
техно
2019
infotecs
фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ
12
09
2019
Новые решения ИнфоТеКС для защиты рабочих станций и серверов. Обзор продуктов ViPNet SafePoint и ViPNet Endpoint Protection.

Текущее состояние линейки продуктов для защиты рабочих станций и серверов

ТехноФест 2019 infotecs

ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки уровня UEFI BIOS

ViPNet Client

ViPNet Client (Клиент) — это программный комплекс для защиты рабочих мест пользователей.

ViPNet Personal Firewall

Программный межсетевой экран, предназначенный для контроля и управления трафиком рабочих мест и серверов пользователей информационных систем

ViPNet IDS HS

Система обнаружения вторжений для рабочих станций ViPNet IDS HS

Что имеем сейчас

- Доверие к платформе, разграничение доступа, доверенная загрузка ОС
- VPN-клиент
- Межсетевое экранирование
- Обнаружение атак и вторжений

Самые распространённые обращения

Средство защиты от несанкционированного доступа

Объедините всё в один многомодульный продукт

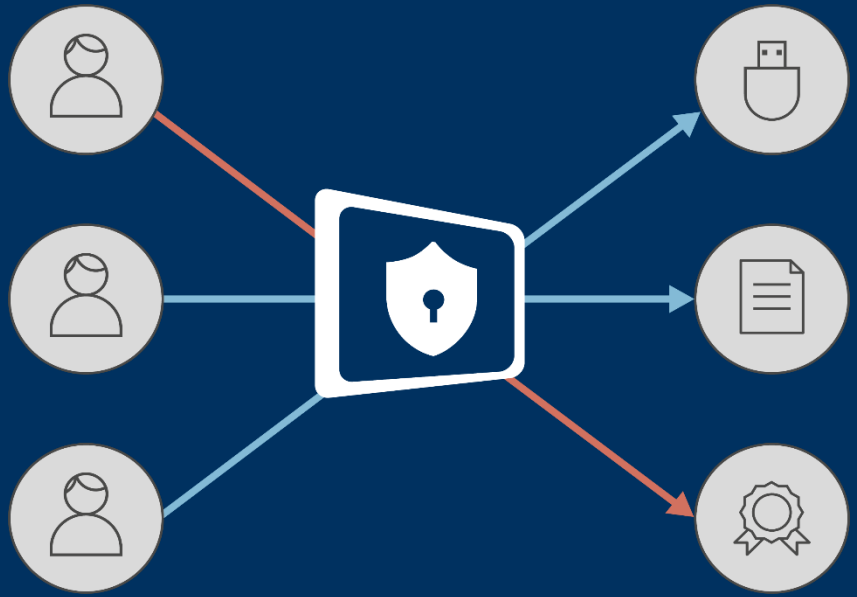
ViPNet SafePoint

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.

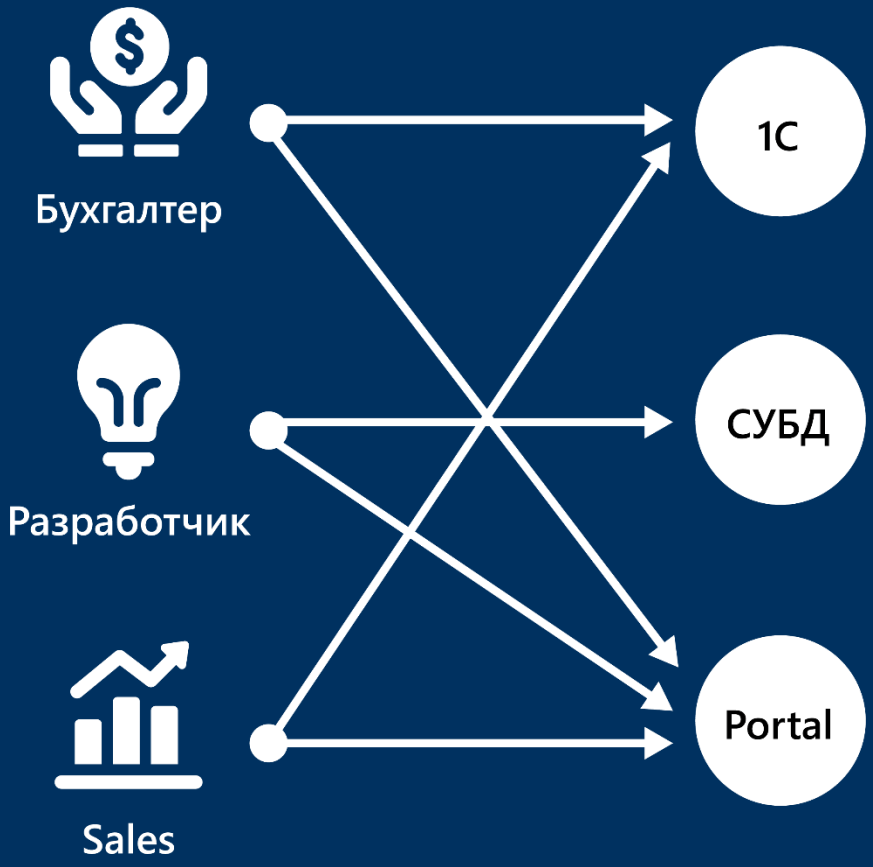
Ключевая функциональность

- 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

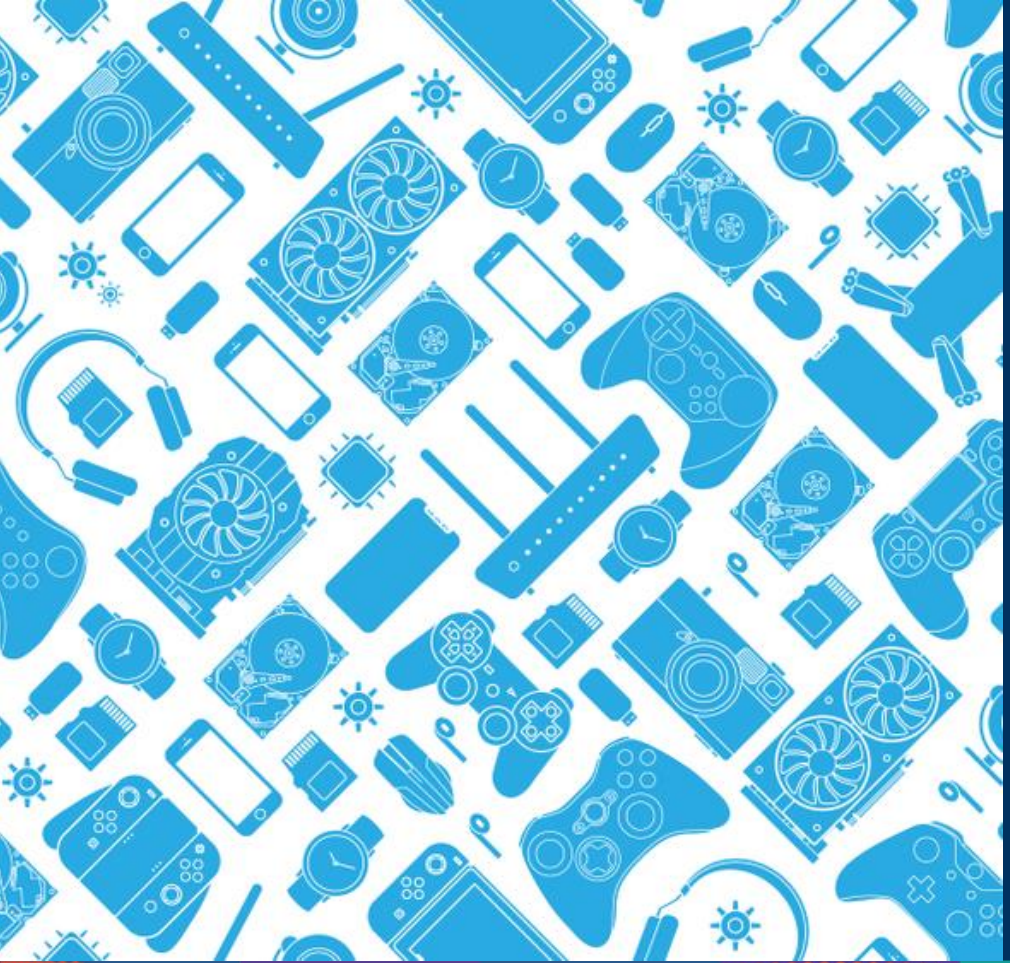


Мандатный контроль доступа пользователей и процессов

Разграничительная политика на основе меток безопасности

Замкнутая программная среда

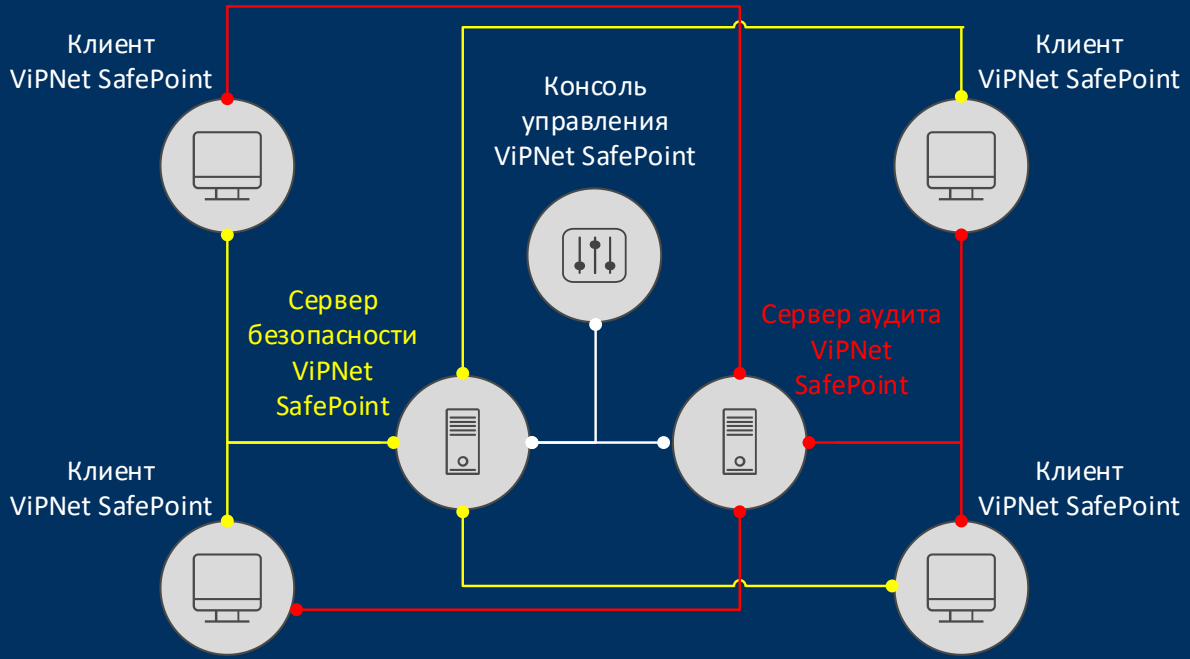
- Защита от модификации запускаемых модулей
- Контроль запуска скриптов Active Scripts
- Контроль запуска задач



ТЕХНО 2019 infotecs Фест

Контроль устройств

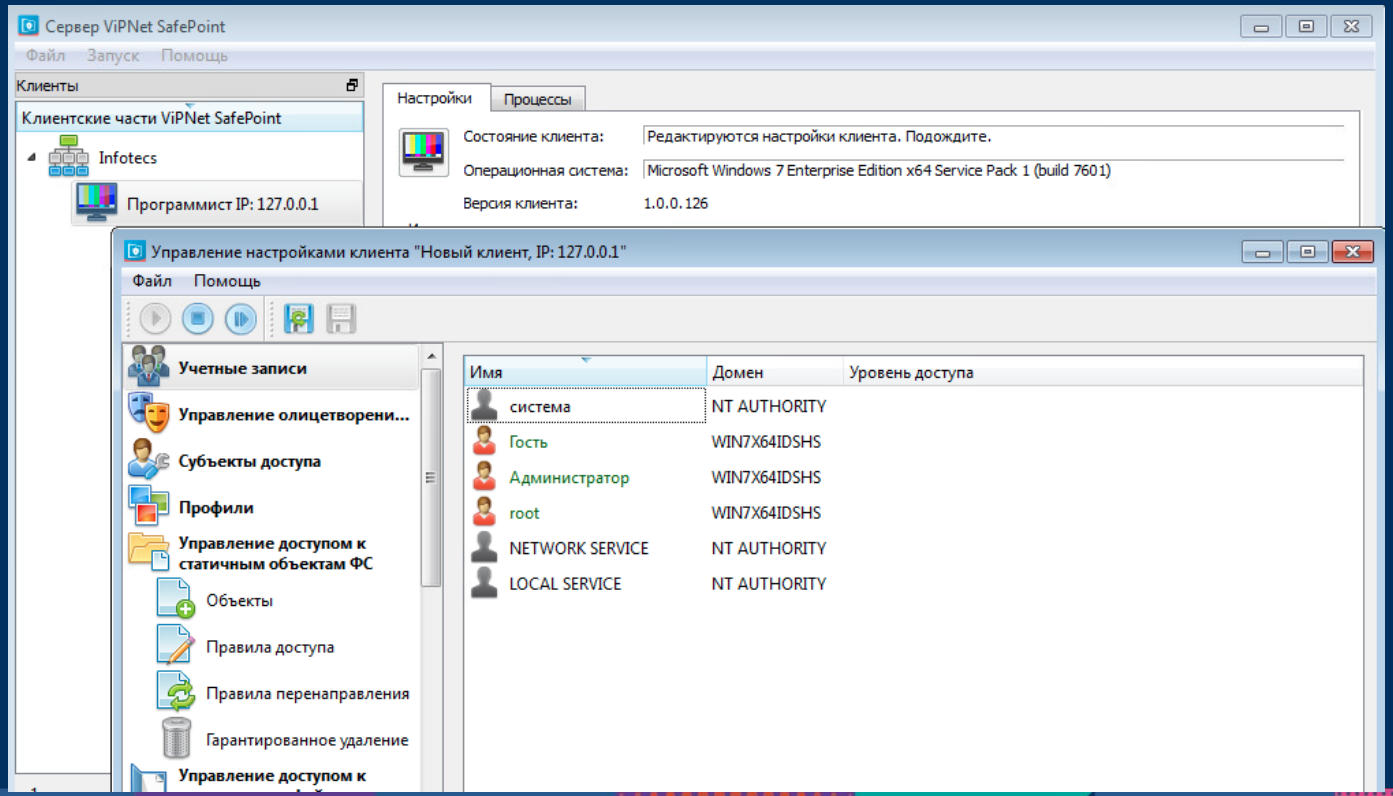
- Контроль и разграничения доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам



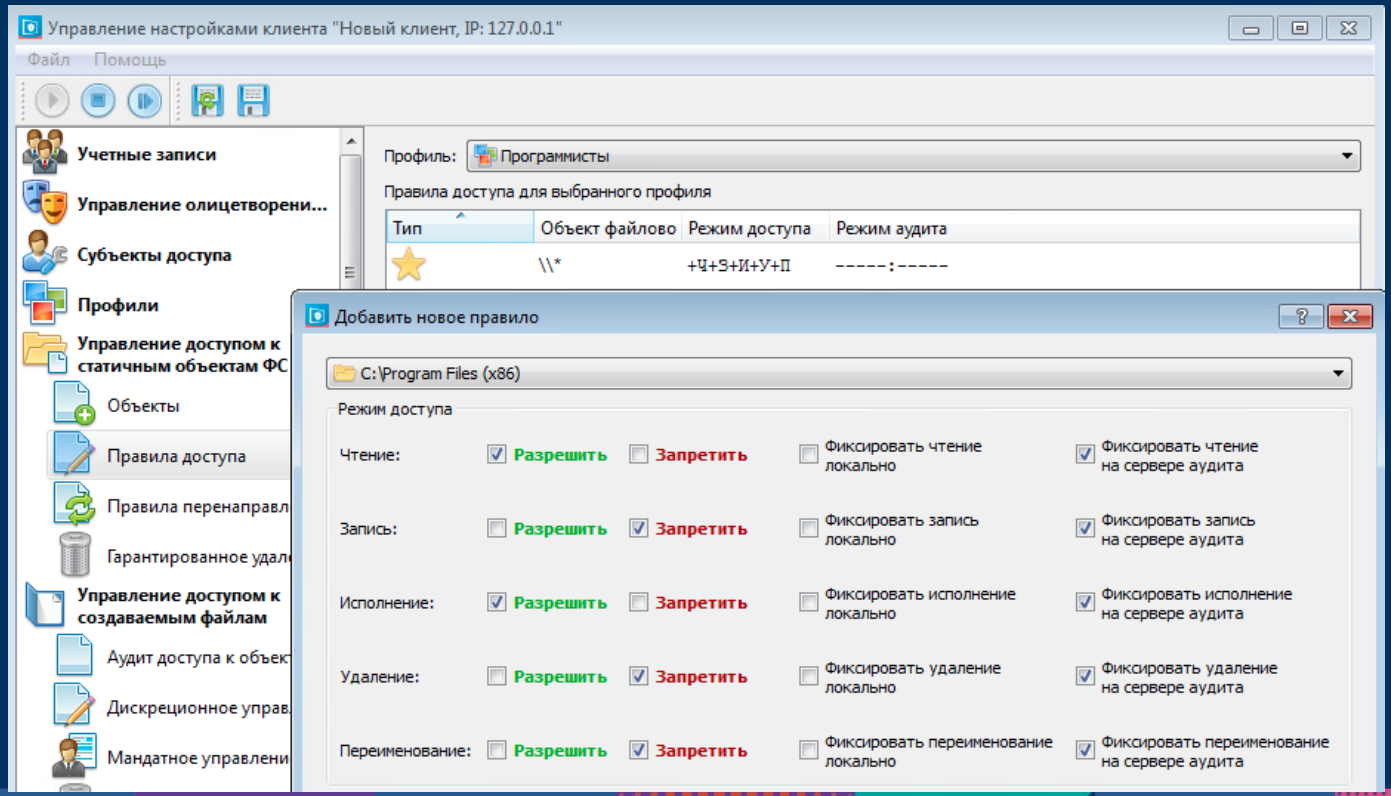
Архитектура ViPNet SafePoint

- Клиент
- Сервер аудита
- Сервер безопасности
- Консоль управления

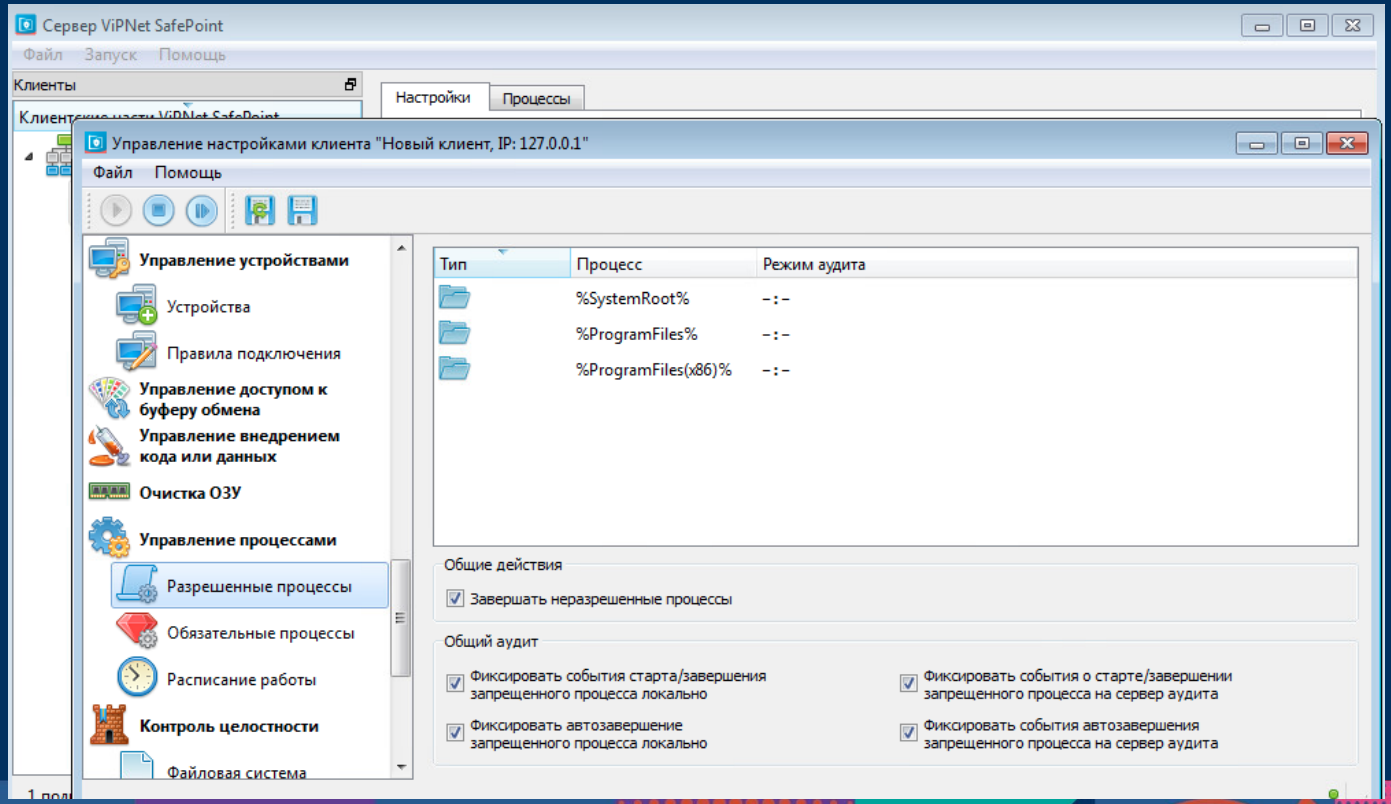
Интеграция с Active Directory



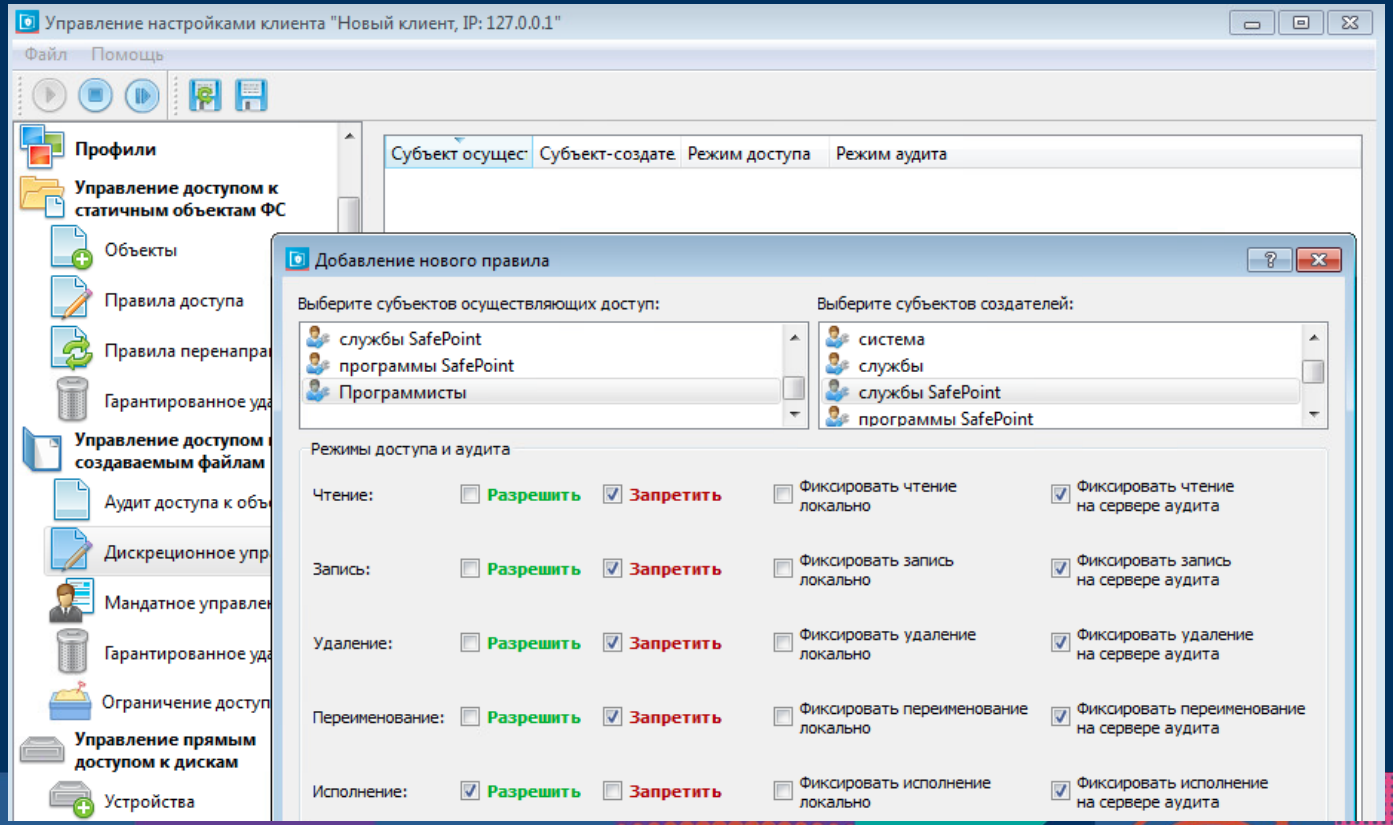
Создание правила доступа



Настройка разрешённых процессов



Дискреционное управление доступом



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 Endpoint Protection

ТЕХНО 2019 infotecs Фест

ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия. Ключевыми модулями системы являются – персональный межсетевой экран, система обнаружения и предотвращения вторжений, а также контроль приложений.

Обнаружение и предотвращение атак

Используем:

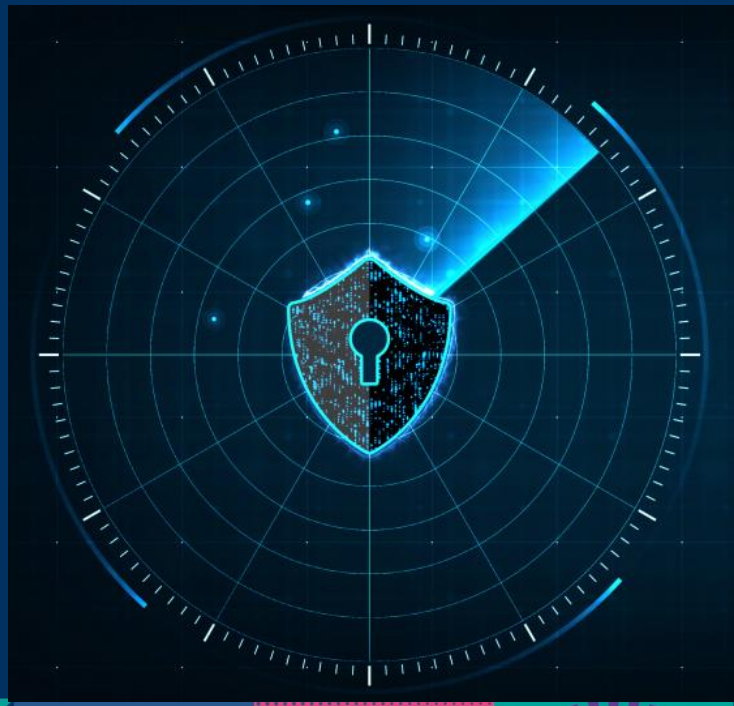
- Эвристический метод
- Сигнатурный метод

Следим за:

- Системными журналами Windows
- Журналами и логами приложений
- Изменениями в файловой системе и реестре
- Сетевым трафиком

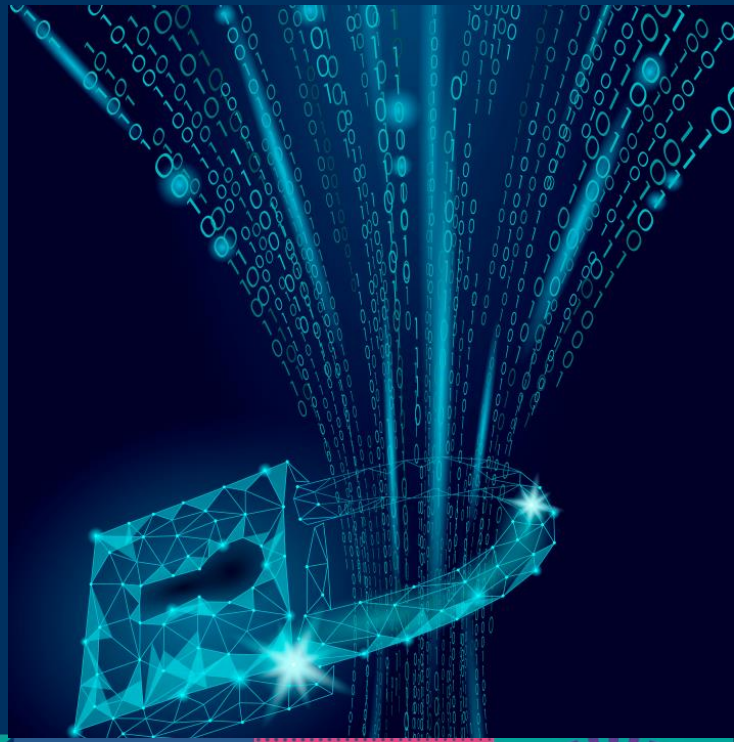
Блокируем

- Подозрительный сетевой трафик
- Атакующие хосты



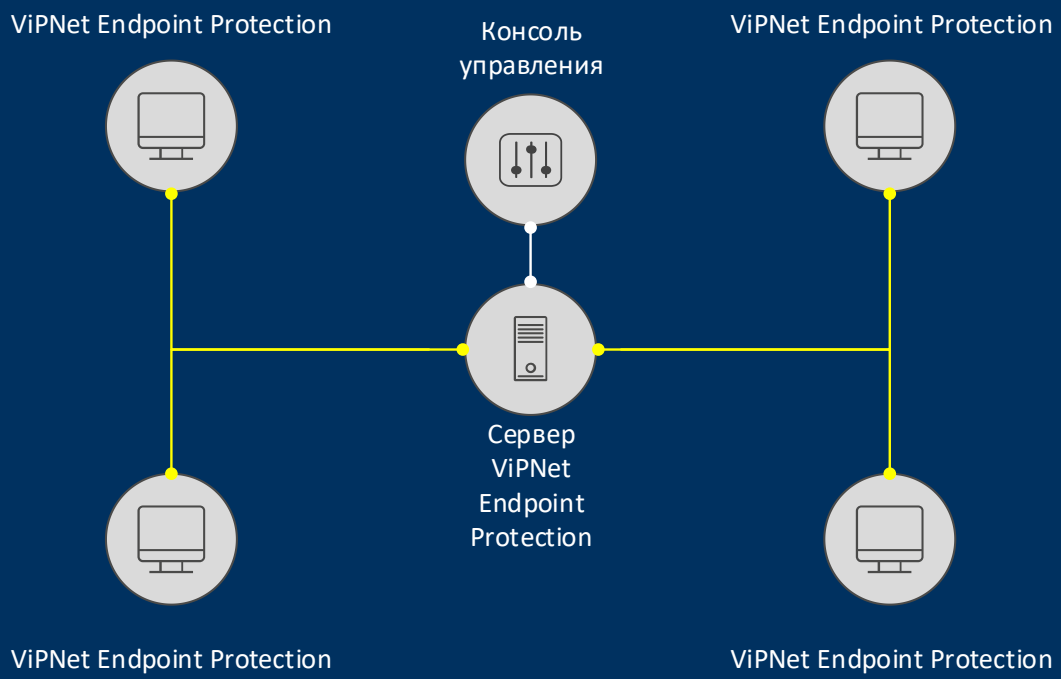
Межсетевое экранирование

- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие преднастроенных фильтров
- Создание фильтров для определённых групп хостов
- Создание правил фильтрации из журнала трафика



Контроль приложений

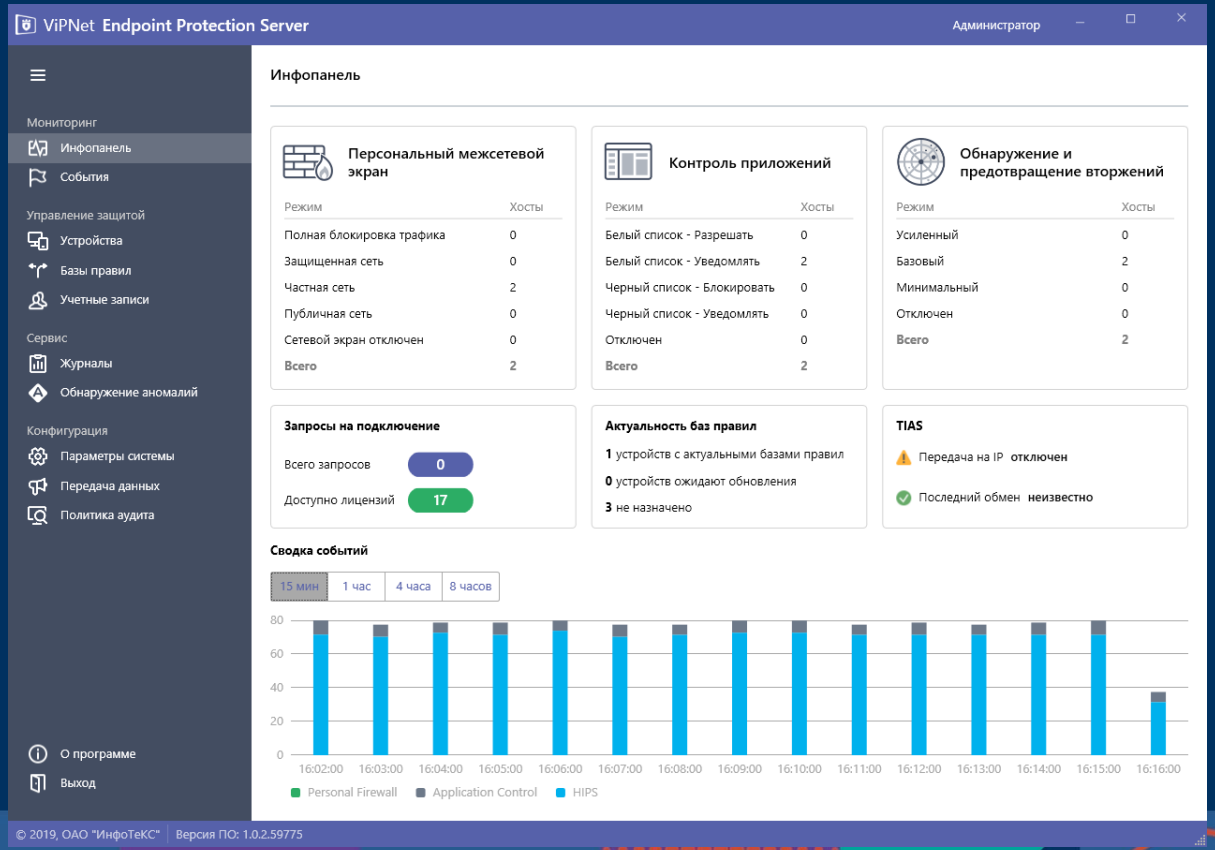
- Контроль запуска программ, используя Чёрные и белые списки программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений



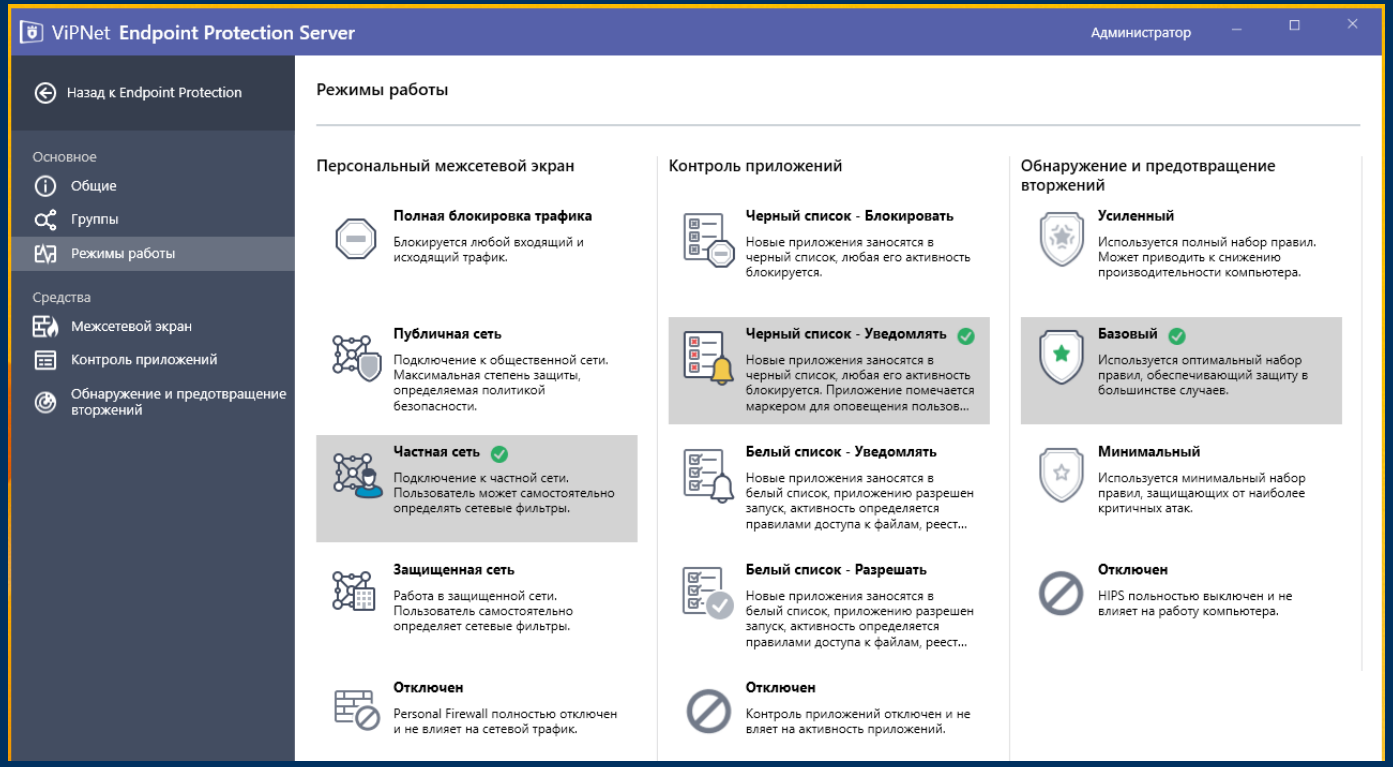
Архитектура ViPNet Endpoint Protection

- Клиент
- Сервер
- Консоль управления

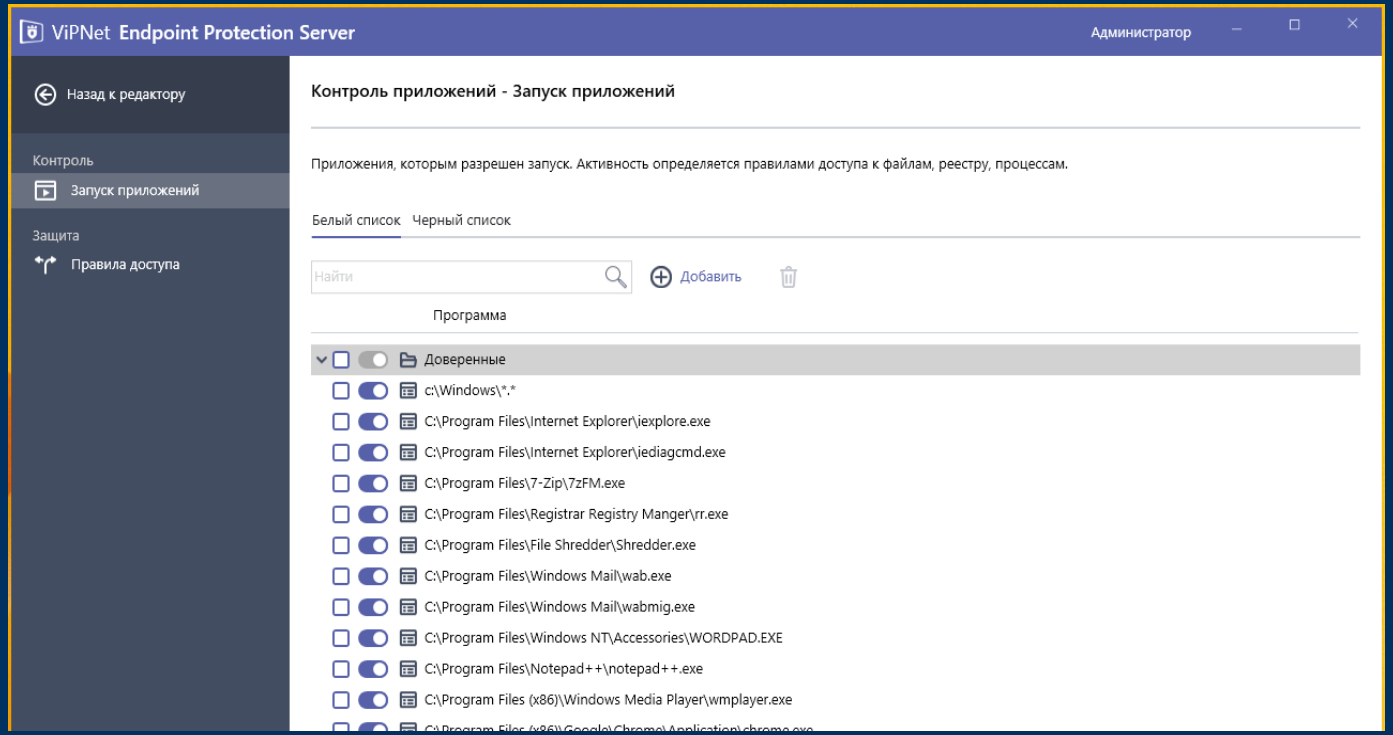
Внешний вид


ViPNet Endpoint Protection Server
Администратор
Мониторинг
Инфопанель
События
Управление защитой
Устройства
Базы правил
Учетные записи
Сервис
Журналы
Обнаружение аномалий
Конфигурация
Параметры системы
Передача данных
Политика аудита
О программе
Выход
Инфопанель
Персональный межсетевой экран
Режим Хосты
Полная блокировка трафика 0
Защищенная сеть 0
Частная сеть 2
Публичная сеть 0
Сетевой экран отключен 0
Всего 2
Контроль приложений
Режим Хосты
Белый список - Разрешать 0
Белый список - Уведомлять 2
Черный список - Блокировать 0
Черный список - Уведомлять 0
Отключен 0
Всего 2
Обнаружение и предотвращение вторжений
Режим Хосты
Усиленный 0
Базовый 2
Минимальный 0
Отключен 0
Всего 2
Запросы на подключение
Всего запросов 0
Доступно лицензий 17
Актуальность баз правил
1 устройств с актуальными базами правил
0 устройств ожидают обновления
3 не назначено
TIAS
Передача на IP отключен
Последний обмен неизвестно
Сводка событий
15 мин
1 час
4 часа
8 часов
80
60
40
20
0
16:02:00
16:03:00
16:04:00
16:05:00
16:06:00
16:07:00
16:08:00
16:09:00
16:10:00
16:11:00
16:12:00
16:13:00
16:14:00
16:15:00
16:16:00
Personal Firewall
Application Control
HIPS
© 2019, ОАО "ИнфоТеКС"
Версия ПО: 1.0.2.59775

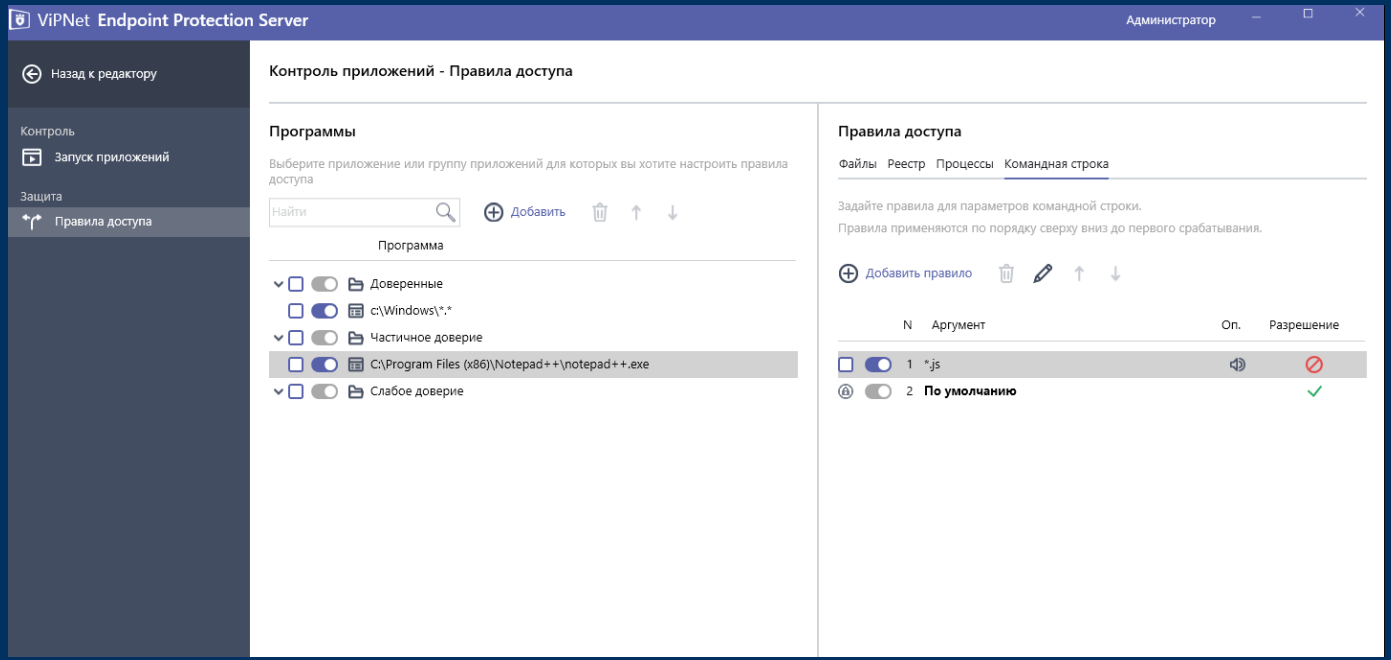
Выбор режима работы



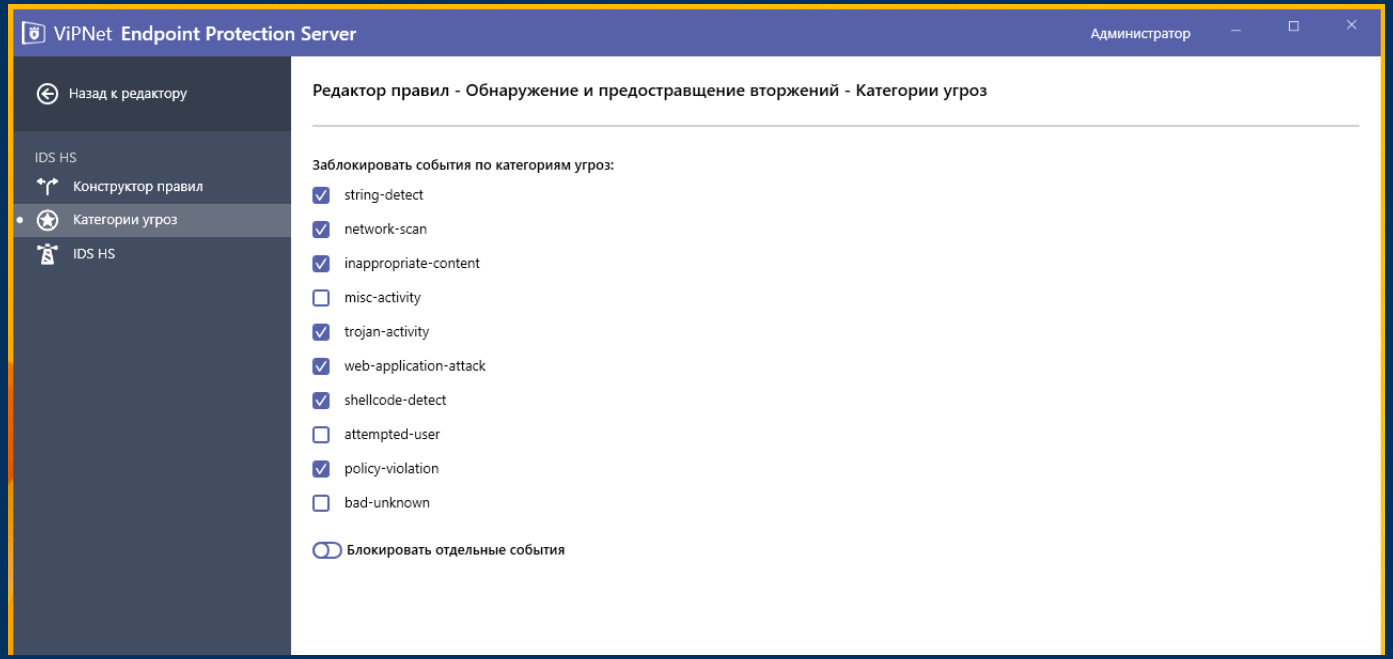
Чёрные и белые списки



Контроль запуска приложений из командной строки



Обнаружение и предотвращение



Ожидание по сертификации

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

- Системам обнаружения вторжений уровня узла 4 класс ИТ.СОВ.У4.ПЗ
- Межсетевым экранам типа В класса 4 (ИТ.МЭ.В4.ПЗ)
- 4 классу ТДБ

Спасибо
за внимание!