ViPNet SafeBoot

Руководство администратора

infotecs

ФРКЕ.00180-01 32 01, версия 1.1.0.19

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.00180-01 (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 и паролю.

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
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

Комплект поставки

В комплект поставки ViPNet SafeBoot входит:

- Программный комплекс «Программный модуль доверенной загрузки ViPNet SafeBoot» ФРКЕ.00180-01;
- Формуляр;
- Документация в формате PDF, в том числе:
  - «ViPNet SafeBoot. Руководство администратора» (данный документ).
  - «ViPNet SafeBoot. Руководство пользователя».

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.
- 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.

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. Способы аутентификации	Идентификация и аутентификация пользователей на стр. 13
Доверенная загрузка операционной системы. ViPNet SafeBoot обеспечивает загрузку компонент операционной системы только с определенных носителей, назначенных администратором, предоставляет администратору возможность выбрать режим загрузки операционной системы	Управление параметрами загрузки ОС на стр. 42
Контроль целостности. ViPNet SafeBoot выполняет контроль целостности собственного программного обеспечения, образа BIOS и других компонентов	Контроль целостности на стр. 47
Управление учетными записями пользователей. ViPNet SafeBoot позволяет создавать, редактировать и удалять учетные записи пользователей	Управление учетными записями пользователей на стр. 59
Управление настройками аутентификации. ViPNet SafeBoot позволяет задать настройки сессии аутентификации	Управление настройками аутентификации на стр. 34
Управление сертификатами. ViPNet SafeBoot позволяет загрузить корневые сертификаты и список отзыва сертификатов	Управление сертификатами на стр. 83
Проверка и установка обновлений. Автоматический поиск файла обновления и установка обновлений посредством меню управления настройками	Обновление ViPNet SafeBoot на стр. 17
Экспорт и импорт настроек ViPNet SafeBoot	Экспорт настроек на стр. 36 Импорт настроек на стр. 41
Ведение журнала событий. Регистрация всех значимых событий безопасности и действий пользователя.	Управление журналом событий на стр. 90

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 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 по истечении заданного периода выводится соответствующе сообщение о необходимости смены пароля, пользователь блокируется до смены пароля.

Электронный идентификатор представляет собой специальное USB устройство, содержащее личный сертификат пользователя формата X.509, а также закрытый ключ, соответствующий публичному ключу, содержащемуся в сертификате.

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

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. 25.

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

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

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.

2

Установка, обновление и удаление ViPNet SafeBoot

Установка и удаление ViPNet SafeBoot

Программный комплекс ViPNet SafeBoot поставляется в предустановленном виде или устанавливается специально подготовленными сервисными инженерами.

По вопросам удаления ViPNet SafeBoot необходимо связаться со специалистами ОАО «ИнфоТеКС» любым способом, приведенным в разделе **Обратная связь** на стр. 10.

Обновление ViPNet SafeBoot

Чтобы загрузить обновления ViPNet SafeBoot, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).

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. 40). После обновления рекомендуется выполнить импорт настроек (см. Импорт настроек на стр. 41)

---

2 Подключите USB накопитель, 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 накопитель не подключен, появится соответствующее сообщение. Вставьте USB накопитель, 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.

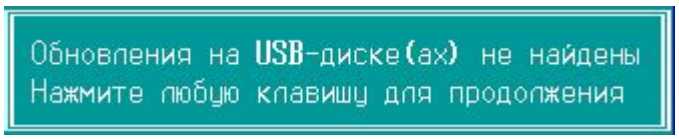


Рисунок 1. Сообщение обновление не найдено

Если USB накопитель содержит устаревшую версию, то на экране появится сообщение: «Пакет обновления найден, но является устаревшим (версия ниже текущей)». Нажмите любую клавишу для продолжения работы.

Рисунок 2. Сообщение об устаревшей версии обновления

Если USB накопитель содержит обновление для другой платформы, то на экране появится сообщение «Пакет обновления найден, но для другой платформы». Нажмите любую клавишу для продолжения работы.

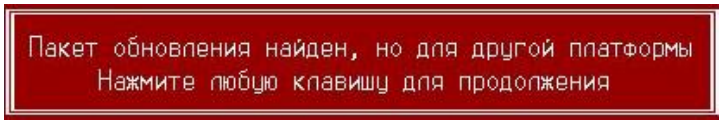


Рисунок 3. Сообщение о не совпадении платформы

5 Откроется окно с указанием версии обновления. В открывшемся окне выбрать **Обновить ViPNet SafeBoot.**

Рисунок 4. Выбор найденной версии обновления

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

Рисунок 5. 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 6. Сообщение о верификации пакета обновления

В случае ошибке при верификации пакета будет выдано сообщение:

Рисунок 7. Сообщение об ошибке верификации пакета обновления

8 В ходе установки обновления будет выдано следующее сообщение

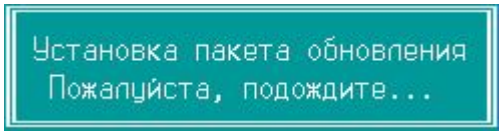


Рисунок 8. Сообщение об установке пакета обновления

при нахождении нескольких разделов с рабочим каталогом «EFI\Infotecs» будет выдано сообщение:

Рисунок 9. Сообщение об ошибке при установке обновления

9 По окончании установки пакета обновления будет выполнена перезагрузка. В журнале событий появится сообщение об установленном обновлении.

3

Начало работы

Первый запуск

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

Порядок действий при первом запуске следующий:

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

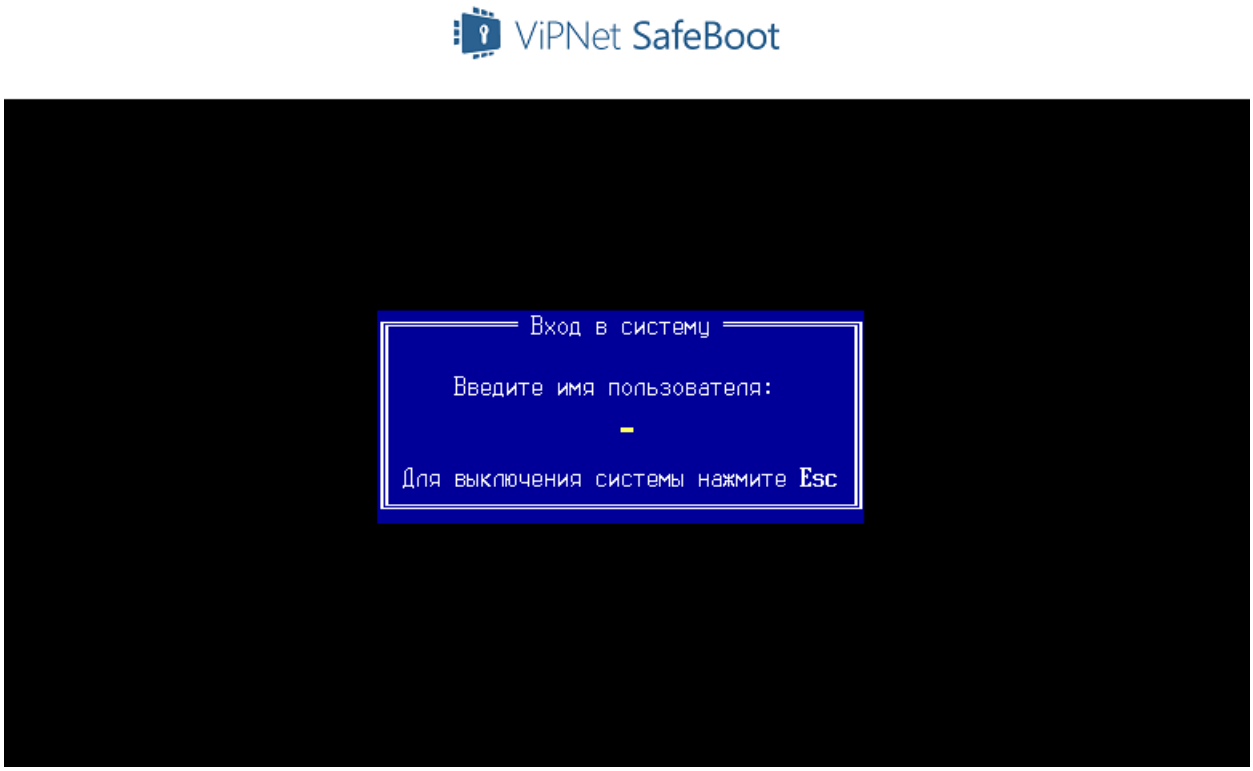


Рисунок 10. Начало аутентификации (ввод имени пользователя)

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

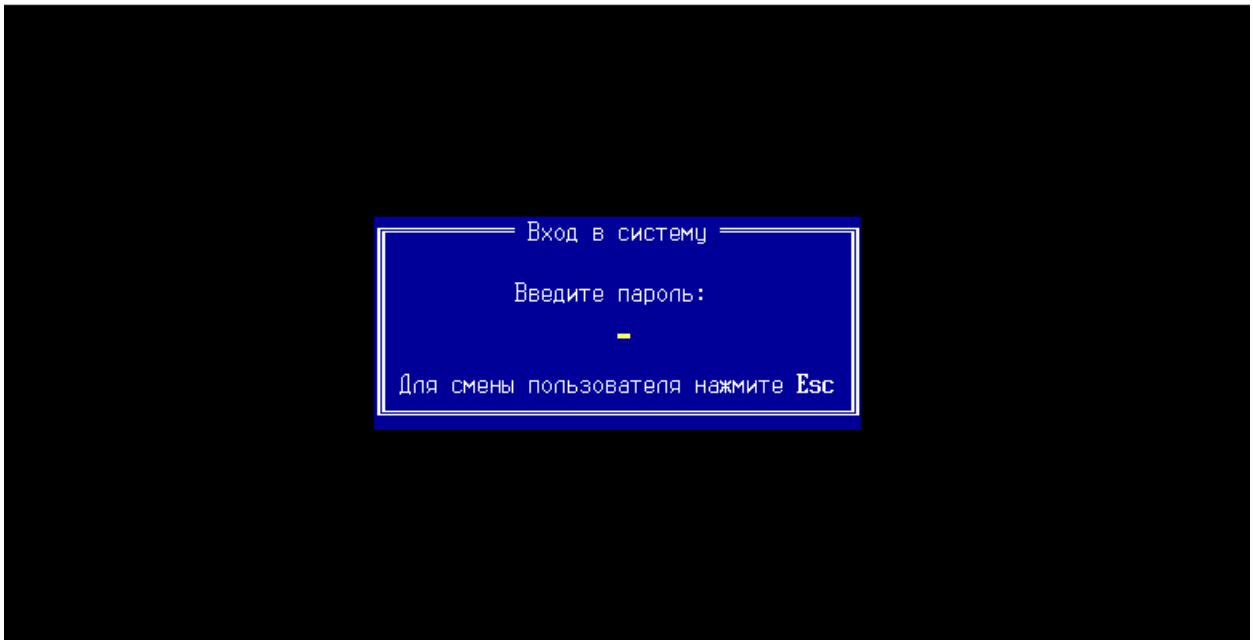


Рисунок 11. Приглашение ввести пароль

3 После успешной аутентификации будет выдано следующее сообщение:

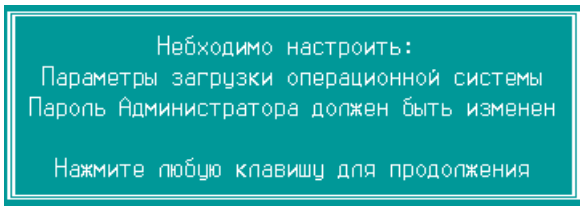


Рисунок 12. Сообщение о необходимых настройках при первом включении

4 Нажмите любую клавишу.

Откроется меню настроек ViPNet SafeBoot:

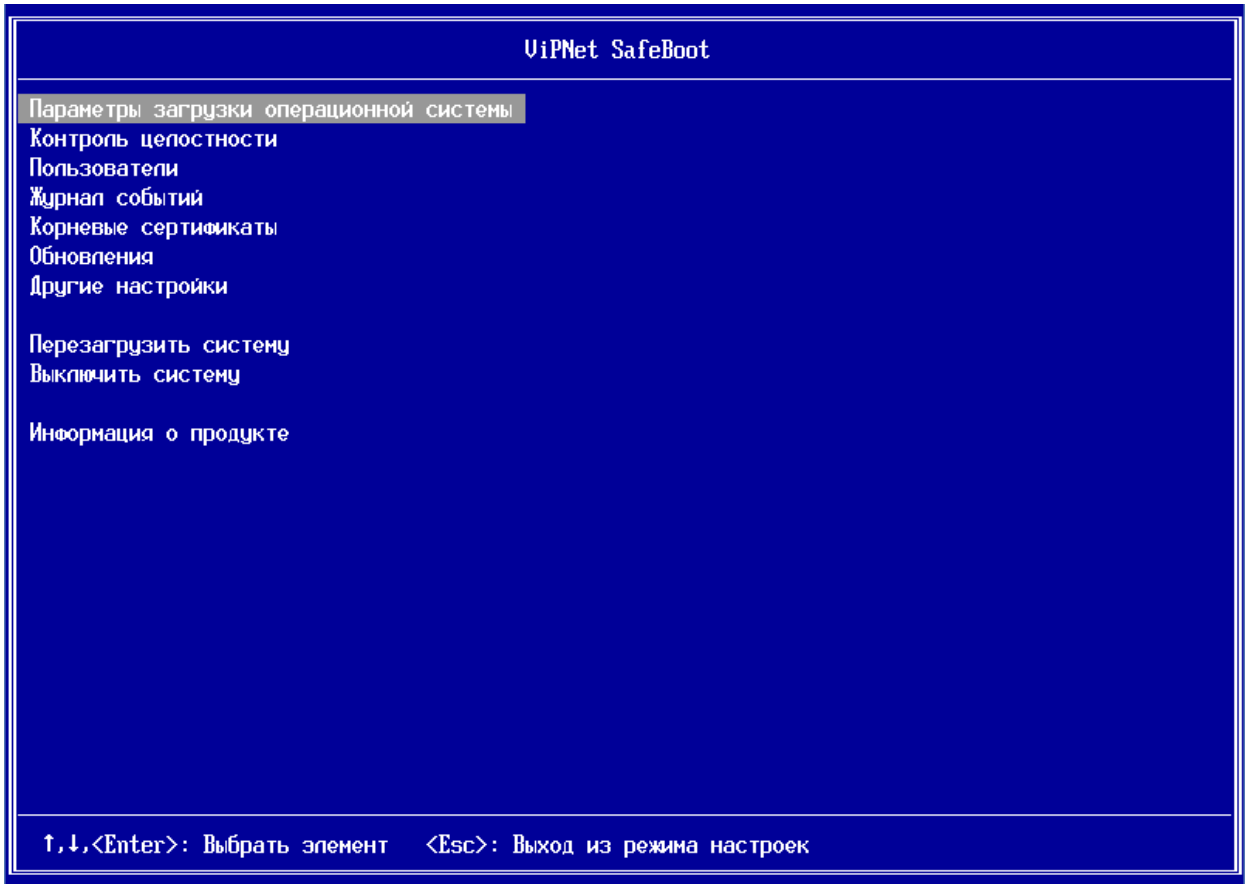


Рисунок 13. Меню режима настроек ViPNet SafeBoot

5 В меню режима настроек выберите **Пользователи**.

6 В открывшемся окне выберите из списка текущих пользователей – **Administrator**.

7 В окне **Настройки пользователя** выберите **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:

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

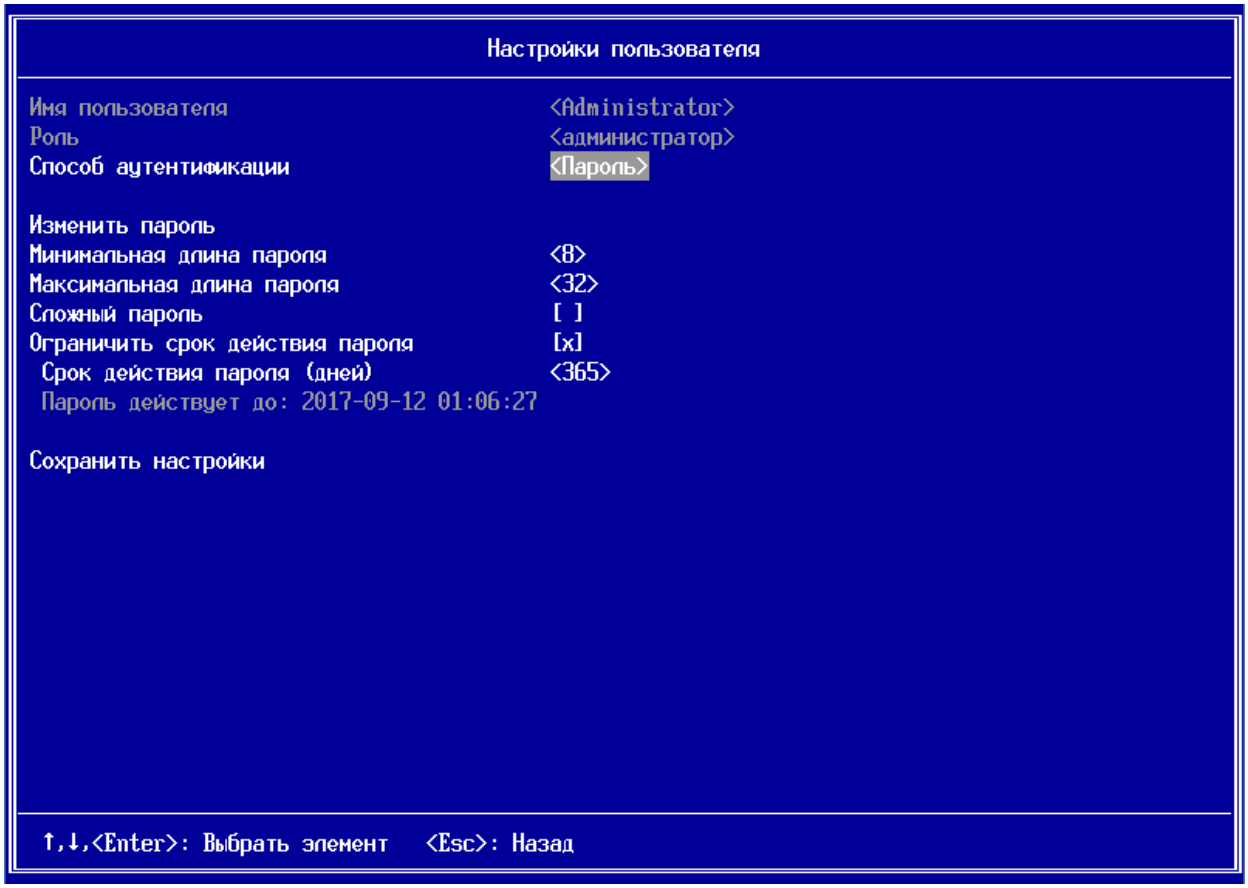
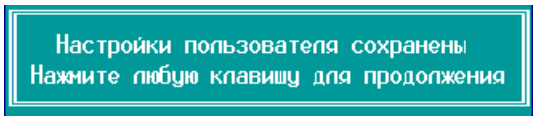


Рисунок 14. Меню настроек пользователя

8 Сохраните настройки, выбрав соответствующий пункт меню.

Дождитесь появления следующей надписи:



9 Нажмите любую клавишу.

10 Для выхода в основное меню дважды нажмите Esc.

Запуск и завершение работы

Запуск ViPNet SafeBoot осуществляется автоматически при включении компьютера, на котором он установлен, 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. 30), необходимо выполнить процедуру идентификации и аутентификации (см. ниже).

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 либо отключении питания компьютера.

Аутентификация по паролю

Для выполнения аутентификации по паролю, выполните следующие действия:

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

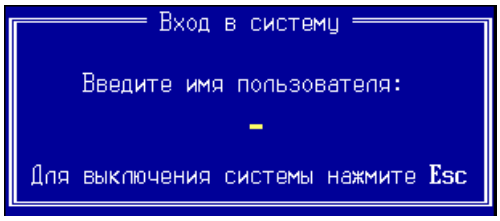


Рисунок 15. Начало аутентификации (ввод имени пользователя)

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

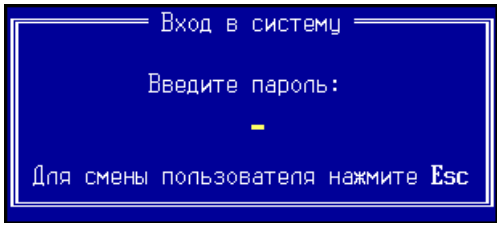


Рисунок 16. Приглашение ввести пароль

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**.

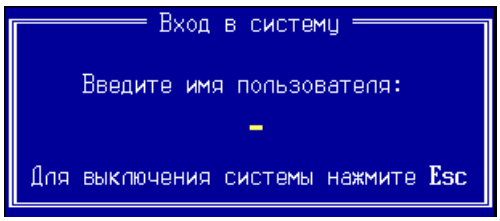


Рисунок 17. Начало аутентификации (ввод имени пользователя)

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

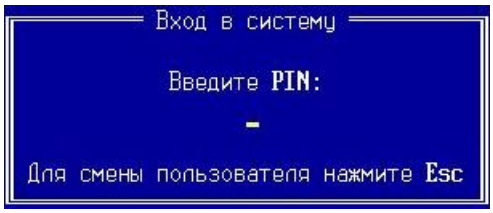


Рисунок 18. Приглашение ввести PIN-код

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**.

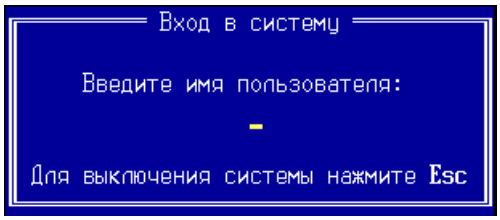


Рисунок 19. Начало аутентификации (ввод имени пользователя)

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

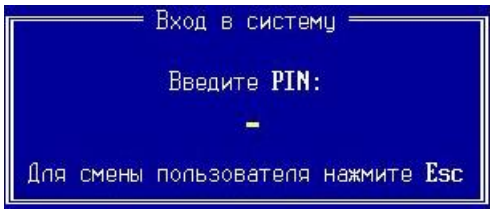


Рисунок 20. Приглашение ввести PIN-код

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

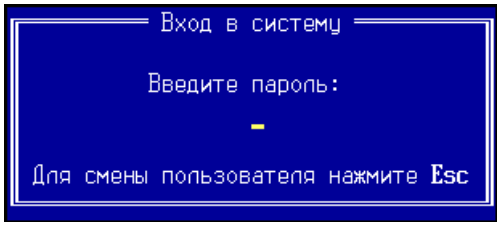


Рисунок 21. Приглашение ввести пароль

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. 25).

После успешной аутентификации в нижней части экрана появится надпись:

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

3 Нажмите **F2**.

Откроется основное меню режима настроек ViPNet SafeBoot.

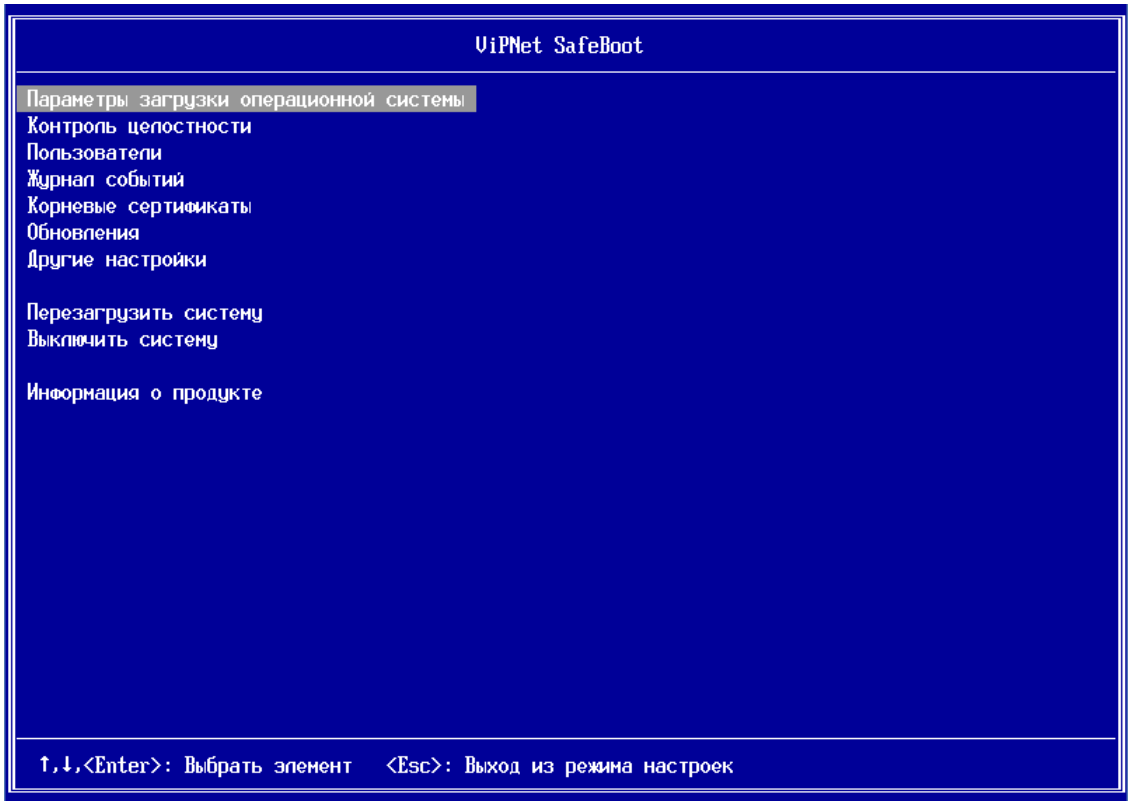


Рисунок 22. Вид меню режима настроек ViPNet SafeBoot для Администратора

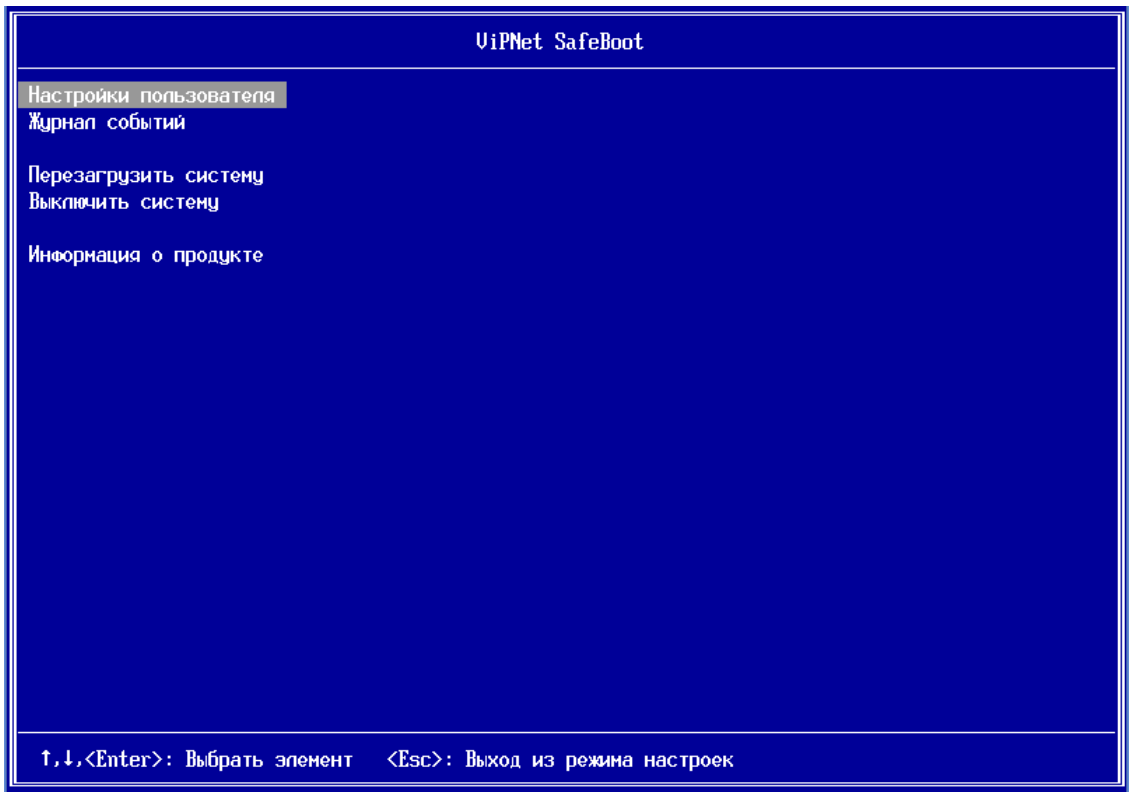


Рисунок 23. Вид меню режима настроек ViPNet SafeBoot для Аудитора

Интерфейс режима настройки

Интерфейс режима настройки представляет собой список функций для управления ViPNet SafeBoot. Перемещение по пунктам списка и выбор необходимого элемента осуществляется клавишами клавиатуры:

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

Выбор элемента управления **Параметры загрузки операционной системы** 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:

- выбрать контролируемые объекты:
  - файлы на разделах накопителя;
  - CMOS, PCI, ACPI, SMBIOS, карта памяти;
  - BIOS;
  - загрузочные сектора выбранного диска (MBR);
  - журналы транзакций файловых систем NTFS, EXT3, EXT4.
- выполнить принудительную проверку целостности контролируемых объектов;
- выполнить перерасчет эталонов всех объектов.

Выбор элемента управления **Пользователи** позволяет просматривать, редактировать, удалять и создавать новые учетные записи пользователей.

Выбор элемента управления **Журнал событий** позволяет просматривать и выгружать записи журнала событий, выбирать режим журналирования и уровень регистрации событий.

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

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

Выбор элемента управления **Другие настройки** позволяет:

- ограничить время сессии аутентификации на ввод аутентификационных данных;
- установить защиту BIOS от перезаписи из ОС;
- разрешить однократный вход в BIOS Setup;
- экспортировать настройки;
- импортировать настройки;
- настроить автоматический вход в систему.

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

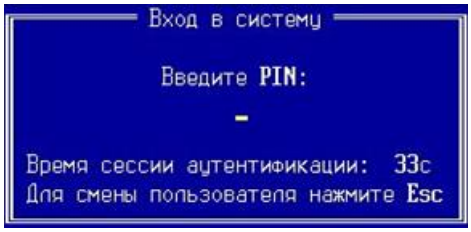
Выбор элемента управления **Выключить систему** осуществляет немедленное выключение системы.

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

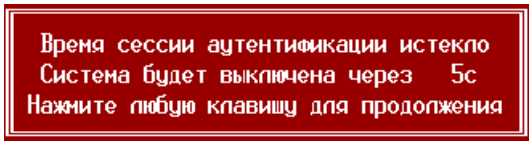
Ограничение сессии аутентификации

Опция «Ограничение сессии аутентификации» ограничивает время для аутентификации пользователя. 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. 25). 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. 30).
2. В меню режима настроек выберите **Другие настройки**.
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.

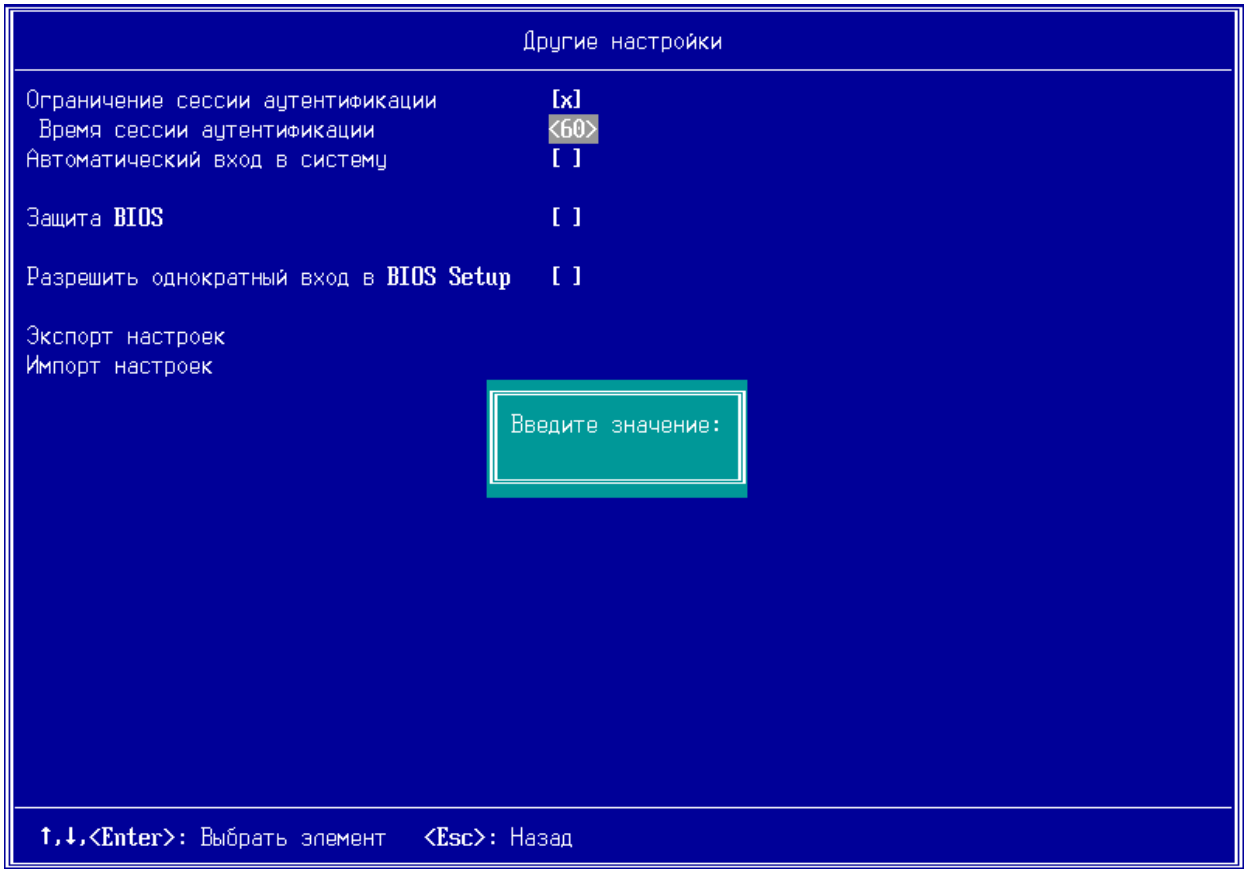


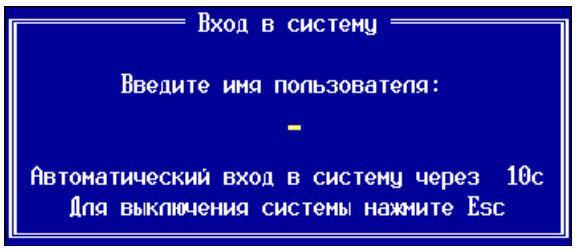
Рисунок 24. Ввод значения времени сессии аутентификации

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

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. 25).

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

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. 30).
2. В меню режима настроек выберите **Другие настройки**.
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.

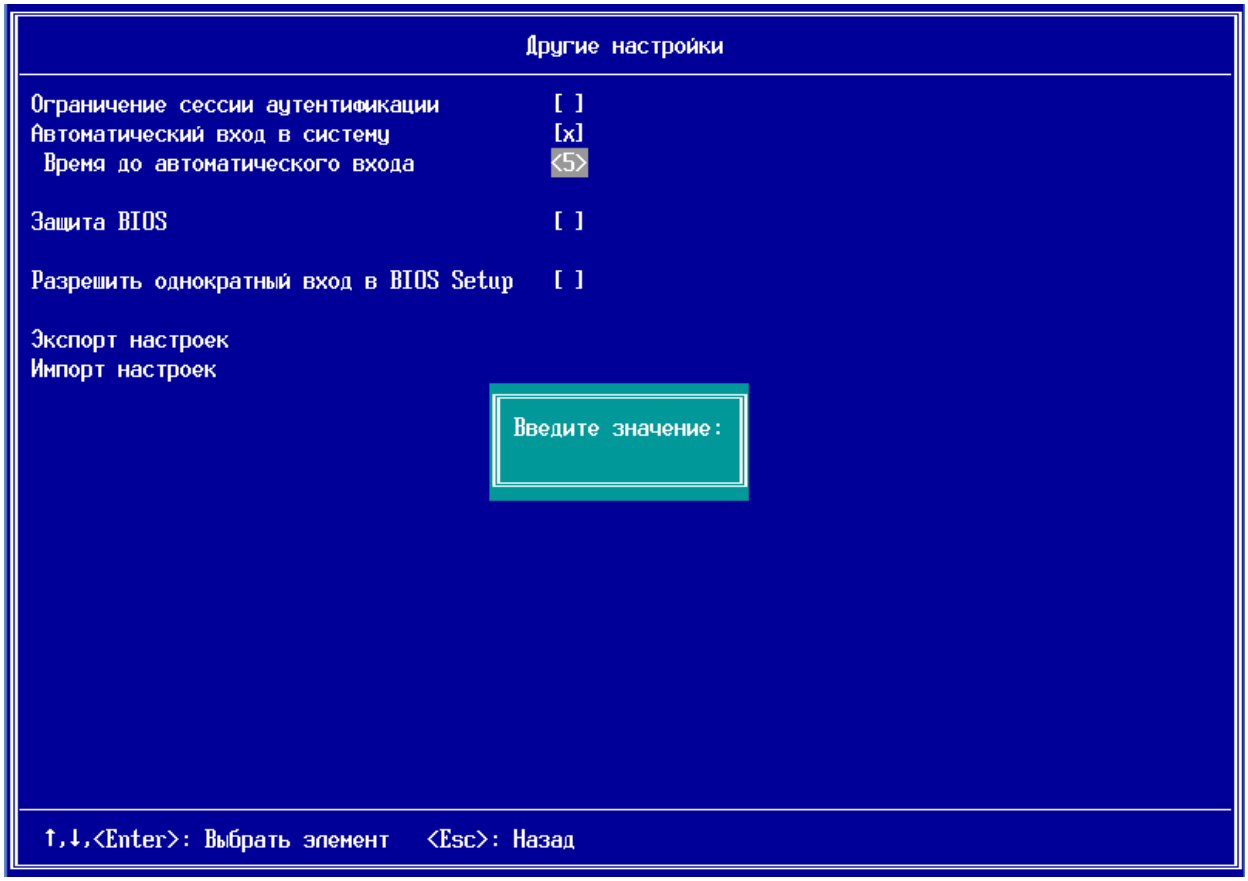


Рисунок 25. Ввод значения времени до автоматического входа в систему

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

Защита BIOS

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

Чтобы установить функцию защиты BIOS, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).
2. В меню режима настроек выберите **Другие настройки**.
3. В открывшемся окне установите флажок **Защита BIOS**.

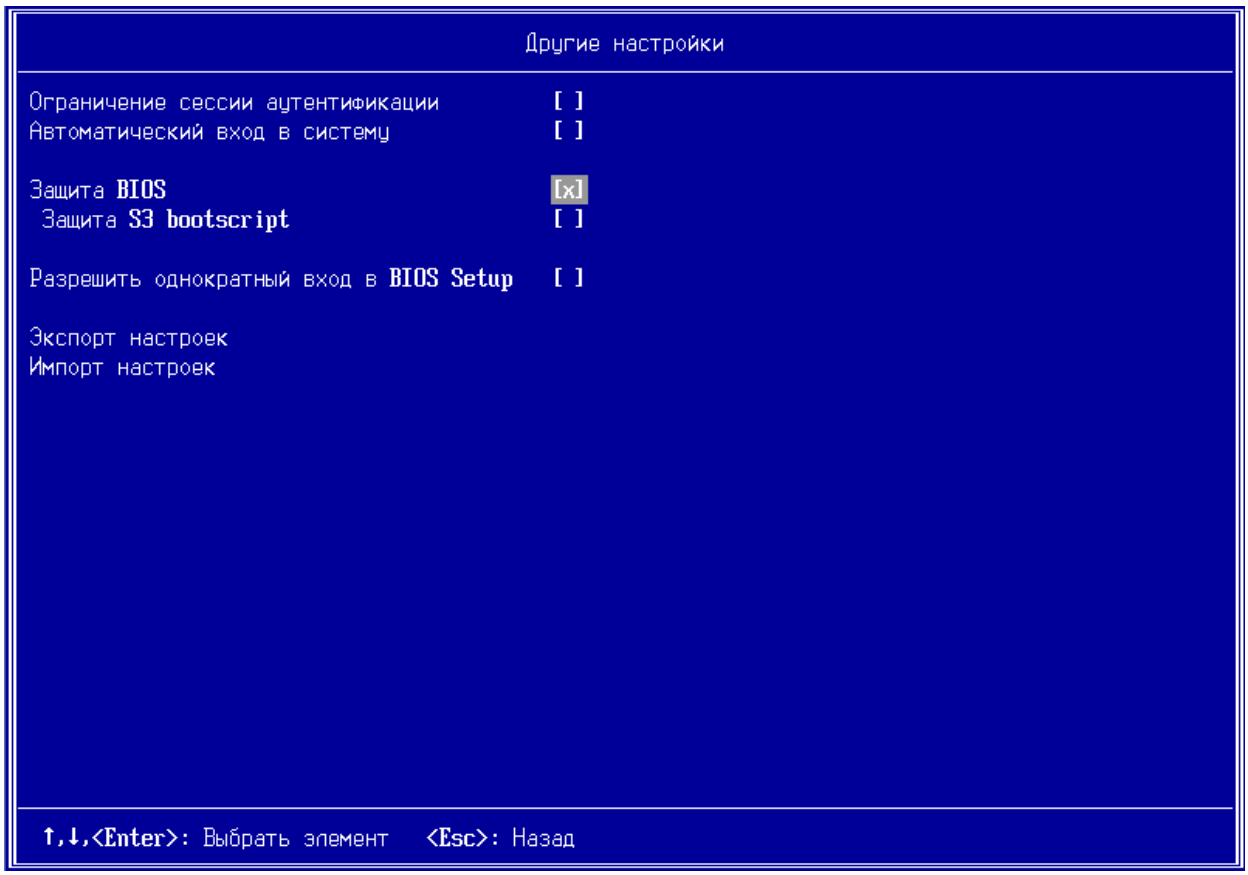


Рисунок 26. Меню Другие настройки

4. Для установки функции защиты BIOS при выходе из спящего режима, установите флажок **Защита S3 Boot Script**.
5. Для выхода в основное меню нажмите **Esc**.

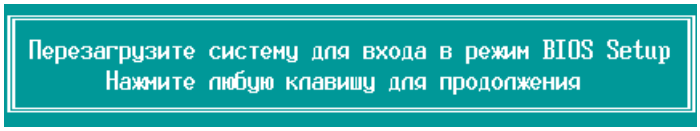
Вход в BIOS Setup

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. 30).
2. В меню режима настроек выберите **Другие настройки**.
3. В открывшемся окне установите флажок **Разрешить однократный вход в BIOS Setup**.

   Появится сообщение о необходимости перезагрузить систему:



4. Нажмите любую клавишу, затем Esc для выхода в основное меню режима настройки.
5. В меню режима настройки выберите **Перезагрузить систему**.

   После перезагрузки будет доступно меню настроек BIOS.

Экспорт настроек

Экспорт настроек осуществляется на первый найденный USB-накопитель в фиксированный файл **itsbdb.bin** (в корень раздела), также на диске появляется файл с подписью **itsbdb.sig**.

Экспортируются (и далее могут быть импортированы) следующие настройки:

- Общие настройки:
  - Параметры загрузки операционной системы;
  - Настройки процедуры входа в систему;
  - Значение режима защиты BIOS.
- Пользователи и их настройки;
- Корневые сертификаты;
- Параметры контроля целостности, списки контролируемых элементов и соответствующие контрольные суммы (в случае если в настройках Контроля целостности значение параметра – «в базе данных», в противном случае соответствующие параметры можно экспортировать/импортировать вручную, копируя соответствующие файлы – см. описание «Хранение эталонов» на стр. 58 при значении «на диске»).

Чтобы экспортировать настройки, выполните следующие действия:

1. Вставьте USB-накопитель в соответствующий разъем.
2. Войдите в режим настройки ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).
3. В меню режима настроек выберите **Другие настройки**.
4. В открывшемся окне выберите **Экспорт настроек**.

   После завершения экспорта появится следующее сообщение:

Импорт настроек

Чтобы импортировать настройки, выполните следующие действия:

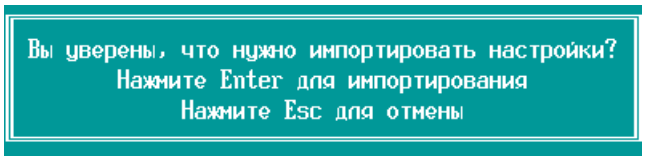
1 Вставьте USB-накопитель, содержащий файл настроек **itsbdb.bin**, в соответствующий разъем.

2 Войдите в режим настройки ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).

3 В меню режима настроек выберите **Другие настройки**.

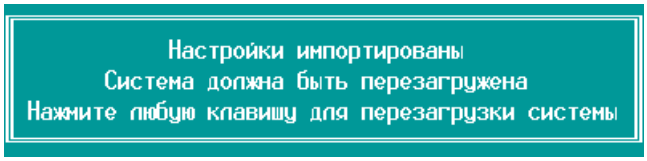
4 В открывшемся окне выберите **Импорт настроек**.

Появится окно с предупреждением:



5 Нажмите Enter.

После успешного импорта настроек появится сообщение о необходимости перезагрузить систему.



6 Нажмите любую клавишу, система перезагрузится.

5

Управление параметрами загрузки операционной системы

Режим загрузки операционной системы

ViPNet SafeBoot поддерживает следующие режимы загрузки:

- 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).

Выбор режим загрузки операционной системы зависит от способа ее установки и версии. Подробности могут быть найдены в документации по используемой операционной системе.

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. 30).

2 В меню режима настроек выберите **Параметры загрузки операционной системы**.

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

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

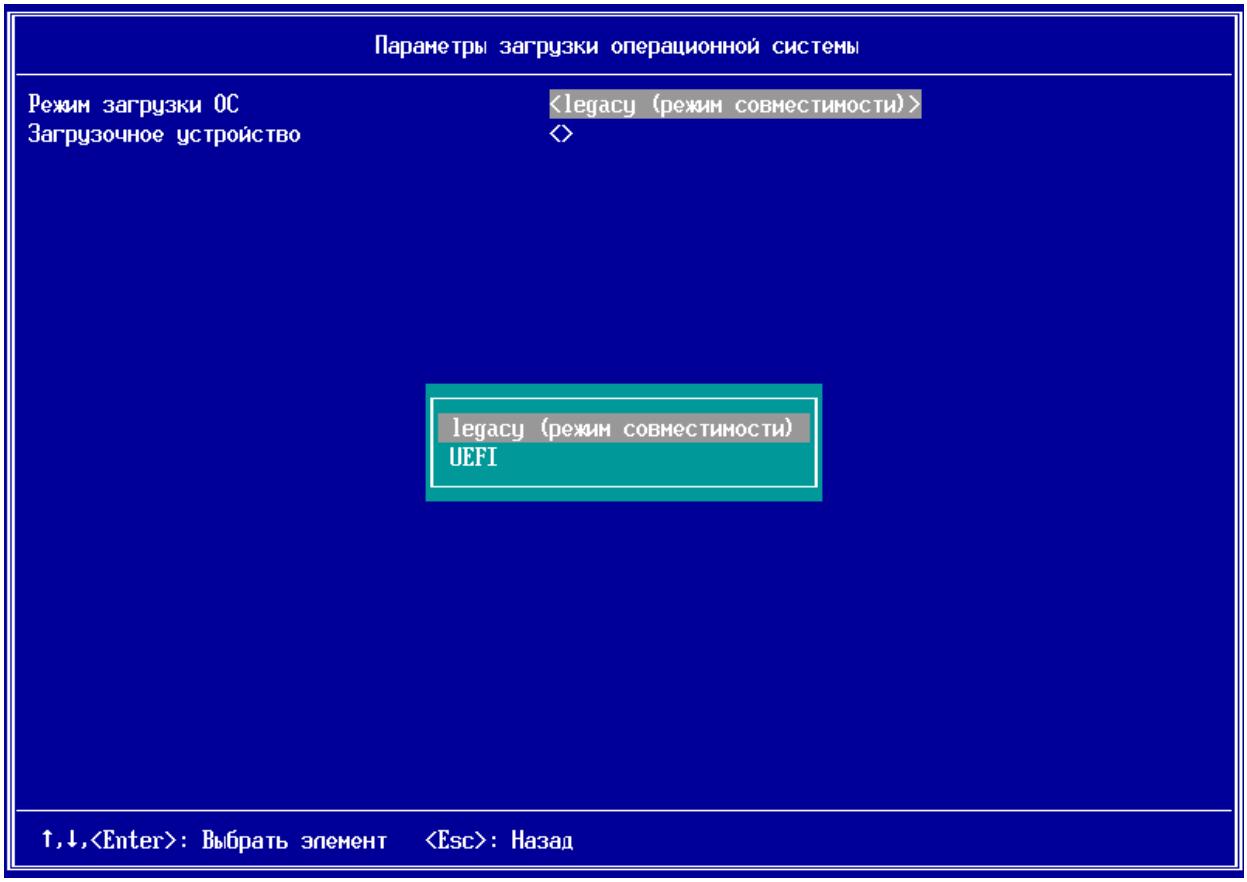


Рисунок 27. Меню выбора режима загрузки операционной системы – legacy (режима совместимости)

5 Выберите **Загрузочное устройство**.

Из списка выберите нужное загрузочное устройство.

6 Вернитесь в основное меню режима настроек ViPNet SafeBoot, нажав **Esc**.

7 Нажмите **Esc** для выхода из режима настройки и начала загрузки операционной системы в выбранном режиме.

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. 30).
2. В меню режима настроек выберите **Параметры загрузки операционной системы**.
3. В открывшемся окне выберите **Режим загрузки ОС**.
4. В меню **Режим загрузки ОС** выберите из списка **UEFI**.
5. Выберите **Загрузочный раздел (ESP)**.
6. Из открывшегося списка выберите нужное загрузочное устройство.
7. В пункте меню **Загрузчик операционной системы** выберите непосредственный файл загрузчика ОС.
8. Вернитесь в основное меню режима настроек ViPNet SafeBoot, нажав **Esc**.
9. Нажмите **Esc** для выхода из режима настройки и начала загрузки операционной системы в выбранном режиме.

6

Контроль целостности

Контролируемые объекты

ViPNet SafeBoot позволяет осуществлять контроль целостность следующих типов объектов:

- файлы на файловых системах FAT32, NTFS, EXT2, EXT3 и EXT4;
- содержимое энергонезависимой памяти CMOS;
- ресурсы конфигурационного пространства PCI/PCIe;
- таблиц ACPI;
- таблиц SMBIOS;
- карты распределения памяти;
- образ BIOS и собственных модулей ViPNet SafeBoot;
- загрузочных секторов (MBR) на носителях информации;
- 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. 57), а также выполнить перерасчет эталонов (см. «Перерасчет эталонных контрольных сумм» на стр. 56).

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. 30).

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

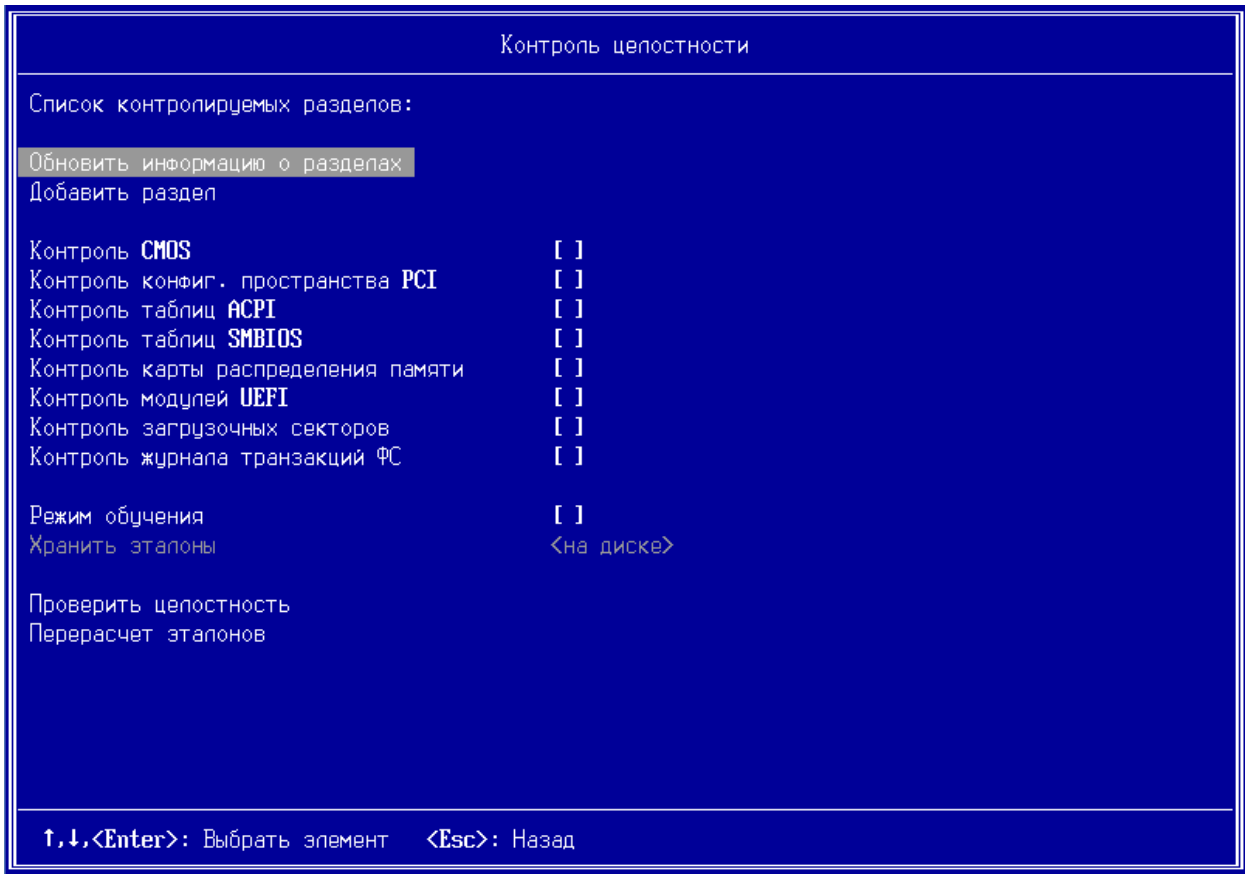


Рисунок 28. Меню Контроль целостности

3 Для контроля целостности всех разделов со списками файлов в корне, выберите пункт меню **Обновить информацию о разделах**.

4 Для добавления разделов, которые необходимо поставить на контроль, выберите **Добавить раздел**.

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

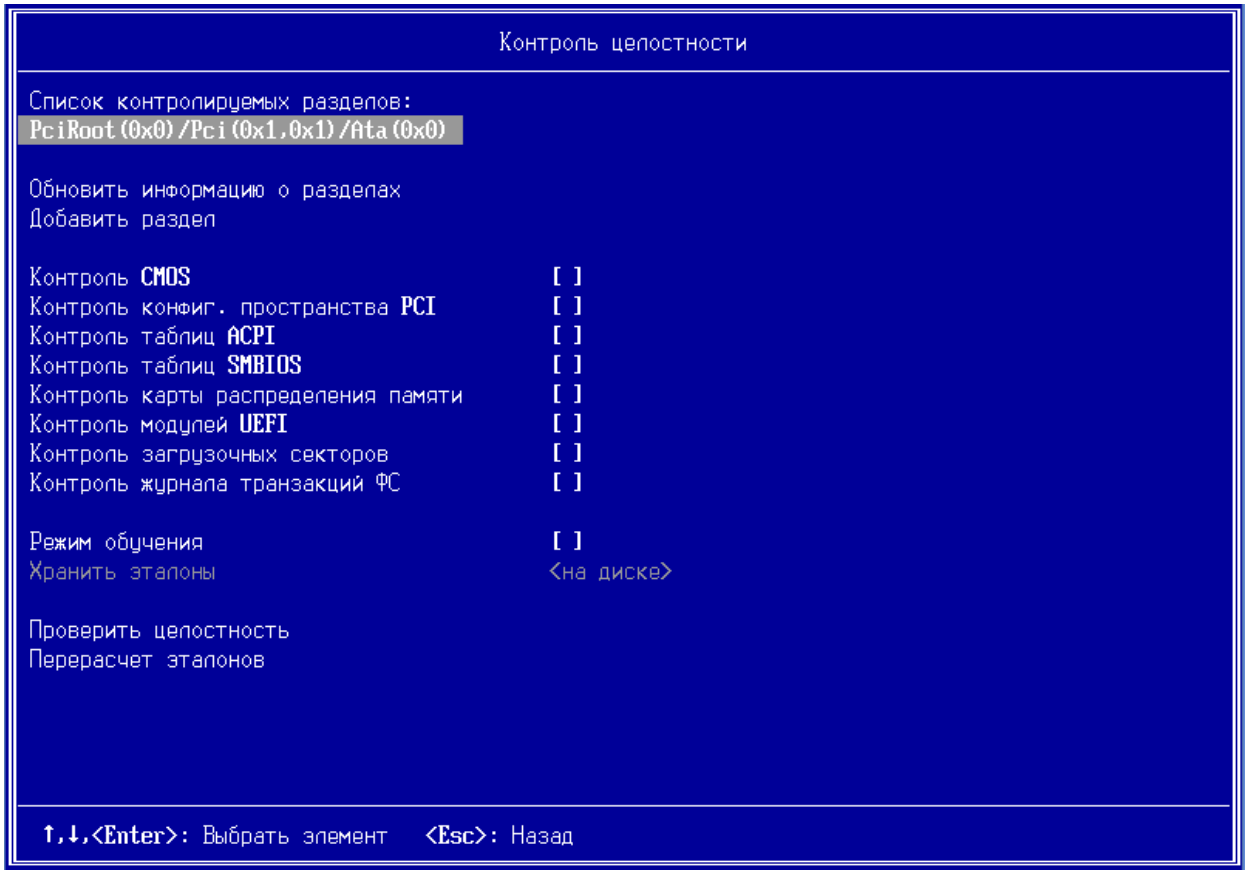


Рисунок 29. Список контролируемых разделов

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

---

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

В отрывшемся окне (см. рис. 30) доступны следующие операции над файлами:

- Список контролируемых файлов – просмотр списка контролируемых файлов на разделе файловой системы и их контрольных сумм;
- 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.

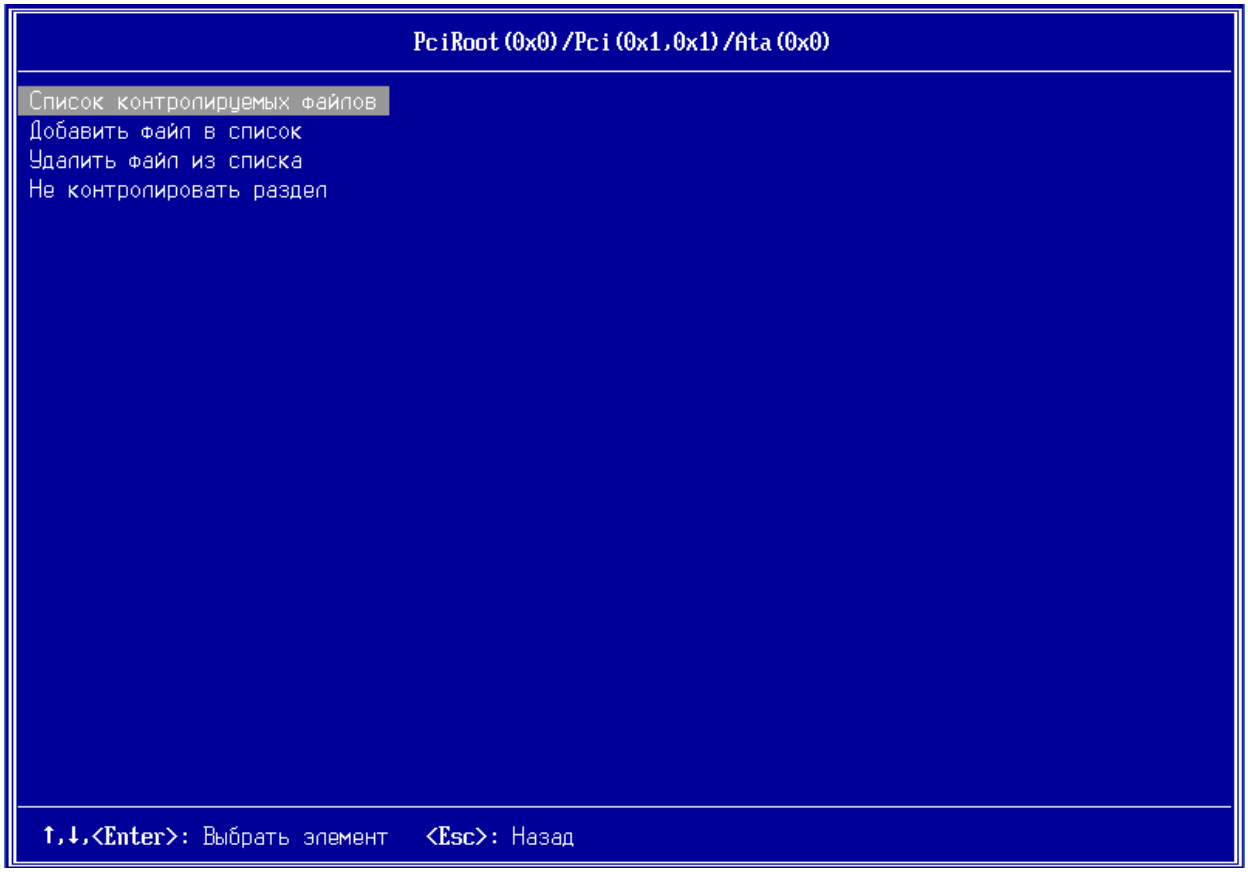


Рисунок 30. Операции контроля файлов

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.

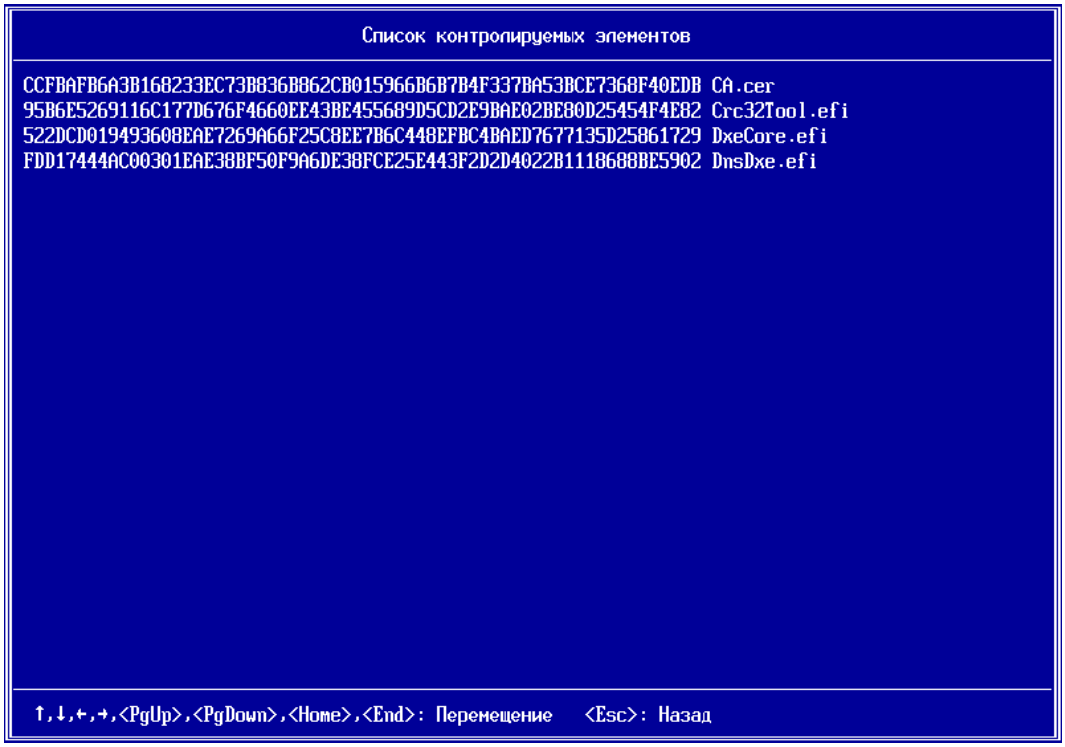


Рисунок 31. Список контролируемых файлов на разделе файловой системы

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

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

Для удаления всех файлов и раздела из списка контролируемых объектов выберите пункт **Не контролировать раздел**.

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. 30).

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

3 В меню **Контроля целостности** нажмите **Enter** на пункте **Контроль конфиг. пространства PCI**.

Система выполнит расчет контрольных сумм состава подключенных аппаратных средств.

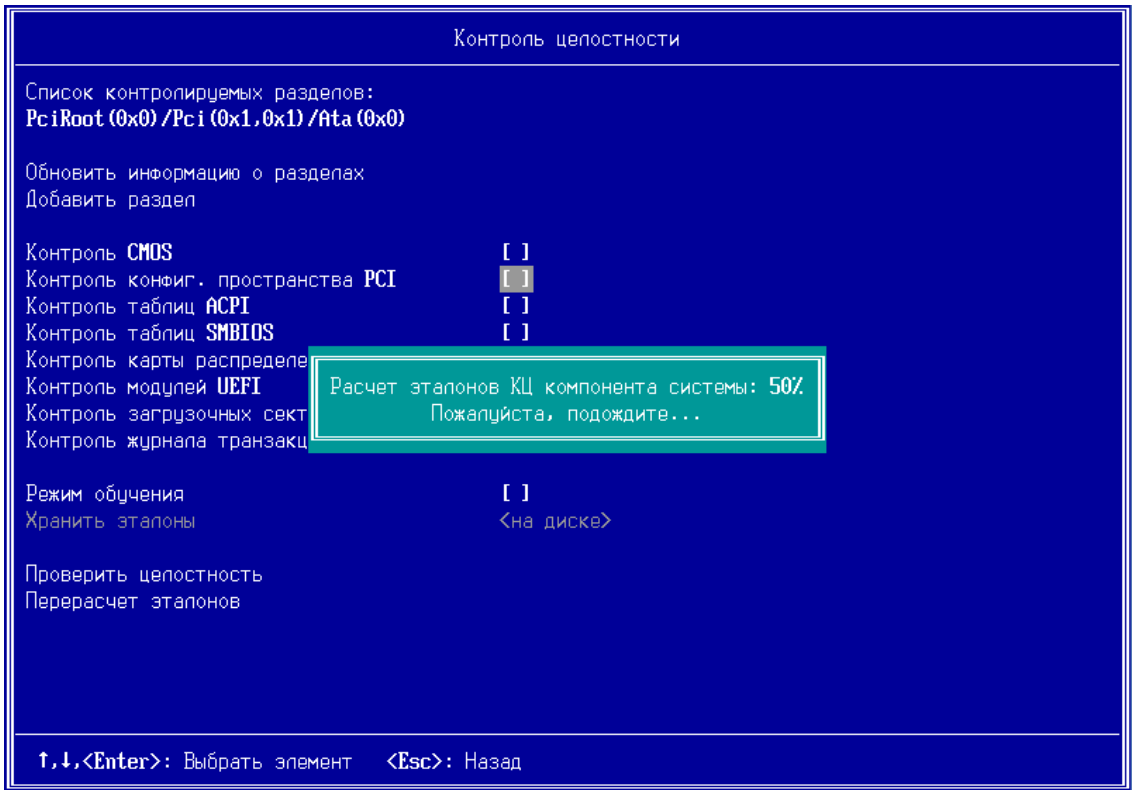


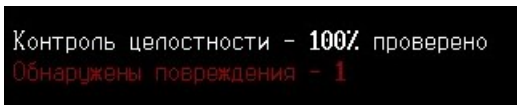
Рисунок 32. Расчет эталонов контрольных сумм состава аппаратных средств

Примечание. При установленной опции «Контроль конфиг. пространства PCI», после подключения или отключения PCI устройства, необходимо пересчитать контрольные суммы или отключить опцию «Контроль конфиг. пространства PCI».

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 ViPNet SafeBoot в журнале событий можно увидеть для каких элементов зафиксировано нарушение целостности.

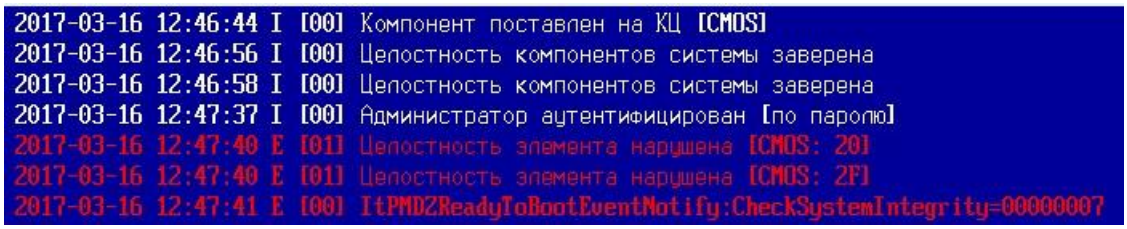


Рисунок 33. Записи в журнале событий о нарушении целостности

Для начала режима обучения выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).
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** нажмите **Enter** на пункте **Режим обучения**.

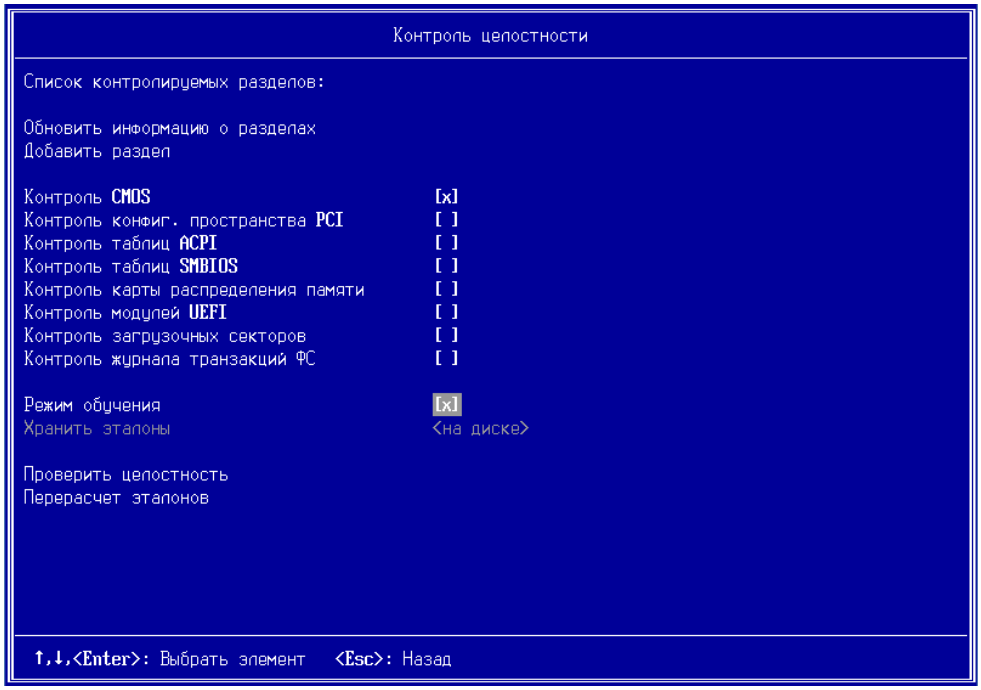
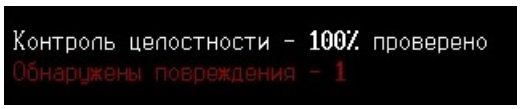


*Рисунок 34. Включение опции **Режим обучения***

При обнаружении нарушения целостности контролируемых элементов, на экране появится ошибка:



Загрузка операционной системы будет продолжена. После перезагрузки ViPNet SafeBoot в журнале событий можно будет увидеть сообщение о снятых с контроля целостности элементах.

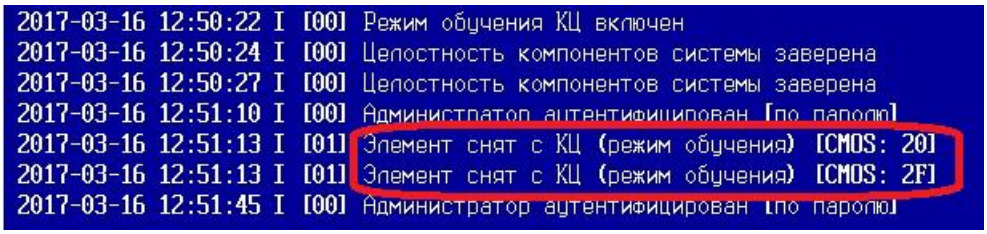


Рисунок 35. Записи в журнале событий о снятых с контроля целостности элементах

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**.

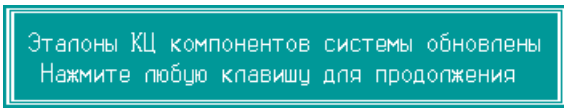
Примечание. Для того чтобы вновь поставить на контроль целостности элементы, снятые режимом обучения, следует в меню Контроль целостности снять с контроля компонент, измененный режимом обучения, а затем опять поставить его на контроль.

Перерасчет эталонных контрольных сумм

В случае обновления или штатного изменения конфигурации системы, Администратор имеет возможность провести перерасчет эталонов контролируемых объектов без необходимости снова ставить их на контроль.

Чтобы пересчитать эталонные контрольные суммы, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).
2. В меню режима настроек выберите **Контроль целостности**.
3. В открывшемся окне выберите **Перерасчет эталонов**.
4. Дождитесь появления на экране сообщения:



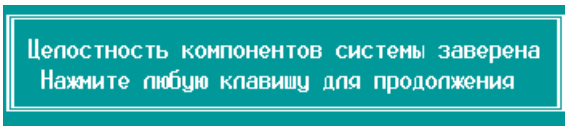
Принудительная проверка целостности

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. 30).
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 непродолжительного времени проверка целостности будет завершена и появится следующее сообщение:

5. Нажмите любую клавишу, затем Esc для выхода в основное меню.

Хранение эталонов

Для параметра **Хранение эталонов** можно выбрать следующие значения:

- на диске;
- в базе данных.

Хранение эталонов по умолчанию осуществляется **на диске**. Вся соответствующая информация сохраняется на диск в подписанном виде: информация, необходимая для контроля целостности файлов, находится в файлах **files**, **files.sig** в корне каждого контролируемого раздела, а вся остальная информация в каталоге – **EFI\Infotecs\etalons**.

В случае, если было выбрано хранение эталонов **в базе данных**, вся необходимая для контроля целостности информация, включая списки контролируемых элементов и их эталонные значения (хэши), хранится во внутренней базе данных ПМДЗ (в NVRAM – памяти BIOS).

Примечание. Размер NVRAM ограничен. Не стоит выбирать значение параметра **в базе данных** без необходимости, особенно в случае большого количества контролируемых элементов.

7

Управление учетными записями пользователей

Учетные записи пользователей

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

- Имя учетной записи (также известное как логин пользователя).
- 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! В изделии возможен только один пользователь с ролью Администратор. Общее максимальное количество пользователей 32.

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. 30).

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

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

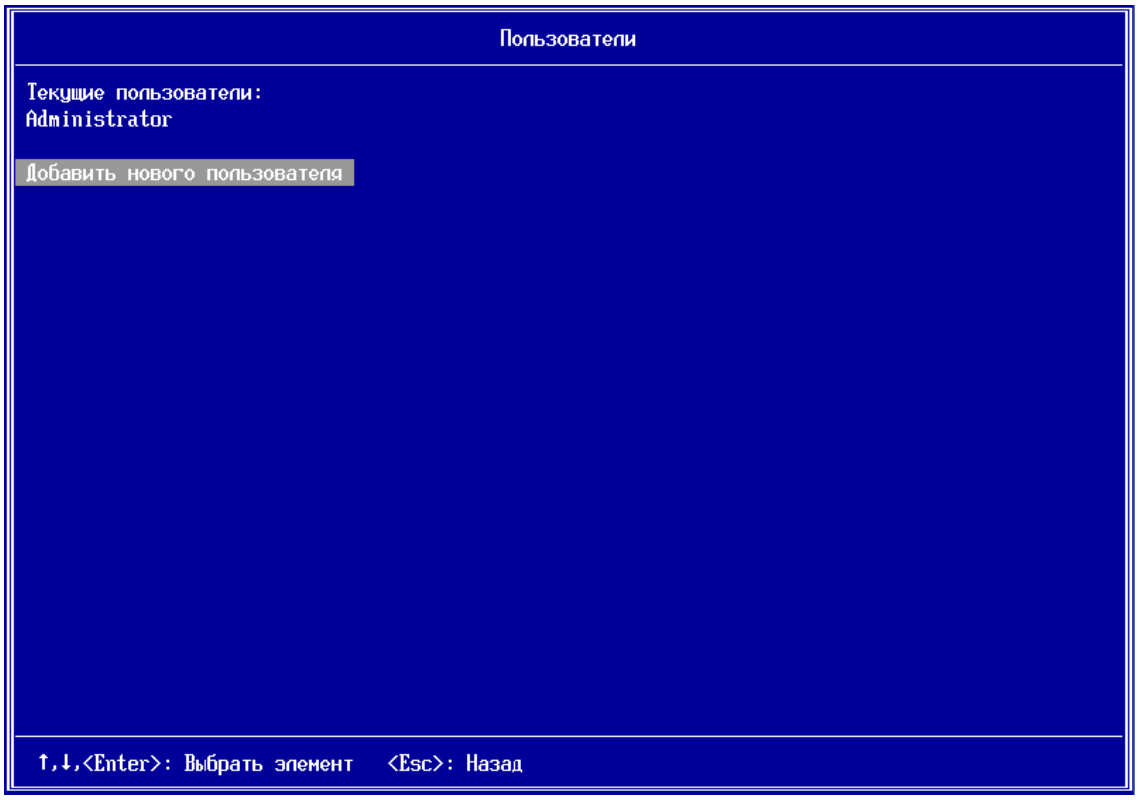


Рисунок 36. Добавление нового пользователя

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

Введите имя пользователя.

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

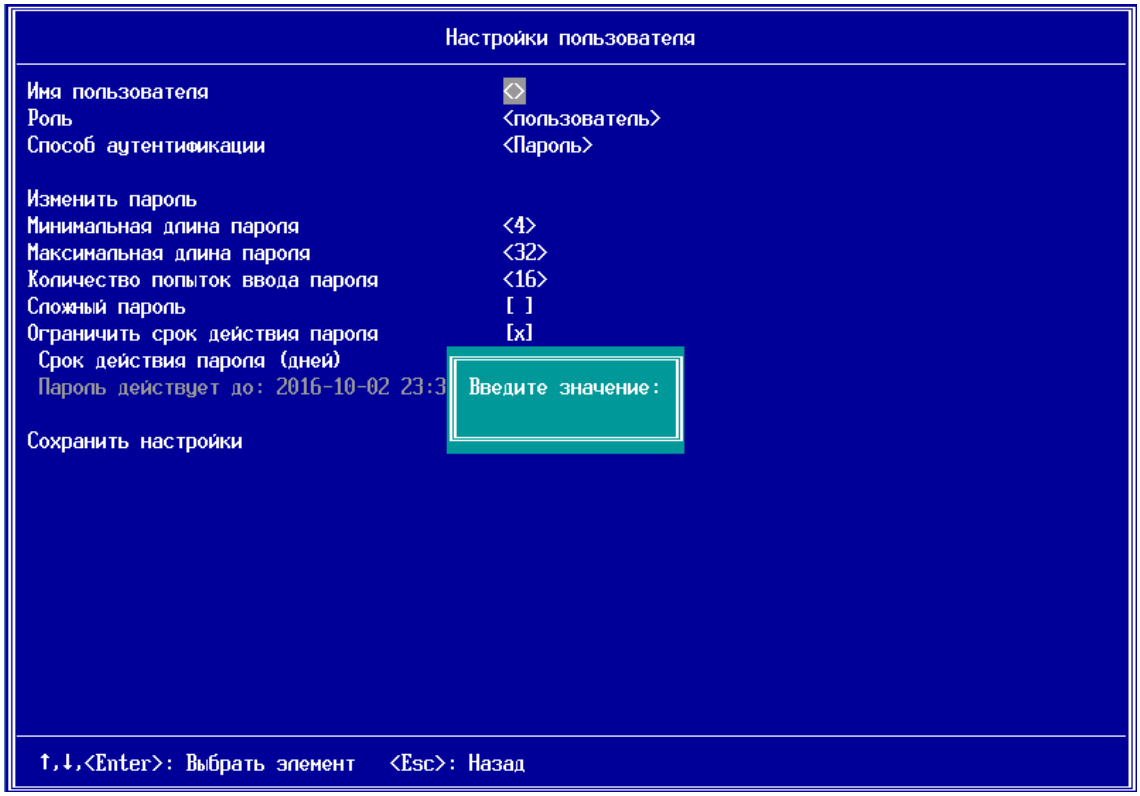
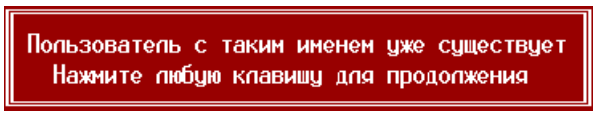


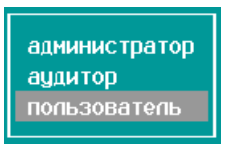
Рисунок 37. Приглашение ввести Имя пользователя

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



5 Выберите элемент **Роль**.

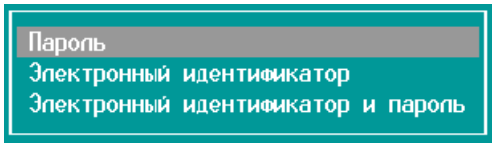
В открывшемся списке выберите роль:



Внимание! В изделии возможен только один пользователь с ролью Администратор. Общее максимальное количество пользователей 32.

6 Выберите элемент **Способ аутентификации**.

В открывшемся списке выберите способ аутентификации **Пароль**:



7 Выберите элемент **Изменить пароль**.

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

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

Ограничения, действующие при создании пароля для администратора и аудитора:

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

7.1 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.

7.2 Для ограничения количества попыток ввода пароля выберите соответствующий элемент 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.

---

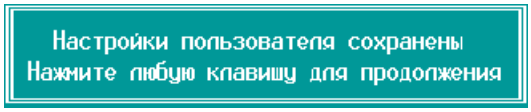
8 Измените настройки ограничения срока действия пароля или оставьте значение по умолчанию.

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

8.2 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 соответствующе сообщение о необходимости смены пароля, пользователь блокируется до смены пароля.

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



10 Нажмите любую клавишу, затем **Esc** для выхода в меню **Пользователи**.

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. 30).

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

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

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

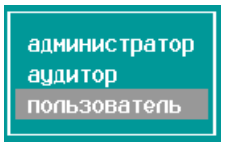
Введите имя пользователя.

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

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

5 Выберите элемент **Роль**.

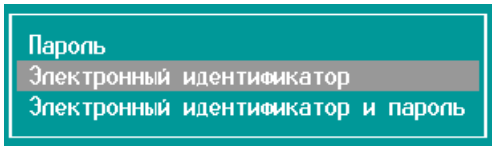
В открывшемся списке выберите роль:



Внимание! В изделии возможен только один пользователь с ролью Администратор. Общее максимальное количество пользователей 32.

6 Выберите элемент **Способ аутентификации**.

В открывшемся списке выберите способ аутентификации **Электронный идентификатор**:



Меню **Настройки пользователя** примет следующий вид:

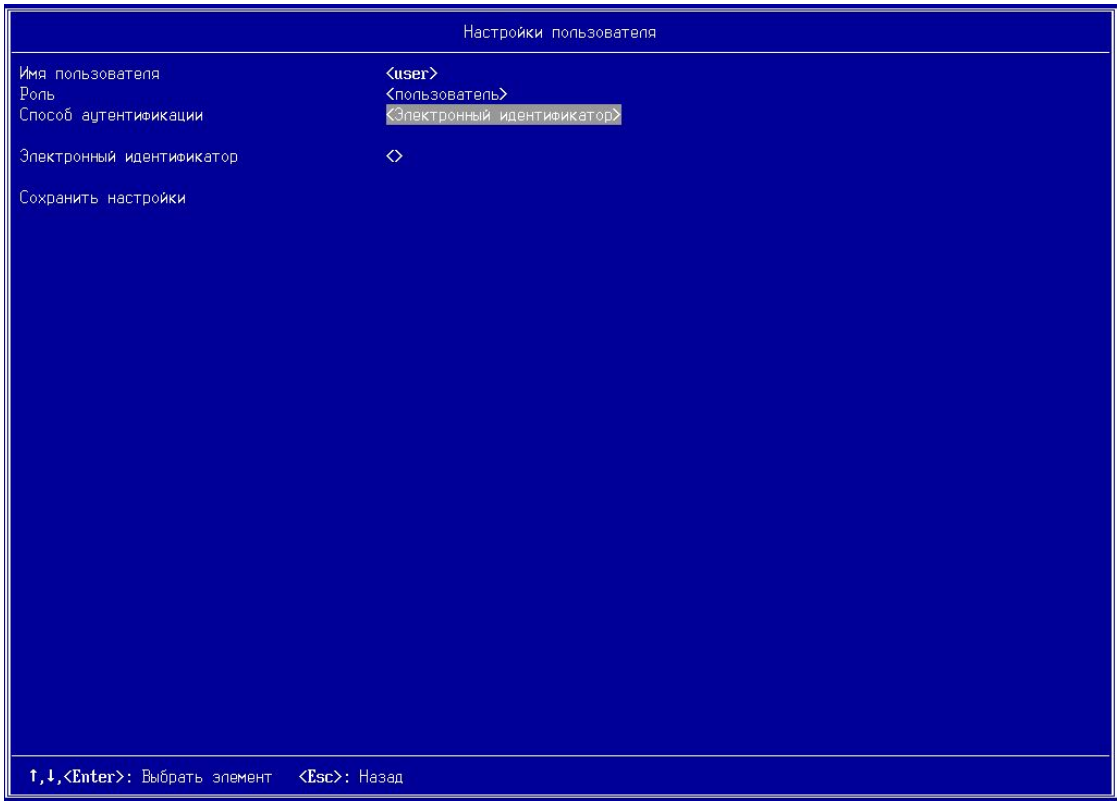


Рисунок 38. Меню Настройки пользователя при выбранном способе аутентификации Электронный идентификатор

Внимание! Перед созданием пользователей с аутентификацией по электронному идентификатору, необходимо установить корневые сертификаты (см. на стр. 70).

7 Настройки при использовании электронного идентификатора Guardant Id.

7.1 Выберите элемент **Электронный идентификатор**.

Примечание. Перед инициализацией электронного идентификатора Guardant Id необходимо подготовить USB-диск, на котором должны быть сохранены ключевой контейнер, сформированный средствами ViPNet CSP, и сертификат.

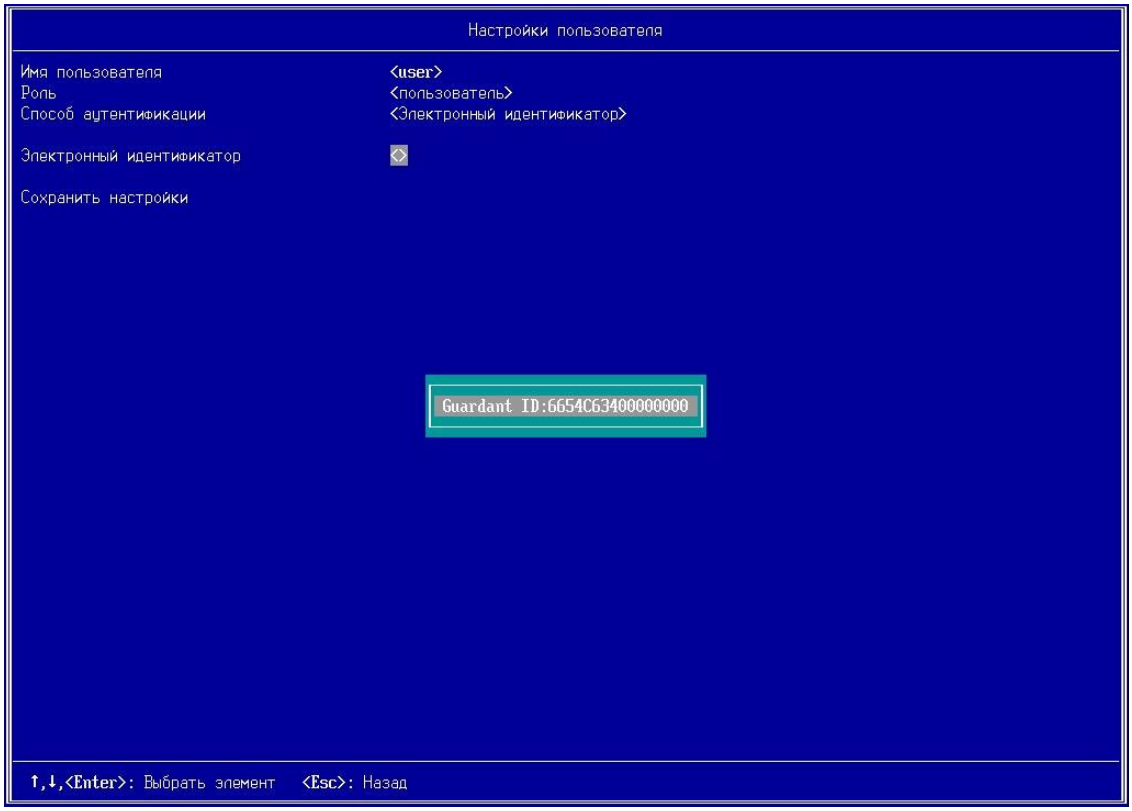


Рисунок 39. Выбор в качестве электронного идентификатора Guardant Id

7.2 После приглашения ввести PIN, введите текущий PIN-код для установленного Guardant Id.

При неправильно введенном PIN-коде появится сообщение об ошибке:

Нажмите любую клавишу.

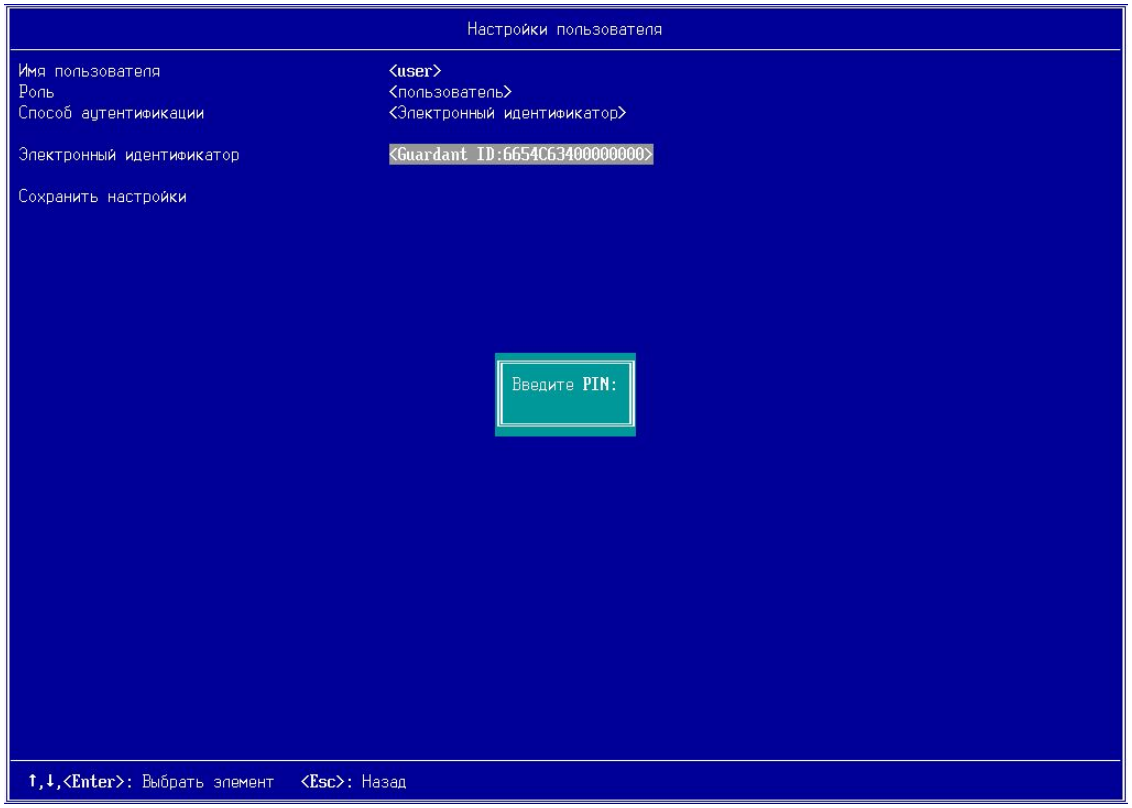


Рисунок 40. Приглашения ввести текущий PIN-код электронного идентификатора

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

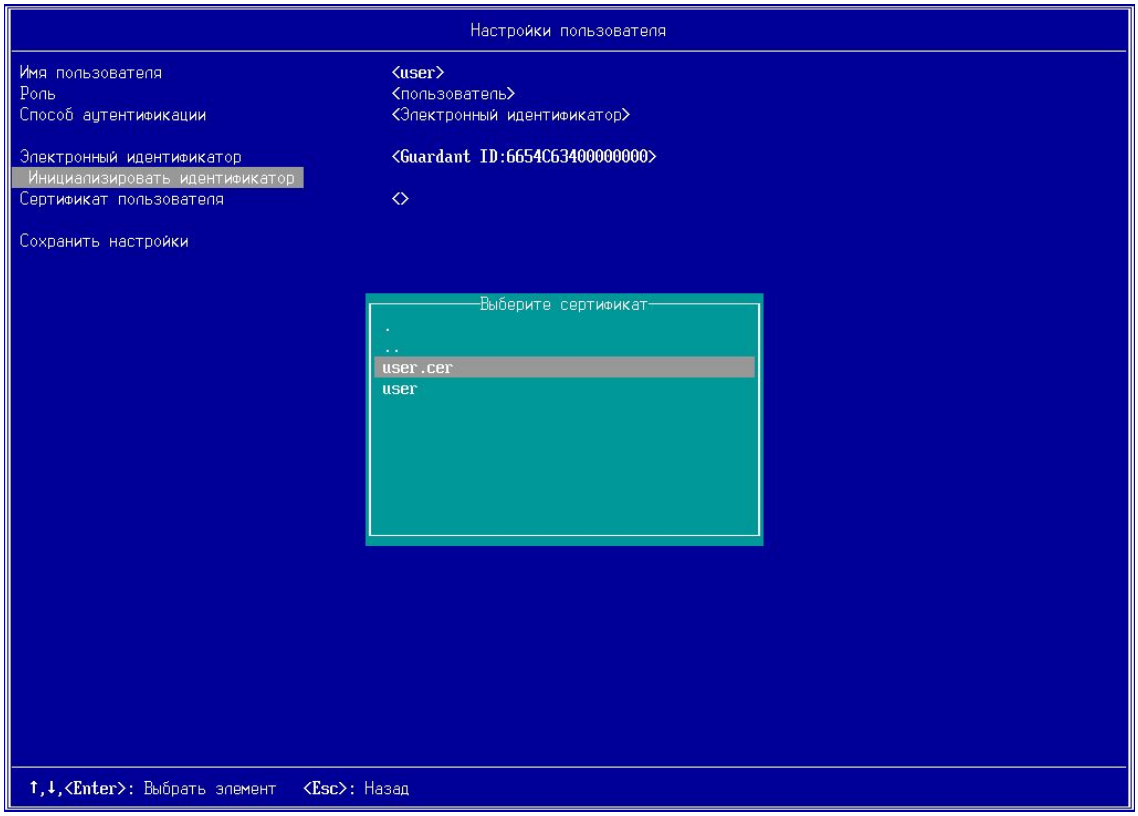


Рисунок 41. Выбор сертификата пользователя.

7.4 Выберите ключевой контейнер, соответствующий сертификату.

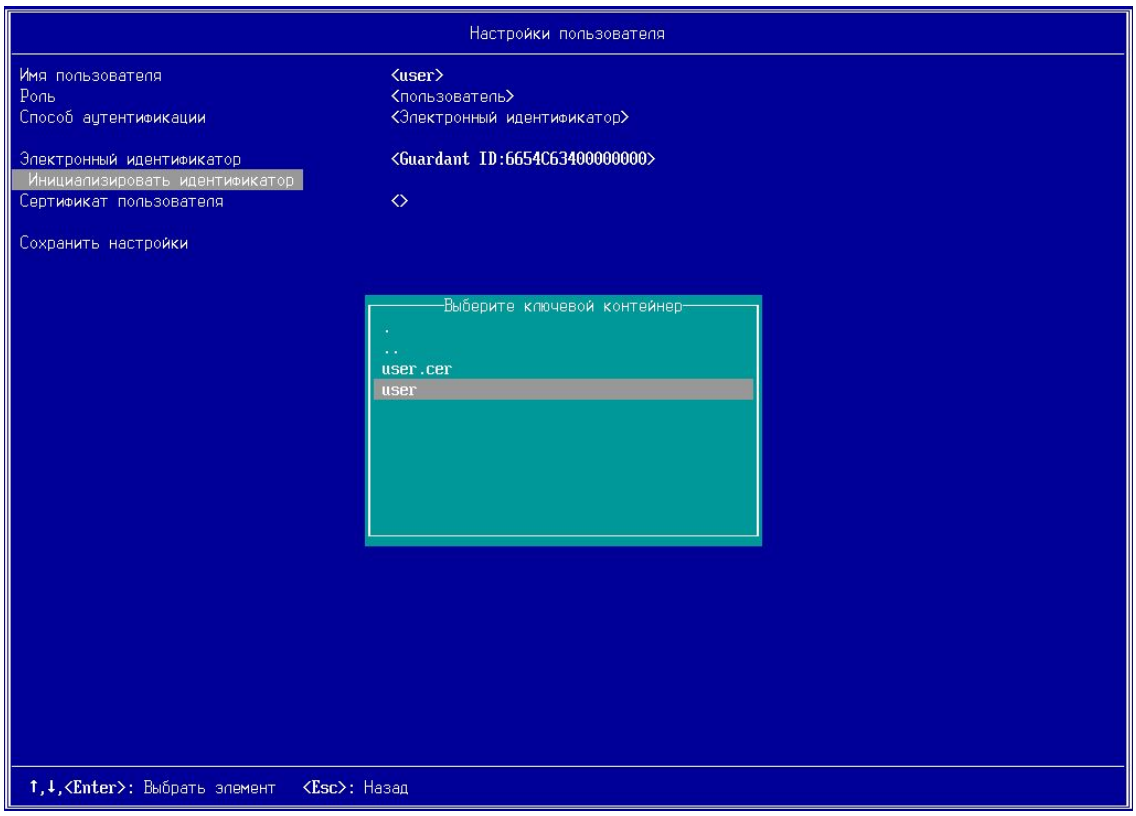


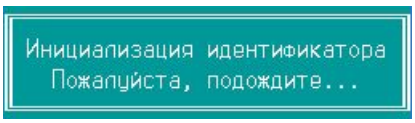
Рисунок 42. Выбор ключевого контейнера

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

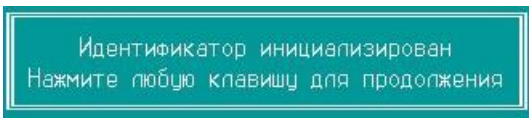
Появится сообщение о смене PIN-кода электронного идентификатора на соответствующий PIN-код контейнера:

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

7.6 Нажмите **Enter**. На экране появится сообщение об инициализации идентификатора:



7.7 Дождитесь сообщения об окончании инициализации:



Нажмите любую клавишу.

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

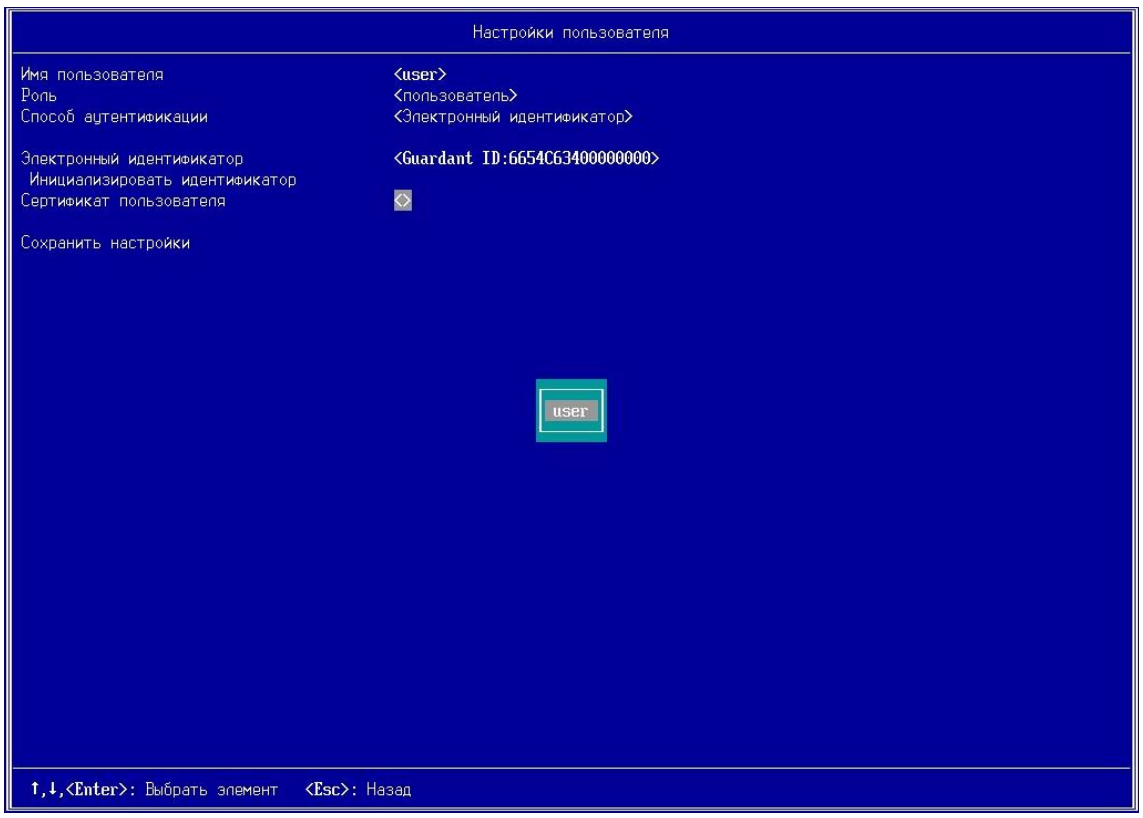
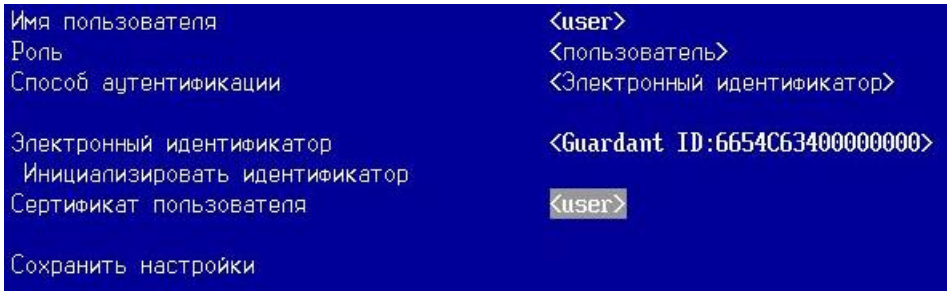


Рисунок 43. Выбор сертификата пользователя

Назначенный сертификат появится в строке **Сертификат пользователя**:



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

8.1 Выберите элемент **Электронный идентификатор**.

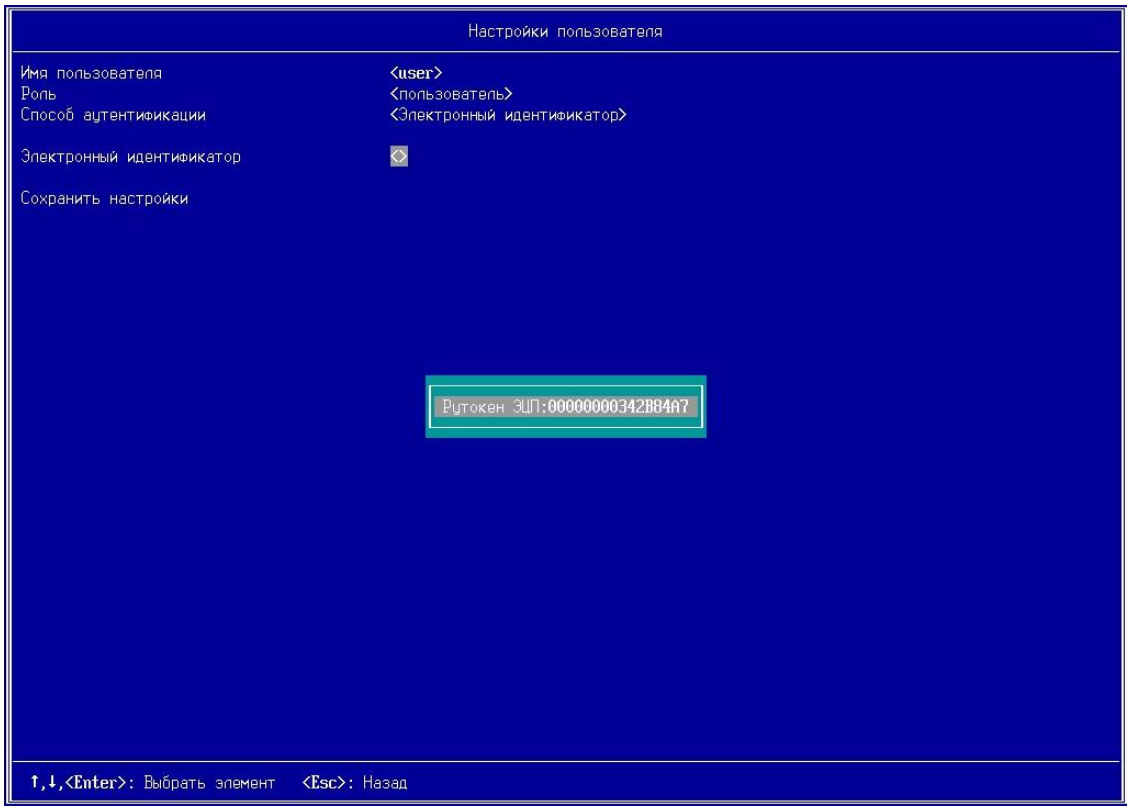


Рисунок 44. Выбор в качестве электронного идентификатора Рутокен ЭЦП

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

При неправильно введенном PIN-коде появится сообщение об ошибке:

Нажмите любую клавишу.

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

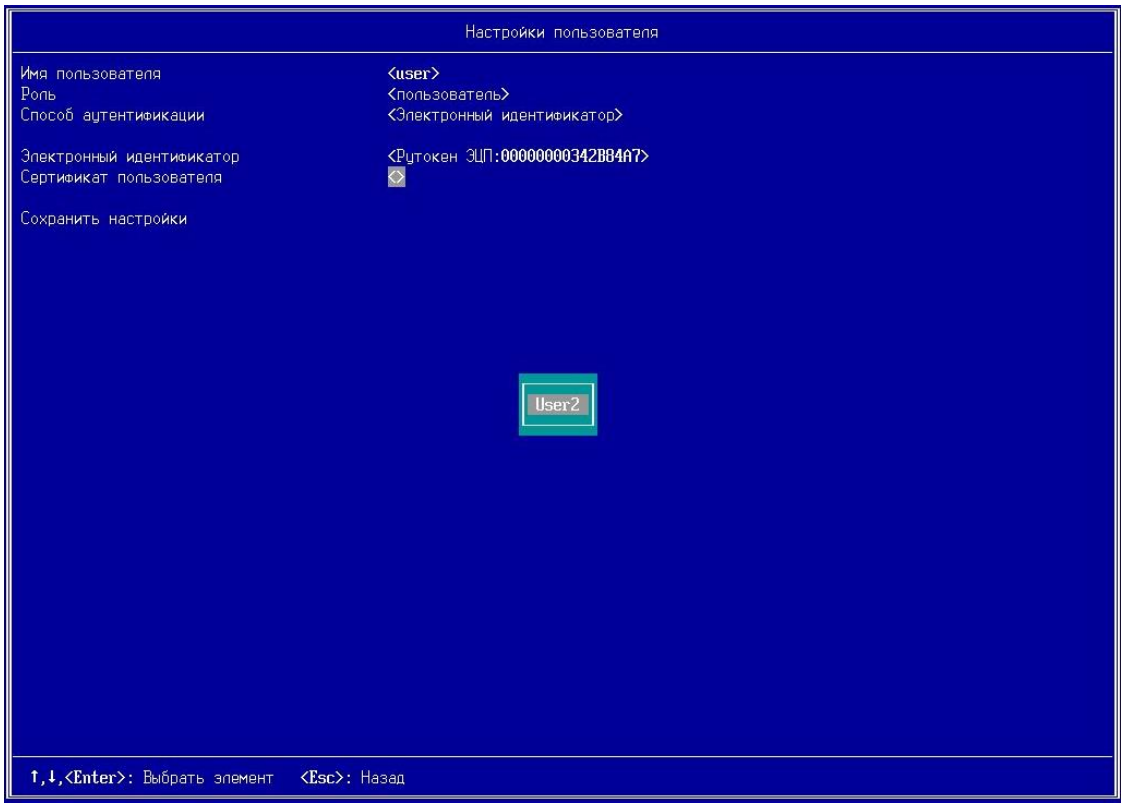
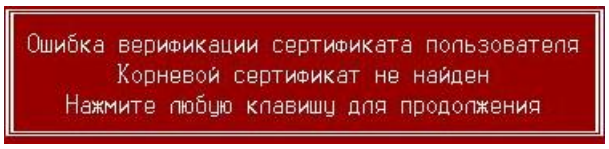


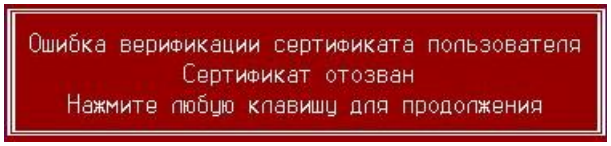
Рисунок 45. Выбор сертификата пользователя

Если корневой сертификат отсутствует, появится сообщение об ошибке:



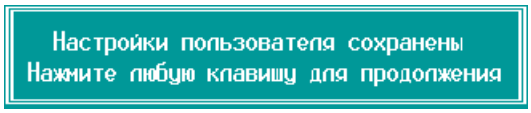
Если сертификат просрочен, появится следующее сообщение:

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**:

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



10 Нажмите любую клавишу, затем **Esc** для выхода в меню **Пользователи**.

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, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).

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

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

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

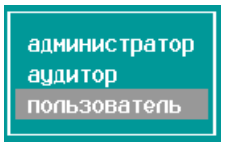
Введите имя пользователя.

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

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

5 Выберите элемент **Роль**.

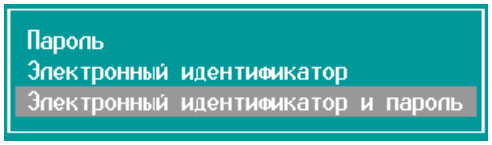
В открывшемся списке выберите роль:



Внимание! В изделии возможен только один пользователь с ролью Администратор. Общее максимальное количество пользователей 32.

6 Выберите элемент **Способ аутентификации**.

В открывшемся списке выберите способ аутентификации **Электронный идентификатор и пароль**:



Меню **Настройки пользователя** примет следующий вид:

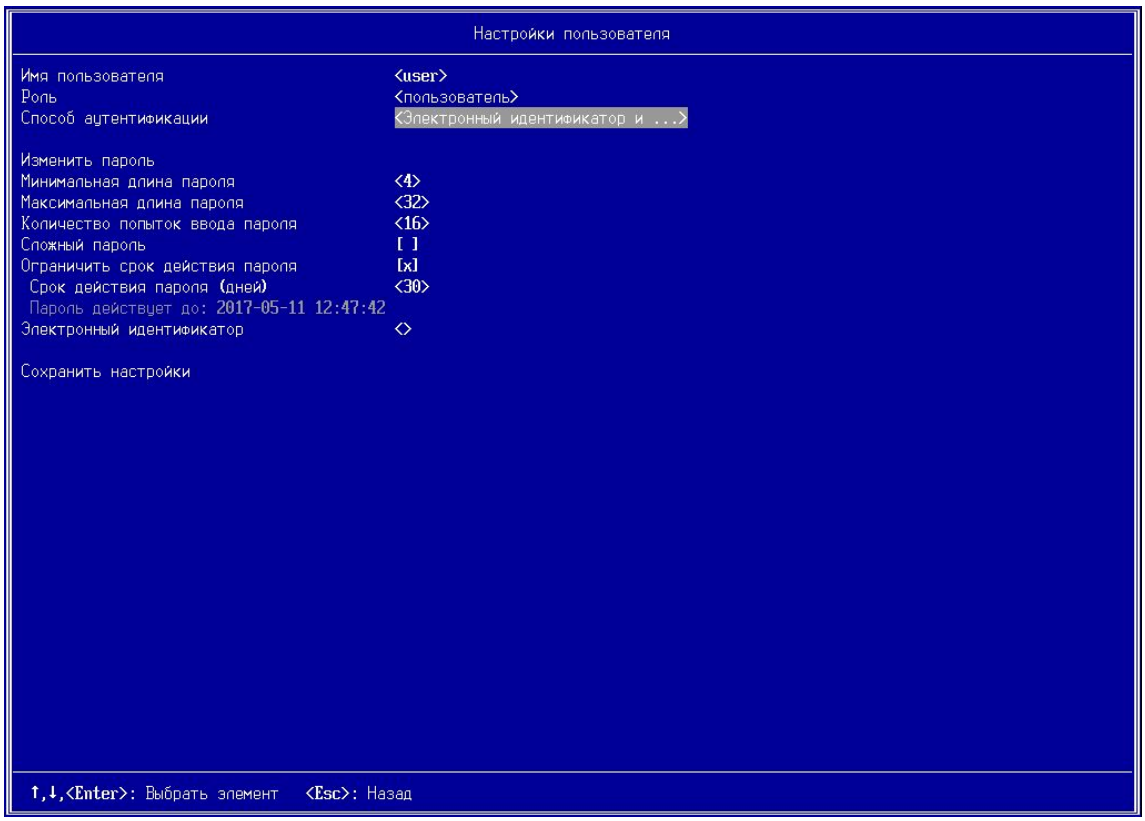


Рисунок 46. Меню Настройки пользователя при выбранном способе аутентификации Электронный идентификатор и пароль

7 Выберите элемент **Электронный идентификатор**.

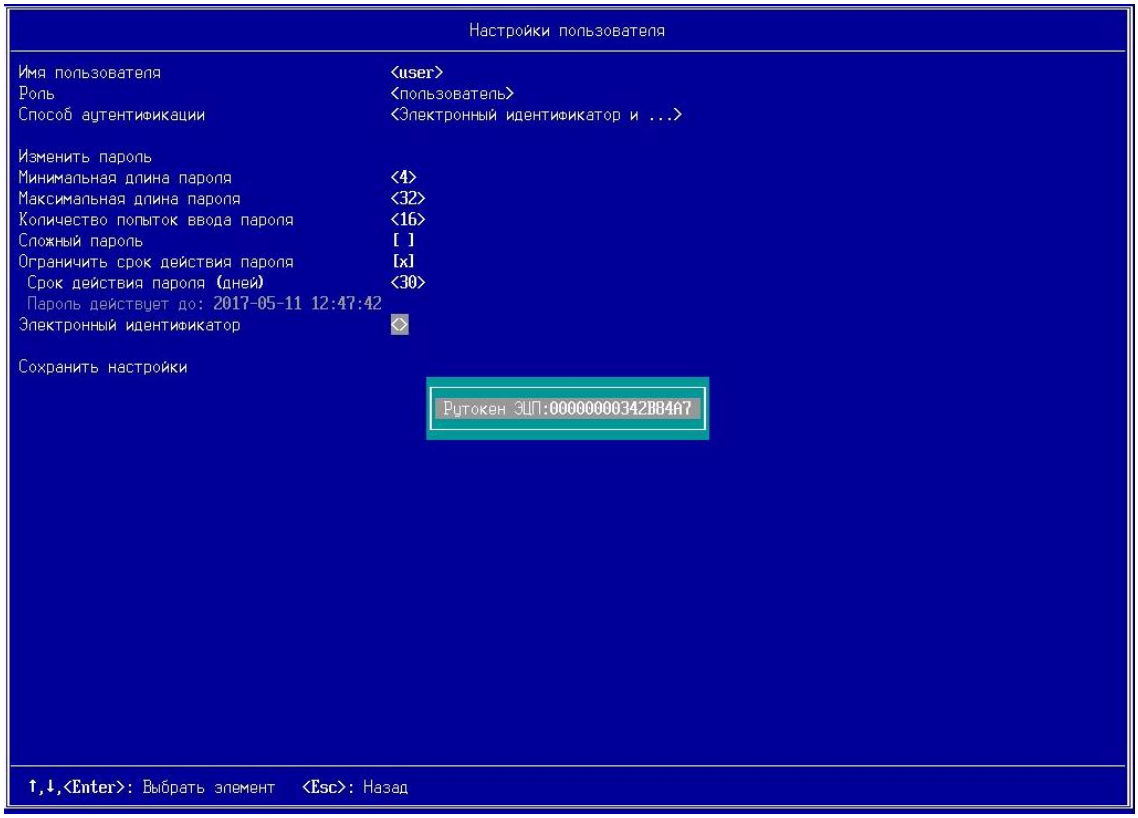


Рисунок 47. Выбор в качестве электронного идентификатора Рутокен ЭЦП

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

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

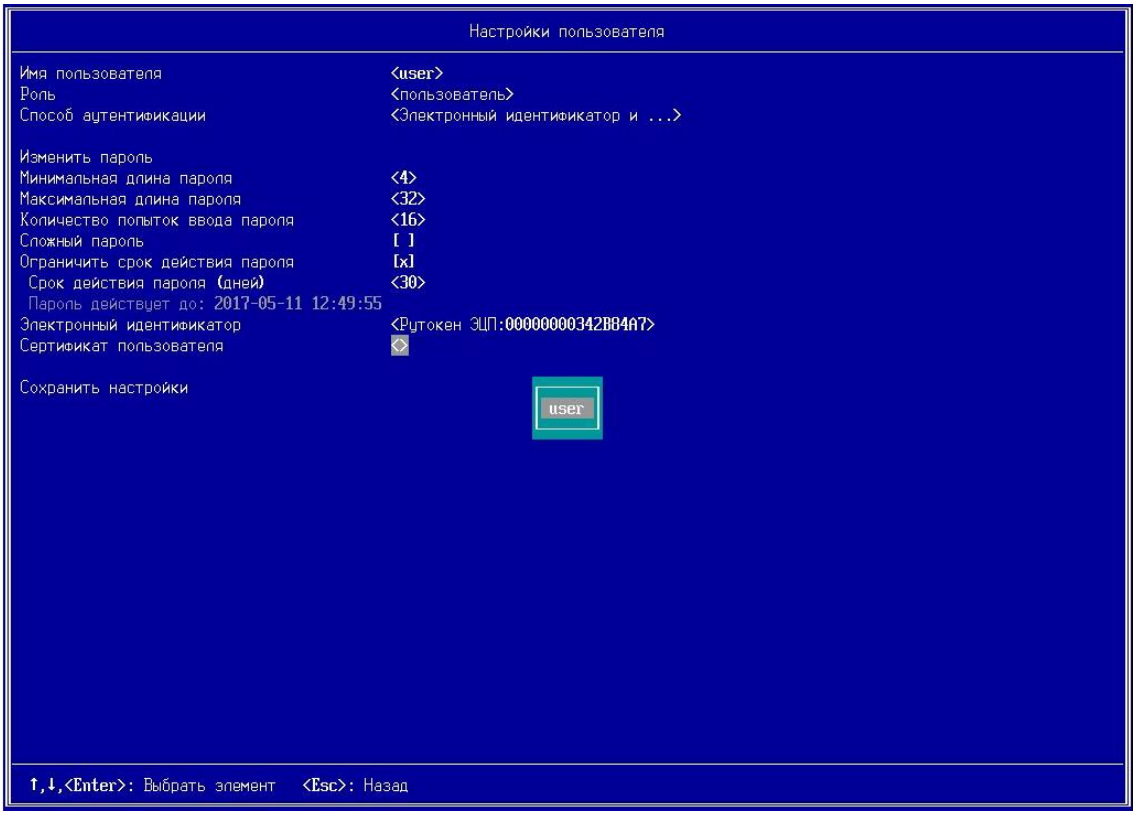
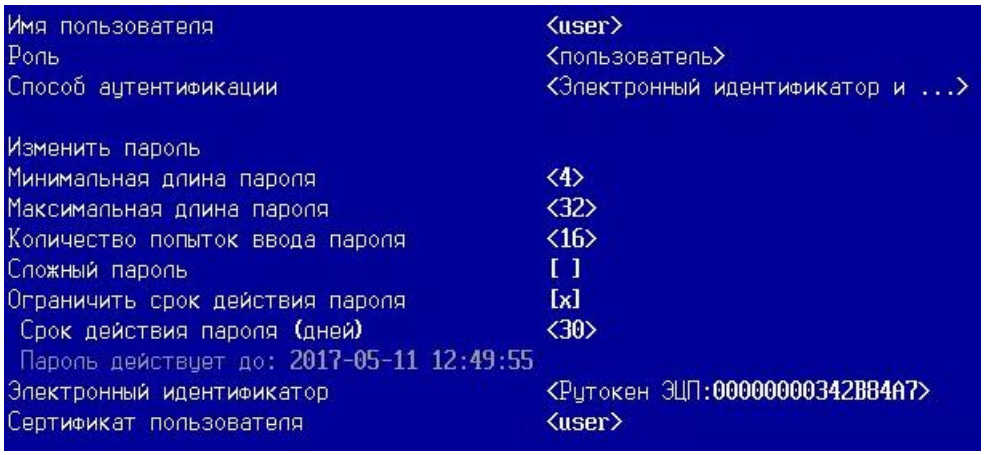


Рисунок 48. Выбор сертификата пользователя

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



10 Выберите элемент **Изменить пароль**.

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

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

Ограничения, действующие при создании пароля для администратора и аудитора:

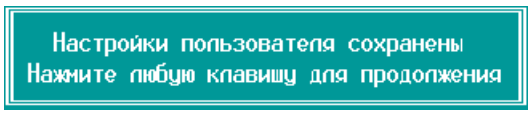
- минимальная длина пароля — 8 символов;
- максимальная длина пароля — 32 символа.

10.1 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 любую клавишу, затем **Esc** для выхода в меню **Пользователи**.

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

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. 30).
2. В меню режима настроек выберите **Пользователи**.
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. 30).
2. Подключите электронный идентификатор, назначенный пользователю.
3. В меню режима настроек выберите **Пользователи**.
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:

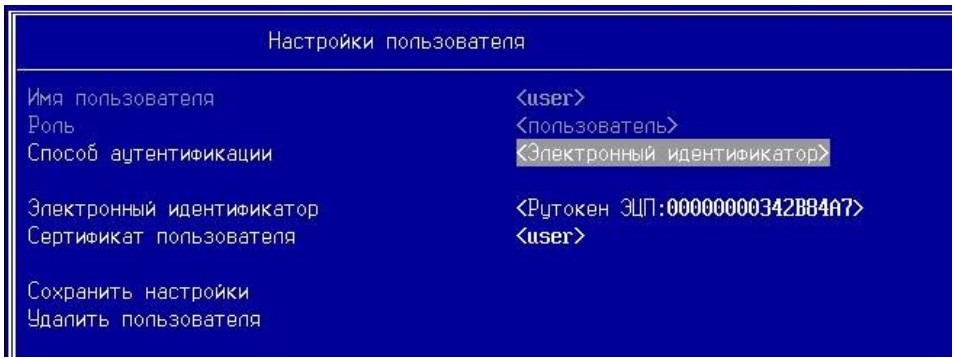


Рисунок 49. Вход в настройки пользователя с вводом PIN-кода

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

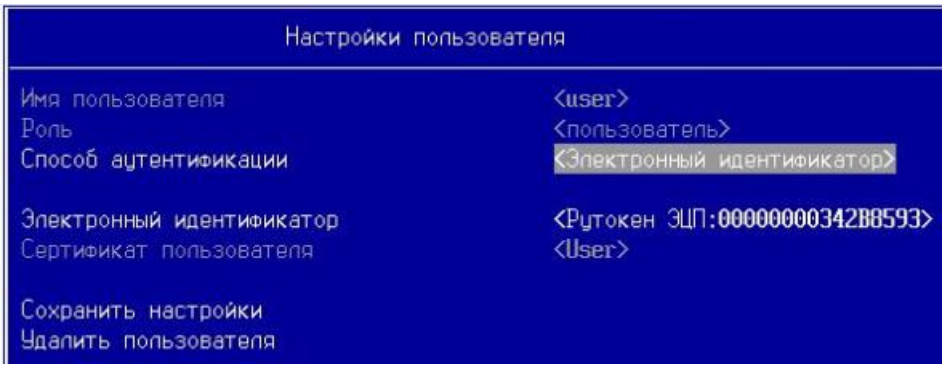


Рисунок 50. Вход в настройки пользователя без ввода PIN-кода (электронный идентификатор не подключен)

7 Выполненные изменения необходимо сохранить, выбрав **Сохранить настройки.**

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. 30).
2. В меню режима настроек выберите **Пользователи**.
3. В открывшемся окне выберите из списка **Текущие пользователи** имя пользователя, которого необходимо удалить.
4. В окне **Настройки пользователя** выберите **Удалить пользователя.**

   Появится следующая надпись:

   После подтверждения учетная запись пользователя будет удалена.

8

Управление сертификатами

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. Формат сертификата, используемый в ViPNet SafeBoot – формат X.509 (DER или PEM). Корневые сертификаты используются в случае аутентификации пользователей по электронному идентификатору. 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, от имени которого был выдан сертификат пользователя, 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. 30).
2. В меню режима настроек выберите **Корневые сертификаты**.
3. В открывшемся окне выберите **Установить корневой сертификат**.
4. Из списка выберите файл сертификата.

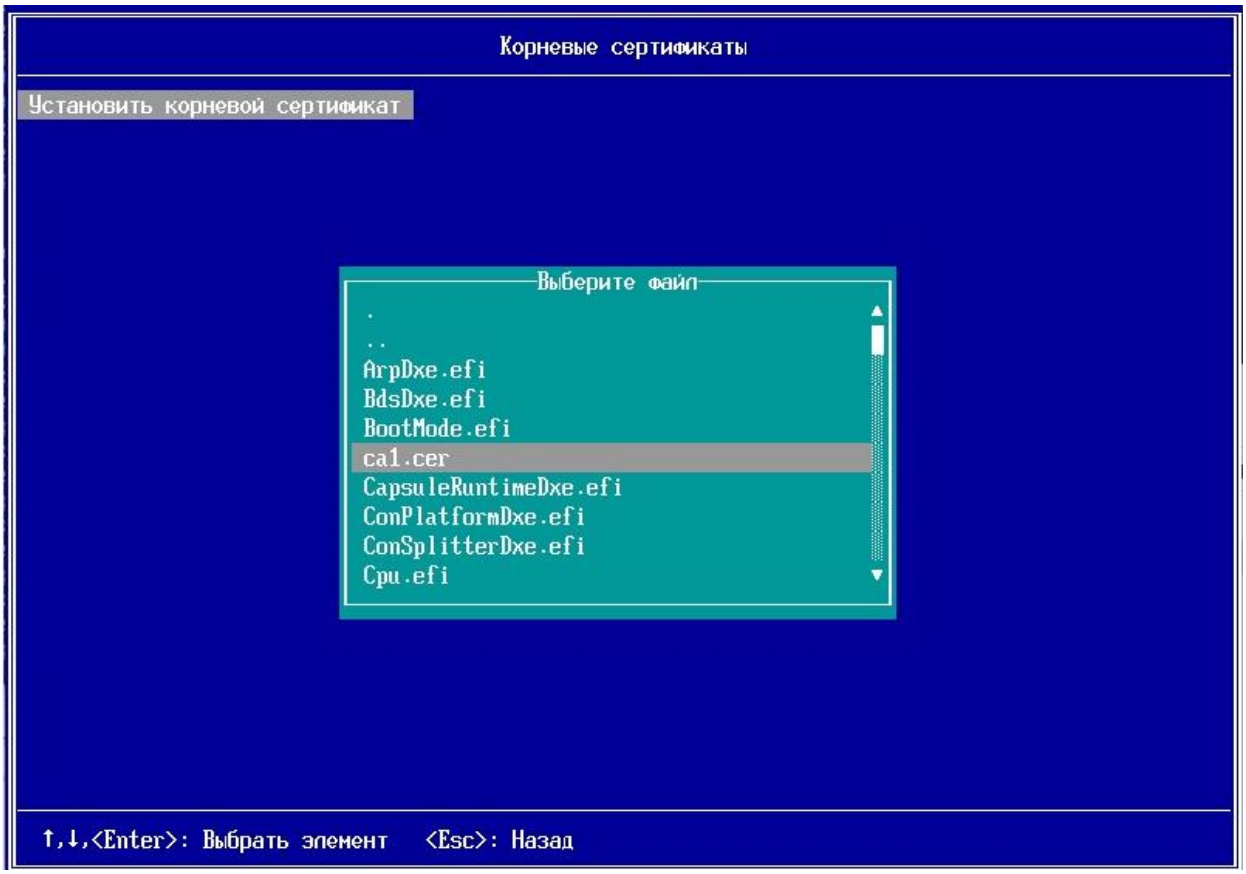


Рисунок 51. Выбор корневого сертификата

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

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. 30).
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 текущий корневой сертификат**

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

Операции со списком отозванных сертификатов (CRL)

Установка CRL

Чтобы установить CRL, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).

2 В меню режима настроек выберите **Корневые сертификаты**.

3 В открывшемся окне из списка **Установленные корневые сертификаты** выберите нужный сертификат.

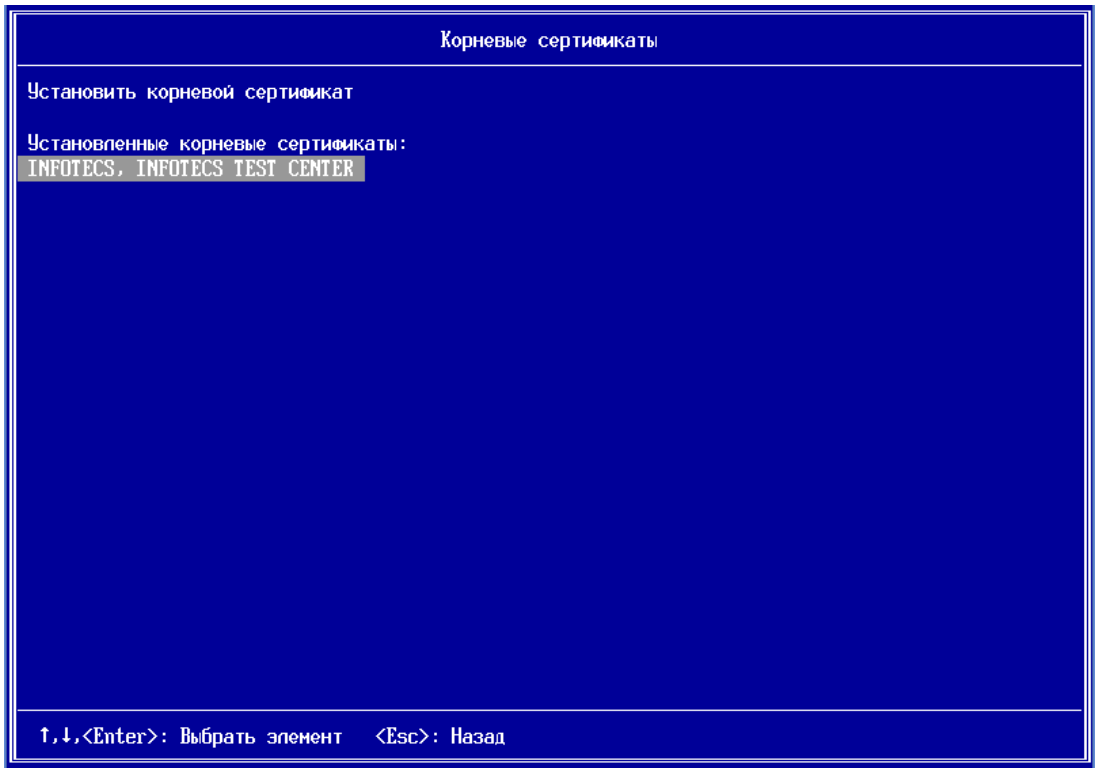


Рисунок 52. Выбор установленного сертификата

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

Откроется список доступных файлов для выбора.

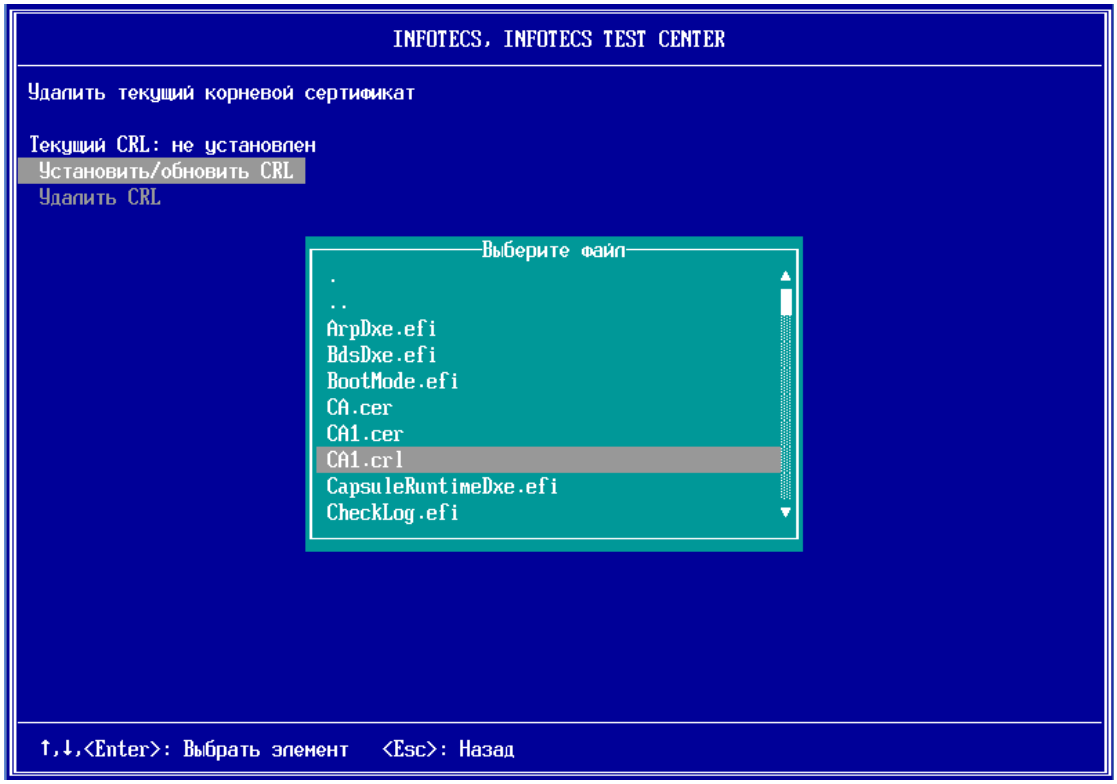


Рисунок 53. Выбор файла CRL

5 Выберите нужный файл CRL.

Серийный номер выбранного CRL отобразится в поле **Текущий CRL**, CRL будет установлен

Обновление CRL

Чтобы обновить CRL, выполните следующие действия:

1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).

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 **Установить/обновить CRL**.

Откроется список доступных файлов для выбора.

5 Выберите нужный файл CRL.

Серийный номер выбранного CRL отобразится в поле **Текущий CRL**, CRL будет обновлен.

Удаление CRL

Чтобы удалить CRL, выполните следующие действия:

1. Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 30).
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.

9

Управление журналом событий

Настройки журнала событий

Настройки журнала событий включают:

- Режим журналирования:
  - при переполнении добавлять записи циклически;
  - при переполнении переносить журнал на диск;
  - вести журнал на диске.
- Уровень регистрации событий:
  - подробный;
  - основной.

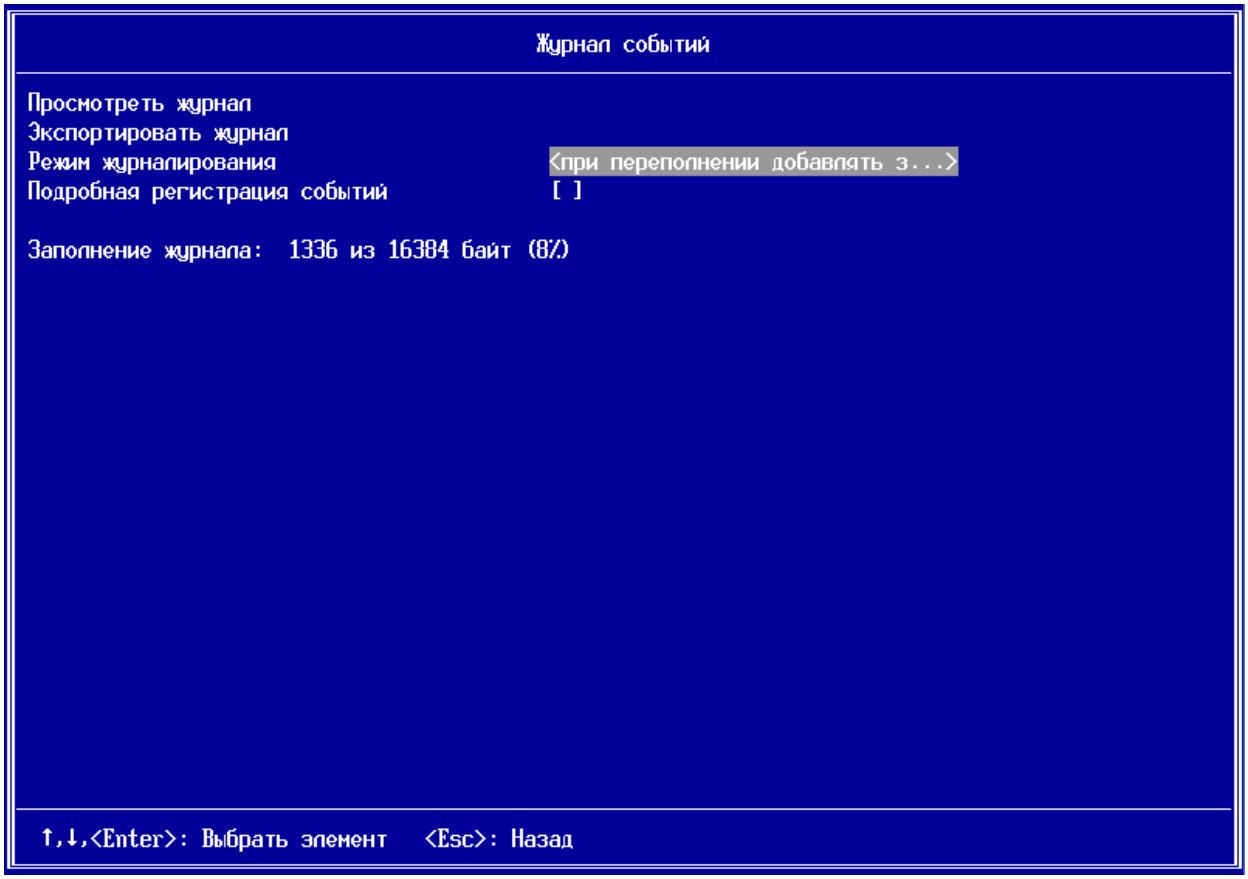


Рисунок 54. Меню управления настройками журнала событий

Режим «при переполнении добавлять записи циклически»

В режиме записи событий «**при переполнении добавлять записи циклически**»:

- 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 «**вести журнал на диске**», рекомендуется экспортировать журнал на USB диск.

Примечание. При переключении на режим «**вести журнал 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 журналирования будет переведен на «**вести журнал 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 журналирования будет переведен на «**вести журнал на диске**»;
- на локальном диске в каталоге **efi\infotecs\log** будет создан новый журнал, и все записи будут вестись в него.

Режим «при переполнении переносить журнал на диск»

В режиме записи событий «**при переполнении переносить журнал на диск**»:

- 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 «**вести журнал на диске**», рекомендуется экспортировать журнал на USB-носитель (см. примечание выше).

Режим «вести журнал на диске»

В режиме записи событий «**вести журнал на диске**»:

- журнал хранится на диске (EFI System Partition) в каталоге EFI\Infotecs\Log\;
- при переключении режима на другой, новый журнал начинает вестись в NVRAM-памяти BIOS с нуля (старый журнал остается на диске).

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. 30).
2. В меню режима настроек выберите **Журнал событий**.
3. Для изменения режима записи событий выберите **Режим журналирования**.

   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 циклическом режиме записи или при переполнении переносится на диск, то в режиме просмотра отображаются записи журнала событий из памяти ViPNet SafeBoot. В случае, если журнал ведется на диске, то отображаются записи журнала событий 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. 30).
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.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. 30).
2. В меню режима настроек выберите **Журнал событий**.
3. 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	**ошибка**	Неподдерживаемая версия БД конфигурации ПМДЗ
2	**ошибка**	БД конфигурации ПМДЗ переполнена
3	**ошибка**	Ошибка инициализации ItIntegrMgr
4	**детальный**	Ошибка формата файла подписи
5	**ошибка**	Целостность элемента нарушена
6	**ошибка**	Элемент не найден
7	**информация**	Элемент снят с КЦ (режим обучения)
8	**информация**	Незарегистрированный элемент
9	**информация**	Журнал экспортирован
10	**информация**	Журнал заполнен и заблокирован
11	**информация**	Журнал пересоздан
12	**информация**	Установка обновления...
13	**информация**	Старт ПМДЗ
14	**информация**	Система перезагружена
15	**информация**	Система выключена
16	**ошибка**	Неверное системное время

№ п/п	тип события	Текст сообщения
17	**информация**	Системное время изменено Администратором
18	**детальный**	Модуль верифицирован
19	**детальный**	Модуль выгружен
20	**ошибка**	Ошибка выгрузки модуля
21	**детальный**	Модуль загружен
22	**ошибка**	Ошибка формата модуля
23	**ошибка**	Неверная подпись модуля
24	**ошибка**	Рабочая директория ПМДЗ не найдена
25	**ошибка**	Рабочая директория ПМДЗ инициализирована
26	**информация**	Автоматический вход в систему
27	**информация**	Система выключена: истекло время сессии аутентификации
28	**информация**	Система выключена: превышено количество попыток аутентификации за сессию аутентификации
29	**информация**	Система выключена: превышено количество допустимых неверных попыток аутентификации
30	**информация**	Превышено количество допустимых неверных попыток аутентификации: загрузка ОС заблокирована
31	**информация**	Счетчик допустимых неверных попыток аутентификации сброшен: загрузка ОС разрешена
32	**ошибка**	Пользователь не существует
33	**информация**	Попытка аутентификации в неинициализированной/заблокированной системе (разрешен вход только Администратору)
34	**ошибка**	Неверный пароль
35	**ошибка**	Пользователь заблокирован
36	**ошибка**	Срок действия пароля пользователя истек
37	**ошибка**	Неверный PIN смарт-карты
38	**ошибка**	Смарт-карта пользователя не подключена
39	**ошибка**	Сертификат пользователя не найден
40	**ошибка**	Ошибка верификации сертификата пользователя
41	**информация**	Администратор аутентифицирован
42	**информация**	Аудитор аутентифицирован

№ п/п	тип события	Текст сообщения
43	**информация**	Пользователь аутентифицирован
44	**информация**	Опции загрузки ПМДЗ должны быть настроены
45	**информация**	Режим загрузки изменен
46	**информация**	Изменено устройство загрузки (legacy)
47	**информация**	Раздел ESP изменен
48	**информация**	EFI-загрузчик изменен
49	**информация**	Обновлен список разделов на КЦ
50	**информация**	Раздел поставлен на КЦ
51	**информация**	Раздел снят с КЦ
52	**информация**	Элемент поставлен на КЦ
53	**информация**	Элемент снят с КЦ
54	**информация**	Компонент поставлен на КЦ
55	**информация**	Компонент снят с КЦ
56	**информация**	Изменен диск для контроля загрузочных секторов
57	**информация**	Контроль журнала транзакций ФС включен
58	**информация**	Контроль журнала транзакций ФС выключен
59	**информация**	Режим обучения КЦ включен
60	**информация**	Режим обучения КЦ выключен
61	**информация**	Эталоны КЦ компонентов системы обновлены
62	**детальный**	Целостность элемента заверена
63	**ошибка**	Эталоны компонента не найдены
64	**информация**	Целостность компонентов системы заверена
65	**детальный**	Журнал транзакций ФС пуст
66	**ошибка**	Журнал транзакций ФС не пуст
67	**информация**	Добавлен пользователь
68	**информация**	Пользователь удален
69	**информация**	Изменен тип аутентификации пользователя
70	**информация**	Пароль пользователя изменен
71	**информация**	Настройки пароля пользователя изменены
72	**информация**	Пароль пользователя изменен Администратором
73	**информация**	Смарт-карта пользователя инициализирована

№ п/п	тип события	Текст сообщения
74	**информация**	Изменена смарт-карта пользователя
75	**информация**	Изменен сертификат пользователя
76	**информация**	Изменен режим журналирования
77	**информация**	Изменен уровень журналирования
78	**информация**	Установлен корневой сертификат
79	**информация**	Корневой сертификат удален
80	**информация**	CRL установлен/обновлен
81	**информация**	CRL удален
82	**информация**	Вход в режим настроек BIOS разрешен
83	**информация**	Вход в режим настроек BIOS запрещен
84	**информация**	Защита SPI flash включена
85	**информация**	Защита SPI flash выключена
86	**информация**	Защита S3 bootscript включена
87	**информация**	Защита S3 bootscript выключена
88	**информация**	БД конфигурации ПМДЗ экспортирована
89	**ошибка**	Ошибка при экспорте БД конфигурации ПМДЗ
90	**информация**	БД конфигурации ПМДЗ импортирована
91	**ошибка**	Ошибка при импорте БД конфигурации ПМДЗ
92	**информация**	Ограничение сессии аутентификации включено
93	**информация**	Ограничение сессии аутентификации выключено
94	**информация**	Время сессии аутентификации изменено
95	**информация**	Автоматический вход в систему разрешен
96	**информация**	Автоматический вход в систему запрещен
97	**информация**	Время до автоматического входа в систему изменено
98	**информация**	EFI-загрузчик возвратил управление ПМДЗ
99	**ошибка**	Найдено несколько разделов ESP
100	**ошибка**	Ошибка верификации пакета обновления
101	**ошибка**	Неверная версия пакета обновления
102	**ошибка**	Пакет обновления не соответствует текущей платформе
103	**информация**	Пакет обновления установлен

№ п/п	тип события	Текст сообщения
104	**ошибка**	Ошибка при установке пакета обновления

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, выполнить пересчет контрольных сумм (см. Контроль целостности на стр. 47).

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. 47).

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 журналирования на «при переполнении добавлять записи циклически» (см. Управление журналом событий на стр. 90).

Пользователь заблокирован

Основные причины блокирования пользователя:

- Превышено допустимое количество неудачных попыток аутентификации;
- Время действия пароля пользователя истекло;

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. 59).

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. 59).

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.