Обзор ключевых изменений в продуктовой линейке Endpoint Security

Кадыков Иван
Руководитель направления

Чтобы защищаться, надо понимать от чего!

Растущее количество атак и не доверенных аппаратных компонент

Удаленная работа, проведение приватных разговоров

Пользователь – внутренний нарушитель, низкий уровень осведомленности

Malware, Ransomeware, Fileless & Never-seen-before attacks

Требования регуляторов

Описывают и регламентируют необходимую функциональность, способы и подходы к защите рабочих станций, серверов, и создаваемым системам, в целом.

- Требования ФСТЭК России к ИС:
  - ГИС
  - ИСПДн
  - АСУ ТП
  - КИИ
- Требования ФСБ России
  - СКЗИ
  - Защита от НСД

ГИС, ИСПДн, АСУ ТП, КИИ

- Чтобы полностью защитить компьютер не достаточно 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

ГИС, ИСПДн, АСУ ТП, КИИ

- До 2021 года предлагаемый спектр продуктов для защиты рабочих станций состоял из:
  - ViPNet SafeBoot
  - ViPNet IDS HS
  - ViPNet Client 4

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

ViPNet SafeBoot
СЗИ от НСД
ViPNet IDS HS / СПВ
ViPNet Client 4
АВЗ
АНЗ
ViPNet Clinet 4

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
СЗИ от НСД
ViPNet IDS HS / СПВ
ViPNet Client 4
АВЗ
АНЗ
ViPNet Clinet 4

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

Построение ИС с СКЗИ

- Обычная ситуация у наших клиентов до прошлого года

Какой-то АПМДЗ
Какое-то СЗИ от НСД

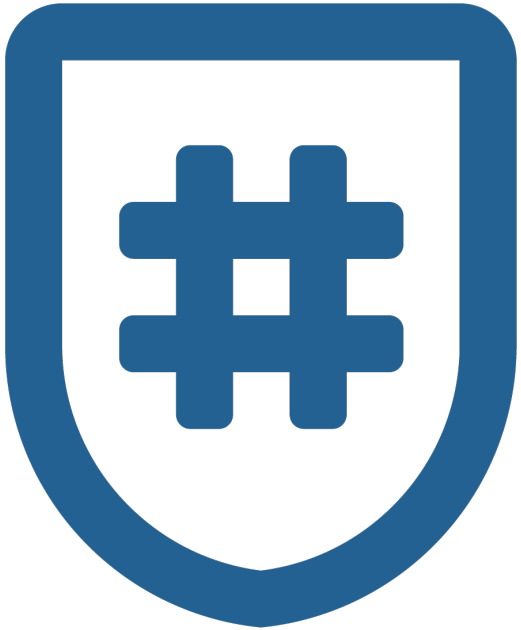
У нас есть ВСЁ

- Возможность использования программного замка ViPNet SafeBoot, вместо аппаратного.
- В Формулярах на ViPNet CSP и ViPNet Client уже приписана возможность использования СЗИ МДЗ (Средства защиты информации реализующие механизмы доверенной загрузки II класса, тип сервиса Б.)
- Если используете несертифицированную ОС и требуется замкнутая программная среда – ViPNet SafePoint

ТЕХНО 2024 infotecs ФЕСТ

ViPNet SafeBoot 3
Новое поколение МДЗ

ViPNet SafeBoot 3

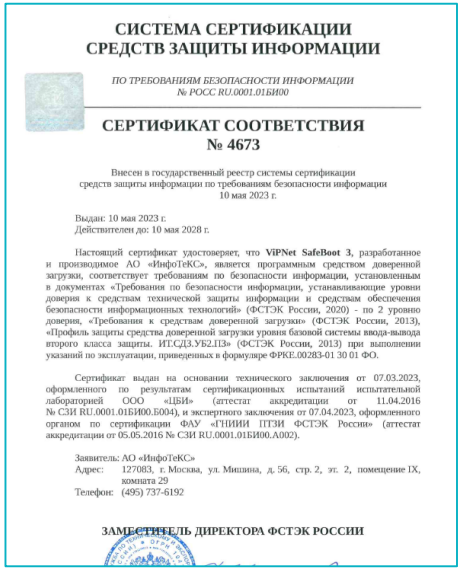


Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ). Предназначен для создания точки доверия к платформе и её компонентам, а также к загружаемой операционной системе. Ключевыми задачами продукта являются разграничение доступа к платформе, защита UEFI BIOS, контроль неизменности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

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.

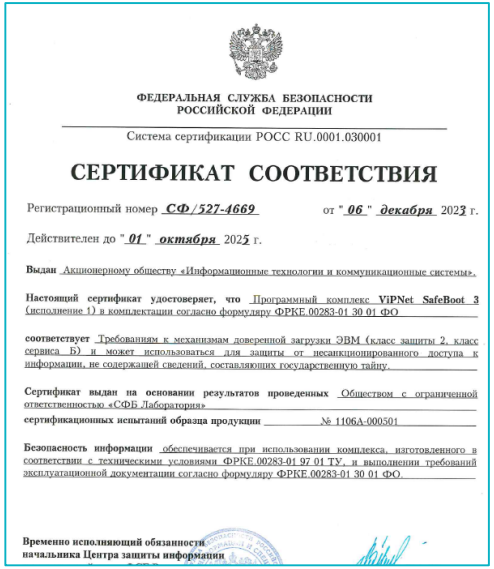
Выдан: 10 мая 2023 г.
Действителен до: 10 мая 2028 г.

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

Расширяя границы доверенной загрузки

ТЕХНО infotecs 2024 ФЕСТ

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

Доверенная загрузка это:

Доверие и защита платформы

- Защита UEFI BIOS
  - защиту BIOS от перезаписи, чтения и от изменений EFI-переменных
  - 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 системных таблиц
  - Защита дисков от записи
  - Блокировка UEFI Option Rom
- Эмуляция NVRAM

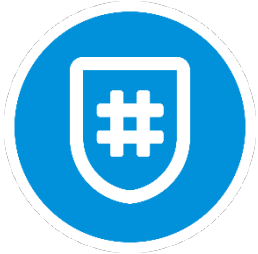
ViPNet SafeBoot – два исполнения

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

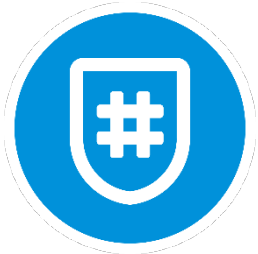
Необходим, при построении систем СКЗИ и соответствовать требованиям ГИС, ИСПДн, АСУ ТП, КИИ.

- **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



ViPNet SafePoint
Продолжение развития, наращиваем функциональность

ViPNet SafePoint

ТЕХНО infotecs 2024 ФЕСТ

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

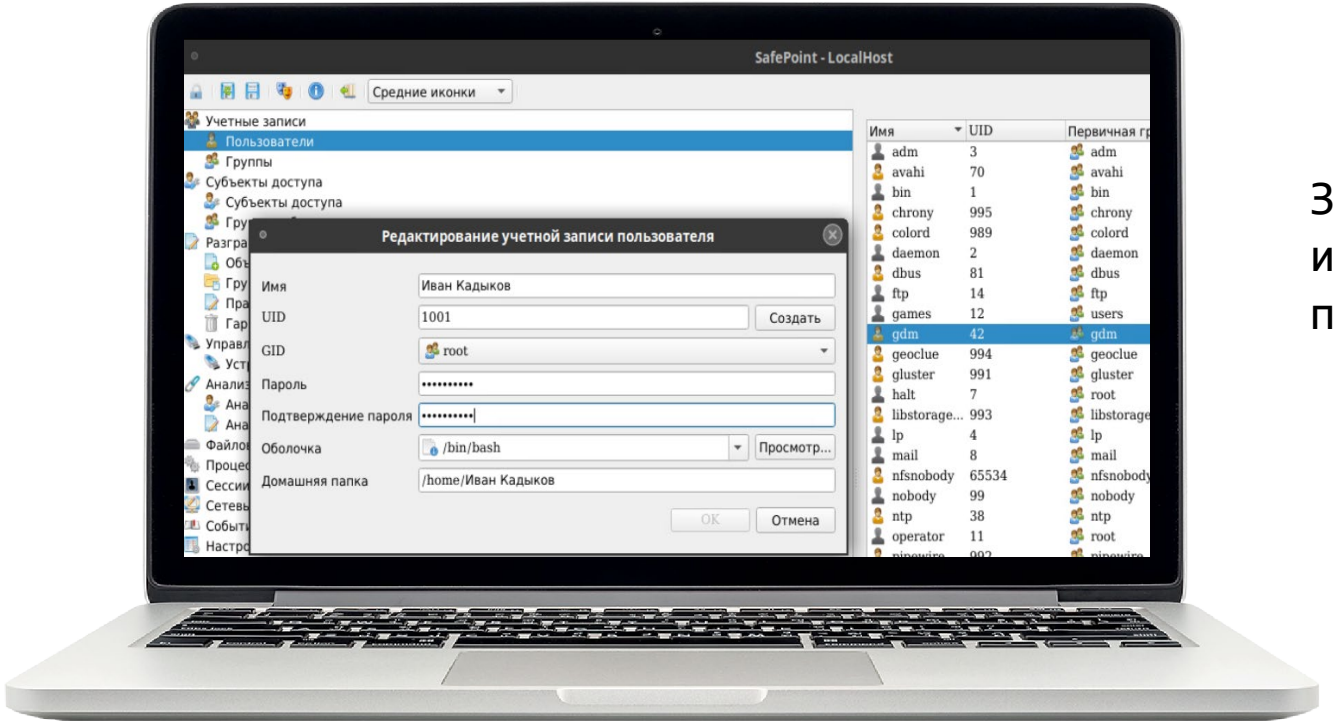
- Защита от внедрения и выполнения вредоносных программ и кода
- Защита от атак на повышение привилегий
- Защита данных от атак на уязвимости системного ПО
- Защита от инсайдеров
- Защита данных от атак на уязвимости прикладного ПО

ViPNet SafePoint

Поддерживаемые ОС Linux:

- Альт Рабочая станция 10.1 ядро Linux 5.10.164
- РЕД ОС 7.3.2 «Муром» Рабочая станция, стандартная редакция, ядро Linux 5.15.72 и 5.15.125
- РЕД ОС 7.3.3 «Муром» Рабочая станция, стандартная редакция, ядро Linux 6.1.38
- Astra Linux Special Edition 1.7.4, ядро Linux 5.15.0-70-generic
- Debian 11 (bullseye), ядро Linux 5.10.0-10-amd64

Идентичность интерфейсов



Заведение
и редактирование
пользователей

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

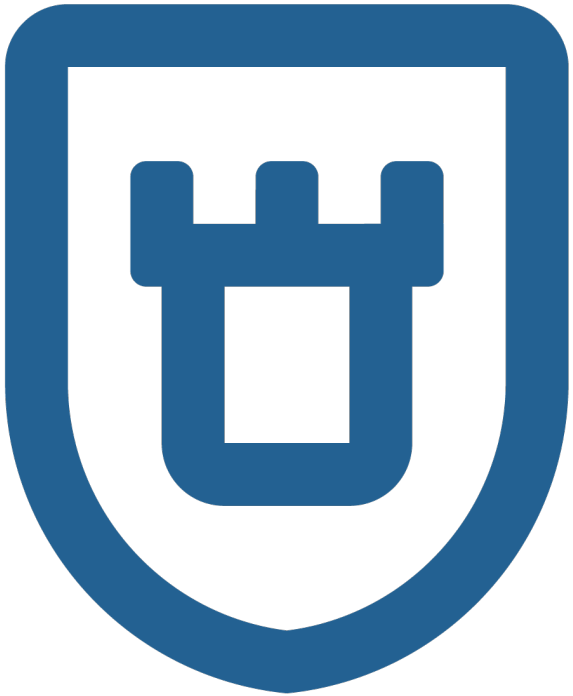
В.Лютиков

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
Новые версии! Новая функциональность!



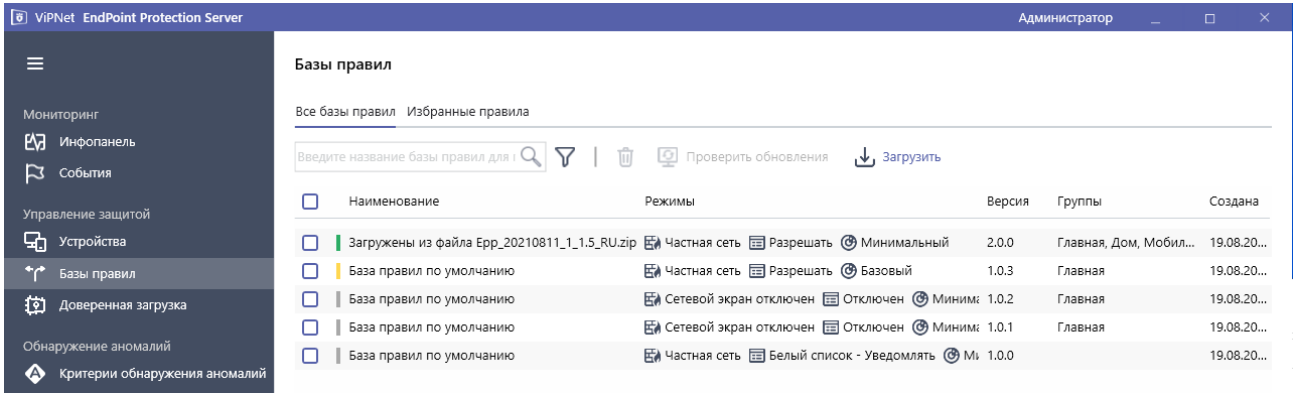
ViPNet EndPoint Protection

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

Работаем по правилам!

EndPoint Protection работает по БРП



Состоит из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевого экрана
- Списков ПО для Черного и Белого списка
- Эвристический движок Anti-malware
- Движок обнаружения аномального поведения системных утилит

Версия 1.6 – что нового?

- 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.

Ещё больше защитных механизмов

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

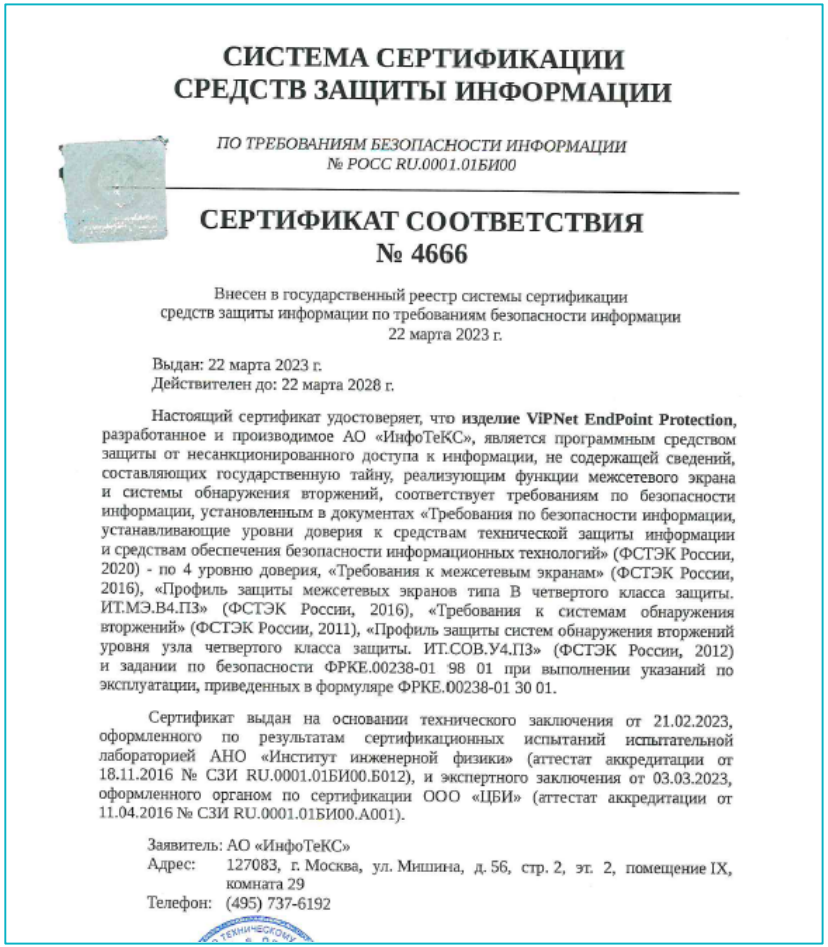
- SafeBrowsing – безопасный сёрфинг в интернете (веб-фильтрация)

И ещё…

- Новых сервер для управления агентами под Linux (пока имеется возможность управления функциональностью СОВ и МЭ)
- Внедрение новых методик предотвращения бесфайловых атак:
  - Hollowed / replaced
  - Doppelganger
- Дополнительные механизмы удалённого управления ViPNet SafeBoot:
  - Обновление МДЗ
  - Управление пользователями
  - Установка корневых сертификатов
- И ещё много чего

Поддержка Linux

- Операционная система GNU/Linux (64-разрядная) одного из следующих дистрибутивов:
  - Astra Linux Special Edition 1.6 «Смоленск», ядро Linux 5.15.0-33-generic #astra2+ci122 (с установленным оперативным обновлением БЮЛЛЕТЕНЬ № 20221220SE16 (оперативное обновление 12));
  - Astra Linux Special Edition 1.7.2, ядро Linux 5.15.0-33-generic #astra2+ci56 (с установленным оперативным обновлением БЮЛЛЕТЕНЬ № 2022-0819SE17 (оперативное обновление 1.7.2));
  - Astra Linux Special Edition 1.7.4, ядро Linux 5.15.0-70-generic #astra2+ci6 (с установленным оперативным обновлением БЮЛЛЕТЕНЬ № 2023-0630SE17MD (срочное оперативное обновление 1.7.4.UU.1);
  - Альт 8 СП Рабочая станция, ядро Linux 5.10.83-std-def-alt0.c9f.2;
  - Альт СП Рабочая станция релиз 10, ядро Linux 6.1.29-un-def-alt1;
  - Альт Рабочая станция 10.1, ядро Linux 5.10.164-std-def-alt1;
  - РЕД ОС 7.3.1 «Муром» Рабочая станция, стандартная редакция, ядро Linux 5.15.10-1.el7.x86_64;
  - РЕД ОС 7.3.2 «Муром» Рабочая станция, стандартная редакция, ядро Linux 5.15.87-1.el7.3.x86_64;
  - РЕД ОС 7.3.3 «Муром» Рабочая станция, стандартная редакция, ядро Linux 5.15.125-1.el7.3.x86_64
  - РЕД ОС 7.3 «Муром» Рабочая станция, сертифицированная редакция, ядро Linux 5.15.87-1.el7.3.x86_64;
  - РЕД ОС 7.3 «Муром» Рабочая станция, сертифицированная редакция, ядро Linux 5.15.125-1.el7.3.x86_64;
  - Debian Linux 11 (bullseye), ядро Linux 5.10.0-10-amd64.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4666

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
22 марта 2023 г.

Выдан: 22 марта 2023 г.
Действителен до: 22 марта 2028 г.

Настоящий сертификат удостоверяет, что **изделие ViPNet EndPoint Protection**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции межсетевого экрана и системы обнаружения вторжений, 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 межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности ФРКЕ.00238-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00238-01 30 01.

Сертификат выдан на основании технического заключения от 21.02.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией АНО «Институт инженерной физики» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 03.03.2023, 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

Сертифицировано

- МЭ тип В класс 4
- СОВ У4
- 4 класс ТДБ

Endpoint Security

ТЕХНО 2024 infotecs ФЕСТ

ViPNet SafeBoot

ViPNet Client

ViPNet SafePoint

ViPNet EndPoint Protection

ТЕХНО 2024 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363