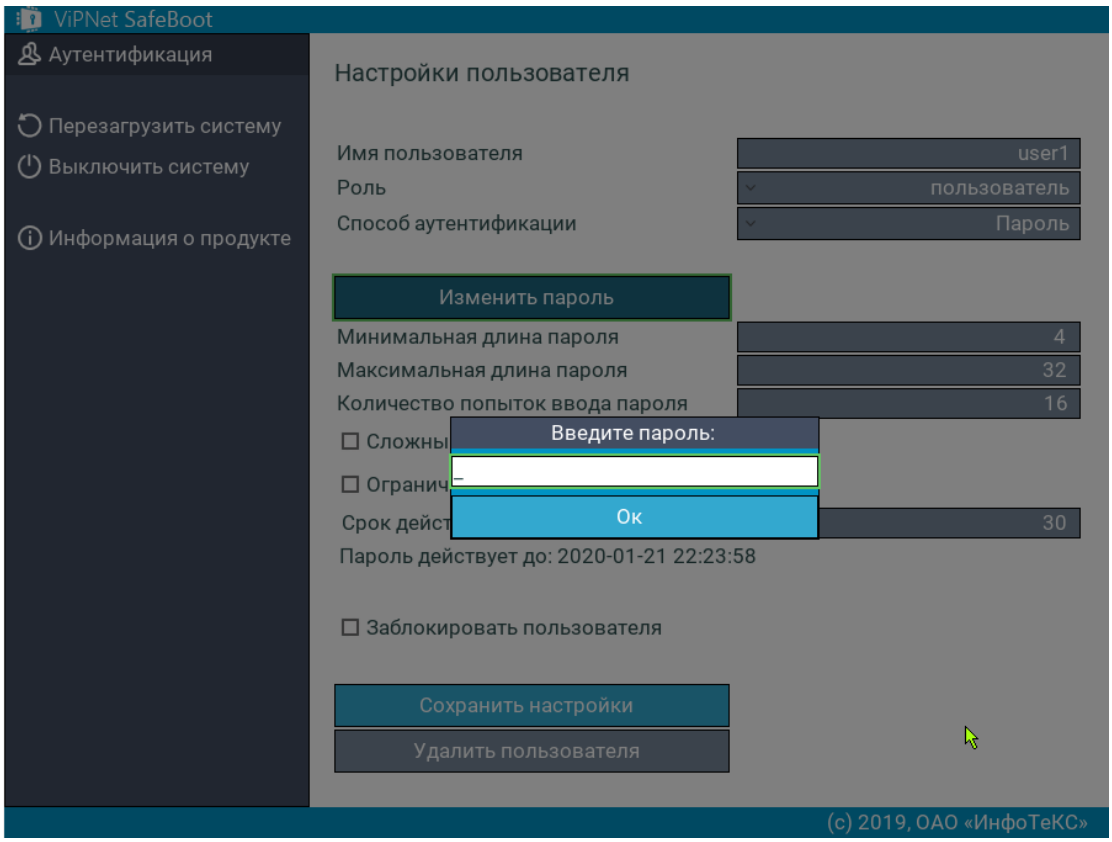


Рисунок 17. Меню настройки пользователя

5 Введите пароль.

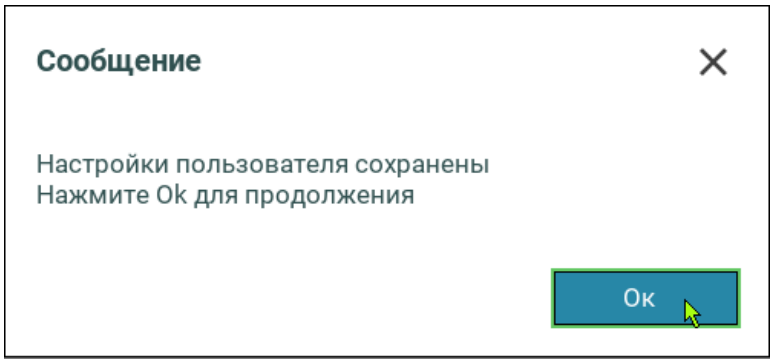
Примечание. Ограничения, действующие при создании пароля:

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

Данные ограничения задаются администратором и могут отличаться от указанных.

6 Сохраните настройки, выбрав соответствующий пункт меню.

Дождитесь появления следующей надписи:

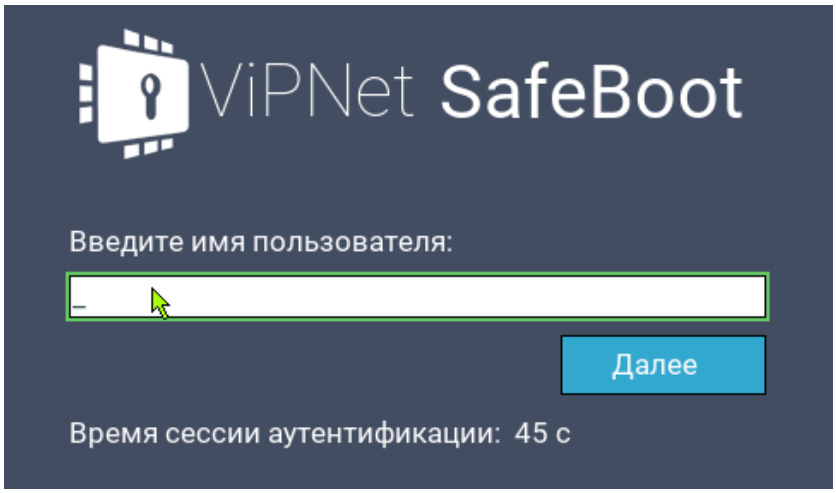


7 Нажмите **Ok**.

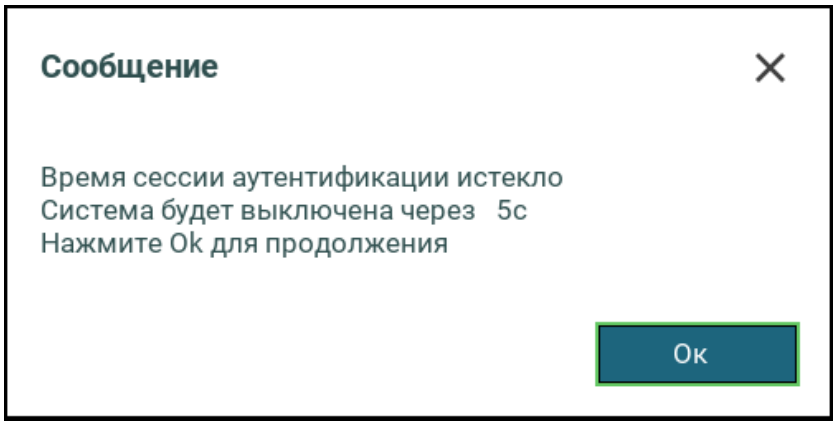
8 Перезагрузите или выключите систему.

Ограничение сессии аутентификации

Время сессии аутентификации может быть ограничено администратором от 15 до 180 секунд. В этом случае в окне для ввода учетных данных в строке **Время сессии аутентификации** будет вестись обратный отсчет установленного времени.

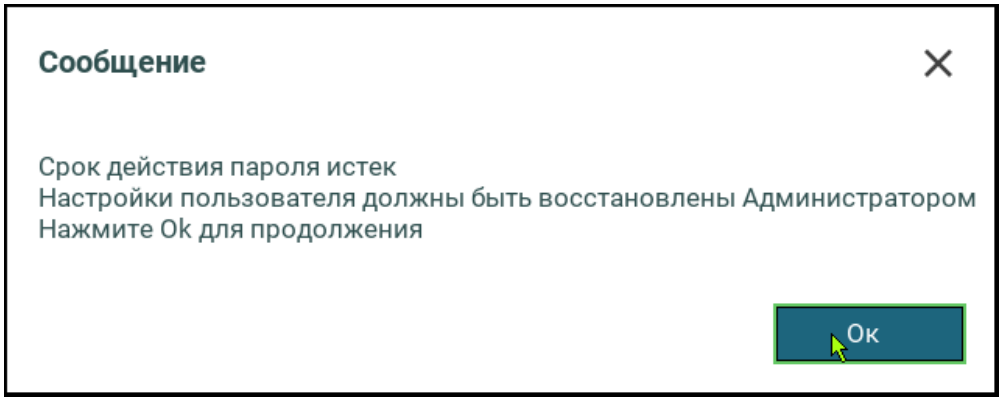


Если вы не успели ввести учетные данные до истечения времени, ограничивающего аутентификацию, то появится следующее сообщение:



Ограничение времени действия пароля

Время действия пароля может быть ограничено администратором. В этом случае, по окончании периода действия пароля, при попытке ввести пароль появится следующее сообщение:



Обратитесь к администратору для получения нового пароля.

A

Сообщения, выдаваемые пользователю

Название сообщения	Описание
Время сессии аутентификации истекло	Время, отведенное на аутентификацию, истекло. Для повторной попытки необходимо дождаться окончания перезагрузки системы.
Количество попыток аутентификации в текущей сессии превышено	Предупреждение о превышении количества ввода неправильных данных при аутентификации
Аутентификация пользователями временно недоступна	При возникновении данного события обратитесь к администратору
Не все подсистемы ПМДЗ настроены. Нужно войти Администратором, чтобы настроить их	Аутентификация невозможна. При возникновении данного события обратитесь к администратору
Пользователь заблокирован	Аутентификация невозможна. При возникновении данного события обратитесь к администратору
Время жизни пароля истекло	Аутентификация невозможна. При возникновении данного события обратитесь к администратору
Настройки пользователя должны быть восстановлены Администратором	Аутентификация невозможна. При возникновении данного события обратитесь к администратору
Неверный пароль	Предупреждение о неверно введенном пароле
Сертификат пользователя не найден на электронном идентификаторе	На электронном идентификаторе отсутствует сертификат, соответствующий аутентификационным данным пользователя

Название сообщения	Описание
Вход данного пользователя невозможен	Аутентификация невозможна. При возникновении данного события обратитесь к администратору
Пользователь не зарегистрирован в системе	Аутентификация невозможна. При возникновении данного события обратитесь к администратору

B

Возможные неполадки и способы их устранения

По всем вопросам, связанным с неполадками и возникающими ошибками, необходимо обращаться к уполномоченному администратору.

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).

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.

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.