



ViPNet SafeBoot 3

Руководство администратора

Версия продукта 3.2.1

© АО «ИнфоТеКС», 2025

ФРКЕ.00283-01 32 01

Версия продукта 3.2.1, документ обновлен 31.03.2026

Этот документ входит в комплект поставки продукта ViPNet, 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 АО «ИнфоТеКС».

ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	7
О документе.....	8
Соглашения документа.....	8
Обратная связь.....	9
О программе	10
Что нового в версии 3.2.1	11
Совместимые продукты ViPNet.....	12
Совместимые электронные идентификаторы	13
Функциональные ограничения	15
Комплект поставки	18
 Глава 1. Первый запуск.....	20
Порядок действий.....	21
Включение ViPNet SafeBoot	22
Включение с помощью программы установки ViPNet SafeBoot	22
Включение на этапе инициализации BIOS.....	22
Инициализация датчика случайных чисел.....	24
Подготовка файла itsbeg.bin со случайной последовательностью	24
Интерфейс	26
Вход в настройки ViPNet SafeBoot.....	28
Первый вход	29
Создание диска восстановления	31
Регистрация.....	32
Порядок базовой настройки	34
 Глава 2. Настройка параметров загрузки ОС	36
Профиль загрузки по умолчанию	37
Настройка профилей загрузки ОС.....	38
 Глава 3. Управление учетными записями пользователей.....	40
Учётные записи пользователей	41
Режим SSO	42
Полномочия пользователей.....	43
Восстановление пароля администратора.....	44
Добавление учетной записи.....	45

Настройка политики паролей	45
Настройка графика доступа.....	45
Добавление пользователя с аутентификацией по паролю	45
Добавление пользователя с аутентификацией по электронному идентификатору ..	47
Добавление пользователя с аутентификацией по электронному идентификатору и паролю	49
Добавление пользователя с аутентификацией по коду на электронном идентификаторе	51
Добавление пользователя с LDAP-аутентификацией	53
Параметры аутентификации	53
Изменение, блокирование и удаление учётной записи пользователя	55
Глава 4. Аутентификация с помощью электронного идентификатора.....	57
Порядок подготовки электронного идентификатора	58
JaCarta.....	58
Рутoken ЭЦП, Рутoken ЭЦП 2.0, Рутoken ЭЦП 3.0, Рутoken Lite.....	59
Guardant ID.....	59
ФОРОС.....	60
ESMART Token.....	60
Порядок обновления информации на электронном идентификаторе	61
Установка корневого сертификата и списка отозванных сертификатов	62
Экспорт корневого сертификата и списка отозванных сертификатов.....	63
Удаление корневого сертификата	64
Глава 5. Настройки сети и LDAP	65
Настройка сети	66
Настройки подключения к LDAP-серверу	67
Настройка режима SSO для аутентификации доменного пользователя	69
Глава 6. Контроль целостности	70
Контроль компонентов ОС	71
Сертификаты контроля целостности	71
Автоопределение компонентов ОС	73
Контроль параметров реестра Windows	73
Контроль файлов	75
Контроль файлов сетевой загрузки.....	76
Контроль аппаратных компонентов.....	77
Контроль зашифрованных дисков LUKS.....	80
Режим обучения.....	81

Отключение контроля целостности	83
Принудительная проверка целостности	84
Повторный расчёт контрольных сумм	85
Глава 7. Настройки ViPNet SafeBoot	86
Защита	87
Блокировка устройств	89
Удалённое управление.....	90
Изменение даты и времени.....	91
Глава 8. База данных конфигурации	92
Ведение базы данных конфигурации.....	93
Бездисковый режим работы.....	93
Экспорт настроек	95
Формат настроек при импорте и экспорте	95
Режимы экспорта.....	96
Особенности импорта и экспорта эталонов контроля целостности.....	97
Импорт настроек.....	99
Сброс настроек	100
Глава 9. Управление журналом событий	101
Настройки журнала событий	102
Режим ведения журнала внутренний, циклический	102
Режим ведения журнала внутренний, экспортируемый	103
Режим ведения журнала внешний (на диске).....	103
Отправка событий журнала по протоколу syslog	103
Просмотр журнала событий.....	105
Фильтрация журнала событий	105
Экспорт записей журнала событий	107
Глава 10. Обновление	108
Порядок обновления ViPNet SafeBoot	109
Глава 11. Переустановка ОС при активных механизмах защиты ViPNet SafeBoot	111
Переустановка ОС	112
Ошибка восстановления рабочей директории	113
Глава 12. Дополнительные возможности ViPNet SafeBoot	114
Временное отключение функциональности ViPNet SafeBoot	115
Автоматическое восстановление рабочей директории.....	116

Автоматическое восстановление системного времени	117
Глава 13. Возможные неполадки	118
Система заблокирована.....	119
Нарушена целостность операционной системы или объектов, поставленных на контроль.....	119
Нарушена целостность состава аппаратных средств, поставленных на контроль...	119
Журнал событий переполнен.....	120
Журнал событий поврежден	120
Пользователь заблокирован	121
Превышено допустимое количество неудачных попыток аутентификации.....	121
Время действия пароля пользователя истекло	121
Сертификат пользователя просрочен или отозван	122
Не загружается BIOS	123
Приложение А. События, регистрируемые в ViPNet SafeBoot	124
Приложение В. Режимы контроля целостности компонентов ОС	136
Приложение С. История версий	141
Что нового в версии 3.2.0.....	141
Что нового в версии 3.0.3.....	144
Что нового в версии 3.0.1.....	144
Приложение D. Термины и сокращения	146
Приложение Е. Изменения в документации	149



Введение

О документе	8
Обратная связь	9
О программе	10
Что нового в версии 3.2.1	11
Совместимые продукты ViPNet	12
Совместимые электронные идентификаторы	13
Функциональные ограничения	15
Комплект поставки	18

О документе

Документ предназначен для администраторов, которые настраивают ViPNet SafeBoot на рабочих местах пользователей. Предполагается, что у читателя есть опыт администрирования операционных систем.

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется [политикой ответственного разглашения](#).

О программе

ViPNet SafeBoot — программный модуль доверенной загрузки, который устанавливается в BIOS. Он защищает компьютер от угроз несанкционированного доступа на этапе загрузки и от атак на BIOS (загрузка вредоносного кода в BIOS, перехват данных и отключение базовых защитных механизмов).

ViPNet SafeBoot позволяет контролировать целостность BIOS, защищаемых компонентов операционной системы, а также блокировать загрузку модифицированной копии операционной системы.

ViPNet SafeBoot версии 3.2.1 представлен только в исполнении 2.

Что нового в версии 3.2.1

- **Изменен порядок повторной инициализации ПДСЧ**

Теперь вы можете повторно инициализировать ПДСЧ в разделе **Ключи**. Теперь ViPNet SafeBoot после трех лет с момента последней инициализации ПДСЧ не блокируется. Подробнее см. в [Инициализация датчика случайных чисел](#).

- **Поддержка новых электронных идентификаторов и считывателей смарт-карт**

Теперь для аутентификации пользователей вы можете использовать электронные идентификаторы и смарт-карты ФОПОС и ESMART Token ГОСТ. Добавлена поддержка считывателей смарт-карт серии ESMART Reader ER773x. Подробнее см. в [Совместимые электронные идентификаторы](#).

- **Поддержка новых ARM-платформ**

Добавлена поддержка ARM-платформ архитектуры aarch64 с процессорами:

- Broadcom 2711;
- Broadcom 2837;
- RockChip 3566;
- RockChip 3568.

- **Оптимизирована работа контроля целостности**

- **Обновлен список совместимого ПО**

Подробнее см. в [Совместимые продукты ViPNet](#).

- **Изменены системные требования для установки ViPNet SafeBoot**

Подробнее см. в разделе «Системные требования» в документе «ViPNet SafeBoot 3. Руководство по установке».

Совместимые продукты ViPNet

- ViPNet CSP версий 4.4.2, 4.4.4 и 4.4.8;
- ViPNet OSSL версии 5.6;
- ViPNet SafePoint версий 1.5.0 и 1.6.0;
- ViPNet EndPoint Protection версии 1.6.0, 1.7.1.

Совместимые электронные идентификаторы

Электронные идентификаторы в формате USB-токенов:

- Рутокен ЭЦП;
- Рутокен ЭЦП 2.0 2000, 2100, 4000;
- Рутокен Lite 1000;
- Рутокен ЭЦП PKI 1800;
- Рутокен S 1100;
- Рутокен ЭЦП 3.0 3100, 3120;
- JaCarta LT;
- JaCarta PKI;
- JaCarta-2 ГОСТ;
- JaCarta PKI/ГОСТ;
- JaCarta-2 PKI/ГОСТ;
- JaCarta-2 SE;
- JaCarta PRO;
- Guardant ID;
- Guardant ID версии 2;
- ФОРОС ST23L80;
- ФОРОС ST23R160;
- ФОРОС ST31H320;
- ESMART Token ГОСТ с разметкой 2.2.

Смарт-карты:

- JaCarta PKI;
- JaCarta-2 ГОСТ;
- Рутокен ЭЦП 2.0 2100;
- Рутокен ЭЦП 3.0 3100;
- ФОРОС ST23L80;
- ФОРОС ST23R160;
- ФОРОС ST31H320;

- ESMART Token ГОСТ с разметкой 2.2.

Считыватели смарт-карт:

- ACS ACR38;
- ASEDive IIIe;
- JCR721;
- HID Omnikey 5422;
- ESMART Reader ER773x series.



Совет. Не используйте USB-хабы для подключения считывателей смарт-карт. Для корректной работы смарт-карт рекомендуется подключать их напрямую к устройству.

При использовании комбинированных электронных идентификаторов JaCarta PKI/ГОСТ используется только режим PKI.

При использовании комбинированных электронных идентификаторов JaCarta-2 PKI/ГОСТ используется только режим ГОСТ.

Электронные идентификаторы JaCarta ГОСТ и ESMART Token ГОСТ с разметкой 1.2 не поддерживаются.

Совместимость смарт-карт и считывателей смарт-карт

- Смарт-карта ФОПОС ST23R160 не работает со считывателями Alladin JCR721, HID Global OmniKey 5422 Smartcard Reader 0, подтверждена совместимость только со считывателем ESMART Reader ER7735.
- Смарт-карта ФОПОС ST31H320 не работает со считывателем HID Global OmniKey 5422 Smartcard Reader 0, подтверждена совместимость только со считывателями Alladin JCR721 и ESMART Reader ER7735.
- Для смарт-карты ФОПОС ST23L80 подтверждена совместимость только со считывателями ESMART Reader ER7735 и ASEDive IIIe.
- Смарт-карта ESMARTToken GOST не работает со считывателем Alladin JCR721, подтверждена совместимость только со считывателями HID Global OmniKey 5422 Smartcard Reader 0 и ESMART Reader ER7735.

Функциональные ограничения

В ViPNet SafeBoot функция защиты микросхемы BIOS от перезаписи и чтения поддерживается только для перечисленных ниже процессоров.



Внимание! Чтобы обеспечить защиту BIOS, необходимо убедиться, что регистр HSFS разблокирован — бит FLOCKDN регистра должен быть установлен в 0. Чтобы изменить значение бита, обратитесь к производителю материнской платы.

Таблица 1. Процессоры, для которых ViPNet SafeBoot поддерживает защиту микросхемы BIOS от перезаписи и чтения

Семейство процессоров	Модификация
Intel Alder Lake	Alder Lake N/S
Intel Apollo Lake	Apollo Lake E/N/J
Intel Bay Trail	Bay Trail I/M/D
Intel Braswell	Braswell N/J
Intel Broadwell	Broadwell ULT, Broadwell H, Broadwell EP/EX, Broadwell DE
Intel Cannon Lake	Cannon Lake U/Y, Cannon Lake DT/HALO
Intel Coffee Lake	Coffee Lake H/S, Coffee Lake U
Intel Gemini Lake	Gemini Lake N/J
Intel Haswell	Haswell, Crystal Well, Haswell ULT, Haswell EP/EX
Intel Ice Lake	Ice Lake U/Y
Intel Ivy Bridge	Ivy Bridge M/H/Gladden (Client), Ivy Bridge E/EN/EP/EX (Server)
Intel Jasper Lake	Jasper Lake P/C
Intel Kaby Lake	Kaby Lake U/Y, Kaby Lake DT/HALO
Intel Purley	Purley
Intel Rangeley	Atom C2000
Intel Raptor Lake	Raptor Lake H/S
Intel Rocket Lake	Rocket Lake H/S
Intel Sandy Bridge	Sandy Bridge M/H (Client), Sandy Bridge E/EN/EP (Server)
Intel Sky Lake	Sky Lake SP, Sky Lake ULT/ULX, Sky Lake DT/HALO
Intel Tiger Lake	Tiger Lake H35

Семейство процессоров	Модификация
Intel Whiskey Lake	Whiskey Lake U/Y
AMD Bobcat	Desna/Ontario/Zacate
AMD Bulldozer	Zambezi
AMD Excavator	Carrizo/Bristol Ridge/Stoney Ridge
AMD Jaguar	Kabini/Temsh
AMD Piledriver	Vishera
AMD Puma	Beema/Mullins
AMD Steamroller	Kaveri
AMD Zen	Naples/Whitehaven/Summit Ridge/Raven Ridge/Dali/Snowy Owl/Great Horned Owl/Banded Kestrel/Dhyana
AMD Zen+	Colfax/Pinnacle Ridge/Picasso
AMD Zen2	Rome/Castle Peak/Matisse/Renoir/Xbox Series X/Grey Hawk/Lucienne/Van Gogh
AMD Zen3	Cezanne/Milan/Vermeer
ARM Cortex A57	Baikal-M

В зависимости от ОС и [режима загрузки ОС](#) может быть недоступна функциональность ViPNet SafeBoot:

- автоопределение контроля целостности;
- загрузка Legacy ОС.

В виду отсутствия некоторых технических возможностей ARM систем, в ViPNet SafeBoot:

- может не иметь эффекта или будет недоступна функциональность:
 - контроль программных SMI;
 - защита после S3;
 - контроль таблиц ACPI;
 - блокировка ACPI WPBT;
 - контроль CMOS;
- возможны ограничения:
 - недоступность защиты дисков от записи;
 - замедленный отклик ViPNet SafeBoot;
 - события ранней стадии загрузки и события после [Exit Boot Services](#) могут отсутствовать в журнале событий из-за архитектурных особенностей организации NVRAM платформы.

Для платформ модели Orange Pi рекомендуется во время настройки ViPNet SafeBoot подключать только один USB-носитель. Одновременное использование нескольких USB-носителей может привести к неправильной работе ViPNet SafeBoot из-за идентичного именования носителей.

Комплект поставки

CD-диск с архивами:

- с программой установки:
 - `vipnet_safeboot-m-e-x64-r-<номер версии>.zip` (папка `Исполнение 2\SOFT\x64`) — для платформы x64, исполнение 2;
 - `vipnet_safeboot-m-e-aarch64-r-<номер версии>.zip` (папка `Исполнение 2\SOFT\aarch64`) — для платформы aarch64, исполнение 2.
- `vipnet_safeboot-win_tools-x64-r-bin-<номер версии>.zip` с утилитами для Windows, платформы x64:
 - `prng_ext_gamma_init.exe` — для подготовки инициализирующей последовательности для программного датчика случайных чисел;
 - `recovery_disk_init.exe` — для подготовки ключа восстановления;
 - `registration` — папка с утилитами и скриптами для регистрации ViPNet SafeBoot.
- `vipnet_safeboot-win_tools-x86-r-bin-<номер версии>.zip` с утилитами для Windows, платформы x86:
 - `prng_ext_gamma_init.exe` — для подготовки инициализирующей последовательности для программного датчика случайных чисел;
 - `recovery_disk_init.exe` — для подготовки ключа восстановления;
 - `registration` — папка с утилитами и скриптами для регистрации ViPNet SafeBoot.
- `vipnet_safeboot-lin_tools-x64-r-bin-<номер версии>.zip` с утилитами для Linux, платформы x64:
 - `registration` — папка с утилитами и скриптами для регистрации ViPNet SafeBoot.
- `vipnet_safeboot-lin_tools-aarch64-r-bin-<номер версии>.zip` с утилитами для Linux, платформы aarch64:
 - `registration` — папка с утилитами и скриптами для регистрации ViPNet SafeBoot.
- Документы в формате PDF:
 - Руководство по установке.
 - Руководство администратора.
 - Руководство пользователя.
 - Формуляр.
 - Сертификат соответствия.
 - Сторонние лицензии.



Примечание. ПО, поддерживающее режим единого входа Single Sign-On, для установки в ОС не включено в комплект поставки.

1

Первый запуск

Порядок действий	21
Включение ViPNet SafeBoot	22
Инициализация датчика случайных чисел	24
Интерфейс	26
Вход в настройки ViPNet SafeBoot	28
Первый вход	29
Создание диска восстановления	31
Регистрация	32
Порядок базовой настройки	34

Порядок действий

ViPNet SafeBoot запускается первый раз в режиме, заданном администратором перед установкой:

- Режим неактивности — позволяет начать использовать ViPNet SafeBoot не сразу, а через некоторое время. Из этого режима можно перевести программу в Деморежим 2.
- Деморежим 1 — позволяет зарегистрировать ViPNet SafeBoot, без регистрации можно использовать 60 дней, после этого переходит в режим неактивности. По умолчанию в деморежиме 1 выполняется установка ViPNet SafeBoot.
- Деморежим 2 — позволяет зарегистрировать ViPNet SafeBoot, без регистрации можно использовать 60 дней, после этого будут доступны только регистрация и настройка загрузки ОС.

Чтобы посмотреть в каком режиме работает ViPNet SafeBoot в меню продукта перейдите в раздел **О продукте**.

При первом запуске:

- 1 Первый запуск ViPNet SafeBoot проводите с подключенным установочным диском и с файлом восстановления, если он был создан на этапе установки.
- 2 [Выполните инициализацию ПДСЧ](#).
- 3 [Создайте диск восстановления пароля администратора](#), если не создали его при установке ViPNet SafeBoot.
- 4 [Измените пароль администратора](#).
- 5 [Зарегистрируйте ViPNet SafeBoot](#).
- 6 [Настройте параметры загрузки ОС](#).

Если вы впервые работаете с ViPNet SafeBoot и хотите обеспечить базовый уровень защиты компьютеров пользователей, выполните действия из Порядка базовой настройки.

Включение ViPNet SafeBoot

Если ViPNet SafeBoot находится в режиме неактивности, возможны два варианта его включения: с помощью программы установки или на этапе инициализации BIOS.

Включение с помощью программы установки ViPNet SafeBoot

- 1 Подключите установочный USB-носитель.
- 2 Включите компьютер и зайдите в настройки BIOS.
- 3 В настройках BIOS задайте загрузку с USB-носителя и сохраните настройки.
После перезагрузки с установочного USB-носителя запустится EFI Shell.
- 4 На запрос **Press ESC in 5 seconds to skip startup.nsh, any other key to continue** нажмите любую клавишу, кроме **ESC**, или через 5 секунд программа установки запустится автоматически.
- 5 Выберите **Enable**.
- 6 Появится сообщение об успешном включении ViPNet SafeBoot. Для перезагрузки компьютера нажмите любую клавишу, кроме **q**.
После перезагрузки ViPNet SafeBoot готов к работе.



Примечание. Если появится сообщение `Unknown current install profile`, значит ViPNet SafeBoot не установлен.

Включение на этапе инициализации BIOS

- 1 Подключите установочный USB-носитель с файлом восстановления в корневой папке.
- 2 Включите компьютер и нажмите клавиши **правый Ctrl+E**.
 - Чтобы подтвердить запрос на включение, нажмите **Enter**. ViPNet SafeBoot включится.



Примечание. После подтверждения запроса может запуститься программа установки ViPNet SafeBoot, которая автоматически включит ViPNet SafeBoot. Дополнительные действия не требуются.

- Чтобы отклонить запрос на включение, нажмите **Esc**. Компьютер перезагрузится, ViPNet SafeBoot останется выключенным.

В результате ViPNet SafeBoot перейдет в деморежим 2:

- если ViPNet SafeBoot перешел в режим неактивности из деморежима 1, то в деморежиме 2 функциональность будет ограничена (доступны регистрация и настройка загрузки ОС);
- если ViPNet SafeBoot был установлен в режиме неактивности, то в деморежиме 2 будет доступна полная функциональность в течение 60 дней.

Инициализация датчика случайных чисел

При первом запуске ViPNet SafeBoot инициализируйте [программный датчик случайных чисел \(ПДСЧ\)](#):

- С помощью клавиатуры (БиоДСЧ), диск восстановления не требуется.
- С помощью заранее подготовленной случайной последовательности, потребуется диск восстановления.

Повторная инициализация ПДСЧ не требуется, но рекомендуется. Чтобы инициализировать ПДСЧ, перейдите в раздел **Ключи** и нажмите **Инициализировать ПДСЧ**.

Чтобы инициализировать датчик с помощью:

- БиоДСЧ. Нажимайте случайные клавиши, пока не появится уведомление о завершении инициализации. Нажмите **ОК**.
- Заранее подготовленной последовательности:



Примечание. Подготовленная случайная последовательность упрощает и ускоряет процесс инициализации, так как её можно использовать при инициализации датчика случайных чисел на нескольких компьютерах последовательно. Последовательность содержится в файле `itsbeg.bin`. Его можно использовать столько раз, сколько блоков содержит последовательность.

- Создайте файл `itsbeg.bin` и скопируйте его на установочный USB-носитель.
- В корневой папке установочного USB-носителя поместите файл `itrecovery.bin` с диска восстановления.

Подготовка файла `itsbeg.bin` со случайной последовательностью

Подготовка файла `itsbeg.bin` выполняется на технологическом компьютере с Windows 8.1 или выше и криптопровайдером [ViPNet CSP](#) версий 4.4.2, 4.4.4 и 4.4.8 или [ViPNet OSSL](#) версии 5.6.

Файл со случайной последовательностью формируется утилитой `prng_ext_gamma_init.exe` из комплекта поставки. Формат запуска утилиты:

```
prng_ext_gamma_init <ext_gamma_path> <blocks_amount> [-m (pkcs11 | capi) [-f] | -v | -h],  
где:
```

- `ext_gamma_path` — путь и имя файла (обязательно `itsbeg.bin`) со случайной последовательностью;
- `blocks_amount` — количество блоков случайной последовательности (от 1 до 100);
- `-m (pkcs11 | capi)` — используемый криптоинтерфейс:
 - `capi` — по умолчанию и для ViPNet CSP 4.4.2, 4.4.4 и 4.4.8;
 - `pkcs11` — для ViPNet OSSSL.
- `-f` — перезаписать файл с последовательностью случайных чисел.

Например, для создания случайной последовательности в файл `itsbeg.bin` размером в 100 блоков введите команду:

```
prng_ext_gamma_init.exe itsbeg.bin 100 -m capi -f.
```

Чтобы получить информацию об утилите, запустите `prng_ext_gamma_init.exe` с ключами:

- `-v` — показать версию утилиты;
- `-h` — показать страницу помощи.

Интерфейс

Вы можете выбрать графический или псевдографический интерфейс. Для переключения интерфейса включите компьютер и нажмите клавиши **Правый Ctrl+G**.

Интерфейсы отличаются только внешним видом, функции выполняют одинаковые.

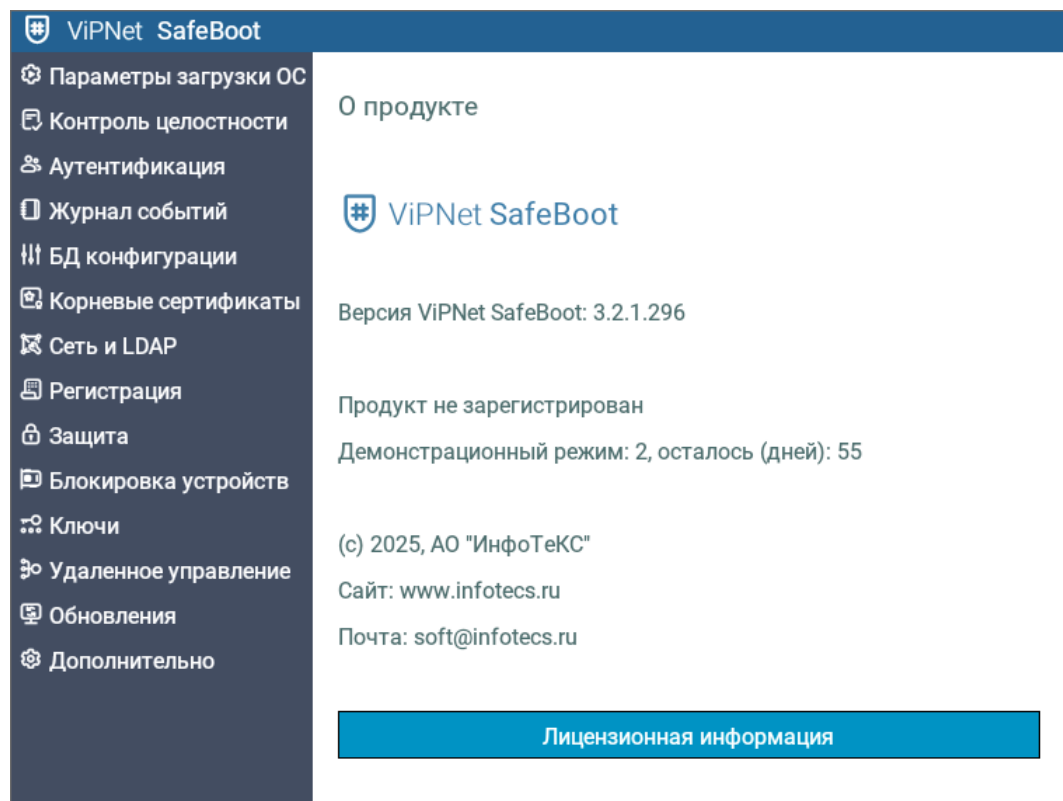


Рисунок 1. Графический интерфейс администратора

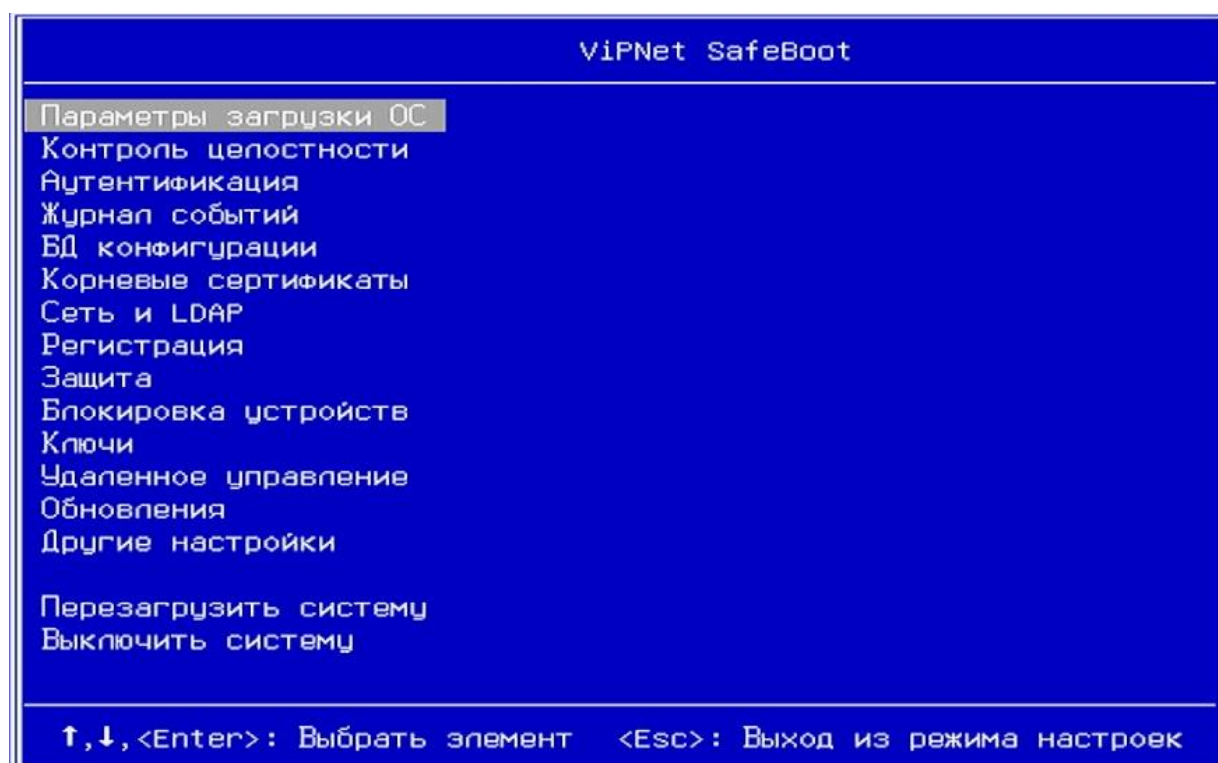


Рисунок 2. Текстовый интерфейс администратора

Вход в настройки ViPNet SafeBoot

Настройки ViPNet SafeBoot доступны в соответствии с [полномочиями администратора](#). Чтобы войти в настройки ViPNet SafeBoot:

- 1 Включите компьютер.
- 2 ViPNet SafeBoot запустится автоматически.



Примечание. При запуске ViPNet SafeBoot происходит проверка исполняемой памяти модулей. Модули загружаются только в проверенный участок памяти.

-
- 3 Введите имя пользователя и пароль в ViPNet SafeBoot.



Внимание! Количество попыток ввода пароля при аутентификации ограничено. Администратор будет заблокирован при превышении количества неудачных попыток аутентификации. Для возможности восстановления пароля администратора или сброса пароля до значения при первом включении [создайте диск восстановления](#).

-
- 4 Чтобы войти в настройки, нажмите клавишу F2.
 - 5 Ознакомьтесь с уведомлениями и нажмите ОК.

Первый вход

- 1 При появлении окна аутентификации введите имя пользователя **Administrator**.
- 2 Введите пароль **12345678**.
- 3 Чтобы войти в настройки, нажмите клавишу **F2**.
- 4 Ознакомьтесь с уведомлениями и нажмите **ОК**. Откроется окно с настройками.
- 5 Вы можете ознакомиться с лицензионным соглашением, для этого выберите **О продукте** и нажмите **Лицензионная информация**.
- 6 Выберите **Аутентификация**.
- 7 В списке **Текущие пользователи** выберите **Administrator**.
- 8 **Создайте диск восстановления**, если не создали его при установке ViPNet SafeBoot. Вы не сможете изменить пароль администратора, пока не подготовите диск восстановления.
- 9 Если в качестве способа аутентификации вы выбрали пароль:
 - 9.1 Вы можете изменить минимально и максимально допустимую длину пароля.
 - 9.2 Вы можете задать использование сложного пароля. Для этого выберите **Сложный пароль**.

Примечание. Требования к сложному паролю:



- хотя бы одна буква латинского алфавита от А до Z и от а до z;
- хотя бы одна цифра от 0 до 9;
- хотя бы один **специальный символ**: \ / ? . , < > ; " ' { } [] _ - = + () * & ? ^ % \$ # № @ ! ` ~ .

-
- 9.3 Можно создать новый пароль с помощью программного датчика случайных чисел или вручную. Чтобы создать пароль с помощью ПДСЧ, выберите **Сгенерировать пароль**. Чтобы создать пароль вручную, нажмите **Изменить пароль**.

При создании пароля с помощью ПДСЧ, если функция **Сложный пароль** неактивна, будет создан пароль, содержащий латинские буквы в верхнем и нижнем регистрах.
 - 9.4 Введите новый пароль и нажмите клавишу **Enter**. Повторите ввод пароля.
 - 9.5 Вы можете ограничить срок действия вашего пароля. Для этого выберите **Ограничить срок действия пароля**. В строке **Срок действия пароля (дней)** установите нужное значение. По умолчанию установлено ограничение 365 дней.
 - 10 Вы можете установить режим единого входа в ViPNet SafeBoot и в ОС. Для этого выберите **Single Sign-On**.
 - 11 Выберите **профиль загрузки**. Если профиль загрузки не выбран, учётной записи будет назначен профиль загрузки по умолчанию.
 - 12 Чтобы **настроить график работы**, нажмите **Настройки доступа**.

- 13 Если диск восстановления создан, вы можете назначить для себя другой способ аутентификации (см. [Добавление учетной записи](#)).
- 14 Нажмите **Сохранить настройки**.
- 15 Ознакомьтесь с уведомлениями и нажмите **ОК**.

Создание диска восстановления



Совет. Рекомендуется создавать диск восстановления на установочном USB-носителе.

Диск восстановления понадобится для временного отключения функциональности и при потере аутентификационных данных администратора по умолчанию.

Если для установки ViPNet SafeBoot вы использовали диск восстановления по умолчанию, вы можете создать его в настройках ViPNet SafeBoot.

Если перед установкой ViPNet SafeBoot вы создавали диск восстановления, его изменение для установленного ViPNet SafeBoot будет недоступно.

Чтобы создать диск восстановления:

- 1 Подключите USB-носитель.
- 2 [Войдите в настройки ViPNet SafeBoot](#) под встроенной учетной записью администратора.
- 3 Выберите **Аутентификация**.
- 4 Выберите пользователя **Administrator**.
- 5 Нажмите **Подготовить диск восстановления**.
- 6 Ознакомьтесь с уведомлениями и нажмите **ОК**.



Внимание! Храните диск восстановления в надежном месте. Доступ к диску восстановления должен быть ограничен в соответствии с требованиями к безопасности в вашей организации.

Регистрация

При первом запуске ViPNet SafeBoot переходит в демонстрационный режим, который длится 60 дней. В демонстрационном режиме доступны все функции. При включении ViPNet SafeBoot в нижнем левом углу экрана появляется надпись: **Демонстрационный режим, осталось (дней)**.

Если не зарегистрировать ViPNet SafeBoot до окончания демонстрационного периода, он перейдет в режим ограниченной функциональности или будет выключен — в зависимости от выбранного режима (см. «Руководство по установке» раздел «Подготовка установочного USB-носителя»).

Регистрация выполняется с использованием технологического компьютера с Windows 7 или выше и доступом к интернету.

Чтобы зарегистрировать ViPNet SafeBoot:

- 1 На USB-носителе создайте папку `itregdata`.
- 2 В папке `itregdata` создайте файл `serial.txt` с серийным номером ViPNet SafeBoot, полученным в ИнфоТеКС.

Для регистрации ViPNet SafeBoot на партии компьютеров создайте файл `serial_list.txt` со списком серийных номеров. Каждый номер записывайте с новой строки.

На каждом компьютере, где нужно зарегистрировать ViPNet SafeBoot:

- 2.1 Включите компьютер.
- 2.2 Подключите USB-носитель.
- 2.3 [Войдите в настройки ViPNet SafeBoot](#).
- 2.4 Выберите **Регистрация**.
- 2.5 Нажмите **Импортировать серийный номер**.

В строке **Серийный номер** появится серийный номер.

- 2.6 Выберите **Создать запрос на регистрацию**.
- 2.7 В окне подтверждения нажмите **ОК**.

На USB-носителе в папке `itregdata` будет создана папка с данными для регистрации на основе рассчитанного при первом запуске ViPNet SafeBoot уникального кода компьютера.

- 3 После сбора серийных номеров папка `itregdata` примет вид:

```
itregdata\  
  
    serial_list.txt (или serial.txt с серийным номером одного компьютера)  
  
    <Код компьютера 1>_<Серийный номер 1>  
  
    <Код компьютера 2>_<Серийный номер 2>  
  
    ...
```

- 4 [Выберите архив с утилитами](#) для вашей операционной системы, платформы и исполнения.

- 5 На технологическом компьютере распакуйте архив

`vipnet_safeboot-[ОС]_tools-[платформа]-r-bin-<номер версии>.zip.`

- 6 Подключите USB-носитель с данными регистрации к технологическому компьютеру.

- 7 На компьютере запустите командную строку и выполните:

- 7.1 Перейдите в папку `registration`:

`cd <Путь до папки>\registration`

- 7.2 Запустите скрипт `process_reg_requests.bat` и укажите путь до папки `itregdata` на USB-носителе:

`process_reg_requests.bat <Путь до папки>\itregdata`

Содержимое папки `registration` менять нельзя.

Файл `code.txt` с кодом регистрации сохранится в папке `itregdata\<Код компьютера>_<Серийный номер>` для регистрируемого компьютера или для каждого компьютера из партии.

- 8 Загрузите код регистрации (для лицензирования) на каждый компьютер с ViPNet SafeBoot:

- 8.1 Подключите USB-носитель с кодом регистрации к компьютеру.

- 8.2 Выберите **Регистрация**.

- 8.3 Нажмите **Импортировать код регистрации**.

- 8.4 Появится уведомление об обновлении кода регистрации. Нажмите **ОК** и **Перезагрузить систему**.

Порядок базовой настройки

Для обеспечения базовой защиты компьютеров:

- 1 [Создайте диск восстановления](#), если не создали его при установке ViPNet SafeBoot.
- 2 [Измените пароль администратора](#), если еще не меняли его. Используйте генерацию пароля с помощью ПДСЧ.
- 3 [Установите политику паролей для пользователей](#). Рекомендуется включить сложный пароль, ограничить срок его действия и установить 10 и менее попыток ввода.
- 4 [Настройте профиль загрузки ОС по умолчанию](#). Не используйте параметр загрузки BIOS, данная опция используется в особых случаях и не является доверенным способом загрузки по умолчанию.
- 5 [Установите необходимые корневые сертификаты и CRL](#).
- 6 [Создайте учетную запись](#) дополнительного администратора для управления настройками продукта. [Заблокируйте](#) от имени дополнительного администратора учетную запись администратора по умолчанию.
- 7 [Добавьте учётные записи](#). Для этого выберите:
 - [полномочия пользователя](#) учётной записи,
 - способ аутентификации,
 - настройки доступа.
- 8 [Настройте контроль целостности](#) компонентов ОС и аппаратных компонентов.
- 9 Включите необходимые функции [защиты](#):
 - защита BIOS,
 - эмуляция NVRAM,
 - контроль программных SMI.
- 10 [Измените ключи](#):
 - установите сертификат проверки запросов управления,
 - установите сертификат контроля целостности данных,
 - измените ключ защиты данных.

Сертификат проверки запросов и ключ защиты данных должны соответствовать используемым сертификату и ключу в управляющем приложении, например ViPNet EPP.

Для тонкой настройки ознакомьтесь со всеми возможностями ViPNet SafeBoot в разделе [Настройки ViPNet SafeBoot](#).

Рекомендуемые действия по настройке ViPNet SafeBoot:

- Выбирайте для пользователей способ аутентификации, включающий электронный идентификатор:

- Добавление пользователя с аутентификацией по электронному идентификатору;
- Добавление пользователя с аутентификацией по электронному идентификатору и паролю;
- Добавление пользователя с аутентификацией по коду на электронном идентификаторе.
- Настройте профили загрузки ОС.
- Выполните [автоопределение компонентов ОС](#) в режиме полный для каждого профиля загрузки ОС. При необходимости, дополните список контроля целостности вручную.
- Ограничьте время сессии аутентификации.
- Включите блокировку PCI Option ROM.
- Включите функции [защиты](#):
 - блокировка встроенных средств обновления BIOS,
 - фильтрация передачи управления,
 - блокировка ACPI WPBT,
 - защита дисков от записи,
 - блокировка клавиатуры на стадии загрузчика ОС,
 - защита системных таблиц UEFI.

2

Настройка параметров загрузки ОС

Профиль загрузки по умолчанию	37
Настройка профилей загрузки ОС	38

Профиль загрузки по умолчанию

Вы можете настроить профиль загрузки, который будет использоваться по умолчанию, или создать дополнительные профили загрузки.

Профиль загрузки по умолчанию изначально присутствует в списке профилей. Вы можете его изменить, но не можете удалить.

Профиль загрузки по умолчанию используется для пользователей, для которых не найдена в базе данных связь с другим профилем загрузки, например:

- пользователи, добавленные с помощью импорта базы данных ViPNet SafeBoot версии ниже 3.2.0;
- пользователи, которые были в базе данных до обновления на версию 3.2.0 (до изменения профиля);
- пользователи, для которых назначен профиль по умолчанию;
- пользователи LDAP;
- при загрузке ОС после автохода.

[Настройте профиль загрузки по умолчанию](#) при первоначальной настройке ViPNet SafeBoot. Если профиль по умолчанию заполнен не полностью, загрузка ОС невозможна.

Настройка профилей загрузки ОС

Чтобы настроить профиль загрузки ОС:

- 1 Войдите в настройки **ViPNet SafeBoot**.
- 2 Для режима загрузки ОС по сети **настройте сеть**.
- 3 Выберите **Параметры загрузки ОС**.
- 4 Нажмите **Профиль загрузки по умолчанию** или **Добавить профиль загрузки** (для создания дополнительного профиля).
- 5 Для дополнительного профиля введите название. В названии нельзя использовать специальные символы.
- 6 Выберите режим загрузки ОС в соответствии с документацией на ОС.

ViPNet SafeBoot поддерживает несколько режимов загрузки ОС:

- **Использование параметров загрузки BIOS.**
ViPNet SafeBoot использует порядок загрузки ОС, определенный в BIOS Setup.
 - **Legacy (режим совместимости).**
Подходит для загрузки всех ОС, установленных в режиме legacy.
 - **UEFI.**
Подходит для загрузки всех ОС, установленных в режиме UEFI.
 - **По сети.**
Поддерживается только для UEFI ОС, IPv4, протоколов PXE и HTTP при наличии драйвера в BIOS.
- 7 Для режима загрузки **UEFI** выберите загрузочный раздел и загрузчик операционной системы, для режима загрузки **legacy** выберите загрузочное устройство, а для режима **по сети** выберите устройство сетевой загрузки и получите загрузчик ОС.
 - 8 Нажмите **Сохранить настройки**.
 - 9 В окне подтверждения нажмите **ОК**.

Чтобы изменить настройки профиля загрузки, в разделе **Параметры загрузки ОС** выберите профиль, внесите изменения и нажмите **Сохранить настройки**.

Чтобы удалить дополнительный профиль загрузки:

- 1 В разделе **Параметры загрузки ОС** выберите профиль.
- 2 Нажмите **Удалить профиль загрузки**.
- 3 Подтвердите удаление.

При удалении профиля удаляются и эталоны контроля целостности, относящиеся к этому профилю. Если профиль, который использовался пользователем, удалили, назначьте пользователю новый профиль.

Профиль по умолчанию удалить нельзя.

3

Управление учетными записями пользователей

Учётные записи пользователей	41
Полномочия пользователей	43
Восстановление пароля администратора	44
Добавление учетной записи	45
Изменение, блокирование и удаление учётной записи пользователя	55

Учётные записи пользователей

Вы можете создать несколько учётных записей пользователей на одном компьютере для разграничения прав, а также соответствия учётных записей в ViPNet SafeBoot и ОС. Каждой учётной записи назначаются параметры:

- Имя учётной записи.
- Способ аутентификации.
- [Роль пользователя](#).
- Аутентификационные данные.
- Профиль загрузки ОС.
- Дополнительные параметры, определяющие ограничение к качеству аутентификационных данных и их времени действия.
- Включение [Single Sign-On](#) — автоматического входа в ОС с текущими аутентификационными данными.
- Блокирование пользователя.
- Настройки доступа, определяющие в какое время у пользователя есть доступ в ОС.

При аутентификации в ViPNet SafeBoot действует ограничение на количество неудачных попыток:

- После 5 неудачных попыток подряд компьютер выключается.
- После 10 неудачных попыток подряд вход в ОС для всех пользователей блокируется. Счетчик неудачных попыток аутентификации сбросится в следующих случаях:
 - после успешной аутентификации пользователя, если было выполнено менее 10 неудачных попыток;
 - после аутентификации администратора, если было выполнено 10 неудачных попыток.



Внимание! Кроме учётной записи администратора по умолчанию максимально можно создать 31 учётную запись.

Для обеспечения безопасности рекомендуем создать новую учётную запись администратора, а учётную запись администратора по умолчанию заблокировать. Учётную запись администратора по умолчанию можно будет восстановить с помощью диска восстановления.

Режим SSO



Внимание! Для работы режима Single Sign-On ОС должна быть установлена в режиме UEFI.

При аутентификации в режиме Single Sign-On ViPNet SafeBoot записывает аутентификационные данные в энергозависимую переменную NVRAM. Данные считываются специализированным ПО, например ViPNet SafePoint, и происходит автоматический вход в ОС:

Данные для аутентификации в ОС, в том числе пароль, передаются в зашифрованном виде. Режим работает для следующих способов аутентификации:

- по паролю;
- по электронному идентификатору и паролю;
- по коду на электронном идентификаторе.

Если режим Single Sign-On включен, пароль вводится только для аутентификации в ViPNet SafeBoot.



Примечание. Если в системе есть диски LUKS, кроме пароля ViPNet SafeBoot потребуется вводить пароль от диска LUKS.

Полномочия пользователей

В ViPNet SafeBoot можно создать учётную запись с одной из трех ролей:

- Администратор. Может менять все настройки ViPNet SafeBoot и загружать ОС. Вы можете создать несколько учётных записей с полномочиями администратора.
- Аудитор. Может просматривать и выгружать журнал событий ViPNet SafeBoot, менять свой пароль и загружать ОС.
- Пользователь. Может только загружать ОС и менять пароль в настройках ViPNet SafeBoot.

Восстановление пароля администратора

Вы можете восстановить пароль администратора только при наличии [диска восстановления](#):

- 1 Подключите установочный USB-носитель с файлом восстановления.
- 2 Перезагрузите компьютер, при инициализации ViPNet SafeBoot нажимайте клавиши **правый Ctrl+R** до появления приглашения к аутентификации.
- 3 Следуйте указаниям программы.
- 4 В окне аутентификации введите имя пользователя — **Administrator**, пароль — **12345678**.
- 5 Установите новый пароль.
- 6 В журнале событий появится информация о восстановлении пароля.

Добавление учётной записи

Настройка политики паролей

Вы можете назначить для каждой роли свою политику паролей. Политику паролей удобно использовать, если требования к паролям одинаковые для многих учётных записей с одной ролью. Значения, установленные в политике паролей, можно изменить для каждого пользователя.

При настройке политики паролей вы можете изменять параметры только в рамках значений, установленных в ViPNet SafeBoot по умолчанию.

В политике паролей вы можете установить следующие требования:

- минимальную и максимальную длину пароля;
- количество попыток ввода пароля;
- сложный пароль;
- срок действия пароля.

Настройка графика доступа

Для каждого пользователя вы можете настроить время, когда пользователю разрешен доступ в ViPNet SafeBoot:

- график работы (фиксированный или плавающий);
- рабочие дни;
- день начала работы;
- время начала и окончания рабочего дня;
- время начала и окончания перерыва на обед;
- начало и окончание ближайшего отсутствия.



Примечание. Все пользователи, кроме пользователей с LDAP-аутентификацией, могут просматривать настройки доступа своей учётной записи.

Добавление пользователя с аутентификацией по паролю

Если для входа в учётную запись будет использоваться режим Single Sign-On, необходимо:

- Дополнительное ПО уровня ОС. Чтобы получить его, [обратитесь в ИнфоТеКС](#).
- Совпадение имени пользователя и пароля в ОС и в ViPNet SafeBoot.

Чтобы добавить учётную запись:

- 1 [Войдите в настройки ViPNet SafeBoot](#).
- 2 Выберите **Аутентификация**.
- 3 Нажмите **Добавить нового пользователя**.
- 4 Введите **Имя пользователя**.

Имя пользователя может содержать от 1 до 32 символов русского или латинского алфавита.



Примечание. Для переключения языка ввода в ViPNet SafeBoot нажмите **Shift+Alt** или правый **Ctrl+L**.

Имя пользователя не должно содержать символ \.

- 5 В списке **Роль** [выберите роль](#) нового пользователя.
- 6 В списке **Способ аутентификации** выберите **Пароль**.
- 7 Вы можете задать пароль вручную или создать с помощью ПДСЧ.
 - Чтобы создать пароль с помощью ПДСЧ, выберите **Сгенерировать пароль**.
 - Чтобы создать пароль вручную, выберите **Изменить пароль**.

При создании пароля с помощью ПДСЧ, если функция **Сложный пароль** неактивна, будет создан пароль, содержащий латинские буквы в верхнем и нижнем регистрах.

- 8 Вы можете изменить минимальную и максимальную длину пароля, заданную по умолчанию.



Примечание. По умолчанию в ViPNet SafeBoot пароль может содержать от 8 до 32 символов. Дополнительные ограничения задаются администратором в политике паролей и не могут выходить за эти рамки.

- 9 Вы можете ограничить количество попыток ввода пароля. Для этого в строке **Количество попыток ввода пароля** установите нужное значение. По умолчанию установлено ограничение 10 попыток.

Если пользователь превысит установленное количество неудачных попыток ввода пароля, учётная запись заблокируется. Для разблокировки учётной записи пользователя [выполните вход](#) с учётной записью администратора.

- 10 Вы можете задать использование сложного пароля. Для этого выберите **Сложный пароль**.

Сложный пароль должен содержать:

- хотя бы одну букву латинского алфавита от А до Z и от а до z;
- хотя бы одну цифру от 0 до 9;
- хотя бы один [специальный символ](#): | \ / ? . , < > ; ' ' { } [] _ - = + () * & ? ^ % \$ # № @ ! ` ~ .

- 11 Вы можете ограничить срок действия пароля. Для этого выберите **Ограничить срок действия пароля**. В строке **Срок действия пароля (дней)** установите нужное значение. По умолчанию для пользователя установлено ограничение 30 дней, для администратора и аудитора — 365 дней.

При установленном флажке **Ограничить срок действия пароля** за 7 дней до истечения срока действия у пользователя будет появляться сообщение о смене пароля. Если по истечении срока пароль не изменен, пользователь будет заблокирован. На работу других учётных записей на компьютере это не повлияет.

- 12 Вы можете установить режим единого входа в ViPNet SafeBoot и в ОС. Для этого выберите **Single Sign-On**.
- 13 Выберите **профиль загрузки**. Если профиль загрузки не выбран, учётной записи будет назначен профиль загрузки по умолчанию.
- 14 **Настройте график работы пользователя**, для этого нажмите **Настройка доступа**.
- 15 Нажмите **Сохранить настройки**.
- 16 Ознакомьтесь с уведомлением и нажмите **ОК**.

Имя пользователя появится в списке **Текущие пользователи**.

Добавление пользователя с аутентификацией по электронному идентификатору



Примечание. Перед инициализацией электронного идентификатора Guardant ID и Guardant ID версии 2 подготовьте USB-носитель с ключевым контейнером, созданным в ViPNet CSP, и сертификат (см. [Guardant ID](#)).

-
- 1 Войдите в настройки ViPNet SafeBoot.
 - 2 Подготовьте электронный идентификатор.
 - 3 Установите корневой сертификат и список отозванных сертификатов.
 - 4 Подключите электронный идентификатор.
 - 5 Выберите **Аутентификация**.
 - 6 Нажмите **Добавить нового пользователя**.
 - 7 Введите **Имя пользователя**.

Имя пользователя может содержать от 1 до 32 символов русского или латинского алфавита. Не используйте символ \.



Примечание. Для переключения языка ввода нажмите **Shift+Alt** или **правый Ctrl+L**.

- 8 В списке **Роль** выберите **роль** нового пользователя.
- 9 В списке **Способ аутентификации** выберите **Эл.идентификатор**.
- 10 Если вы используете электронный идентификатор Guardant ID, задайте настройки:
 - 10.1 В строке **Эл.идентификатор** выберите электронный идентификатор.
 - 10.2 Введите ПИН для установленного Guardant ID.

Примечание. Если в списке **Эл. идентификатор** нет сертификатов **Guardant ID** или вы хотите перезаписать сертификат, инициализируйте электронный идентификатор:



- 1 Выберите **Инициализировать идентификатор**.
- 2 В окне подтверждения нажмите **ОК**.
- 3 Откроется файловый менеджер. Выберите сертификат пользователя, расположенный на USB-носителе.
- 4 Выберите ключевой контейнер, соответствующий сертификату.
- 5 Введите ПИН контейнера.
- 6 В окне подтверждения нажмите **ОК**.
- 7 Произойдет инициализация электронного идентификатора. В окне подтверждения нажмите **ОК**.

-
- 10.3 Выберите сертификат пользователя в списке **Сертификат**.
 - 11 Если вы используете электронный идентификатор Рутокен, JaCarta, ФОПОС или ESMART Token, задайте настройки:
 - 11.1 В строке **Эл.идентификатор** выберите электронный идентификатор.
 - 11.2 Введите ПИН для электронного идентификатора.
 - 11.3 Выберите сертификат пользователя в списке **Сертификат**
 - 11.4 Вы можете изменить ПИН электронного идентификатора — нажмите **Изменить PIN**
 - 12 Для автоматической аутентификации при подключении электронного идентификатора, выберите **Неинтерактивная аутентификация**.

Автоматическая аутентификация не поддерживается на электронных идентификаторах Guardant.



Примечание. Для работы неинтерактивной аутентификации разрешите её использование в разделе **Параметры аутентификации**.

- 13 Выберите **профиль загрузки**. Если профиль загрузки не выбран, учётной записи будет назначен профиль загрузки по умолчанию.
- 14 **Настройте график работы пользователя**, для этого нажмите **Настройка доступа**.
- 15 Нажмите **Сохранить настройки**.
- 16 В окне подтверждения нажмите **ОК**.

Имя пользователя появится в списке **Текущие пользователи**.



Примечание. Если при аутентификации не подключен назначенный пользователю электронный идентификатор и подключен не назначенный пользователю электронный идентификатор, в журнале аудита фиксируется информация об этом идентификаторе. Эта информация может быть передана администратору безопасности или в SIEM-систему.

Добавление пользователя с аутентификацией по электронному идентификатору и паролю

Если для входа в учетную запись будет использоваться режим Single Sign-On:

- Обратитесь за дополнительным ПО уровня ОС в [ИнфоТеКС](#) и установите его.
- Установите одинаковые имя пользователя и пароль в ОС и в ViPNet SafeBoot.

Чтобы добавить учётную запись:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 [Подготовьте электронный идентификатор.](#)
- 3 [Установите корневой сертификат и список отозванных сертификатов.](#)
- 4 Подключите электронный идентификатор.
- 5 Выберите **Аутентификация**.
- 6 Нажмите **Добавить нового пользователя**.
- 7 Введите **Имя пользователя**.

Имя пользователя может содержать от 1 до 32 символов русского или латинского алфавита. Не используйте символ \.



Примечание. Для переключения языка ввода в ViPNet SafeBoot нажмите **Shift+Alt** или правый **Ctrl+L**.

- 8 В списке **Роль** [выберите роль](#) нового пользователя.
- 9 В списке **Способ аутентификации** выберите **Эл.идентификатор и пароль**.
- 10 Если вы используете электронный идентификатор Guardant ID:
 - 10.1 В строке **Эл.идентификатор** выберите электронный идентификатор.
 - 10.2 Введите ПИН для установленного Guardant ID.

Примечание. Если в списке **Эл. идентификатор** нет сертификатов **Guardant ID** или вы хотите перезаписать сертификат, инициализируйте электронный идентификатор:



- 1 Выберите **Инициализировать идентификатор**.
 - 2 В окне подтверждения нажмите **ОК**.
 - 3 Откроется файловый менеджер. Выберите сертификат пользователя, расположенный на USB-носителе.
 - 4 Выберите ключевой контейнер, соответствующий сертификату.
 - 5 Введите ПИН контейнера.
 - 6 В окне подтверждения нажмите **ОК**.
 - 7 Произойдет инициализация электронного идентификатора. В окне подтверждения нажмите **ОК**.
-

10.3 Выберите сертификат пользователя в списке **Сертификат**.

11 Если вы используете электронный идентификатор Рутокен, JaCarta, ФОРОС или ESMART Token:

11.1 В строке **Эл.идентификатор** выберите электронный идентификатор.

11.2 Введите ПИН для электронного идентификатора.

11.3 Выберите сертификат пользователя в списке **Сертификат**.

11.4 Вы можете изменить ПИН электронного идентификатора — нажмите **Изменить PIN**.

12 Укажите настройки пароля:

12.1 Вы можете изменить минимальную и максимальную длину пароля, заданные по умолчанию.



Примечание. По умолчанию в ViPNet SafeBoot пароль может содержать от 8 до 32 символов. Дополнительные ограничения задаются администратором в политике паролей и не могут выходить за эти рамки.

12.2 Если требуется, укажите количество попыток ввода пароля (по умолчанию установлено 10). Если это значение будет превышено, учётная запись заблокируется.

12.3 Вы можете задать использование сложного пароля. Для этого выберите **Сложный пароль**.

Сложный пароль должен содержать:

- хотя бы одну букву латинского алфавита от A до Z и от a до z;
- хотя бы одну цифру от 0 до 9;
- хотя бы один **специальный символ**: | \ / ? . , < > ; " ' { } [] _ - = + () * & ? ^ % \$ # № @ ! ` ~ .

12.4 Чтобы ограничить срок действия пароля: выберите **Ограничить срок действия пароля**. В строке **Срок действия пароля (дней)** установите значение. По умолчанию для пользователя установлено ограничение 30 дней, для администратора и аудитора — 365 дней.

При установленном флажке **Ограничить срок действия пароля** за 7 дней до истечения срока действия у пользователя будет появляться сообщение о смене пароля. Если по

истечении срока пароль не изменен, пользователь будет заблокирован. На работу других учётных записей на компьютере это не повлияет.

13 Задайте пароль одним из способов:

- Вручную — выберите **Изменить пароль**.
- Автоматически — выберите **Сгенерировать пароль**.

Если функция **Сложный пароль** неактивна, будет создан пароль, содержащий латинские буквы в верхнем и нижнем регистрах.

14 Вы можете установить режим единого входа в ViPNet SafeBoot и в ОС. Для этого выберите **Single Sign-On**.

15 Выберите **профиль загрузки**. Если профиль загрузки не выбран, учетной записи будет назначен профиль загрузки по умолчанию.

16 **Настройте график работы пользователя**, для этого нажмите **Настройка доступа**.

17 Нажмите **Сохранить настройки**.

18 В окне подтверждения нажмите **ОК**.

Имя пользователя появится в списке **Текущие пользователи**.



Примечание. Если при аутентификации не подключен назначенный пользователю электронный идентификатор и подключен не назначенный пользователю электронный идентификатор, в журнале аудита фиксируется информация об этом идентификаторе. Эта информация может быть передана администратору безопасности или в SIEM-систему.

Добавление пользователя с аутентификацией по коду на электронном идентификаторе

Если для входа в учётную запись будет использоваться режим Single Sign-On:

- Обратитесь за дополнительным ПО уровня ОС в **ИнфоТеКС** и установите его.
- Установите одинаковые пароль в ОС и код на электронном идентификаторе.

Чтобы добавить учётную запись:

- 1 **Войдите в настройки ViPNet SafeBoot**.
- 2 **Подготовьте электронный идентификатор**.
- 3 Подключите электронный идентификатор.
- 4 Выберите **Аутентификация**.
- 5 Нажмите **Добавить нового пользователя**.
- 6 Введите **Имя пользователя**.

Имя пользователя может содержать от 1 до 32 символов русского или латинского алфавита. Не используйте символ \.



Примечание. Для переключения языка ввода в ViPNet SafeBoot нажмите **Shift+Alt** или правый **Ctrl+L**.

-
- 7 В списке **Роль** выберите роль нового пользователя.
 - 8 В списке **Способ аутентификации** выберите **Код на эл.идентификаторе**.
 - 9 Чтобы установить режим единого входа в ViPNet SafeBoot и в ОС, перед изменением кода выберите **Single Sign-On**.
 - 10 Нажмите **Изменить код**. Будет создан код с помощью программного датчика случайных чисел.
При включении Single Sign-On создание кода с помощью программного датчика случайных чисел отключается, код задается вручную.



Примечание. Код может содержать от 8 до 32 символов.
Дополнительные ограничения задаются администратором, но не могут выходить за эти рамки.

-
- 11 В окне подтверждения нажмите **ОК**.
 - 12 Чтобы ограничить срок действия кода: выберите **Ограничить срок действия кода**. В строке **Срок действия кода (дней)** установите нужное значение. По умолчанию для пользователя установлено ограничение 30 дней, для администратора и аудитора — 365 дней.



Примечание. Нельзя изменить срок действия кода, записанного на электронный идентификатор. Чтобы изменить срок действия, измените код.

При установленном флажке **Ограничить срок действия кода** за 7 дней до истечения срока действия у пользователя будет появляться сообщение о смене кода. Если по истечении срока код не изменен, пользователь будет заблокирован. На работу других учетных записей на компьютере это не повлияет.

-
- 13 В строке **Эл.идентификатор** выберите электронный идентификатор.
 - 14 Введите ПИН для электронного идентификатора.
Вы можете изменить ПИН электронного идентификатора Рутокен или JaCarta, для этого нажмите **Изменить PIN**.
 - 15 Выберите **профиль загрузки**. Если профиль загрузки не выбран, учётной записи будет назначен профиль загрузки по умолчанию.
 - 16 **Настройте график работы пользователя**, для этого нажмите **Настройка доступа**.
 - 17 Нажмите **Сохранить настройки**.
 - 18 Ознакомьтесь с уведомлениями и нажмите **ОК**.

Имя пользователя появится в списке **Текущие пользователи**.



Примечание. Если при аутентификации не подключен назначенный пользователю электронный идентификатор и подключен не назначенный пользователю электронный идентификатор, в журнале аудита фиксируется информация об этом идентификаторе. Эта информация может быть передана администратору безопасности или в SIEM-систему.

Добавление пользователя с LDAP-аутентификацией

При отсутствии связи с сервером LDAP пользователь сможет пройти аутентификацию, если ранее он успешно проходил аутентификацию и в кеше есть его учётная запись.

Для доступа к функции LDAP-аутентификации:

- 1 [Настройте сеть и LDAP](#).
- 2 Вы можете установить список пользователей, зарегистрированных на LDAP-сервере, которым разрешена LDAP-аутентификация в ViPNet SafeBoot.

Параметры аутентификации

Вы можете ограничить время, по окончании которого:

- Компьютер выключится.
Время до окончания сеанса аутентификации указано в окне аутентификации в строке **Время сессии аутентификации**.
- Произойдет автоматический вход в систему.
Время до автоматического входа в систему указано в окне аутентификации в строке **Время до загрузки без аутентификации**.
- Произойдет автоматическая аутентификация, если подключен электронный идентификатор пользователя, которому назначена неинтерактивная аутентификация. Если электронный идентификатор не подключен или найдено несколько пользователей, которым назначена неинтерактивная аутентификация, автоматическая аутентификация не произойдет.
Время до автоматической аутентификации указывается в окне аутентификации в строке **Время до неинтерактивной аутентификации**.

Чтобы ограничить время аутентификации:

- 1 [Войдите в настройки ViPNet SafeBoot](#).
- 2 Выберите **Аутентификация**.
- 3 Выберите **Ограничение сессии аутентификации**.

- 4 Задайте от 15 до 180 секунд.

Чтобы разрешить автоматический вход в систему:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Аутентификация**.
- 3 Выберите **Загрузка без аутентификации**.
- 4 Задайте от 1 до 30 секунд.

Чтобы разрешить автоматическую аутентификацию по электронному идентификатору:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Аутентификация**.
- 3 Выберите **Неинтерактивная аутентификация**.
- 4 Задайте от 1 до 60 секунд.

Ограничения проверяются в следующем порядке:

- 1 Неинтерактивная аутентификация.
- 2 Автоматический вход.
- 3 Интерактивная аутентификация.

Изменение, блокирование и удаление учётной записи пользователя

Изменение

Полный доступ к настройкам пользователя с аутентификацией по электронному идентификатору предоставляется после ввода ПИН.

Вы можете изменить все настройки учётной записи, кроме имени и роли.

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Если задана аутентификация по электронному идентификатору, подключите идентификатор.
- 3 Выберите **Аутентификация**.
- 4 В списке **Текущие пользователи** выберите имя пользователя.
- 5 Введите ПИН для электронного идентификатора.
- 6 Если войти в учётную запись без ввода ПИН, изменение сертификата пользователя будет недоступно.
- 7 Внесите изменения.
- 8 Нажмите **Сохранить настройки**.

Блокирование

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Аутентификация**.
- 3 В списке **Текущие пользователи** выберите имя пользователя.
- 4 Выберите **Заблокировать пользователя**.
- 5 Нажмите **Сохранить настройки**.
Вход в ViPNet SafeBoot для этой учётной записи будет заблокирован.

Чтобы разблокировать учётную запись:

- 1 Снимите флажок **Заблокировать пользователя**.
- 2 Нажмите **Сохранить настройки**.

Удаление

- 1 [Войдите в настройки ViPNet SafeBoot.](#)

- 2 Выберите **Аутентификация**.
- 3 В списке **Текущие пользователи** выберите имя пользователя.
- 4 Нажмите **Удалить пользователя**.
- 5 В окне подтверждения нажмите **ОК**.

4

Аутентификация с помощью электронного идентификатора

Порядок подготовки электронного идентификатора	58
Установка корневого сертификата и списка отозванных сертификатов	61
Экспорт корневого сертификата и списка отозванных сертификатов	63
Удаление корневого сертификата	64

Порядок подготовки электронного идентификатора

- 1 Проверьте, что ваш электронный идентификатор поддерживается (см. [Совместимые электронные идентификаторы](#)).
- 2 На технологическом компьютере создайте запрос на сертификат.
- 3 Доверенным способом передайте запрос в удостоверяющий центр и получите: сертификат пользователя, корневой сертификат, CRL. Использовать сертификаты, полученные другим способом, не допускается.
ViPNet SafeBoot поддерживает форматы сертификатов X.509 (DER или PEM) и PKCS#7.
- 4 Запишите сертификат на электронный идентификатор.
- 5 [Установите корневой сертификат и список отозванных сертификатов](#).
- 6 [Создайте учётную запись в ViPNet SafeBoot](#).
- 7 Доверенным способом передайте электронный идентификатор пользователю.

JaCarta

Подготовка электронного идентификатора JaCarta PKI/ГОСТ:

- 1 Установите на технологический компьютер [ViPNet CSP](#).
- 2 Создайте запрос на сертификат с помощью утилиты «Создание запроса на сертификат» из комплекта ViPNet CSP. Укажите в качестве носителя ключевой информации электронный идентификатор.
- 3 Передайте запрос в удостоверяющий центр.
- 4 Получите сертификат, корневой сертификат и CRL.
- 5 Запишите полученный сертификат на электронный идентификатор с помощью криптопровайдера ViPNet CSP.

Подготовка электронного идентификатора JaCarta-2 PKI/ГОСТ:

- 1 Установите на технологический компьютер ПО «Единый клиент JaCarta» производства [компании «Аладдин»](#).
- 2 Отформатируйте электронный идентификатор с помощью ПО «Единый клиент JaCarta».
- 3 Создайте запрос на сертификат в ПО «Единый клиент JaCarta».
- 4 Передайте запрос в удостоверяющий центр.
- 5 Получите сертификат, корневой сертификат и CRL.

- 6 Запишите сертификат на электронный идентификатор с помощью ПО «Единый клиент JaCarta».
- 7 При загрузке сертификата пользователя в ПО «Единый клиент JaCarta» снимите флажок **Задать имя контейнера**.

Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен Lite

- 1 Установите на технологический компьютер комплект ПО «Драйверы Рутокен для Windows» производства [компании «Актив»](#).
- 2 Установите криптопровайдер ViPNet CSP.
- 3 Отформатируйте электронный идентификатор с помощью ПО «Панель управления Рутокен».
- 4 Создайте запрос на сертификат с помощью утилиты «Создание запроса на сертификат» из комплекта ViPNet CSP. Укажите в качестве носителя ключевой информации электронный идентификатор.
- 5 Передайте запрос в удостоверяющий центр.
- 6 Получите сертификат.
- 7 Запишите сертификат на электронный идентификатор с помощью криптопровайдера ViPNet CSP.

Для электронных идентификаторов Рутокен ЭЦП, Рутокен ЭЦП 2.0 и Рутокен ЭЦП 3.0 вы можете создать ключевой контейнер в формате `rfx` или `p12` и записать на электронный идентификатор с помощью ПО «Панель управления Рутокен».

Guardant ID

- 1 Установите на технологический компьютер криптопровайдер ViPNet CSP.
- 2 Создайте запрос на сертификат с помощью утилиты «Создание запроса на сертификат» из комплекта [ViPNet CSP](#). Укажите в качестве носителя ключевой информации корневую папку на USB-носителе.
- 3 Передайте запрос в удостоверяющий центр.
- 4 Получите сертификат.
- 5 Запишите сертификат на USB-носитель.
- 6 В ViPNet SafeBoot инициализируйте электронный идентификатор (см. [Добавление пользователя с аутентификацией по электронному идентификатору](#)).

ViPNet SafeBoot 3.2.1 поддерживает только один сертификат на электронном идентификаторе Guardant ID.

ФОРОС

- 1 Установите на технологический компьютер утилиту FOROS-Master производства [компании «СмартПарк»](#).
- 2 Отформатируйте электронный идентификатор с помощью утилиты FOROS-Master.
- 3 Установите на технологический компьютер [ViPNet CSP](#).
- 4 Создайте запрос на сертификат с помощью утилиты «Создание запроса на сертификат» из комплекта ViPNet CSP. Укажите в качестве носителя ключевой информации электронный идентификатор.



Примечание. При запросе на сертификат используйте алгоритмы ГОСТ 34.10-2018 (ГОСТ 34.10-2012), 256/512 бит или ГОСТ 34.10-2001. ViPNet SafeBoot поддерживает только эти алгоритмы для электронного идентификатора ФОРОС.

- 5 Передайте запрос в удостоверяющий центр.
- 6 Получите сертификат, корневой сертификат и CRL.
- 7 Запишите полученный сертификат на электронный идентификатор с помощью криптопровайдера ViPNet CSP.

ESMART Token

- 1 Установите на технологический компьютер ПО «ESMART PKI Client» производства [компании «ESMART»](#).
- 2 Отформатируйте электронный идентификатор с помощью ПО «ESMART PKI Client».
- 3 Создайте запрос на сертификат в ПО «ESMART PKI Client».



Примечание. При запросе на сертификат используйте алгоритмы ГОСТ 34.10-2018 (ГОСТ 34.10-2012), 256/512 бит или ГОСТ 34.10-2001. ViPNet SafeBoot поддерживает только эти алгоритмы для электронного идентификатора ESMART Token ГОСТ.

- 4 Передайте запрос в удостоверяющий центр.
- 5 Получите сертификат, корневой сертификат и CRL.
- 6 Запишите сертификат на электронный идентификатор с помощью ПО «ESMART PKI Client».

Порядок обновления информации на электронном идентификаторе

Обновление сертификата на электронном идентификаторе

Чтобы обновить сертификат на электронном идентификаторе, выполните [порядок подготовки соответствующего электронного идентификатора](#).

Обновление кода на электронном идентификаторе

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 Подключите электронный идентификатор пользователя.
- 3 Выберите **Аутентификация**.
- 4 Нажмите имя пользователя.
- 5 Нажмите **Изменить код**. Будет создан код с помощью программного датчика случайных чисел.

В исполнении 2 при включении Single Sign-On создание кода с помощью программного датчика случайных чисел отключается, код задается вручную.



Примечание. Код может содержать от 8 до 32 символов.

Дополнительные ограничения задаются администратором, но не могут выходить за эти рамки.

- 6 В окне подтверждения откажитесь от использования существующего кода.
- 7 Нажмите **Сохранить настройки**.
- 8 Ознакомьтесь с уведомлениями и нажмите **ОК**.

Установка корневого сертификата и списка отозванных сертификатов

ViPNet SafeBoot использует сертификаты форматов X.509 (DER или PEM) и PKCS#7.

Чтобы установить корневой сертификат:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Подключите USB-носитель с сертификатом.
- 3 Выберите **Корневые сертификаты**.
- 4 Нажмите **Установить корневой сертификат**.
- 5 В списке сертификатов выберите файл сертификата.
- 6 Сертификат появится в списке **Установленные корневые сертификаты**.

Чтобы установить или обновить список отозванных сертификатов (CRL):



Внимание! CRL требуется периодически обновлять. Следите за актуальностью установленного списка.

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Подключите USB-носитель, содержащий CRL.
- 3 Выберите **Корневые сертификаты**.
- 4 В списке **Установленные корневые сертификаты** выберите сертификат.
- 5 Нажмите **Установить/обновить CRL**.
- 6 Выберите файл *.crl.
- 7 В поле **Текущий CRL** отобразится номер и срок действия CRL.

Экспорт корневого сертификата и списка отозванных сертификатов

Вы можете выгрузить сертификат из ViPNet SafeBoot для повторного использования.

Чтобы выгрузить корневой сертификат:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Подключите USB-носитель, на который будете выгружать сертификат.
- 3 Выберите **Корневые сертификаты**.
- 4 В списке **Установленные корневые сертификаты** выберите сертификат.
- 5 Нажмите **Экспортировать корневой сертификат**.
- 6 Появится сообщение, что корневой сертификат выгружен. Нажмите **ОК**.

Корневой сертификат выгружается в файл `ca.crt` в корневую папку USB-носителя.

Чтобы выгрузить установленный в ViPNet SafeBoot CRL:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Подключите USB-носитель, на который будете выгружать CRL.
- 3 Выберите **Корневые сертификаты**.
- 4 В списке **Установленные корневые сертификаты** выберите сертификат.
- 5 Нажмите **Экспортировать CRL**.

CRL экспортируется в файл `crl.crl` в корневую папку USB-носителя.

Удаление корневого сертификата

Если установленный корневой сертификат был скомпрометирован или истек срок его действия, вы можете удалить его:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Корневые сертификаты**.
- 3 В списке **Установленные корневые сертификаты** выберите сертификат.
- 4 Нажмите **Удалить корневой сертификат**.

Если установленный список отозванных сертификатов (CRL) не актуален, вы можете удалить его:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Корневые сертификаты**.
- 3 В списке **Установленные корневые сертификаты** выберите сертификат.
- 4 Нажмите **Удалить CRL**.

5

Настройки сети и LDAP

Настройка сети	66
Настройки подключения к LDAP-серверу	67
Настройка режима SSO для аутентификации доменного пользователя	69

Настройка сети

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 Выберите **Сеть и LDAP**.
- 3 В списке **Сетевой интерфейс** выберите сетевой интерфейс для подключения к сети.
- 4 В списке **Получение IP** выберите:



Примечание. Поддерживается только IPv4-протокол.

-
- **динамически** — для автоматического назначения IP-адресов с использованием DHCP;
 - **статически** — для ручного способа назначения IP-адресов.

Заполните поля **IP**, **маска** и **шлюз**.

- 5 Нажмите **Сохранить и применить настройки сети**.

Появится сообщение о сохранении настроек сети. Нажмите **ОК**.

Настройки подключения к LDAP-серверу



Примечание. Для использования Single Sign-On установите дополнительное ПО, поддерживающее SSO, для установки в ОС. Для получения ПО обратитесь в [службу поддержки](#).

Настройте подключение к LDAP-серверу для аутентификации пользователей, зарегистрированных на сервере LDAP.

Предварительно подготовьте на USB-носителе список в виде текстового файла в кодировке utf-8/cp1251, каждая строка которого представляет собой полный DN пользователя, которому разрешается доступ. Например:

```
CN=user_2,CN=Users,CN=SafeBoot
```

```
CN=user_3,CN=Users,CN=SafeBoot
```

```
CN=user_4,CN=Users,CN=SafeBoot
```



Примечание. Вы можете подготовить список вручную или выгрузить его с LDAP-сервера с помощью утилиты для Windows `adsiedit` и привести к формату, подходящему для ViPNet SafeBoot.

Установите [корневой сертификат](#) сервера LDAP.

Убедитесь, что сертификат LDAP-сервера получен доверенным способом. Если нет возможности получить сертификат LDAP-сервера доверенным способом отключите аутентификацию по LDAP или использование TLS для аутентификации по LDAP.



Внимание! Корневой сертификат LDAP импортируется только в DER-формате.

- 1 [Войдите в настройки ViPNet SafeBoot](#).
- 2 Выполните [настройку сети](#).
- 3 Выберите **Сеть и LDAP**.
- 4 В разделе **Настройки LDAP** выберите **Разрешение аутентификации по LDAP**.
- 5 Заполните поля **IP сервера LDAP** и **Имя сервера LDAP**.



Примечание. При аутентификации пользователя будет использоваться указанное имя сервера.

6 Нажмите Проверить доступность сервера LDAP.

Дождитесь сообщения, что сервер доступен.

7 Выберите Использование TLS в сессии LDAP.



Внимание! LDAP поддерживает использование TLS версий 1.2 и 1.3.

8 Выберите корневой сертификат сервера LDAP для использования TLS.

9 Нажмите Настройки пользователей LDAP.

10 В строках Суффикс DN пользователей и Префикс DN пользователей задайте суффикс DN и префикс DN, которые указывают место хранения учетных записей.

Эти поля используются для упрощения ввода имени пользователя при аутентификации по LDAP.

Для аутентификации на сервере Astra ALD Pro в поле **Префикс DN пользователей** укажите атрибут UID. Если UID не указан, для аутентификации будет использоваться атрибут CN.



Примечание. Если не указывать значение в полях **Суффикс DN пользователей** и **Префикс DN пользователей**, то при аутентификации по LDAP нужно вводить полный DN пользователя, например: <ldap_server_name>\CN=User,CN=Users,CN=SafeBoot.

Если для полного DN пользователя "CN=User,CN=Users,CN=SafeBoot" в качестве суффикса DN пользователей указать значение "CN=Users,CN=SafeBoot", то при вводе имени пользователя нужно будет вводить: <ldap_server_name>\User.

11 Если для учетной записи нужно использовать режим единого входа, выберите Single Sign-On.

12 Чтобы загрузить белый список пользователей LDAP, которым разрешена аутентификация в ViPNet SafeBoot, нажмите Импортировать список.

12.1 Чтобы просмотреть список пользователей, нажмите **Просмотреть список**.

12.2 Чтобы удалить список пользователей, нажмите **Удалить список**.

13 Нажмите клавишу Esc, чтобы вернуться в меню Сеть и LDAP.

14 Нажмите Сохранить настройки LDAP.

15 Ознакомьтесь с уведомлениями и нажмите OK.

Настройка режима SSO для аутентификации доменного пользователя

Режим Single Sign-On в ViPNet SafeBoot доступен для локальных и доменных пользователей ОС. Для доменных пользователей ОС доступно два сценария настройки ViPNet SafeBoot:

Аутентификация в формате <имя сервера>\<имя учётной записи пользователя>:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Сеть и LDAP**.
- 3 [Задайте настройки подключения к LDAP-серверу.](#)
- 4 Нажмите **Настройки пользователей LDAP**.
- 5 Выберите **Single Sign-On для пользователей LDAP**.

При смене доменного пароля пользователя новый пароль актуален и при аутентификации в ViPNet SafeBoot.

Аутентификация в формате `UserName@domain`:

- 1 Создайте или выберите учётную запись локального пользователя в ViPNet SafeBoot с доменным форматом имени.
- 2 Установите для локального пользователя такой же пароль, как и для доменного.
- 3 В настройках ViPNet SafeBoot выберите **Аутентификация**. Выберите учётную запись пользователя и выберите **Single Sign-On**. Нажмите **Сохранить настройки**.

При смене доменного пароля измените пароль в ViPNet SafeBoot вручную.

6

Контроль целостности

Контроль компонентов ОС	71
Контроль аппаратных компонентов	77
Контроль зашифрованных дисков LUKS	80
Режим обучения	81
Отключение контроля целостности	83
Принудительная проверка целостности	84
Повторный расчёт контрольных сумм	85

Контроль компонентов ОС

При контроле целостности сравниваются эталонные контрольные суммы файлов (эталонные) с рассчитанными контрольными суммами.

Сертификаты контроля целостности

В ViPNet SafeBoot все данные, которые хранятся на диске, зашифровываются на ключе защиты данных. Для подтверждения целостности зашифрованных данных используют сертификат контроля целостности данных.

Запросы управления, обновления и программные модули проходят подтверждение целостности в ViPNet SafeBoot с помощью сертификата контроля целостности запросов управления, сертификата контроля целостности обновлений и сертификата контроля целостности кода.

В ViPNet SafeBoot предустановлены сертификаты контроля целостности по умолчанию. Замените эти сертификаты на новые.



Примечание. Сертификат контроля целостности кода и сертификат контроля целостности обновлений нельзя изменить.

Чтобы получить сертификаты контроля целостности, для каждого сертификата выполните:

- 1 С помощью ViPNet CSP создайте запрос на сертификат и получите контейнер с закрытым ключом:
 - алгоритм: ГОСТ Р 34.10-2012 256;
 - параметры алгоритма: CryptoPro_A_ParamSet.
- 2 Передайте запрос в удостоверяющий центр.
- 3 Получите:
 - Для контроля целостности запросов управления — сертификат формата DER или PEM.
 - Для контроля целостности данных — сертификат в формате DER или PEM.
- 4 Установите сертификат в ключевой контейнер.
- 5 Запишите ключевой контейнер на USB-носитель.

При изменении

сертификата контроля целостности запросов управления, сертификата контроля целостности данных или ключа защиты данных — сертификат или ключ, установленные по умолчанию, остаются храниться в модуле ViPNet SafeBoot. Вы можете вернуть изменённые сертификат и ключ к настройкам по умолчанию.

Чтобы изменить предустановленный сертификат контроля целостности запросов управления:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Подключите USB-носитель, содержащий файл сертификата.
- 3 Выберите **Ключи**.
- 4 Под строкой **Сертификат КЦ запросов управления** нажмите **Изменить сертификат**.
- 5 В окне подтверждения нажмите **ОК**.
- 6 В окне со списком сертификатов выберите файл сертификата.
- 7 Сертификат появится в строке **Сертификат КЦ запросов управления**.

Чтобы изменить предустановленный сертификат контроля целостности данных:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Подключите USB-носитель, содержащий контейнер с сертификатом.
- 3 Выберите **Ключи**.
- 4 Под строкой **Сертификат КЦ данных** нажмите **Изменить сертификат**.
- 5 В окне подтверждения нажмите **ОК**.
- 6 В окне со списком ключевых контейнеров с сертификатом выберите файл контейнера.
- 7 Введите ПИН.
- 8 Сертификат появится в строке **Сертификат КЦ данных**.

Чтобы изменить предустановленный ключ защиты данных:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Ключи**.
- 3 Под строкой **Ключ защиты данных** нажмите **Изменить ключ**.
- 4 В окне подтверждения нажмите **ОК**.
- 5 Введите новый пароль.
Длина пароля не менее 8 символов.
- 6 Повторите ввод пароля.
- 7 В строке **Ключ защиты данных** значение **по умолчанию** изменится на **изменен**.

Чтобы вернуться к сертификату или ключу по умолчанию:

- 1 Выберите **Сбросить сертификат** или **Сбросить ключ**.
- 2 В окне подтверждения нажмите **ОК**.

Автоопределение компонентов ОС

При автоопределении компонентов ОС выполняется сканирование ОС, ее компоненты (файлы и ключи реестра) автоматически ставятся на контроль. [Список контроля](#) автоматически создается:

- для Windows 7 и выше;
- UEFI Linux. Автоопределение доступно только в режиме загрузки UEFI с диска GPT.



Внимание! Для разделов LUKS список контроля автоматически не создается.

Компоненты ОС выбираются отдельно для каждого профиля.

Чтобы включить автоопределение компонентов:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Контроль целостности**.
- 3 Нажмите **Профили контроля целостности**.
- 4 Выберите профиль загрузки в списке.
- 5 Выберите системный и загрузочный разделы для ОС, загрузка которой настроена в выбранном профиле загрузки.
- 6 В списке **Режим автоопределения компонентов ОС** выберите [режим](#):
 - **базовый** — на контроль целостности ставится сокращенный перечень файлов и параметров реестра Windows,
 - **полный** — на контроль целостности ставится полный список файлов и параметров реестра Windows.
- 7 Нажмите **Автоопределение компонентов ОС**.
- 8 В окне подтверждения нажмите **ОК**.

Автоопределение компонентов ОС может занимать длительное время.
- 9 После окончания процедуры автоопределения появится сообщение о постановке компонентов на контроль. Нажмите **ОК**.

Чтобы прервать процедуру автоопределения, нажмите клавишу **Esc**. В окне подтверждения нажмите **ОК**.

Контроль параметров реестра Windows

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Контроль целостности**.

- 3 Нажмите **Профили контроля целостности**.
- 4 Выберите профиль загрузки, для которого настраиваете контроль целостности.
- 5 Нажмите **Контроль реестра Windows**.
- 6 Поставьте флажок **Контроль реестра Windows**.
- 7 Чтобы просмотреть перечень контролируемых параметров, нажмите **Список контролируемых параметров**.
- 8 Чтобы загрузить эталоны, нажмите **Импортировать эталоны КЦ**.
Выберите раздел и файл эталонов контроля целостности для загрузки.
- 9 Чтобы добавить контролируемый параметр, нажмите **Добавить параметры в список**.
Выберите параметр реестра, который нужно поставить на контроль.

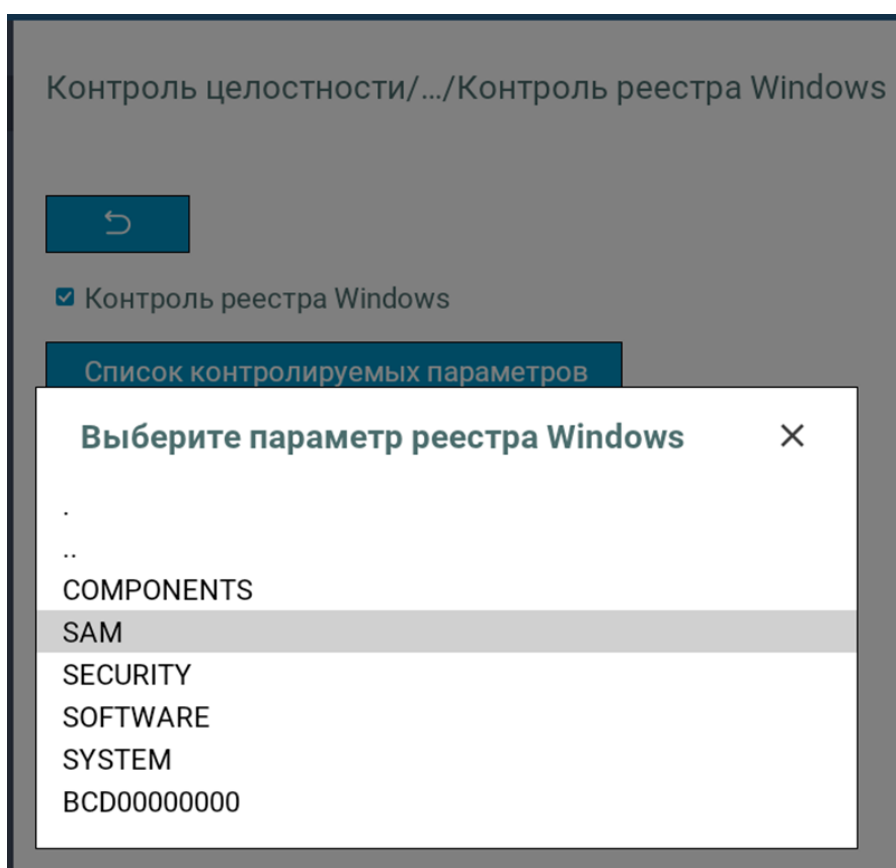


Рисунок 3. Выбор параметров для контроля

- Чтобы поставить на контроль целостности ветку реестра, выберите символ <.>.
- Чтобы поставить на контроль целостности все содержимое вложенных веток, нажмите **ОК**.
 - Чтобы поставить на контроль целостности ветку до первого уровня вложенности, нажмите **Отмена**.
 - Чтобы прервать постановку на контроль целостности, нажмите клавишу **Esc**.
- 10 Чтобы удалить параметры реестра Windows из контролируемого списка, нажмите **Удалить параметры из списка**.

Выберите параметр и нажмите клавишу **Enter**.

- 11 Чтобы просмотреть статистику по списку контроля целостности, а также информацию о размере списка эталонов и времени их последнего изменения, нажмите **Информация**.

После ознакомления с информацией нажмите **ОК**.

Контроль файлов

В списке контролируемых разделов может быть не более 8 записей.

Чтобы поставить на контроль целостности файлы:

- 1 [Войдите в настройки ViPNet SafeBoot](#).
- 2 Выберите **Контроль целостности**.
- 3 Нажмите **Профили контроля целостности**.
- 4 Выберите профиль загрузки, для которого настраиваете контроль целостности.
- 5 Нажмите **Контроль файлов**.

- 6 Чтобы добавить раздел в список контроля целостности:

6.1 Нажмите **Добавить раздел** и выберите в списке раздел.

6.2 Раздел появится в списке контролируемых разделов. Выберите его.

6.3 Вы можете:

- Добавить элементы в список.
- Просмотреть список контролируемых элементов.
- Удалить элементы из списка.
- Импортировать эталоны контроля целостности раздела диска.
- Отменить контроль целостности всех файлов раздела диска.

При снятии раздела диска с контроля целостности, он будет полностью снят с контроля, эталоны раздела диска можно будет использовать при повторной постановке этого раздела на контроль.

- Просмотреть статистику по списку контроля целостности, а также информацию о размере списка эталонов и времени их последнего изменения — нажмите **Информация**.

Выберите действие.

- 7 Чтобы добавить контролируемый элемент, нажмите **Добавить элементы в список**.

Выберите файл, который нужно поставить на контроль.

Чтобы поставить на контроль целостности папку, выберите символ <.>.

- Чтобы поставить на контроль целостности все вложенное содержимое папки, нажмите **ОК**.

- Чтобы поставить на контроль целостности папку до первого уровня вложенности, нажмите **Отмена**.
 - Чтобы прервать постановку на контроль целостности, нажмите клавишу **Esc**.
- 8 Чтобы импортировать эталоны контроля целостности (см. [Особенности импорта и экспорта эталонов контроля целостности](#)), нажмите **Импортировать эталоны КЦ**.
- Выберите раздел и файл эталонов. Формат может быть `bin` и `json`.



Примечание. USB-носители при импорте эталонов контроля целостности на контроль не ставятся.

Контроль файлов сетевой загрузки

Для загрузки ОС по сети без использования жесткого диска с сервера сетевой загрузки выгружается первичный загрузчик ОС и через него загружается ОС.

Вы можете контролировать целостность файлов сетевой загрузки, если выбран режим загрузки ОС **по сети**.

- 1 Войдите в настройки **ViPNet SafeBoot**.
- 2 Настройте сеть.
- 3 Добавьте профиль загрузки с режимом загрузки ОС по сети и получите загрузчик ОС.
- 4 Выберите **Контроль целостности**.
- 5 Нажмите **Профили контроля целостности**.
- 6 Выберите профиль загрузки, для которого настраиваете контроль целостности.
- 7 Нажмите **Контроль файлов сетевой загрузки**.
- 8 Выберите **Контроль файлов сетевой загрузки**.
- 9 В окне подтверждения нажмите **ОК**.
- 10 После окончания расчета эталонов контроля целостности для компонентов системы, вы сможете:
 - просмотреть **Список контролируемых элементов**,
 - **Импортировать эталоны КЦ**,
 - **Добавить элементы в список**,
 - **Удалить элементы из списка**.

Контроль аппаратных компонентов

Параметры контроля целостности аппаратных компонентов общие для всех профилей.

Вы можете поставить на контроль:

- Содержимое энергонезависимой памяти CMOS.
- Конфигурационное пространство PCI.
- Таблицы ACPI.
- SMBIOS,
- Карту распределения памяти.
- Модули UEFI.
- Загрузочные сектора на носителях информации. Выберите диск для постановки на контроль целостности.

На контроль целостности ставятся:

- для MBR-разметки — первые 63 сектора диска;
- для GPT-разметки — сектора GPT-разметки.
- Переменные NVRAM.

Переменная NVRAM содержит множество настроек. Чтобы при включенном [режиме обучения](#) изменение одной настройки не приводило к снятию с контроля целостности всей переменной, введены диапазоны, которые позволяют снимать с контроля только часть переменной, а остальные части продолжают контролироваться. Таким образом, на контроле остаются только стабильные участки переменных.

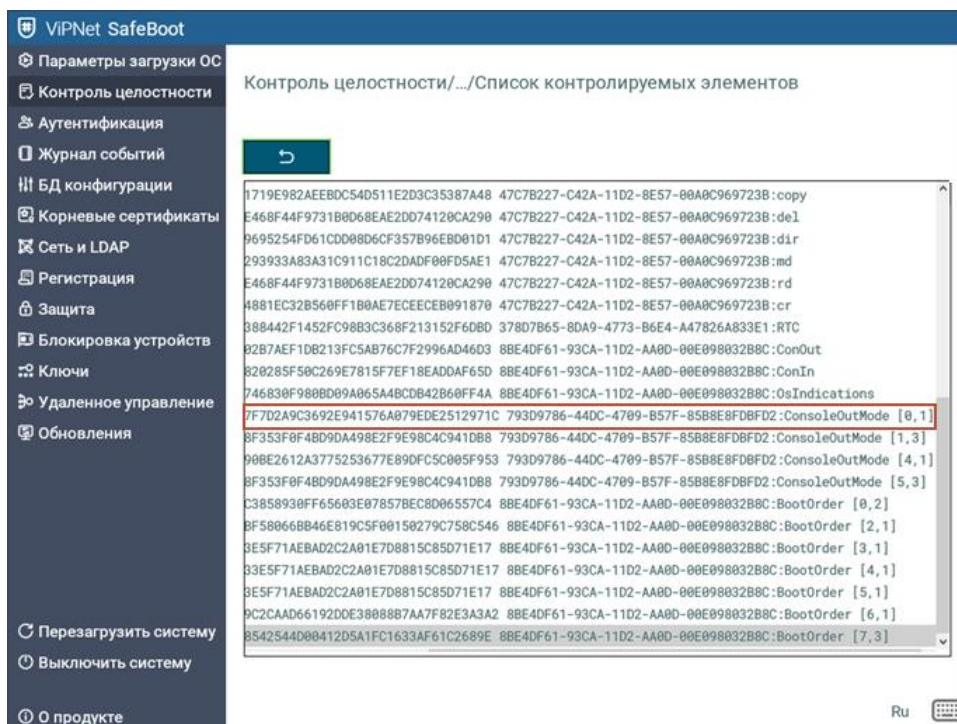


Рисунок 4. Диапазон NVRAM-переменной

Чтобы просмотреть контролируемый диапазон переменной, перейдите в **Список контролируемых элементов**. Диапазон указывается в квадратных скобках после переменной, например [4, 1], где первая цифра показывает смещение начала диапазона в байтах, вторая — количество байт в диапазоне.

- Системные таблицы UEFI — таблицу boot-сервисов BS и таблицу runtime-сервисов RT.

При постановке на контроль целостности эталонные значения рассчитываются не целиком для всей таблицы, а для каждого сервиса отдельно. Это позволяет ставить на контроль целостности как все сервисы, содержащиеся в таблице, так и часть из них. При включенном режиме обучения, если изменяется адрес сервиса, с контроля снимается не вся таблица целиком, а только один сервис, остальные остаются на контроле.

- Завершенность транзакций ФС (NTFS, EXT3 и EXT4).
- Диски.

На контроль целостности ставятся все диски, находящиеся в системе, при этом учитываются название диска, его серийный номер и порт, к которому подключен диск. При изменении любого из этих значений диск определяется как незарегистрированный и регистрируется нарушение контроля целостности.

Чтобы поставить на контроль:

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 Выберите **Контроль целостности**.
- 3 Нажмите **Контроль аппаратных компонентов**.
- 4 Выберите компоненты в списке.

- 5 В списке компонента **Диск для контроля загрузочных секторов** выберите диск. На контроль можно поставить только один элемент из списка.
- 6 Чтобы поставить все элементы на контроль, под списком компонентов нажмите **Выбрать все элементы**.
- 7 Если компонент ранее ставился на контроль целостности, появится сообщение о возможности использования существующих эталонов или создания новых.
 - 7.1 Чтобы использовать существующие эталоны, нажмите **ОК**.
 - 7.2 Чтобы рассчитать контрольные суммы состава подключенных аппаратных средств, нажмите **Отмена**.
- 8 Чтобы добавить или удалить элементы из компонента контроля целостности:
 - 8.1 Нажмите **Управление списками элементов**.
 - 8.2 В списке **Компонент контроля целостности** выберите компонент и выполните одно из действий:
 - Чтобы просмотреть список элементов, нажмите **Список контролируемых элементов**.
 - Чтобы добавить элементы в список, нажмите **Добавить элементы в список**, выберите элементы и нажмите клавишу **Enter**.
 - Чтобы удалить элементы из списка, нажмите **Удалить элементы из списка**, выберите элементы и нажмите клавишу **Enter**. В окне подтверждения нажмите **ОК**.
 - Чтобы просмотреть статистику по эталонам, информацию о размере списка эталонов и времени их последнего изменения, нажмите **Информация**. После ознакомления с информацией нажмите **ОК**.

Контроль зашифрованных дисков LUKS

Вы можете поставить на контроль целостности файлы на зашифрованном диске LUKS:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Контроль целостности**.
- 3 Нажмите **LUKS**.
- 4 Если в системе есть диски LUKS, выберите диск в списке **Раздел LUKS**.

Нажмите **Изменить пароль**. Введите пароль от диска LUKS и подтвердите его.

Произойдет расшифровка и монтирование диска. Пароль сохранится в базу данных ViPNet SafeBoot.

- 5 В списке **Точки монтирования** появятся все смонтированные разделы.



Внимание! При каждой загрузке ViPNet SafeBoot будет происходить монтирование дисков LUKS, что может увеличить время загрузки ViPNet SafeBoot.

- 6 [Поставьте на контроль целостности файлы](#) на смонтированном разделе диска LUKS.

Если вы удалите пароль от диска LUKS, диск перестанет монтироваться, но разделы останутся на контроле целостности. Снимите разделы LUKS с контроля целостности, иначе при загрузке ОС контроль целостности будет нарушен.

Если на контроле целостности стоит диск LUKS, при добавлении еще одного диска LUKS может измениться индексация разделов и нарушиться соответствие эталонов разделам LUKS. При добавлении нового диска LUKS, поставьте заново на контроль целостности все стоящие на контроле диски LUKS и импортируйте их эталоны.

Режим обучения

Режим обучения позволяет исключить из контроля целостности отдельные компоненты, диапазоны переменных NVRAM или адреса сервисов из системных таблиц UEFI, которые изменяются при нормальном функционировании системы. Элементы, которые не прошли проверку целостности, снимаются с контроля, система «обучается» контролировать определенный набор элементов.

- Если на контроле целостности стоит папка, то контролируется целостность всех вложенных файлов и существование вложенных папок.
- Если изменяется файл из папки, стоящей на контроле целостности, то этот файл снимается с контроля целостности.
- Если в папку, стоящую на контроле целостности, добавляется файл или вложенная папка, то файл ставится на контроль целостности, а папка — на контроль существования.
- Если из папки, стоящей на контроле целостности, удаляется файл или вложенная папка, то файл снимается с контроля целостности, а вложенная папка — с контроля существования.
- Если из папки, стоящей на контроле целостности, удаляется вложенная папка, то вложенная папка снимается с контроля существования.



Примечание. Если в системе произошло изменение компонентов, поставленных на контроль целостности, активируйте режим обучения повторно или измените список элементов на контроле целостности вручную.

Чтобы включить режим обучения:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Контроль целостности**.
- 3 Выберите компоненты ОС и аппаратные компоненты.
- 4 Выберите **Режим обучения**.
- 5 В окне подтверждения нажмите **ОК**.

Когда ViPNet SafeBoot обнаружит нарушение целостности контролируемых элементов, появится сообщение, что эти элементы сняты с контроля целостности. Информация об этих элементах заносится в журнал событий.

Режим обучения выключится автоматически после трех успешных загрузок ОС. Перед перезагрузкой выполните какие-либо действия, характерные для пользователя ОС, чтобы режим обучения снял с контроля целостности элементы, которые изменяет система.

Чтобы поставить на контроль целостности аппаратный компонент, который снял с контроля режим обучения:

- 1 Выберите **Контроль целостности > Контроль аппаратных компонентов**.

- 2 Снимите с контроля аппаратный компонент, измененный режимом обучения и поставьте его обратно на контроль.

Чтобы поставить на контроль целостности элементы компонента:

- 1 Выберите **Контроль целостности > Контроль аппаратных компонентов > Управление списками элементов**.
- 2 Выберите в списке компонент контроля целостности и нажмите **Добавить элементы в список**.

Чтобы поставить на контроль целостности параметр реестра Windows, который снял с контроля режим обучения:

- 1 Выберите **Контроль целостности > Профили контроля целостности > Контроль реестра Windows**.
- 2 Нажмите **Добавить параметры в список** и выберите параметр, который нужно поставить на контроль повторно.

Чтобы поставить на контроль целостности файлы, которые снял с контроля режим обучения:

- 1 Выберите **Контроль целостности > Профили контроля целостности > Контроль файлов**.
- 2 Нажмите **Добавить раздел** и выберите раздел, файлы в котором нужно поставить на контроль повторно.

Выбранный раздел появится в списке контролируемых разделов.

- 3 В списке контролируемых разделов выберите раздел и нажмите **Добавить элементы в список**.
- 4 Выберите файлы, которые нужно повторно поставить на контроль.

Отключение контроля целостности

Вы можете отключить контроль целостности в текущем сеансе, чтобы не тратить время на проведение контроля, например в процессе настройки ОС:

- 1 Войдите в настройки **ViPNet SafeBoot**.
- 2 Выберите **Контроль целостности**.
- 3 Выберите **Отключить КЦ в текущем сеансе**.

При выходе из ViPNet SafeBoot и продолжении загрузки ОС появится предупреждение **Контроль целостности отключен для текущего сеанса**.

Принудительная проверка целостности

Вы можете провести принудительную проверку целостности без последующей загрузки ОС:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Контроль целостности**.
- 3 Выберите объекты для контроля.
- 4 Нажмите **Проверить целостность**.

Контроль целостности выполняется для всех объектов, включенных в активные списки контроля целостности, и для всех модулей ViPNet SafeBoot.

- 5 В окне подтверждения нажмите **ОК**.

Повторный расчёт контрольных сумм

Вы можете повторно рассчитать эталоны контролируемых объектов в случае их штатного изменения:

- 1 Войдите в настройки [ViPNet SafeBoot](#).
- 2 Выберите **Контроль целостности**.
- 3 Нажмите **Перерассчитать эталоны КЦ**.



Примечание. Повторный расчёт производится только по компонентам из списка контроля целостности, новые элементы не добавятся.

- 4 В окне подтверждения нажмите **ОК**.

7

Настройки ViPNet SafeBoot

Защита	87
Блокировка устройств	89
Удалённое управление	90
Изменение даты и времени	91

Защита

В разделе **Защита** вы можете включить функции:

- **Защита BIOS.**

Позволяет защитить BIOS от записи и чтения, изменений UEFI-переменных, обеспечивает защиту при выходе из спящего режима (S3).

- **Блокировка встроенных средств обновления BIOS.**

Заблокируйте обновления BIOS, чтобы защитить ViPNet SafeBoot от удаления при обновлении BIOS. Эта функция поддерживается на платформах MSI, ASUS, Gigabyte, AsRock и для стандартного протокола FMP обновления BIOS.

- **Эмуляция NVRAM.**

При эмуляции NVRAM копируется во временную область памяти. Запись и чтение UEFI-переменных происходит во временной области памяти, в BIOS данные не записываются. Это позволяет предотвратить атаки на NVRAM. При включении защиты BIOS включите эмуляцию NVRAM для загрузки ОС.

- **Контроль программных SMI.**

Включает запрет на использование прерываний, которые можно использовать для получения доступа к BIOS Setup и перезаписи BIOS.

- **Блокировка ACPI WPBT.**

Блокирует создание ACPI-таблиц WPBT (Windows Platform Binary Table), с помощью которых в Windows автоматически запускаются исполняемые файлы, предоставляемые BIOS, которые могут содержать вредоносное ПО.

- **Защита дисков от записи.**

Блокирует запись на диски со стороны компонентов BIOS на ранней стадии загрузки.

- **Защита системных таблиц UEFI.**

Позволяет защитить системные таблицы UEFI от перезаписи адреса сервиса в таблице злоумышленником для получения управления при работе BIOS или ОС. Блокирует перехват системных таблиц UEFI путем замещения системных таблиц UEFI на их копии для всех модулей, которые загружаются после передачи управления операционной системе. Перехват системных таблиц выявляется при сравнении содержимого копий таблиц с эталонной копией.

Если в качестве загрузчика используется `shimx64.efi`, данную функцию необходимо отключить. Этот загрузчик перехватывает системные таблицы UEFI, что регистрируется ViPNet SafeBoot. Если в качестве загрузчика используется `bootx64.efi`, это не влияет на работу ViPNet SafeBoot и данную функцию можно оставить включенной.

- **Фильтрация передачи управления.**

Позволяет предотвратить передачу управления UEFI-загрузчикам и legacy-устройствам загрузки в обход механизма доверенной загрузки ОС, реализованной ViPNet SafeBoot. При блокировке передачи управления событие фильтрации фиксируется в журнале событий.

Данную функцию необходимо отключать для платформ, в которых BIOS Setup выполнен в виде UEFI-приложения, а не драйвера. Например, платформы с прошивками, собранными на базе стандартного EDK II. При включенной фильтрации вход в BIOS Setup для таких платформ будет блокироваться.

- **Блокировка клавиатуры на стадии загрузчика ОС.**

Позволяет предотвратить изменение стандартной конфигурации UEFI загрузчика ОС. Клавиатура недоступна пользователю во время UEFI-стадии загрузки (до передачи управления ОС или legacy загрузчику).

- **Разрешить однократный вход в BIOS Setup.**

ViPNet SafeBoot по умолчанию запрещает вход в BIOS Setup, чтобы защитить компьютер от нештатной загрузки ОС и изменения параметров конфигурации. Активация этой функции позволяет однократно зайти в BIOS.

При попытке несанкционированного входа в BIOS Setup с помощью клавиш **Del**, **Esc**, **F1—F12**, **Enter**, **Home**, **End**, **>**, **Tab**, сочетания клавиш **Ctrl+p**, **Ctrl+s**, **Ctrl+Home**, **PageUp**, **PageDown**:

- появится сообщение о запрете доступа к BIOS Setup — нажмите любую клавишу, чтобы перезагрузить компьютер;
- в журнале событий зафиксировается попытка входа в BIOS Setup и будут указаны клавиша или сочетание клавиш, которые использовались для входа.

Механизмы защиты, которые всегда включены:

- **Фильтрация доступа к NVRAM-переменным.**

Внутренний механизм защиты ViPNet SafeBoot, ограничивающий доступ к NVRAM-переменным (чтение, запись, перечисление), доступ разрешается или запрещается на основе имени или GUID переменной. Фильтрация работает на стадии времени исполнения и на стадии загрузки. Запрещается доступ к NVRAM-переменным журнала и конфигурации ViPNet SafeBoot, а также к переменным, критичным для загрузки в UEFI BIOS. Разрешается однократный доступ на чтение к переменным, относящимся к SSO.

Блокировка устройств

Блокировка устройств для UEFI PCI Option ROM — полный запрет запуска UEFI PCI Option ROM всех PCI-устройств. Все подключенные устройства с UEFI OpRom на момент включения функции добавляются в список разрешённых устройств. Вы можете добавить устройство из списка подключенных PCI-устройств в список разрешённых устройств или удалить из списка. Для управления блокировкой:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Блокировка устройств.**
- 3 Выберите **Включить блокировку PCI Option ROM.**
- 4 Чтобы просмотреть список разрешенных для запуска PCI-устройств, нажмите **Список разрешенных устройств.**
- 5 Чтобы включить возможность работы PCI Option ROM PCI-устройства, нажмите **Добавить устройство в список.**
- 6 Чтобы отключить возможность работы PCI Option ROM PCI-устройства, исключите его из списка разрешённых устройств. Для этого нажмите **Удалить устройство из списка** и выберите устройство.
- 7 Чтобы включить возможность работы PCI Option ROM всех подключенных PCI-устройств:
 - 7.1 Нажмите **Разрешить подключенные устройства.** Список разрешённых устройств будет обновлен.
 - 7.2 Ознакомьтесь с уведомлениями и нажмите **ОК.**

Удалённое управление

Вы можете удаленно управлять ViPNet SafeBoot с помощью ViPNet EndPoint Protection версии 1.6.0 (см. «ViPNet EndPoint Protection. Руководство администратора»):

- отправлять и активировать лицензии;
- управлять учетными записями пользователей с аутентификацией по паролю: создавать, изменять, удалять;
- управлять корневыми сертификатами и CRL: устанавливать, обновлять, удалять;
- обновлять ViPNet SafeBoot;
- просматривать журнал событий;
- экспортировать и импортировать базу данных.

Включение удаленного управления:

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 Установите [сертификат контроля целостности запросов управления](#).
- 3 Выберите **Удаленное управление**.
- 4 Выберите **Разрешить удаленное управление**.

Запрос управления — текстовый файл, подписанный откреплённой подписью, содержащий список контролируемых файлов (БД и эталонов контроля целостности продукта) и зафиксированных контрольных сумм по ним, что обеспечивает контроль целостности запроса управления.

При включении удалённого управления в настройках продукта:

- 1 В начале работы ViPNet SafeBoot:
 - проверяет наличие запроса управления на диске (в папке `EFI\Infotecs\mgmt`);
 - проверяет сертификат контроля целостности запроса управления;
 - контролирует целостность запроса управления;
 - выполняет запрос управления (обновление, импорт базы данных, списки эталонов контроля целостности);
 - фиксирует результат выполнения запроса управления.
- 2 При завершении работы ViPNet SafeBoot сохраняет в зашифрованном виде базу данных и журнал на диск в папку `EFI\Infotecs\mgmt`.

При удалённом управлении в журнале событий фиксируются все изменения настроек в загруженной базе данных с пометкой **[импорт БД]**.

Изменение даты и времени

1 Войдите в настройки ViPNet SafeBoot.

2 Выберите **Другие настройки > Дата и время**.

В окне отображаются текущие системные дата и время.

3 Выберите **Изменить дату**, введите дату в указанном формате, нажмите **ОК**.

Изменённая дата сразу отобразится в окне.

4 Выберите **Изменить время**, введите время в указанном формате, нажмите **ОК**.

Изменённое время сразу отобразится в окне.

8

База данных конфигурации

Ведение базы данных конфигурации	93
Экспорт настроек	95
Импорт настроек	99
Сброс настроек	100

Ведение базы данных конфигурации

База данных (БД) конфигурации ViPNet SafeBoot ведётся во внутренней памяти BIOS (NVRAM). В ней хранятся все текущие настройки продукта.

Администратор может использовать базу данных конфигурации ViPNet SafeBoot для переноса настроек на другие компьютеры, для восстановления настроек.

Базу данных можно хранить на диске. Чтобы выбрать режим ведения базы данных:

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 Выберите **БД конфигурации**.
- 3 В списке **Режим ведения БД конфигурации** выберите **внутренняя** или **внешняя (на диске)**.

В списке **Режим хранения эталонов КЦ** по умолчанию установлено значение **на диске**. Если ViPNet SafeBoot работает в **бездисковом режиме**, то в списке **Режим хранения эталонов КЦ** по умолчанию установлено значение **в БД**.

Бездисковый режим работы

Вы можете установить ViPNet SafeBoot на бездисковые устройства. Все модули ViPNet SafeBoot устанавливаются в память микросхемы BIOS.

В бездисковом режиме действуют следующие ограничения:

- база данных и журнал ViPNet SafeBoot хранятся в NVRAM;
- постановка компонентов программно-аппаратной среды на контроль целостности ограничена размером базы данных, зависящим от свободного места в NVRAM;
- нет возможности использовать режим удалённого управления.

При переходе в бездисковый режим происходят следующие изменения:

- режим ведения журнала переключается на **внутренний, циклический**;
- режим ведения базы данных переключается на **внутренняя**;
- с контроля целостности снимаются все компоненты;
- режим хранения эталонов контроля целостности переключается на **в БД**;
- режим удалённого управления отключается;
- в базе данных сбрасывается путь до рабочей папки.

Для включения бездискового режима все модули должны быть установлены в BIOS платформы.

Чтобы включить бездисковый режим:

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 В разделе **БД конфигурации** выберите **Бездисковый режим**.

ViPNet SafeBoot может автоматически переключиться в бездисковый режим в случае, когда невозможно восстановить рабочую папку, если все модули ViPNet SafeBoot установлены в памяти микросхемы BIOS.

При переключении из бездискового режима в обычный в базе данных включается режим хранения эталонов контроля целостности на диске.

Экспорт настроек

Вы можете выгрузить настройки на любой USB-носитель в корневую папку в файл `itsbdb.bin`. На USB-носителе появляется файл с подписью `itsbdb.bin.sig`. Для формата `json` имена файлов будут `itsbdb.json` и `itsbdb.json.sig`.

Настройки, которые можно выгрузить и загрузить:

- Общие настройки:
 - Параметры загрузки ОС.
 - Настройки процедуры входа в ОС.
 - Значение режима защиты BIOS.
- Учётные записи и настройки аутентификации.
- Корневые сертификаты, ключи.
- Настройки журнала и базы данных.
- Настройки сети и LDAP.

Чтобы выгрузить настройки:

- 1 Подключите USB-носитель.
- 2 [Войдите в настройки ViPNet SafeBoot](#).
- 3 Выберите **БД конфигурации**.
- 4 В списке **Формат настроек при экспорте/импорте** [выберите формат](#).
- 5 В списке **Режим экспорта настроек** [выберите режим](#).
- 6 Нажмите **Экспортировать настройки**.
- 7 В окне подтверждения нажмите **ОК**.
- 8 Ознакомьтесь с уведомлением и нажмите **ОК**.

Формат настроек при импорте и экспорте

Настройки базы данных конфигурации можно загрузить в ViPNet SafeBoot и выгрузить в форматах:

- `json`,
- бинарный.



Примечание. Формат настроек выбирается по усмотрению администратора. Для загрузки настроек ViPNet SafeBoot версий до 1.3 включительно используется бинарный формат.

Чтобы выбрать формат настроек БД:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **БД конфигурации**.
- 3 В списке **Формат настроек при экспорте/импорте** выберите формат.

Режимы экспорта

Базу данных можно экспортировать в одном из трёх режимов:

- базовый,
- расширенный,
- полный.

В базовом режиме выгружаются поля:

- Использование параметров загрузки BIOS.
- Режим ведения журнала.
- Подробная регистрации событий.
- Время ожидания сеанса аутентификации.
- Время ожидания автовогода.
- Режим обучения контроля целостности.
- Включение удалённого управления.
- Корневые сертификаты и CRL.

В расширенном режиме к полям базового режима добавляются:

- Контроль журнала транзакций ФС.
- Настройки LDAP.
- Защита BIOS и защита BIOS после S3.
- Включение эмуляции NVRAM.
- Контроль программных SMI.
- Блокировка ACPI WPBT.
- Защита системных таблиц UEFI.
- Фильтрация передачи управления стороннему коду.
- Блокировка клавиатуры на стадии загрузчика ОС.
- Настройка блокировки PCI OpROM.
- Защита дисков от записи.
- Сведения о пользователях и их настройки.

- Время ожидания неинтерактивной аутентификации.

В полном режиме база данных экспортируется со всеми полями, в том числе с данными регистрации. Не экспортируются только уникальное состояние ПДСЧ и время его инициализации.

Только в составе полной базы данных экспортируются структура профиля и связи пользователей с профилями.

При импорте формат базы данных определяется автоматически и поля в загружаемой базе данных перезаписывают поля в текущей базе данных. Групповые поля (корневые сертификаты и пользователи) перезаписываются целиком из новой базы данных.

Особенности импорта и экспорта эталонов контроля целостности

Эталоны контроля целостности вы можете экспортировать в режимах **расширенный** или **полный**. Будут экспортированы только эталоны компонентов, которые контролируются в момент экспорта. Файлы эталонов, которые не контролируются в момент экспорта, не экспортируются.

При экспорте файлы эталонов сохраняются в папку `itsbdb.<формат>.files`, которая расположена на том же уровне вложенности, что и файл базы данных (БД). Если такая папка уже была на носителе, она удаляется вместе с содержимым.



Примечание. <Формат> может быть bin и json.

При экспорте в режиме **базовый** эталоны не копируются, но, если на носителе найдена папка `itsbdb.<формат>.files`, она будет удалена.

Если на носителе найдена папка `itsbdb.<формат>.files` с эталонами, эталоны контроля целостности импортируются из неё независимо от формата импортируемой БД.

- Если установлен флажок **Перерассчитать эталоны КЦ при импорте**, эталоны файлов и реестра рассчитываются повторно.

Если флажок не установлен, эталоны импортируются без изменения.

- Для аппаратных компонентов эталоны рассчитываются повторно независимо от наличия флажка **Перерассчитать эталоны КЦ при импорте**.

При импорте базы данных с эталонами загружаются те эталоны, для которых будет найден профиль импорта в результирующей базе данных.



Примечание. Если папка с эталонами не найдена на носителе, эталоны не импортируются. При импорте неполной базы данных настройки контроля целостности не меняются.

Если в импортируемой базе данных включен контроль целостности, но на диске нет эталонов контроля целостности, то импорт произойдет без эталонов, что приведет к нарушению целостности при передаче управления ОС.

Экспортировать эталоны можно только в составе базы данных. Импортировать эталоны отдельно от базы данных можно, например для контроля целостности одинакового перечня файлов на разных компьютерах.

Импорт настроек

- 1 Подключите USB-носитель.
- 2 [Войдите в настройки ViPNet SafeBoot](#).
- 3 Выберите **БД конфигурации**.
- 4 Выберите формат в списке **Формат настроек при экспорте/импорте**.



Примечание. Файлы настроек `itsbdb.bin` и `itsbdb.bin.sig` соответствуют бинарному формату.

Файлы настроек `itsbdb.json` и `itsbdb.json.sig` соответствуют формату json.

- 5 Выберите **Перерассчитать эталоны КЦ при импорте**, если это необходимо (см. [Особенности импорта и экспорта эталонов контроля целостности](#)).
- 6 Если вы загружаете базу данных ViPNet SafeBoot версии 1.3 или 1.4, выберите **Не проверять подпись БД при импорте**.
- 7 Нажмите **Импортировать настройки**.
- 8 В окне подтверждения нажмите **ОК**.
- 9 Ознакомьтесь с уведомлением и нажмите **ОК**.
- 10 Нажмите любую клавишу, чтобы перезагрузить систему.

При локальной загрузке базы данных в журнале событий фиксируется импорт базы данных, а также все изменения настроек в загруженной базе данных с пометкой **[импорт БД]**.

Сброс настроек

Сброс всех настроек до настроек по умолчанию выполняется в случаях:

- когда нужно сбросить много настроек;
- когда нужно удалить конфиденциальную информацию в базе данных при переносе компьютера вне доверенного контура.

Чтобы сбросить настройки:

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 Выберите **БД конфигурации**.
- 3 Нажмите **Сбросить настройки**.
- 4 В окне подтверждения нажмите **ОК**.
- 5 Ознакомьтесь с уведомлением и нажмите любую клавишу, чтобы перезагрузить систему.

9

Управление журналом событий

Настройки журнала событий	102
Просмотр журнала событий	105
Экспорт записей журнала событий	107

Настройки журнала событий

В журнале регистрируются события учётных записей всех пользователей, администраторов и аудиторов.

- 1 [Войдите в настройки ViPNet SafeBoot](#).
- 2 Выберите **Журнал событий**.
- 3 В списке **Режим просмотра и экспорта журнала** выберите режим:
 - **весь журнал** — доступны все записи журнала, установлен по умолчанию;
 - **регион «основной»** — доступны записи без информации по контролю целостности;
 - **регион «КЦ»** — доступны записи, регистрирующие события контроля целостности.
- 4 В списке **Режим ведения журнала** выберите режим:
 - [внутренний, циклический](#) — установлен по умолчанию;
 - [внутренний, экспортируемый](#);
 - [внешний \(на диске\)](#).
- 5 Чтобы изменить уровень регистрации событий с основного на подробный, выберите **Подробная регистрация событий**.



Примечание. Режим подробной регистрации событий сильно нагружает систему, приводит к быстрому заполнению журнала в режиме внутренний и замедлению работы. Этот режим ведения журнала не предназначен для постоянного использования.

- 6 Чтобы [отправлять события по протоколу syslog](#), выберите **Журналирование по syslog**.
- 7 Чтобы отправлять CEF-сообщения на определенный сервер, введите его адрес в поле **IP сервера syslog**, иначе сообщения будут отправляться в широковещательном режиме.

Режим ведения журнала внутренний, циклический

Особенности ведения журнала **внутренний, циклический**:

- Журнал хранится в NVRAM-памяти BIOS.
- События регистрируются циклически, новые записи о событиях записываются вместо старых.
- При переключении режима на **внешний (на диске)** [выгрузите журнал](#) на USB-носитель.

При переключении на режим **внешний (на диске)** появится уведомление о выгрузке журнала. Для продолжения нажмите клавишу **Enter**, для отмены — **Esc**.

Перед выгрузкой журнала подключите USB-носитель и нажмите клавишу **Enter**. В результате:

- текущий журнал будет выгружен из NVRAM на USB-носитель;
- режим ведения журнала будет переведен на **внешний (на диске)**;
- на локальном диске в папке `EFI\Infotecs\log` будет создан новый журнал, все записи будут добавляться в него.

В случае отказа от выгрузки:

- текущий журнал сохраняется в NVRAM;
- режим ведения журнала будет переведен на **внешний (на диске)**;
- на локальном диске в папке `EFI\Infotecs\log` будет создан новый журнал, все записи будут добавляться в него.

Режим ведения журнала внутренний, экспортируемый

Особенности ведения журнала **внутренний, экспортируемый**:

- Журнал хранится в NVRAM-памяти BIOS.
- Если журнал заполнен более чем на 85%, при входе в систему будет появляться предупреждение о переполнении журнала.
- Если журнал переполнен, вход пользователей в систему блокируется, пока администратор или аудитор не выгрузит записи журнала.
- При переключении режима на **внешний (на диске)** [выгрузите журнал](#) на USB-носитель.

Режим ведения журнала внешний (на диске)

Особенности ведения журнала **внешний (на диске)**:

- Журнал хранится в зашифрованном виде на диске (EFI System Partition) в папке `EFI\Infotecs\Log\`.
- При переключении на другой режим журнал с диска не удаляется, но продолжаете в NVRAM.

Отправка событий журнала по протоколу syslog

Вы можете включить отправку событий журнала на сервер в формате CEF-сообщений по протоколу syslog в режиме реального времени. События записываются в журнал и отправляются на сервер в соответствии с выбранным уровнем журналирования. ViPNet SafeBoot может отправлять события по syslog в двух режимах:

- Широковещательный режим — не требует настраивать сеть, что позволяет отправлять более ранние события.
- Режим с указанием IP-адреса сервера — требует настройки сети.

Если включена отправка по протоколу syslog, но не введен адрес сервера, сообщения по умолчанию отправляются в широковещательном режиме.

Независимо от включения отправки событий по протоколу syslog все события записываются в локальный журнал, который можно выгрузить.

Пример CEF-сообщения

```
<134> 2022-11-10T15:00:00Z 192.168.0.1 CEF:0|Infotecs|ViPNet  
SafeBoot|<версия>|0053|Администратор аутентифицирован|5|msg=[Administrator, по паролю]
```

Просмотр журнала событий

Отображение журнала событий зависит от выбранного режима записи событий.

Для внутреннего режима ведения журнала вы можете просмотреть как объединенный журнал (весь журнал), так и отдельные его регионы (основной и «КЦ»). Объединение записей регионов в общий журнал происходит через сортировку событий по времени их наступления, поэтому возможно расхождение порядка следования событий в объединенном журнале при переводах времени назад (в отдельных регионах порядок сохраняется корректным).

Чтобы просмотреть записи журнала событий:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Журнал событий**.
- 3 Чтобы [настроить фильтрацию событий](#), нажмите **Настройки фильтра** и выберите параметры.
- 4 Вернитесь в раздел **Журнал событий**.
- 5 Нажмите **Просмотреть журнал**.

Записи в журнале событий выделяются цветом:

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

Детализированная информация предназначена для диагностики проблем разработчиками.

Фильтрация журнала событий

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Выберите **Журнал событий**.
- 3 Нажмите **Настройки фильтра**.
- 4 Выберите типы событий для просмотра:

- **Информационный (I).**

Содержит информационные сообщения и сообщения об успешно выполненных действиях.

- **Детальный (D).**

Содержит сообщения о работе модулей.

- **Ошибочный (E).**

Содержит сообщения об ошибках.

- 5 В списке **Модуль** выберите модуль, связанные с которым события нужно просмотреть.
Чтобы просмотреть события по всем модулям, в списке выберите **Значение не выставлено**.
- 6 В списке **Период времени** выберите период, за который нужно просмотреть события или выберите **Настраиваемый диапазон** и введите даты начала и окончания диапазона.
- 7 В поле **Строка поиска** введите набор символов или ID события для поиска по столбцу журнала **Событие**.

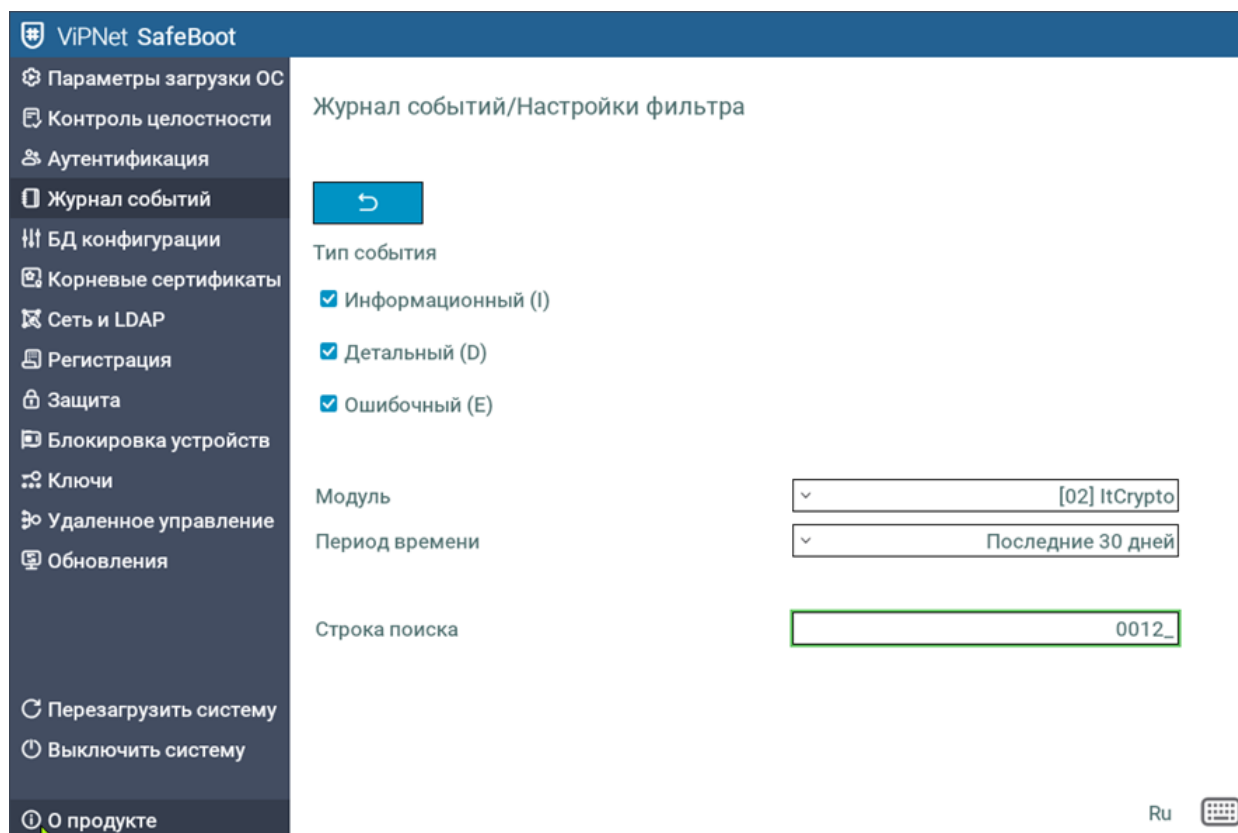


Рисунок 5. Настройка фильтра журнала событий

Экспорт записей журнала событий

Вы можете выгрузить записи журнала событий на USB-носитель в фиксированный файл `itsblog.txt` в корневую папку. На диске появится файл с подписью `itsblog.txt.sig`.

Вы можете выгрузить журнал событий полностью или частично. Записи региона «основной» выгружаются в файл `itsblog0.txt`, записи региона «КЦ» — в `itsblog1.txt` в корневую папку на USB-носителе.

При переполнении журнала:

- Если журнал переполняется в режиме записи событий, выгрузить его на диск может только администратор или аудитор.
- Если журнал переполняется до процедуры аутентификации или в процессе работы пользователя (не администратора или аудитора), журнал блокируется. На экране и во внутреннем журнале появляется сообщение о блокировке журнала. Дальнейшие записи во внутренний журнал игнорируются, аутентификация пользователей запрещается. Администратор или аудитор должен выгрузить журнал.
- Если журнал переполняется после аутентификации пользователя, система блокируется. Администратор или аудитор должен выгрузить журнал.

Чтобы выгрузить записи журнала событий:

- 1 [Войдите в настройки ViPNet SafeBoot.](#)
- 2 Подключите USB-носитель.
- 3 Выберите **Журнал событий**.
- 4 Нажмите **Экспортировать журнал**.

10

Обновление

Порядок обновления ViPNet SafeBoot

109

Порядок обновления ViPNet SafeBoot



Внимание! Во время обновления не выключайте питание и не перезагружайте компьютер, это выведет его из строя.

Перед обновлением подключите компьютер к источнику бесперебойного питания.

- 1 Получите файлы обновления в ИнфоТеКС.
- 2 Запишите файлы обновления на USB-носитель. Вы можете для этого использовать диск восстановления. Если вы записываете файлы обновления на новый USB-носитель, скопируйте на него файл `itrecovery.bin` с диска восстановления или [создайте новый диск восстановления](#).



Внимание! Чтобы при обновлении ViPNet SafeBoot сохранить настройки и журнал, а также при изменении конфигурации установленного ViPNet SafeBoot на USB-носителе в папке `itinstallcfg` переименуйте файл `clean_all` в `clean_modules`.

- 3 Подключите USB-носитель с файлами обновления.
- 4 Войдите в настройки ViPNet SafeBoot:
 - 4.1 Включите компьютер.
ViPNet SafeBoot запустится автоматически.
 - 4.2 Введите имя учетной записи и пароль в ViPNet SafeBoot.
 - 4.3 Нажмите клавишу **F2** для входа в настройки.
 - 4.4 Ознакомьтесь с уведомлениями и нажмите **ОК**.
- 5 Выберите **Обновления**.
- 6 Нажмите **Проверить наличие обновлений**.
Когда ViPNet SafeBoot найдет файлы обновления, появится информация об обновлении, вы сможете рассчитать контрольные суммы модулей обновления или обновить ViPNet SafeBoot.
- 7 Чтобы рассчитать и сравнить контрольные суммы модулей в пакете обновления и формуляре, выберите **Контрольные суммы модулей**.



Примечание. Контрольные суммы рассчитываются по ГОСТ 34.11.2018 (256 бит).

- 8 Чтобы установить обновление, нажмите **Обновить ViPNet SafeBoot**.
- 9 В окне подтверждения нажмите **ОК**.

После установки обновлений компьютер перезагрузится. В журнале событий появится запись о выполненном обновлении.

11

Переустановка ОС при активных механизмах защиты ViPNet SafeBoot

Переустановка ОС	112
Ошибка восстановления рабочей директории	113

Переустановка ОС

Для удобства переустановки ОС нужно отключить ViPNet SafeBoot и после переустановки ОС снова включить:

- 1 Войдите в настройки ViPNet SafeBoot.
- 2 Снимите с контроля целостности все компоненты ОС и аппаратные компоненты.
- 3 Подключите установочный USB-носитель. На USB-носителе должен быть только один раздел в формате FAT32.
- 4 Выберите **Параметры загрузки ОС**.
- 5 Нажмите **Загрузить Shell с диска**.
Запустится программа установки.
- 6 Нажмите **Esc**, чтобы выйти из меню установки.
- 7 В UEFI Shell последовательно выполните команды:

```
itinstall\tools\ProductManager.efi -m disabled
```

```
itinstall\tools\SeparateConfDBManager.efi -r
```
- 8 Отключите установочный USB-носитель и перезагрузите компьютер.
ViPNet SafeBoot будет отключен.
- 9 Вставьте установочный диск ОС и установите ОС в режиме UEFI.
- 10 Извлеките установочный диск ОС.
- 11 Подключите установочный USB-носитель ViPNet SafeBoot.
- 12 Перезагрузите ОС, на этапе инициализации BIOS включите ViPNet SafeBoot — нажмите клавиши **правый Ctrl+E**.
- 13 Чтобы подтвердить запрос на включение, нажмите **Enter**. Будет восстановлена рабочая директория и ViPNet SafeBoot включится.
- 14 Отключите установочный USB-носитель.
- 15 Настройте **профили загрузки** и **контроль целостности**.

Ошибка восстановления рабочей директории

Если после переустановки ОС не удалось восстановить рабочую директорию:

- 1 Убедитесь, что к компьютеру не подключены защищённые от записи диски в формате FAT32. Если подключены, отключите.
- 2 Убедитесь, что на установочном USB-носителе размечен только один раздел формата FAT32. Если разделов несколько, и диск инициализирован как диск восстановления:
 - 2.1 Сохраните файл `itrecovery.bin`.
 - 2.2 Подготовьте другой USB-носитель — отформатируйте раздел в формате FAT32.
 - 2.3 Скопируйте на USB-носитель установочные файлы ViPNet SafeBoot и файл `itrecovery.bin`.
- 3 Убедитесь, что на ESP-разделе свободно не менее 50 Мбайт. Если места недостаточно, освободите.
- 4 Создайте на системном диске дополнительный раздел FAT32, размером не менее 100 Мбайт. Создайте в корне раздела структуру каталогов `EFI\Infotecs`.
- 5 Повторите восстановление рабочей директории ViPNet SafeBoot.

Если восстановить рабочую директорию не удалось, обратитесь в [службу поддержки](#).

12

Дополнительные возможности ViPNet SafeBoot

Временное отключение функциональности ViPNet SafeBoot	115
Автоматическое восстановление рабочей директории	116
Автоматическое восстановление системного времени	117

Временное отключение функциональности ViPNet SafeBoot



Примечание. Если вы не создали диск восстановления ViPNet SafeBoot до установки, подготовьте его в соответствии с разделом [Создание диска восстановления](#).

При возникновении нештатной ситуации отключите функциональность ViPNet SafeBoot на время восстановления его работоспособности:

- 1 Подключите установочный USB-носитель с файлом восстановления.
- 2 Включите компьютер, нажмите клавиши **правый Ctrl+X**.

ViPNet SafeBoot будет временно отключен, загрузится ОС. При последующих загрузках функциональность ViPNet SafeBoot восстановится.

Автоматическое восстановление рабочей директории

После появления сообщения об отсутствии рабочей директории ViPNet SafeBoot запустится автоматическое восстановление. Следуйте указаниям программы восстановления.



Примечание. Может потребоваться подключение установочного USB-носителя.

Если не удалось восстановить рабочую директорию автоматически, выполните восстановление в ручном режиме (см. «Руководство по установке» раздел «Ручное восстановление»).

Автоматическое восстановление системного времени

Если BIOS не передает управление ViPNet SafeBoot более 300 секунд, ViPNet SafeBoot сравнивает текущие дату и время с сохраненными в базе данных при последнем старте.

Если время изменилось, автоматическое восстановление времени произойдет в случаях:

- Если текущее время меньше времени последнего старта ViPNet SafeBoot, сохраненного в базе данных.
- Если текущее время больше или равно 03:14:07 19.01.2038.

Если при загрузке BIOS появляется ошибка, см. [Не загружается BIOS](#).

Подтвердите изменение времени. Вам потребуются права администратора с аутентификацией по паролю. Если такой учётной записи в системе нет, [восстановите пароль администратора с помощью диска восстановления](#).

13

Возможные неполадки

Система заблокирована	119
Пользователь заблокирован	121
Не загружается BIOS	123

Система заблокирована

К блокированию системы может привести:

- Нарушение целостности операционной системы или объектов, поставленных на контроль.
- Нарушение целостности состава аппаратных средств, поставленных на контроль.
- Переполнение журнала событий.

Нарушена целостность операционной системы или объектов, поставленных на контроль

Возможная причина

Обнаружено повреждение или несанкционированная замена поставленных на контроль объектов.

Решение

Устраните нарушения в поставленных на контроль объектах.

Если изменения правомерны, снимите и вновь [поставьте компоненты на контроль](#).

Нарушена целостность состава аппаратных средств, поставленных на контроль

Возможная причина

К компьютеру подключено или отключено PCI-устройство при включенной в ViPNet SafeBoot опции контроля аппаратных средств.

Решение

Проверьте состав подключенных аппаратных средств, отключите неправомерно подключенное устройство или подключите необходимое.

Если PCI-устройство было подключено или отключено правомерно, пересчитайте контрольные суммы или отключите [Контроль конфигурационного пространства PCI](#).

Журнал событий переполнен

Возможная причина

Несвоевременная выгрузка журнала, установка детального режима ведения журнала.

Решение

Экспортируйте журнал событий или [измените режим ведения журнала](#) на внутренний, циклический.

Журнал событий поврежден

Возможная причина

Эксплуатация незарегистрированной уязвимости оборудования, которая привела к сбою.

Решение

Чтобы восстановить работоспособность системы, выгрузите журнал событий и базу данных. Для этого подключите диск восстановления и нажмите **Enter**.

После экспорта журнала и его резервной копии в ViPNet SafeBoot будет создан новый журнал, а в экспортированном журнале администратор сможет проанализировать события, которые привели к нарушению целостности.

Пользователь заблокирован

Основные причины блокировки пользователя:

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

Превышено допустимое количество неудачных попыток аутентификации

Возможная причина

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

Решение

Войдите в ViPNet SafeBoot с учетной записью администратора. В [управлении учётными записями пользователей](#) измените пароль или способ аутентификации заблокированного пользователя.

Время действия пароля пользователя истекло

Возможная причина

В учётной записи пользователя установлено ограничение срока действия пароля.

Решение

[Продлите срок действия пароля.](#)

Сертификат пользователя просрочен или отозван

Возможная причина

Срок действия сертификата на электронном идентификаторе истек или сертификат попал в список отозванных.

Решение

[Проверьте статус сертификата.](#)

Не загружается BIOS

В случае возникновения ошибки в BIOS или нештатного изменения времени может остановиться загрузка BIOS. Появится сообщение о необходимости нажатия определенной клавиши или комбинации (для разных версий BIOS может отличаться). При этом ViPNet SafeBoot перехватывает нажатия клавиш и запрещает вход в BIOS Setup, система перезагружается.

Решение

- 1 Дождитесь сообщения от ViPNet SafeBoot «Время ожидания истекло. Нажмите требуемую клавишу для продолжения».

Сообщение появится через 5 минут после начала загрузки платформы.

- 2 Нажмите клавишу, например Del или F2 (для разных версий BIOS может отличаться).

Устройство перезагрузится и работа будет восстановлена.

Если неполадку устранить не удалось, администратору требуется временно отключить ViPNet SafeBoot и настроить BIOS.



События, регистрируемые в ViPNet SafeBoot

Таблица 2. События

Код в журнале (hex)	Тип события	Текст сообщения
0002	детальный	Версия продукта
0003	информация	Система перезагружена
0004	информация	Система выключена
0005	ошибка	Вход в режим настроек BIOS заблокирован
0006	ошибка	Неверное системное время
0007	информация	Измененное системное время подтверждено администратором
0008	ошибка	Критическая ошибка
0009	информация	Первичная БД конфигурации импортирована
000A	информация	Режим ограниченного функционирования активирован
000B	ошибка	Режим ограниченного функционирования заблокирован
000C	ошибка	Ошибка при импорте первичной БД конфигурации
0010	детальный	Модуль верифицирован
0011	детальный	Модуль выгружен

Код в журнале (hex)	Тип события	Текст сообщения
0012	ошибка	Ошибка выгрузки модуля
0013	детальный	Модуль загружен с диска и верифицирован
0014	ошибка	Ошибка загрузки модуля с диска и/или его верификации
0015	ошибка	Ошибка формата модуля
0016	ошибка	Неверная подпись модуля
0017	детальный	Модуль загружен из BIOS и верифицирован
0018	ошибка	Загрузка модуля заблокирована
0019	ошибка	Модуль не загружен (замкнутое исполняемое окружение)
0021	ошибка	Ошибка инициализации модуля
0030	ошибка	Рабочая директория не найдена
0031	информация	Рабочая директория инициализирована
0032	ошибка	Ошибка восстановления рабочей директории
0033	информация	Рабочая директория восстановлена
0034	ошибка	Раздел с рабочей директорией не найден
0035	ошибка	Рабочая директория повреждена
0036	ошибка	Модули в рабочей директории повреждены или не найдены
0040	информация	Автоматический вход в систему
0041	информация	Система выключена: истекло время сессии аутентификации
0042	информация	Система выключена: превышено количество попыток аутентификации за сессию аутентификации
0043	информация	Система выключена: превышено количество допустимых неверных попыток аутентификации
0044	информация	Превышено количество допустимых неверных попыток аутентификации: загрузка ОС заблокирована
0045	информация	Счетчик допустимых неверных попыток аутентификации сброшен: загрузка ОС разрешена
0046	ошибка	Пользователь не существует
0047	ошибка	Попытка аутентификации в неинициализированной/заблокированной системе

Код в журнале (hex)	Тип события	Текст сообщения
		(разрешен вход только администратору)
0048	ошибка	Неверный пароль пользователя
0049	ошибка	Пароль пользователя заблокирован
004A	ошибка	Срок действия пароля пользователя истек
004B	ошибка	Неверный PIN эл.идентификатора пользователя
004C	ошибка	Эл.идентификатор пользователя не подключен
004D	ошибка	Сертификат пользователя не найден
004E	ошибка	Ошибка протокола аутентификации на эл.идентификаторе
004F	ошибка	Корневой сертификат не установлен
0050	ошибка	Ошибка верификации сертификата пользователя
0051	ошибка	Неверное имя или пароль пользователя LDAP
0052	ошибка	Пользователь LDAP не включен в белый список
0053	информация	Администратор аутентифицирован
0054	информация	Аудитор аутентифицирован
0055	информация	Пользователь аутентифицирован
0056	информация	Пользователь LDAP аутентифицирован
0057	информация	Пользователь LDAP аутентифицирован (из кэша)
0058	ошибка	Попытка аутентификации заблокированным пользователем
0059	ошибка	«PIN эл.идентификатора пользователя заблокирован»
005A	ошибка	Превышено количество допустимых неверных попыток аутентификации для пользователей LDAP
005B	информация	Счетчик допустимых неверных попыток аутентификации для пользователей LDAP сброшен
005C	ошибка	Код на эл.идентификаторе пользователя заблокирован
005D	ошибка	Срок действия кода на эл.идентификаторе пользователя истек
005E	ошибка	Аутентификация пользователя заблокирована по расписанию доступа
005F	ошибка	Найдено несколько пользователей для аутентификации на эл.идентификаторе: неинтерактивная аутентификация недоступна

Код в журнале (hex)	Тип события	Текст сообщения
0080	ошибка детальный	Нарушение БД конфигурации
0081	детальный	Неподдерживаемая версия БД конфигурации
0082	информация	Изменен режим ведения БД конфигурации
0083	информация ошибка	БД конфигурации пересоздана
0084	ошибка	БД конфигурации переполнена
0086	ошибка	Нарушение распределенной БД конфигурации
0092	информация	Журнал заполнен и заблокирован
0093	ошибка	Журнал пересоздан
0094	информация	Журнал экспортирован
0095	ошибка	Ошибка при экспорте журнала
00A0	информация	Профиль загрузки по умолчанию должен быть настроен
00A1	информация	Режим загрузки ОС изменен
00A2	детальный	Изменено устройство загрузки (legacy)
00A3	информация	Раздел ESP изменен
00A4	информация	EFI-загрузчик изменен
00A5	информация	Использование параметров загрузки BIOS включено
00A6	информация	Использование параметров загрузки BIOS выключено
00A7	информация	Изменено устройство сетевой загрузки
00A8	информация	Изменен загрузчик сетевой ОС
00B0	информация	Параметры КЦ настроены автоматически
00B2	информация	Раздел поставлен на КЦ
00B3	информация	Раздел снят с КЦ
00B4	информация	Элемент поставлен на КЦ
00B5	информация	Элемент снят с КЦ
00B6	информация	Компонент поставлен на КЦ
00B7	информация	Компонент снят с КЦ
00B8	информация	Изменен диск для контроля загрузочных секторов

Код в журнале (hex)	Тип события	Текст сообщения
00B9	информация	Контроль журнала транзакций ФС включен
00BA	информация	Контроль журнала транзакций ФС выключен
00BB	информация	Режим обучения КЦ включен
00BC	информация	Режим обучения КЦ выключен
00BD	информация	Режим хранения эталонов КЦ изменен
00BE	информация	Эталон КЦ компонента системы перерассчитан
00BF	информация	Эталон КЦ компонента импортирован
00C0	детальный	Неверный формат подписи
00C1	ошибка	Неверная подпись
00C2	информация	Эталон КЦ компонента сгенерирован автоматически
00C3	ошибка	Ошибка обработки компонентов загрузки ОС
00C4	ошибка	Ошибка при импорте эталонов КЦ
00C5	информация	Режим обучения КЦ выключен автоматически
00C6	информация	Пароль диска LUKS изменен
00C7	информация	Пароль диска LUKS удален
00C8	информация	Диск LUKS смонтирован
00F0	детальный	Целостность элемента заверена
00F1	ошибка	Целостность элемента нарушена
00F2	детальный ошибка	Элемент не найден
00F3	ошибка	Элемент снят с КЦ (режим обучения)
00F4	ошибка	Незарегистрированный элемент
00F5	детальный	Целостность компонента заверена
00F6	детальный	Целостность компонента нарушена
00F7	ошибка	Эталон КЦ компонента не найден
00F8	ошибка	Ошибка при верификации подписи эталонов компонента
00F9	информация	Целостность компонентов системы заверена
00FA	информация	Незарегистрированный элемент снят с КЦ (режим обучения)

Код в журнале (hex)	Тип события	Текст сообщения
00FB	ошибка	Эталоны КЦ компонента не соответствуют БД конфигурации
00FC	информация	Эталоны КЦ компонента перерассчитаны
00FD	ошибка	Незарегистрированный элемент поставлен на КЦ (режим обучения)
00FE	ошибка	Целостность компонентов системы нарушена
0100	информация	Журнал транзакций ФС пуст
0101	информация	Журнал транзакций ФС не пуст
0110	информация	Добавлен пользователь
0111	информация	Пользователь удален
0112	информация	Изменен тип аутентификации пользователя
0113	информация	Пароль пользователя изменен
0114	информация	Настройки пароля пользователя изменены
0115	информация	Пароль пользователя изменен администратором
0116	информация	Эл.идентификатор пользователя инициализирован
0117	информация	Изменен PIN эл.идентификатора пользователя
0118	информация	Изменен эл.идентификатор пользователя
0119	информация	Изменен сертификат пользователя
011A	информация	Пользователь заблокирован
011B	информация	Пользователь разблокирован
011C	информация	Включен Single Sign-On для пользователя
011D	информация	Выключен Single Sign-On для пользователя
011E	информация	Код на эл.идентификаторе пользователя изменен
011F	информация	Настройки кода на эл.идентификаторе пользователя изменены
0120	информация	Код на эл.идентификаторе пользователя изменен администратором
0121	информация	Расписание доступа пользователя изменено
0122	информация	Расписание доступа пользователя сброшено
0123	информация	Профиль загрузки пользователя изменен
0124	информация	Профиль загрузки пользователя сброшен

Код в журнале (hex)	Тип события	Текст сообщения
0125	информация	Неинтерактивная аутентификация пользователя разрешена
0126	информация	Неинтерактивная аутентификация пользователя запрещена
0130	информация	Изменен режим журналирования
0131	информация	Изменен уровень журналирования
0132	информация	Журналирование по syslog включено
0133	информация	Журналирование по syslog выключено
0134	информация	Настройки syslog изменены
0135	информация	Сервер syslog недоступен
0140	информация	Корневой сертификат установлен
0141	информация	Корневой сертификат удален
0142	информация	CRL установлен/обновлен
0143	информация	CRL удален
0144	ошибка	Корневой сертификат уже установлен
0145	ошибка	Корневой сертификат просрочен
0146	ошибка	CRL просрочен
0147	ошибка	Установлено максимальное количество корневых сертификатов
0148	ошибка	Сертификат не является корневым сертификатом
0149	ошибка	CRL не соответствует корневому сертификату
014A	информация	Корневой сертификат экспортирован
014B	ошибка	Ошибка при экспорте корневого сертификата
014C	информация	CRL экспортирован
014D	ошибка	Ошибка при экспорте CRL
0150	информация	Вход в режим настроек BIOS разрешен
0151	информация	Вход в режим настроек BIOS запрещен
0152	информация	Защита BIOS включена
0153	информация	Защита BIOS выключена
0154	информация	Защита BIOS после S3 включена
0155	информация	Защита BIOS после S3 выключена

Код в журнале (hex)	Тип события	Текст сообщения
0156	информация	БД конфигурации экспортирована
0157	ошибка	Ошибка при экспорте БД конфигурации
0158	информация	БД конфигурации импортирована
0159	ошибка	Ошибка при импорте БД конфигурации
015A	информация	Ограничение сессии аутентификации включено
015B	информация	Ограничение сессии аутентификации выключено
015C	информация	Время сессии аутентификации изменено
015D	информация	Автоматический вход в систему разрешен
015E	информация	Автоматический вход в систему запрещен
015F	информация	Время до автоматического входа в систему изменено
0160	информация	Защита от чтения BIOS включена
0161	информация	Защита от чтения BIOS выключена
0162	информация	Эмуляция NVRAM включена
0163	информация	Эмуляция NVRAM выключена
0164	информация	Контроль программных SMI включен
0165	информация	Контроль программных SMI выключен
0166	информация	Блокировка ACPI WPBT включена
0167	информация	Блокировка ACPI WPBT выключена
0168	информация	Защита дисков от записи включена
0169	информация	Защита дисков от записи выключена
016A	информация	Блокировка встроенных средств обновления BIOS включена
016B	информация	Блокировка встроенных средств обновления BIOS выключена
016C	информация	Защита системных таблиц UEFI включена
016D	информация	Защита системных таблиц UEFI выключена
016E	информация	Фильтрация передачи управления включена
016F	информация	Фильтрация передачи управления выключена
0170	детальный	Ошибка выставления защиты BIOS
0171	детальный	Информация о защите BIOS

Код в журнале (hex)	Тип события	Текст сообщения
0172	детальный	Защита BIOS установлена
0173	детальный	Ошибка выставления защиты BIOS после S3
0174	детальный	Информация о защите BIOS после S3
0175	детальный	Защита BIOS после S3 установлена
0176	детальный	Защита BIOS заблокирована
0181	детальный	Ошибка при работе с устройствами загрузки (legacy)
0182	ошибка	Управление возвращено от загрузчика ОС
0183	информация	Управление передано доверенной ОС
0184	информация	Управление передано недоверенной ОС
0185	информация	Управление передано Shell
0186	информация	Управление возвращено от Shell
0190	ошибка	Найдено несколько разделов ESP
0191	ошибка	Shell из пакета обновления не найден
0192	ошибка	Ошибка верификации пакета обновления
0193	ошибка	Неверная версия пакета обновления
0195	информация	Установка обновления
0196	детальный	Обновление установлено
0197	информация	Ошибка при установке обновления
0198	ошибка	Пакет обновления не найден
0199	ошибка	Найдено несколько пакетов обновлений
01B0	информация	Настройки сети изменены
01B1	информация	Настройки LDAP изменены
01B2	детальный	Протокол конфигурирования сети:
01B3	детальный	Статистика ping:
01B4	ошибка	Включение сетевого стека не поддерживается
01B5	ошибка	Сервер LDAP недоступен
01B6	ошибка	Корневой сертификат сервера LDAP не установлен
01B7	информация	Сетевой стек включен
01B8	информация	Сетевой стек выключен
01D0	информация	Белый список пользователей LDAP импортирован

Код в журнале (hex)	Тип события	Текст сообщения
01D1	информация	Белый список пользователей LDAP удален
01E0	детальный	Ошибка данных кода на эл.идентификаторе
01E1	ошибка	Код на эл.идентификаторе не найден
01E2	ошибка	Неверный код на эл.идентификаторе
01E3	ошибка	Неподдерживаемый формат кода на эл.идентификаторе
01F0	ошибка	Неверные данные диска восстановления
01F1	информация	Диск восстановления подготовлен
01F2	информация	Диск восстановления импортирован
01F3	информация	Первичный администратор восстановлен
01F4	ошибка	Неверные данные восстановления
0202	информация	Свободное место в NVRAM распределено
0213	ошибка	Продукт выключен
0214	информация	Продукт работает в демо-режиме
0215	ошибка	Демо-период использования продукта завершен
0220	информация	Серийный номер изменен
0221	информация	Запрос на регистрацию создан
0222	информация	Код регистрации изменен
0224	информация детальный	Идентификатор устройства сгенерирован
0226	ошибка	Неверный код регистрации
0227	ошибка	Код регистрации просрочен
0228	ошибка	Неверный формат серийного номера
0229	ошибка	Несовместимый серийный номер
022A	ошибка	Серийный номер не найден на диске
022B	ошибка	Код регистрации не найден на диске
022C	ошибка	Код регистрации не установлен
0238	информация	Продукт переведен в состояние 'не зарегистрирован'
0240	информация	Удаленное управление включено
0241	информация	Удаленное управление выключено

Код в журнале (hex)	Тип события	Текст сообщения
0242	ошибка	Ошибка верификации запроса управления
0243	информация	БД конфигурации импортирована в режиме управления
0244	информация	Эталоны импортированы в режиме управления
0245	детальный	Журнал и БД конфигурации подготовлены для агента управления
0246	информация	Корневые сертификаты и CRL импортированы в режиме управления
0247	ошибка	Ошибка обработки запроса управления
0248	информация	Установка обновления в режиме управления
0260	информация	Сертификат КЦ данных изменен
0261	информация	Сертификат КЦ данных сброшен
0262	информация	Сертификат КЦ запросов управления изменен
0263	информация	Сертификат КЦ запросов управления сброшен
0264	информация	Ключ защиты данных изменен
0265	информация	Ключ защиты данных сброшен
0280	информация	Программное SMI заблокировано
0290	информация	ACPI-таблица заблокирована
02A0	информация	Запись на диск заблокирована
02B0	ошибка	Обновление BIOS заблокировано
02C0	ошибка	Целостность runtime-модуля нарушена
02C1	детальный	КЦ runtime-модулей включен
02C2	детальный	КЦ runtime-модулей выключен
02C3	информация	Предотвращена попытка перехвата сервиса UEFI
02C4	ошибка	Попытка передачи управления исполняемому модулю заблокирована
02D0	ошибка	Целостность данных протокола нарушена
0300	информация	ПДСЧ инициализирован с БюДСЧ
0301	информация	ПДСЧ инициализирован с внешней гаммы
0302	ошибка	Инициализация ПДСЧ отменена
0310	ошибка	Ошибка тестирования криптографической подсистемы

Код в журнале (hex)	Тип события	Текст сообщения
0320	информация	Механизм блокировки PCI Option ROM включен
0321	информация	Механизм блокировки PCI Option ROM выключен
0322	информация	Устройство добавлено в список устройств, для которых разрешена загрузка модулей из PCI Option ROM
0323	информация	Устройство удалено из списка устройств, для которых разрешена загрузка модулей из PCI Option ROM
0324	информация	Подключенные устройства добавлены в список устройств, для которых разрешена загрузка модулей из PCI Option ROM
0325	информация	Заблокирована загрузка модулей из PCI Option ROM
0326	ошибка	Ошибка при блокировке загрузки модулей из PCI Option ROM
0330	информация	Бездисковый режим включен
0331	информация	Бездисковый режим выключен
0340	информация	Настройки паролей по умолчанию изменены для роли
0350	информация	Добавлен профиль загрузки
0351	информация	Профиль загрузки изменен
0352	информация	Профиль загрузки удален
0360	информация	Произведен вход в режим настроек
0361	информация	Произведен выход из режима настроек
0370	информация	Неинтерактивная аутентификация разрешена
0371	информация	Неинтерактивная аутентификация запрещена
0372	информация	Время до неинтерактивной аутентификации изменено
0380	информация	Системное время изменено
0400	информация	Блокировка клавиатуры на стадии загрузчика ОС включена
0401	информация	Блокировка клавиатуры на стадии загрузчика ОС выключена

В

Режимы контроля целостности компонентов ОС

При автоопределении компонентов для контроля целостности в зависимости от выбранного режима и ОС отличаются перечни файлов, которые ставятся на контроль.

В Windows

Фиксированные файлы для полного и базового режима:

- UEFI, раздел ESP:
 - EFI\Boot\BOOTX64.efi;
 - EFI\Microsoft\Boot\bootmgfw.efi;
 - EFI\Microsoft\Boot\bootmgr.efi;
 - EFI\Microsoft\Boot\boot.stl;
 - EFI\Microsoft\Boot\kdstub.dll;
 - EFI\Microsoft\Boot\memtest.efi;
- legacy, системный раздел:
 - bootmgr;
 - Boot\memtest.exe;
- UEFI/legacy, системный раздел:
 - Windows\system32\ntoskrnl.exe;
 - Windows\system32\ntkrnlpa.exe;

- o Windows\System32\hal.dll;
- o Windows\System32\halacpi.dll;
- o Windows\System32\halmacpi.dll;
- o Windows\System32\smss.exe;
- o Windows\System32\wininit.exe;
- o Windows\System32\services.exe;
- o Windows\System32\svchost.exe;
- o Windows\System32\winlogon.exe;
- o Windows\System32\lsass.exe;
- o Windows\System32\csrss.exe;
- o Windows\System32\Taskmgr.exe;
- o Windows\explorer.exe.

Полный режим:

- файлы из:
 - o HKLM\BCD00000000\Objects\<GUID>\Elements\<ID>\Element;
 - o HKLM\SYSTEM\ControlSet001\Services\<Name>*\ImagePath;
 - o HKLM\SYSTEM\ControlSet001\Services\<Name>\Parameters*\ServiceDll;



Примечание. На контроль ставится файл, путь которого лежит в значении реестра.

-
- зависимые динамические библиотеки для всех полученных файлов;
 - реестр:
 - o HKLM\BCD00000000\Objects\<GUID>\Elements\<ID>\Element;
 - o HKLM\SYSTEM\ControlSet001\Services\<Name>*;
 - o HKLM\SYSTEM\ControlSet001\Services\<Name>\Parameters*.



Примечание. На контроль ставится значение реестра.

Базовый режим:

- файлы из:
 - o HKLM\BCD00000000\Objects\<GUID>\Elements\<ID>\Element;



Примечание. На контроль ставится файл, путь которого лежит в значении реестра.

-
- реестр:
 - o HKLM\BCD00000000\Objects\<GUID>\Elements\<ID>\Element.



Примечание. На контроль ставится значение реестра.

В Linux

Фиксированные файлы для полного и базового режима:

UEFI, x64, раздел ESP:

- общие файлы для всех дистрибутивов (при наличии):
 - `EFI\Boot\BootX64.efi;`
 - `EFI\Boot\fbx64.efi;`
- ALT Linux:
 - `EFI\altlinux\grubx64.efi;`
- Astra Linux:
 - `EFI\astralinux\grubx64.efi;`
- Astra Linux CE:
 - `EFI\astralinuxce\grubx64.efi;`
- Astra Linux SE:
 - `EFI\astralinuxse\grubx64.efi;`
- RedOS:
 - `EFI\redos\grubx64.efi;`
 - `EFI\redos\shimx64.efi;`
 - `EFI\redos\shimx64-redos.efi;`
- Debian:
 - `EFI\debian\grubx64.efi;`
- Ubuntu:
 - `EFI\ubuntu\grubx64.efi;`
- CentOS:
 - `EFI\centos\grubx64.efi;`
- Fedora:
 - `EFI\fedora\shim.efi;`
 - `EFI\fedora\grubx64.efi;`
 - `EFI\fedora\shimx64-fedora.efi;`
 - `EFI\fedora\shimx64.efi;`
 - `EFI\fedora\gcdx64.efi;`
 - `EFI\redhat\grub.efi;`
 - `EFI\redhat\grubx64.efi;`

- OpenSUSE:
 - `EFI\opensuse\grubx64.efi;`

UEFI, aarch64, раздел ESP:

- общие файлы для всех дистрибутивов (при наличии):
 - `EFI\Boot\Bootaa64.efi;`
- ALT Linux:
 - `EFI\altlinux\grubaa64.efi;`
- RedOS:
 - `EFI\redos\grubaa64.efi;`
- Debian:
 - `EFI\debian\grubaa64.efi;`
- Ubuntu:
 - `EFI\ubuntu\grubaa64.efi;`
- CentOS:
 - `EFI\centos\grubaa64.efi;`
- Fedora:
 - `EFI\fedora\grubaa64.efi;`
- RedHat:
 - `EFI\redhat\grubaa64.efi;`
- OpenSUSE:
 - `EFI\opensuse\grubaa64.efi;`

Полный режим:

- фиксированные файлы:
 - конфигурация с 2 разделами (ESP и rootfs (физический раздел или раздел LVM));
 - `/boot/*` (включая вложенные папки);
 - `/bin/*` (включая вложенные папки);
 - `/sbin/*` (включая вложенные папки);
 - `/usr/bin/*` (включая вложенные папки);
 - `/usr/sbin/*` (включая вложенные папки);
 - `/etc/*` (включая вложенные папки);
 - конфигурация с 3 разделами (ESP, boot, rootfs (физический раздел или раздел LVM));
 - `/boot/*` (включая вложенные папки).

Базовый режим:

- фиксированные файлы:

- конфигурация с 2 разделами (ESP и rootfs (физический раздел или раздел LVM)):
 - /boot/* (включая вложенные папки);
 - /sbin/* (включая вложенные папки);
 - /usr/sbin/* (включая вложенные папки);
- конфигурация с 3 разделами (ESP, boot, rootfs (физический раздел или раздел LVM)):
 - /boot/* (включая вложенные папки).



История версий

В этом приложении описаны основные изменения в предыдущих версиях ViPNet SafeBoot.

Что нового в версии 3.2.0

Новые возможности ViPNet SafeBoot 3 версии 3.2.0 по сравнению с ViPNet SafeBoot 3 версии 3.0.3.

- **Новое меню установщика ViPNet SafeBoot**

Теперь у установщика ViPNet SafeBoot появился более удобный псевдографический интерфейс. Подробнее см. в разделе [Включение с помощью программы установки ViPNet SafeBoot](#) и в документе «Руководство по установке».

- **Возможность выбирать только необходимые дополнительные модули ViPNet SafeBoot**

Теперь перед установкой или обновлением ViPNet SafeBoot вы можете выбрать, какие дополнительные модули установить или удалить. Подробнее см. в документе «Руководство по установке».

- **Отображение регистрационного номера ViPNet SafeBoot (для учета экземпляров ViPNet SafeBoot) в лицензионном соглашении ViPNet SafeBoot исполнение 1**

- **Профили загрузки ОС**

Теперь вы можете создать несколько разных профилей загрузки ОС и назначить их разным пользователям. Подробнее см. в разделе [Настройка профилей загрузки ОС](#).

- **Вы можете настраивать контроль целостности для каждого профиля загрузки ОС отдельно**

Подробнее см. в разделе [Контроль компонентов ОС](#).

- **Поддержка новых электронных идентификаторов: JaCarta-2 SE и JaCarta PRO**

- **Возможность автоматической аутентификации по электронному идентификатору**

Теперь вы можете назначить пользователям автоматическую аутентификацию по электронному идентификатору, без ввода имени пользователя и ПИНа идентификатора. Подробнее см. в разделах [Добавление пользователя с аутентификацией по электронному идентификатору](#) и [Параметры аутентификации](#).

- **Бездисковый режим работы ViPNet SafeBoot**

Теперь вы можете использовать ViPNet SafeBoot на бездисковых устройствах. Подробнее см. в разделе [Бездисковый режим работы](#). Как установить ViPNet SafeBoot в бездисковом режиме см. в документе «Руководство по установке» в разделе «Установка».

- **Возможность при постановке на контроль целостности выбрать режим автоопределения компонентов ОС**

Теперь вы можете автоматически поставить на контроль целостности список файлов, зависящий от ОС и выбранного режима автоопределения компонентов. Подробнее см. в разделе [Автоопределение компонентов ОС](#).

- **Новые настройки контроля целостности аппаратных компонентов:**

- **Контроль целостности дисков**
- **Контроль целостности системных таблиц EFI**
- **Возможность поставить на контроль целостности сразу все элементы аппаратных компонентов**
- **Дополнительные возможности контроля целостности:**
 - При постановке на контроль целостности загрузочных секторов теперь контролируется и целостность таблиц GPT
 - При постановке на контроль целостности переменных NVRAM введены диапазоны, которые позволяют снимать с контроля целостности часть переменной

Подробнее см. в разделе [Контроль аппаратных компонентов](#).

- **Доступ к содержимому томов LVM**

Теперь вы можете работать с логическими томами LVM: контролировать целостность разделов и использовать их для загрузки ОС.

- **Контроль целостности зашифрованных дисков LUKS**

Теперь вы можете смонтировать зашифрованный диск LUKS и поставить на контроль целостности файлы на нем.

Подробнее см. в разделе [Контроль зашифрованных дисков LUKS](#).

- **Новые настройки контроля целостности компонентов ОС:**

- **Возможность просмотра статистики по эталонам контроля целостности**

Теперь вы можете просмотреть обобщенную информацию по каждому списку эталонов, включающую общее количество элементов в списке, размер списка эталонов и время его последнего изменения.
- **Возможность рекурсивной постановки на контроль целостности папок файловых систем и реестра Windows**

Подробнее см. в разделе [Контроль компонентов ОС](#).

- **Отключение контроля целостности в текущем сеансе загрузки ОС**

Теперь вы можете отключить контроль целостности в случае проведения работ, которые могут повлиять на контроль целостности. Подробнее см. в разделе [Отключение контроля целостности](#).

- **Новые механизмы защиты ViPNet SafeBoot:**

- Защита системных таблиц UEFI
- Фильтрация передачи управления стороннему коду
- Фильтрация доступа к NVRAM-переменным
- Блокировка клавиатуры на стадии загрузчика ОС

Подробнее см. в разделе [Защита](#).

- **Расписание доступа пользователей в ОС**

Теперь вы можете для каждого пользователя выбрать время, когда ему разрешен доступ в ОС. Подробнее см. в разделе [Настройка графика доступа](#).

- **Политика паролей для групп пользователей**

Теперь вы можете для каждой роли назначить свою политику паролей. Подробнее см. в разделе [Настройка политики паролей](#).

- **Изменение системных даты и времени в настройках ViPNet SafeBoot**

Теперь вы можете изменять системное время из интерфейса ViPNet SafeBoot, не заходя в BIOS. Подробнее см. в разделе [Изменение даты и времени](#).

- **Автовосстановление системного времени при нештатном изменении времени**

Теперь при обнаружении некорректного значения времени оно будет автоматически восстановлено из базы данных ViPNet SafeBoot. Подробнее см. в разделе [Автоматическое восстановление системного времени](#).

- **Вычисление и отображение контрольных сумм обновления ПО**

Теперь вы можете просмотреть контрольные суммы найденного пакета обновления и сравнить их с контрольными суммами, указанными в формуляре. Подробнее см. в разделе [Обновление](#).

- **Настройка фильтра журнала событий**

Подробнее см. в разделе [Настройка фильтра журнала событий](#).

- **Возможность отправлять CEF-сообщения по протоколу syslog**

Теперь вы можете отправлять оповещения о событиях в режиме реального времени. Подробнее см. в разделе [Отправка событий журнала по протоколу syslog](#).

- **Дополнительное журналирование:**

- Регистрация всех подключенных электронных идентификаторов при ошибке аутентификации

- Регистрация импорта базы данных и всех изменений в ней
- Регистрация попытки доступа в BIOS Setup с указанием клавиши, по которой была попытка входа

Что нового в версии 3.0.3

В разделе приведены новые возможности ViPNet SafeBoot 3 версии 3.0.3 по сравнению с ViPNet SafeBoot версии 3.0.1.

- Теперь повторная инициализация ПДСЧ проводится по новым правилам
Подробнее см. в разделе [Инициализация датчика случайных чисел](#).
- Реализована возможность экспорта базы данных и журнала событий на диск восстановления при повреждении
Подробнее см. в разделе [Журнал событий поврежден](#).
- Реализован режим Single Sign-On для исполнения 1 в режиме передачи идентификационной информации
Подробнее см. в разделе [Учетные записи пользователей](#).
- Реализована функция проверки выделяемой динамической памяти и исполняемой памяти модулей
- Добавлена блокировка протокола Firmware management protocol как протокола обновления BIOS

Что нового в версии 3.0.1

В разделе приведены новые возможности ViPNet SafeBoot 3 версии 3.0.1 по сравнению с ViPNet SafeBoot версии 2.1.2.

- Реализована поддержка платформ с процессорами «Байкал-М» (архитектура aarch64).
- Реализована возможность использования ViPNet SafeBoot в одном из двух исполнений в зависимости от требуемой функциональности:
 - исполнение 1 — обеспечение защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну;
 - исполнение 2 — обеспечение защиты информации, содержащей сведения, составляющие государственную тайну (до степени секретности «совершенно секретно»). Дополнительно включены модули, обеспечивающие возможность удаленного управления, загрузки по сети, конфигурирования сети, аутентификации по LDAP, использования режима аутентификации Single Sign-On.
- Реализована возможность блокировки встроенных средств обновления BIOS.
- Реализована возможность контроля целостности и загрузки ОС по сети (по PXE и Http Boot).

- Реализован контроль целостности кода продукта во время исполнения ОС (после завершения основной фазы работы продукта).
- Реализован контроль целостности структур данных протоколов (программных интерфейсов взаимодействия подсистем продукта).
- Реализован механизм блокировки выполнения PCI Option ROM.
- Реализована поддержка считывателя HID Omnikey 5422.
- Реализована поддержка LDAP-аутентификации на сервере Astra ALD Pro.
- Реализована поддержка Single Sign-On для пользователей LDAP.
- Реализована инициализация ПДСЧ (с БиодСЧ и внешней гаммы).
- Реализована возможность генерации паролей с помощью ПДСЧ. В ViPNet SafeBoot исполнение 1 доступно создание паролей только с помощью ПДСЧ.
- Реализовано разделение областей для хранения событий журнала (для отдельного хранения событий контроля целостности программной среды).
- Реализована поддержка создания замкнутого исполняемого окружения.
- Реализовано освобождение и затирание используемой динамической памяти при завершении основной фазы работы продукта.
- Реализовано автоматическое восстановление рабочей директории при повреждении или удалении.

Исправление ошибок

Устранены ошибки и уязвимости, выявленные в процессе эксплуатации предыдущих версий продукта.



Термины и сокращения

Exit Boot Services

Событие, вызов, которого завершает работу служб загрузки в UEFI. Данное событие сигнализирует загрузчику ОС готовность платформы для передачи управления под его контроль.

GPT (GUID Partition Table)

Стандарт формата размещения структуры разделов на физическом жестком диске.

LDAP (Lightweight Directory Access Protocol)

Упрощённый протокол доступа к службе каталогов стандарта X.500. Используется для доступа к AD, AD LDS.

LUKS (Linux Unified Key Setup)

Спецификация формата шифрования дисков. Диски (HDD, SSD) зашифровываются в одиночном или групповом (LVM) режиме.

LVM (Logical Volume Management)

Менеджер логических томов, который позволяет использовать разные области на одном или нескольких жестких дисках как один логический том.

NVRAM (Non Volatile Random Access Memory)

Энергонезависимая память, которая сохраняет информацию при отключении питания компонента.

Single Sign-On

Технология единого входа, при использовании которой пользователь переходит из одной системы в другую, не связанную с первой системой, без повторной аутентификации.

SMI (System Management Interrupt)

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

SMM (System Management Mode)

В этом режиме останавливается нормальная работа процессора (в том числе работа ОС и обработка всех других прерываний) и управление передается специальным программным обработчикам BIOS (обработчикам SMI), работающим с наивысшим приоритетом.

UEFI (Unified Extensible Firmware Interface)

Унифицированный расширяемый интерфейс между операционной системой и программами, управляющими оборудованием.

Основное назначение: правильно определить оборудование при включении системы и передать управление загрузчику или непосредственно ядру операционной системы.

Администратор

Обладает правом загрузки операционной системы, правом доступа в настройки ViPNet SafeBoot.

Аудитор

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

Аутентификация

Процесс односторонней или двусторонней (взаимной) проверки подлинности между клиентом (пользователем) и системой (сервером), например, с использованием учётных данных или сертификатов ключей проверки электронной подписи.

Ключ проверки электронной подписи (ключ проверки ЭП)

Несекретный (открытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, однозначно связанную с секретным ключом (ключом электронной подписи или закрытым ключом) и предназначенную для проверки подлинности электронной подписи.

Отличительное имя (DN)

У каждой записи каталога LDAP, включая объекты пользователей, есть уникальное отличительное имя (Distinguished Name), которое может быть представлено в текстовом виде.

Программный датчик случайных чисел (ПДСЧ)

Датчик, который преобразует инициализирующую последовательность (первичную ключевую информацию) в последовательность псевдослучайных чисел заданной длины, необходимую для выполнения криптографических операций.

Сертификат издателя

Сертификат ключа проверки электронной подписи, принадлежащий удостоверяющему центру и служащий для подписи сертификатов, издаваемых удостоверяющим центром.

Специальные символы

Любой печатный символ базовой таблицы ASCII (0-127), не являющийся цифрой и буквой латинского алфавита: | \ / ? . , < > ; " ' { } [] _ - = + () * & ? ^ % \$ # № @ ! ` ~.



Изменения в документации

В разделе перечислены изменения в документации после выпуска релиза ViPNet SafeBoot версии 3.2.1.

- 31.03.2026 — обновлен документ «Руководство администратора», разделы «Защита», «Порядок обновления информации на электронном идентификаторе», «Добавление пользователя с аутентификацией по коду на электронном идентификаторе».
- 06.03.2026 — обновлен юридический адрес АО «ИнфоТеКС» во всех документах. В документе «Руководство администратора» обновлен раздел «Регистрация». В документе «Руководство по установке» обновлены разделы «Системные требования» и «Изменение конфигурации».
- 11.08.2025 — обновлен документ «Руководство администратора». Обновлен раздел «Совместимые электронные идентификаторы».