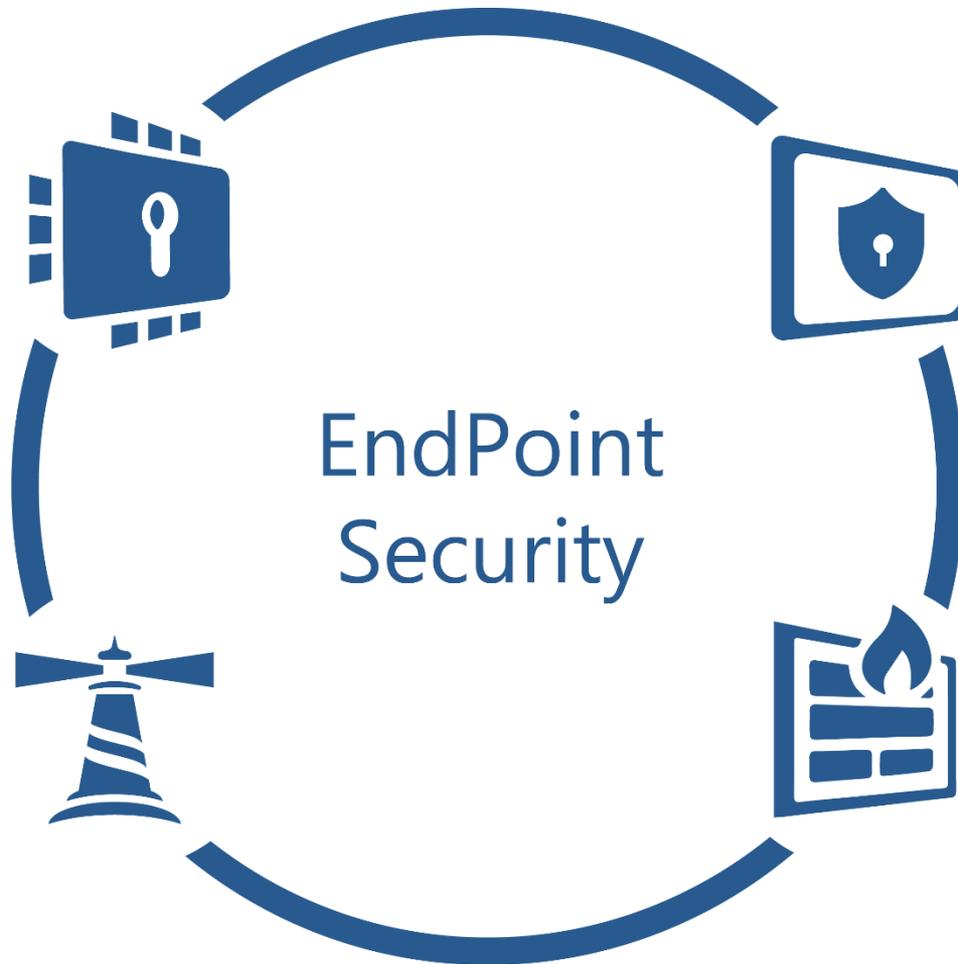


Обеспечение защиты рабочих станций и серверов

A decorative orange circle is partially visible on the right edge of the slide.



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

Организация доверенной загрузки

Контроль целостности

Разграничение
доступа

UEFI BIOS

MBR

Таблицы ACPI,
SMBIOS, карты
распределения
памяти

Файлов

CMOS

Двухфакторная
аутентификация

Журнал
Аудита

Сертифицировано



- Сертифицирован по требованиям руководящих документов к средствам доверенной загрузки уровня базовой системы ввода-вывода второго класса и возможность использования в ИСПДн до УЗ1 включительно и в ГИС до 1-го класса защищенности включительно
- Набор мер прописан в формуляре



Что нового в продукте ViPNet SafeBoot?



Выпуск официального релиза и прохождение инспекционного контроля версией 1.4



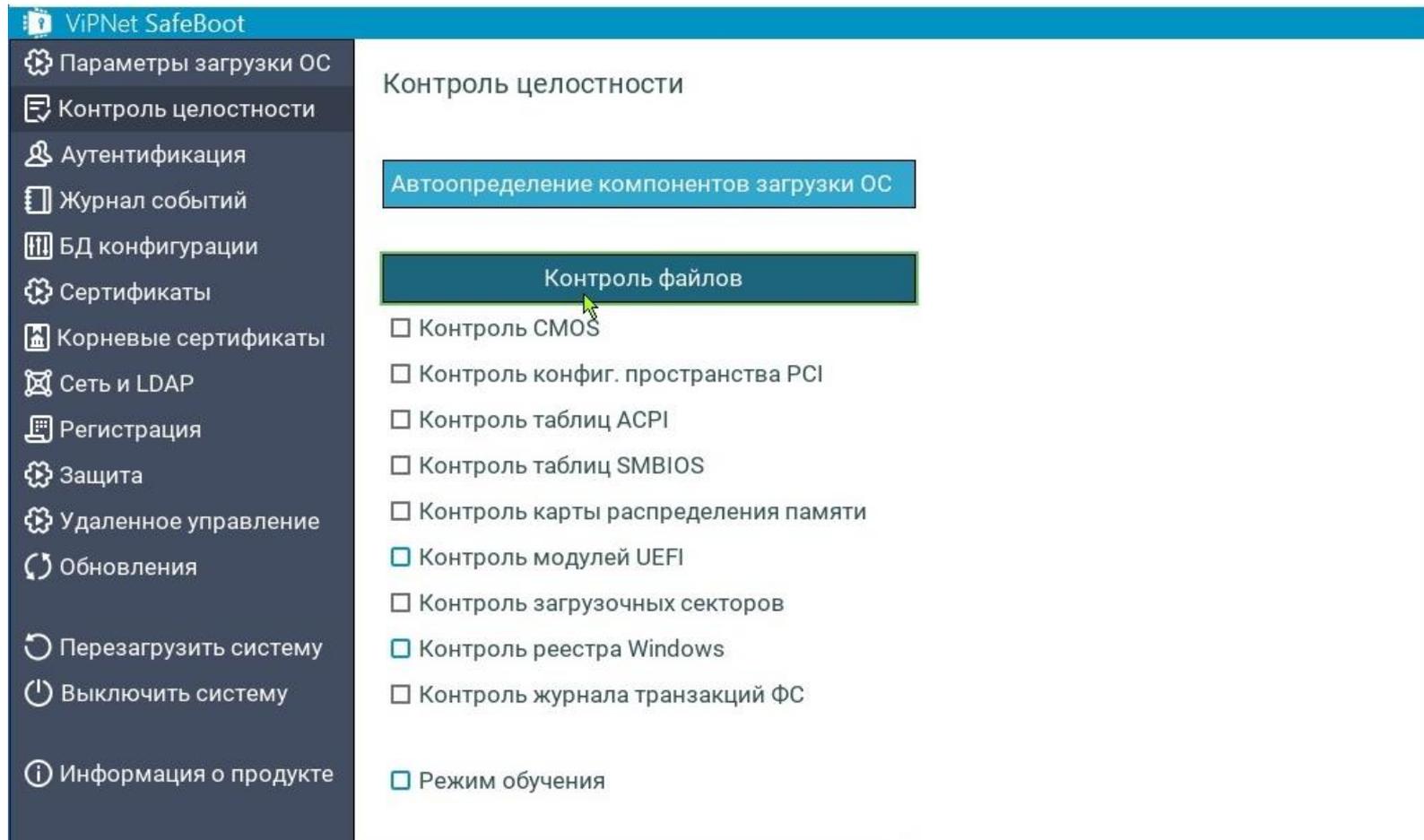
- Поддержка JaCarta-2 ГОСТ
- Лицензирование по «ключу»
- Режим неактивности - ключевая возможность, направленная на удобство OEM-поставки
- Поддержка авторизации по западным сертификатам

ViPNet SafeBoot 2.0

- Новый графический интерфейс
- Защита на уровне SMM
- Поддержка новых чипсетов и платформ

Передана на сертификацию

Новый интерфейс



The screenshot displays the ViPNet SafeBoot configuration interface. The left sidebar contains a list of menu items, with 'Контроль целостности' (Integrity Control) selected. The main content area is titled 'Контроль целостности' and features a sub-section 'Автоопределение компонентов загрузки ОС' (Automatic OS component detection). Below this, the 'Контроль файлов' (File Control) section is highlighted, showing a list of checkboxes for various system components.

ViPNet SafeBoot

- Параметры загрузки ОС
- Контроль целостности
- Аутентификация
- Журнал событий
- БД конфигурации
- Сертификаты
- Корневые сертификаты
- Сеть и LDAP
- Регистрация
- Защита
- Удаленное управление
- Обновления
- Перезагрузить систему
- Выключить систему
- Информация о продукте

Контроль целостности

Автоопределение компонентов загрузки ОС

Контроль файлов

- Контроль CMOS
- Контроль конфиг. пространства PCI
- Контроль таблиц ACPI
- Контроль таблиц SMBIOS
- Контроль карты распределения памяти
- Контроль модулей UEFI
- Контроль загрузочных секторов
- Контроль реестра Windows
- Контроль журнала транзакций ФС

- Режим обучения



ViPNet SafePoint

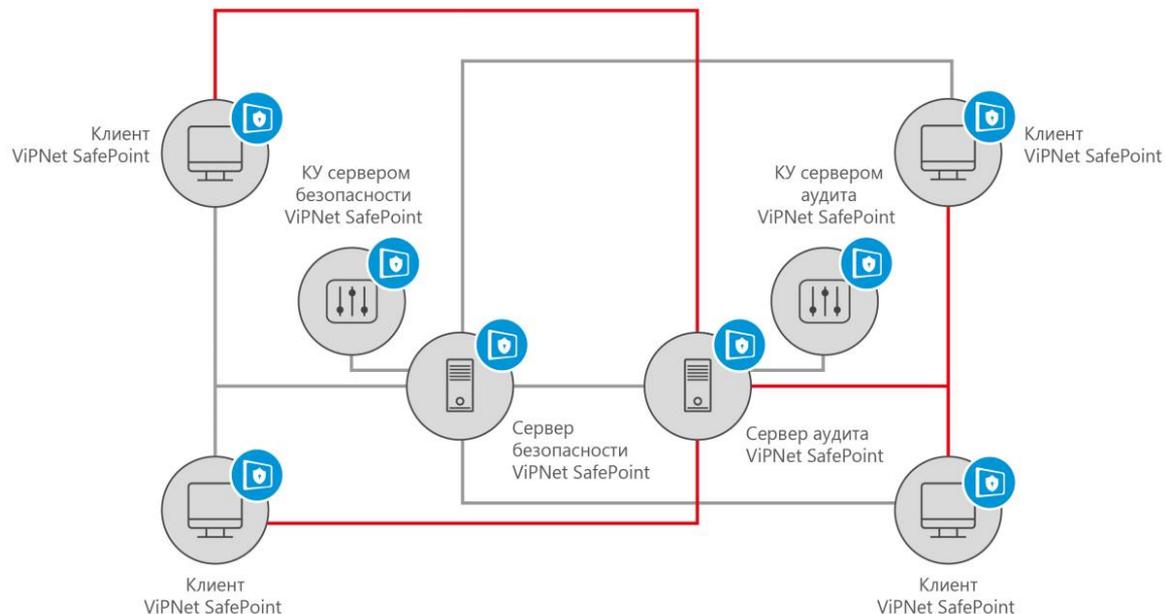
Новый продукт
в линейке
EndPoint Security



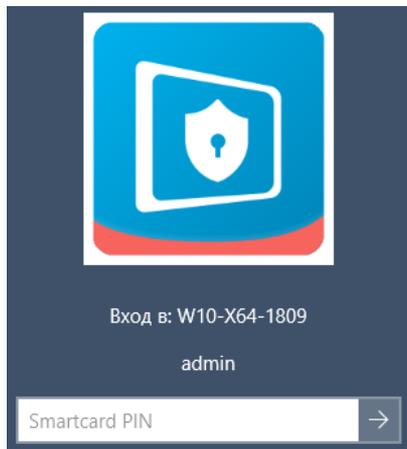
Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации. Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

Архитектура

- Клиент - ПО, устанавливаемое на рабочие станции и сервера, обеспечивает все заявленные защитные механизмы
- Сервер безопасности - необходим для управления клиентской частью, рассылки политик защиты
- Сервер аудит - необходим для просмотра записей событий аудита в реальном времени



Идентификация и аутентификация пользователей при вход в систему

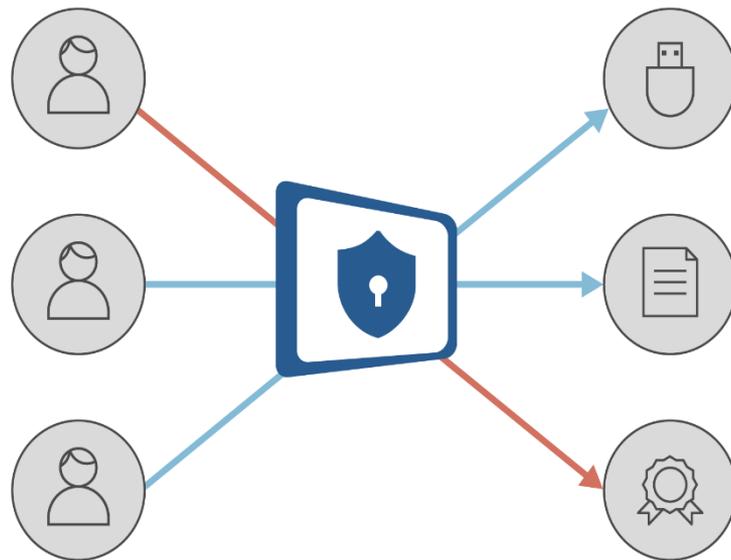


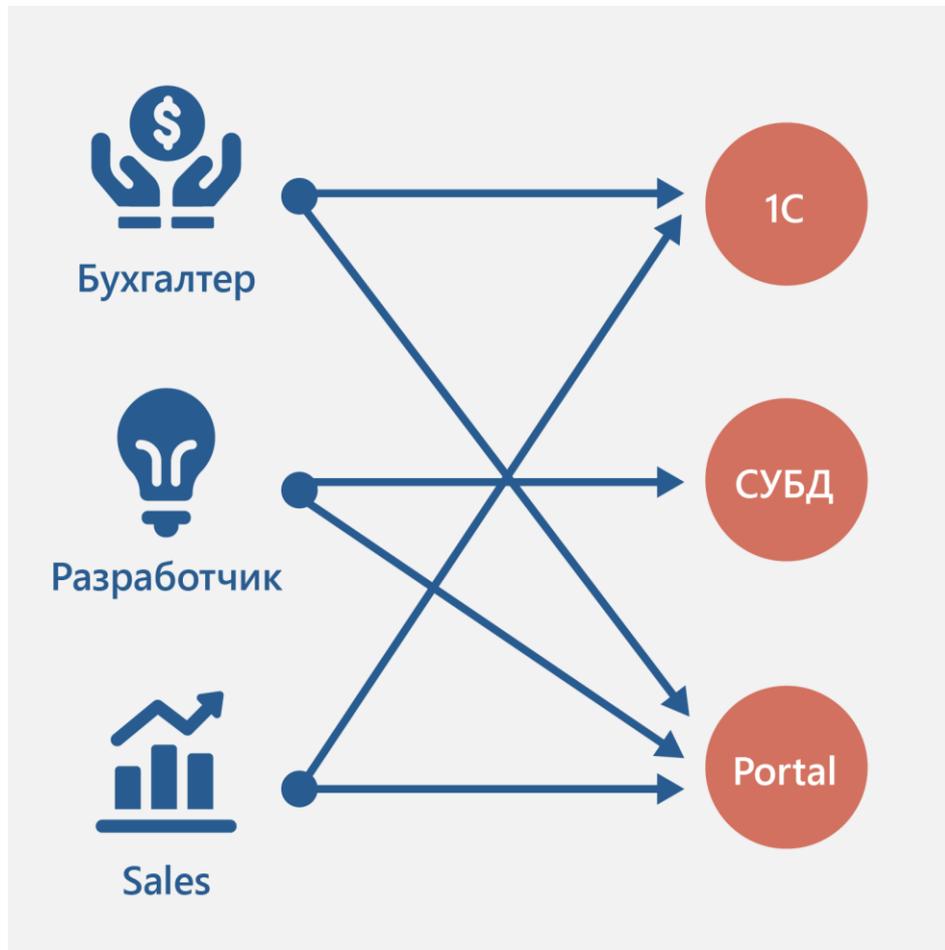
- Двухфакторная аутентификация пользователей
- Поддержка USB-токенов и смарт-карт:
 - JaCarta ГОСТ
 - JaCarta PKI
 - JaCarta LT
 - Rutoken S
 - Rutoken Lite
 - Rutoken ЭЦП

Дискреционный контроль доступа

Разграничительная политика на основе матрицы доступа

- ФС (вкл. сменные)
- прямой доступ к диску
- реестр
- принтеры
- службы
- устройства
- буфер обмена
- виртуальные машины

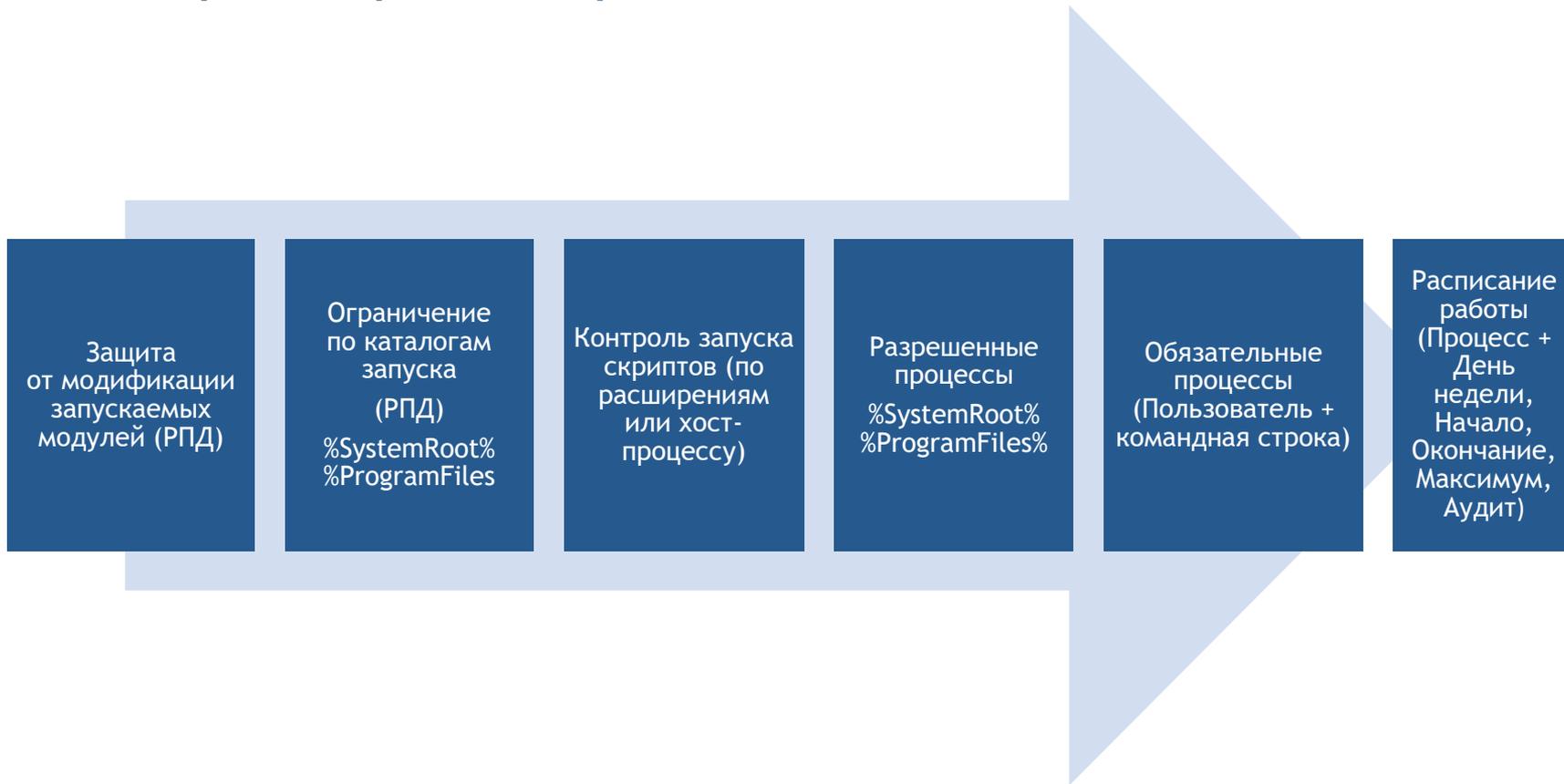




Мандатный контроль доступа пользователей и процессов

Разграничительная политика на основе меток безопасности

Замкнутая программная среда и контроль времени работы



USB,
SATA/ATA/ATAPI,
PCMCIA,
CD/DVD/BD, SD

COM, LPT, FIREWIRE,
IEEE 1284.4

Wi-Fi, Bluetooth,
MTP, сетевые
адаптеры,
модемы, смарт-
карты, ИК

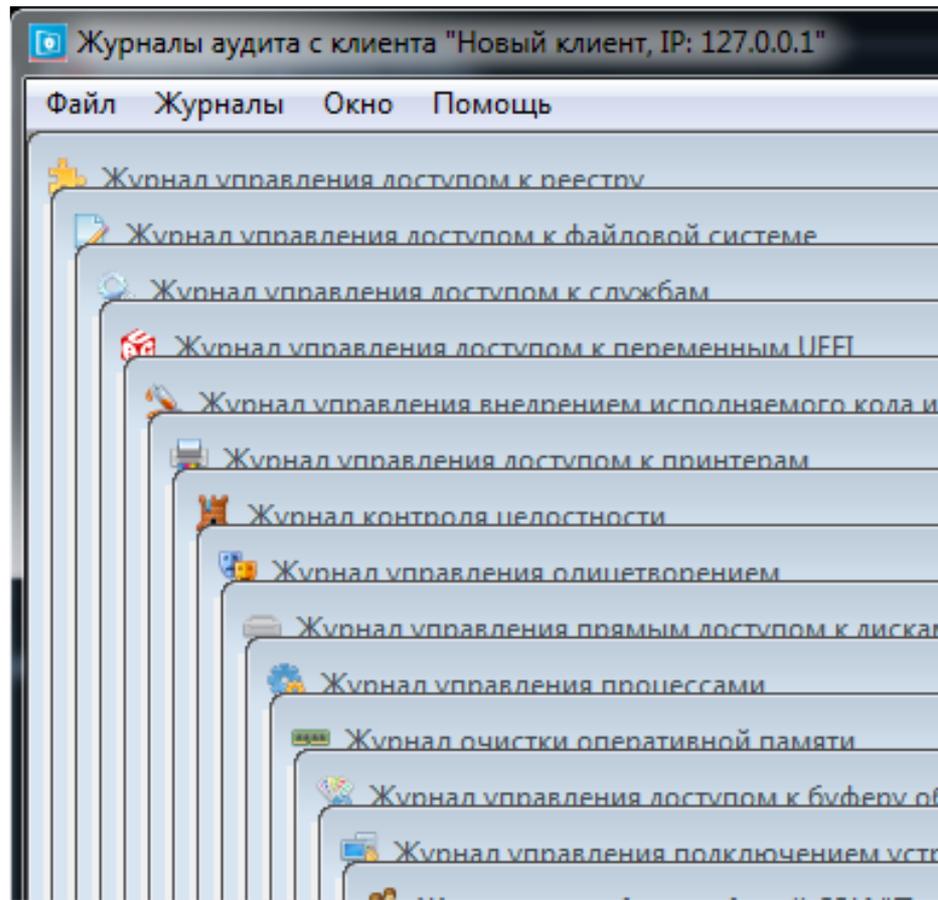
принтеры,
дисководы,
ленточные, любые
съёмные носители
и устройства Plug
and Play

Контроль устройств

- Контроль монтирования (подключения) и отключения
- При наличии файловой системы поддерживаются: Чтение, Запись, Исполнение, Удаление, Переименование
- Аудит этих событий

Аудит событий безопасности

Сервер аудита -
осуществляет
регистрацию событий
в реальном времени



Поддерживаемые ОС

- Microsoft Windows 10 (64-разрядная)
- Microsoft Windows 8.1 (64-разрядная)
- Microsoft Windows Server 2012 R2 (Standard или Datacenter)
- Microsoft Windows Server 2016 (Standard или Datacenter)



Ожидание по сертификации



Продукт будет передан на сертификацию по линии ФСТЭК России по требованиям к:

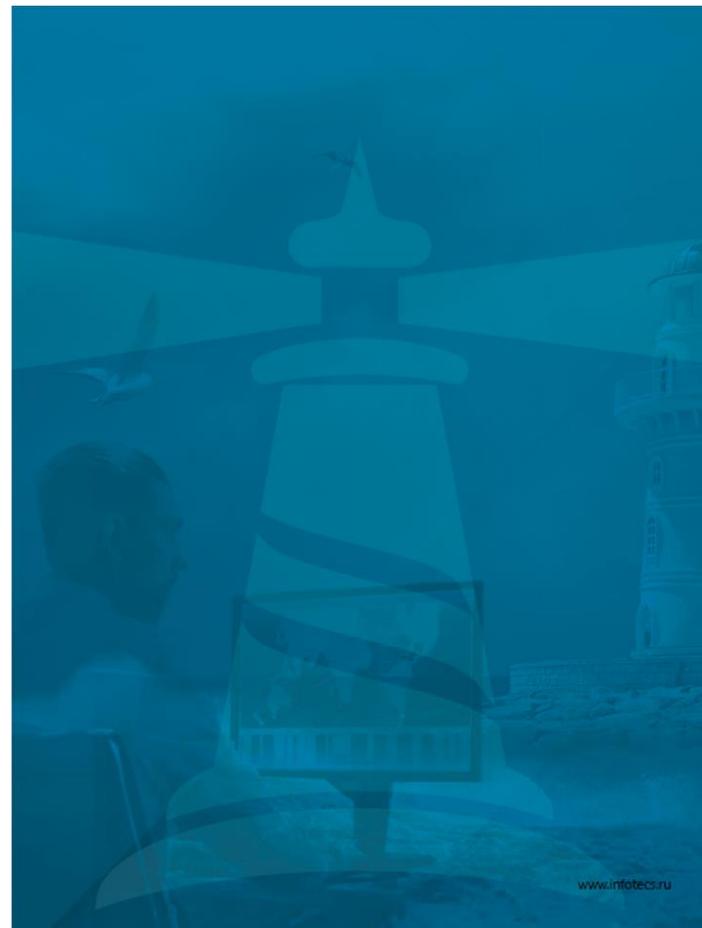
- 5 классу защищенности СВТ
- 4 классу защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 классу ТДБ



ViPNet IDS HS

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



Мониторинг файловой активности и реестра

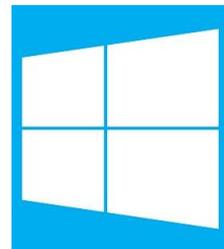
Результаты выполнения команд или изменений результатов команд



Анализ трафика проходящего через хост

Поддерживаемые ОС

- Семейство операционных систем Windows
- AstraLinux 1.5/ 1.6 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.0001.01БН00**

**СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3802**

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

Настоящий сертификат удостоверяет, что система обнаружения вторжений VFPNet IDS HS, разработанная и произведенная ОАО «ИнфоТекс» в соответствии с техническими условиями ФФКЕ.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 ИТЕСОБ.У4.123» (ФСТЭК России, 2012).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦНИ» (аттестат аккредитации от 11.04.2016 № СМ И.0001.01БН00.0004) - техническое заключение от 23.05.2017, испытательного заключения от 29.08.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СМ И.0001.01БН00.А002).

Заявитель: ОАО «ИнфоТекс» (ИНН 770013790)
Адрес: 127287, г. Москва, Старый Петровский-Разумовский проезд, д.1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркирования знаков соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЦНИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



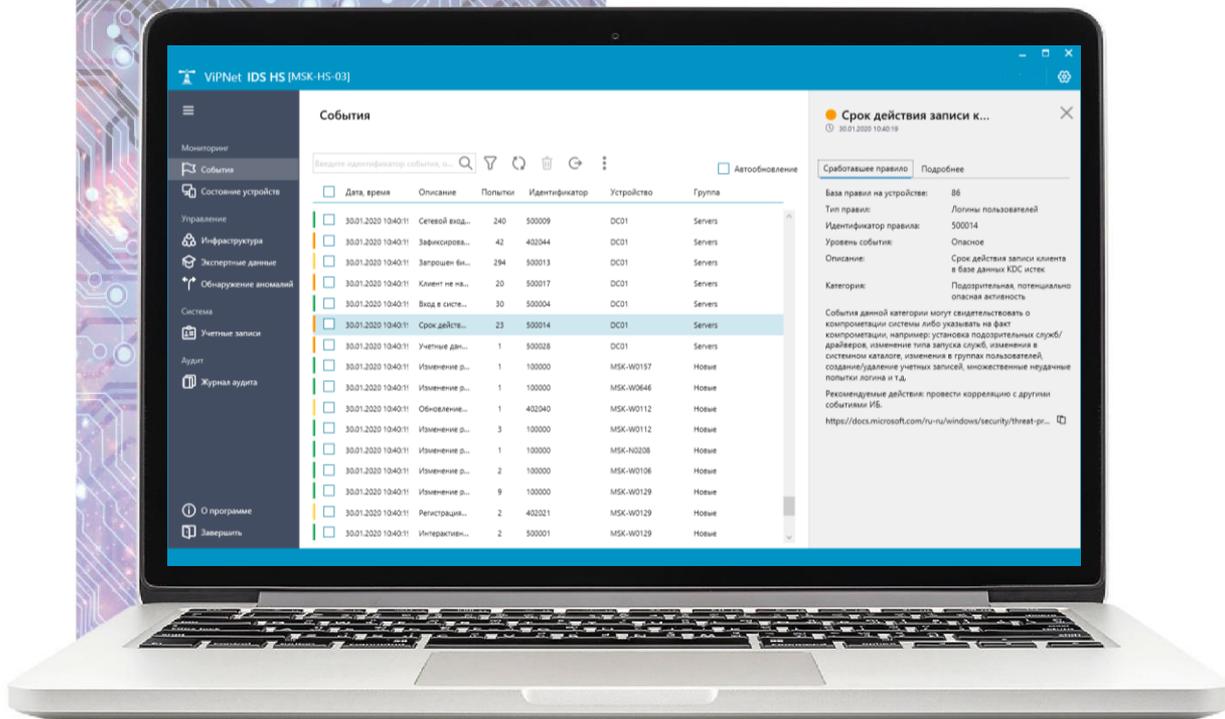

В. Люткин

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

Что нового было за 2019 год



- Поддержка ОС Astra Linux Special Edition 1.6 релиз «Смоленск»
- Регистрация событий об обнаруженных вирусах на рабочих станциях
- Обнаружение активности вредоносной программы RemSec
- Расширение списка алгоритмов для получения контрольной суммы файлов - MD5, SHA256 и SpamSum
- Отслеживание установки системных обновлений ОС Windows
- Возможность выгрузки событий по протоколу syslog на несколько серверов SIEM (в т.ч. и ViPNet TIAS)
- Новый дизайн интерфейса консоли управления ViPNet IDS HS



Текущая
официальная
версия
ViPNet IDS HS 1.5.

Передана на
сертификацию
для продления
сертификата



ViPNet Personal Firewall 4.5



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.



ViPNet Personal Firewall

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

И Windows и Linux

VIPNet Personal Firewall

Панель управления

Сетевые фильтры

Публичная сеть

Частная сеть

Защищенная сеть

Журналы

Активные соединения

Трафик

Аудит

Самотестирование

Справочники

Протоколы

Адреса и сети

Расписания

Учетные записи

О программе

Настройки

Выход

Режим работы: Защищенная сеть

Фильтры режима "Частная сеть"

Поиск по названию фильтра...

Создать фильтр

Название фильтра	Статус	Действие	Протокол	Источник	Назначение	Расписание
Фильтры политик безопасности						
Веб-серфинг	Включено	Разрешить	DNS; DHCP; HTTPS; HT	Все	Все	Всегда
Почта	Включено	Разрешить	IMAP; SMTP; POP3	Все	Все	Всегда
Доступ к частной сети	Включено	Разрешить	Все	Мой компьютер	Частная сеть	Всегда
Обращения из частной сети	Включено	Разрешить	Все	Частная сеть	Мой компьютер	Всегда
Доступ из корпоративной сети	Включено	Разрешить	Все	Корпоративная сеть	Мой компьютер	Всегда
Удаленные подключения	Включено	Разрешить	RDP	Мой компьютер	Все	Всегда
Удаленные подключения	Включено	Разрешить	RDP	Другие компьютеры	Мой компьютер	Всегда
Пользовательские фильтры						
Исходящий трафик	Включено	Разрешить	Все	Мой компьютер	Другие компьютеры	Всегда
Фильтры по умолчанию						
Действие по умолчанию	Включено	Блокировать	Все	Все	Все	Всегда

Applications Menu: fw_linux_control 02:47 test

VIPNet Personal Firewall

Панель управления

Сетевые фильтры

Публичная сеть

Частная сеть

Защищенная сеть

Журналы

Справочники

Учетные записи

О программе

Настройки

Выход

Отключен

Фильтры режима частная сеть

Поиск по названию фильтра...

Создать

Название фильтра	Статус	Действие	Протокол	Источники	Назначение	Расписание
Фильтры политик безопасности						
Веб-серфинг	Включено	Разрешить	HTTP; DNS; HTTPS; ...	Все	Все	Всегда
Почта	Включено	Разрешить	IMAP; SMTP; POP3; ...	Все	Все	Всегда
Доступ к частной сети	Включено	Разрешить	Все	Мой компьютер	Частная сеть	Всегда
Обращения из частной сети	Включено	Разрешить	Все	Частная сеть	Мой компьютер	Всегда
Доступ из корпоративной сети	Включено	Разрешить	Все	Корпоративная сеть	Мой компьютер	Всегда
Пользовательские фильтры						
Исходящий трафик	Включено	Разрешить	Все	Мой компьютер	Другие компьютеры	Всегда
Фильтры по умолчанию						
Действие по умолчанию	Включено	Блокировать	Все	Все	Все	Всегда

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

The logo for 'infotecs' features a red dot above the letter 'i', followed by a red curved line that arches over the letters 'f' and 'o'. The word 'infotecs' is written in a bold, blue, sans-serif font.

infotecs

A vertical red line that acts as a separator between the logo and the text.

Вопросы?



Спасибо
за внимание!