



# ViPNet SafeBoot

Руководство пользователя

1991–2016 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00180-01 34 01, версия 1.1.0.19

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

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](mailto:hotline@infotecs.ru)

# Содержание

<b>Введение.....</b>	<b>4</b>
О документе .....	5
Для кого предназначен документ .....	5
Соглашения документа .....	5
О ViPNet SafeBoot.....	6
Назначение ViPNet SafeBoot .....	6
Системные требования .....	6
Обратная связь .....	8
<b>Глава 1. Общие сведения .....</b>	<b>9</b>
Основные возможности ViPNet SafeBoot.....	10
Идентификация и аутентификация пользователей .....	11
Управление ViPNet SafeBoot.....	12
<b>Глава 2. Начало работы .....</b>	<b>13</b>
Перед началом работы .....	14
Запуск и завершение работы .....	15
<b>Глава 3. Процедура идентификации и аутентификации.....</b>	<b>16</b>
Аутентификация по паролю.....	17
Аутентификация по электронному идентификатору .....	18
Аутентификация по электронному идентификатору и паролю .....	20
Смена пароля .....	22
Ограничение сессии аутентификации .....	24
Ограничение времени действия пароля .....	25
<b>Приложение А. События, регистрируемые в ViPNet SafeBoot .....</b>	<b>26</b>
<b>Приложение В. Возможные неполадки и способы их устранения .....</b>	<b>28</b>
<b>Приложение С. Глоссарий .....</b>	<b>29</b>



# Введение

О документе	5
О ViPNet SafeBoot	6
Обратная связь	8

# 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 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
	<b>Внимание!</b> Указывает на обязательное для исполнения или следования действие или информацию.
	<b>Примечание.</b> Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	<b>Совет.</b> Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
<b>Название</b>	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
<b>Клавиша+Клавиша</b>	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
<b>Меню &gt; Подменю &gt; Команда</b>	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
<b>Код</b>	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 исполнением ViPNet SafeBoot, совместимостью с используемым процессором; BIOS платы должен соответствовать спецификации UEFI версии: 2.3.1, 2.4; 2.5; 2.6;
- Видеокарта — дискретная или встроенная;
- Объем оперативной памяти — не менее 1 Гбайт;
- Жесткий диск — объем диска определяется требованиями установленной ОС.

Механизм защиты BIOS (в части защиты микросхемы BIOS от перезаписи) поддерживается для чипсетов Intel, приведенных в таблице ниже. При использовании ViPNet SafeBoot на платформах с другими чипсетами необходимо обеспечить невозможность перезаписи микросхемы BIOS другими средствами, если это не выполнено производителем платформы.

chipset	vendor id	device id
Intel B85	0x8086	0x8C50
Intel Lynx Point LP Premium	0x8086	0x9C43

chipset	vendor id	device id
Intel Bay Trail	0x8086	0x0F1C
Intel C224	0x8086	0x8C54
Intel C60x/X79	0x8086	0x1D41
Intel C610/X99 (Wellsburg)	0x8086	0x8D44
Intel H87	0x8086	0x8C4A
Intel H97	0x8086	0x8CC6
Intel H170	0x8086	0xA144
Intel B150	0x8086	0xA148

# 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>.
- Законодательная база в сфере защиты информации <http://www.infotecs.ru/laws/>.

## 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](mailto: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).

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



# 1

## Общие сведения

Основные возможности ViPNet SafeBoot	10
Идентификация и аутентификация пользователей	11
Управление ViPNet SafeBoot	12

# Основные возможности ViPNet SafeBoot

Основные возможности ViPNet SafeBoot представлены в таблице ниже.

Функциональная возможность	Ссылка
<b>Идентификация и аутентификация пользователей.</b> Обеспечение идентификации и аутентификации зарегистрированных пользователей	Идентификация и аутентификация пользователей на стр. 11
<b>Доверенная загрузка операционной системы.</b> ViPNet SafeBoot обеспечивает загрузку компонент операционной системы только с определенных носителей, назначенных администратором, предоставляет администратору возможность выбрать режим загрузки операционной системы	Управление ViPNet SafeBoot на стр. 12
<b>Контроль целостности.</b> ViPNet SafeBoot выполняет контроль целостности собственного программного обеспечения, образа BIOS и других компонентов	Управление ViPNet SafeBoot на стр. 12
<b>Управление учетными записями пользователей.</b> ViPNet SafeBoot позволяет создавать, редактировать и удалять учетные записи пользователей	Управление ViPNet SafeBoot на стр. 12
<b>Управление настройками аутентификации.</b> ViPNet SafeBoot позволяет задать настройки сессии аутентификации	Управление ViPNet SafeBoot на стр. 12
<b>Управление сертификатами.</b> ViPNet SafeBoot позволяет загрузить корневой сертификат и список отозванных сертификатов	Управление ViPNet SafeBoot на стр. 12
<b>Проверка и установка обновлений.</b> Автоматический поиск файла обновления и установка обновлений посредством меню управления настройками	Управление ViPNet SafeBoot на стр. 12
<b>Экспорт и импорт настроек ViPNet SafeBoot</b>	Управление ViPNet SafeBoot на стр. 12
<b>Ведение журнала событий.</b> Регистрация событий и учет действий в меню ViPNet SafeBoot	Управление ViPNet SafeBoot на стр. 12

# 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 может содержать от 4 до 32 символов.



**Примечание.** Срок действия пароля может быть ограничен.

Если администратор установил ограничение на срок действия пароля, то по истечении заданного периода выводится соответствующее сообщение о необходимости смены пароля, загрузка операционной системы блокируется.

---

Электронный идентификатор представляет собой специальное USB устройство, содержащее личный сертификат пользователя формата X509, а также закрытый ключ, соответствующий публичному ключу, содержащемуся в сертификате. Для доступа к информации, содержащейся на электронном идентификаторе, требуется ввести PIN-код пользователя.

В ViPNet SafeBoot поддерживаются следующие электронные идентификаторы: Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен Lite, JaCarta PKI (USB/SC), Guardant ID.

Процедура идентификации и аутентификации приведена на стр. 16.



**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:

- Доверенная загрузка операционной системы.
- Контроль целостности.
- Управление учетными записями пользователей.
- Управление настройками аутентификации.
- Управление сертификатами.
- Проверка и установка обновлений.
- Экспорт и импорт настроек ViPNet SafeBoot настройки ViPNet SafeBoot
- Ведение и управление журналом событий.

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

Обычному пользователю в режиме настройки ViPNet SafeBoot доступна только смена своего пароля.

# 2

## Начало работы

Перед началом работы	14
Запуск и завершение работы	15

# 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):

- 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. на стр. 11).

Завершение работы ViPNet SafeBoot осуществляется при запуске операционной системы либо отключении питания компьютера.

# 3

## Процедура идентификации и аутентификации

Аутентификация по паролю	17
Аутентификация по электронному идентификатору	18
Аутентификация по электронному идентификатору и паролю	20
Смена пароля	22
Ограничение сессии аутентификации	24
Ограничение времени действия пароля	25



# 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**.

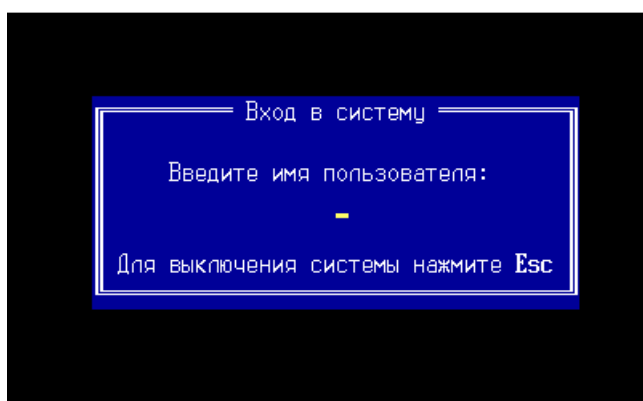


Рисунок 1. Начало аутентификации (ввод имени пользователя)

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

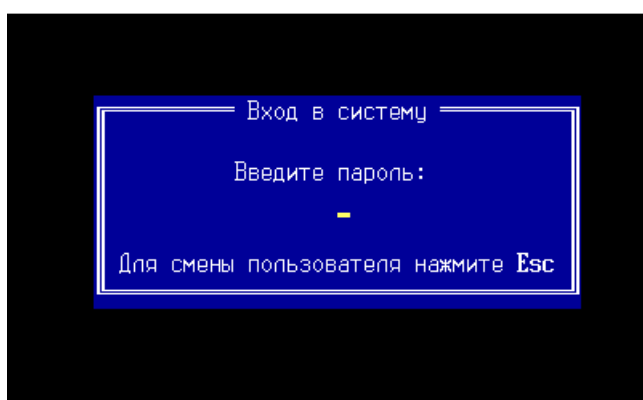


Рисунок 2. Приглашение ввести пароль

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

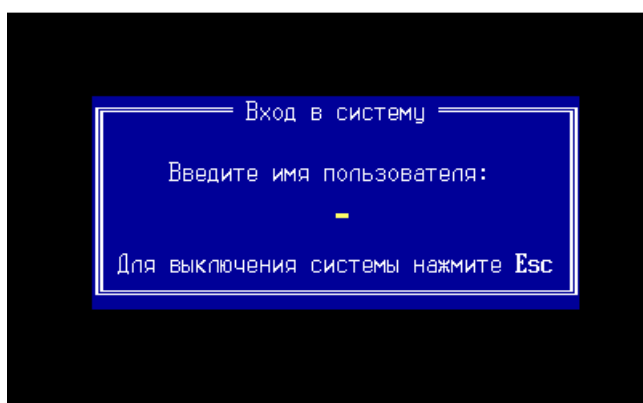


Рисунок 3. Начало аутентификации (ввод имени пользователя)

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

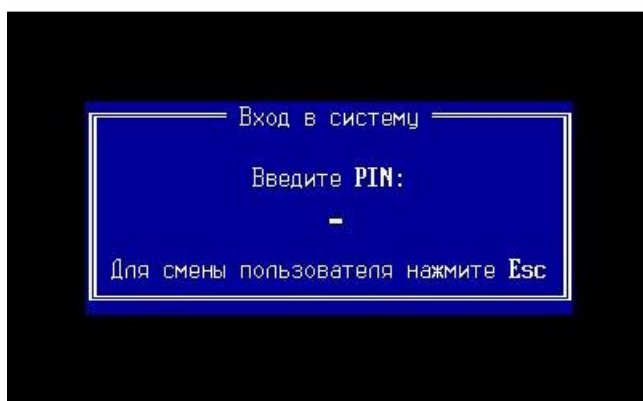


Рисунок 4. Приглашение ввести PIN-код

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

# Аутентификация по электронному идентификатору и паролю

Для выполнения аутентификации по электронному идентификатору, выполните следующие действия:

- 1 Вставьте электронный идентификатор.
- 2 При появлении приглашения ввести имя пользователя, введите логин, выданный администратором и нажмите **Enter**.

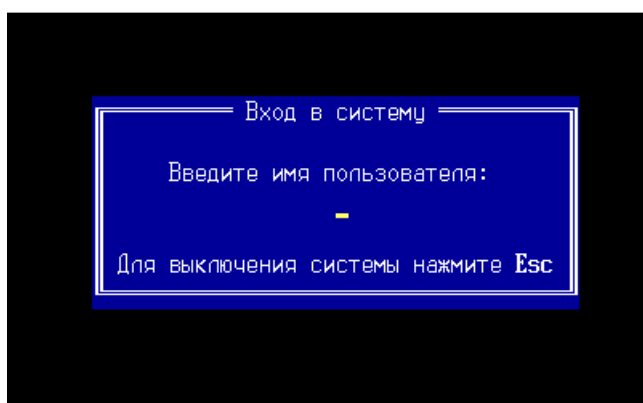


Рисунок 5. Начало аутентификации (ввод имени пользователя)

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

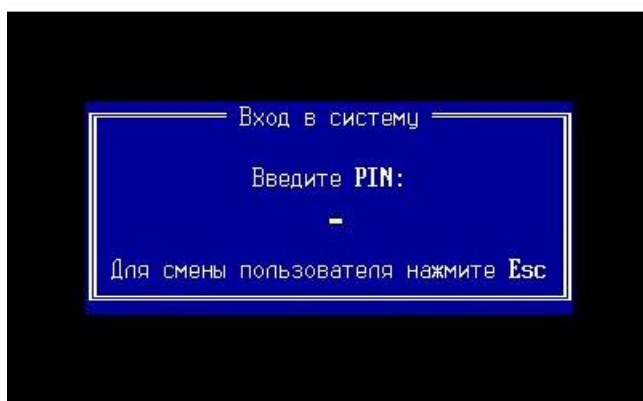
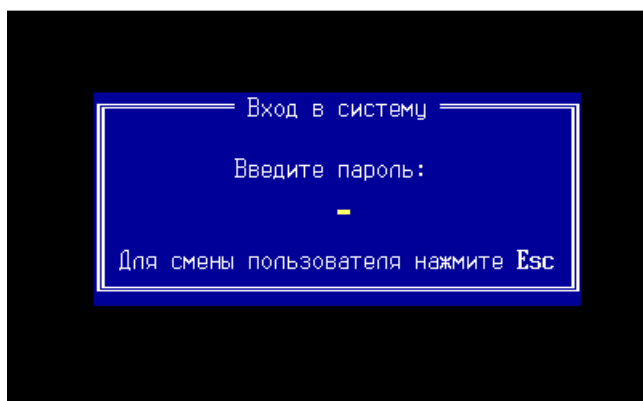


Рисунок 6. Приглашение ввести PIN-код

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



*Рисунок 7. 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:

**Нажмите [F2] для входа в режим настройки**



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

---

- 2 Нажмите **F2**.

Откроется меню режима настроек ViPNet SafeBoot.

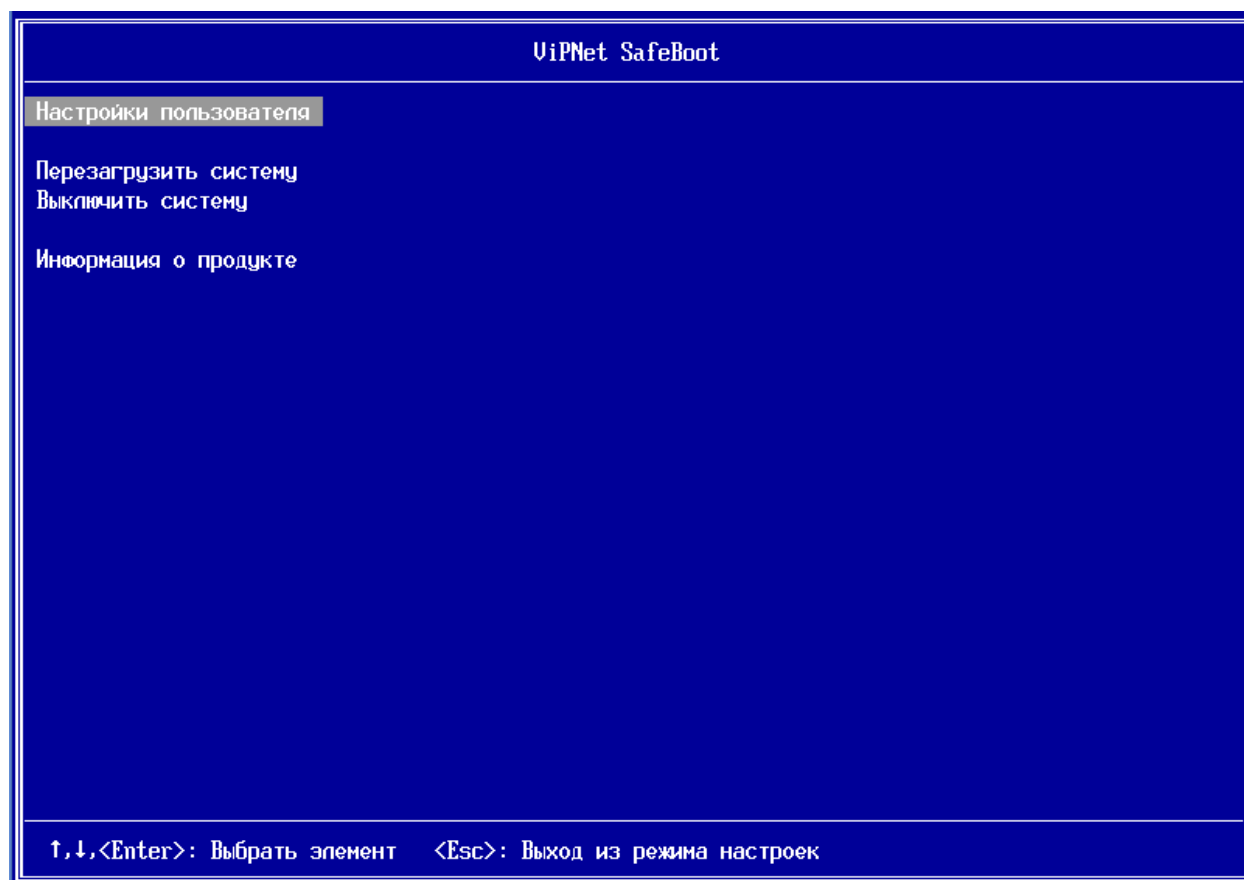


Рисунок 8. Меню режима настроек ViPNet SafeBoot

- 3 Выберите **Настройки пользователя**.
- 4 В открывшемся меню настроек пользователя выберите **Изменить пароль**.

Настройки пользователя	
Имя пользователя	<user1>
Роль	<пользователь>
Способ аутентификации	<Пароль>
<b>Изменить пароль</b>	
Минимальная длина пароля	<4>
Максимальная длина пароля	<32>
Количество попыток ввода пароля	<16>
Сложный пароль	[ 1 ]
Ограничить срок действия пароля	[ x ]
Срок действия пароля (дней)	
Пароль действует до: 2016-09-20 15:18	Введите пароль :
Сохранить настройки	
Удалить пользователя	

↑,↓,<Enter>: Выбрать элемент    <Esc>: Назад

Рисунок 9. Меню настройки пользователя

5 Введите пароль.



**Примечание.** Ограничения, действующие при создании пароля:

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

6 Сохраните настройки, выбрав соответствующий пункт меню.

Дождитесь появления следующей надписи:

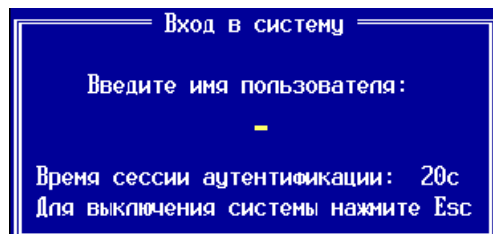
Настройки пользователя сохранены  
Нажмите любую клавишу для продолжения

7 Нажмите Esc для выхода в основное меню.

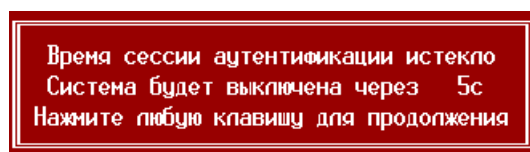
8 Перезагрузите или выключите систему.

# 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, ограничивающем 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:

Время жизни пароля истекло  
Настройки пользователя должны быть восстановлены Администратором  
Нажмите любую клавишу для продолжения

Обратитесь к администратору для получения нового пароля.



## События, регистрируемые в ViPNet SafeBoot

№ события	Название события	Описание события
1	<b>Время сессии аутентификации истекло</b>	Время, отведенное на аутентификацию, истекло. Для повторной попытки необходимо дождаться окончания перезагрузки системы.
2	<b>Количество попыток аутентификации в текущей сессии превышено</b>	Предупреждение о превышении количества ввода неправильных данных при аутентификации
3	<b>Аутентификация пользователями временно недоступна</b>	При появлении данного события, необходимо обратиться к администратору
4	<b>Не все подсистемы ПМДЗ настроены. Нужно войти Администратором, чтобы настроить их</b>	Аутентификация невозможна. При появлении данного события, необходимо обратиться к администратору
5	<b>Пользователь заблокирован</b>	Аутентификация невозможна. При появлении данного события, необходимо обратиться к администратору
6	<b>Время жизни пароля истекло</b>	Аутентификация невозможна. При появлении данного события, необходимо обратиться к администратору
7	<b>Настройки пользователя должны быть восстановлены Администратором</b>	Аутентификация невозможна. При появлении данного события, необходимо обратиться к администратору

№ события	Название события	Описание события
8	<b>Неверный пароль</b>	Предупреждение о неверно введенном пароле
9	<b>Сертификат пользователя не найден на электронном идентификаторе</b>	На электронном идентификаторе отсутствует сертификат, соответствующий аутентификационным данным пользователя
10	<b>Вход данного пользователя невозможен</b>	Аутентификация невозможна. При появлении данного события, необходимо обратиться к администратору
11	<b>Пользователь не зарегистрирован в системе</b>	Аутентификация невозможна. При появлении данного события, необходимо обратиться к администратору



# В

## 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.