Обзор новых версий продуктов для защиты рабочих станций и серверов от компании ИнфоТеКС

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

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

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».

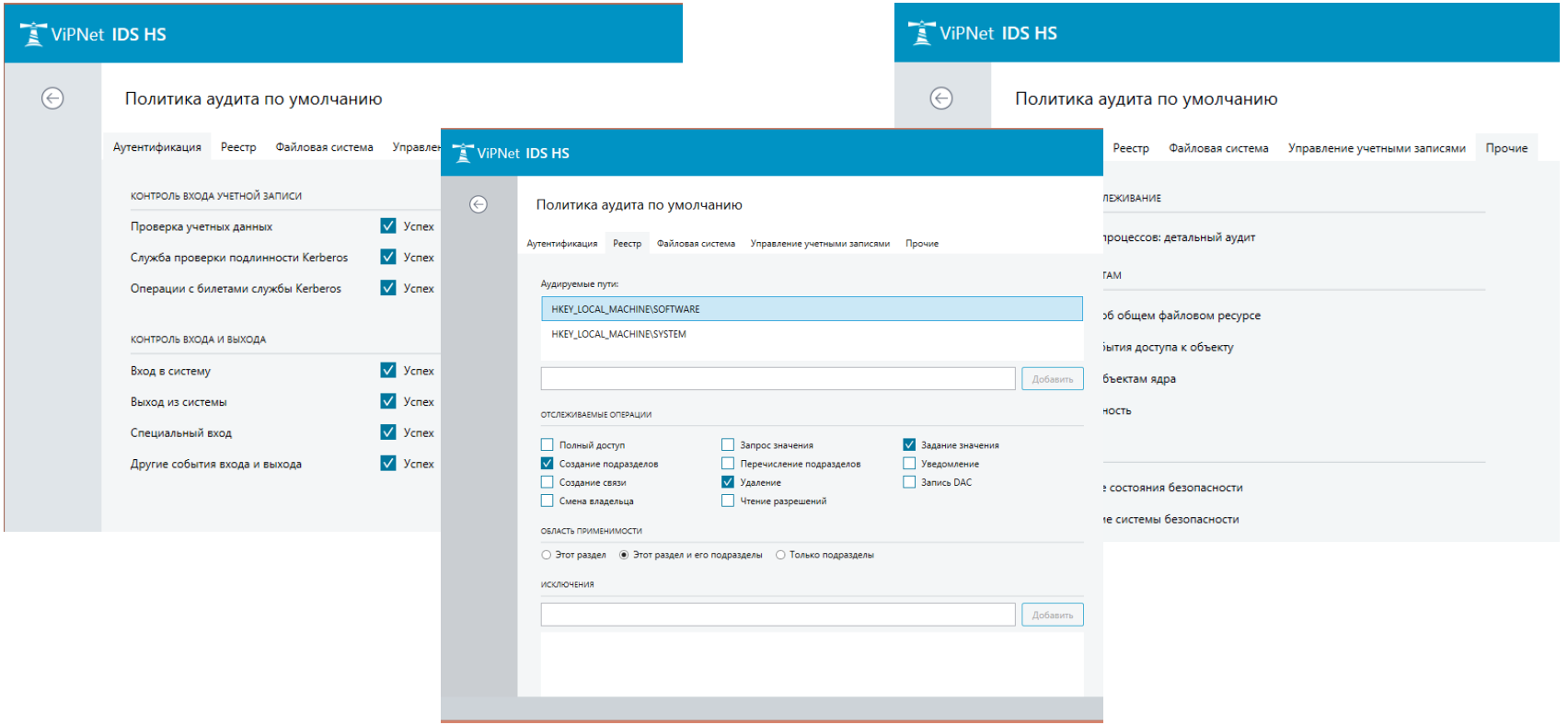
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

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

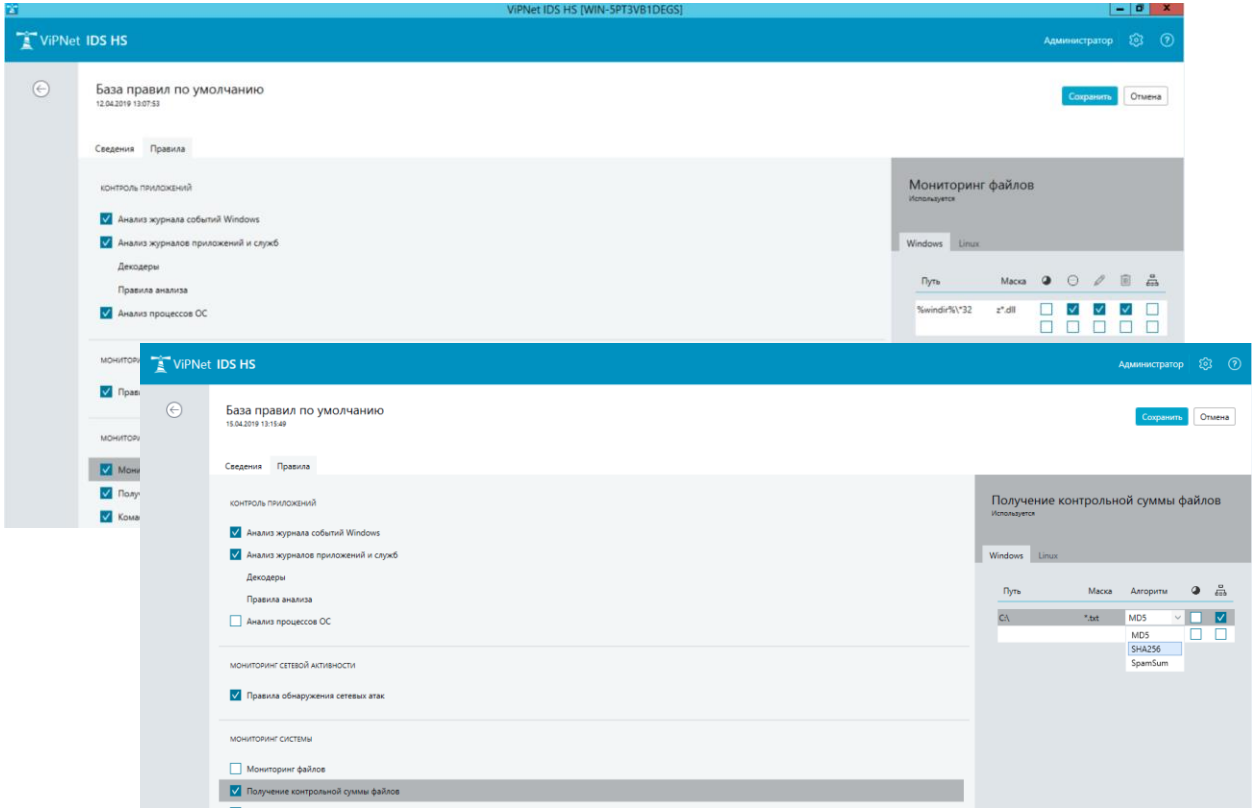
Что нового в ViPNet IDS HS версии 1.4?

Политики аудита

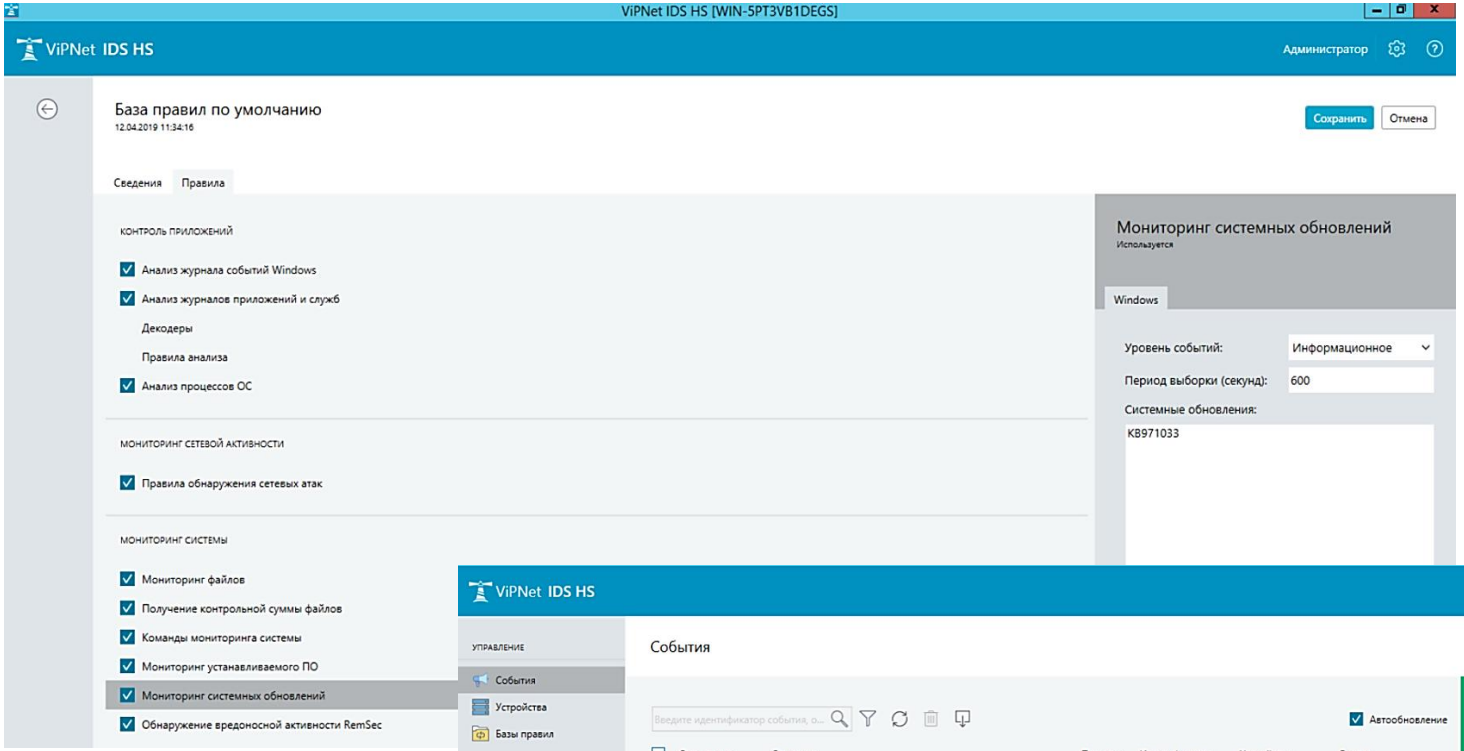


Мониторинг и ХЭШ MD5

- Контроль директорий по маске
- Расчёт КС файлов для дальнейшего анализа и сравнение с базой «зловредов»

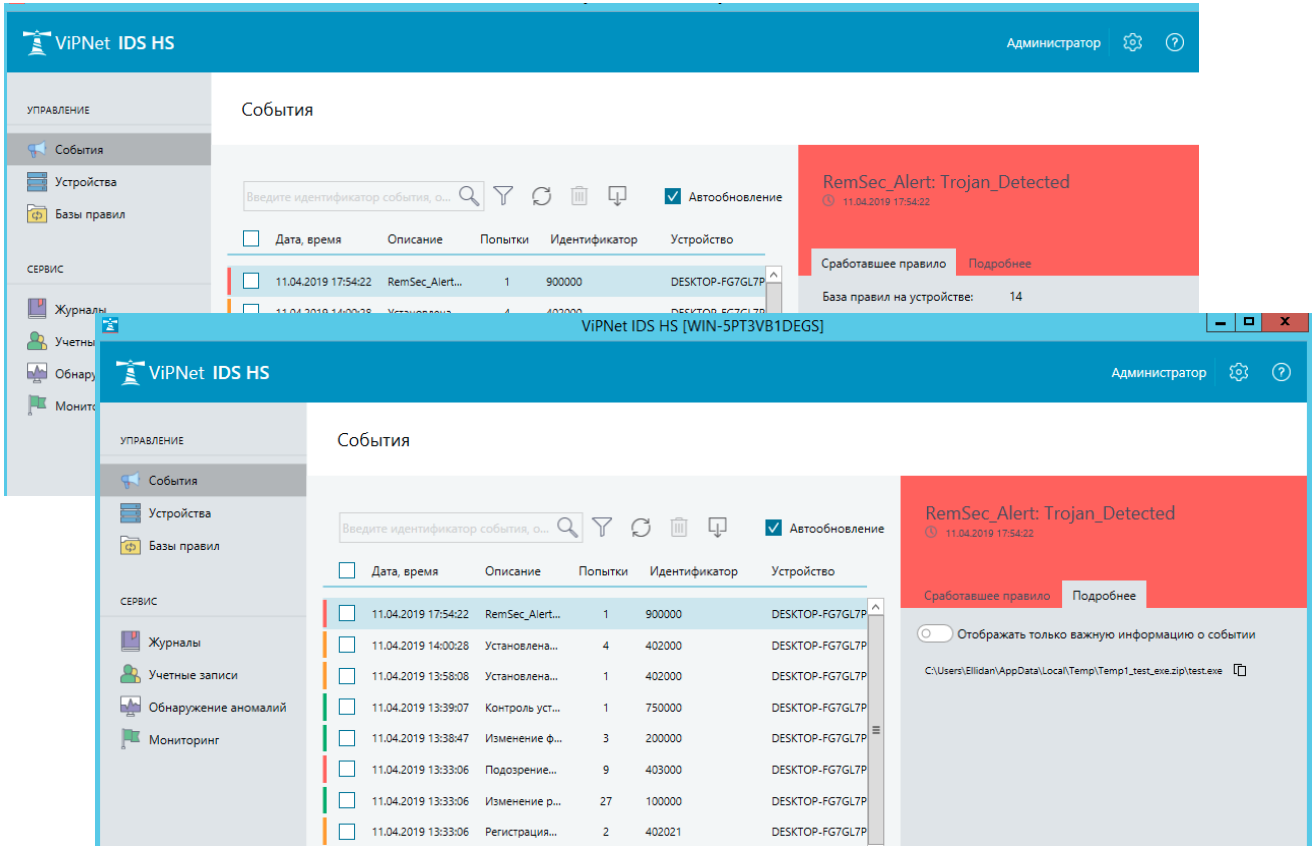


Контроль обновлений Windows



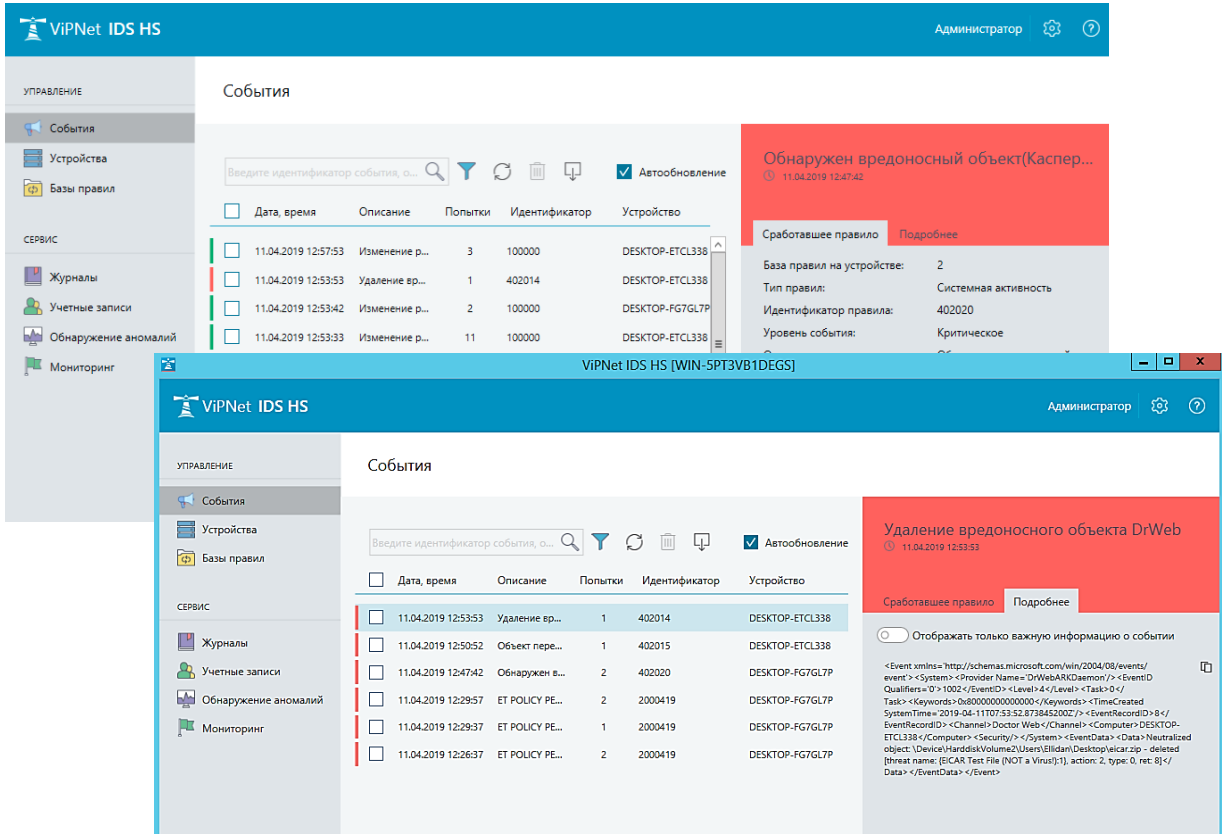
Remsec угрозы

Обнаружение RemSec угроз (трояны)



События от антивируса

Получаем информацию о вредоносных объектах от Антивируса Касперского и Dr. Web



Сертификация

- Находится на инспекционном контроле по линии ФСТЭК России
- Находится на сертификации в ФСБ от требованиям к СОА тип В

ViPNet SafeBoot

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 атакна сам BIOS

Решаемые задачи ViPNet SafeBoot

infotecs

Организация доверенной загрузки

Контроль целостности

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

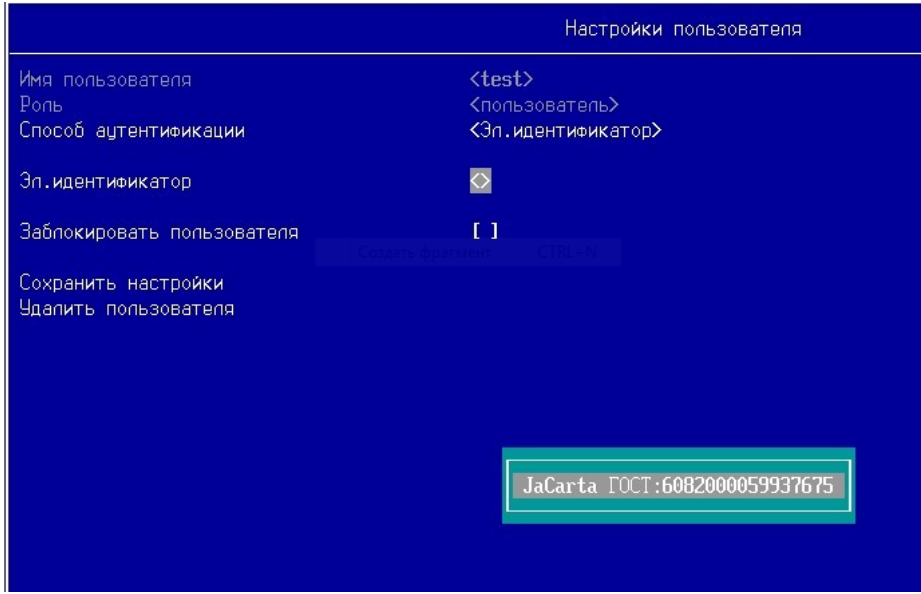
Разграничение доступа

- Двухфакторная аутентификация
- Токены: JaCarta Rutoken Guradant ID

Что нового в ViPNet SafeBoot версии 1.4?

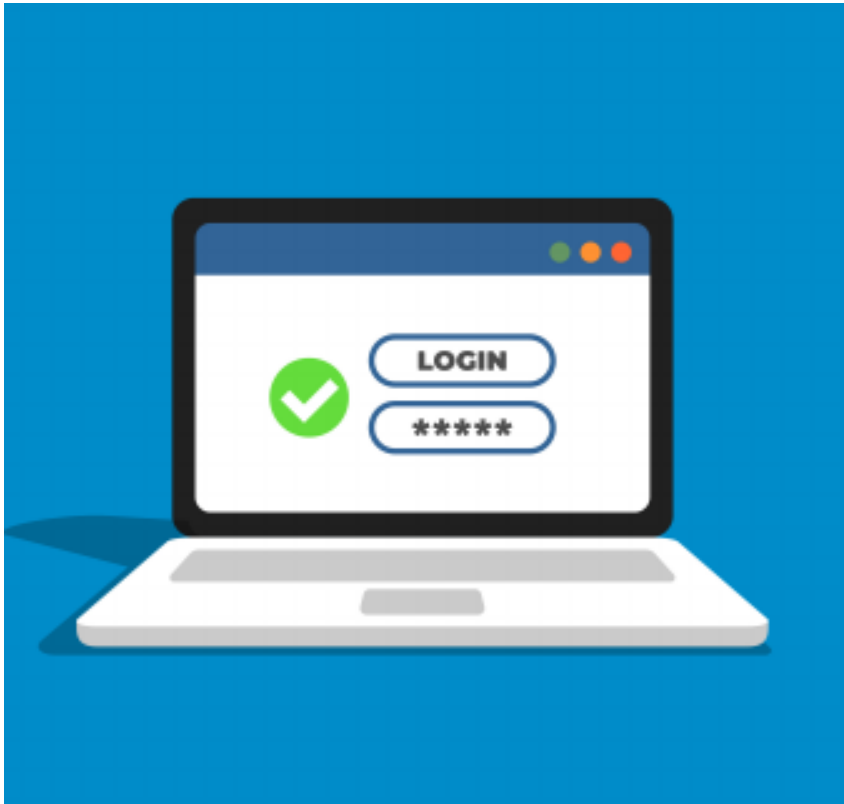
Поддержка JaCarta-2 ГОСТ

- Поддержка токена JaCarta-2 ГОСТ
- Возможность аутентификации в ViPNet SafeBoot по «сертификату ГОСТ»



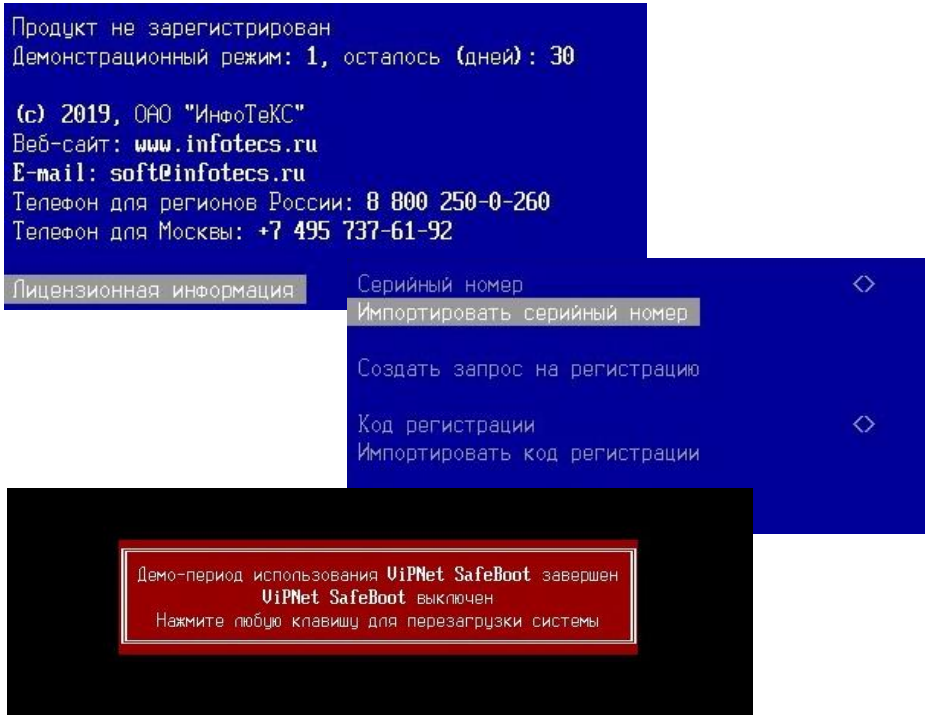
Аутентификация по западным сертификатам в AD

- Зачастую в компаниях развёрнут Microsoft CA
- Для аутентификации используются сертификаты выданные MS CA
- Для входа в SafeBoot или аутентификации на LDAP через SafeBoot имеется возможность использовать западные сертификаты выданные MS CA

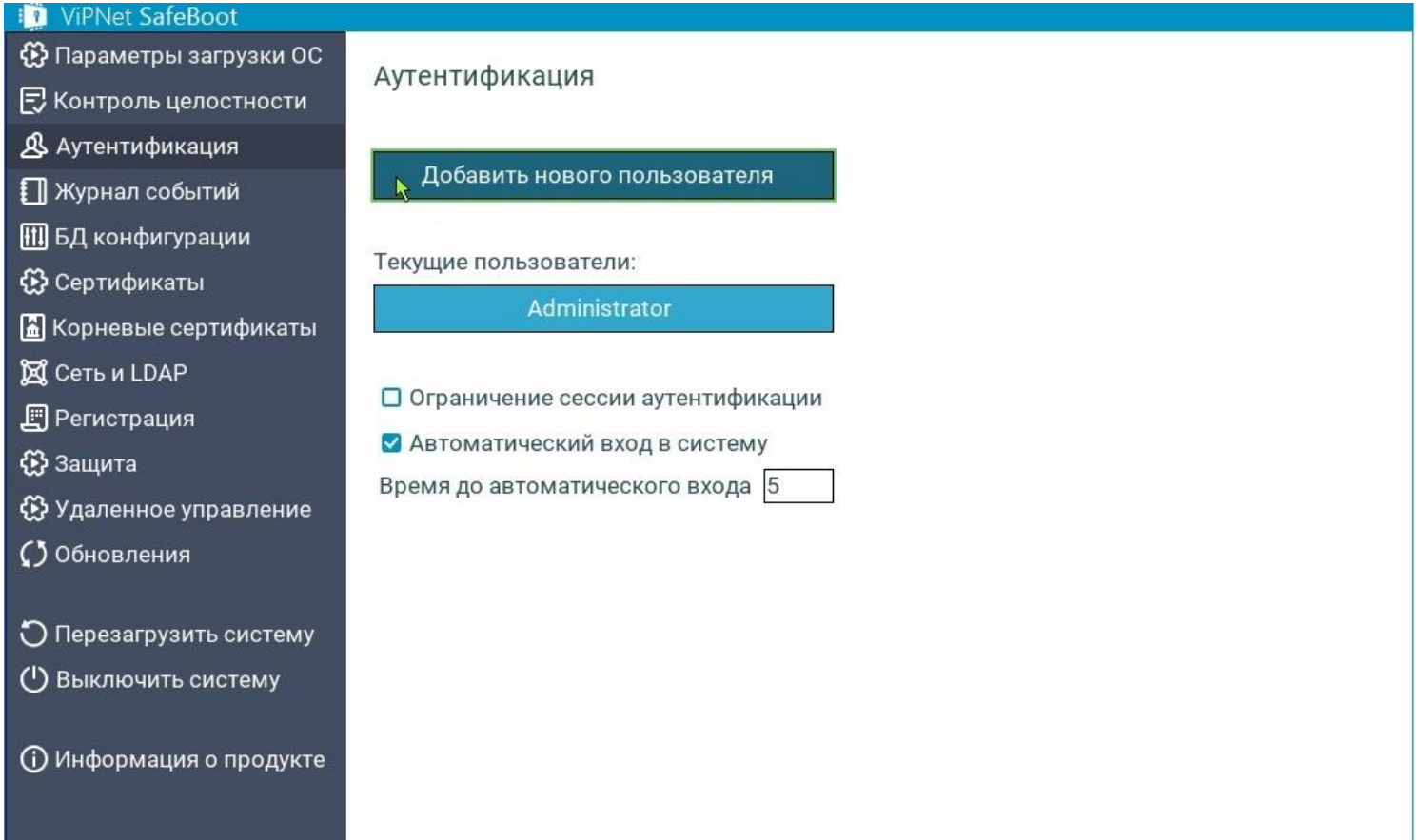


Режим неактивности

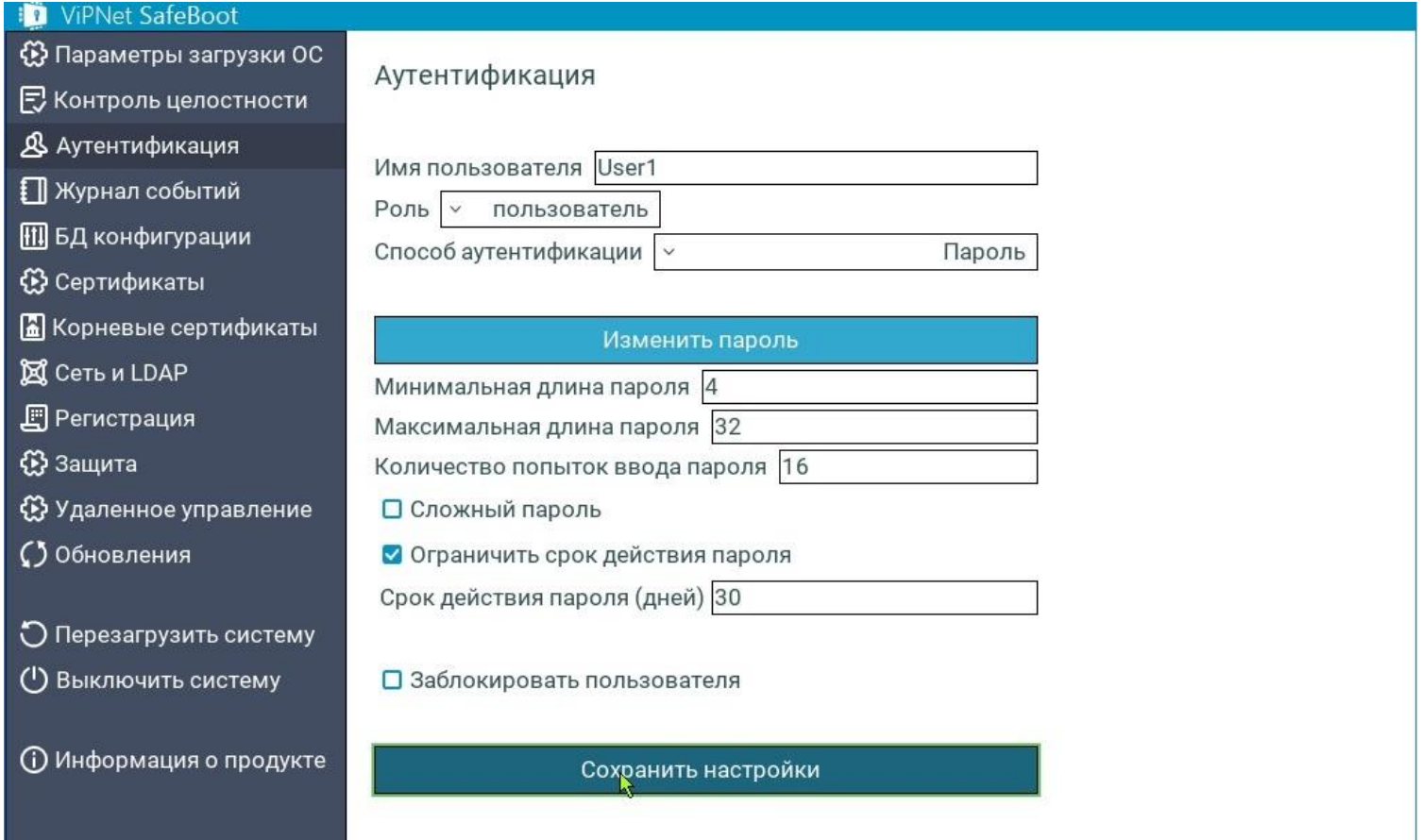
Режим неактивности – специализированная возможность средства доверенной загрузки (СДЗ) ViPNet SafeBoot для OEM поставок в составе платформ различных производителей



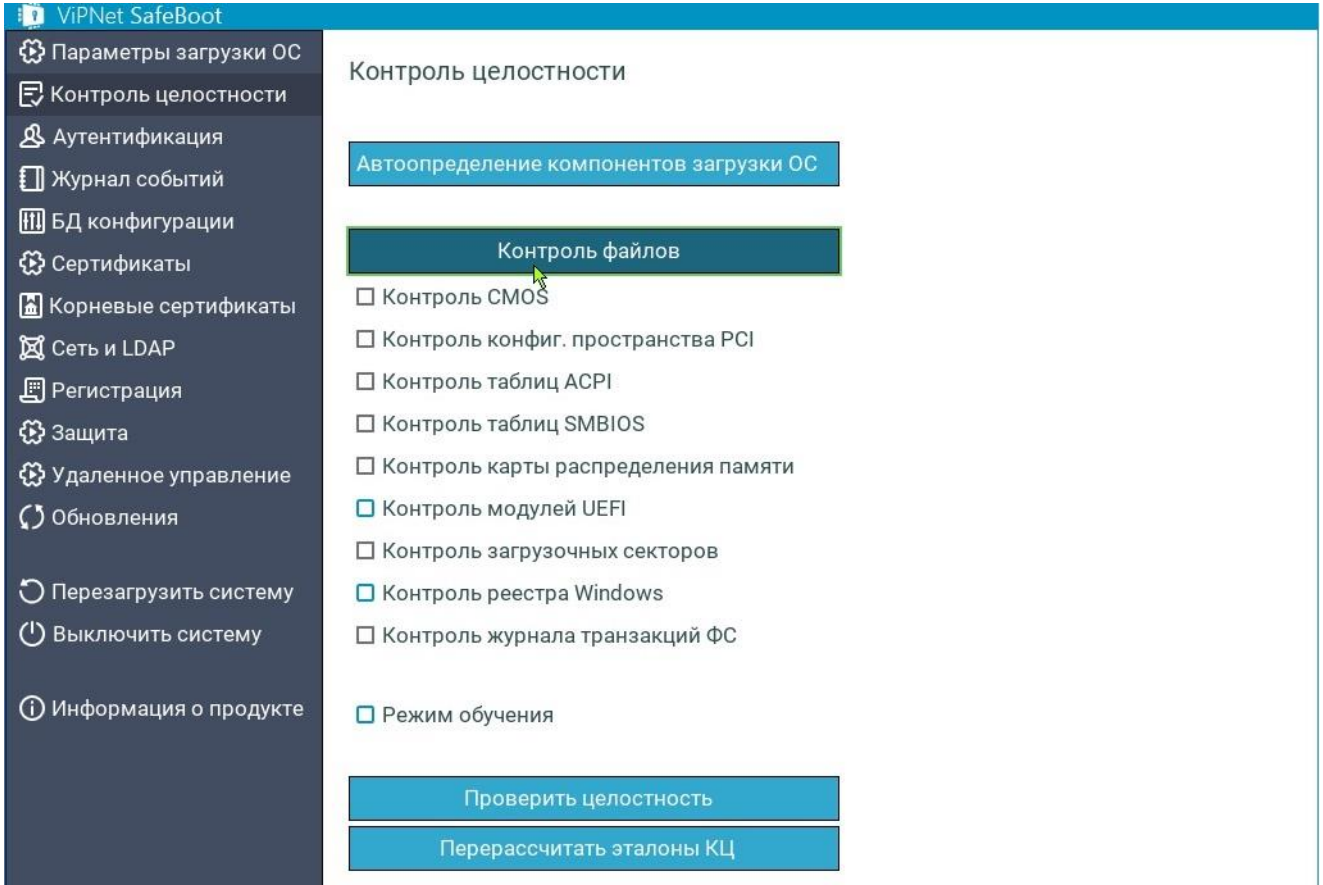
В ноябре обновлённый интерфейс!



В ноябре обновлённый интерфейс!



В ноябре обновлённый интерфейс!



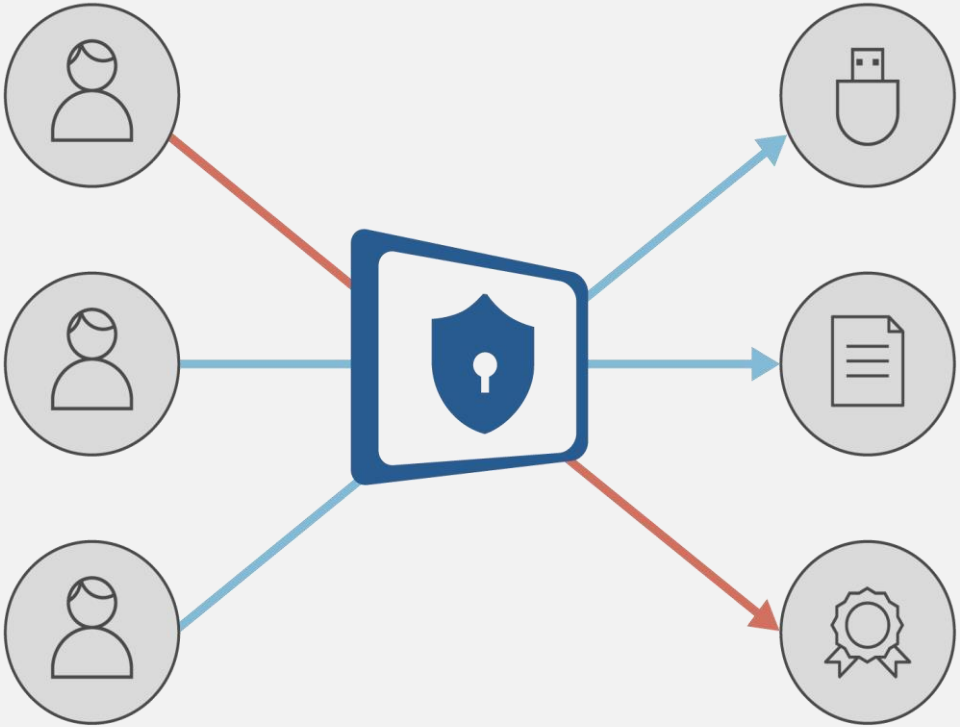
Что совсем новое!

ViPNet SafePoint

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.

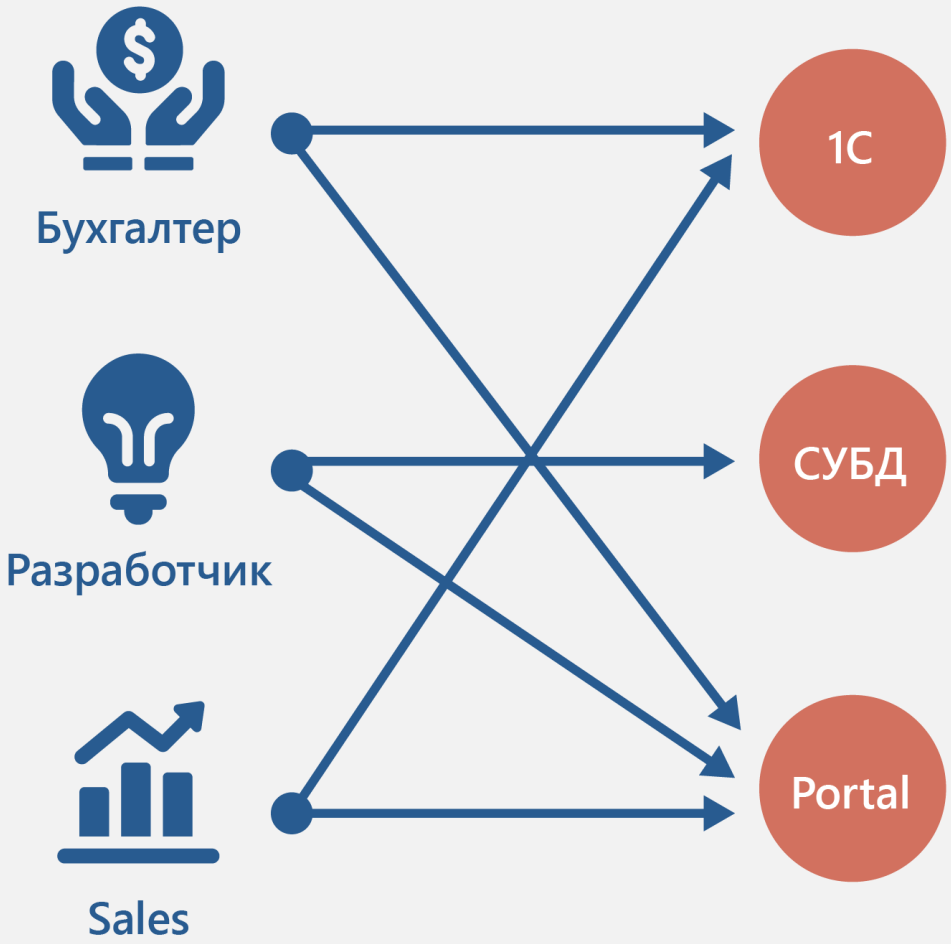
Идентификация и аутентификация

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



Дискреционный контроль доступа пользователей

Разграничительная политика
на основе матрицы доступа



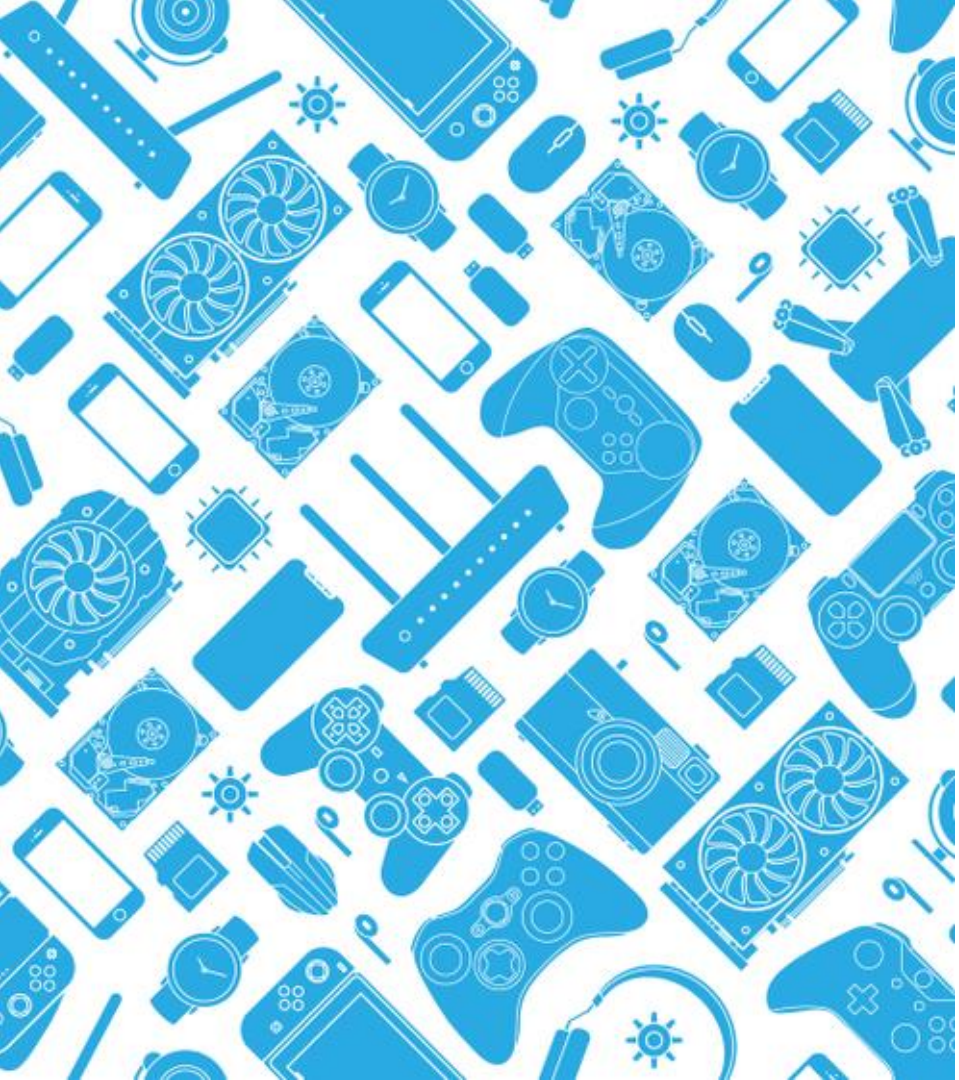
infotecs

Мандатный контроль доступа пользователей и процессов

Разграничительная политика
на основе меток безопасности

Замкнутая программная среда

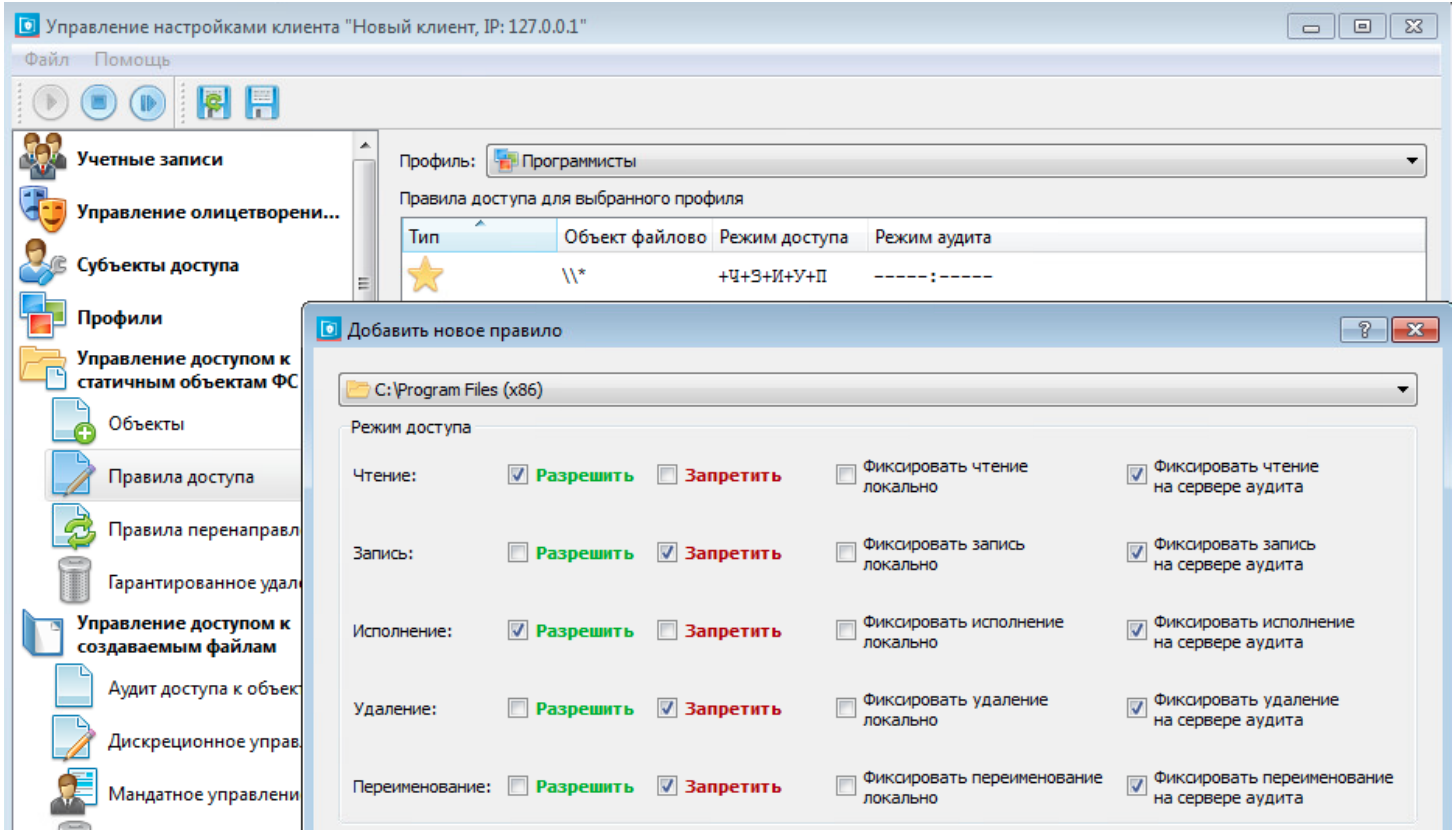
- Защита от модификации запускаемых модулей
- Контроль запуска скриптов Active Scripts
- Контроль запуска задач



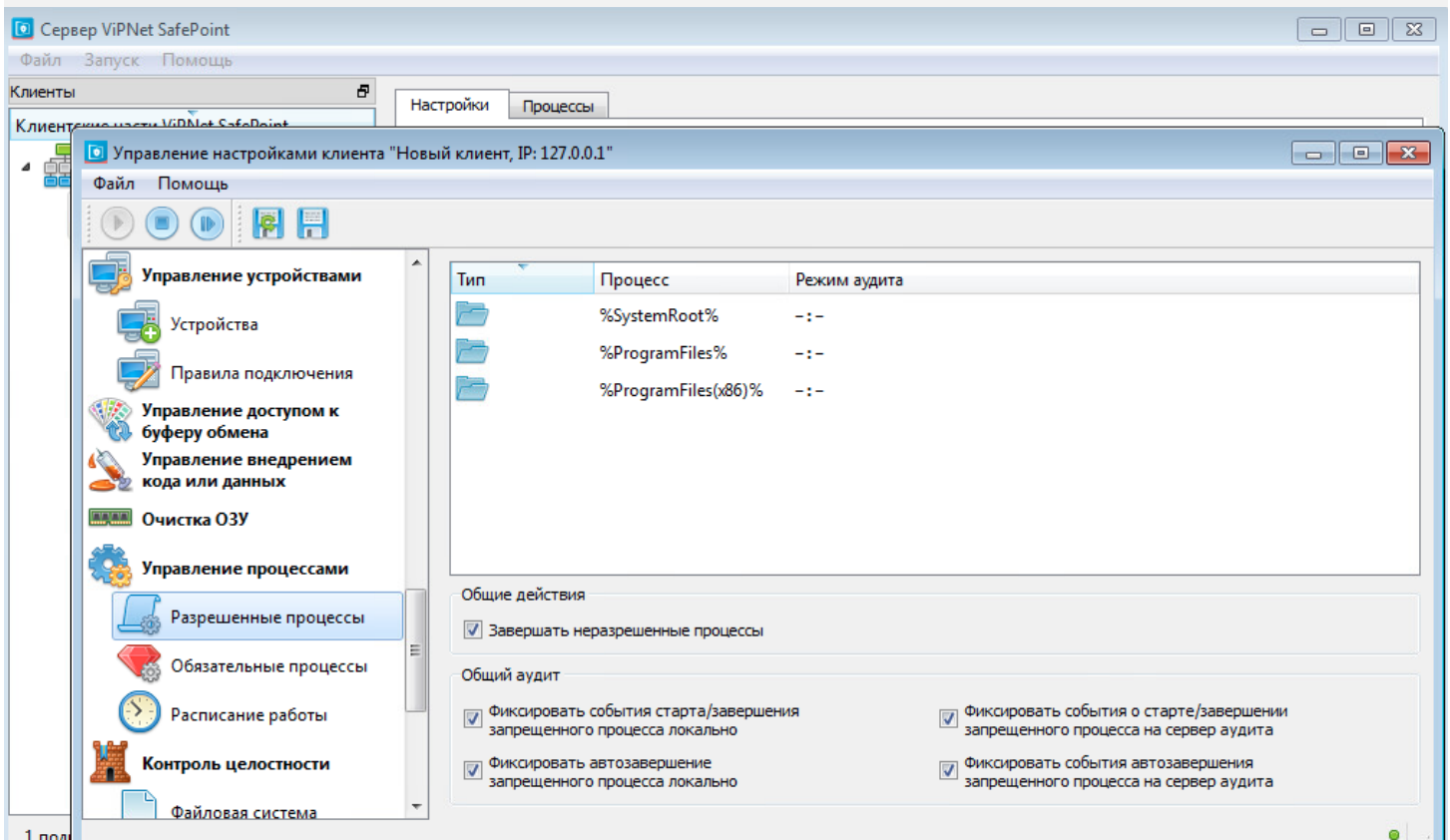
Контроль устройств

- Контроль и разграничения доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам

Создание правила доступа



Настройка разрешённых процессов



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

infotecs

Спасибо
за внимание!