



ViPNet SafeBoot 3

Руководство по установке

Версия продукта 3.2.1

© АО «ИнфоТеКС», 2025

ФРКЕ.00283-01 90 19

Версия продукта 3.2.1, документ обновлен 06.03.2026

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.....	4
О документе.....	4
Соглашения документа.....	4
Обратная связь.....	4
Основные сведения.....	6
Назначение	6
Системные требования	6
Установка	7
Подготовка установочного USB-носителя.....	7
Сбор информации о платформе	8
Изменение конфигурации.....	9
Дополнительные модули.....	10
Создание диска восстановления.....	11
Установка ViPNet SafeBoot.....	12
Установка пакета SSO.....	13
Режим SSO для Windows.....	13
Режим SSO для Linux.....	14
Удаление.....	15
Восстановление рабочей директории.....	16
Автоматическое восстановление.....	16
Ручное восстановление	17
Возможные неполадки и способы их устранения	18
Термины и сокращения	19

Введение

О документе

Документ предназначен для администраторов, которые устанавливают и настраивают ViPNet SafeBoot на рабочих местах пользователей. Для этого потребуется 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](#).

Основные сведения

Назначение

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). Защита действует с момента включения компьютера.

ViPNet SafeBoot контролирует целостность BIOS, защищаемых компонентов операционной системы, а также блокирует загрузку модифицированной копии операционной системы.

ViPNet SafeBoot версии 3.2.1 представлен только в исполнении 2.

Системные требования

- Процессор — x86-совместимый с поддержкой режима x86-64 (AMD64/Intel64) или ARM v8 с частотой от 500 МГц и наличием RTC.
- BIOS должен соответствовать спецификации UEFI версии 2.4, 2.5, 2.6, 2.7, 2.8, 2.9.
- Оперативная память — минимум 1 Гбайт, максимум определяется ограничениями используемой платформы.
- Свободное место в образе firmware (UEFI BIOS) для:
 - исполняемого кода (модули — DXE Firmware Volume): минимум 510 Кбайт для архитектуры x64, 1166 Кбайт для архитектуры aarch64, максимум определяется ограничениями используемой аппаратной платформы;
 - данных (журнал, база данных — NVRAM Firmware Volume): минимум 32 Кбайт, оптимально 100 Кбайт, максимум определяется ограничениями используемой платформы.
- Жесткий диск:
 - должен содержать раздел, отформатированный в системе FAT, EXT или NTFS, доступный для записи из среды UEFI;
 - объем определяется требованиями установленной ОС. Необходимое свободное место на жестком диске (с разметкой разделов MBR/GPT): минимум 50 Мбайт, оптимально 200 Мбайт, максимум определяется ограничениями используемой аппаратной платформы.



Примечание. Для установки в BIOS ([бездисковый режим работы](#)) жесткий диск не требуется.

Установка



Внимание! Устанавливайте ViPNet SafeBoot только при наличии средств восстановления, таких как программатор.

- 1 Подготовьте установочный USB-носитель.
- 2 Соберите информацию о платформе.
- 3 Выберите архив с программой установки для платформы.
- 4 Создайте конфигурацию для установки ViPNet SafeBoot.
- 5 Создайте диск восстановления.
- 6 Установите ViPNet SafeBoot.
- 7 Установите пакет SSO.



Внимание! Некорректное встраивание в платформу может привести к [повреждению](#) содержимого BIOS.

Если вы устанавливаете ViPNet SafeBoot на несколько компьютеров, подготовку USB-носителя и создание диска восстановления можно выполнить на одном компьютере с установленной Windows 8.1 или выше и криптопровайдером [ViPNet CSP](#) (технологический компьютер). Остальные шаги нужно выполнять на всех компьютерах.

Системные требования к компьютеру для установки ViPNet CSP см. в документе «ViPNet CSP. Руководство пользователя».

Подготовка установочного USB-носителя

- 1 Подключите USB-носитель.
- 2 Отформатируйте USB-носитель в файловую систему FAT32.
- 3 Распакуйте содержимое установочного архива в корневую папку USB-носителя.
- 4 Определитесь с режимом запуска ViPNet SafeBoot:
 - Режим неактивности — выберите его, если планируете начать использовать ViPNet SafeBoot 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.
 - Деморежим 2 — позволяет зарегистрировать ViPNet SafeBoot, без регистрации можно использовать 60 дней, после этого будут доступны только регистрация, настройка загрузки ОС и аутентификация только администратора.
- 5 На установочном USB-носителе в папке `itinstallcfg` создайте файл без расширения с именем (содержимое файла может быть любым):
- `disabled` — для перехода в режим неактивности;
 - `demo1` — для перехода в деморежим 1;
 - `demo2` — для перехода в деморежим 2.
- 6 Вы можете установить ViPNet SafeBoot в бездисковом режиме, если в микросхеме BIOS достаточно места — то есть ViPNet SafeBoot не будет использовать диск компьютера для размещения своих модулей и данных. Для этого в папке `itinstallcfg` создайте файл `diskless` с любым содержимым. Установить ViPNet SafeBoot в бездисковом режиме можно с любым режимом запуска.

Сбор информации о платформе

Перед установкой ViPNet SafeBoot проверьте, совместим ли ваш компьютер с ViPNet SafeBoot. Для этого запустите диагностику и отправьте в ИнфоТеКС полученную информацию о вашем компьютере:

- 1 Убедитесь, что на жестком диске компьютера есть раздел в одной из файловых систем: FAT32, NTFS или EXT 2/3/4.

Если подходящего раздела нет, создайте раздел размером не менее 100 Мбайт (рекомендуется 200 Мбайт) для ViPNet SafeBoot и отформатируйте его в FAT32.
- 2 Выключите компьютер.
- 3 Подключите установочный USB-носитель.
- 4 Включите компьютер и зайдите в BIOS.
- 5 Отключите режим быстрой загрузки (Fast Boot или аналоги).
- 6 Отключите механизмы контроля загрузки (Secure Boot или аналоги), если в настройках BIOS есть такая возможность.
- 7 В настройках BIOS выберите загрузку с установочного USB-носителя и сохраните настройки.

После перезагрузки с установочного USB-носителя запустится EFI Shell.
- 8 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.
- 9 Выберите **Run diagnostics**.

Результаты диагностики сохраняются на USB-носитель в папку `itinstalllog`.

10 Отправьте содержимое папки `itinstallllog` в [ИнфоТеКС](#).

11 Получите рекомендации по установке ViPNet SafeBoot на данную платформу.

Для сбора информации о других компьютерах можно использовать тот же USB-носитель.

Изменение конфигурации

Если у вас ограничено место на микросхеме BIOS, вы можете выбрать, какие модули устанавливать. Вы можете настроить конфигурацию ViPNet SafeBoot как при первичной установке, так и при обновлении уже установленного ViPNet SafeBoot.

ViPNet SafeBoot состоит из основных и дополнительных модулей. Основные модули устанавливаются всегда, вы не можете удалить их. Дополнительные модули вы можете включать в конфигурацию или исключать из нее.

Для изменения конфигурации ViPNet SafeBoot используются файлы с любым содержимым и [определенными именами, указывающими на группу модулей](#), которую требуется добавить в конфигурацию или исключить из неё.

Вы можете установить нужную конфигурацию двумя способами:

1 Установить только необходимые модули:

- 1.1 На установочном USB-носителе в папке `itinstallcfg` создайте папку `plugins\include`.
- 1.2 Создайте в папке `include` файлы с [именами групп модулей](#), которые устанавливаете. Содержимое файлов может быть любым.
- 1.3 Установите ViPNet SafeBoot, если устанавливаете его впервые или Обновите ViPNet SafeBoot до версии не ниже 3.2.1, если изменяете конфигурацию уже установленного ViPNet SafeBoot. Подробнее см. в документе «Руководство администратора», в разделе «Обновление».

Установятся основные модули и те группы дополнительных модулей, для которых созданы файлы в папке `include`.

2 Установить все модули, кроме определенных:

- 2.1 Перед изменением конфигурации снимите с контроля целостности компоненты и отключите функции защиты, входящие в модули, которые будут удалены.



Примечание. Убедитесь, что настройки базы данных соответствуют изменяемой функциональности.

- 2.2 На установочном USB-носителе в папке `itinstallcfg` создайте папку `plugins\exclude`.
- 2.3 Создайте в папке `exclude` файлы с [именами групп модулей](#), которые исключаете из конфигурации. Содержимое файлов может быть любым. Группу основных модулей нельзя исключить.

- 2.4 Установите **ViPNet SafeBoot**, если устанавливаете его впервые или Обновите ViPNet SafeBoot до версии не ниже 3.2.1, если изменяете конфигурацию уже установленного ViPNet SafeBoot. Подробнее см. в документе «Руководство администратора», в разделе «Обновление».

Установятся основные модули и все группы дополнительных модулей, кроме тех, для которых созданы файлы в папке `exclude`.



Примечание. Если вы создали файлы с именами модулей в обеих папках `include` и `exclude`, файлы в папке `exclude` будут проигнорированы.

Основные модули, входящие в группу core

ItCore, ItAlloc, ItStorage, ItLog, ItConfDB, ItDefender, ItRuntime, ItNvramEmu, ItBiosUpdateLock, ItIntegrMgr, ItCrypto, ItOpenssl, ItAuth, ItScAuth, ItGraph, ItSettings, ItUpdater, ItRecovery, ItOsLoader, ItConfDBEx, ItReg.

Дополнительные модули

Имя файла модуля	Функции модулей	Модули
gui	Реализация графического пользовательского интерфейса ViPNet SafeBoot	ItGuiEngine
sc	Аутентификация по токенам	ItCcidDxe; ItRutokenDxe; ItJaCartaDxe; ItGuardantIdDxe; ItEsmartDxe; ItForosDxe
ldap	Аутентификация по LDAP. Этот модуль работает только при наличии модуля конфигурирования сети <code>net</code>	ItLdap
net	Конфигурирование сети — для отправки сообщений по syslog, аутентификации по LDAP, загрузки ОС по сети	ItNetCfg
winreg	Контроль целостности реестра Windows	ItCheckHive
autoic	Автоопределение компонентов ОС для контроля целостности	ItOsBootInfo

Имя файла модуля	Функции модулей	Модули
fslog	Контроль журнала транзакций файловой системы NTFS, EXT3, EXT4	ItCheckLog
smbios	Возможность контроля SMBIOS	ItSmbios
imagefilter	Блокировка передачи управления на загрузчик в обход механизмов защиты ViPNet SafeBoot	ItImageFilter
am	Функциональность anti malware: блокируется для сторонних модулей UEFI BIOS запись на диск и создание таблиц ACPI WPBT. Контроль целостности системных таблиц UEFI и периодический контроль целостности модулей SafeBoot, исполняемых на фазе ОС	ItDiskFilter; ItDisableWpbt
rg	Контроль целостности системных таблиц UEFI и периодический контроль целостности модулей SafeBoot, исполняемых на фазе ОС	ItRuntimeGuard
swsmi	Блокирование обновления UEFI BIOS через интерфейс программных SMI с фазы ОС	ItSwSmi
pciblk	Блокирование исполнения PCI Option ROM (UEFI) внешних PCI/PCIe-устройств	ItPciOpromLock
mgmt	Поддержка удаленного управления	ItMgmt
sso	Поддержка Single Sign-On	ItSingleSignOn
luks	Доступ к томам LVM и LUKS для контроля целостности файлов на них	ItLvmDxe
netboot	Поддержка сетевой загрузки ОС	ItNetBoot
extntfs	Доступ к файлам файловой системы NTFS, EXT2, EXT3, EXT4	ExtNtfs

Создание диска восстановления

Перед установкой ViPNet SafeBoot создайте диск восстановления с уникальным ключом восстановления пароля администратора. Иначе при установке ViPNet SafeBoot будет использован общий ключ восстановления.



Внимание! При использовании общего ключа восстановления возможность отключить ViPNet SafeBoot будет у любого, обладающего общим ключом.

Диск восстановления понадобится при потере аутентификационных данных либо для временного отключения функциональности ViPNet SafeBoot. Для создания диска восстановления можно использовать установочный USB-носитель.



Примечание. Рекомендуется создать уникальный ключ восстановления до установки ViPNet SafeBoot.

При создании ключей восстановления ViPNet SafeBoot для партии компьютеров используйте технологический компьютер.

Чтобы создать уникальный ключ восстановления:

- 1 Установите на компьютере криптопровайдер [ViPNet CSP](#).
- 2 Выберите архив с утилитами для вашей операционной системы, платформы и исполнения.
- 3 Подключите установочный USB-носитель.
- 4 Распакуйте архив с утилитами.
- 5 В командной строке перейдите в папку `recovery` и выполните команду `recovery_disk_init.exe -f`.

После создания ключа появится сообщение **ViPNet SafeBoot recovery disk successfully initialized**.



Внимание! Храните USB-носитель с ключом восстановления в надежном месте.

Установка ViPNet SafeBoot

- 1 Подключите компьютер к источнику бесперебойного питания.



Внимание! Прерывание электропитания может привести к [повреждению содержимого микросхемы BIOS](#).

- 2 В настройках BIOS установите дату и время с точностью до минуты, сохраните изменения.
- 3 Подключите установочный USB-носитель.
- 4 После перезагрузки с установочного USB-носителя запустится EFI Shell.
- 5 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.
- 6 Выберите **Install**.

- 7 После появления сообщения об успешном завершении установки нажмите любую клавишу, кроме **q**.



Внимание! Не отключайте установочный USB-носитель до появления приглашения ввести имя пользователя.



Примечание. После установки в ViPNet SafeBoot будет создан профиль администратора:

- имя пользователя — Administrator;
- пароль — 12345678.

Если вы установили ViPNet SafeBoot с общим ключом восстановления, создайте диск с новым ключом (см. «Руководство администратора» раздел «Создание диска восстановления»). Общий ключ восстановления хранится на USB-носителе в файле `itrecovery.bin`.

При установке ViPNet SafeBoot из микросхемы BIOS считывается образ BIOS, на его основе создается модифицированный образ со встроенными модулями ViPNet SafeBoot. После этого модифицированный образ записывается в микросхему BIOS.

Если для встраивания всех модулей в BIOS недостаточно места, часть модулей ViPNet SafeBoot сохранится в папке `EFI\Infotecs`. Подробнее см. [Изменение конфигурации](#).



Внимание! Не удаляйте и не переименовывайте файлы и папки в `EFI\Infotecs`.

Если установка завершилась ошибкой, направьте описание ошибки, а также содержимое папки `itinstalllog` на USB-носителе, в [службу поддержки ИнфоТекС](#).

Установка пакета SSO

Чтобы пользователь выполнял аутентификацию только в ViPNet SafeBoot и аутентификация в ОС выполнялась автоматически, установите пакет [Single Sign-On \(SSO\)](#).

Это необязательный пакет, он не входит в комплект поставки. Для получения пакета обратитесь в [службу поддержки ИнфоТекС](#).

Режим SSO для Windows



Внимание!

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

- 1 Распакуйте архив `vipnet_safeboot-sso_tools-x64-r-<номер версии>.zip`, полученный в ИнфоТекС.

- 2 На каждом компьютере пользователя установите сначала `vc_redist.x64.exe`, а затем `SafeBootSSO.exe`.
- 3 Дождитесь завершения установки и перезагрузите компьютер. Single Sign-On будет готов к работе.

Если данные учетной записи в ViPNet SafeBoot и в ОС совпадают, после аутентификации в ViPNet SafeBoot пользователь автоматически входит в ОС.

Если данные учетной записи в ViPNet SafeBoot и Windows не совпадают, отобразится сообщение об ошибке. Выберите имя пользователя и пароль, используя штатные средства ОС.

Режим SSO для Linux



Внимание!

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

Для работы SSO в Linux:

- 1 Добавьте строку `auth sufficient pam_sso.so`:
 - для ОС с Gnome Display Manager — в начало конфигурационного файла `/etc/pam.d/gdm-password`;
 - для Astra Linux — в конфигурационный файл `/etc/pam.d/fly-dm` после строки `auth required pam_parsec_mac.so`.
- 2 Скопируйте файл `pam_sso.so` в папку `/lib/x86_64-linux-gnu/security`.

Особенность реализации SSO в Linux:

- После загрузки ОС выберите имя пользователя или введите его вручную, автоматического выбора нет. Произойдет вход в ViPNet SafeBoot без запроса аутентификационных данных.
- Если учетные данные SafeBoot и Linux не совпадают, после выбора пользователя запрашиваются аутентификационные данные.

Удаление



Внимание! Прерывание электропитания может привести к повреждению содержимого микросхемы BIOS.

- 1 Подключите установочный USB-носитель.
- 2 Войдите в настройки ViPNet SafeBoot:
 - 2.1 Включите компьютер.
ViPNet SafeBoot запустится автоматически.
 - 2.2 Введите имя пользователя и пароль в ViPNet SafeBoot.
 - 2.3 Нажмите клавишу **F2** для входа в настройки.
 - 2.4 Ознакомьтесь с уведомлениями и нажмите **OK**.
- 3 В ViPNet SafeBoot выберите параметры загрузки ОС:
 - 3.1 Выберите **Параметры загрузки ОС**.
 - 3.2 Нажмите **Загрузить Shell с диска**.
- 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 **Uninstall**.
- 6 После удаления ViPNet SafeBoot для завершения работы нажмите любую клавишу, кроме **q**.

Восстановление рабочей директории

Если появится сообщение об отсутствии рабочей директории ViPNet SafeBoot `EFI\Infotecs`, восстановите её. Это можно сделать в ручном или автоматическом режиме.

Автоматическое восстановление

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](#).

Ручное восстановление

- 1 Подключите установочный USB-носитель с ключом восстановления.
- 2 Временно отключите ViPNet SafeBoot:
 - 2.1 Перезагрузите компьютер.
 - 2.2 При загрузке нажмите клавиши **правый Ctrl+X**.
 - 2.3 Войдите в BIOS.
- 3 В настройках BIOS выберите загрузку EFI-типа с USB-носителя.
- 4 После перезагрузки с установочного USB-носителя запустится EFI Shell.
- 5 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.
- 6 Выберите **Recover**.
- 7 После восстановления появится сообщение со списком следующих шагов:
 - 7.1 Перезагрузите компьютер или он перезагрузится автоматически через 10 секунд.
 - 7.2 После перезагрузки ViPNet SafeBoot будет переключен на временную рабочую директорию, расположенную на установочном USB-носителе.
 - 7.3 Отключите USB-носитель и повторно перезагрузите компьютер.
 - 7.4 После перезагрузки ViPNet SafeBoot начнет работу с восстановленной рабочей директорией, расположенной на жестком диске.
- 8 Чтобы перезагрузить компьютер, нажмите любую клавишу, кроме **q**.

Возможные неполадки и способы их устранения

Повреждение содержимого микросхемы BIOS

Для восстановления оригинального образа BIOS скачайте его на сайте производителя или выгрузите программатором перед установкой ViPNet SafeBoot.

Термины и сокращения

Single Sign-On

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

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.

Доверенная загрузка

Способ загрузки компьютера аппаратно-программными средствами, предотвращающий несанкционированный доступ к конфиденциальной информации. В область действия средств, обеспечивающих доверенную загрузку, входят этапы работы компьютера от запуска микропрограммы BIOS до начала загрузки операционной системы.

Доверенная загрузка выполняется только после аутентификации личности запускающего компьютер.

Программный датчик случайных чисел (ПДСЧ)

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