

A low-angle, upward-looking photograph of a modern skyscraper with a glass facade. The building's structure is composed of dark metal frames and large glass panels, reflecting the sky. The perspective creates a sense of height and architectural scale. A solid orange vertical bar is visible on the far left edge of the image.

ViPNet SafeBoot

Руководство администратора

1991–2018 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00180-01 32 01, версия 1.3.0.24

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

Содержание

Введение.....	7
О документе	8
Для кого предназначен документ	8
Соглашения документа	8
О ViPNet SafeBoot.....	9
Назначение ViPNet SafeBoot	9
Состав ViPNet SafeBoot.....	9
Системные требования	9
Комплект поставки	11
Обратная связь	12
Глава 1. Общие сведения	13
Основные возможности ViPNet SafeBoot.....	14
Идентификация и аутентификация пользователей.....	15
Роли пользователей	16
Глава 2. Установка, обновление и удаление ViPNet SafeBoot	17
Установка и удаление ViPNet SafeBoot	18
Обновление ViPNet SafeBoot.....	19
Глава 3. Начало работы	22
Первый запуск	23
Запуск и завершение работы	27
Аутентификация по паролю	28
Аутентификация по электронному идентификатору	29
Аутентификация по электронному идентификатору и паролю.....	30
Аутентификация по паролю на электронном идентификаторе	31
Аутентификация пользователя, зарегистрированного на LDAP сервере	32
Глава 4. Режим настройки ViPNet SafeBoot	33
Вход в режим настройки ViPNet SafeBoot	34
Интерфейс режима настройки	36
Ограничение сессии аутентификации	38
Автоматический вход в систему	40
Эмуляция NVRAM.....	42

Защита BIOS.....	43
Вход в BIOS Setup	45
Экспорт настроек.....	46
Импорт настроек	47
Глава 5. Управление режимами загрузки операционной системы	48
Режим загрузки операционной системы	49
Использование параметров загрузки BIOS.....	50
Загрузка операционной системы в режиме совместимости	51
Загрузка операционной системы в режиме UEFI.....	52
Временное отключения функциональности ViPNet SafeBoot.....	53
Глава 6. Контроль целостности	54
Контролируемые объекты	55
Автоопределение компонентов загрузки ОС	56
Контроль разделов и файлов	58
Контроль состава аппаратных средств	61
Контроль реестра Windows	62
Режим обучения	66
Перерасчет эталонных контрольных сумм	69
Принудительная проверка целостности.....	70
Хранение эталонов.....	71
Глава 7. Управление учетными записями пользователей.....	72
Учетные записи пользователей.....	73
Создание диска восстановления	74
Восстановление пароля администратора	76
Добавление учетных записей пользователей с аутентификацией по паролю	78
Добавление учетных записей пользователей с аутентификацией по электронному идентификатору	82
Добавление учетных записей пользователей с аутентификацией по электронному идентификатору и паролю	91
Добавление учетных записей пользователей с аутентификацией по паролю на электронном идентификаторе	96
Добавление учетных записей пользователей с LDAP аутентификацией	100
Редактирование учетных записей пользователей.....	101
Редактирование учетной записи пользователя с аутентификацией по электронному идентификатору	102
Удаление учетных записей пользователей.....	104

Глава 8. Управление сертификатами.....	105
Корневой сертификат доверенного центра сертификации.....	106
Установка корневого сертификата	107
Удаление корневого сертификата.....	108
Операции со списком отозванных сертификатов (CRL)	109
Установка CRL	109
Обновление CRL	110
Удаление CRL.....	111
Подготовка к работе электронных идентификаторов	112
Подготовка к работе JaCarta PKI (USB/SC)	112
Подготовка к работе Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен Lite.....	112
Подготовка к работе Guardant ID.....	113
Глава 9. Настройки сети и LDAP	114
Настройки сети	115
Настройки подключения к LDAP серверу	118
Глава 10. Управление журналом событий.....	123
Настройки журнала событий.....	124
Режим «при переполнении добавлять записи циклически».....	124
Режим «при переполнении переносить журнал на диск».....	125
Режим «вести журнал на диске»	125
Изменение настроек журнала событий	126
Просмотр журнала событий.....	127
Экспорт записей журнала событий.....	128
Приложение А. События, регистрируемые в ViPNet SafeBoot	129
Приложение В. Возможные неполадки и способы их устранения.....	135
Система заблокирована	136
Нарушена целостность операционной системы или объектов, поставленных на контроль.....	136
Нарушена целостность состава аппаратных средств, поставленных на контроль	136
Журнал событий переполнен.....	136
Пользователь заблокирован	137
Превышено допустимое количество неудачных попыток аутентификации	137
Время действия пароля пользователя истекло.....	137

Приложение С. Глоссарий	138
-------------------------------	-----



Введение

О документе	8
О ViPNet SafeBoot	9
Обратная связь	12

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, по паролю, по паролю и электронному идентификатору, по паролю на электронном идентификаторе, аутентификация пользователя, зарегистрированного на LDAP.

Системные требования

Требования к компьютеру, предназначенному для установки ViPNet SafeBoot:

- Процессор — X86-совместимый с поддержкой режима x86-64 (AMD64/Intel64), частота от 500 МГц;
- Системная плата — определяется исполнением ViPNet SafeBoot, совместимостью с используемым процессором. BIOS платы должен соответствовать спецификации UEFI версий: 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 операционной системы (ОС).

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

Семейство процессоров	Примечание
Atom C2000 Processor Family	Intel Avoton
Cherry Trail SoC	Braswell
Bay Trail SoC	Bay Trail
Intel Quark SoC X1000	Galileo Board
2nd Generation Core Processor Family (Sandy Bridge)	Desktop 2nd Generation Core Processor (Sandy Bridge CPU / Cougar Point PCH) Mobile 2nd Generation Core Processor (Sandy Bridge CPU / Cougar Point PCH)Intel Xeon Processor E3-1200 (Sandy Bridge CPU, C200 Series PCH)
3rd Generation Core Processor Family (Ivy Bridge)	Desktop 3rd Generation Core Processor (Ivy Bridge CPU / Panther Point PCH) Mobile 3rd Generation Core Processor (Ivy Bridge CPU / Panther Point PCH)Intel Xeon Processor E3-1200 v2 (Ivy Bridge CPU, C200/C216 Series PCH)
4th Generation Core Processor Family (Haswell)	Desktop 4th Generation Core Processor (Haswell CPU / Lynx Point PCH) Mobile 4th Generation Core Processor (Haswell M/H / Lynx Point PCH) Intel Xeon Processor E3-1200 v3 (Haswell CPU, C220 Series PCH)
5th Generation Core Processor Family (Broadwell)	Desktop 5th Generation Core Processor (Broadwell CPU / Wildcat Point PCH) Mobile 5th Generation Core Processor (Broadwell M/H / Wildcat Point PCH)
6th Generation Core Processor Family (Skylake)	Mobile 6th Generation Core Processor (Skylake Y/U) Mobile 6th Generation Core Processor Dual Core (Skylake H) Mobile 6th Generation Core Processor Quad Core (Skylake H) Desktop 6th Generation Core Processor Dual Core (Skylake CPU / Sunrise Point PCH) Desktop 6th Generation Core Processor Quad Core (Skylake CPU / Sunrise Point PCH)

Семейство процессоров	Примечание
7th Generation Core Processor Family (Kabylake)	Mobile 7th Generation Core Processor (Kabylake U/Y) Desktop 7th Generation Core Processor (Kabylake S)
Xeon v1 Processor (Jaketown/Sandy Bridge - EP)	Server 2nd Generation Core Processor (Jaketown CPU / Patsburg PCH)
Xeon v2 Processor (Ivy Town/Ivy Bridge - EP)	Server 3rd Generation Core Processor (Ivytown CPU / Patsburg PCH)
Xeon v3 Processor (Haswell Server)	Server 4th Generation Core Processor (Haswell Server CPU / Wellsburg PCH)
Xeon v4 Processor (Broadwell Server)	Intel Xeon Processor E3 v4 (Broadwell CPU) Intel Xeon Processor E5/E7 v4 (Broadwell Server CPU / Wellsburg PCH)
Xeon v5 Processor (Skylake Server)	Intel Xeon Processor E3 v5 (Skylake CPU / Sunrise Point PCH)
Xeon v6 Processor (Kabylake Server)	Intel Xeon Processor E3 v6 (Kabylake CPU)



Примечание. При использовании ПМД3 ViPNet SafeBoot на платформах с другими чипсетами необходимо обеспечить невозможность перезаписи микросхемы BIOS другими средствами, если это не выполнено производителем платформы.

Комплект поставки

В комплект поставки ViPNet SafeBoot входит:

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

Обратная связь

Дополнительная информация

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

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

Контактная информация

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

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

8 (495) 737-6196,

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

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	14
Идентификация и аутентификация пользователей	15
Роли пользователей	16

Основные возможности ViPNet SafeBoot

Основные возможности ViPNet SafeBoot представлены в таблице ниже.

Функциональная возможность	Ссылка
Идентификация и аутентификация пользователей. Обеспечение идентификации и аутентификации зарегистрированных пользователей	Идентификация и аутентификация пользователей на стр. 15
Доверенная загрузка операционной системы. Обеспечение загрузки компонентов операционной системы только с определенных носителей, назначенных администратором, предоставление администратору возможности выбора режима загрузки ОС	Управление параметрами загрузки ОС на стр. 48
Контроль целостности. Обеспечение целостности собственного программного обеспечения, образа BIOS и других компонентов	Контроль целостности на стр. 54
Управление учетными записями пользователей. Создание, редактирование и удаление учетных записей пользователей	Управление учетными записями пользователей на стр. 72
Управление настройками аутентификации. ViPNet SafeBoot позволяет задать настройки сессии аутентификации	Управление настройками аутентификации на стр. 38
Управление сертификатами. Обеспечение загрузки корневых сертификатов и списка отзыва сертификатов	Управление сертификатами на стр. 105
Проверка и установка обновлений. Автоматический поиск файла обновления и установка обновлений посредством меню управления настройками	Обновление ViPNet SafeBoot на стр. 19
Экспорт и импорт настроек ViPNet SafeBoot	Экспорт настроек на стр. 40 Импорт настроек на стр. 47
Ведение журнала событий. Регистрация всех значимых событий безопасности и действий пользователя.	Управление журналом событий на стр. 123

Идентификация и аутентификация пользователей

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

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

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

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



Примечание. Срок действия пароля может быть ограничен.

Если администратор установил ограничение на срок действия пароля, то по истечении заданного периода выводится соответствующее 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.

В случае использования электронных идентификаторов Рутокен Lite и JaCarta PKI (USB/SC), необходимо, чтобы ключ и сертификат были записаны на электронный идентификатор в виде контейнера, созданного при помощи криптопровайдера ViPNet CSP (см. «Подготовка к работе электронных идентификаторов» стр. 112). Информацию о ViPNet CSP можно получить на сайте <https://infotecs.ru/product/vipnet-csp.html>.

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

Процедура идентификации и аутентификации приведена на стр. 27.

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

18

Обновление ViPNet SafeBoot

19

Установка и удаление ViPNet SafeBoot

Установку и удаления программного комплекса ViPNet SafeBoot производить в соответствии с руководством по установке ФРКЕ.00180-01 90 19, входящем в комплект поставки.

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

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. 34).



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. 46). После обновления рекомендуется выполнить импорт настроек (см. Импорт настроек на стр. 47)

- 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.

Пакет обновления не найден
Нажмите любую клавишу для продолжения

Рисунок 1. Сообщение в случае отсутствия файла обновления

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.

Пакет обновления найден, но является устаревшим (версия ниже текущей)
Нажмите любую клавишу для продолжения

Рисунок 2. Сообщение об устаревшей версии обновления

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

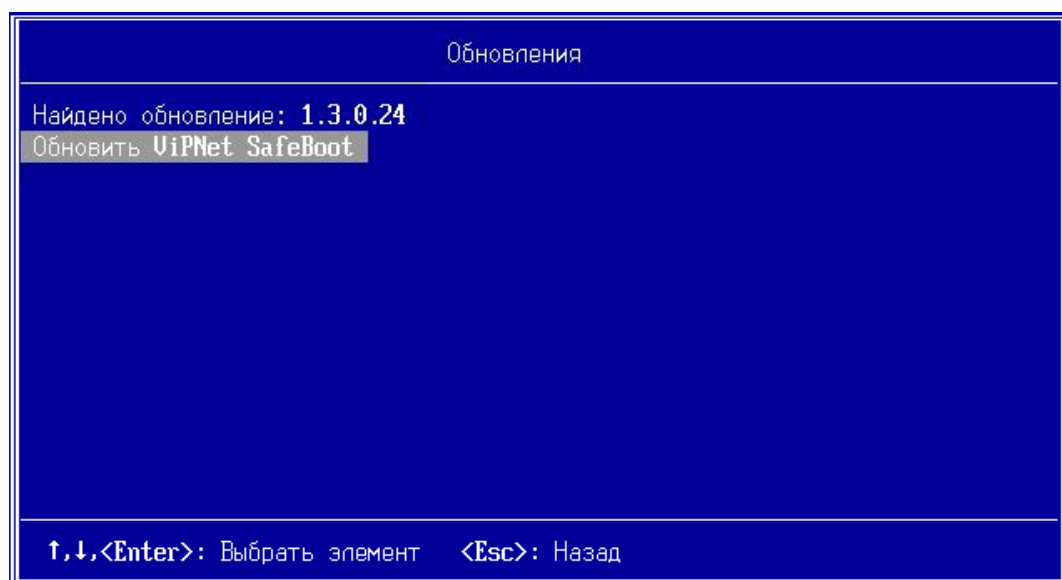


Рисунок 3. Выбор найденной версии обновления

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

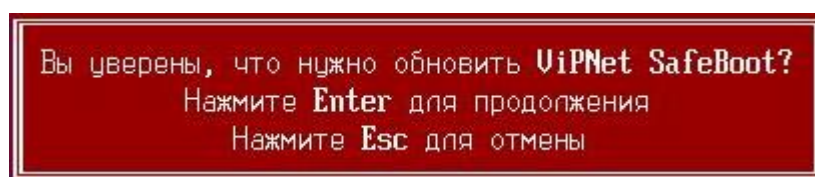


Рисунок 4. Подтверждение обновления



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:

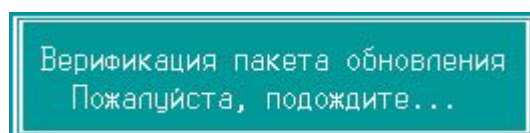


Рисунок 5. Сообщение о верификации пакета обновления

В случае ошибки при верификации пакета будет выдано сообщение:

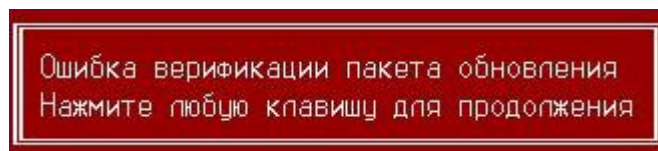


Рисунок 6. Сообщение об ошибке верификации пакета обновления

- 8 В ходе установки обновления будет выдано следующее сообщение

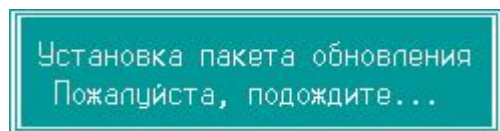


Рисунок 7. Сообщение об установке пакета обновления

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

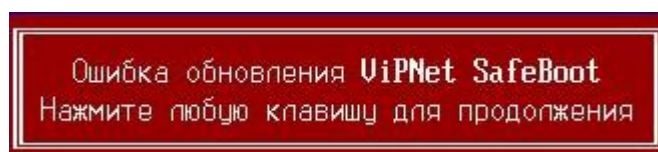


Рисунок 8. Сообщение об ошибке при установке обновления

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



3

Начало работы

Первый запуск	23
Запуск и завершение работы	27

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 9. Начало аутентификации (ввод имени пользователя)

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



Рисунок 10. Приглашение ввести пароль

- 3 После успешной аутентификации будет выдано следующее сообщение:

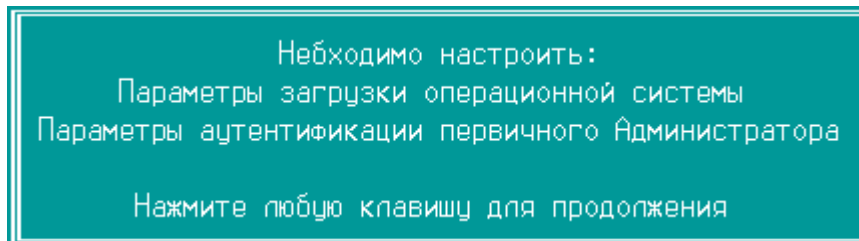
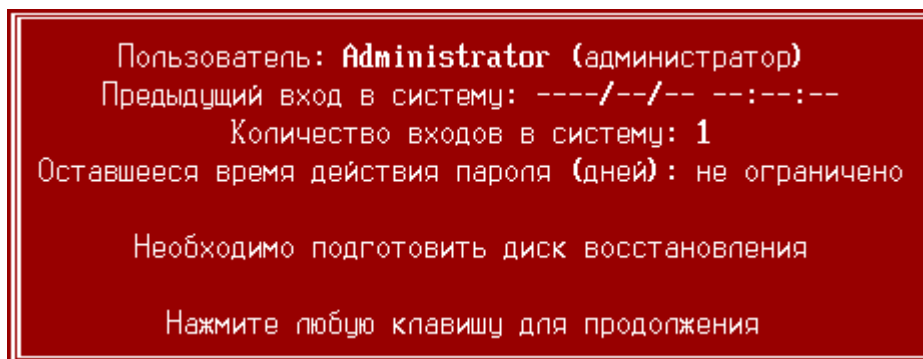


Рисунок 11. Сообщение о необходимых настройках при первом включении

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





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

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

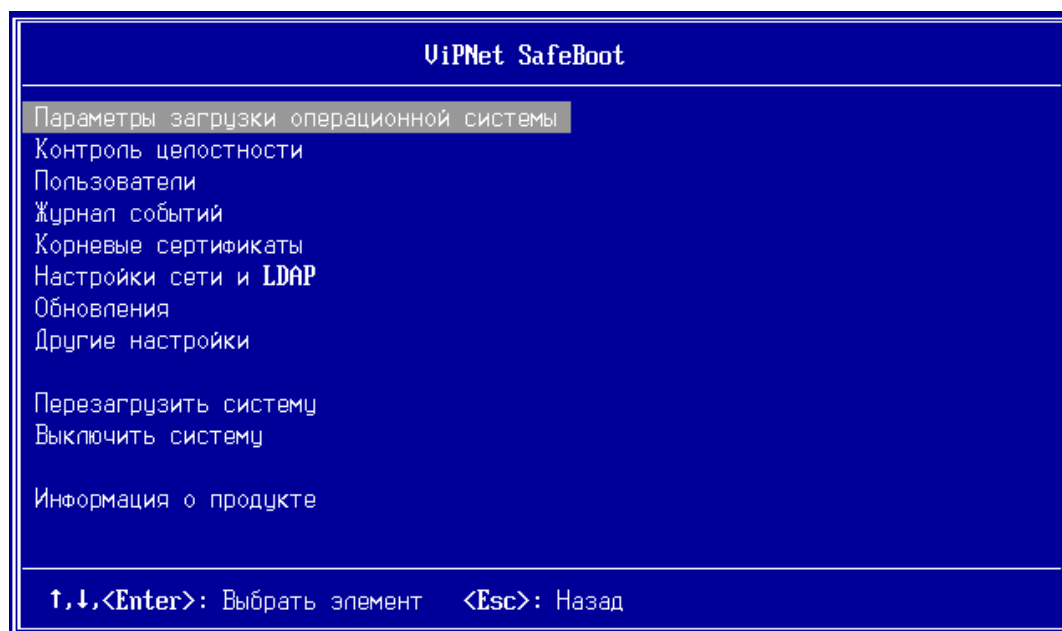


Рисунок 12. Меню режима настроек ViPNet SafeBoot

- 6 В меню режима настроек выберите пункт **Пользователи**. В открывшемся окне выберите из списка текущих пользователей – **Administrator**.
- 7 В окне **Настройки пользователя** выберите пункт **Изменить пароль**.



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

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



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

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

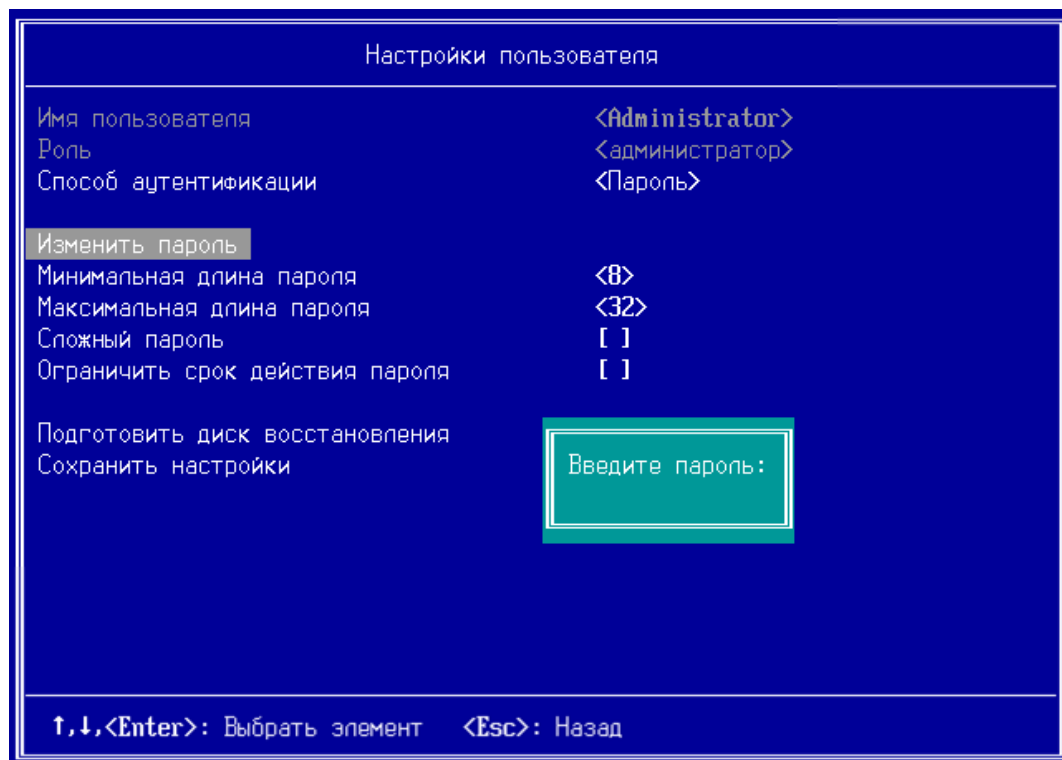
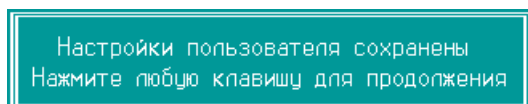


Рисунок 13. Меню настроек пользователя

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

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

Дождитесь появления следующей надписи:



- 9 Нажмите любую клавишу.



Примечание. Для восстановления пароля администратора или сброса пароля до значения при первом включении рекомендуется создать диск восстановления (см. «Создание диска восстановления» на стр. 74).

- 10 Для выхода в основное меню дважды нажмите **Esc**.
- 11 Установите параметры загрузки операционной системы в соответствии с указаниями на стр. 48.

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. 34), 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**.

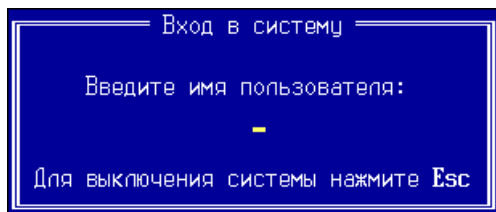


Рисунок 14. Начало аутентификации (ввод имени пользователя)

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

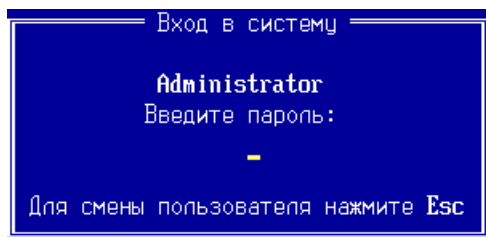


Рисунок 15. Приглашение ввести пароль

Аутентификация по электронному идентификатору

Для выполнения аутентификации по электронному идентификатору, выполните следующие действия:

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

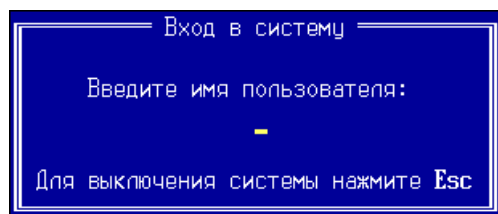


Рисунок 16. Начало аутентификации (ввод имени пользователя)

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

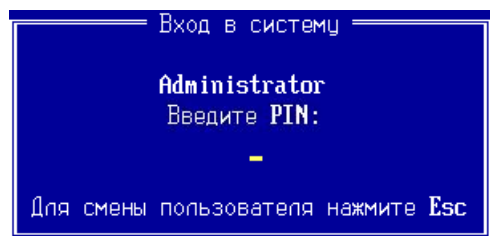
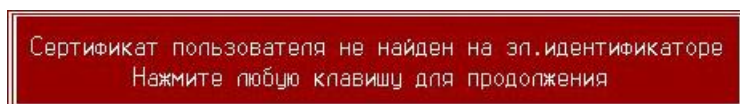


Рисунок 17. Приглашение ввести PIN-код

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



Нажмите любую клавишу и повторите процедуру аутентификации с электронным идентификатором, содержащим сертификат для аутентификации.

Аутентификация по электронному идентификатору и паролю

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

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

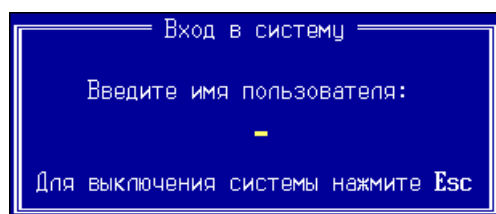


Рисунок 18. Начало аутентификации (ввод имени пользователя)

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

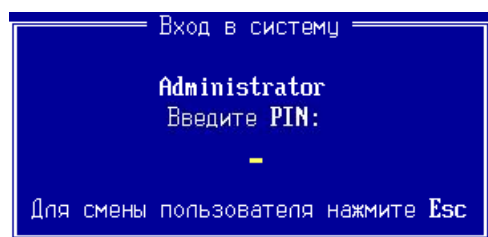


Рисунок 19. Приглашение ввести PIN-код

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

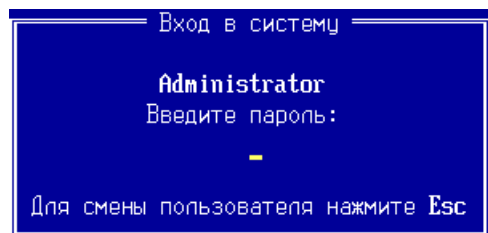


Рисунок 20. Приглашение ввести пароль

Аутентификация по паролю на электронном идентификаторе

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

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

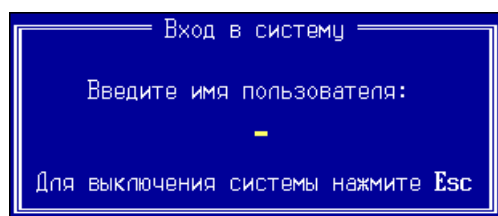


Рисунок 21. Начало аутентификации (ввод имени пользователя)

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

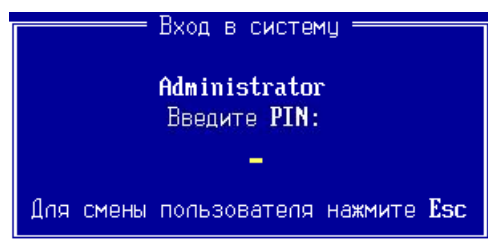
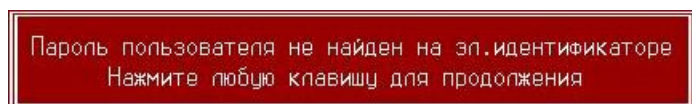


Рисунок 22. Приглашение ввести PIN-код

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



Нажмите любую клавишу для продолжения и повторите процедуру аутентификации с электронным идентификатором, содержащим пароль для аутентификации, или установите новый пароль на электронном идентификаторе в соответствии с рекомендациями на стр. 96.

Аутентификация пользователя, зарегистрированного на LDAP сервере

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

- 1 При появлении приглашения ввести имя пользователя, введите логин пользователя в следующем формате <имя сервера>\<имя учетной записи пользователя>. Имя сервера задается администратором в настройках (см. описание на стр. 100). Нажмите **Enter**.

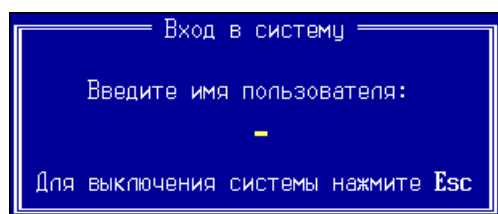


Рисунок 23. Начало аутентификации (ввод имени пользователя)

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

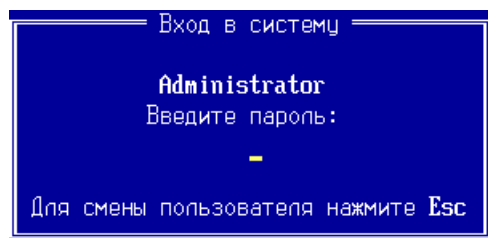


Рисунок 24. Приглашение ввести пароль

4

Режим настройки ViPNet SafeBoot

Вход в режим настройки ViPNet SafeBoot	34
Интерфейс режима настройки	36
Ограничение сессии аутентификации	38
Автоматический вход в систему	40
Эмуляция NVRAM	42
Защита BIOS	43
Вход в BIOS Setup	45
Экспорт настроек	46
Импорт настроек	47

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. 27).

После успешной аутентификации в нижней части экрана появится надпись:

Нажмите [F2] для входа в режим настройки



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

- 3 Нажмите клавишу F2.

Откроется основное меню режима настроек ViPNet SafeBoot.

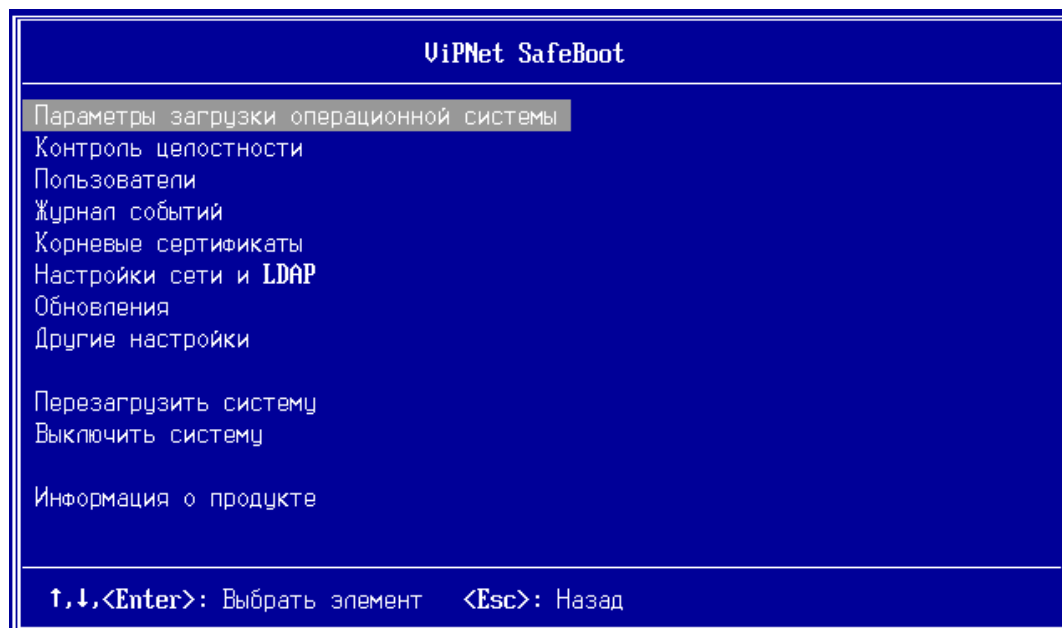


Рисунок 25. Вид меню режима настроек ViPNet SafeBoot для Администратора

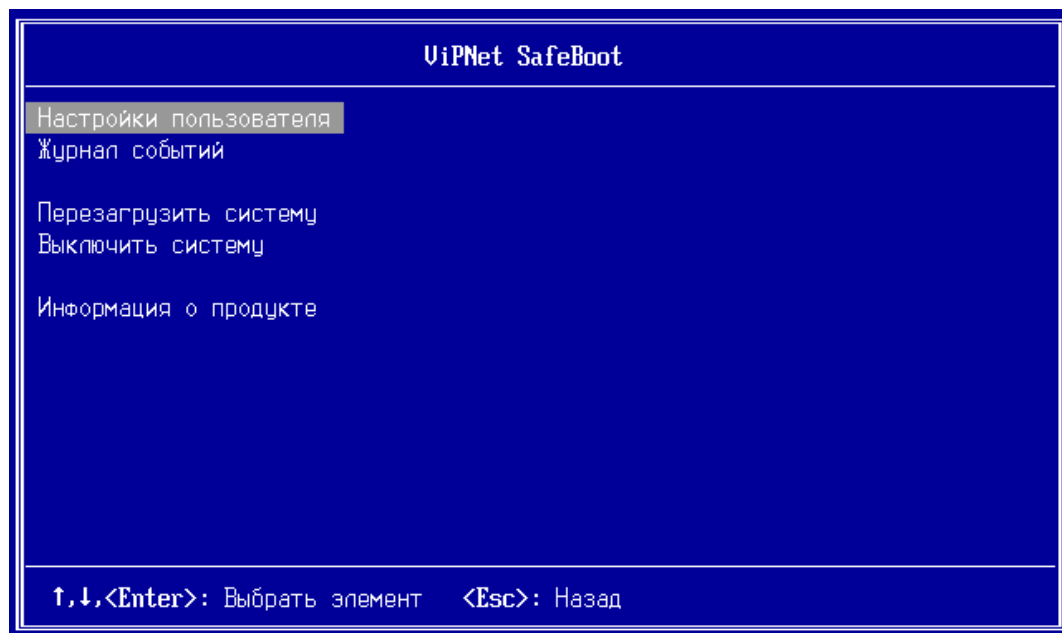


Рисунок 26. Вид меню режима настроек ViPNet SafeBoot для Аудитора

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 пункт;
- 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:

- выполнить автоопределение компонентов загрузки ОС для постановки на контроль;
- выбрать контролируемые объекты:
 - файлы на разделах накопителя;
 - CMOS, PCI, ACPI, SMBIOS, карта памяти;
 - карта распределения памяти, модули UEFI;
 - BIOS;
 - загрузочные сектора выбранного диска (MBR);
 - параметры реестра Windows;
 - журналы транзакций файловых систем NTFS, EXT3, EXT4.
- выполнить принудительную проверку целостности контролируемых объектов;
- выполнить перерасчет эталонов всех объектов, находящихся на контроле.

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

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

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

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

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;
- настроить автоматический вход в систему;
- установить защиту содержимого микросхемы BIOS от чтения и перезаписи из ОС;
- разрешить эмуляцию NVRAM;
- разрешить однократный вход в BIOS Setup;
- экспортировать настройки;
- импортировать настройки.

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

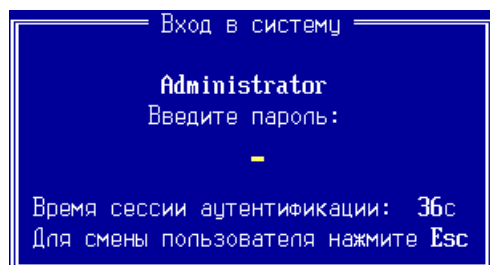
Выбор элемента управления **Выключить систему** осуществляет немедленное выключение системы.

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

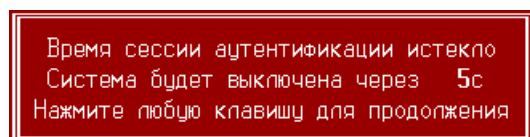
Ограничение сессии аутентификации

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

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



Процедура аутентификации выполняется в установленном порядке (см. «Запуск и завершение работы» на стр. 27). 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. 34).
- 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.

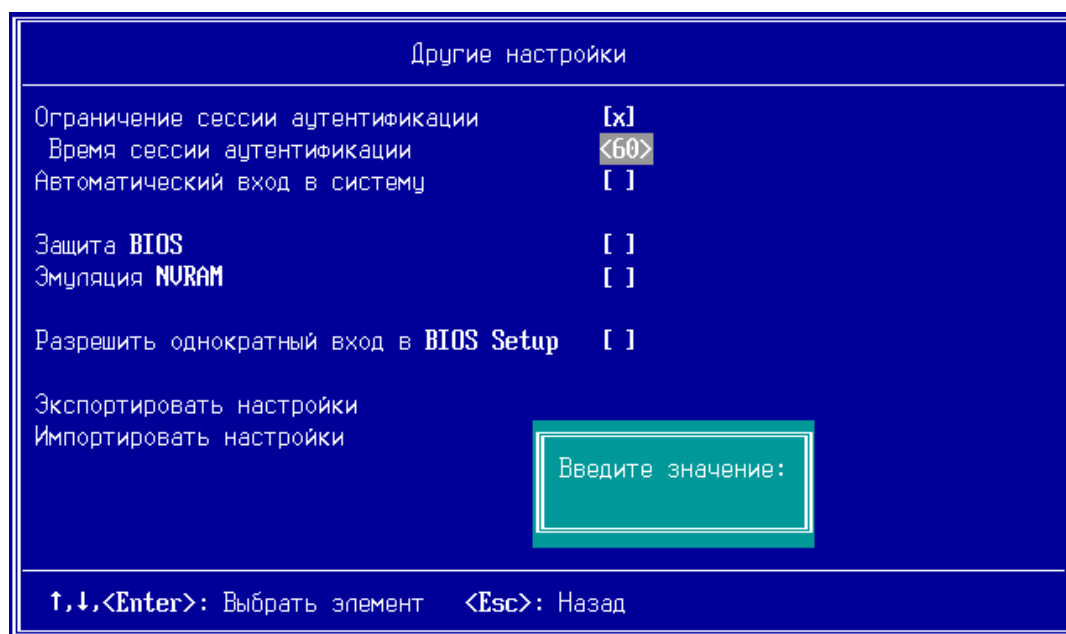


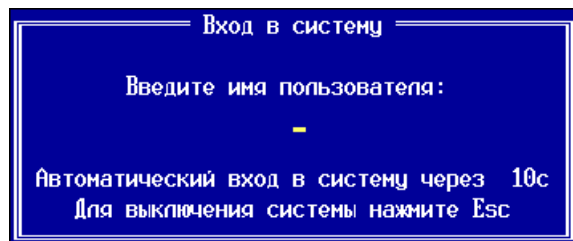
Рисунок 27. Ввод значения времени ограничения сессии аутентификации

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. 27).

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. 34).
- 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.

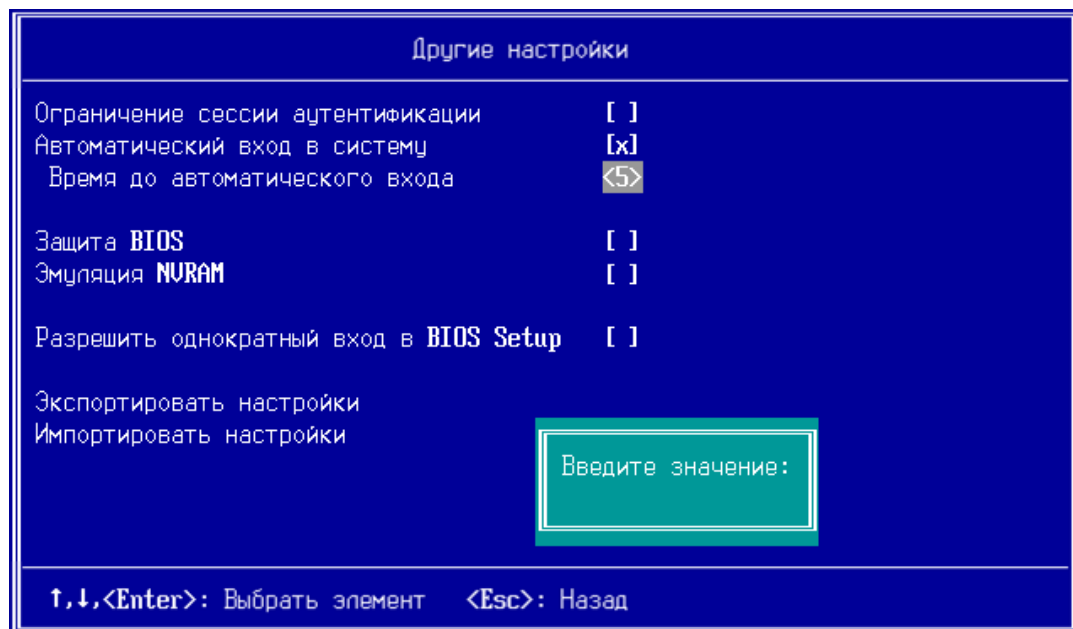


Рисунок 28. Ввод значения времени до автоматического входа в систему

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

Эмуляция NVRAM

Эмуляция NVRAM — это подсистема эмуляции UEFI-переменных. При включенной подсистеме запись и чтение UEFI-переменных осуществляется во временную область памяти, в микросхему BIOS запись данных не производится. Включение эмуляции NVRAM может понадобиться при ошибках загрузки ОС, например, если включена защита BIOS, режим загрузки ОС — Legacy.

Чтобы установить функцию защиты BIOS, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Другие настройки**.
- 3 В открывшемся окне установите флажок **Эмуляция NVRAM**.

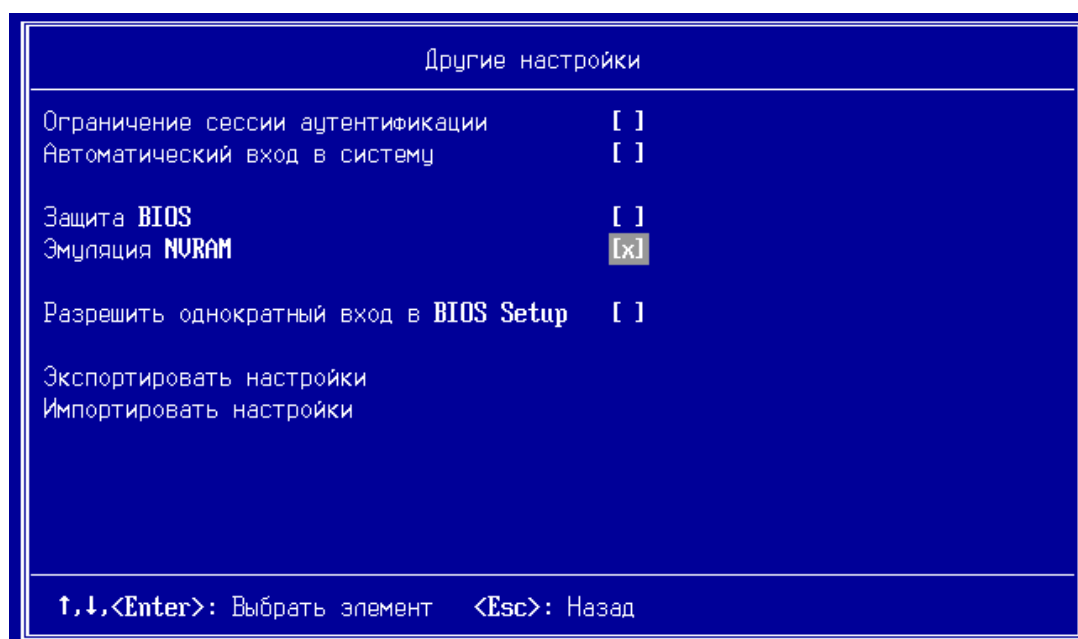


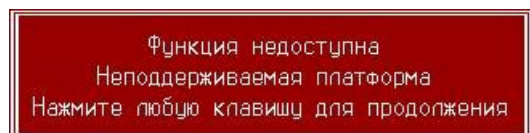
Рисунок 29. Меню *Другие настройки*

- 4 Для выхода в основное меню нажмите **Esc**.

Защита BIOS

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

Для систем с неподдерживаемым чипсетом защита не установится, на экране появится следующее сообщение:



Чтобы установить функцию защиты BIOS, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Другие настройки**.
- 3 В открывшемся окне установите флажок **Защита BIOS**.

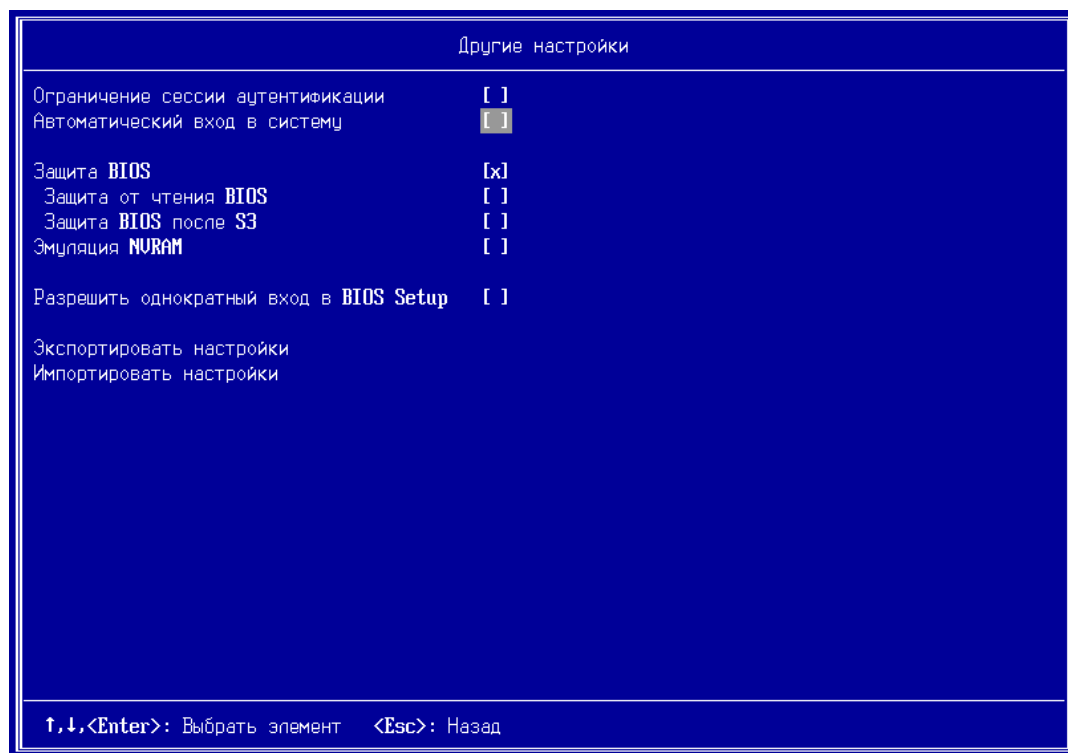


Рисунок 30. Меню Другие настройки

- 4 Для установки функции защиты от чтения содержимого микросхемы BIOS, установите флажок **Защита от чтения BIOS**.
- 5 Для установки функции защиты BIOS при выходе из спящего режима, установите флажок **Защита после S3**.

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

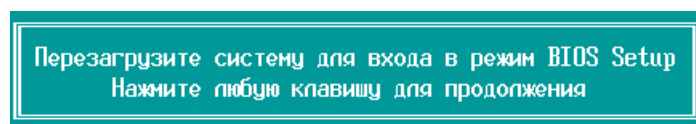
Вход в BIOS Setup

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. 34).
- 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**.

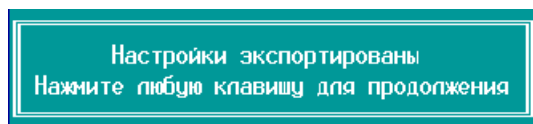
Экспортируются (и далее могут быть импортированы) следующие настройки:

- Общие настройки:
 - Параметры загрузки операционной системы;
 - Настройки процедуры входа в систему;
 - Значение режима защиты BIOS.
- Пользователи и их настройки;
- Корневые сертификаты;
- Эталоны (в случае если в настройках Контроля целостности значение параметра – «в базе данных», в противном случае эталоны можно экспортировать/импортировать вручную, копируя соответствующие файлы – см. описание «Хранение эталонов» на стр. 71 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. 34).
- 3 В меню режима настроек выберите **Другие настройки**.
- 4 В открывшемся окне выберите **Экспортировать настройки**.

После завершения экспорта появится следующее сообщение:

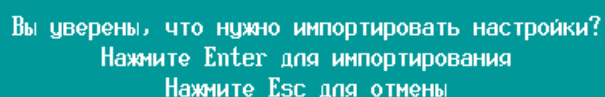


Импорт настроек

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. 34).
- 3 В меню режима настроек выберите **Другие настройки**.
- 4 В открывшемся окне выберите **Импортировать настройки**.

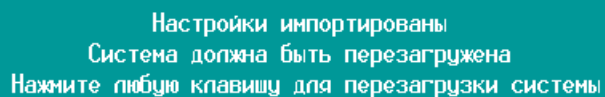
Появится окно с предупреждением:

A teal-colored rectangular dialog box with a double border. It contains the following text:

Вы уверены, что нужно импортировать настройки?
Нажмите Enter для импортирования
Нажмите Esc для отмены

- 5 Нажмите Enter.

После успешного импорта настроек появится сообщение о необходимости перезагрузить систему.

A teal-colored rectangular dialog box with a double border. It contains the following text:

Настройки импортированы
Система должна быть перезагружена
Нажмите любую клавишу для перезагрузки системы

- 6 Нажмите любую клавишу, система перезагрузится.

5

Управление режимами загрузки операционной системы

Режим загрузки операционной системы	49
Использование параметров загрузки BIOS	50
Загрузка операционной системы в режиме совместимости	51
Загрузка операционной системы в режиме UEFI	52
Временное отключения функциональности ViPNet SafeBoot	53

Режим загрузки операционной системы

ViPNet SafeBoot поддерживает следующие режимы загрузки ОС:

- использование параметров загрузки BIOS.

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

- legacy (режим совместимости).

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

- UEFI.

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

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

Использование параметров загрузки BIOS

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

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Параметры загрузки операционной системы**.
- 3 В открывшемся окне выберите **Использовать параметры загрузки BIOS** и нажмите **Enter**.

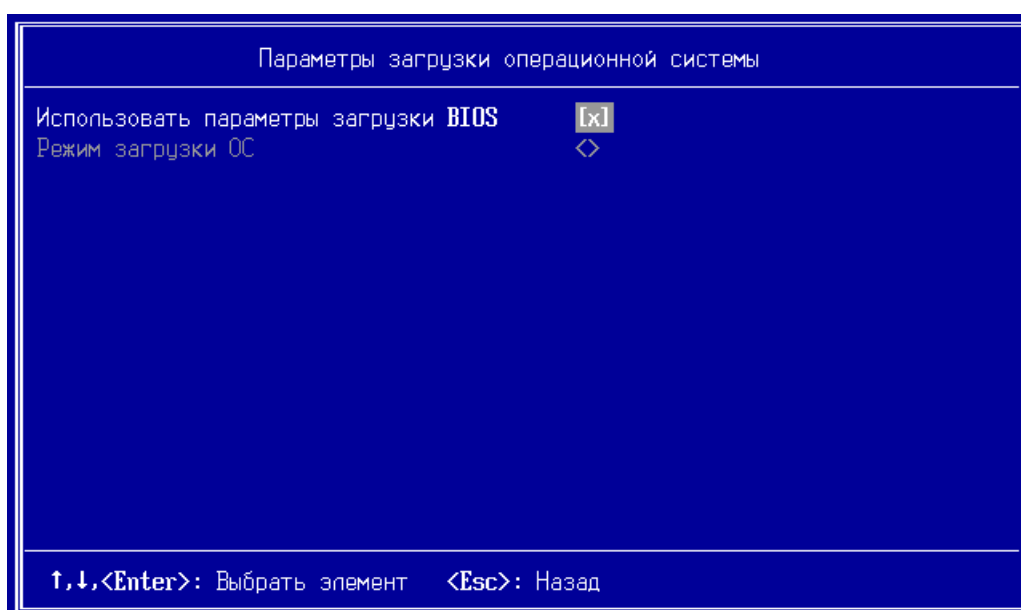
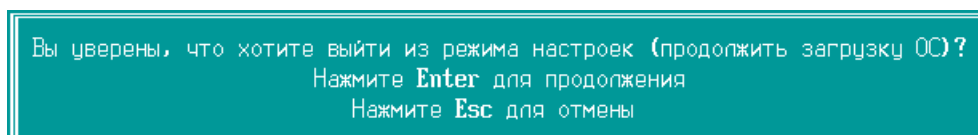


Рисунок 31. Выбор режима загрузки операционной системы

- 4 Вернитесь в основное меню режима настроек ViPNet SafeBoot, нажав **Esc**.
- 5 Нажмите **Esc** для выхода из режима настройки и начала загрузки операционной системы в выбранном режиме.
- 6 Появится окно со следующим сообщением:



Для начала загрузки ОС нажмите **Enter**.

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. 34).
- 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)**.

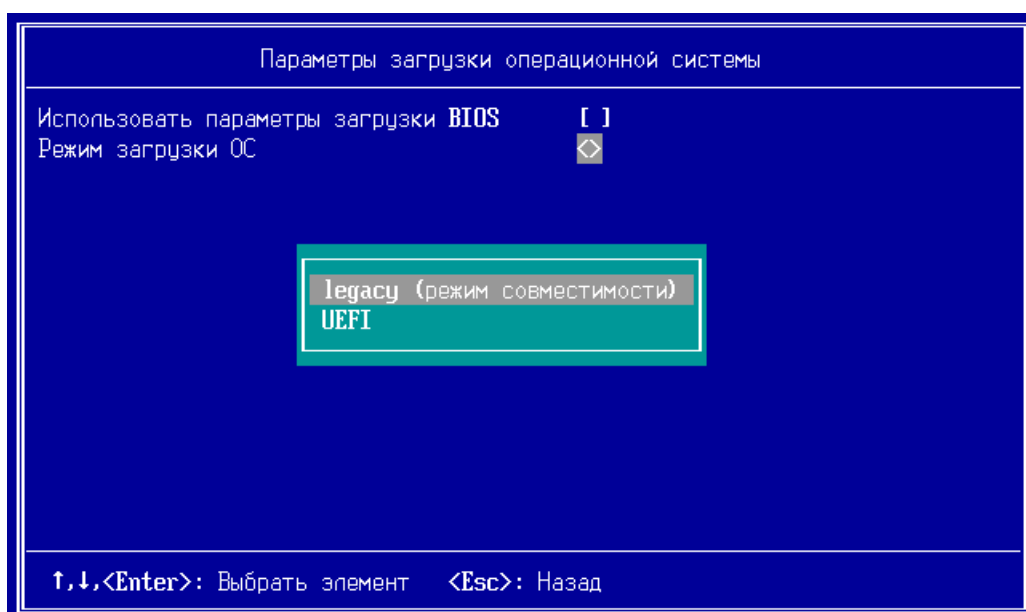
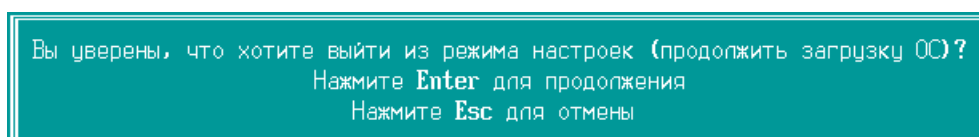


Рисунок 32. Меню выбора режима загрузки операционной системы — legacy (режима совместимости)

- 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.
- 8 При появлении следующего сообщения, нажмите **Enter** для начала загрузки ОС:



Загрузка операционной системы в режиме UEFI

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

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 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)**.

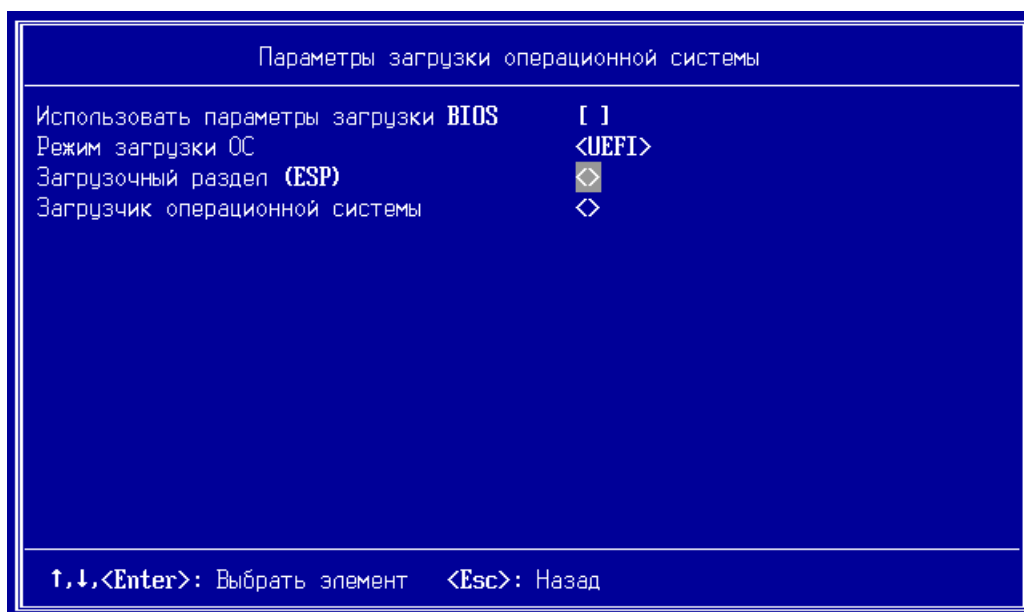
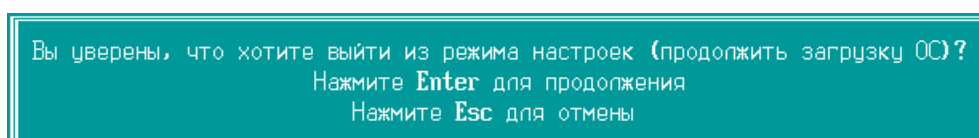


Рисунок 33. Выбор загрузочного раздела при выборе загрузки UEFI

- 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.
- 10 При появлении следующего сообщения, нажмите **Enter** для начала загрузки ОС:



Временное отключения функциональности ViPNet SafeBoot

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

- 1 Подготовьте диск восстановления (см. «Создание диска восстановления» на стр. 74).
- 2 Подключите USB-накопитель, инициализированный как диск восстановления.
- 3 Для отключения функциональности ViPNet SafeBoot при загрузке нажмите сочетание клавиш **Ctrl + x**.

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

6

Контроль целостности

Контролируемые объекты	55
Автоопределение компонентов загрузки ОС	56
Контроль разделов и файлов	58
Контроль состава аппаратных средств	61
Контроль реестра Windows	62
Режим обучения	66
Перерасчет эталонных контрольных сумм	69
Принудительная проверка целостности	70
Хранение эталонов	71

Контролируемые объекты

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

ViPNet SafeBoot позволяет осуществлять контроль целостности следующих типов объектов:

- файлы на файловых системах FAT32, NTFS, EXT2, EXT3 и EXT4;
- содержимое энергонезависимой памяти CMOS;
- ресурсы конфигурационного пространства PCI/PCIe;
- таблиц ACPI;
- таблиц SMBIOS;
- карты распределения памяти;
- образ BIOS и собственных модулей ViPNet SafeBoot;
- загрузочных секторов (MBR) на носителях информации;
- реестра Windows;
- завершенность транзакций в журналах файловых систем NTFS, EXT3 и EXT4.

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

Администратор имеет возможность провести принудительную проверку целостности всех контролируемых объектов (см. «Принудительная проверка целостности» на стр. 70), а также выполнить перерасчет эталонов (см. «Перерасчет эталонных контрольных сумм» на стр. 69).

Автоопределение компонентов загрузки ОС

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

Чтобы запустить автоматическое построение списков контроля, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Контроль целостности**.
- 3 Выберите **Автоопределение компонентов загрузки ОС**.

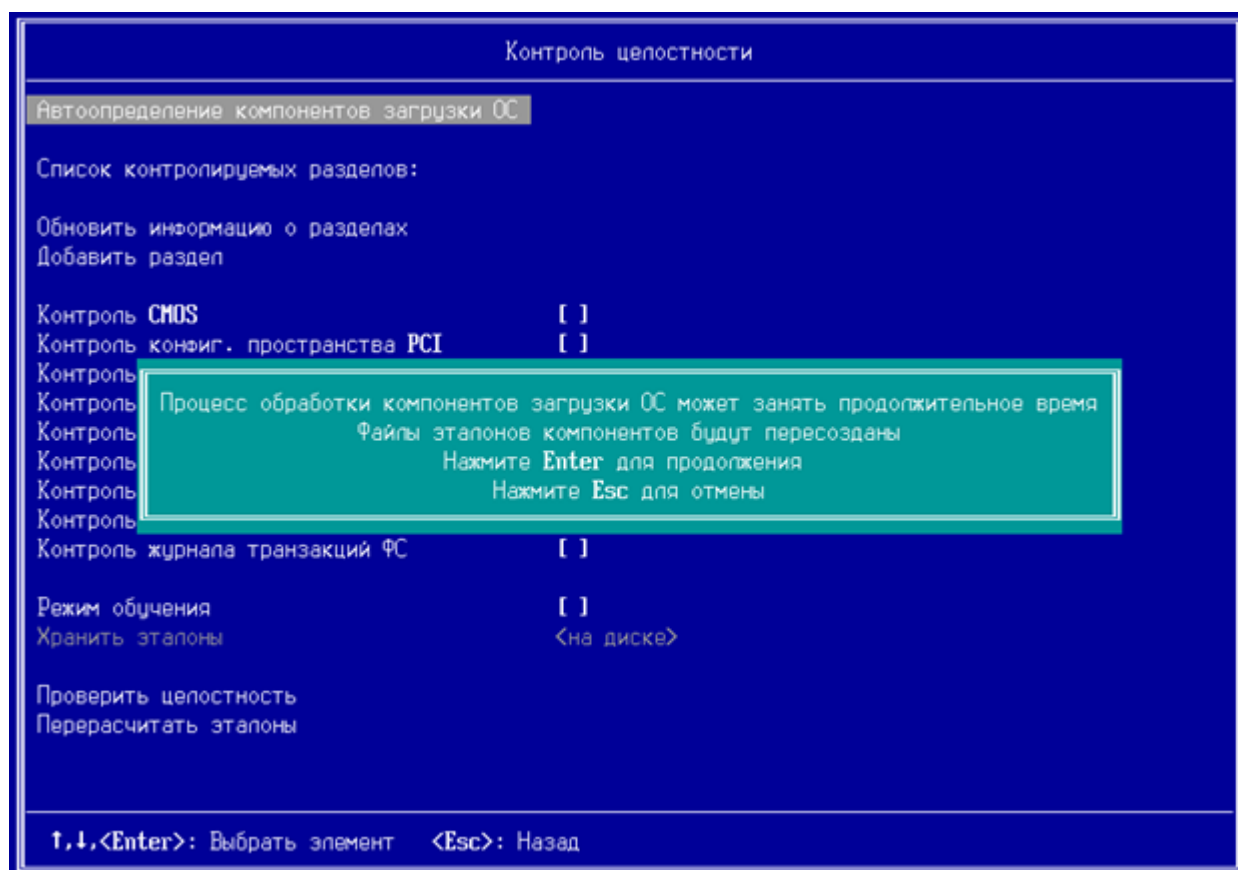
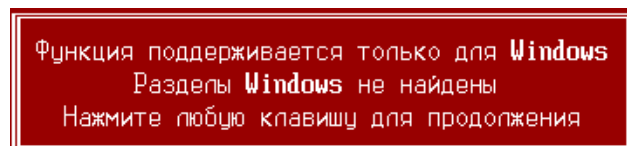


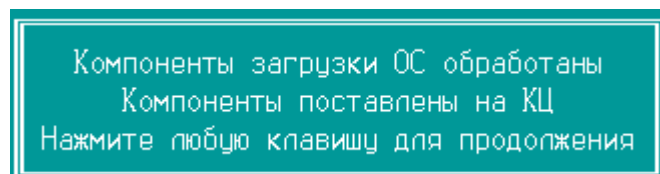
Рисунок 34. Меню Контроль целостности

- 4 Нажмите **Enter** для начала обработки компонентов загрузки ОС.

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



При успешном завершении обработки компонентов загрузки ОС появится следующее сообщение:



Нажмите любую клавишу для продолжения.

Контроль разделов и файлов

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

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Контроль целостности**.

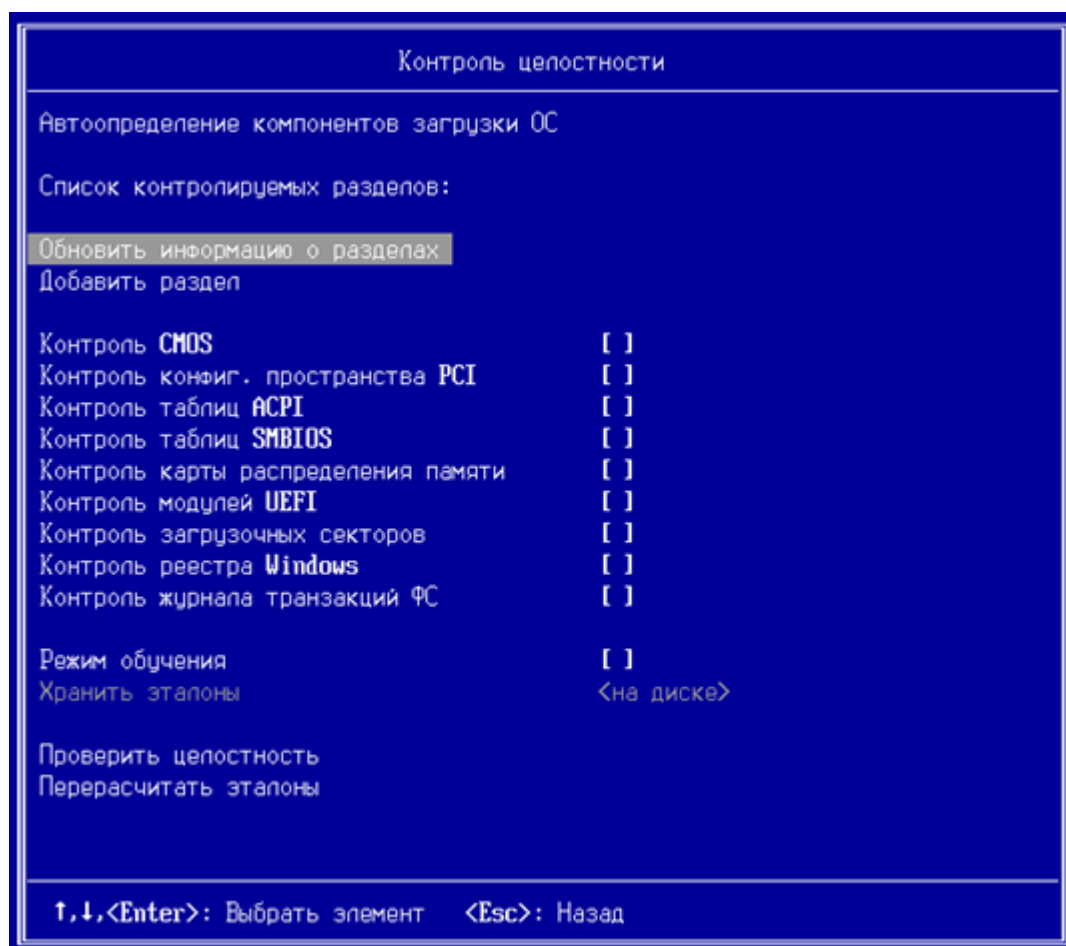


Рисунок 35. Меню Контроль целостности

- 3 Для добавления на контроль целостности всех разделов с подготовленными эталонами 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.

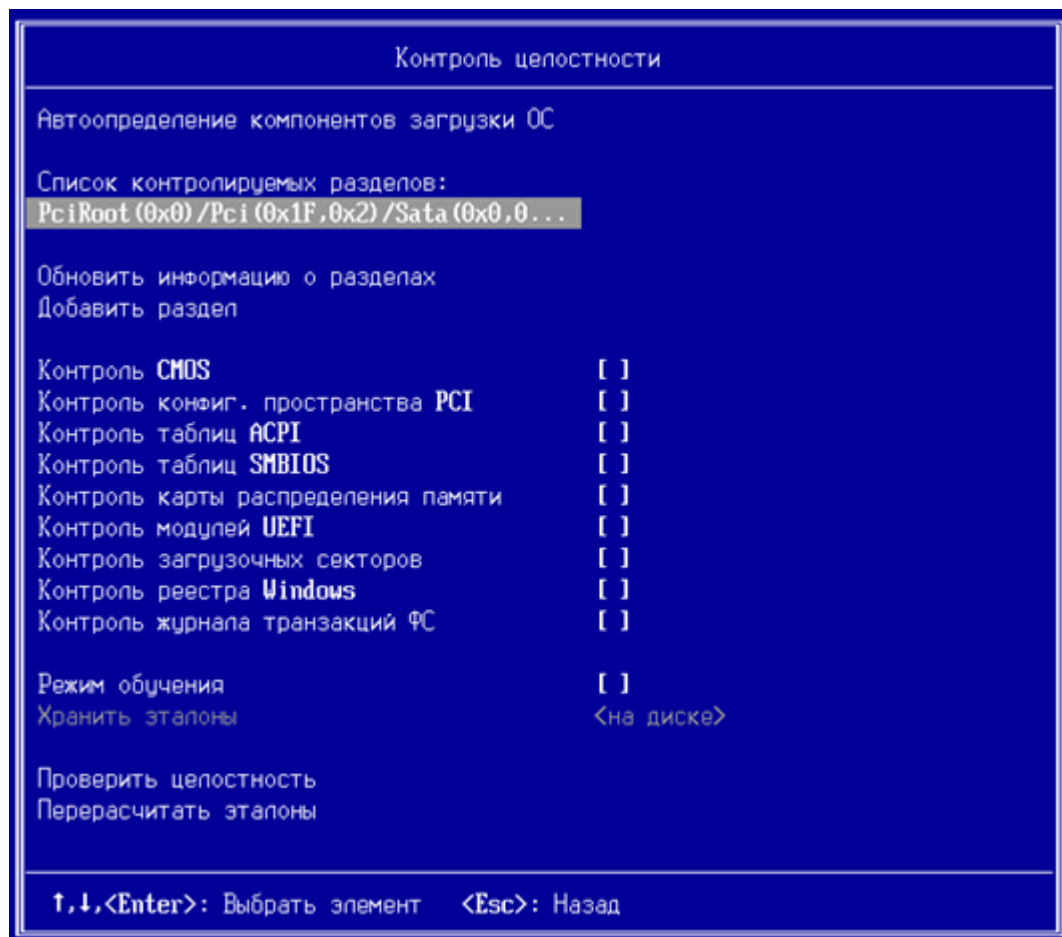


Рисунок 36. Список контролируемых разделов



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

5 Для операций контроля файлов выберите пункт меню **Список контролируемых разделов**.

В отрывшемся окне (см. рис. 37) 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.

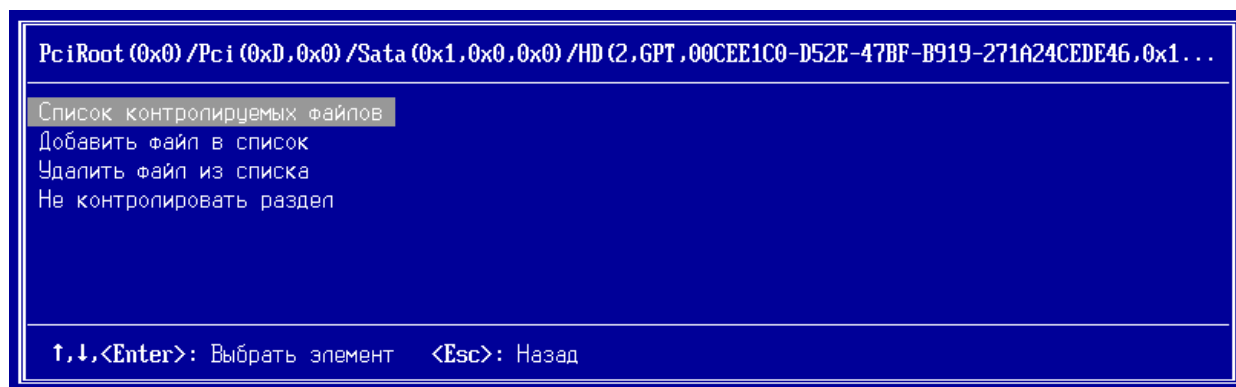


Рисунок 37. Операции контроля файлов

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.

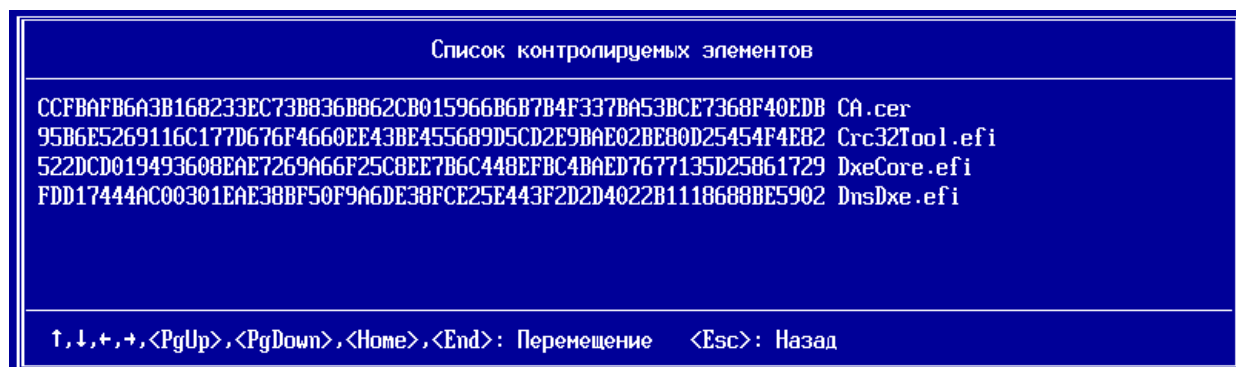


Рисунок 38. Список контролируемых файлов на разделе файловой системы

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**, при этом сами эталоны из раздела не удаляются.

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. 34).
- 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.

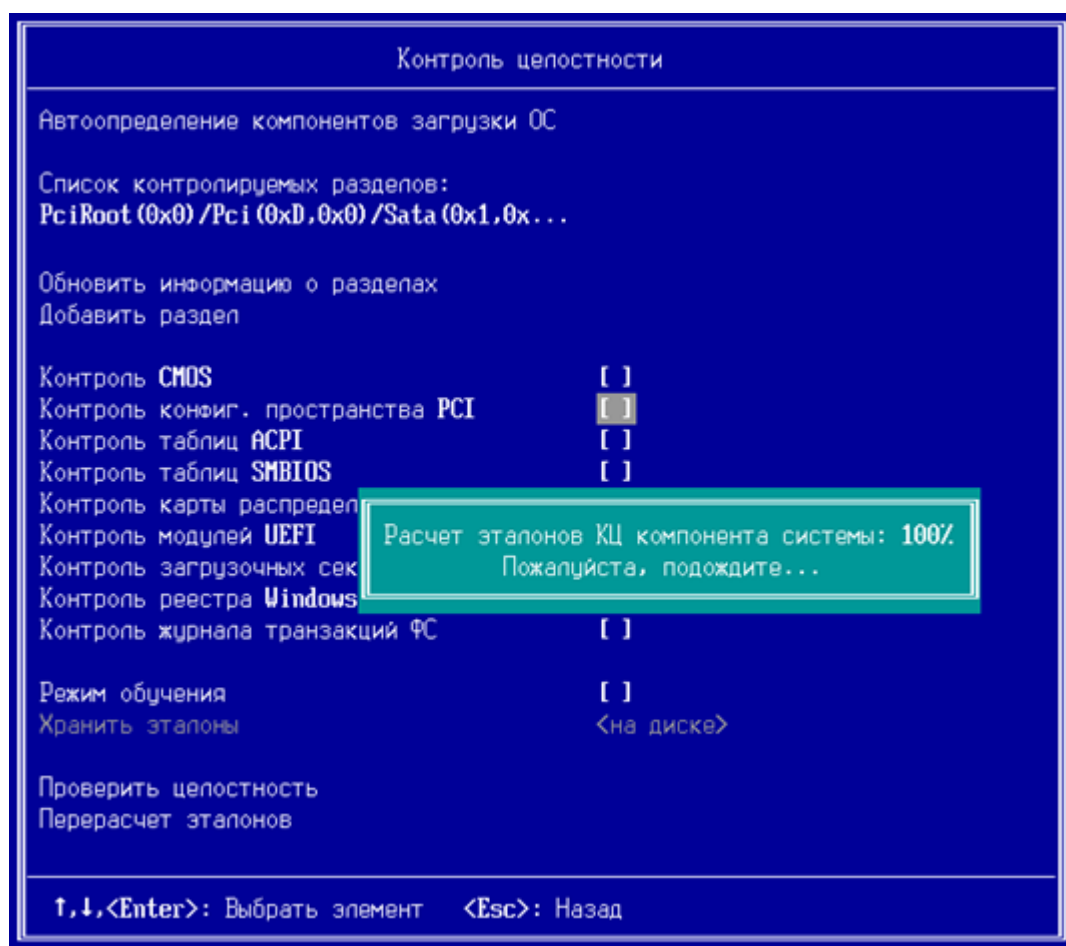


Рисунок 39. Расчет эталонов контрольных сумм состава аппаратных средств



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

Контроль реестра Windows

Для контроля реестра Windows, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Контроль целостности**.
- 3 В меню **Контроля целостности** нажмите **Enter** на пункте **Контроль реестра Windows**.

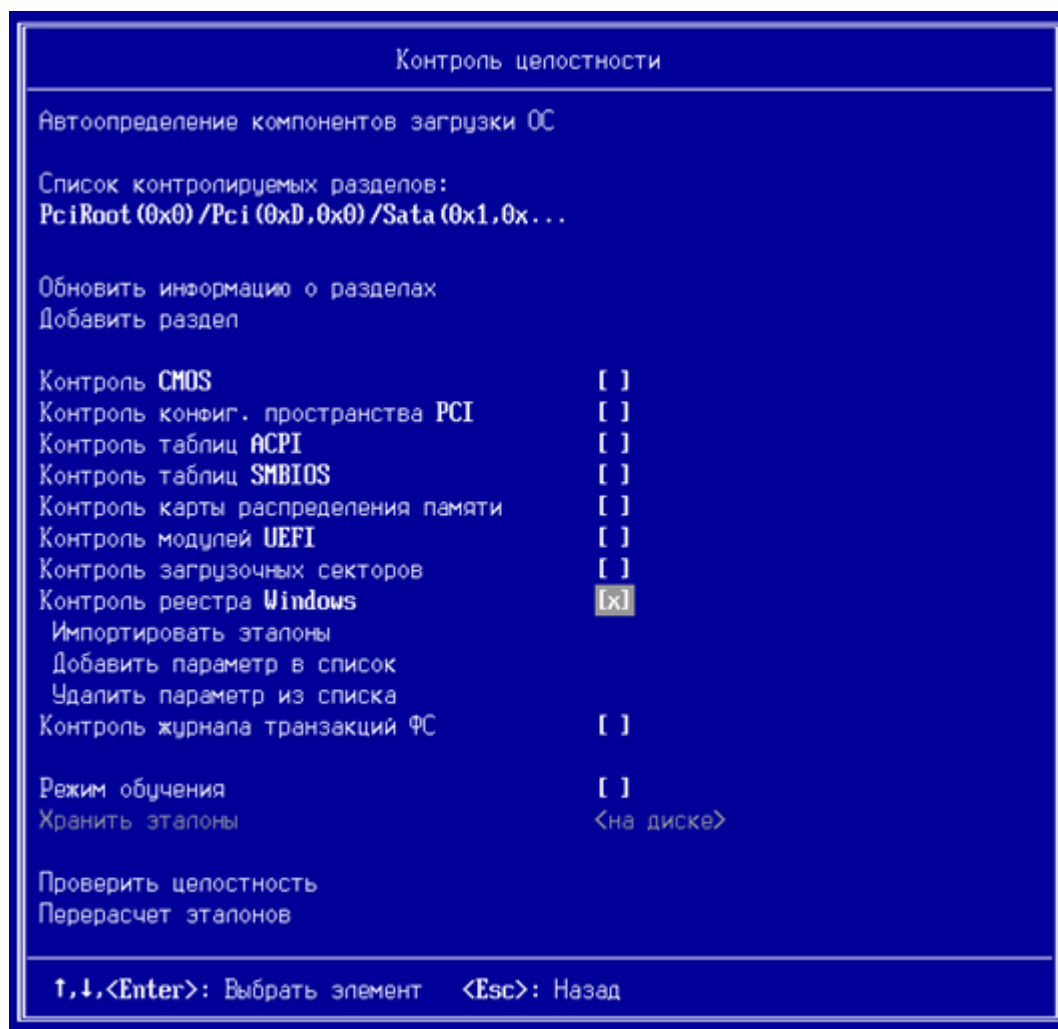


Рисунок 40. Выбор контроля реестра Windows

Откроется меню управления параметрами реестра Windows, содержащее следующие пункты:

- Импортировать эталоны;
- Добавить параметр в список;
- Удалить параметр из списка.

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

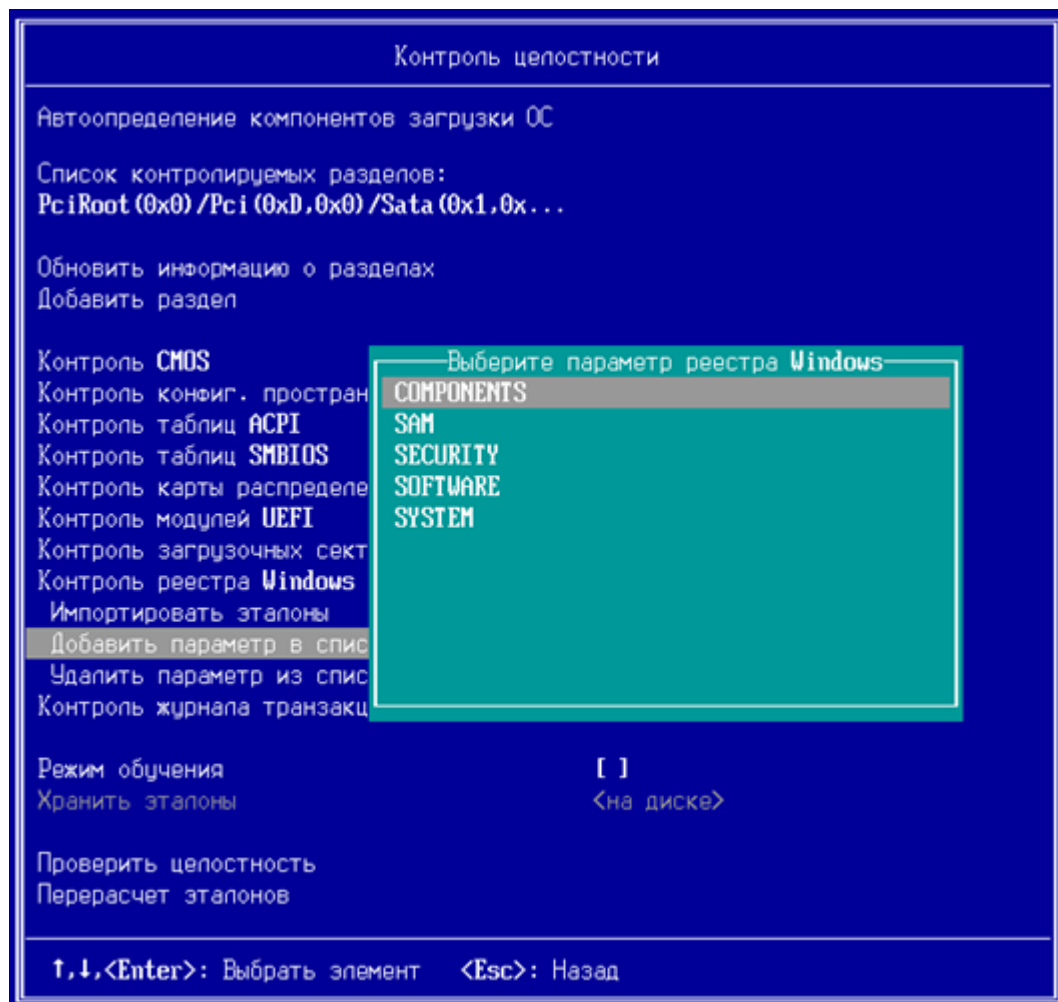


Рисунок 41. Выбор параметра реестра Windows

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

-

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

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

```
0000000000000000000000000000000000000000000000000000000000000000 <имя параметра реестра  
Windows с полным путем>
```

```
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SnIcon
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnCloneVault\Start
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDacs\Group
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnEraser\Icon
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Subsystems\SnLDBType
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Subsystems\SnPcType
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnCDFilter\Group
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDisKEnc\Start
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Subsystems\SnOptions\Type
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sncc0\Type
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDisKEnc\Group
000000000000000000000000000000000000000000000000000 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SnDiskFilter\ImagePath
```

ViPNet SafeBoot. Руководство администратора | 64

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

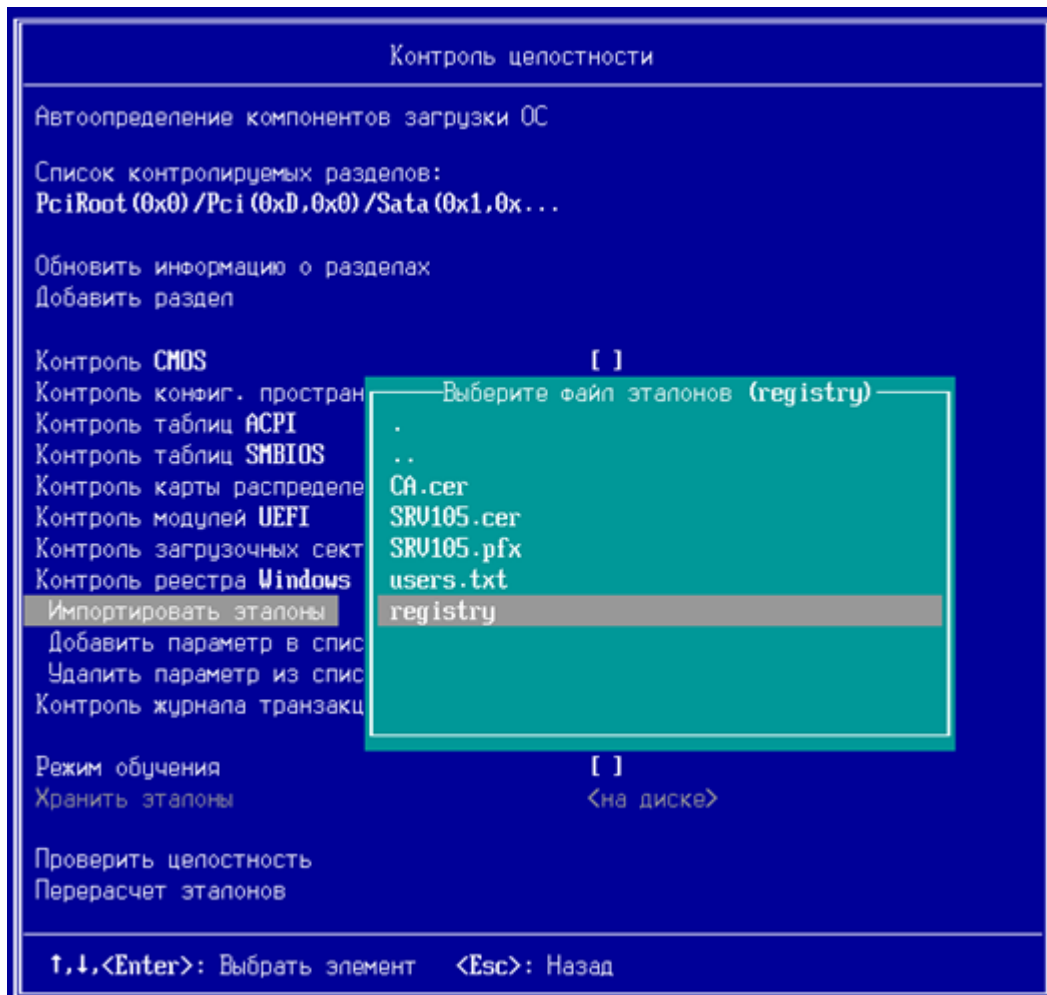
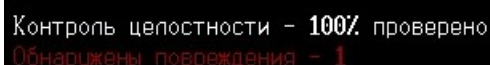


Рисунок 44. Выбор файла эталонов

Режим обучения

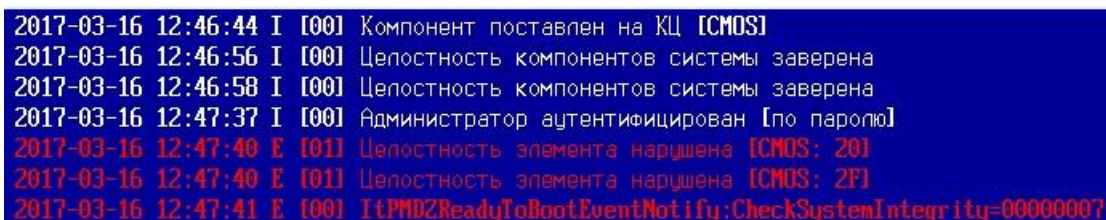
Включение опции **Режим обучения** используется для исключения из контроля целостности отдельных элементов компонентов, изменяемых при нормальном функционировании системы (например, при контроле CMOS). Элементы, не прошедшие проверку целостности, снимаются с контроля целостности, что позволяет «обучить»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

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



Контроль целостности - 100% проверено
Обнаружены повреждения - 1

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



```
2017-03-16 12:46:44 I [00] Компонент поставлен на КЦ [CMOS]
2017-03-16 12:46:56 I [00] Целостность компонентов системы заверена
2017-03-16 12:46:58 I [00] Целостность компонентов системы заверена
2017-03-16 12:47:37 I [00] Администратор аутентифицирован [по паролю]
2017-03-16 12:47:40 E [01] Целостность элемента нарушена [CMOS: 20]
2017-03-16 12:47:40 E [01] Целостность элемента нарушена [CMOS: 2F]
2017-03-16 12:47:41 E [00] ItPMB2ReadyToBootEventNotify:CheckSystemIntegrity=00000007
```

Рисунок 45. 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. 34).
- 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**.

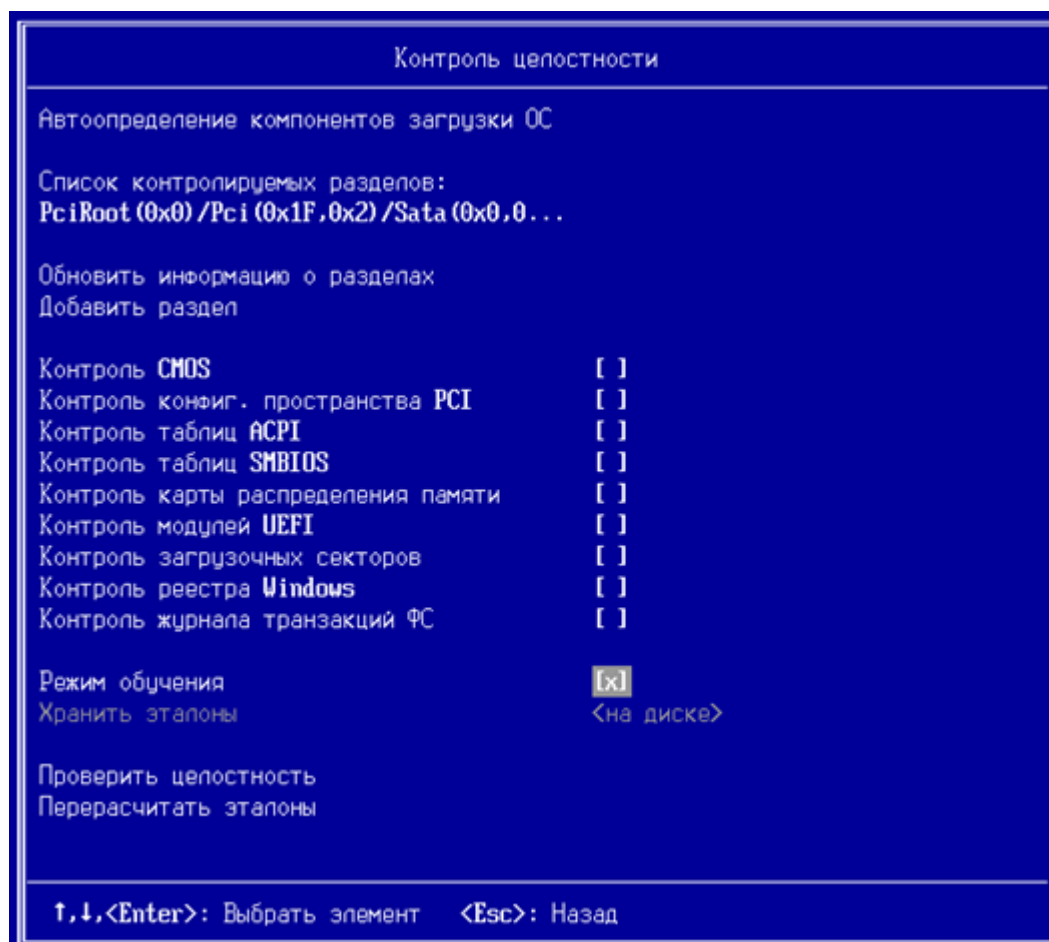


Рисунок 46. Включение опции **Режим обучения**

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

Контроль целостности – 100% проверено
Обнаружены повреждения – 1

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

```
2017-03-16 12:50:22 I [00] Режим обучения КЦ включен
2017-03-16 12:50:24 I [00] Целостность компонентов системы заверена
2017-03-16 12:50:27 I [00] Целостность компонентов системы заверена
2017-03-16 12:51:10 I [00] Администратор аутентифицирован [по паролю]
2017-03-16 12:51:13 I [01] Элемент снят с КЦ (режим обучения) [CMOS: 20]
2017-03-16 12:51:13 I [01] Элемент снят с КЦ (режим обучения) [CMOS: 2F]
2017-03-16 12:51:45 I [00] Администратор аутентифицирован [по паролю]
```

Рисунок 47. Записи в журнале событий о снятых с контроля целостности элементах

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

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



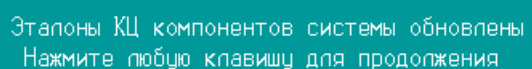
Примечание. Для того чтобы вновь поставить на контроль целостности элементы, снятые режимом обучения, следует в меню **Контроль целостности** снять с контроля компонент, измененный режимом обучения, а затем опять поставить его на контроль.

Перерасчет эталонных контрольных сумм

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

Чтобы пересчитать эталонные контрольные суммы, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Контроль целостности**.
- 3 В открывшемся окне выберите **Перерасчет эталонов**.
- 4 Дождитесь появления на экране сообщения:



Эталонные КЦ компонентов системы обновлены
Нажмите любую клавишу для продолжения

Нажмите любую клавишу для продолжения.

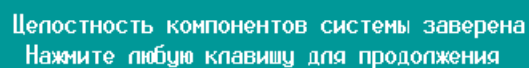
Принудительная проверка целостности

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

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 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:



Целостность компонентов системы завершена
Нажмите любую клавишу для продолжения

- 5 Нажмите любую клавишу, затем клавишу **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 (хэш-функции), 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	73
Создание диска восстановления	74
Восстановление пароля администратора	76
Добавление учетных записей пользователей с аутентификацией по паролю	78
Добавление учетных записей пользователей с аутентификацией по электронному идентификатору	82
Добавление учетных записей пользователей с аутентификацией по электронному идентификатору и паролю	91
Добавление учетных записей пользователей с аутентификацией по паролю на электронном идентификаторе	96
Добавление учетных записей пользователей с LDAP аутентификацией	100
Редактирование учетных записей пользователей	101
Редактирование учетной записи пользователя с аутентификацией по электронному идентификатору	102
Удаление учетных записей пользователей	104

Учетные записи пользователей

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

- Имя учетной записи (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!

Общее максимальное количество учетных записей — 32.

Создание диска восстановления

Диск восстановления может понадобиться Администратору при потере аутентификационных данных либо для временного отключения функциональности ViPNet SafeBoot («Временное отключения функциональности ViPNet SafeBoot» на стр. 53). Процесс создания диска восстановления состоит в создании на USB-носителе уникального ключа восстановления.



Внимание!

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

Чтобы подготовить диск восстановления пароля Администратора, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Пользователи**.
- 3 В открывшемся окне выберите **Administrator**.

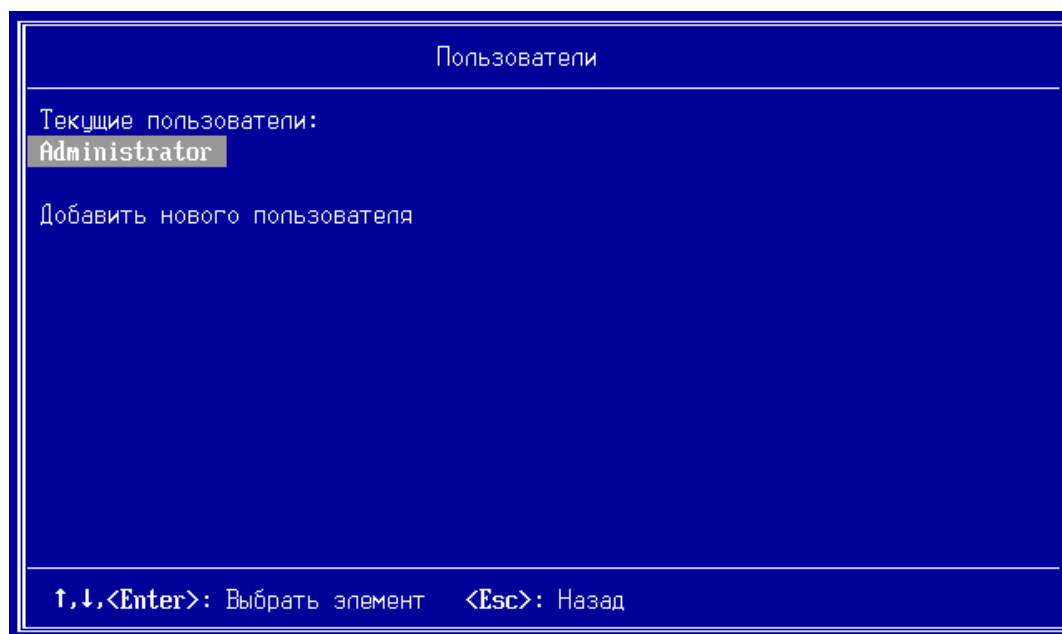
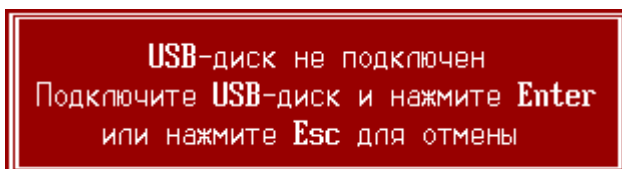


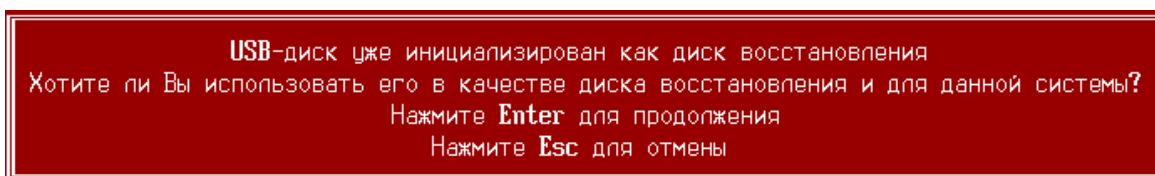
Рисунок 48. Выбор учетной записи Администратора

- 4 Подключите USB-накопитель.
- 5 В окне **Настройки пользователя** выберите **Подготовить диск восстановления**.
 - При отсутствии подключенного USB-накопителя появится следующее сообщение:



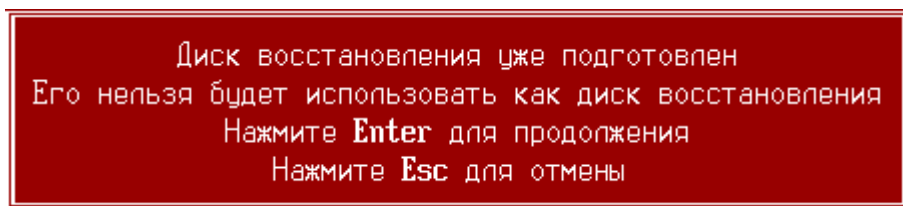
Подключите USB-накопитель и нажмите **Enter**.

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



Нажмите **Enter** для продолжения или **Esc**, если хотите использовать другой USB-накопитель.

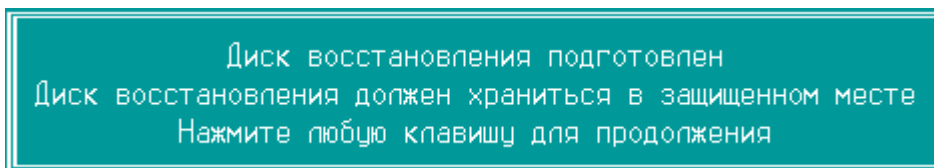
- Если ранее уже создавался диск восстановления, то появится следующее сообщение:



○

Нажмите **Enter** для продолжения или **Esc**, если хотите использовать другой USB-накопитель.

- После успешного создания диска восстановления появится следующее сообщение:



Нажмите любую клавишу для продолжения и уберите созданный диск восстановления в защищенное место.

- 6 Для выхода в основное меню нажмите два раза клавишу **Esc**.

Восстановление пароля администратора

Восстановление пароля Администратора возможно, только если ранее был создан диск восстановления (см. «Создание диска восстановления» на стр. 74).

Для восстановления пароля Администратора, выполните следующие действия:

- 1 Подключите USB-накопитель, инициализированный как диск восстановления.
- 2 Для входа в режим восстановления при загрузке нажмите сочетание клавиш **Ctrl + r**.

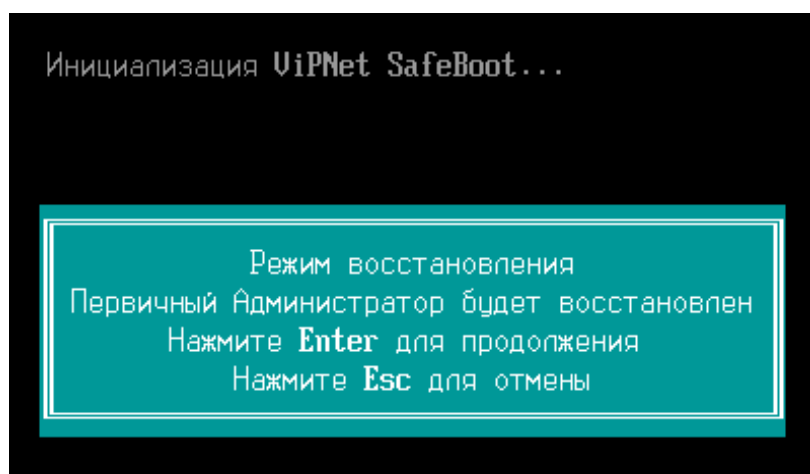
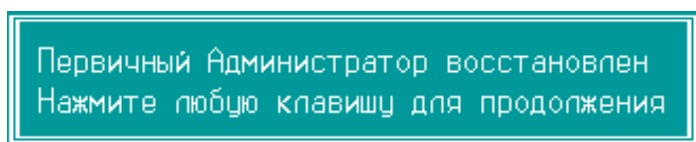


Рисунок 49. Вход в режим восстановления

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



- 4 Нажмите любую клавишу для продолжения.

На экране появится приглашение к авторизации. Порядок действий такой же, как при первом включении (см. «Первый запуск» на стр. 23).

- При появлении приглашения ввести имя пользователя, введите логин **Administrator**.
- При появлении приглашения ввести пароль, введите пароль **12345678**.
- В режиме настройки установите новый пароль Администратора.

Информация о восстановлении будет отражена в журнале событий.

Журнал событий				
2017-12-17 13:03:20	I	[00]	Свободное место в NURAM распределено [журнал: 6990, БД: 6900]	
2017-12-17 13:03:21	I	[00]	Рабочая директория ПМДЗ инициализирована	
2017-12-17 13:03:24	I	[00]	Параметры загрузки должны быть настроены	
2017-12-17 13:03:33	I	[11]	Администратор аутентифицирован [Administrator, по паролю]	
2017-12-17 13:03:37	I	[0F]	Использование параметров загрузки BIOS включено	
2017-12-17 13:04:04	I	[0F]	Пароль пользователя изменен [Administrator]	
2017-12-17 13:06:46	I	[16]	Диск восстановления импортирован	
2017-12-17 13:06:53	I	[0F]	Система перезагружена	
2017-12-17 13:07:17	I	[16]	Первичный Администратор восстановлен	
2017-12-17 13:14:49	I	[11]	Администратор аутентифицирован [Administrator, по паролю]	
↑,↓,+,+,<PgUp>,<PgDown>,<Home>,<End>: Перемещение <Esc>: Назад				

Рисунок 50. Записи журнала событий после восстановления пароля Администратора

Добавление учетных записей пользователей с аутентификацией по паролю

Чтобы добавить учетную запись пользователя, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите **Пользователи**.
- 3 В открывшемся окне выберите **Добавить нового пользователя**.

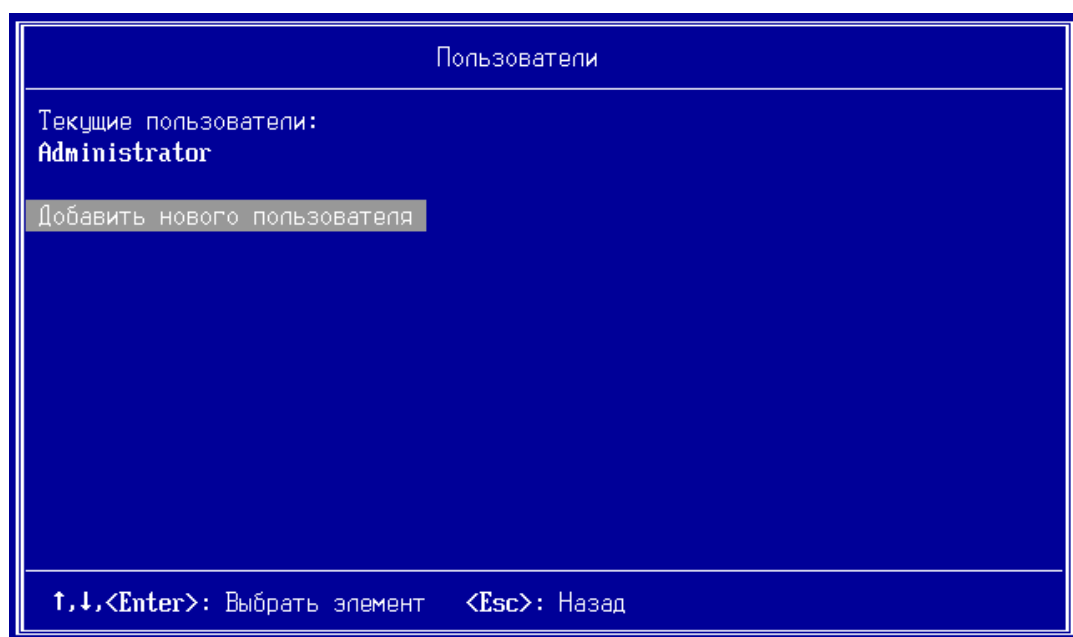


Рисунок 51. Добавление нового пользователя

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

Введите имя пользователя.

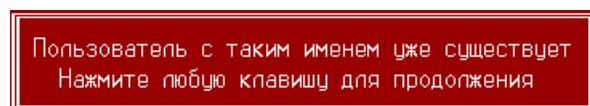


Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».



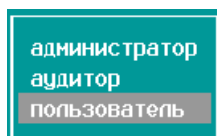
Рисунок 52. Приглашение ввести Имя пользователя

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



5 Выберите пункт **Роль**.

В открывшемся списке выберите роль:

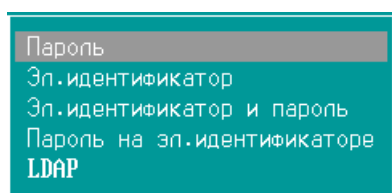


Внимание!

Общее максимальное количество пользователей — 32.

6 Выберите пункт **Способ аутентификации**.

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



7 Выберите пункт **Изменить пароль**.



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

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

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 пункт или оставьте значение по умолчанию.



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

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

8.1 Для изменения срока действия пароля оставьте флажок **Ограничить срок действия пароля**, выберите пункт **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 соответствующее сообщение о необходимости смены пароля, пользователь блокируется до смены пароля.

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

Настройки пользователя сохранены
Нажмите любую клавишу для продолжения

- 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. 34).
- 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.



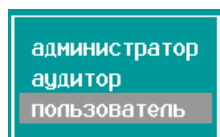
Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

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

Пользователь с таким именем уже существует
Нажмите любую клавишу для продолжения

- 5 Выберите пункт **Роль**.

В открывшемся списке выберите роль:

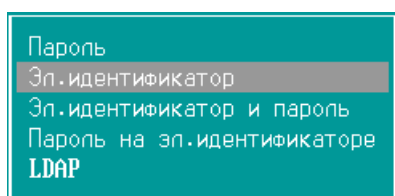


Внимание!

Общее максимальное количество пользователей — 32.

- 6 Выберите пункт **Способ аутентификации**.

В открывшемся списке выберите способ аутентификации **Эл. идентификатор**:



Меню **Настройки пользователя** примет следующий вид:

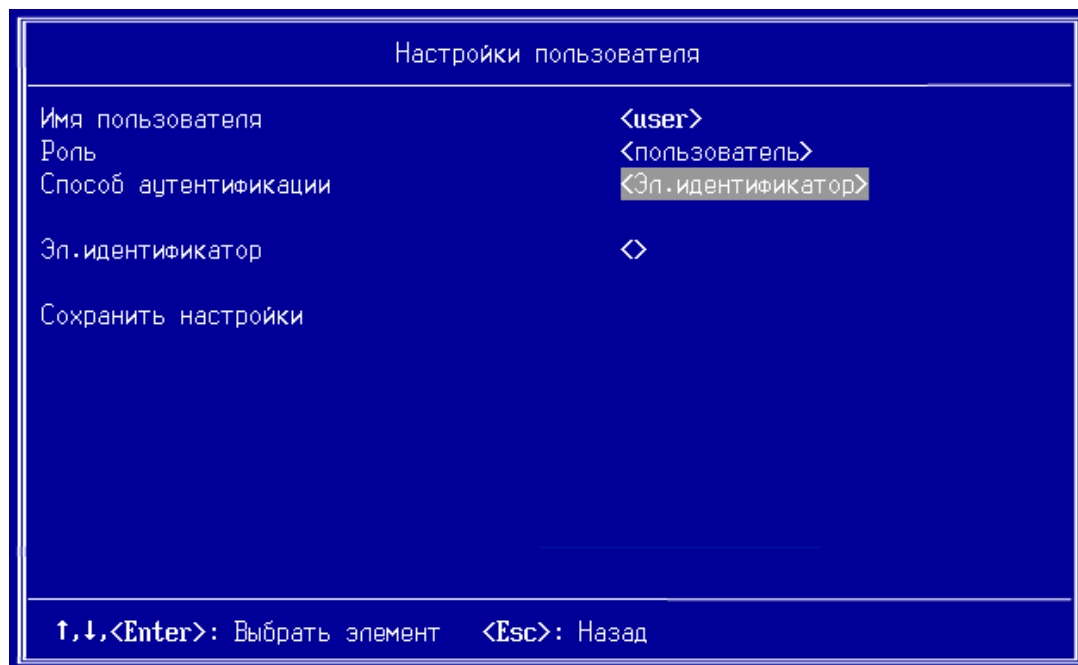


Рисунок 53. Меню *Настройки пользователя* при выбранном способе аутентификации «Электронный идентификатор»



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 пункт **Эл. 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 (см «Подготовка к работе Guardant ID» на стр. 113).

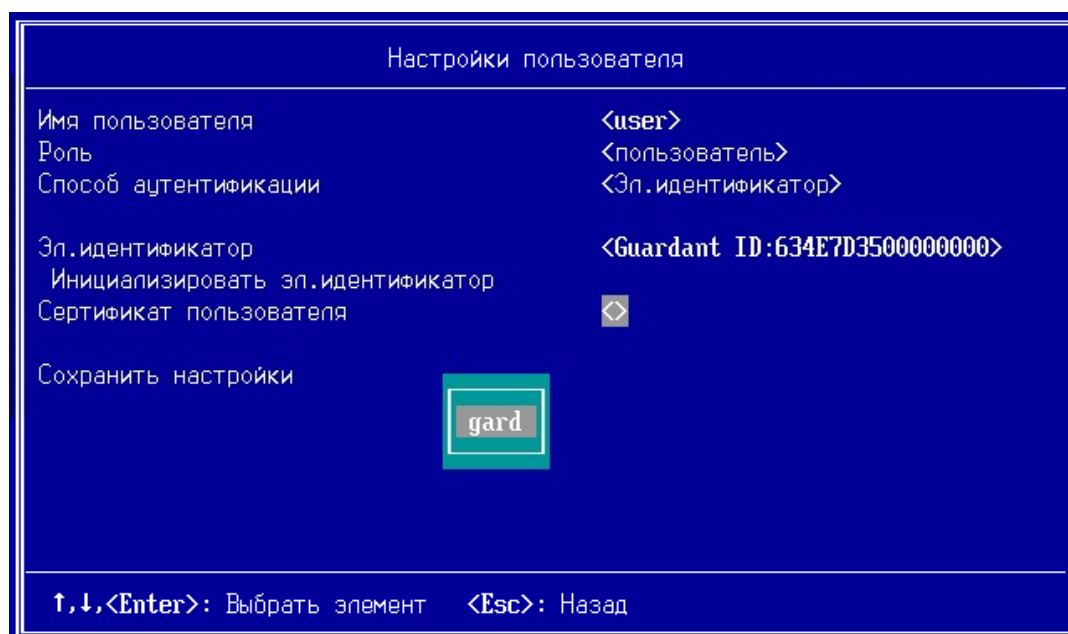
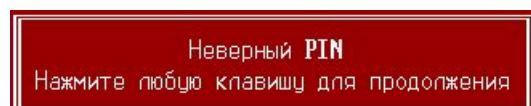


Рисунок 54. Выбор сертификата на электронном идентификаторе Guardant ID

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.

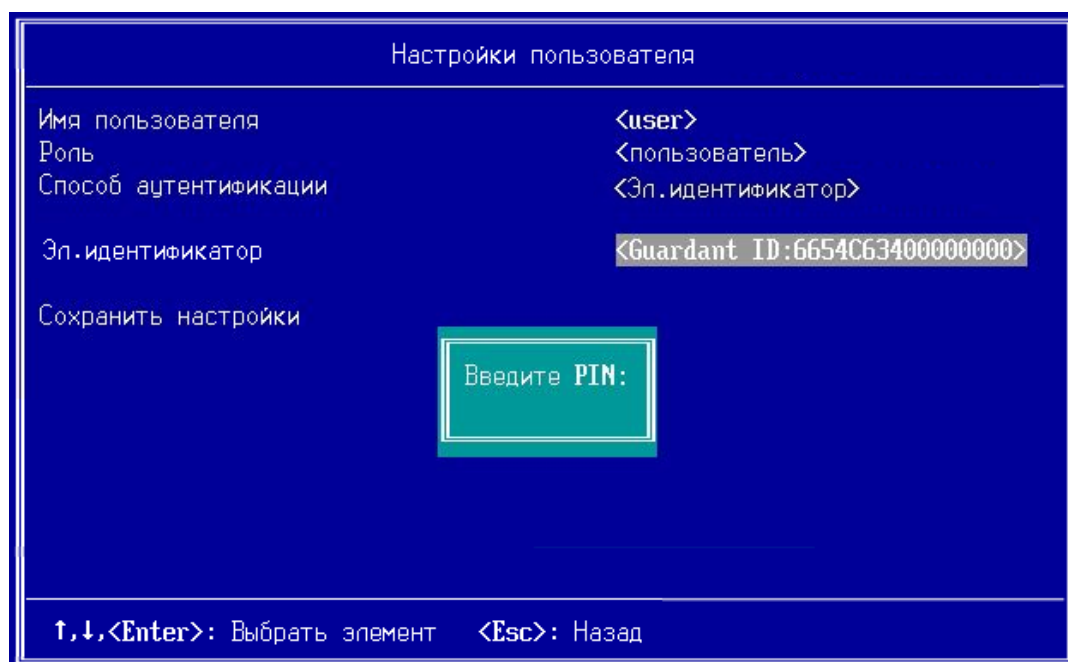


Рисунок 55. Приглашение ввести текущий PIN-код электронного идентификатора

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

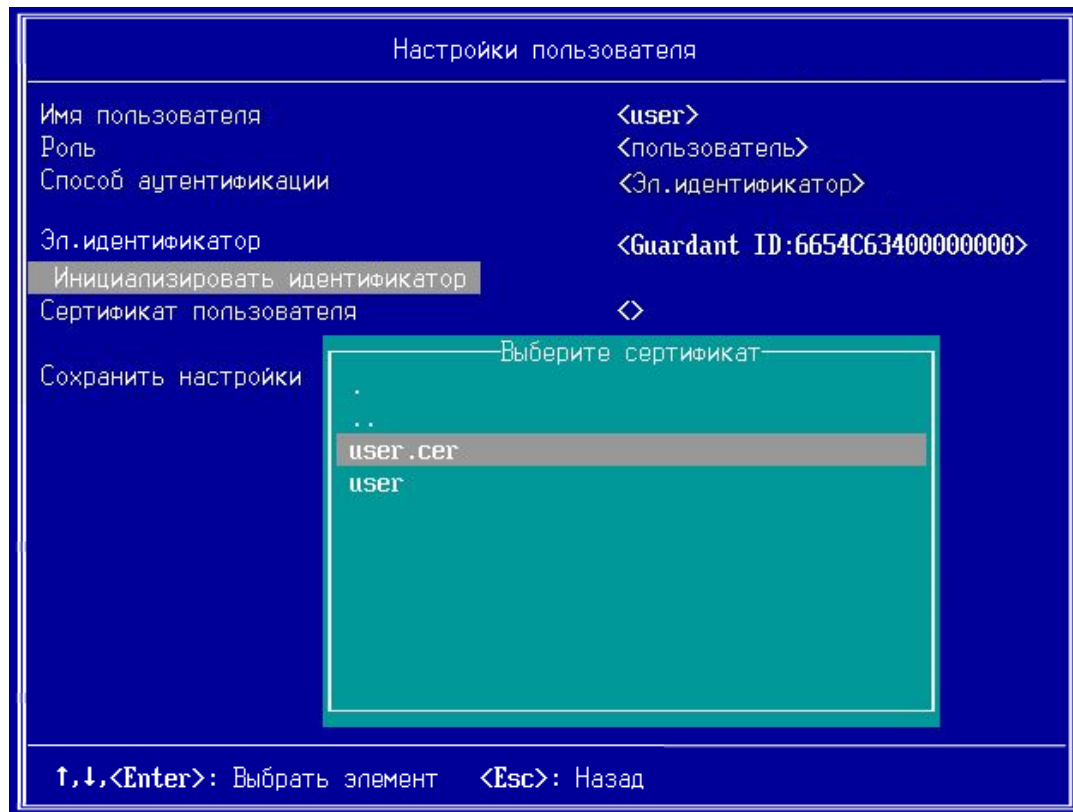


Рисунок 56. Выбор сертификата пользователя.

7.4 Выберите ключевой контейнер, соответствующий сертификату.

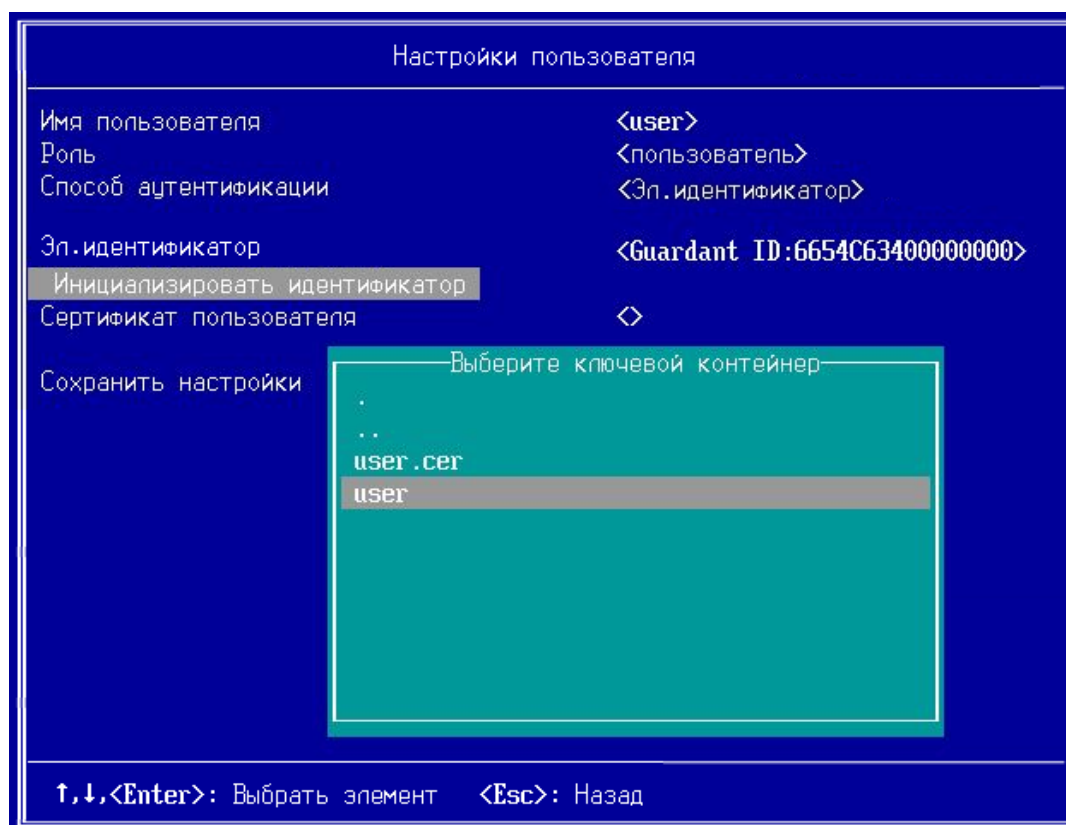


Рисунок 57. Выбор ключевого контейнера

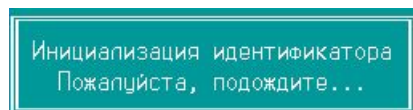
7.5 После приглашения ввести PIN, введите PIN-код контейнера.

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

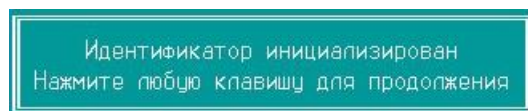


В случае отказа (при нажатии **Esc**) электронный идентификатор не инициализируется.

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**.

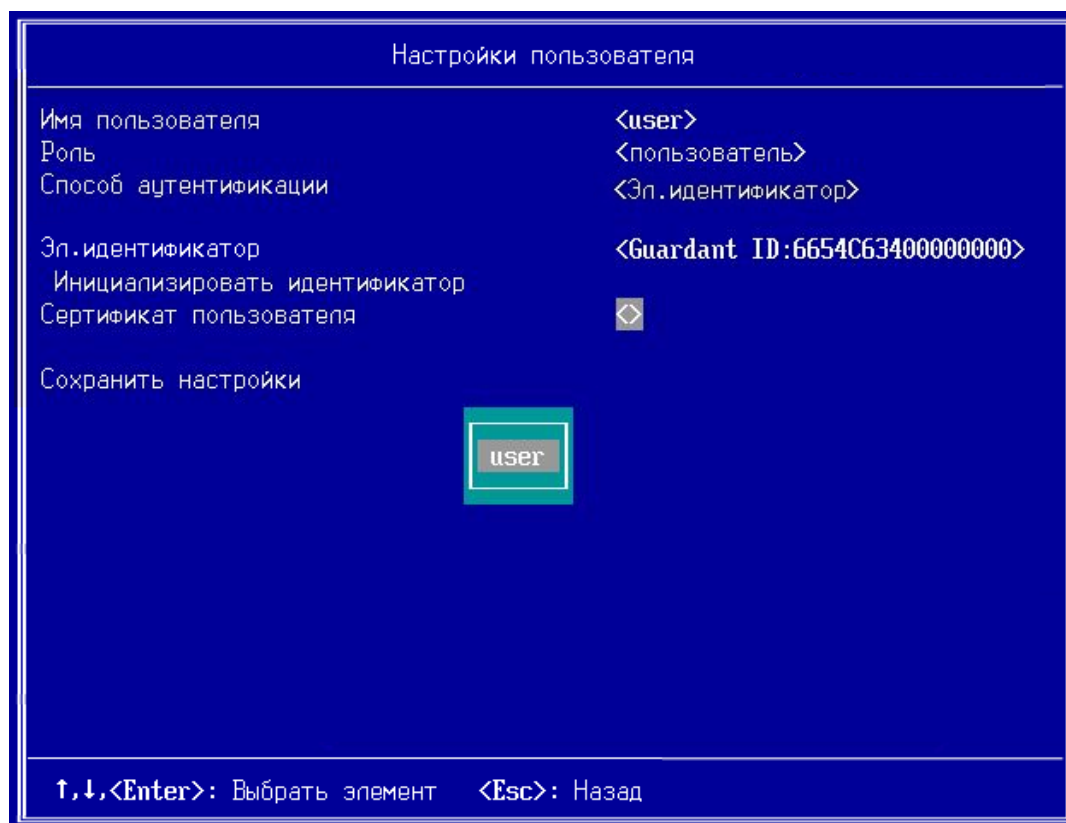
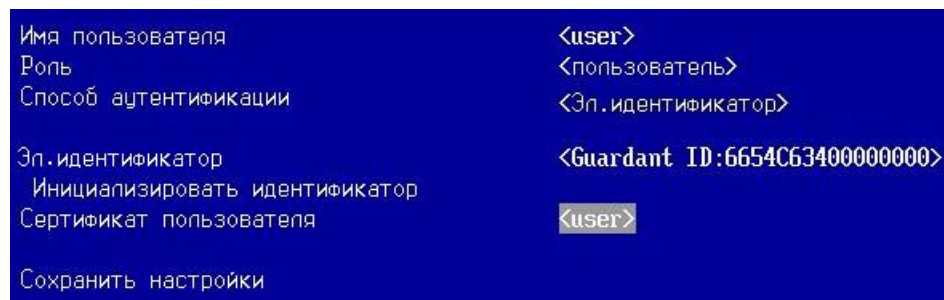


Рисунок 58. Выбор сертификата пользователя

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



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

8.1 Выберите пункт Эл. идентификатор.

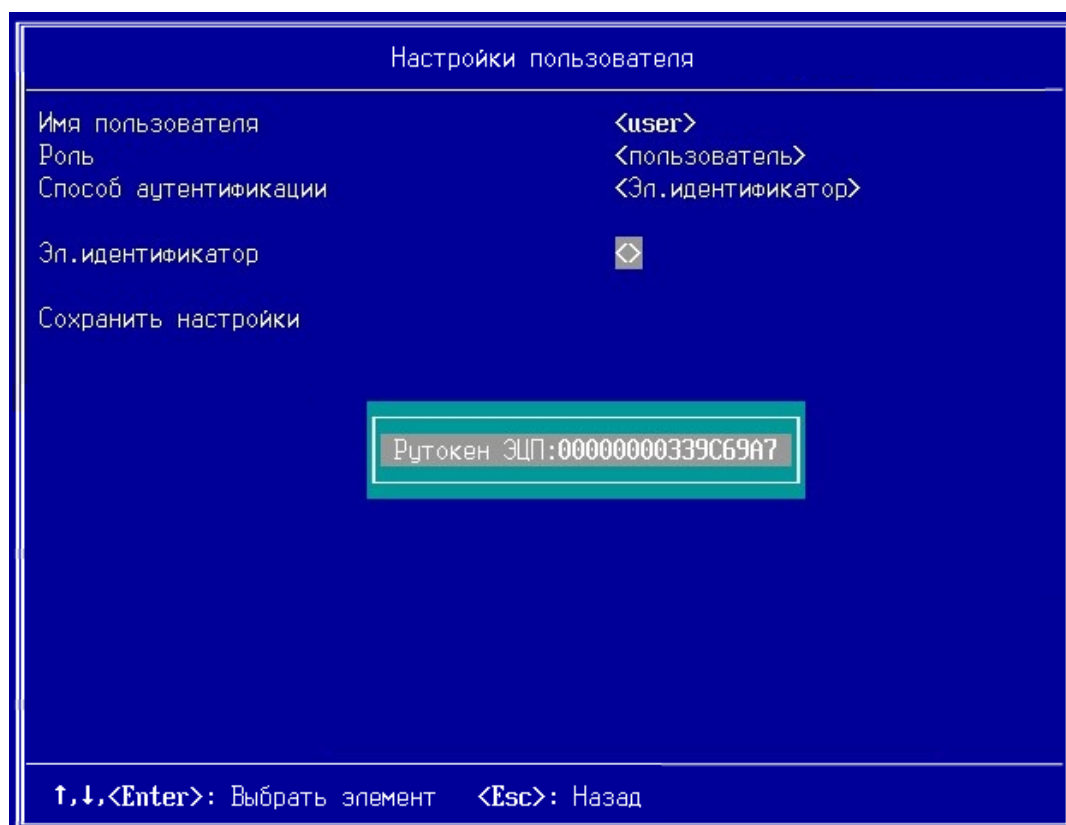
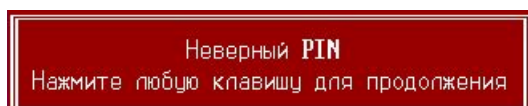


Рисунок 59. Выбор в качестве электронного идентификатора Рутокен ЭЦП

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**.

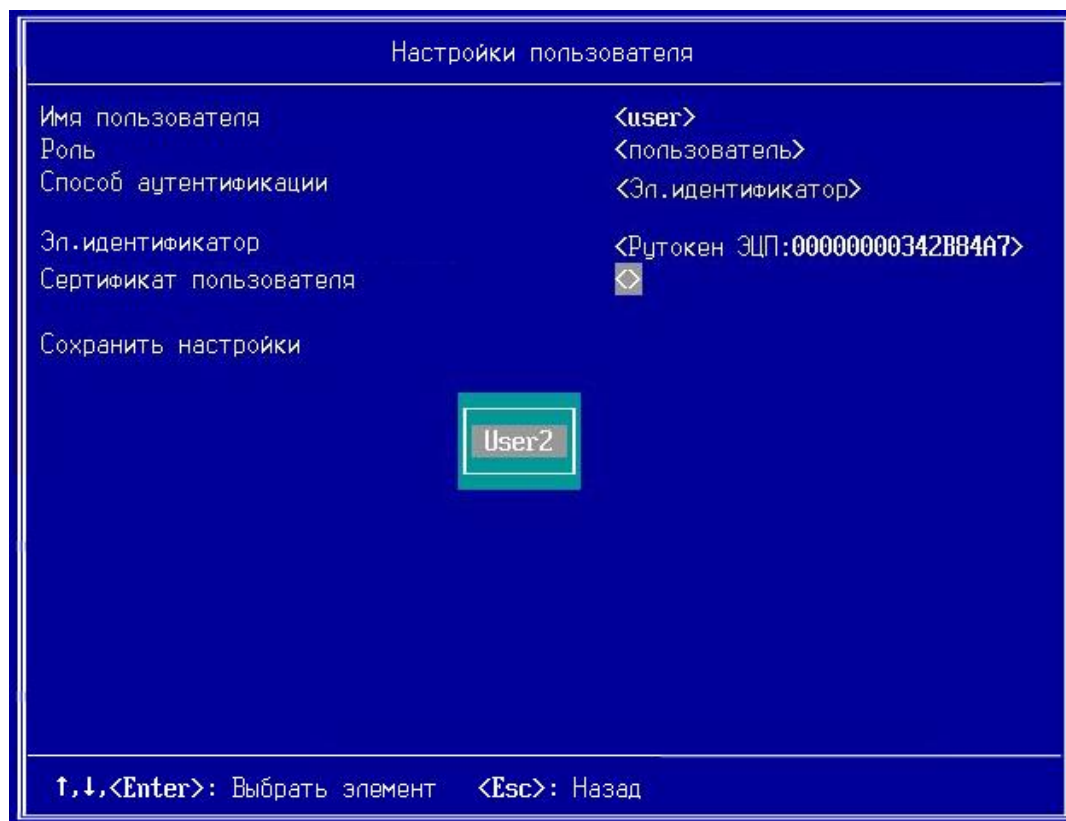
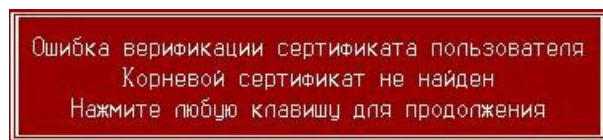
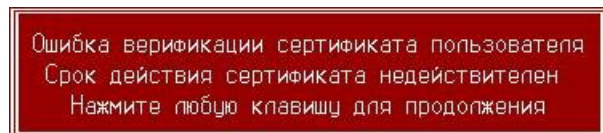


Рисунок 60. Выбор сертификата пользователя

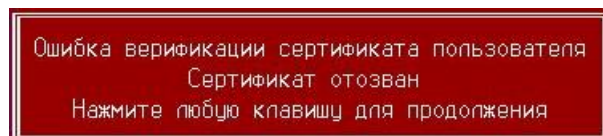
Если корневой сертификат отсутствует, появится сообщение об ошибке:



Если сертификат просрочен, появится следующее сообщение:



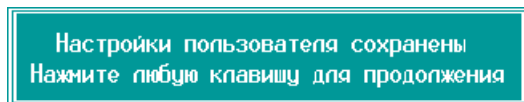
Если сертификат пользователя был внесен в список отозванных сертификатов (CRL), то появится следующее сообщение об ошибке:



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

Имя пользователя	<user>
Роль	<пользователь>
Способ аутентификации	<Эл.идентификатор>
Эл.идентификатор	<Путокен ЭЦП:00000000342BB4A7>
Сертификат пользователя	<user>

- 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. 34).
- 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.



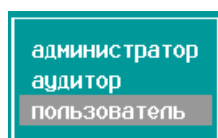
Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

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

Пользователь с таким именем уже существует
Нажмите любую клавишу для продолжения

- 5 Выберите пункт **Роль**.

В открывшемся списке выберите роль:

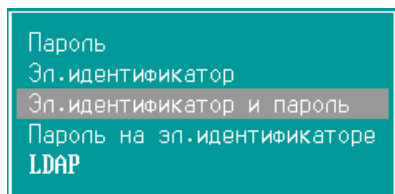


Внимание!

Общее максимальное количество пользователей — 32.

6 Выберите пункт **Способ аутентификации**.

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



Меню **Настройки пользователя** примет следующий вид:

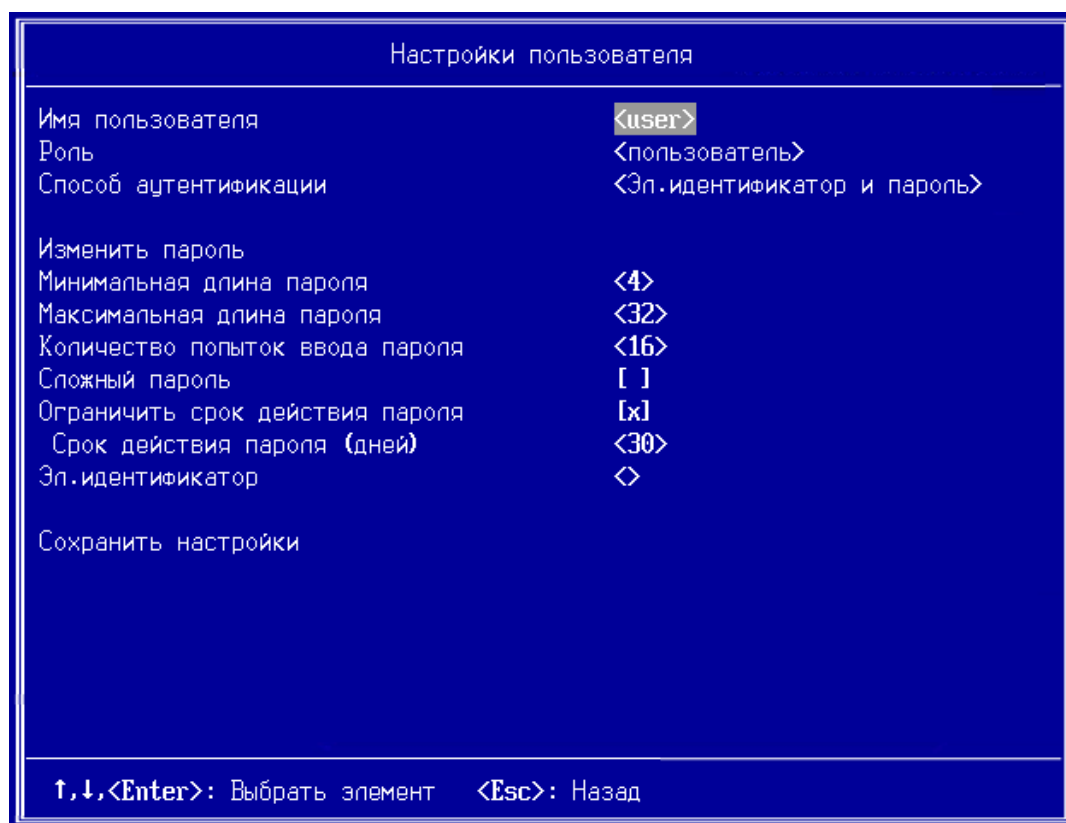


Рисунок 61. Меню **Настройки пользователя** при выбранном способе аутентификации **Электронный идентификатор и пароль**

7 Выберите пункт Эл. идентификатор.

Настройки пользователя

Имя пользователя	<user>
Роль	<пользователь>
Способ аутентификации	<Эл.идентификатор и пароль>
Изменить пароль	
Минимальная длина пароля	<4>
Максимальная длина пароля	<32>
Количество попыток ввода пароля	<16>
Сложный пароль	[]
Ограничить срок действия пароля	[x]
Срок действия пароля (дней)	<30>
Пароль действует до:	2017-05-11 12:47:42
Эл.идентификатор	⏏
Сохранить настройки	

Рутокен ЭЦП: 00000000342BB4A7

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

Рисунок 62. Выбор в качестве электронного идентификатора Рутокен ЭЦП

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

Введите PIN: XXXXXXXXXX

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

Настройки пользователя

Имя пользователя	<user>
Роль	<пользователь>
Способ аутентификации	<Эл.идентификатор и пароль>
Изменить пароль	
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)	<30>
Пароль действует до: 2017-05-11 12:49:55	
Эл.идентификатор	<Руткен ЭЦП:00000000342B84A7>
Сертификат пользователя	

Сохранить настройки

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

Рисунок 63. Выбор сертификата пользователя

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

Имя пользователя	<user>
Роль	<пользователь>
Способ аутентификации	<Эл.идентификатор и пароль>
Изменить пароль	
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)	<30>
Пароль действует до: 2017-05-11 12:49:55	
Эл.идентификатор	<Руткен ЭЦП:00000000342B84A7>
Сертификат пользователя	<user>

10 Выберите пункт **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.
-

11 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.
-

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

Настройки пользователя сохранены
Нажмите любую клавишу для продолжения

13 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 паролю на электронном идентификаторе

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

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 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.



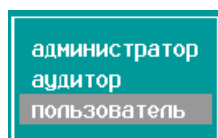
Примечание. Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

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

Пользователь с таким именем уже существует
Нажмите любую клавишу для продолжения

- 5 Выберите пункт **Роль**.

В открывшемся списке выберите роль:

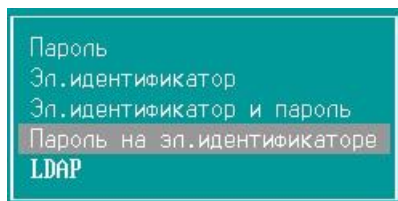


Внимание!

Общее максимальное количество пользователей — 32.

6 Выберите пункт **Способ аутентификации**.

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



7 Выберите пункт **Эл. идентификатор**.

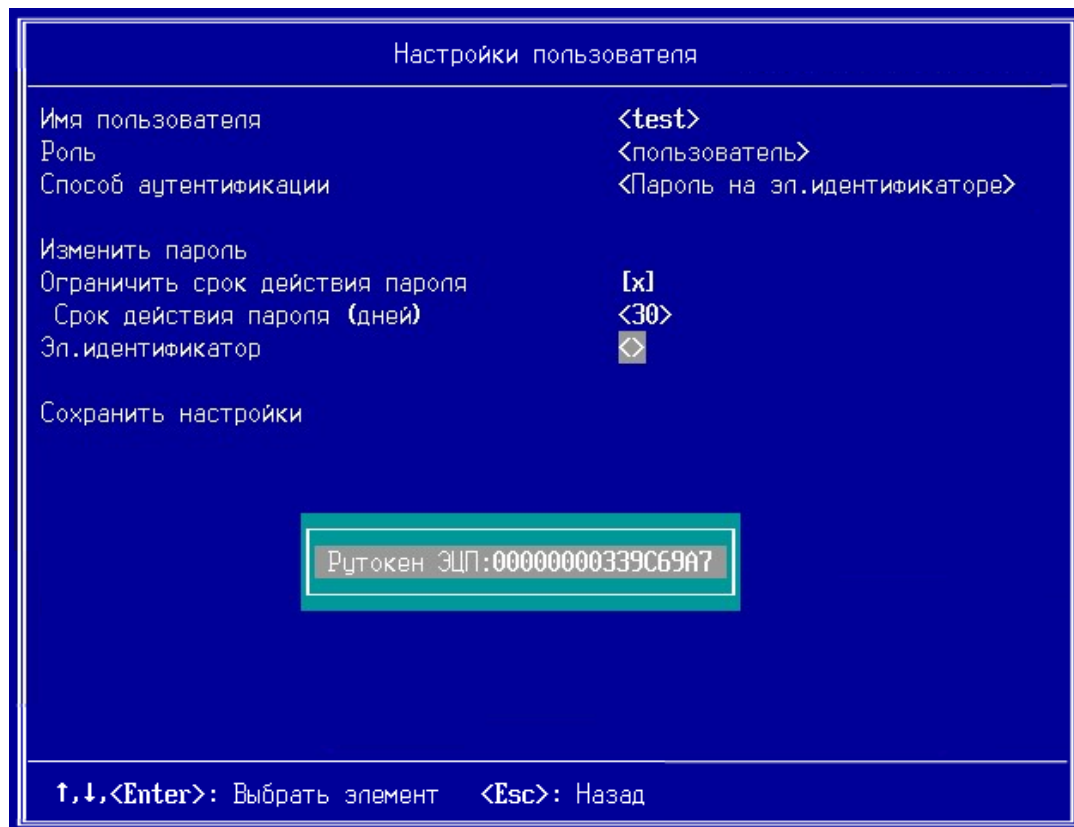


Рисунок 64. Выбор в качестве электронного идентификатора Рутокен ЭЦП

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



9 Выберите пункт **Изменить пароль**.

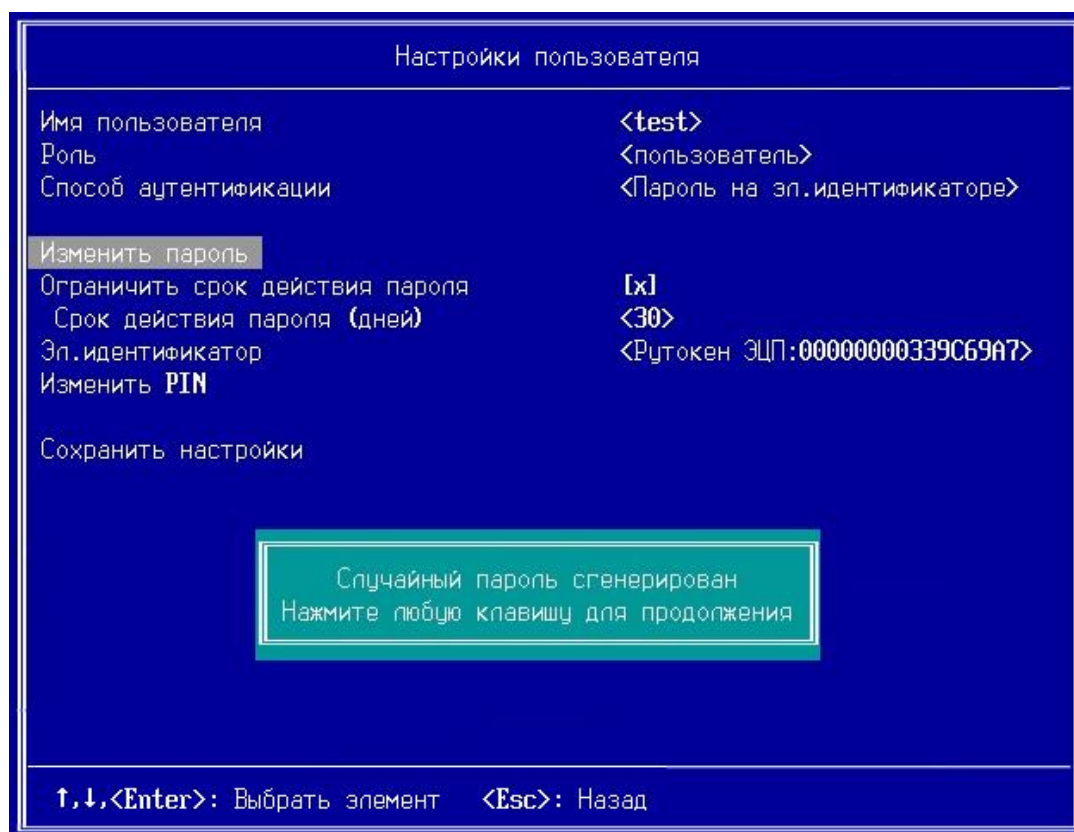


Рисунок 65. Генерация случайного пароля на электронном идентификаторе

10 Дождитесь появления сообщения об окончании генерации случайного пароля и нажмите любую клавишу.

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

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



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



Нажмите **Enter** для сохранения настроек.

Настройки пользователя сохранены
Нажмите любую клавишу для продолжения

- 12 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 LDAP аутентификацией

ViPNet SafeBoot позволяет выполнять аутентификацию пользователей, осуществляемую непосредственно LDAP сервером. Администратору ViPNet SafeBoot предоставляется управление разрешениями путем установки списков разрешенных пользователей. Для доступа к этой функции требуется предварительно осуществить настройку сети и LDAP. Порядок выполнения настроек приведен в разделе «Настройки сети и LDAP» на стр. 114.

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. 34).
- 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. 34).
- 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:

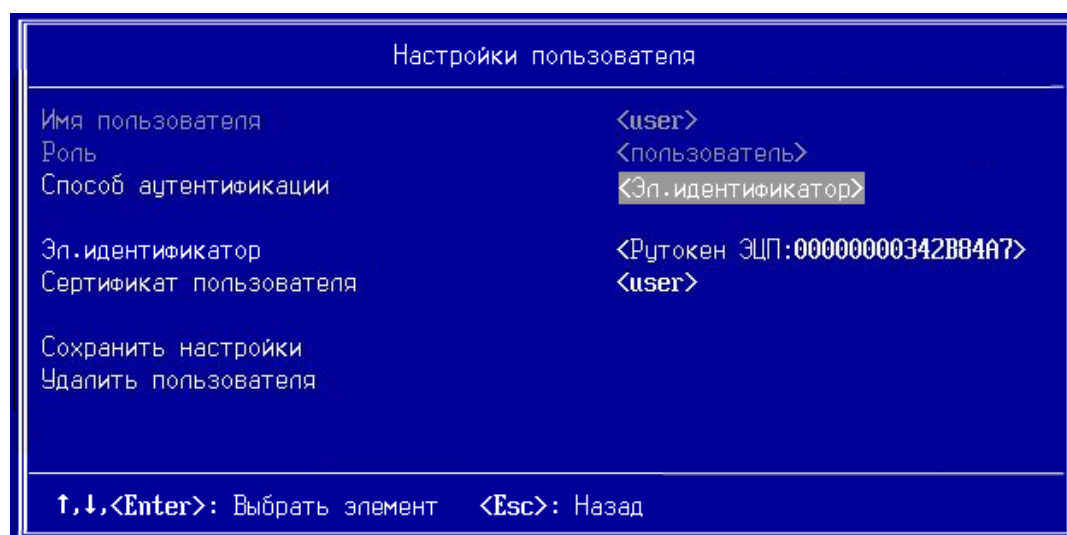


Рисунок 66. Вход в настройки пользователя с вводом PIN-кода

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

Настройки пользователя	
Имя пользователя	<user>
Роль	<пользователь>
Способ аутентификации	<Эл.идентификатор>
Эл.идентификатор	<Рyтокен ЭЦП:00000000342B8593>
Сертификат пользователя	<User>
Сохранить настройки	
Удалить пользователя	

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

Рисунок 67. Вход в настройки пользователя без ввода PIN-кода (электронный идентификатор не подключен)

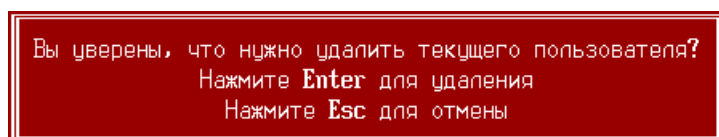
- 7 Выполненные изменения необходимо сохранить, выбрав **Сохранить настройки**.

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. 34).
- 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	106
Установка корневого сертификата	107
Удаление корневого сертификата	108
Операции со списком отозванных сертификатов (CRL)	109
Подготовка к работе электронных идентификаторов	112

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 пользователя, выданный от имени доверенного центра, а также сертификаты вышестоящих центров сертификации.

Чтобы установить корневой сертификат, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 Подключите USB накопитель, содержащий файл сертификата, который необходимо установить.
- 3 В меню режима настроек выберите **Корневые сертификаты**.
- 4 В открывшемся окне выберите **Установить корневой сертификат**.
- 5 Из списка выберите файл сертификата.

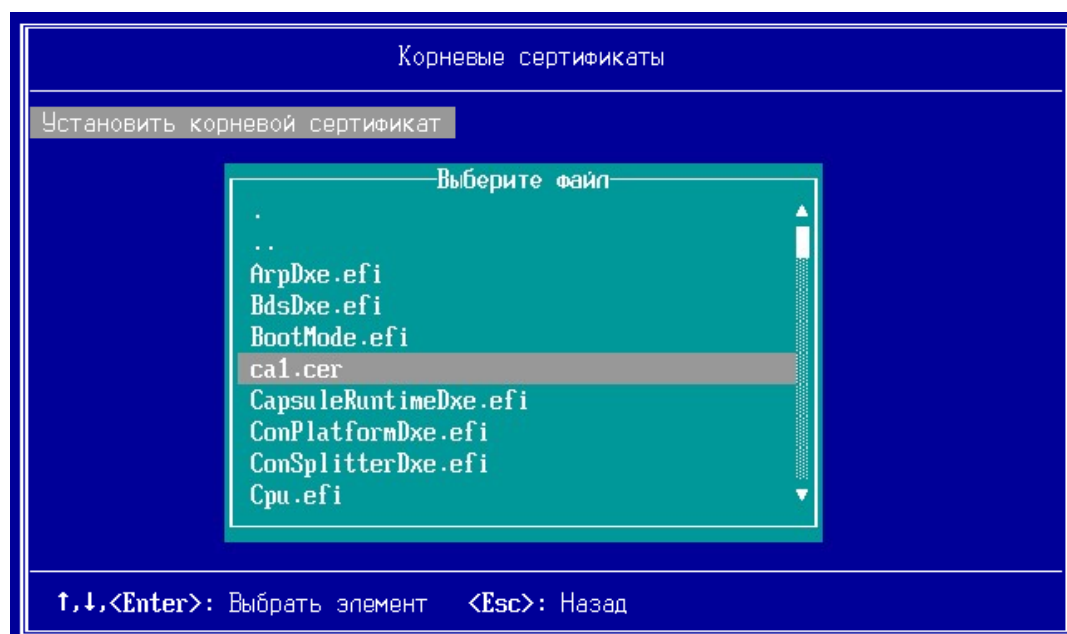


Рисунок 68. Выбор корневого сертификата

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. 34).
- 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. 34).
- 2 Подключите USB накопитель, содержащий файл CRL, который необходимо установить.
- 3 В меню режима настроек выберите **Корневые сертификаты**.
- 4 В открывшемся окне из списка **Установленные корневые сертификаты** выберите нужный сертификат.

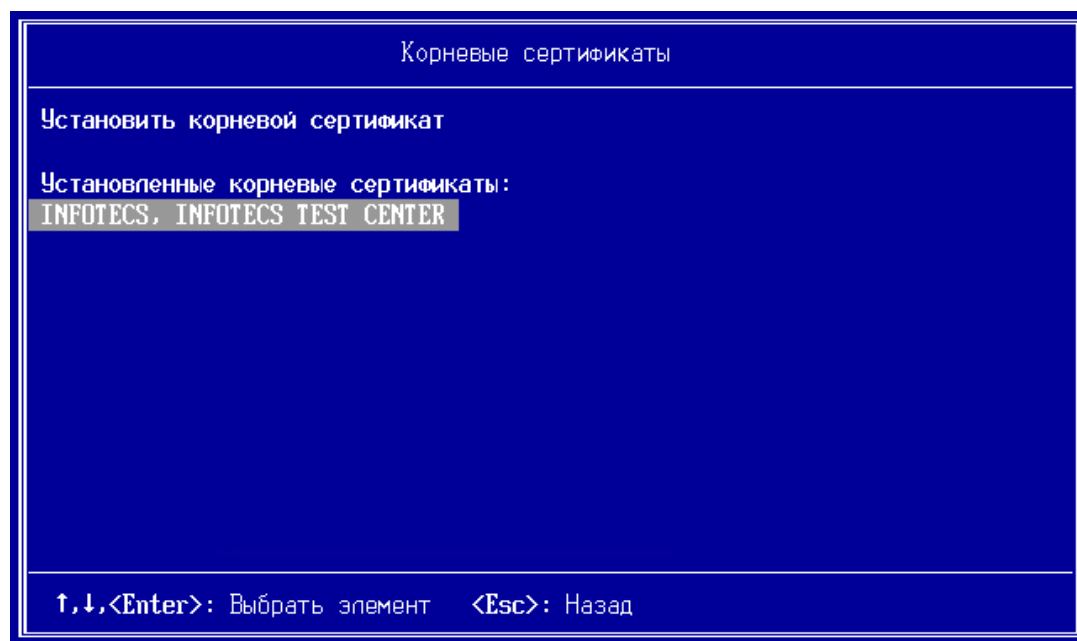


Рисунок 69. Выбор установленного сертификата

- 5 В открывшемся меню установленного сертификата выберите **Установить/обновить CRL**.
Откроется список доступных файлов для выбора.

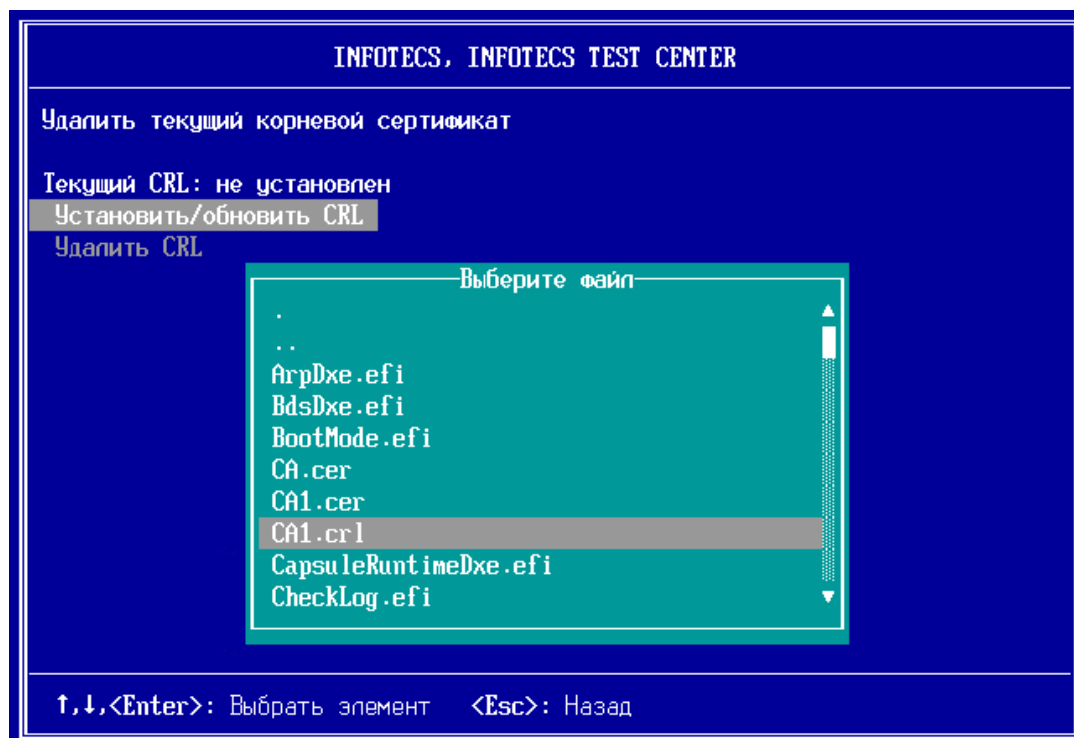


Рисунок 70. Выбор файла CRL

- 6 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. 34).
- 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. 34).
- 2 В меню режима настроек выберите **Корневые сертификаты**.
- 3 В открывшемся окне из списка **Установленные корневые сертификаты** выберите нужный сертификат.
- 4 В открывшемся меню установленного сертификата выберите **Удалить CRL**.

Выбранный CRL будет удален.

Подготовка к работе электронных идентификаторов

Подготовка к работе JaCarta PKI (USB/SC)

Для подготовки к работе электронного идентификатора JaCarta PKI необходимо установить на технологический ПК следующее программное обеспечение:

- «Единый клиент JaCarta» производства компании «Аладдин»;
- криптопровайдер ViPNet CSP;

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

- в ПО «Единый клиент JaCarta» произвести форматирование токена;
- при помощи утилиты «Создание запроса на сертификат» (входит в состав криптопровайдера ViPNet CSP) создать запрос на сертификат, указав носителем ключевой информации электронный идентификатор;
- получить сертификат передав запрос в удостоверяющий центр;
- в криптопровайдере ViPNet CSP записать полученный сертификат на электронный идентификатор;

В данной версии ViPNet SafeBoot поддерживается только один сертификат на электронном идентификаторе. В случае замены сертификата необходимо провести повторное форматирование электронного идентификатора.

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

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

- комплект ПО «Драйверы Рутокен для Windows» производства компании «Актив»;
- криптопровайдер ViPNet CSP;

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

- в ПО «Панель управления Рутокен» (входит в комплект «Драйверы Рутокен для Windows») произвести форматирование токена;

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

В данной версии ViPNet SafeBoot поддерживается только один сертификат на электронном идентификаторе типа Рутокен. В случае замены сертификата необходимо провести повторное форматирование электронного идентификатора.

Подготовка к работе Guardant ID

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

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

- при помощи утилиты «Создание запроса на сертификат» (входит в состав криптопровайдера ViPNet CSP) создать запрос на сертификат, указав носителем ключевой информации корневой каталог на USB-носителе. Контейнер с ключевой информацией будет создан на USB-накопителе в каталоге \Infotecs\Containers;
- получить сертификат передав запрос в удостоверяющий центр;
- записать полученный сертификат на USB-носитель;
- инициализировать электронный идентификатор записав на него контейнер с ключевой информацией и сертификат (см. «Добавление учетных записей пользователей с аутентификацией по электронному идентификатору» стр. 83);

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

9

Настройки сети и LDAP

Настройки сети	115
Настройки подключения к LDAP серверу	118

Настройки сети

Раздел **Настройки сети** позволяет установить параметры, используемые для подключения ViPNet SafeBoot к сети.

Для настройки сети выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 2 В меню режима настроек выберите пункт **Настройки сети и LDAP**.
- 3 В открывшемся меню настроек сети выберите пункт **Сетевой интерфейс**.

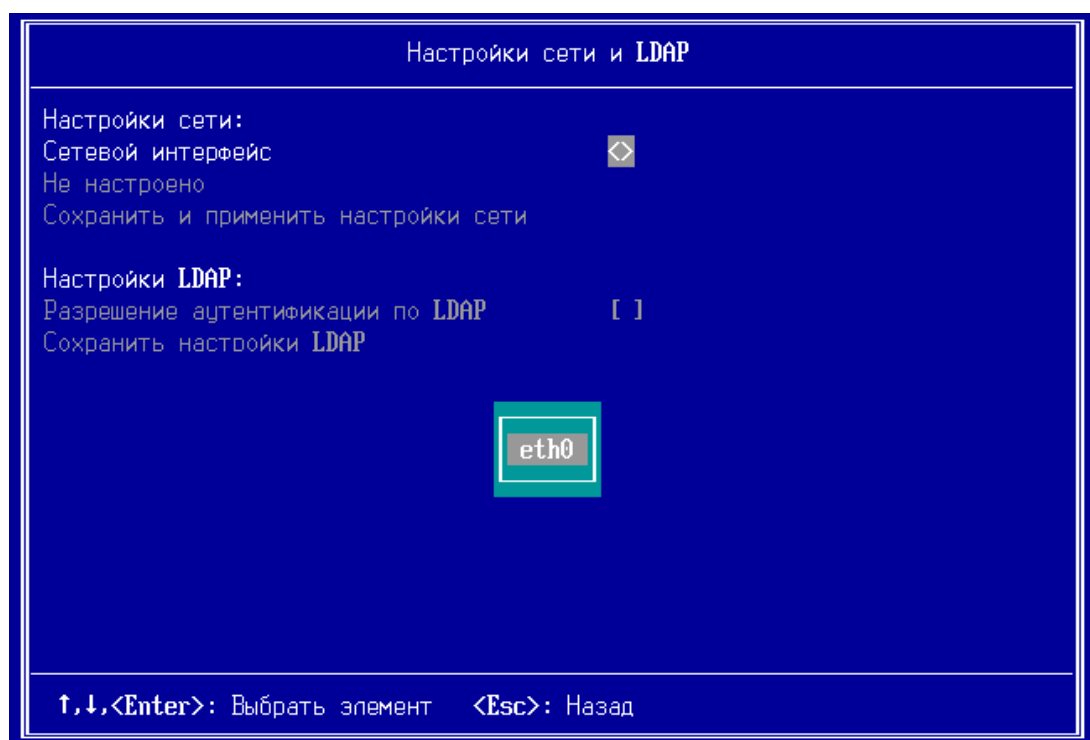


Рисунок 71. Выбор сетевого интерфейса

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

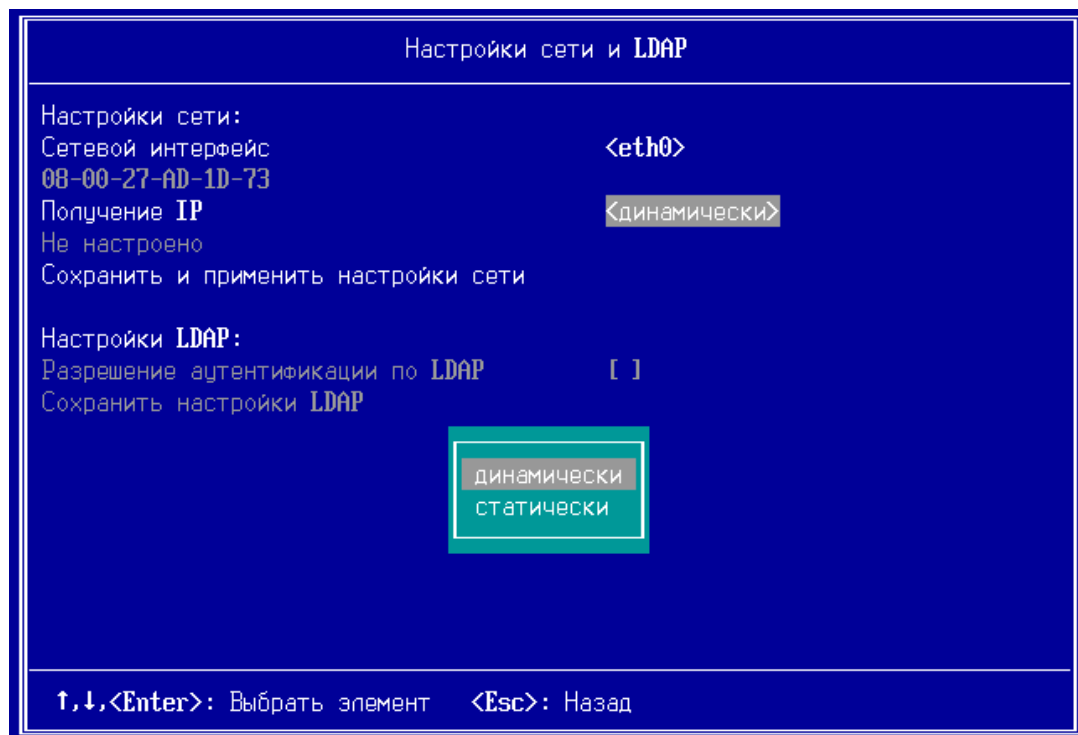


Рисунок 72. Выбор получения IP

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

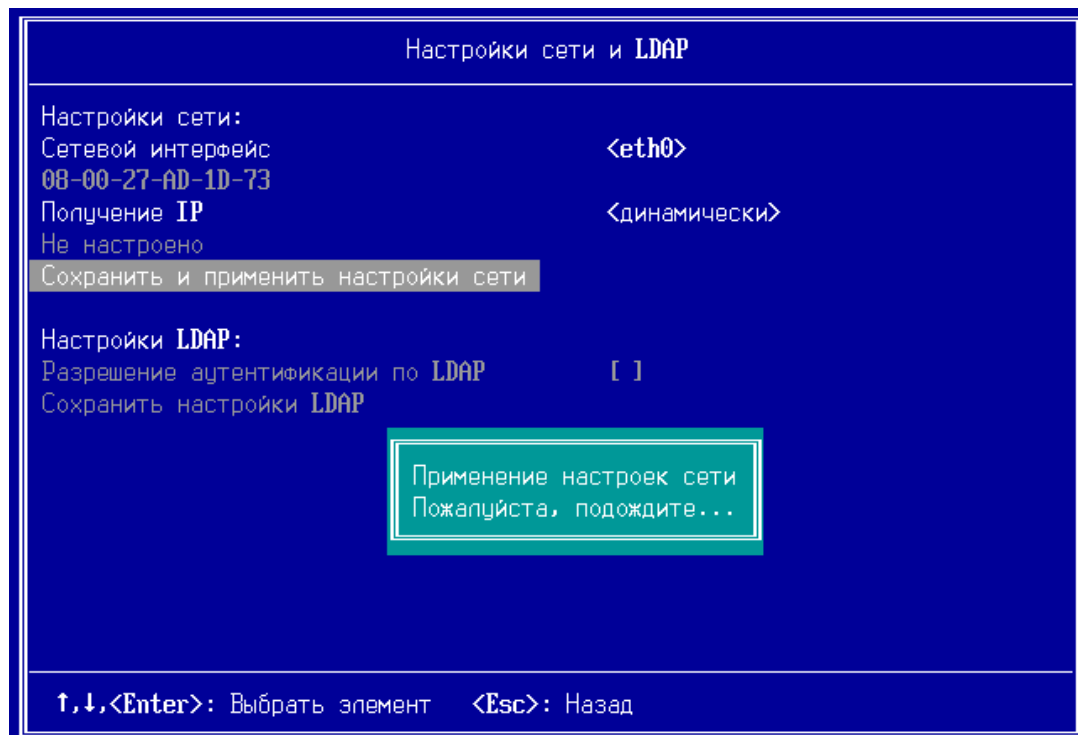


Рисунок 73. Применение заданных настроек сети

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

Сетевой кабель не подключен
Нажмите любую клавишу для продолжения

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

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

Настройки сети не применены
Нажмите любую клавишу для продолжения

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

- 6 Дождитесь появления сообщения о сохранении настроек сети и нажмите любую клавишу для продолжения.

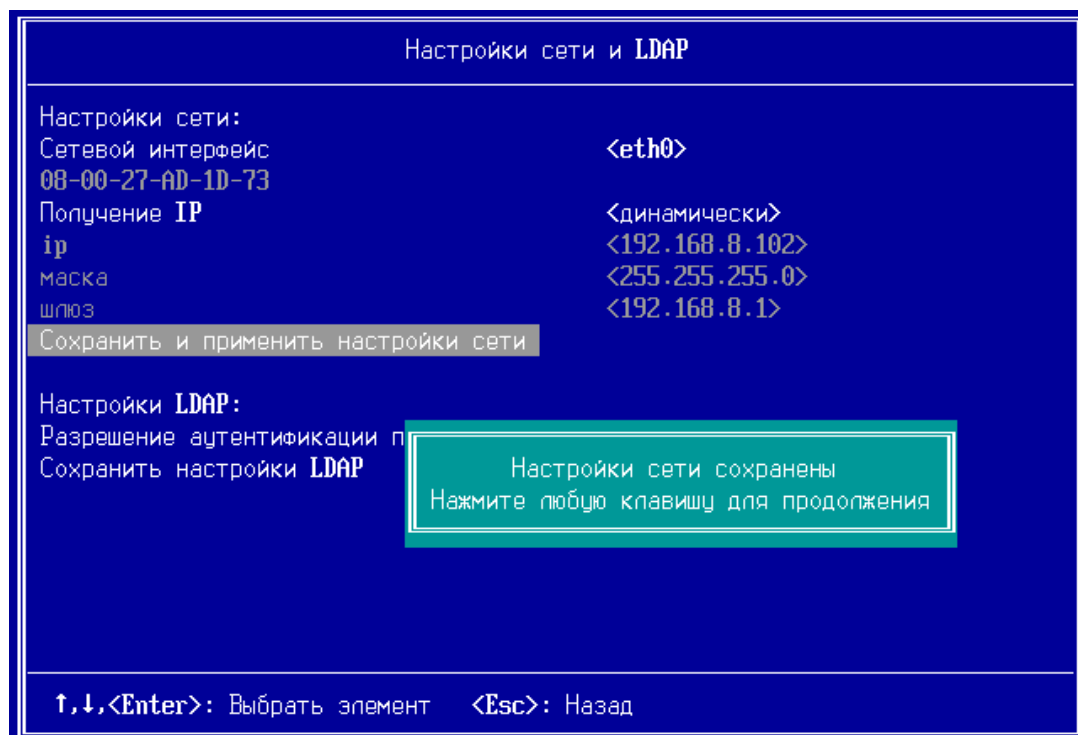


Рисунок 74. Успешное завершение сохранения настроек сети

Настройки подключения к LDAP серверу

Для настройки подключения к LDAP серверу выполните следующие действия:

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

Настройки сети и LDAP

Настройки сети:

Сетевой интерфейс **<eth0>**

08-00-27-AD-1D-73

Получение IP **<динамически>**

ip **<192.168.8.102>**

маска **<255.255.255.0>**

шлюз **<192.168.8.1>**

Сохранить и применить настройки сети

Настройки LDAP:

Разрешение аутентификации по LDAP **[x]**

IP сервера LDAP **<192.168.8.101>**

Имя сервера LDAP **<ldap>**

Проверить доступность сервера LDAP

Использование TLS в сессии LDAP **[]**

Настройки пользователей LDAP

Сохранить настройки LDAP

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

Рисунок 75. Установка настроек LDAP сервера

- 2 Задайте **Имя сервера LDAP**, которое впоследствии будет использоваться пользователем для аутентификации.
- 3 При необходимости проверки соединения с сервером LDAP, выберите **Проверить доступность сервера LDAP**. На экране появится следующее сообщение:

Проверка доступности сервера LDAP
Пожалуйста, подождите...

После успешной проверки соединения с сервером LDAP появится следующее сообщение:

Сетевое соединение с сервером LDAP проверено
Нажмите любую клавишу для продолжения

Если соединение установить не удалось, то появится следующее сообщение:

Сервер **LDAP** недоступен
Нажмите любую клавишу для продолжения

Нажмите любую клавишу. Проверьте настройки LDAP и повторите попытку проверки доступности сервера LDAP.

- 4 В настройках по умолчанию, установлен TLS для защиты соединения – флажок в поле **Использование TLS в сессии LDAP**. Для использования TLS предварительно необходимо установить корневой сертификат (см. «Установка корневого сертификата» на стр. 107).

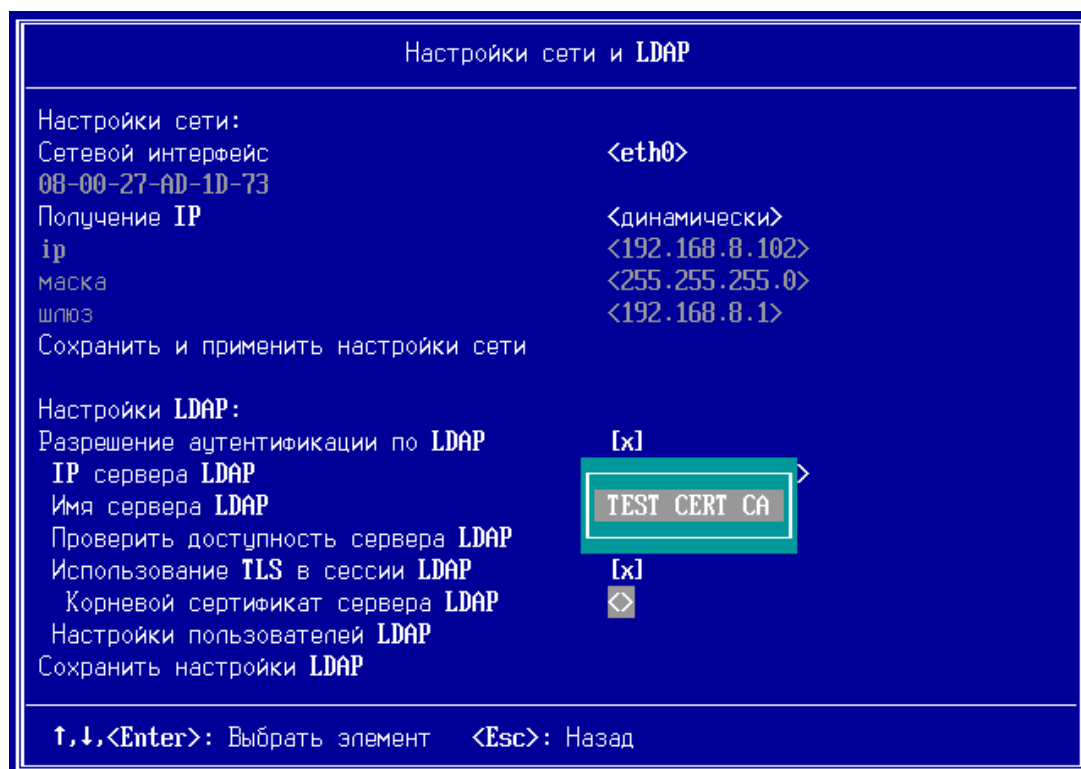


Рисунок 76. Выбор корневого сертификата при использовании TLS в сессии LDAP

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

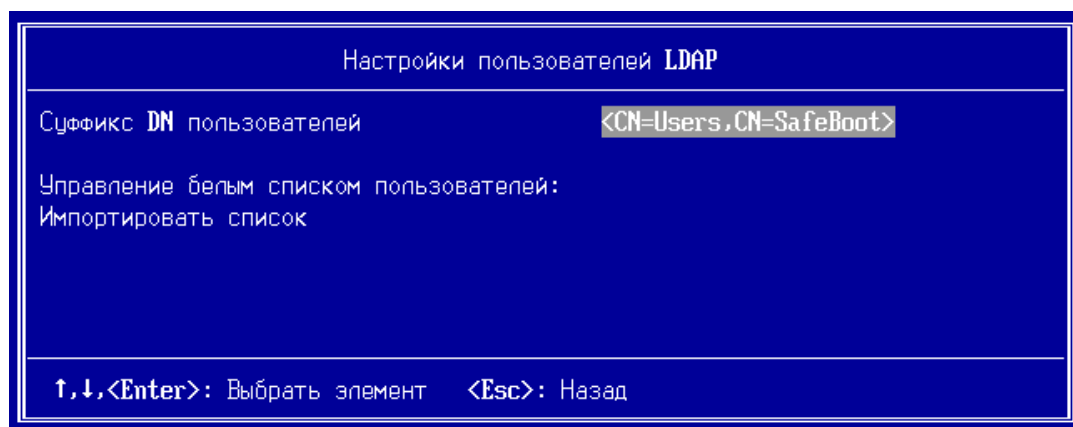


Рисунок 77. Настройка пользователей LDAP

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

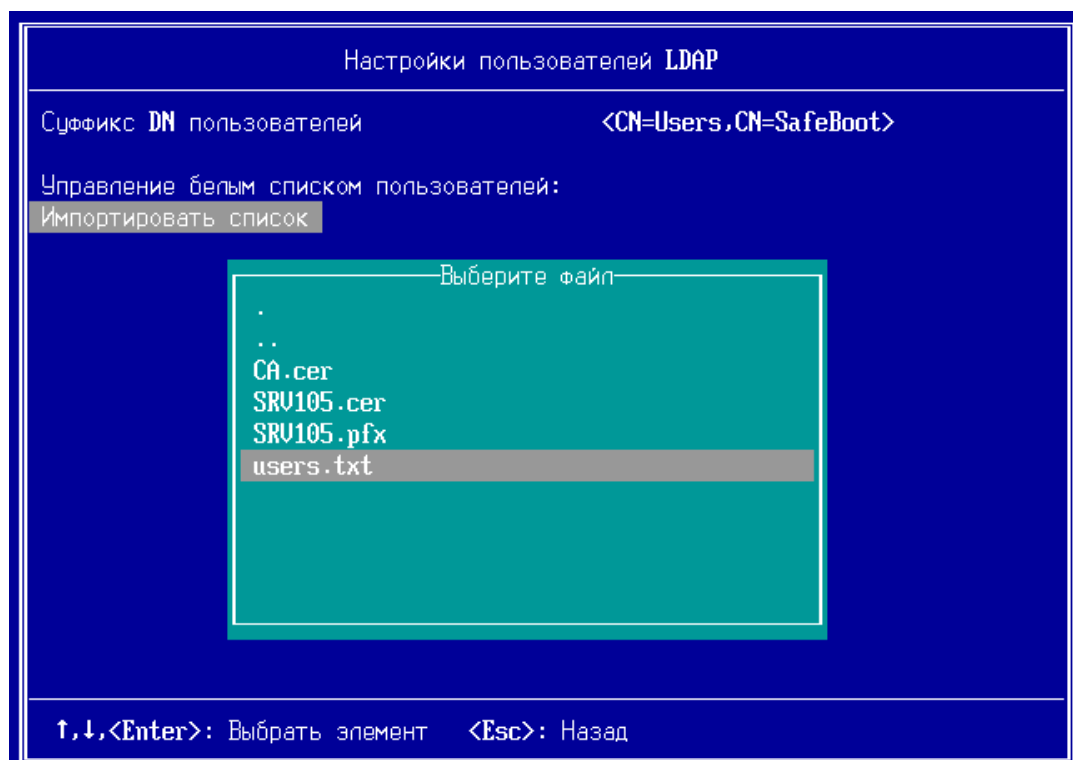


Рисунок 78. Выбор файла со списком разрешенных пользователей LDAP

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

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

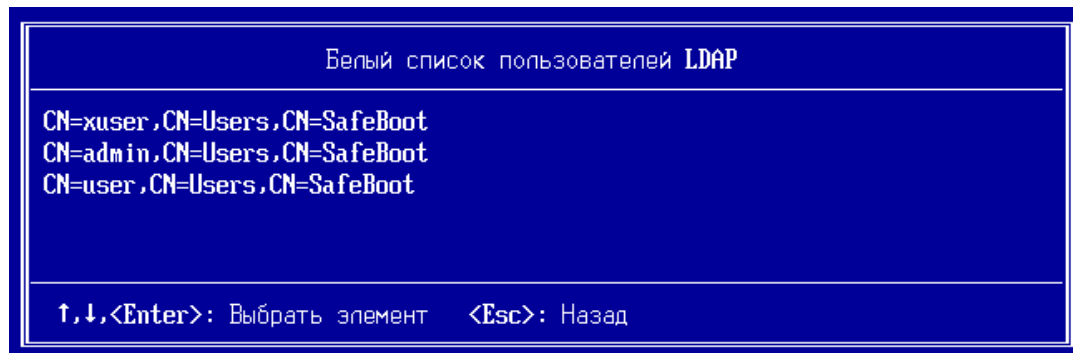


Рисунок 79. Просмотр списка пользователей LDAP

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

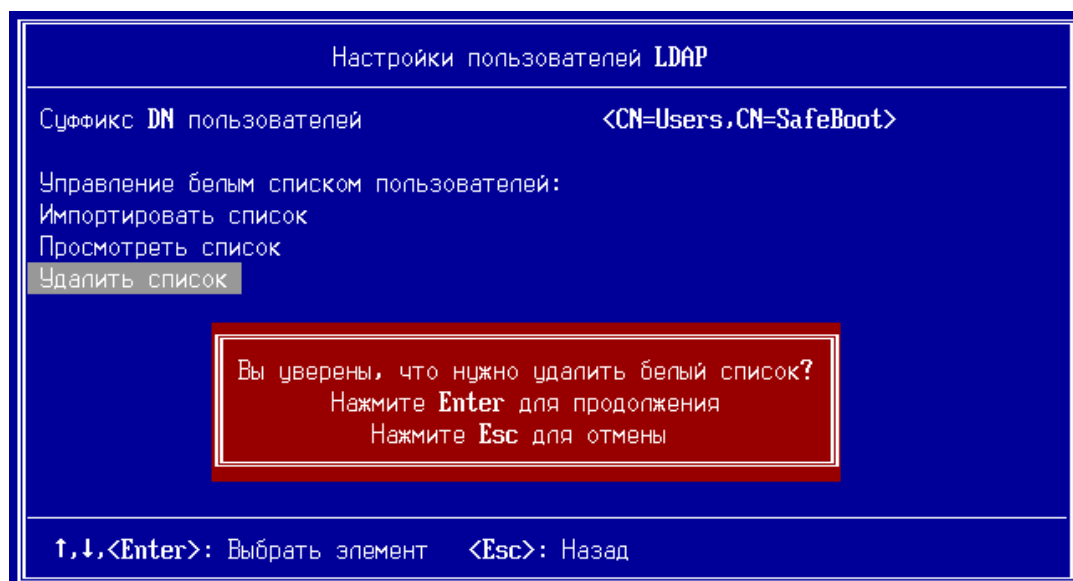
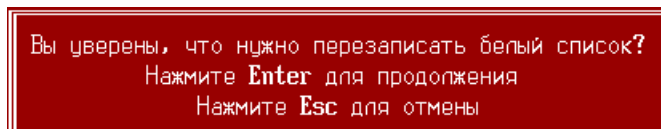


Рисунок 80. Удаление списка пользователей LDAP

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



В случае продолжения новый импортированный список заменит текущий.

- 7 Выйдите из меню настроек пользователей LDAP, нажав **Esc**.
- 8 Выберите **Сохранить настройки LDAP**.

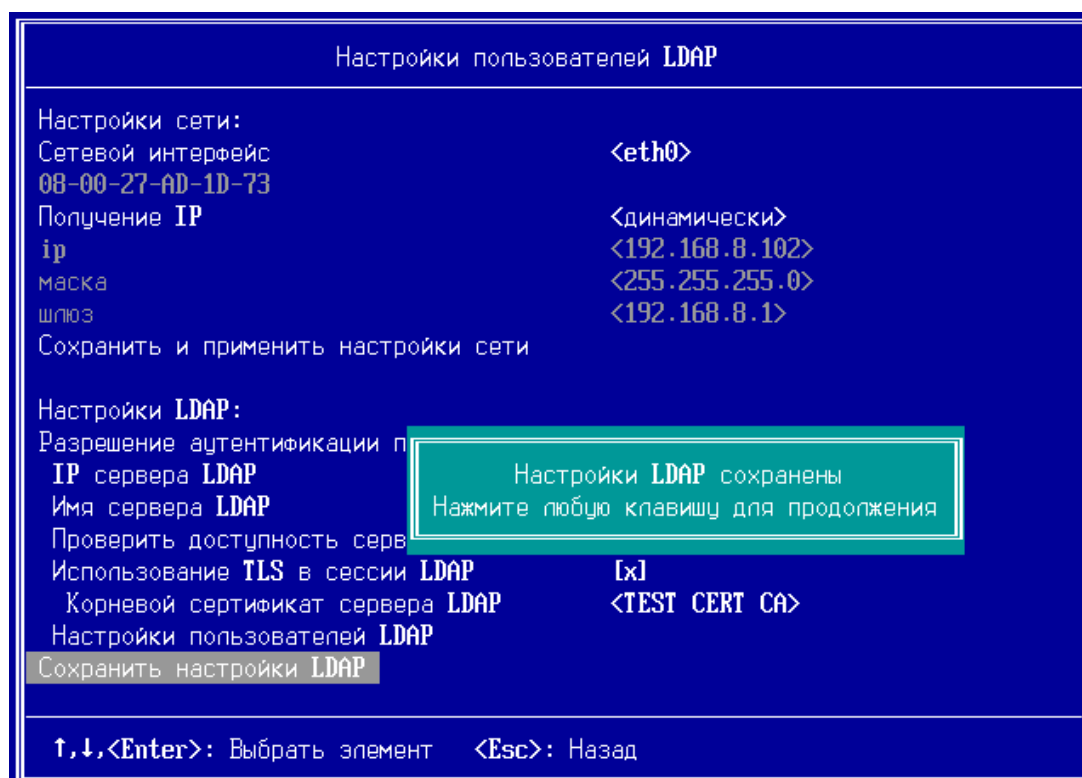


Рисунок 81. Сохранение настроек LDAP

- 9 Нажмите любую клавишу, затем нажмите **Esc** для выхода в основное меню режима настроек.

10

Управление журналом событий

Настройки журнала событий	124
Просмотр журнала событий	127
Экспорт записей журнала событий	128

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.

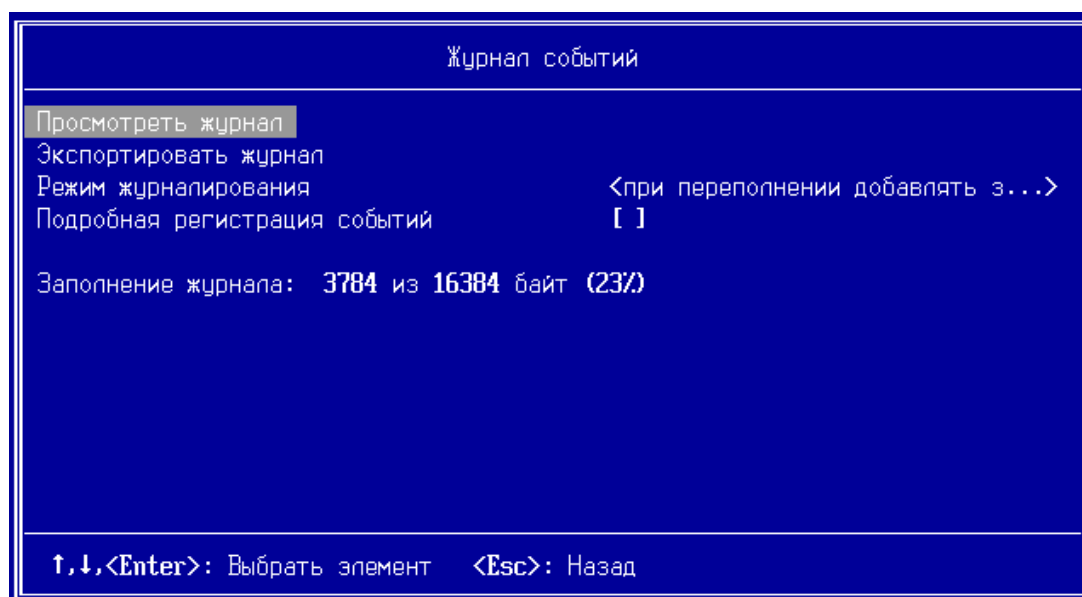


Рисунок 82. Меню управления настройками журнала событий

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, будет продолжен журнал, сохранившийся в NVRAM (в случае отказа от его экспорта).

Изменение настроек журнала событий

Чтобы изменить настройки журнала событий, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 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 режимах «**при переполнении добавлять записи циклически**» и «**при переполнении переносить журнал на диск**», то при просмотре отображаются записи, хранимые в NVRAM. В случае, если журнал ведется на диске, то отображаются записи журнала событий, хранимые на диске.

Чтобы просмотреть записи журнала событий, выполните следующие действия:

- 1 Войдите в режим настроек ViPNet SafeBoot (см. «Вход в режим настройки ViPNet SafeBoot» на стр. 34).
- 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. 34).
- 2 Подключите USB-носитель.
- 3 В меню режима настроек выберите **Журнал событий**.
- 4 В открывшемся окне выберите **Экспортировать журнал**.



Примечания.

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



События, регистрируемые в ViPNet SafeBoot

№ п/п	Тип события	Текст сообщения
1	информация	Старт ПМДЗ
2	информация	Система перезагружена
3	информация	Система выключена
4	ошибка	Вход в режим настроек BIOS заблокирован
5	ошибка	Неверное системное время
6	информация	Системное время изменено Администратором
7	ошибка	Критическая ошибка
8	детальный	Модуль верифицирован
9	детальный	Модуль выгружен
10	ошибка	Ошибка выгрузки модуля
11	детальный	Модуль загружен с диска
12	ошибка	Ошибка загрузки модуля с диска
13	ошибка	Ошибка формата модуля
14	ошибка	Неверная подпись модуля
15	информация	Модуль инициализирован
16	ошибка	Ошибка инициализации модуля

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

№ п/п	Тип события	Текст сообщения
43	ошибка	Неподдерживаемая версия БД конфигурации ПМДЗ
44	детальный	Переключение БД конфигурации ПМДЗ в расширенный режим
45	информация	БД конфигурации ПМДЗ экспортирована
46	ошибка	БД конфигурации ПМДЗ переполнена
47	ошибка	Нарушение журнала ПМДЗ
48	ошибка	Неподдерживаемая версия журнала ПМДЗ
49	информация	Журнал ПМДЗ заполнен и заблокирован
50	информация	Журнал ПМДЗ пересоздан
51	информация	Журнал ПМДЗ экспортирован
52	ошибка	Ошибка при экспорте журнала ПМДЗ
53	информация	Параметры загрузки должны быть настроены
54	информация	Режим загрузки изменен
55	информация	Изменено устройство загрузки (legacy)
56	информация	Раздел ESP изменен
57	информация	EFI-загрузчик изменен
58	информация	Параметры КЦ настроены автоматически
59	информация	Обновлен список разделов на КЦ
60	информация	Раздел поставлен на КЦ
61	информация	Раздел снят с КЦ
62	информация	Элемент поставлен на КЦ
63	информация	Элемент снят с КЦ
64	информация	Компонент поставлен на КЦ
65	информация	Компонент снят с КЦ
66	информация	Изменен диск для контроля загрузочных секторов
67	информация	Контроль журнала транзакций ФС включен
68	информация	Контроль журнала транзакций ФС выключен
69	информация	Режим обучения КЦ включен
70	информация	Режим обучения КЦ выключен
71	информация	Режим хранения эталонов КЦ изменен
72	информация	Эталон КЦ компонентов системы обновлен

№ п/п	Тип события	Текст сообщения
73	информация	Эталоны компонента импортированы
74	ошибка	Неверный формат подписи
75	ошибка	Неверная подпись
76	детальный	Целостность элемента заверена
77	ошибка	Целостность элемента нарушена
78	ошибка	Элемент не найден
79	информация	Элемент снят с КЦ (режим обучения)
80	информация	Незарегистрированный элемент
81	информация	Целостность компонента заверена
82	ошибка	Целостность компонента нарушена
83	ошибка	Эталоны компонента не найдены
84	ошибка	Ошибка при верификации подписи эталонов компонента
85	информация	Целостность компонентов системы заверена
86	детальный	Журнал транзакций ФС пуст
87	ошибка	Журнал транзакций ФС не пуст
88	информация	Добавлен пользователь
89	информация	Пользователь удален
90	информация	Изменен тип аутентификации пользователя
91	информация	Пароль пользователя изменен
92	информация	Настройки пароля пользователя изменены
93	информация	Пароль пользователя изменен Администратором
94	информация	Эл.идентификатор пользователя инициализирован
95	информация	Изменен PIN эл.идентификатора пользователя
96	информация	Изменен эл.идентификатор пользователя
97	информация	Изменен сертификат пользователя
98	информация	Изменен режим журналирования
99	информация	Изменен уровень журналирования
100	информация	Установлен корневой сертификат
101	информация	Корневой сертификат удален
102	информация	CRL установлен/обновлен

№ п/п	Тип события	Текст сообщения
103	информация	CRL удален
104	информация	Вход в режим настроек BIOS разрешен
105	информация	Вход в режим настроек BIOS запрещен
106	информация	Защита SPI flash включена
107	информация	Защита SPI flash выключена
108	информация	Защита S3 bootscript включена
109	информация	Защита S3 bootscript выключена
110	информация	БД конфигурации ПМДЗ пересоздана
111	ошибка	Ошибка при экспорте БД конфигурации ПМДЗ
112	информация	БД конфигурации ПМДЗ импортирована
113	ошибка	Ошибка при импорте БД конфигурации ПМДЗ
114	информация	Ограничение сессии аутентификации включено
115	информация	Ограничение сессии аутентификации выключено
116	информация	Время сессии аутентификации изменено
117	информация	Автоматический вход в систему разрешен
118	информация	Автоматический вход в систему запрещен
119	информация	Время до автоматического входа в систему изменено
120	ошибка	Ошибка выставления защиты SPI flash
121	информация	Информация о защите SPI flash
122	информация	Информация об устройствах загрузки (legacy)
123	ошибка	Ошибка при работе с устройствами загрузки (legacy)
124	информация	EFI-загрузчик возвратил управление ПМДЗ
125	ошибка	Найдено несколько разделов ESP
126	информация	
127	ошибка	Ошибка верификации пакета обновления
128	ошибка	Неверная версия пакета обновления
129	детальный	Пакет обновления не соответствует текущей платформе
130	информация	Установка обновления...
131	ошибка	Пакет обновления установлен
132	ошибка	Ошибка при установке пакета обновления

№ п/п	Тип события	Текст сообщения
133	информация	Настройки сети изменились
134	информация	Настройки LDAP изменились
135	информация	Протокол конфигурирования сети:
136	информация	Статистика ping:
137	информация	Включение сетевого стека не поддерживается
138	информация	Сервер LDAP недоступен при аутентификации пользователя
139	информация	Белый список пользователей LDAP импортирован
140	информация	Белый список пользователей LDAP удален
141	ошибка	Ошибка данных пароля на эл.идентификаторе
142	ошибка	Пароль на эл.идентификаторе не найден
143	ошибка	Неверный пароль на эл.идентификаторе
144	ошибка	Неподдерживаемый формат пароля на эл.идентификаторе
145	ошибка	Неизвестное событие



В

Возможные неполадки и способы их устранения

Система заблокирована	136
Пользователь заблокирован	137

Система заблокирована

Блокированию системы может привести одна из следующих причин:

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

Нарушена целостность операционной системы или объектов, поставленных на контроль

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

Решение: Необходимо устранить нарушения в поставленных на контроль объектах.

В случае, если изменения были правомерны, следует снять и вновь поставить компоненты на контроль (см. Контроль целостности на стр. 54).

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. 54).

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. 123).

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. 72).

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. 72).



Глоссарий

Администратор

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

Аудитор

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

Аутентификация

Процедура проверки подлинности предоставленных пользователем данных при идентификации.

Идентификация

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

Ключ проверки электронной подписи

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

Отличительное имя (DN)

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

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Спецсимвол

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

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

Электронный идентификатор

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

LDAP

англ. Lightweight Directory Access Protocol – облегченный протокол доступа к каталогам. Протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP.