Новое поколение сертифицированного программного модуля доверенной загрузки ViPNet SafeBoot 3

Кадыков Иван
Руководитель направления

infotecs

Зарождение универсальных ПМДЗ

На рынке более 95% аппаратно-программных «замков». Причины:

- «Наследие» участников рынка
- Программные замки не универсальны
- По линии ФСБ России допускается только АПМДЗ

Новая реальность

ФСБ России выпускают требования к программным и аппаратно-программным модулям доверенной загрузки

Готовность к новым вызовам

Вендоры рынка активно работают и выпускают свои версии программных замков, начинают сертификацию по линии ФСТЭК России. Стоимость аппаратных замков существенно вырастает

Начало трансформации

Пользователи получают больше информации по новым требованиям ФСБ России, начинают планировать новые проекты с использованием программных МДЗ.

2017

Появление первой версии универсального высокотехнологичного МДЗ ViPNet SafeBoot

2020

Анализ новых требований с последующей доработкой ViPNet SafeBoot

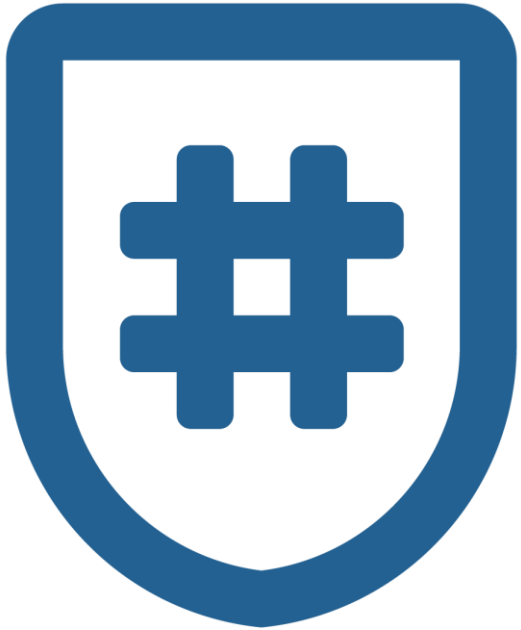
2022

Выпуск версии 3! Реализованы новые требования ФСБ России и добавлены новые механизмы защиты

2023

Получен сертификат ФСТЭК России и ФСБ России на ViPNet SafeBoot 3

ViPNet SafeBoot 3

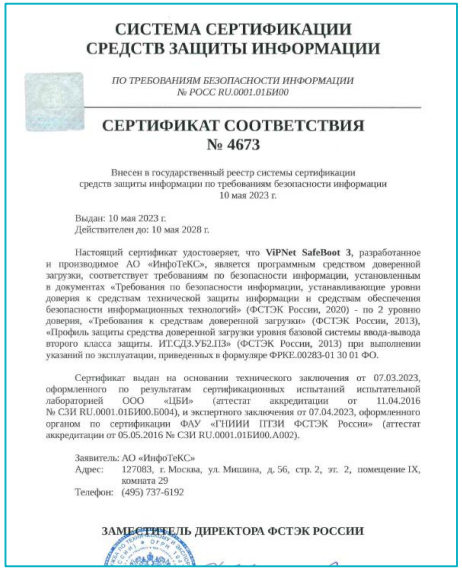


Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ), сертифицированного по требованиям ФСБ России и ФСТЭК России. Предназначен для создания точки доверия к платформе и её компонентам, а также к загружаемой операционной системе. Ключевыми задачами продукта являются разграничение доступа к платформе, защита UEFI BIOS, контроль неизменности и защита компонентов ПК, а также организация доверенной загрузки штатной операционной системы.

ViPNet SafeBoot 3

Первые кто получил два сертификата на одну версию!

- ФСТЭК России № 4673
- ФСБ России № СФ/527-4669



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4673

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 10 мая 2023 г.

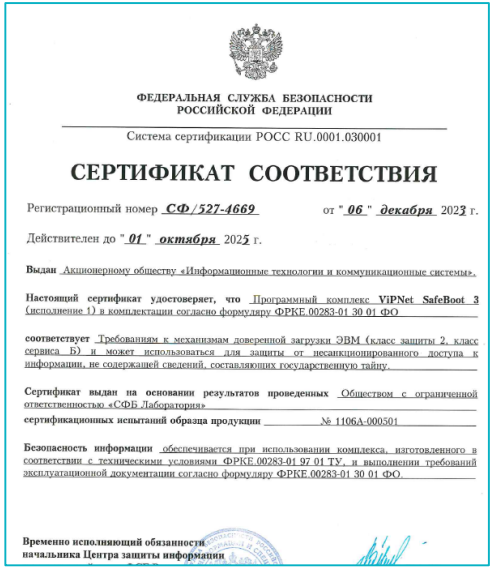
Выдан: 10 мая 2023 г.
Действителен до: 10 мая 2028 г.

Настоящий сертификат удостоверяет, что **ViPNet SafeBoot 3**, разработанное и производимое АО «ИнфоТеКС», является программным средством доверенной загрузки, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 2 уровню доверия, «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00283-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 07.03.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 07.04.2023, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/527-4669* от "*06*" *декабря* 2023 г.

Действителен до "*01*" *октября* 2025 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс **ViPNet SafeBoot 3** (исполнение 1) в комплектации согласно формуляру ФРКЕ.00283-01 30 01 ФО

соответствует Требованиям к механизмам доверенной загрузки ЭВМ (класс защиты 2, класс сервиса Б) и может использоваться для защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»
сертификационных испытаний образца продукции № 1106А-000501

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00283-01 97 01 ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00283-01 30 01 ФО.

Временно исполняющий обязанности
начальника Центра защиты информации

Несколько слов про новые требования

Новые требования

**Средства защиты информации реализующие механизмы доверенной загрузки II класса,
тип сервиса Б.**

Расшифровываем:

II класс – предназначен для защиты информации ограниченного доступа (без ГТ)

Тип сервиса Б – без возможностей удалённого управления

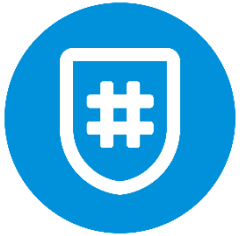
ViPNet SafeBoot – два исполнения

- **Исполнение 1.** ViPNet SafeBoot 3 – обладает двумя сертификатами ФСБ России и ФСТЭК России.

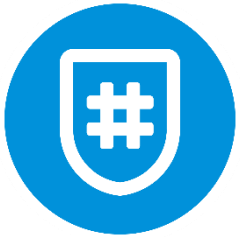
Необходим, при построении систем СКЗИ и соответствовать требованиям ГИС, ИСПДн, АСУ ТП, КИИ.

- **Исполнение 2.** ViPNet SafeBoot 3 – обладает – только сертификатом ФСТЭК России

Необходим, при построении АС только по требованиям ФСТЭК



Похожи как братья близнецы, но есть особенности

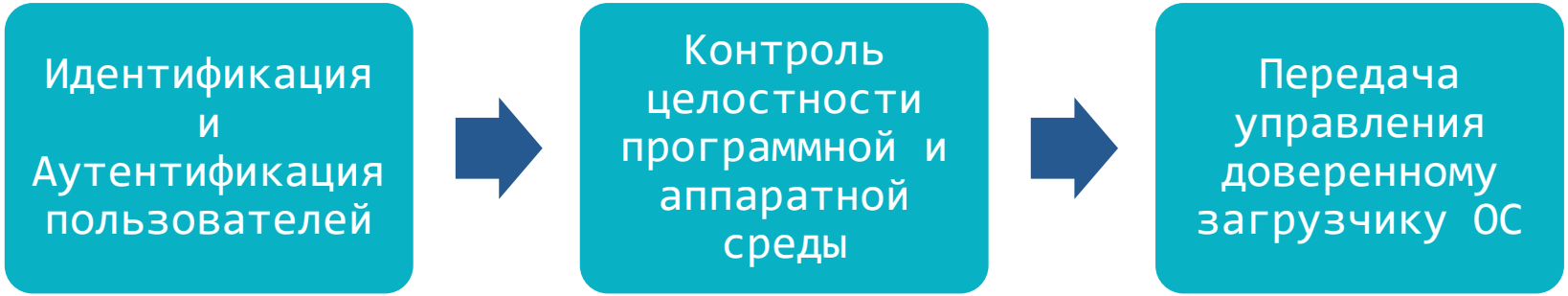


Возможности ViPNet SafeBoot 3

Переходя к возможностям – отметим!

> ViPNet SafeBoot 3 уже давно не просто модуль доверенной загрузки, а ключевой элемент доверия к платформе.

Базовые функциональные блоки «замка»



Идентификация и аутентификация

- Варианты идентификации и аутентификации:
  - Логин + пароль
  - Логин + сертификат на токене
  - Логин + сертификат на токене + пароль
  - Логин + PIN на токене
- Возможность идентификации и аутентификации на LDAP/AD (используются доменные учётные записи)
- Реализация SSO с ViPNet SafePoint и операционными системами

Контроль целостности

- Контроль компонент ОС
  - Файлы на файловых системах FAT32, NTFS, EXT2, EXT3 и EXT4
  - Реестр Windows
  - Завершённости транзакций ФС (NTFS, EXT3 и EXT4)
- Контроль аппаратных компонент платформы
  - Содержимое CMOS
  - Содержимое пространства PCI
  - Таблиц ACPI
  - SMBIOS
  - Карты распределения памяти
  - Модули UEFI
  - Загрузочные сектора

Режимы загрузки ОС

- Использование параметров загрузки BIOS
- Режим совместимости (Legacy – для «старых» платформ)
- UEFI- загрузка, передача управления загрузчику напрямую
- Загрузка ОС по сети (PXE-boot и HTTP-boot)

Дополнительные опции безопасности

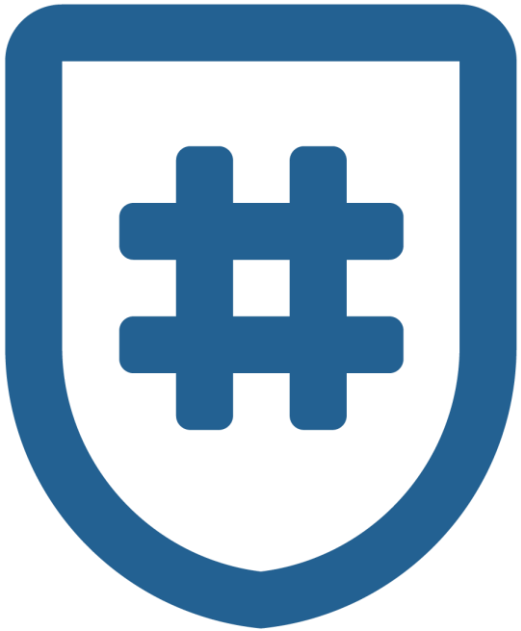
- Защита UEFI BIOS
  - Защиту BIOS от записи и чтения
  - Защита после S3 - защита при выходе из спящего режима
  - Блокировка обновлений UEFI BIOS
  - Фильтрация и контроль программных SMI
- Защита от malware
  - Блокировка ACPI WPBT
  - Защита дисков от записи
  - Блокировка UEFI Option Rom
- Эмуляция NVRAM (защита от записи и чтения EFI-переменных)

Общая схема работы

Вернёмся к исполнениям

- **Исполнение 1.**
  ViPNet SafeBoot 3 –
  обладает двумя сертификатами
  ФСБ России и в ФСТЭК России

- **Исполнение 2.**
  ViPNet SafeBoot 3 – обладает
  только сертификатом
  ФСТЭК России



Раз есть два исполнения, значит есть и отличия в возможностях

Найди 3 отличия

Исполнение 1, за счёт полученного сертификата ФСБ России и выполненных требований накладывает следующие ограничения:

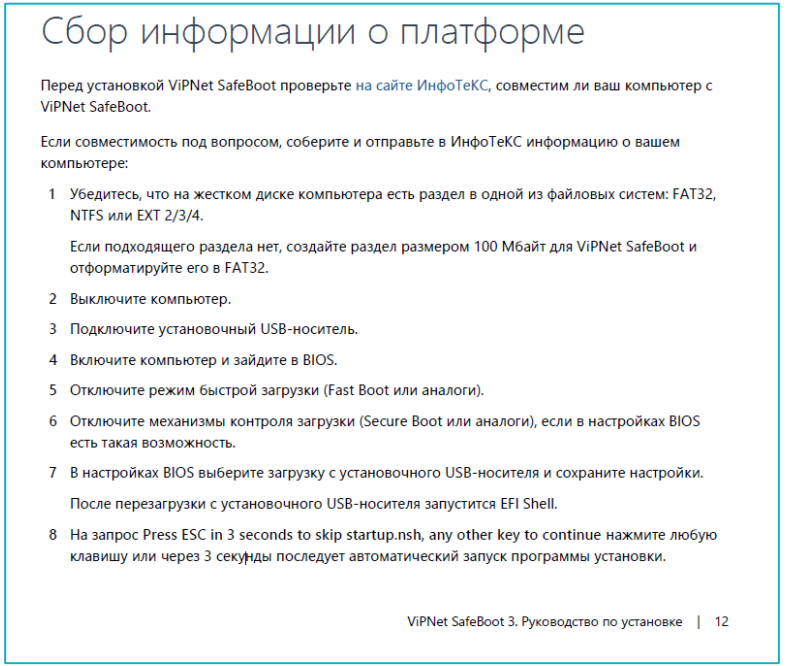
- Отсутствуют «сетевые» возможности:
  - Нет возможности загрузки ОС по сети
  - Нет возможности удалённого управления
  - Нет возможности идентификации/ аутентификации на LDAP/AD
- ViPNet SafeBoot 3 должен размещаться полностью в UEFI BIOS
- Пароль для пользователя задаётся только при помощи ПДСЧ

*Подробнее про ограничения в документации – Правила пользования и Руководство администратора

Проверка на совместимость, встраивание и ввод в эксплуатацию

Как понять – установится ли SafeBoot 3 на платформу?

1. Запросить дистрибутив ViPNet SafeBoot с документацией
2. Запустить дистрибутив в режиме диагностики для сбора логов (см. Руководство по установке)
3. Отправить в техническую поддержку собранные логи
4. Ждать вердикта
   A. Установка возможна
   B. Установка возможна, но необходимо дополнительное расширение
   C. Установка невозможна



Сбор информации о платформе

Перед установкой ViPNet SafeBoot проверьте на сайте ИнфоТеКС, совместим ли ваш компьютер с ViPNet SafeBoot.

Если совместимость под вопросом, соберите и отправьте в ИнфоТеКС 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 100 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 3 seconds to skip startup.nsh, any other key to continue нажмите любую клавишу или через 3 секунды последует автоматический запуск программы установки.

ViPNet SafeBoot 3. Руководство по установке | 12

Создание диска восстановления

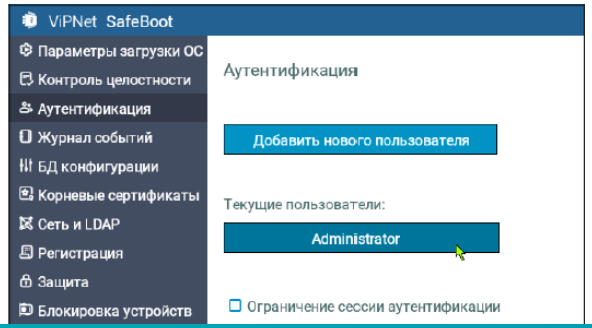
Диск восстановления может понадобиться Администратору при потере аутентификационных данных либо для временного отключения функциональности ViPNet SafeBoot (см. Временное отключение функциональности ViPNet SafeBoot на стр. 106). Процесс создания диска представляет собой создание на USB-носителе уникального ключа восстановления.

Если при установке ViPNet SafeBoot был создан диск восстановления с уникальным ключом восстановления, то повторное создание диска будет недоступно (см. «ViPNet SafeBoot. Руководство по установке»).

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

Чтобы подготовить диск восстановления пароля Администратора:

1. Войдите в режим настроек ViPNet SafeBoot (см. Вход в режим настройки ViPNet SafeBoot на стр. 58).
2. В меню режима настроек выберите Аутентификация.
3. В открывшемся окне выберите Administrator.



Не забывайте!!!

При установке необходимо сделать диск восстановления!

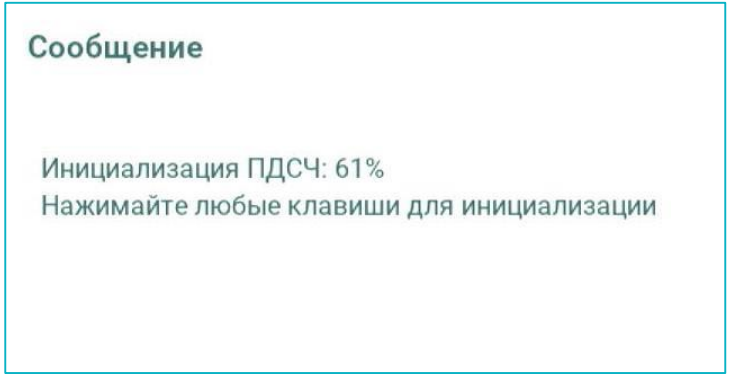
Читайте Руководство администратора стр.136

После установки, при первом включении

Вам потребуется провести инициализацию ПДСЧ (!) с использованием диска восстановления (USB-flash например)

Инициализация ПДСЧ происходит при помощи клавиатуры (БиоДСЧ) или с использованием заранее подготовленной последовательности случайных чисел

«Последовательность» надо подготовить заранее на компьютере, где есть ViPNet CSP или ViPNet OSSL и записать на диск восстановления



ViPNet SafeBoot 3

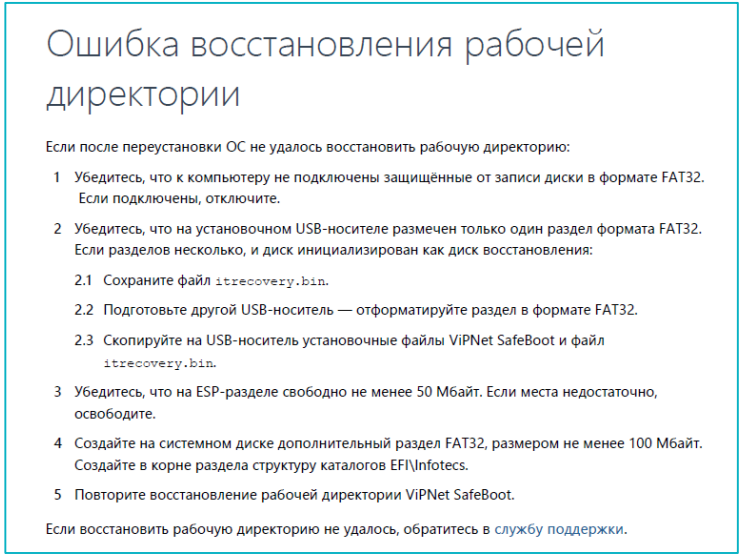
Руководство по установке

infotecs

Далее настройка идёт по стандартному сценарию, описанному в документации

Важное обновление в документации

Появился раздел с описанием шагов по обновлению операционной системы и восстановлению рабочей директории



Ошибка восстановления рабочей директории

Если после переустановки ОС не удалось восстановить рабочую директорию:

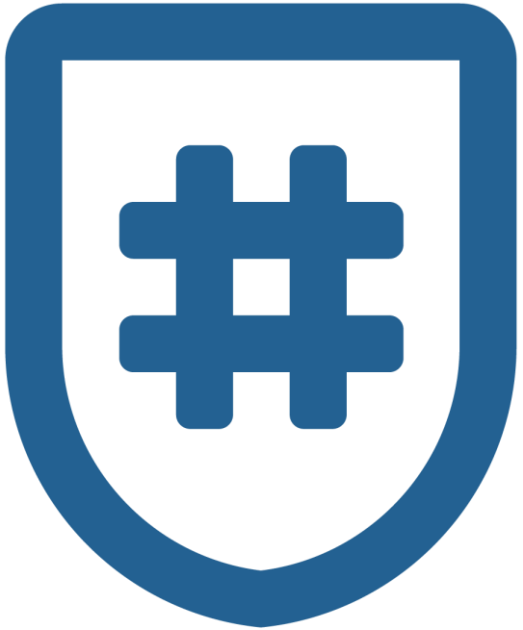
1. Убедитесь, что к компьютеру не подключены защищённые от записи диски в формате FAT32. Если подключены, отключите.
2. Убедитесь, что на установочном USB-носителе размечен только один раздел формата FAT32. Если разделов несколько, и диск инициализирован как диск восстановления:
   - 2.1 Сохраните файл `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.

Новые версии и перспективы развития

Уже есть новый релиз 3.2

- Поддержка syslog – отправка CEF сообщений
- Поддержка ALD PRO (Astra Linux)
- Поддержка работы на бездисковых станциях
- Профили загрузки ОС
- Поддержка LUKS
- Защита системных таблиц UEFI
- Поддержка токена Guardant ID версии 2
- Поддержка JaCarta-2 SE и JaCarta PRO
- Расписание доступа пользователей
- Регистрация всех подключенных устройств аутентификации



Версия передана на сертификацию

Остаётся только ждать

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363