Защита рабочих станций и серверов - что сделано в 2018 и перспективы развития в 2019

Иван Кадыков

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

Организация доверенной загрузки

Контроль целостности

- UEFI BIOS
- MBR
- Таблицы ACPI, SMBIOS, карты распределения памяти
- Файлов
- CMOS

Разграничение доступа

- Двухфакторная аутентификация
- Токены:
  - JaCarta
  - Rutoken
  - Guradant ID

Что нового было в 2018

Версия 1.3

- Авторизация на LDAP/AD
- Контроль целостности реестра
- Автоматическое построение списков контроля для ОС Windows.
- Поддержка режима защиты BIOS для новых платформ
- Средства диагностики UEFI BIOS на предмет возможности установки ViPNet SafeBoot

База совместимости

База совместимости с платформами различных производителей доступна в разделе загрузить

Таблица совместимости SafeBoot с платформами	от 26.12.2018	24.94 Kb

Таблица совместимости ViPNet SafeBoot с платформами различных производителей — **По состоянию на 26.12.2018**

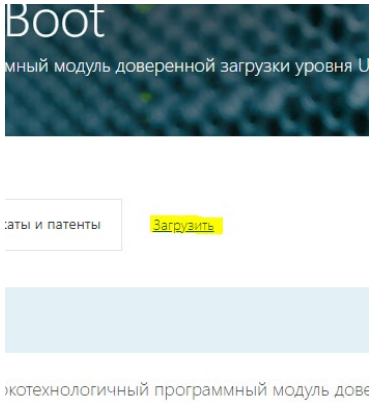
Название	Дата	Производитель	Материнская плата	UEFI	SafeBoot	Способ установки	Тестирование	Совместимость	Защита BIOS
HP Z2 Mini G3 DM	20.12.2018		Hewlett-Packard	v2.4	1.3		Диагностика	Потенциальная	
Supermicro server X11DPi-N(T)	19.12.2018	Supermicro	Supermicro	v2.5	1.3	Штатные средства	Базовое	Потенциальная	
ASUS X555LN	19.12.2018	ASUS	ASUS	v2.31	1.3		Диагностика	Потенциальная	
ASUS Prime X299-Deluxe II	15.12.2018		ASUS	v2.6	1.4		Диагностика	Потенциальная	
ASUS MiniPC VC65-C	15.12.2018		ASUS	v2.6	1.4		Диагностика	Потенциальная	
iEi NANO-ULT3	13.12.2018		iEi	v2.4	1.3	Программа установки	Базовое	Потенциальная	
Supermicro SuperServer 6018R-TDW	11.12.2018	Supermicro	Supermicro	v2.4	1.3	Штатные средства	Базовое	Потенциальная	
Gigabyte X399 Aorus Xtreme	06.12.2018		Gigabyte	v2.7	1.4		Диагностика	Потенциальная	
Huawei 2288H V5	05.12.2018	Huawei	Huawei	v2.5	1.3		Диагностика	Имеются ограничения	Нет
ASRock H310M-HDVM.2	29.11.2018		ASRock	v2.6	1.4	Программа установки	Базовое	Потенциальная	Да*
MSI A320M Pro-VH Plus	26.11.2018		MSI	v2.7	1.4		Диагностика	Имеются ограничения	
Siemens SIMATIC IPC647D	21.11.2018	Siemens	Siemens	v2.4	1.3		Диагностика	Потенциальная	
Siemens SIMATIC IPC427D	21.11.2018	Siemens	Siemens	v2.31	1.3		Диагностика	Имеются ограничения	
ASRock H310CM-DVS	24.10.2018		ASRock	v2.7	1.3	Программа установки	Базовое	Потенциальная	Да*
ASUS ROG Maximus XI Gene	08.11.2018		ASUS	v2.7	1.3		Диагностика	Потенциальная	
ASUS Prime Z390-A	07.11.2018		ASUS	v2.7	1.3		Диагностика	Потенциальная	
ASUS ROG MAXIMUS XI EXTREME	01.11.2018		ASUS	v2.7	1.3		Диагностика	Потенциальная	
MS-AEA11	31.10.2018	EBPAAC	Micro-Star	v2.4	1.3		Диагностика	Потенциальная	
Lenovo IdeaCentre 300-23ISU	26.10.2018		Lenovo	v2.4	1.3	Программа установки	Базовое	Потенциальная	

Если нет в таблице? Начинаем диагностику текущего ~~зоо~~парка

Скачиваем с сайта утилиту для диагностики

1. ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки уровня UEFI BIOS

2. 

3. Диагностическая утилита – получение информации о UEFI BIOS-компьютера

Сертифицировано

Средство доверенной загрузки уровня базовой системы ввода-вывода **2 класса**.

Какие меры приказов закрывает?

- (ГЛАВНОЕ) УПД.17 для 17,21,31 приказов и УПД.3 для 239 приказа – «Обеспечение доверенной загрузки средств вычислительной техники» - актуально для классов 1-2 ИСПДн, ГИС, АСУ ТП и КИИ
- ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.4, УПД.6, РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.7, ОЦЛ.1

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»**, разрабатываемый 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 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.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 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
14 ноября 2017 г.

Банк угроз – что можно закрыть?

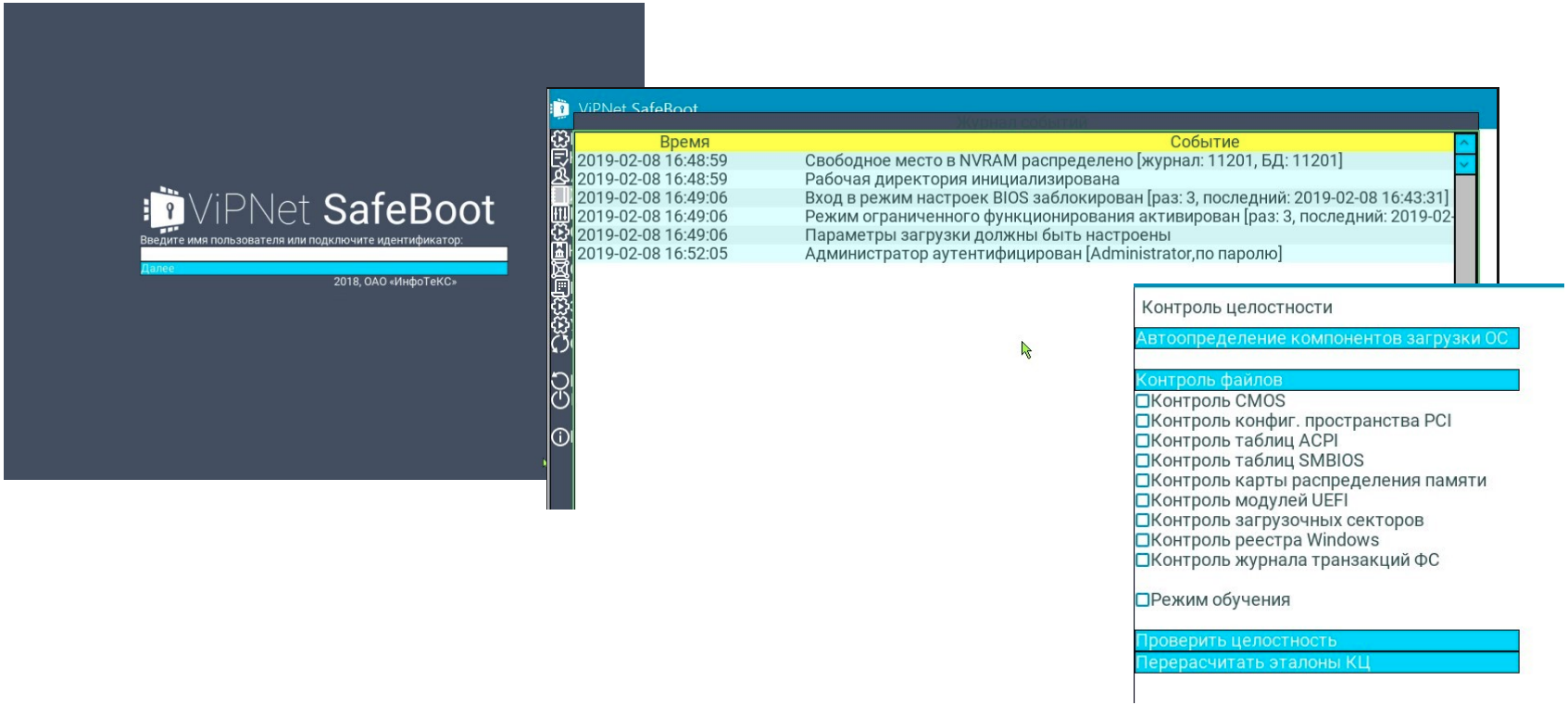
29 УГРОЗ в полной или косвенной мере относящиеся к угрозам BIOS/UEFI BIOS

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

Что запланировано на 2019 г.

- Графический интерфейс
- JaCarta ГОСТ-2
- Авторизация по западным сертификатам (например, выданных Microsoft CA)
- Поддержка новых чипсетов Intel/AMD
- Удалённое управление
- Режим неактивности

Новый интерфейс



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

Как выявляются атаки?

Сигнатурный анализ

Выявление характерных идентифицирующих свойств атаки

Эвристический анализ

Совокупность функций нацеленных на обнаружение неизвестных атак

Ключевая функциональность

Анализ системных журналов и логов ОС и приложений

Мониторинг файловой активности и реестра

Различные источники событий

Результаты выполнения команд или изменений результатов команд

Анализ трафика проходящего через хост

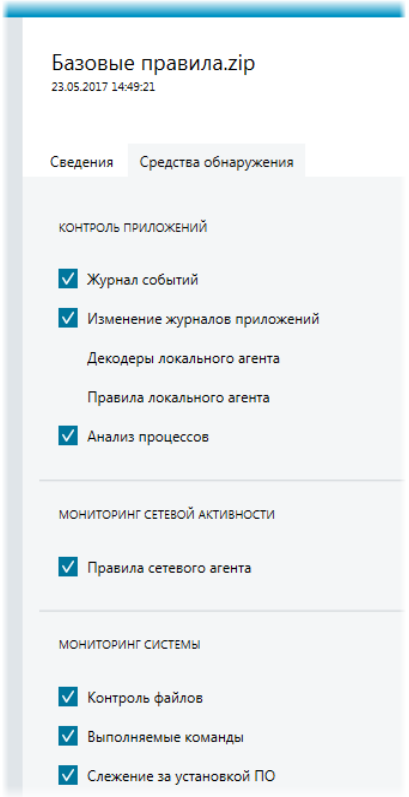
Архитектура

- 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

Особенности реализации агента

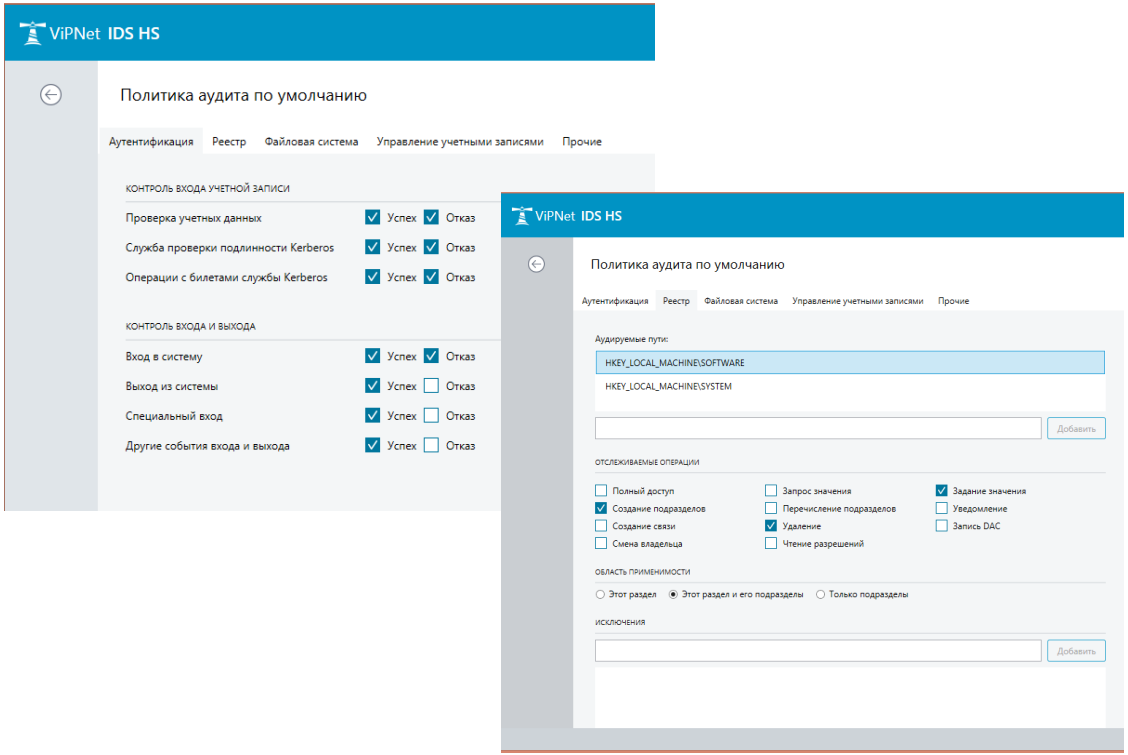
Агент ViPNet IDS HS состоит из двух частей:

- Сетевой агент – осуществляет мониторинг за сетью
- Агент уровня ОС – осуществляет мониторинг за событиями внутри операционной системы



Политики аудита

В 2018 году удалось существенно расширить политики аудита



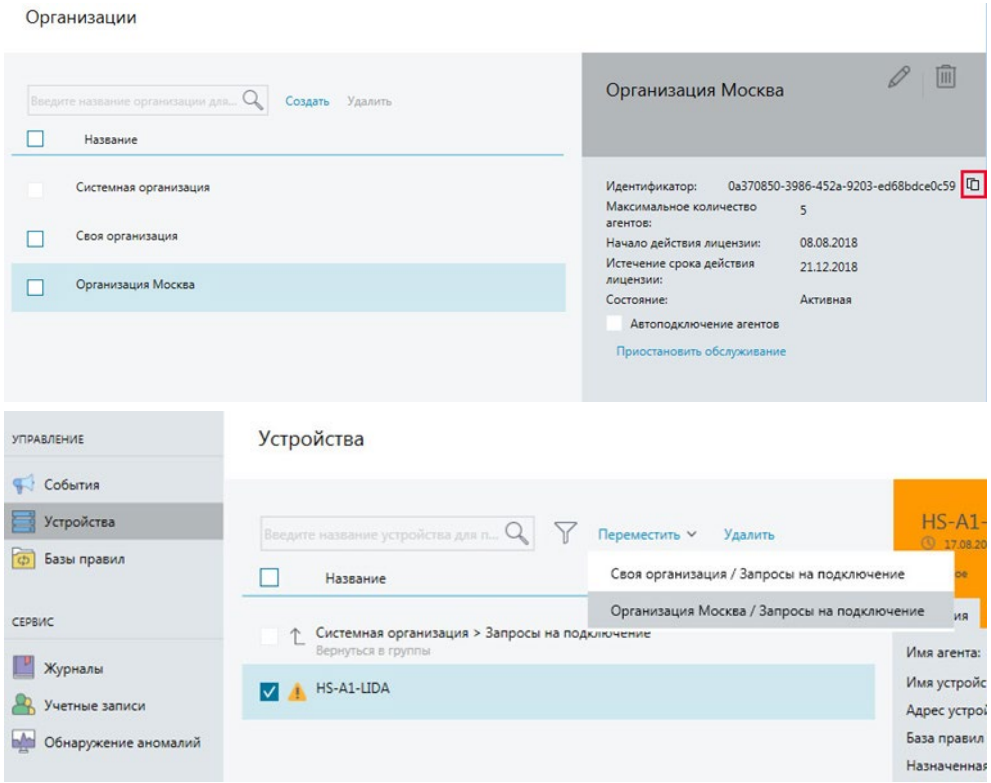
Мультиарендность

В 2018 удалось реализовать режим Мультарендности (multitenancy)

Мультиарендность

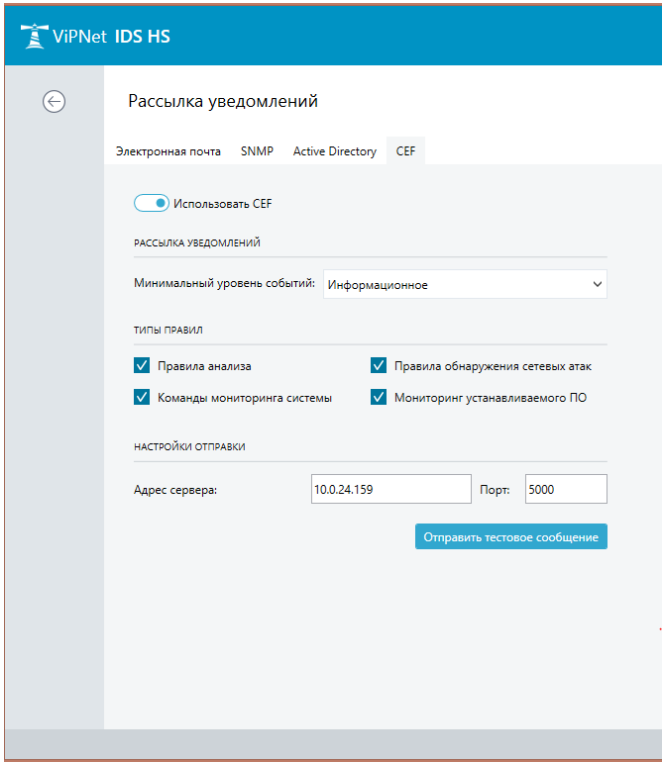
Теперь Сервер можно переключить в режим мультиарендности

Агентов подключать к организации

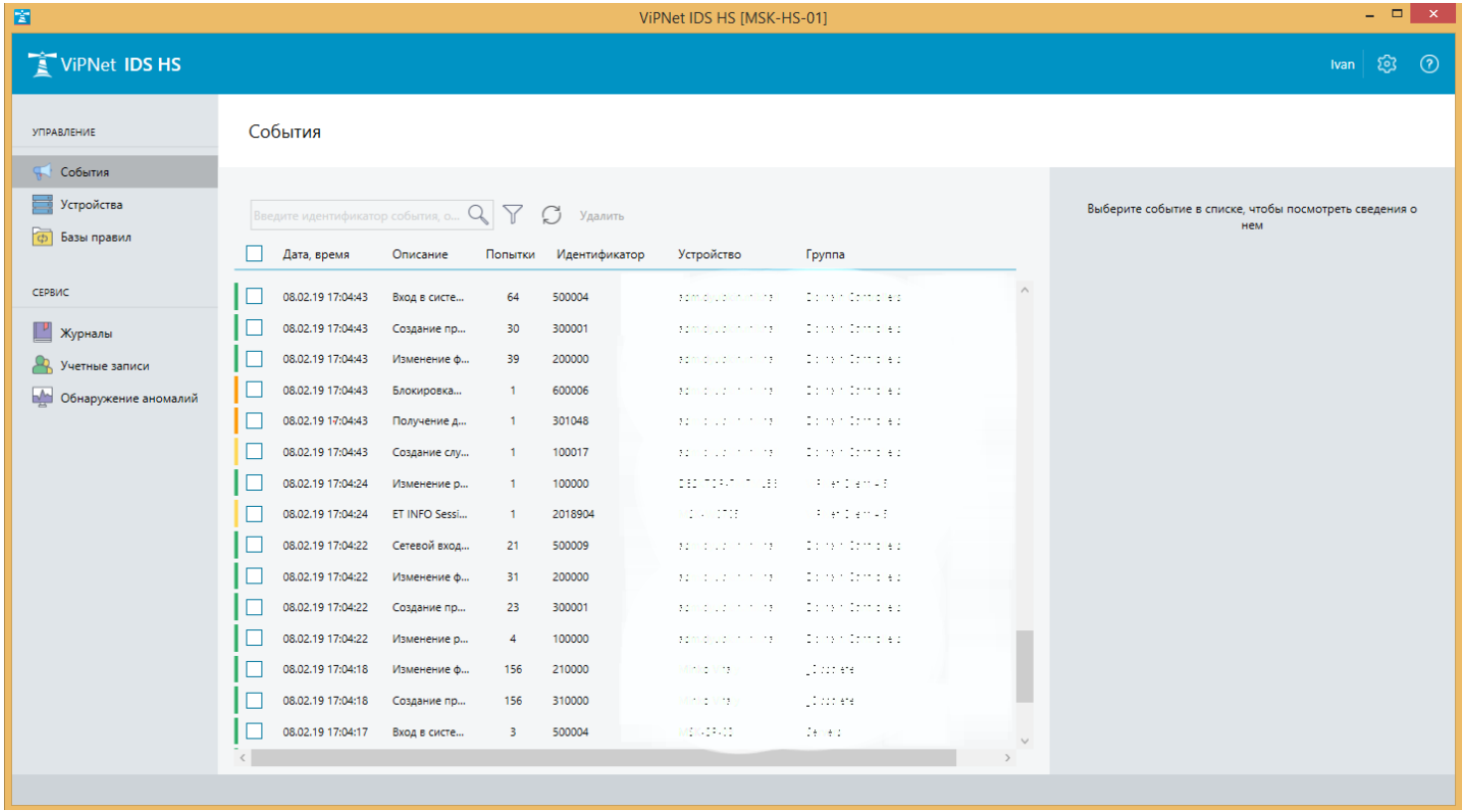


Передача данных

Передача данных по syslog в формате CEF



Реальная эксплуатация



Поддерживаемые ОС

- Семейство операционных систем Windows
- AstraLinux 1.5 релиз «Смоленск» (только агент)
- Debian 8 (только агент)
- AltLinux 7.0 СПТ (только агент)
- CentOS 7.5 (только агент)

Сертифицировано

- Сертификат ФСТЭК России по требованиям к системам обнаружения вторжения уровня узла 4 класса.
- Список мер из приказов 17,21,31:

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) - техническое заключение от 23.05.2017, экспертного заключения от 29.08.2017 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 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.

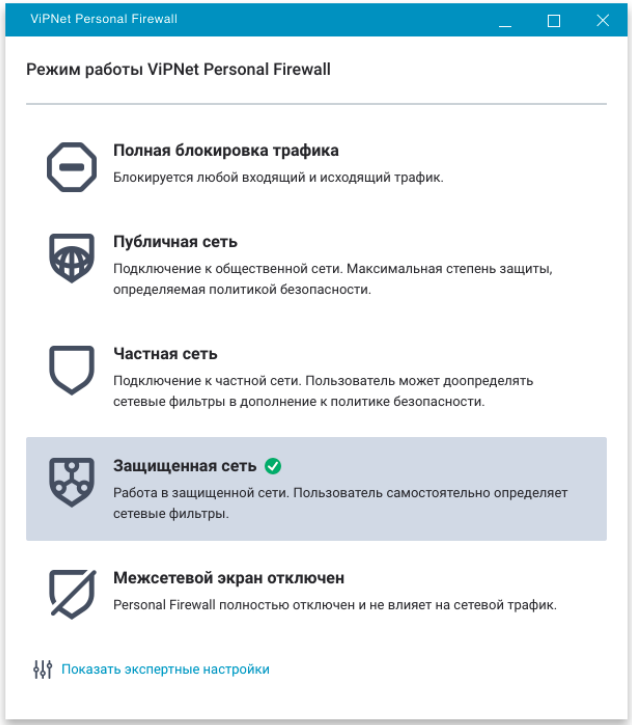
Что запланировано на 2019 г.

- Выполнение требований ФСБ и подача на сертификацию по требованиям СОА В (ТЗ уже согласовано)
- Получение событий от сертифицированных антивирусов
- Контроль обновлений Windows
- Контроль директорий по маске
- Новый интерфейс
- Завершение ИК версии 1.3

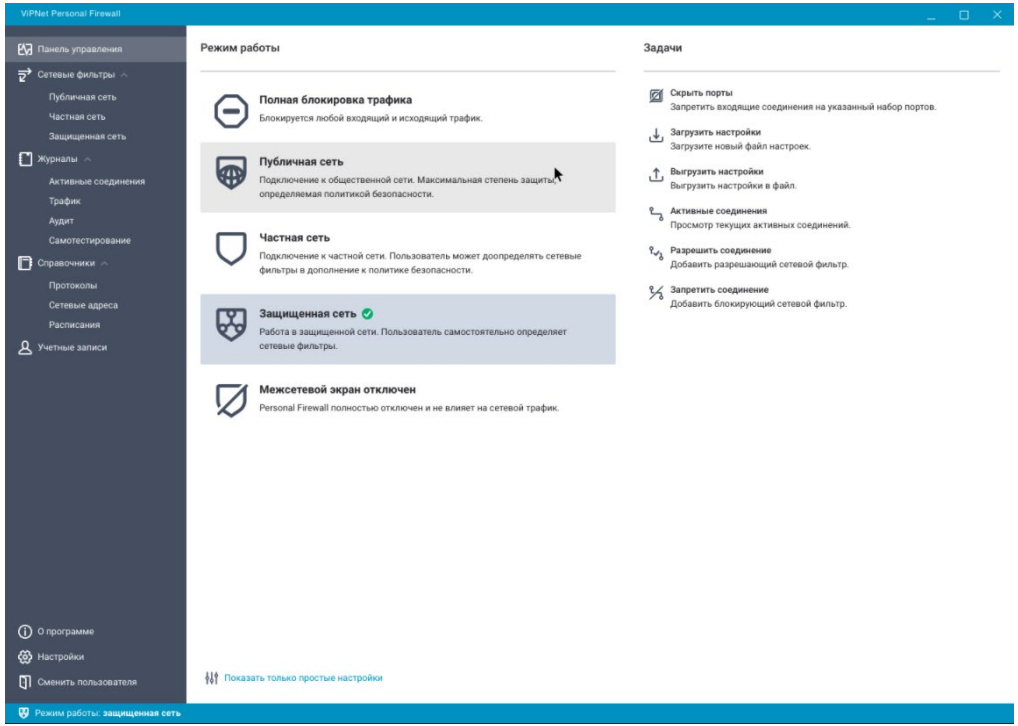
ViPNet Personal Firewall 4.5

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

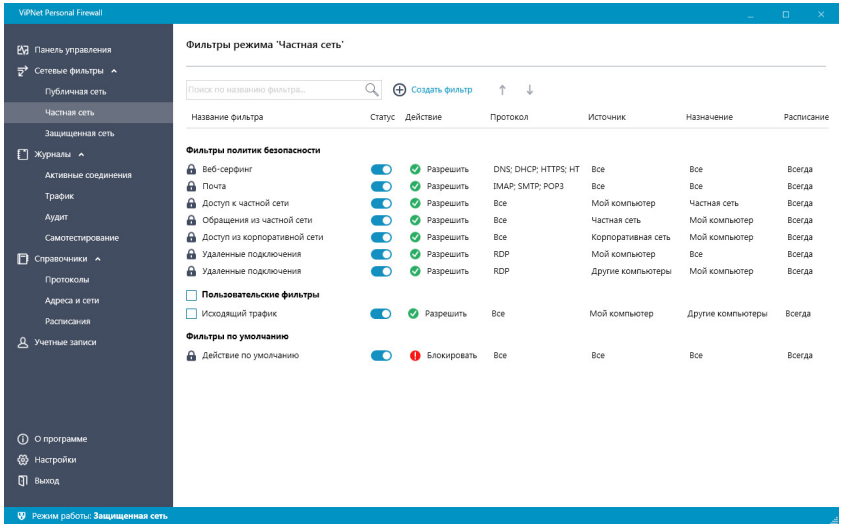


Режим пользователя

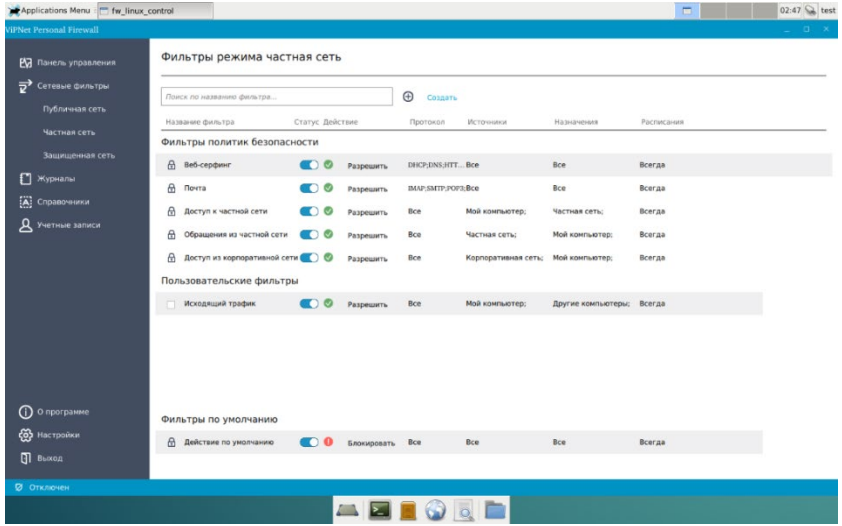


Режим администратора

И Windows и Linux



Windows

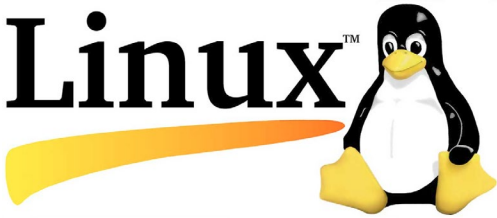


Linux

Список поддерживаемых ОС

- Windows 7
- Windows 8.1
- Windows 10

- Windows Server 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 8.7

Возможности

Фильтрация трафика (IPv4 и IPv6)

Преднастроенные сетевые фильтры:

- Публичная сеть
- Частная сеть
- Защищённая сеть

Контроль сетевой активности приложений

Работа сетевых фильтров по расписанию

Два режима работы

- Уровень пользователя
- Уровень администратора

Сертификация

- Ожидаем сертификат – Межсетевой экран тип «В» четвёртого класса
- Срок получения – Q2 2019 г


infotecs
Благодарю
за внимание!