Обзор продуктов линейки ViPNet для защиты рабочих станций и серверов

Кадыков Иван

Три основных возможности заразить хост

- Атаки на сеть
- Непосредственная атака на рабочие станции
- Внутренний нарушитель

Что предлагают на рынке?

Что предлагаем мы для защиты Endpoint

ViPNet SafeBoot

Высокотехнологичный **программный** модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS

Решаемые задачи ViPNet SafeBoot

Сертифицировано

- Сертифицирован по требованиям руководящих документов к средствам доверенной загрузки уровня базовой системы ввода-вывода **2** класса.
- Ключевая мера из приказов 17, 21, 31:
  - УПД.17 – обеспечение доверенной загрузки средств вычислительной техники

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823

Выдан 14 ноября 2017 г.
Действителен до 14 ноября 2020 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Программный модуль доверенной загрузки VIPNet SafeBoot»**, разработанный и производимый ОАО «ИнфоТеКС» в соответствии с техническими условиями ФРКЕ.00180-01 97 01 ТУ, является программным средством доверенной загрузки уровня базовой системы ввода-вывода соответствует требованиям документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013) и «Профиль защиты средств доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТСДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00180-01 30 01 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.К004) - техническое заключение от 28.07.2017, экспертного заключения от 12.10.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «ИнфоТеКС» (ИНН 7710013769)
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркированием знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляются испытательной лабораторией ООО «ЦБИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации

Банк угроз – что можно закрыть?

В БДУ ФСТЭК имеется

29 УГРОЗ в полной или косвенной мере относящиеся к угрозам BIOS/UEFI BIOS

Угроза	Угроза
УБИ.004: Угроза аппаратного сброса пароля BIOS -	УБИ.053: Угроза невозможности управления правами пользователей BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS	УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.008: Угроза восстановления аутентификационной информации	УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
УБИ.006: Угроза внедрения кода или данных	УБИ.090: Угроза несанкционированного создания учётной записи пользователя
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS	УБИ.108: Угроза ошибки обновления гипервизора
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS	УБИ.121: Угроза повреждения системного реестра
УБИ.018: Угроза загрузки нештатной операционной системы	УБИ.123: Угроза подбора пароля BIOS
УБИ.023: Угроза изменения компонентов системы	УБИ.124: Угроза подделки записей журнала регистрации событий
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера	УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию	УБИ.144: Угроза программного сброса пароля BIOS
УБИ.032: Угроза использования поддельных цифровых подписей BIOS	УБИ.145: Угроза пропуска проверки целостности программного обеспечения
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS	УБИ.150: Угроза сбоя процесса обновления BIOS
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS	УБИ.152: Угроза удаления аутентификационной информации
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS	УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS
	УБИ.179: Угроза несанкционированной модификации защищаемой информации

Новая версия! В ожидании ИК!
ViPNet SafeBoot 1.3

- Авторизация в AD/LDAP
- Контроль целостности системного реестра Windows
- Средства диагностики UEFI BIOS
- Программа установки ViPNet SafeBoot для UEFI

infotecs

БлокХост Сеть 2.0

Комплексная и многофункциональная защита информационных ресурсов рабочих станций и серверов

- Двухфакторная аутентификация
- Контроль запуска процессов
- Контроль изменения реестра
- Контроль вывода информации
- Гарантированное удаление
- Разграничение прав доступа

Особенности Блокхост-сеть 2.0

Удалённое присвоение электронного идентификатора пользователям

Развёртывание без привязки к Active Directory

Удалённое развёртывание стороннего ПО через консоль управления Блокхост

Поиск станций по: IP, DNS, Маске, Active Directory

Сертифицировано!

СЗИ от НСД «Блокхост-сеть 2.0» является программно-техническим средством защиты от несанкционированного доступа к информации и подтверждает соответствие требованиям:

- НДВ.2
- СВТ.3

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3740

Выдан 30 ноября 2016 г.
Действителен до 30 ноября 2019 г.

Настоящий сертификат удостоверяет, что **средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0»**, разрабатываемое и производимое ООО «Газинформсервис» в соответствии с техническими условиями ТУ 5014-051-72410666-2015 и функционирующее под управлением операционных систем, указанных в формуляре 72410666.00051-01 30 01, является программно-техническим средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по **2** уровню контроля, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по **3** классу защищенности, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) - по **4** классу защищенности при выполнении условий эксплуатации, приведенных в формуляре 72410666.00051-01 30 01.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма» (аттестат аккредитации от 10.04.2017 № СЗИ RU.0001.01БИ00.Б017) – техническое заключение от 21.02.2017, и экспертного заключения от 28.02.2017 органа по сертификации ЗАО «Лаборатория ППШБ» (аттестат аккредитации от 09.03.2017 № СЗИ RU.0001.01БИ00.А006).

Заявитель: ООО «Газинформсервис» (ИНН 7838017968)
Адрес: 198188, г. Санкт-Петербург, ул. Кронштадтская, д. 10, лит. А
Телефон: (812) 677-2050

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией Санкт-Петербургский НТЦ ФГУП «НПП «Гамма».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
30 ноября 2016 г.

ViPNet IDS HS

- ViPNet IDS HS — система обнаружения вторжений, осуществляющее мониторинг и обработку событий внутри хоста, с применением сигнатурного и эвристического метода анализа атак, используя отечественные правила и сигнатуры .

Ключевая функциональность – выявление IoC

Анализ системных журналов и логов ОС и приложений

Результаты выполнения команд или изменений результатов команд

Мониторинг файловой активности и реестра

Анализ трафика проходящего через хост

Архитектура

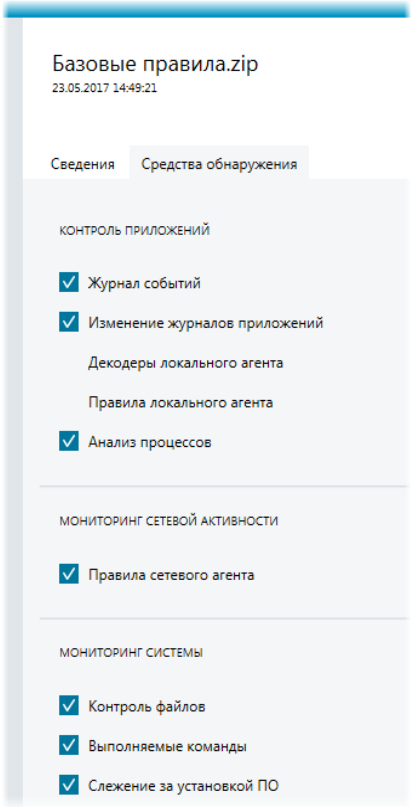
- Агент — собирает необходимую информацию о функционировании хостов и выполняет первичный анализ данных
- Сервер — получает, хранит и анализирует информацию от Агентов, хранит правила, команды и параметры, и передаёт их на Агенты.
- Консоль управления — предоставляет графический интерфейс для управления Агентами и мониторинга их состояния

Поддерживаемые ОС

- Семейство операционных систем Windows
- AstraLinux 1.5 релиз «Смоленск» (только агент)
- Debian 8 (только агент)

Особенности реализации агента

- Агент ViPNet IDS HS состоит из двух частей:
  - Сетевой агент – осуществляет мониторинг за сетью
  - Агент уровня ОС – осуществляет мониторинг за событиями внутри операционной системы



Сертифицировано

- Сертификат ФСТЭК России по требованиям к системам обнаружения вторжения уровня узла 4 класса.
- Список мер из приказов №21 и №17:
  - ИАФ.1, ИАФ.5
  - УПД.4
  - РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7
  - **СОВ.1, СОВ.2**
  - АНЗ.3
  - ОЦЛ.1, ОЦЛ.3
  - ИНЦ.2, ИНЦ.3, ИНЦ.4.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3802

Выдан 12 октября 2017 г.
Действителен до 12 октября 2020 г.

Настоящий сертификат удостоверяет, что **система обнаружения вторжений ViPNet IDS HS**, разработанная и производимая ОАО «ИнфоТеКС» в соответствии с техническими условиями ФРКЕ.00177-01 97 01, является системой обнаружения вторжений уровня узла, соответствует требованиям документов «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004) - технического заключения от 23.05.2017, экспертного заключения от 29.08.2017 органа по сертификации ФАУ «ГНИИ ИТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «ИнфоТеКС» (ИНН 7710013769)
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЦБИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
12 октября 2017 г.

ViPNet IDS HS версия 1.2 закончен ИК в ФСТЭК

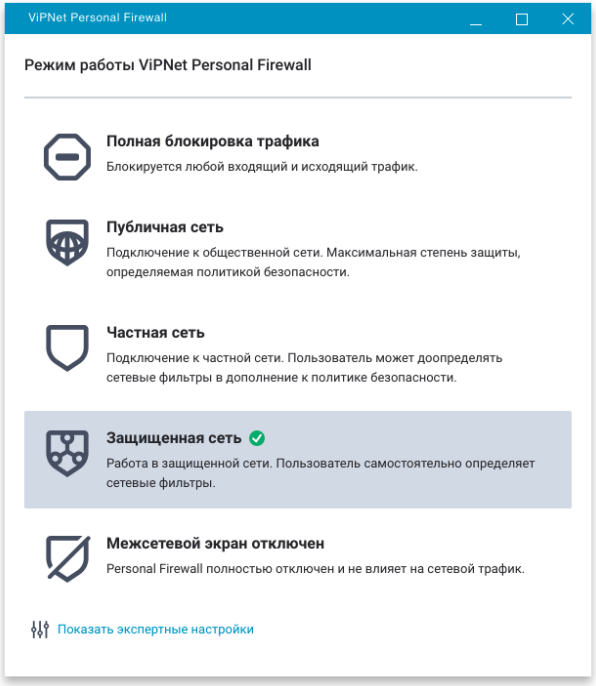
- Интеграция с ViPNet TIAS, ViPNet IDS MC
- Интеграция с Active Directory и ViPNet-сетями
- Агенты Debian 8 и Astra Linux 1.5 «Смоленск»
- Поддержка syslog (CEF) и snmp

ViPNet Personal Firewall 4.5

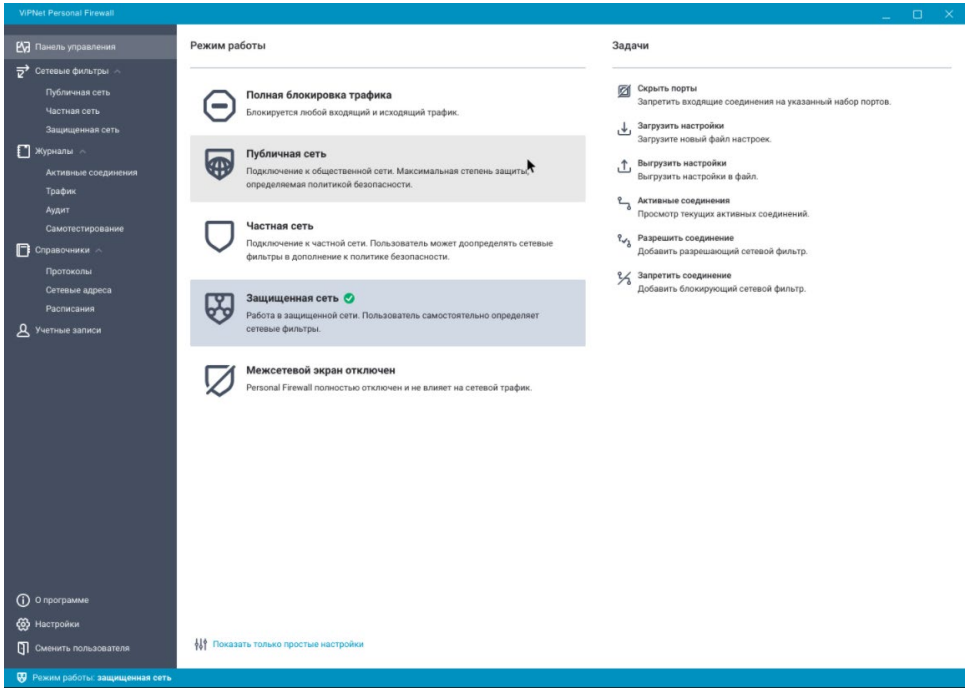
ViPNet Personal Firewall 4.5 — новый, полностью обновлённый программный межсетевой экран, предназначенный для контроля и управления трафиком рабочих мест и серверов пользователей информационных систем.

Удобный UI

Режим пользователя

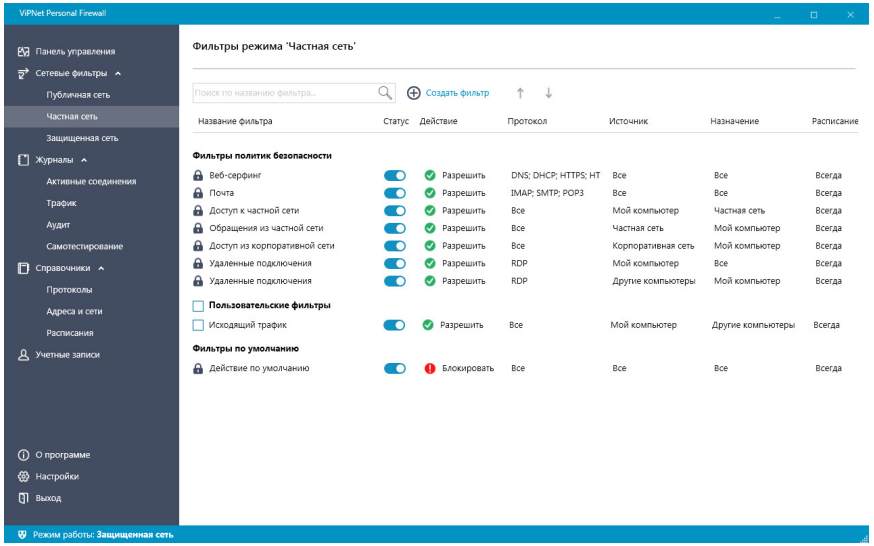


Режим администратора

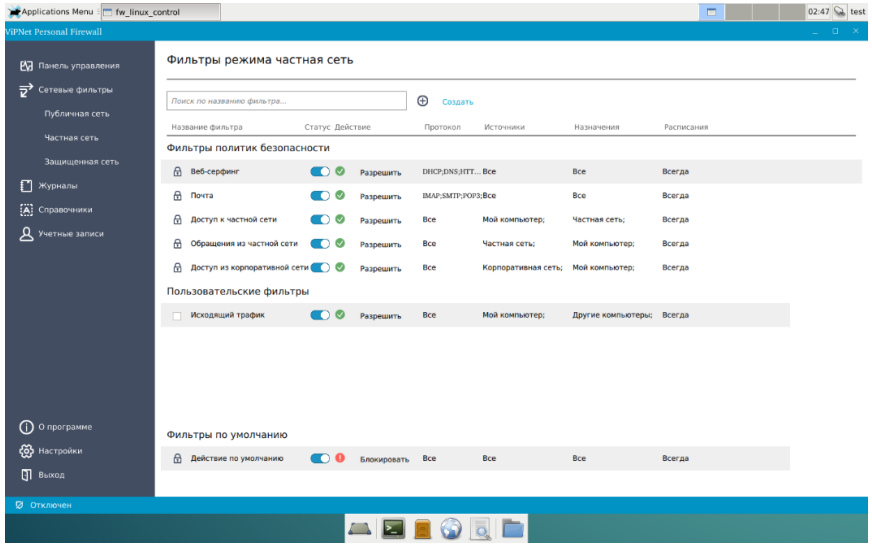


И Windows, и Linux

Windows



Linux



Список поддерживаемых ОС

- Windows 7
- Windows 8.1
- Windows 10

Windows Server

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

- Astra Linux Special Edition 1.5
- АльтЛинукс СПТ 7.0 Рабочая станция
- Debian

Возможности

Фильтрация трафика (IPv4 и IPv6)

Преднастроенные сетевые фильтры:

- Публичная сеть
- Частная сеть
- Защищенная сеть

Контроль сетевой активности приложений

Работа сетевых фильтров по расписанию

Два режима работы

- Уровень пользователя
- Уровень администратора

ViPNet Client

- VPN-клиент для работы в защищенных сетях ViPNet
- Персональный сетевой экран
- Прозрачен для приложений пользователя и ОС
- Независим от физических каналов связи
- Поддерживает ОС Windows, Linux, Android, iOS, MacOS, Sailfish
- Сертифицирован ФСБ на СКЗИ по классам от КС1 до КС3
- Сертифицирован ФСТЭК на соответствие требованиям к МЭ

ViPNet Client for Windows | ViPNet Client for Linux | ViPNet Client for Android | ViPNet Client for iOS | ViPNet Client for MacOS | ViPNet Client for Sailfish


infotecs
Благодарю за внимание!