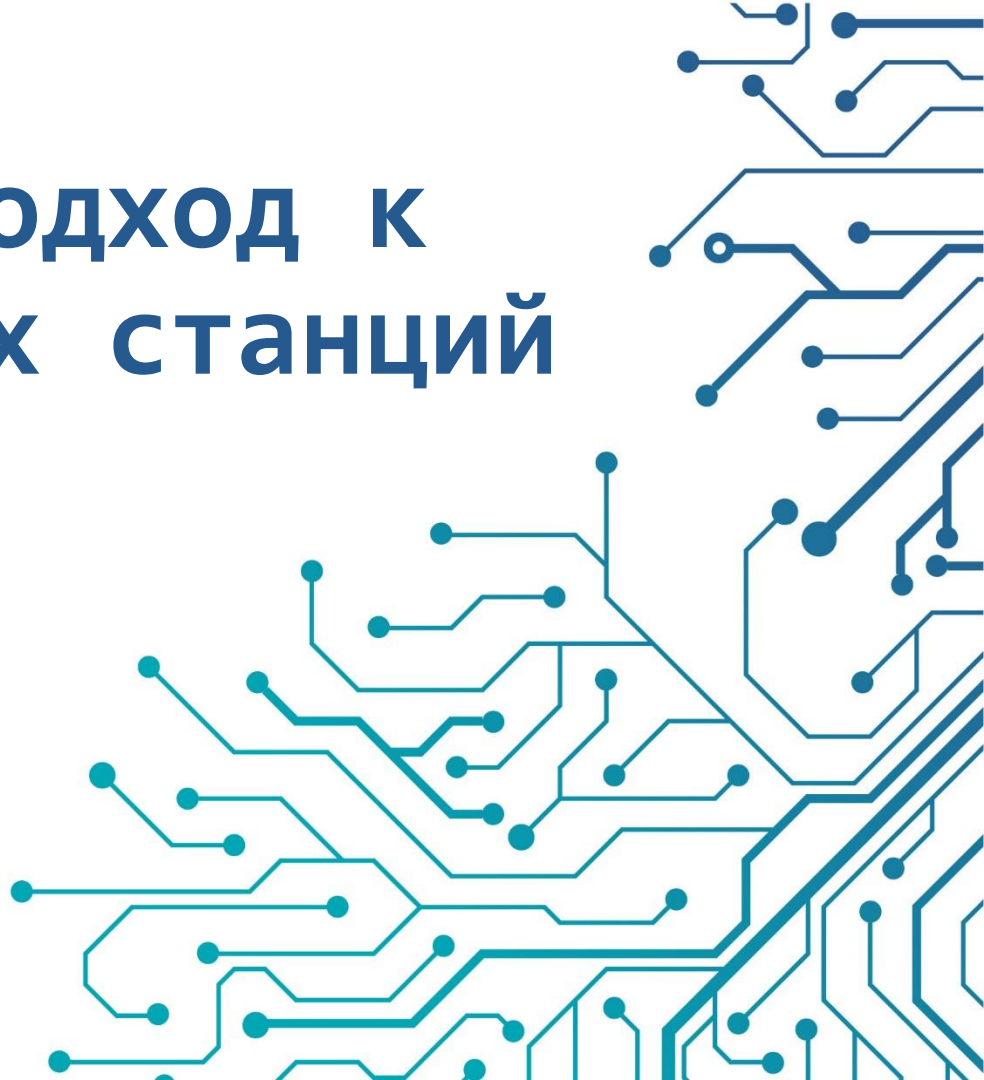
Комплексный подход к защите рабочих станций и серверов

Кадыков Иван
Руководитель направления



infotecs

Комплекс продуктов Endpoint Security

ViPNet SafeBoot
Решаемые задачи - Доверие к платформе и организация доверенной загрузки

ViPNet SafePoint
Решаемые задачи - Доверие к пользователю и организация замкнутой программной среды

ViPNet EndPoint Protection
Решаемые задачи - Защита от внешних нарушителей и обнаружение зловредной активности на хостах

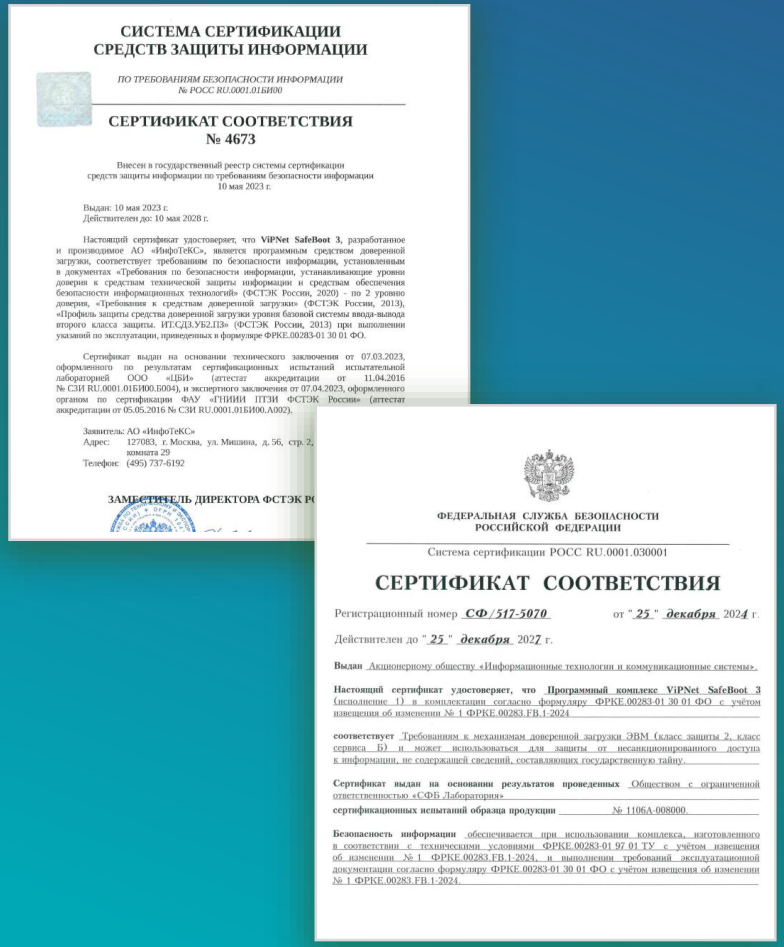
ViPNet Client 4U / ViPNet Client 5
Решаемые задачи – Организация защищённого канала между хостами организации

infotecs

ViPNet SafeBoot 3

Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ). 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.

Общая схема работы



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, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РО

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/517-5070* от "*25*" *декабря* 2024 г.

Действителен до "*25*" *декабря* 2027 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 с учётом извещения об изменении № 1 ФРКЕ.00283.ГВ.1-2024

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-008000.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00283-01 97 01 ТУ с учётом извещения об изменении № 1 ФРКЕ.00283.ГВ.1-2024, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00283-01 30 01 ФО с учётом извещения об изменении № 1 ФРКЕ.00283.ГВ.1-2024.

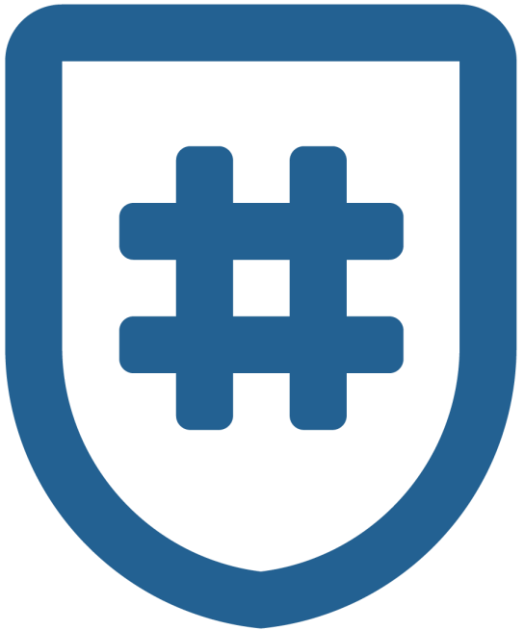
ViPNet SafeBoot 3

Первые! кто получил (второй раз подряд) два сертификата на одну версию!

- ФСТЭК России № 4673
- ФСБ России № СФ/517-5070

Что нового и интересного появилось в ViPNet SafeBoot 3?

- 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



ViPNet SafePoint

ViPNet SafePoint – сертифицированный программный комплекс защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС).

ViPNet SafePoint устанавливается на рабочие станции и сервера в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам.

Идентификация и аутентификация пользователей

Дискреционная модель доступа

Замкнутая программная среда

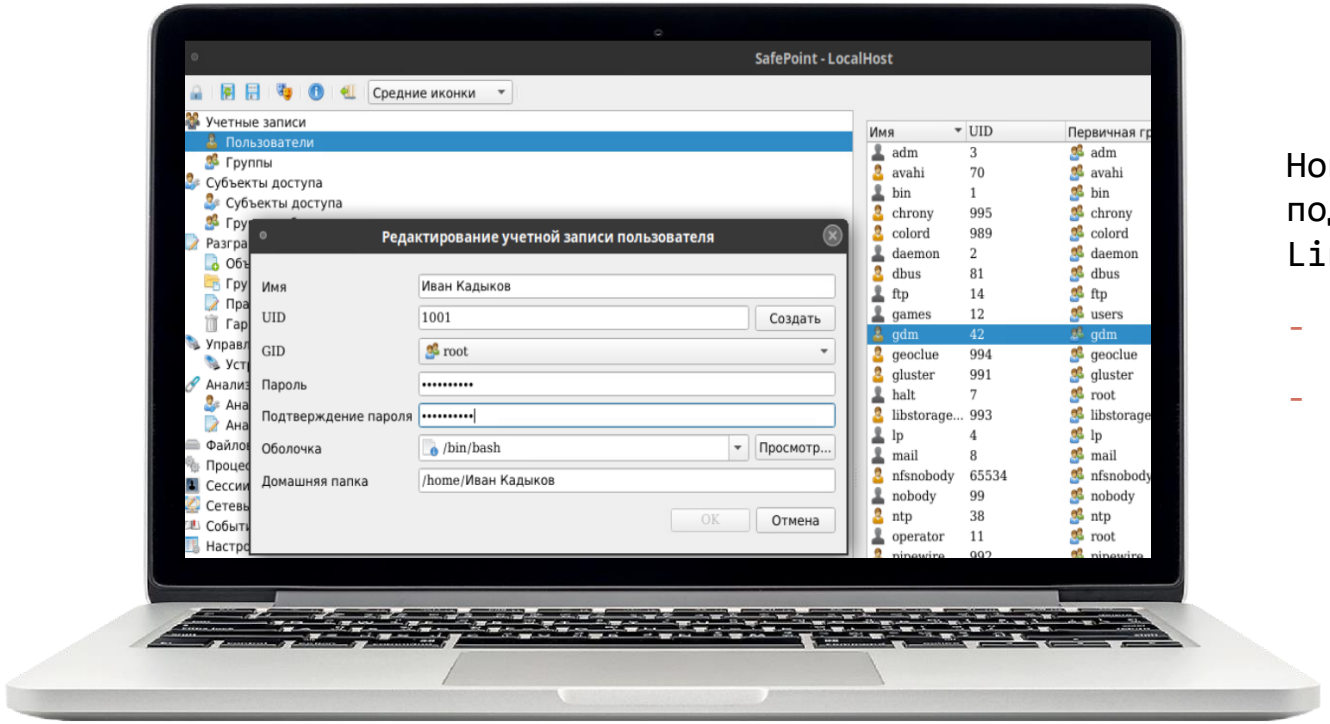
Контроль устройств

Контроль целостности файлов

Дополнительные защитные механизмы

- Защита от внедрения и выполнения вредоносных программ и кода
- Защита от атак на повышение привилегий
- Защита данных от атак на уязвимости системного ПО
- Защита от инсайдеров
- Защита данных от атак на уязвимости прикладного ПО

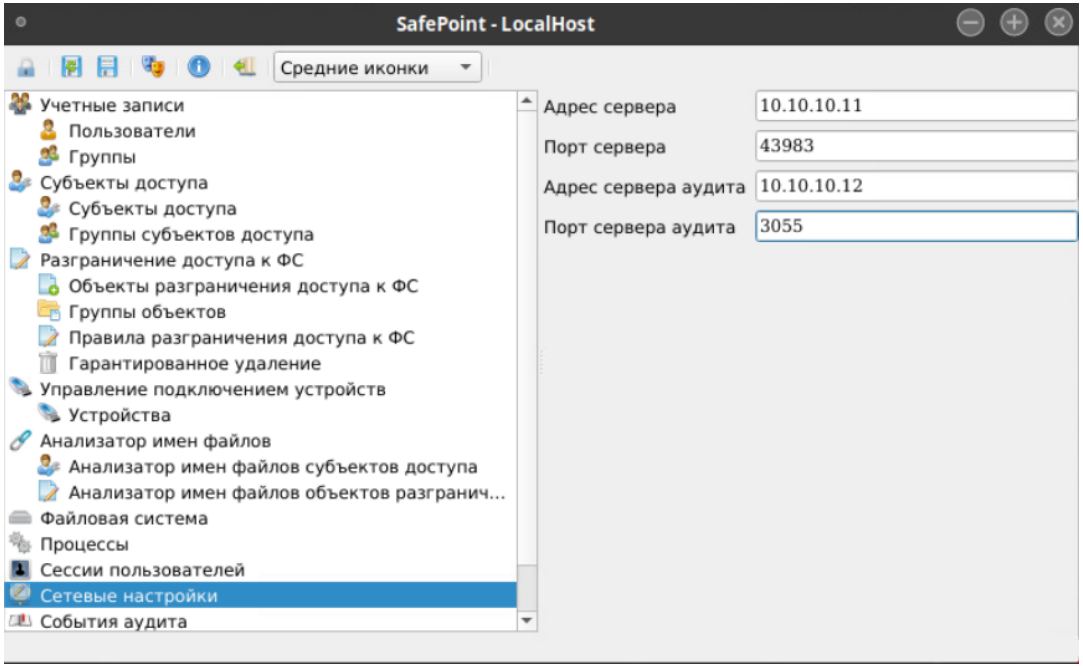
Что нового было в 2024 году



Новый Linux агент с поддержкой отечественных ОС Linux

- Автономная версия
- Сетевая версия

Легко внедряется в имеющуюся инфраструктуру



Подключение к существующему серверу безопасности и серверу аудита не займёт много времени

Можно задать параметры при установке или после установки «в ручную»

СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4468

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
18 октября 2021 г.

Выдан: 18 октября 2021 г.
Действителен до: 18 октября 2026 г.

Настоящий сертификат удостоверяет, что **изделие «ViPNet SafePoint»**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, 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 4 уровню доверия, «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014), «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014), «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности и задании по безопасности ФРКЕ.00240-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00240-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 15.07.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 05.10.2021, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

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

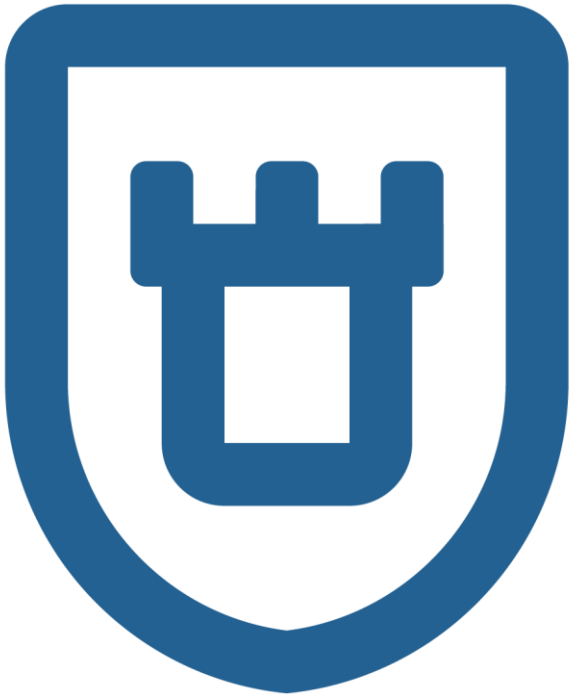
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Сертифицировано

- 5 класс защищенности СВТ
- 4 класс защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 класс ТДБ



ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых», «бесфайловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

Защитные механизмы

Еще больше защитных механизмов

SSL – инспекция – возможность расшифровывания всего трафика проходящего через модули ViPNet EndPoint Protection

SafeBrowsing – безопасный серфинг в интернете (веб-фильтрация)

Интеграционные функции

Интеграция с ViPNet Client 4U/5

Добавление\Редактирование\Удаление фильтров защищённой сети из локальной консоли
ViPNet EndPoint Protection (агент)

Получение фильтров от PMM через 4U/5

ZTNA

Добавление набора функций из стека технологий ZTNA и интеграция с ViPNet Client 4U / 5:

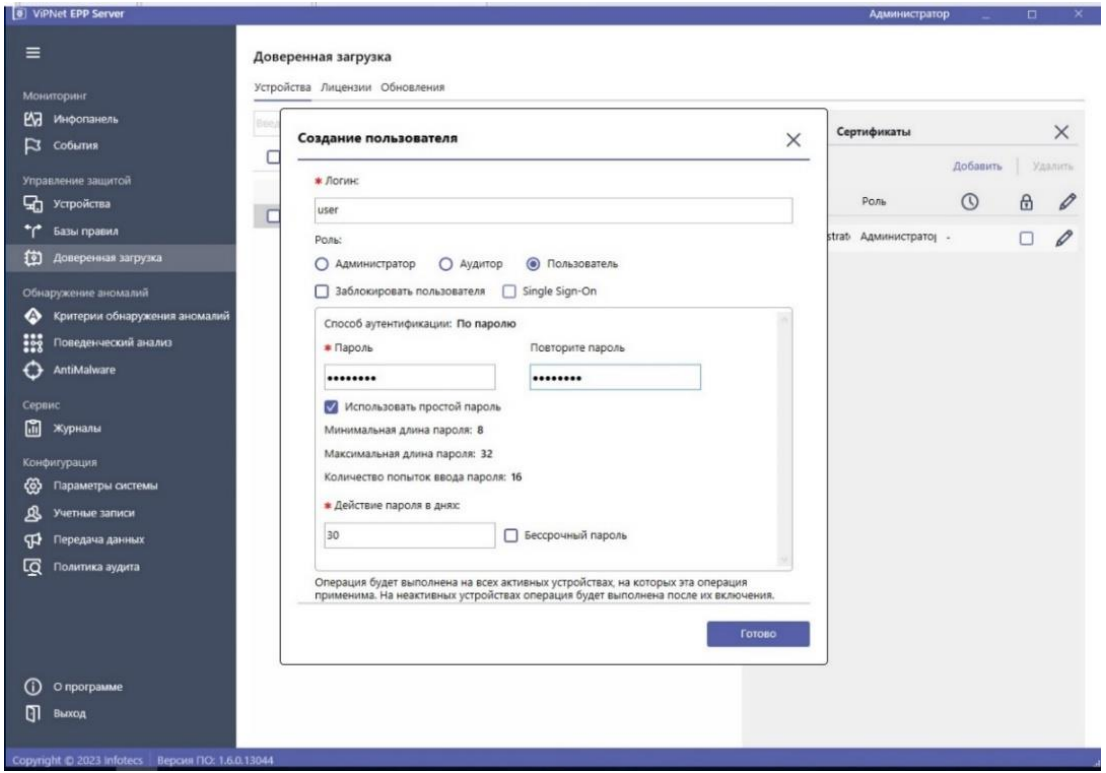
Проверка соответствия хоста на наличие требуемого ПО, обновлений ПО, запущенных процессов, обновление антивирусных баз и т.д.

Блокировка защищенной сети на устройстве при несоответствии устройства политикам ZTNA, информирование пользователя об этом.

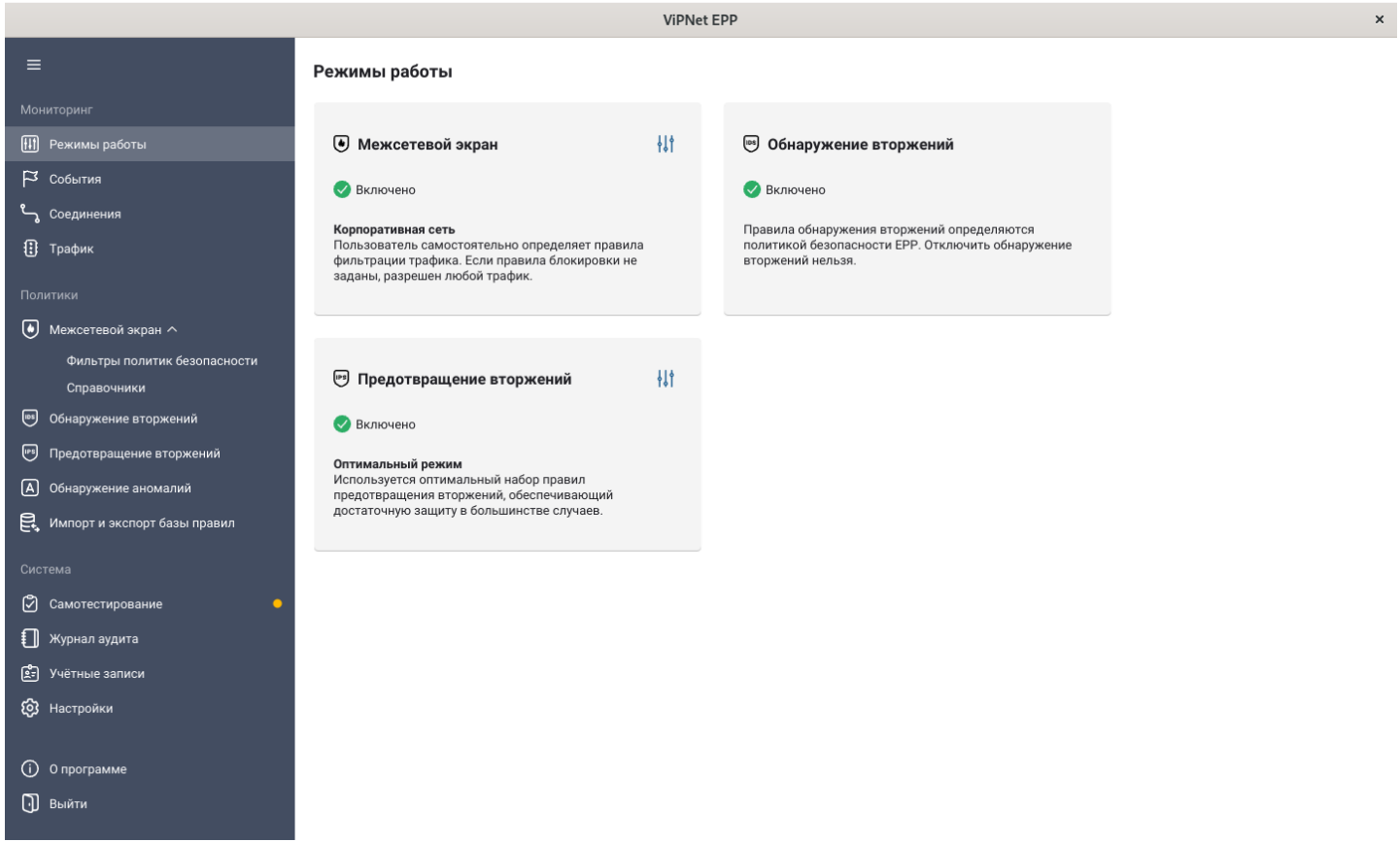
Управление ViPNet SafeBoot

Механизмы удалённого управления ViPNet SafeBoot:

- Лицензирование
- Получение журналов
- Обновление МДЗ
- Управление пользователями
- Установка корневых сертификатов



Новый агент под linux



ViPNet Client 4U for Linux

- Версия ПО: 4.8 и старше
- Используется виртуальный TUN\TAP интерфейс
- Поддержка широкого списка современных ОС Linux
- Не зависит от версии ядра ОС
- Поддерживает двухфакторную авторизацию
- Поддержка архитектур x86, ARM, Байкал (MIPSel), Эльбрус (e2k)

Имеет сертификаты на соответствие требованиям ФСБ России к СКЗИ классов КС1, КС2 и КС3.

Поддержка ОС Linux в сертифицированной версии

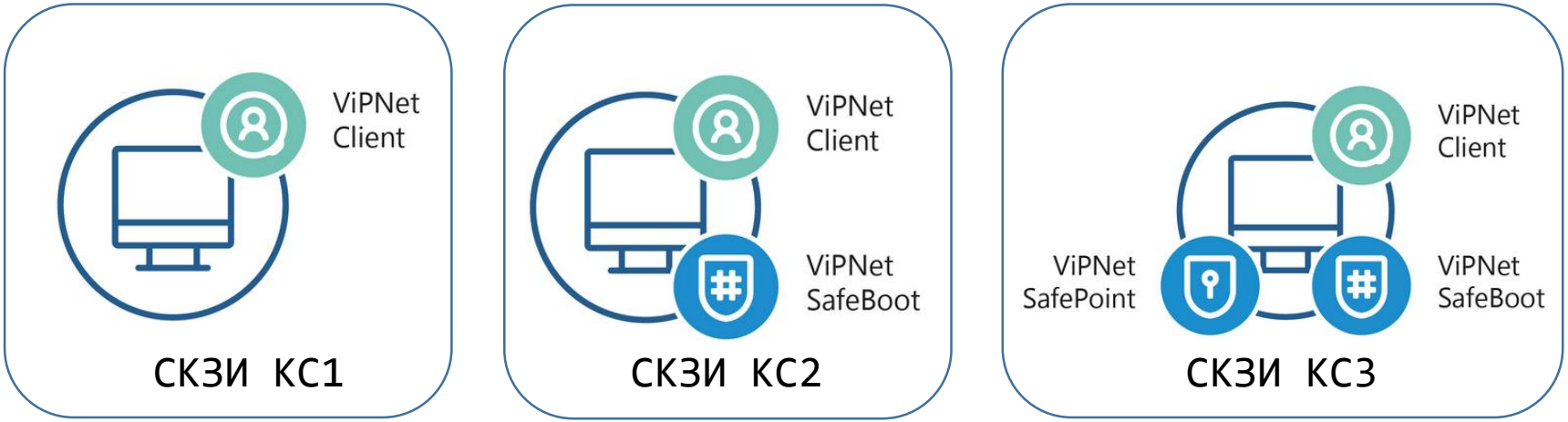
Архитектура	Дистрибутив Linux
x86-64	Astra Linux Special Edition 1.6, 1.7 (РУСБ.10015-01), Common Edition 2.12 «Орел» ГосЛинукс IC5, РЕД ОС 7.2, 7.3 Альт Рабочая станция 8 СП, 9, 10, K 10 AlterOS 7.5, СинтезМ 7.5, Основа 2.5.2, ЛОТОС, РОСА «КОБАЛЬТ», EMIAS OS 1.0 Ubuntu 18.04.2 LTS, 22.04 LTS, Debian 9.9 CentOS 7.1, 7.5, 8
«Байкал-Т1» (mipsel)	Astra Linux Special Edition 6.1 «Севастополь»
«Эльбрус» (e2k)	Astra Linux Special Edition «Ленинград»
ARMv5	OpenWrt Chaos Calmer
ARMv7	Astra Linux Special Edition «Новороссийск» Сборки для микроконтроллеров на Debian и OpenEmbedded

В рамках ИИ обновлён формуляр:

– аппаратно-программный модуль доверенной загрузки либо средство защиты информации, реализующее механизмы доверенной загрузки, имеющие действующие сертификаты ФСБ России, для соответствия требованиям, установленным для классов защиты КС2 и КС3 (исполнения 2 и 3 соответственно);

Наши решения

Схема комплексного решения



ГИС, ИСПДн, АСУ ТП, КИИ

Чтобы полностью защитить компьютер, недостаточно иметь одно СЗИ

Количество СЗИ определяется

Моделью нарушителя

Доступной функциональностью (классом продукта)

МДЗ УБ или БСВВ
СЗИ от НСД
СОВ/СПВ
МЭ
АВЗ
АНЗ
Защита канала связи

Какие ключевые меры закрывает каждый продукт

МДЗ

Блок мер ИАФ, УПД

Важное – УПД.3/17

СЗИ от НСД

Блок мер ИАФ, УПД, ОЦЛ

Очень много важного

СОВ/СПВ

Блок мер СОВ и РСБ

Важное – СОВ.1 и СОВ.2

МЭ

Блок мер ЗИС

Важно ЗИС.7/23 и ЗИС.22/34

САВЗ/АНЗ

Блок мер АВЗ и АНЗ

Защита канала связи (VPN)

Важно ЗИС.4/20

Комплексное решение для защиты ИСПДн, ГИС, АСУ ТП и КИИ

МДЗ УБ или БСВВ
СЗИ от НСД
СОВ/СПВ
МЭ
АВЗ
АНЗ
Защита канала связи

ViPNet SafeBoot
ViPNet SafePoint
ViPNet EndPoint Protection
ViPNet EndPoint Protection
ViPNEt EndPointProtection +АВЗ
АНЗ
ViPNet Clinet 4U / 5

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news