



ViPNet EndPoint Protection

Иван Кадыков



«Болезни» последних 5ти лет





«Конечные устройства» –
главная цель



Состав продуктовой линейки на начало 2020 г.



ViPNet SafeBoot

Средство доверенной загрузки

ViPNet IDS HS

Система обнаружения вторжений

ViPNet Personal Firewall

Персональный межсетевой экран

ViPNet Client

VPN-Клиент, Межсетевой экран, Деловая почта

ViPNet EndPoint Protection

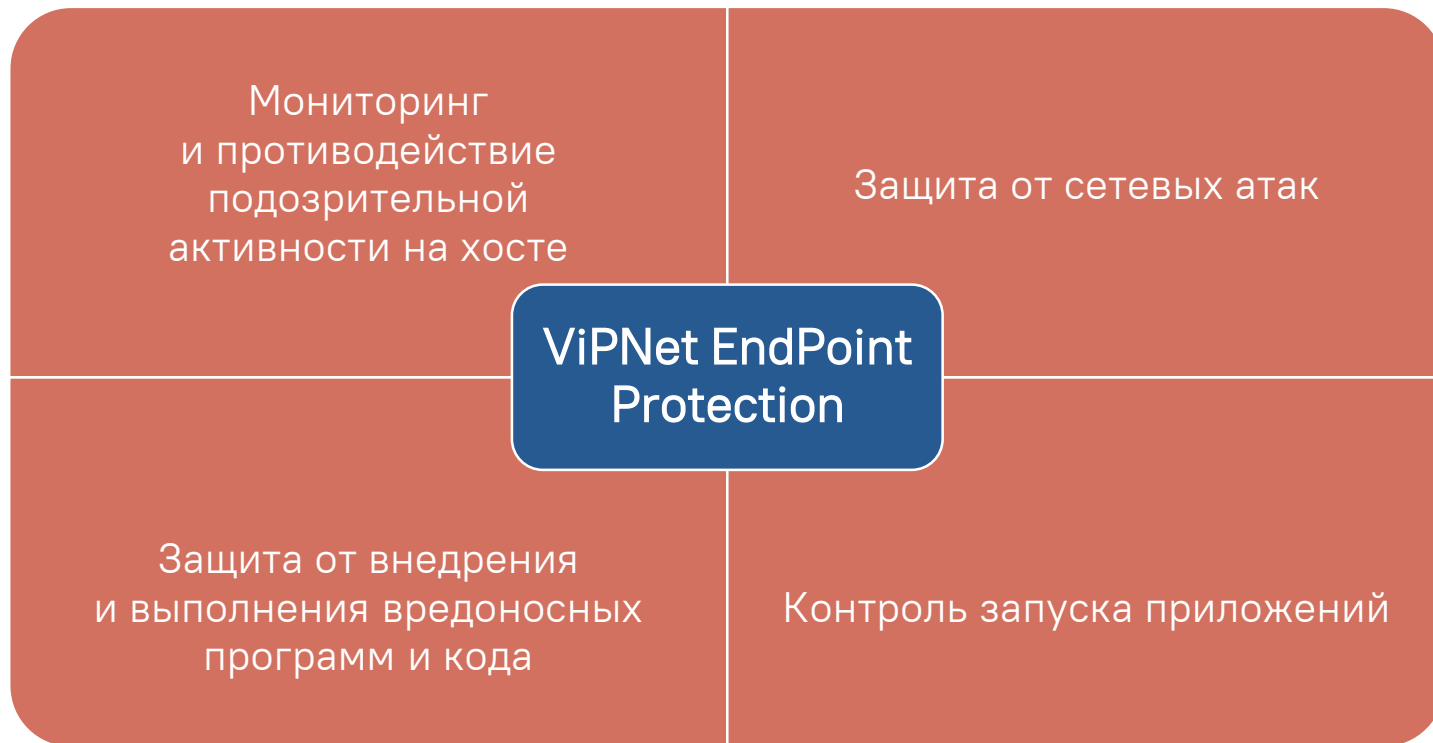


Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

Модули продукта



Решаемые задачи



Обнаружение и предотвращение атак

Используем:

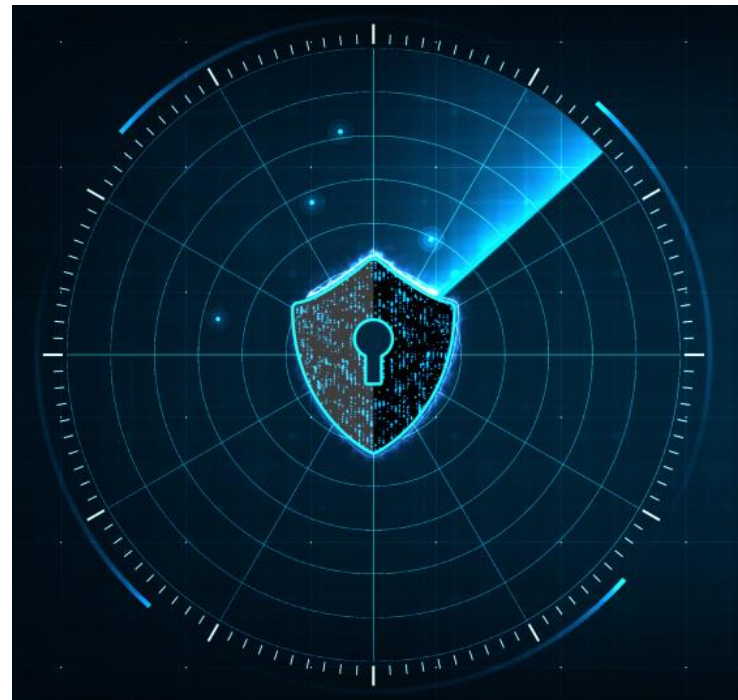
- Эвристический анализ
- Сигнатурный анализ

Следим за:

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

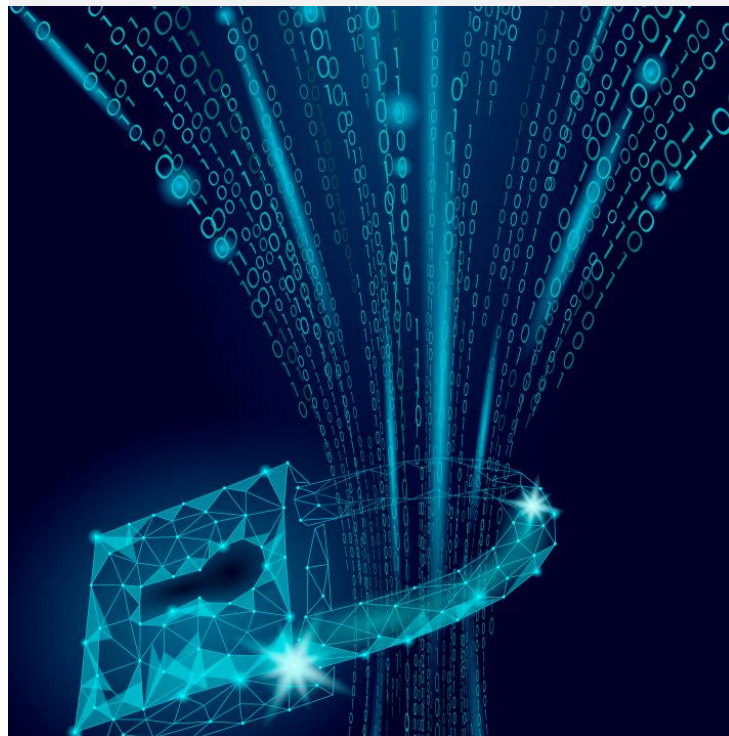
Блокируем

- Подозрительный сетевой трафик
- Атакующие хосты



Межсетевое экранирование

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



Контроль приложений

- Контроль запуска программ с использованием Чёрных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений



VIPNet EndPoint Protection
Агент

VIPNet EndPoint Protection
Консоль управления

VIPNet EndPoint Protection
Агент



VIPNet EndPoint Protection
Сервер

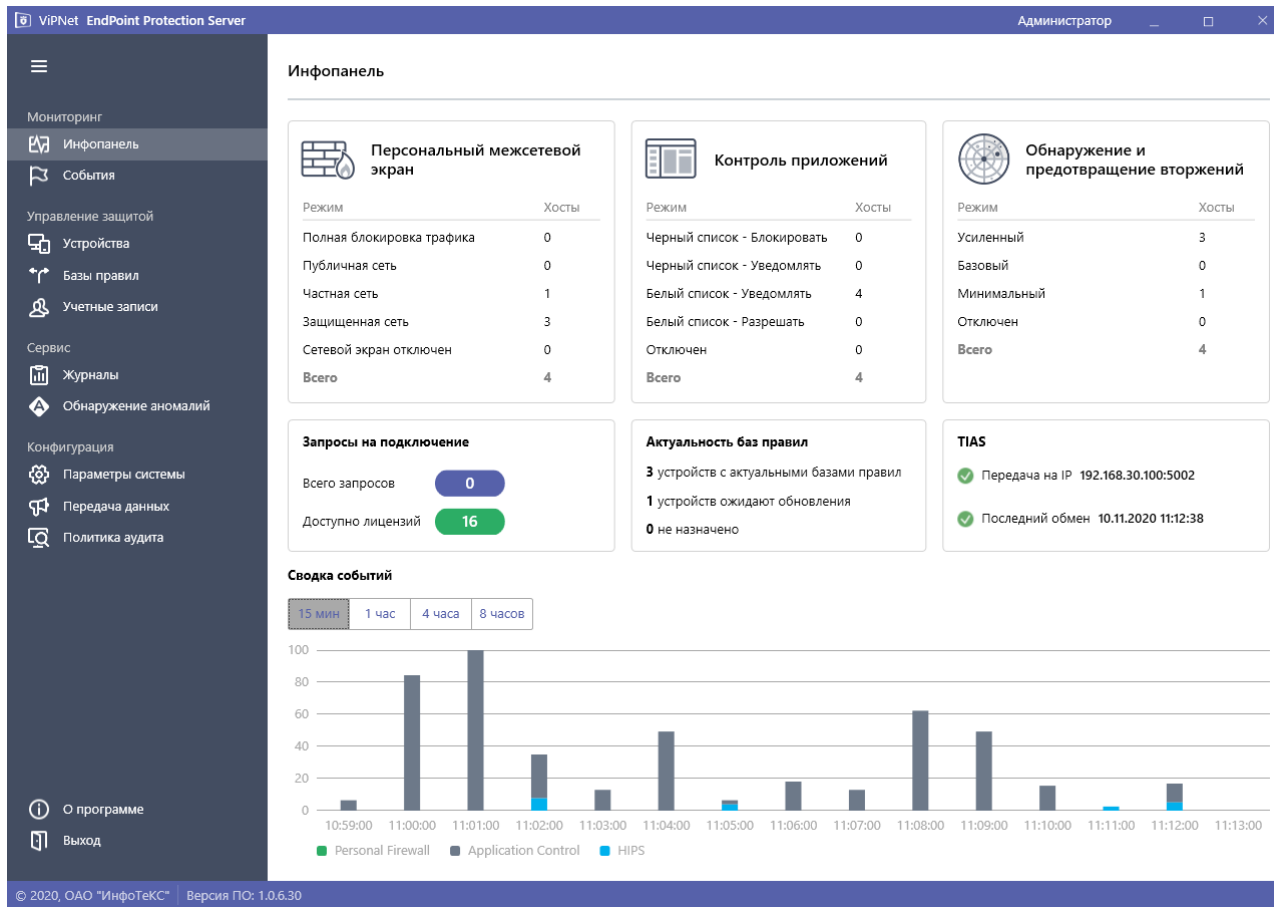


VIPNet EndPoint Protection
Агент

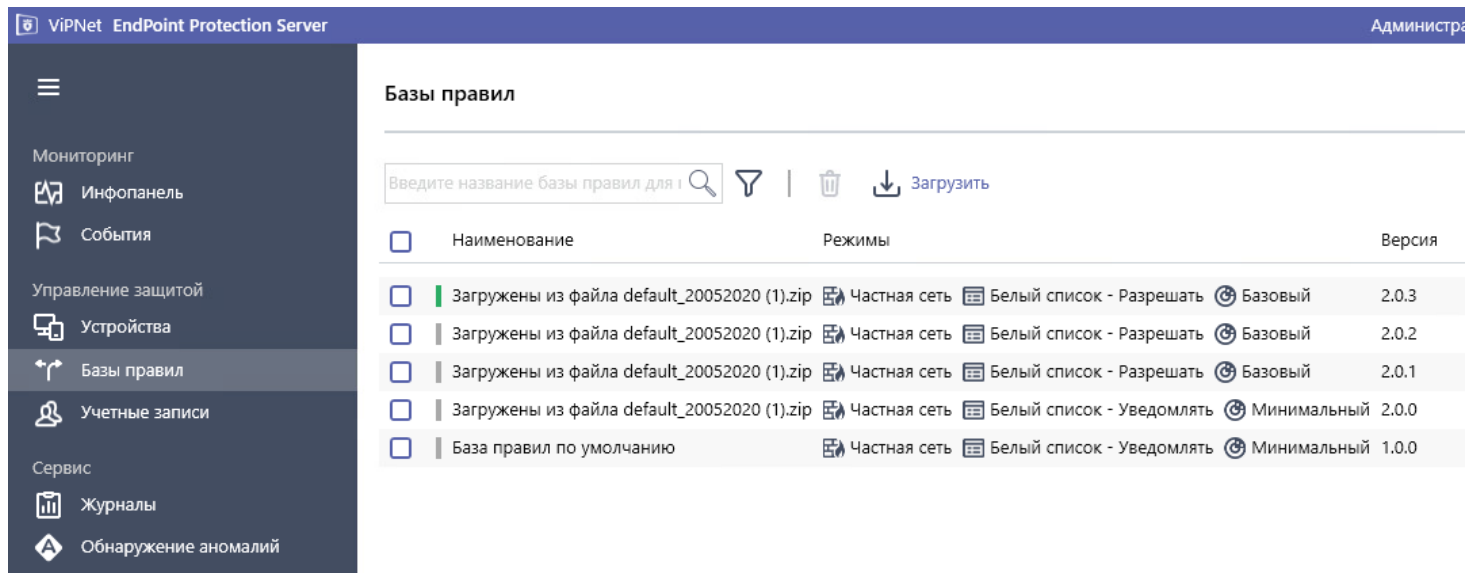
VIPNet EndPoint Protection
Агент

- Агент
- Сервер
- Консоль управления

Консоль управления сервером





















Базы правил (БРП)



ViPNet EndPoint Protection Server Администрация

Базы правил

Введите название базы правил для поиска  |   Загрузить

| <input type="checkbox"/> | Наименование | Режимы | Версия |
|--------------------------|---|--|--------|
| <input type="checkbox"/> | Загружены из файла default_20052020 (1).zip |  Частная сеть  Белый список - Разрешать  Базовый | 2.0.3 |
| <input type="checkbox"/> | Загружены из файла default_20052020 (1).zip |  Частная сеть  Белый список - Разрешать  Базовый | 2.0.2 |
| <input type="checkbox"/> | Загружены из файла default_20052020 (1).zip |  Частная сеть  Белый список - Разрешать  Базовый | 2.0.1 |
| <input type="checkbox"/> | Загружены из файла default_20052020 (1).zip |  Частная сеть  Белый список - Уведомлять  Минимальный | 2.0.0 |
| <input type="checkbox"/> | База правил по умолчанию |  Частная сеть  Белый список - Уведомлять  Минимальный | 1.0.0 |

БРП разрабатываются совместно с дочерней компанией «Перспективный мониторинг» и состоят из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевого экрана
- Списков ПО для Чёрного и Белого списка

Настройки модулей – режимы работы

The screenshot shows the 'Редактор правил - Режимы работы' (Rule Editor - Modes of Operation) window in the ViPNet EndPoint Protection Server administrator interface. The window title is 'Администратор' (Administrator). The interface is divided into three main sections, each with a 'Сохранить' (Save) and 'Отмена' (Cancel) button.

- Персональный межсетевой экран (Personal Network Screen):**
 - Полная блокировка трафика (Full traffic blocking):** Блокируется любой входящий и исходящий трафик.
 - Публичная сеть (Public network):** Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.
 - Частная сеть (Private network):** Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры. (Active)
 - Защищенная сеть (Protected network):** Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.
 - Отключен (Disabled):**
- Контроль приложений (Application Control):**
 - Черный список - Блокировать (Blacklist - Block):** Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий.
 - Черный список - Уведомлять (Blacklist - Notify):** Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.
 - Белый список - Уведомлять (Whitelist - Notify):** Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.
 - Белый список - Разрешать (Whitelist - Allow):** Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий. (Active)
 - Отключен (Disabled):**
- Обнаружение и предотвращение вторжений (Intrusion Detection and Prevention):**
 - Модуль обнаружения вторжений активен (Intrusion detection module is active):** (Active)
 - Усиленный (Enhanced):** Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.
 - Базовый (Basic):** Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев. (Active)
 - Минимальный (Minimal):** Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.
 - Отключен (Disabled):** Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.

Администратор может использовать предоставленные нами режимы работы модулей или сам настроить режимы работы модулей.

Обнаружение и предотвращение вторжений

Обнаружение вторжений активно всегда.

Механизмы работы схожи с ViPNet IDS HS:

1. Загрузили БРП
2. Назначили на группу агентов
3. Агенты, получив БРП, мониторят события в соответствии с заданными политиками аудита

Предотвращение вторжений – имеется несколько уровней защиты – Усиленный, Базовый, Минимальный (разрабатывали совместно с ПМ)

Обнаружение и предотвращение вторжений

✓ Модуль обнаружения вторжений активен



Усиленный

Используется полный набор правил предотвращения вторжений, может приводить к снижению быстродействия компьютера.



Базовый ✓

Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.



Минимальный

Используется минимальный набор правил предотвращения вторжений, защищающий от наиболее критичных атак.



Отключен

Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.

Предотвращение вторжений

Обнаружение и предотвращение вторжений - Категории угроз

- Попытка раскрыть информацию (attempted-recon)**
События данной категории свидетельствуют о попытках сбора информации. Разведовательные атаки не являются успешными, если информация не была успешно собрана.
- misc-attack**
- Атака с использованием веб-приложения (web-application-attack)**
События данной категории свидетельствуют об атаках, направленных на поиск и эксплуатацию уязвимостей: sql инъекции, внедрение кода, обход директорий, межсайтовый скриптинг, отказ в доступе и т.д.
- Прочая активность (misc-activity)**
События данной категории свидетельствуют о таких активностях как: о попытке отправки нестандартных HTTP запросов SMB, аномалии в трафике и т.д.
- Обнаружена активность сетевого трояна (trojan-activity)**
Правила реагируют на загрузку вредоносного семпла, а также на ответный трафик, генерируемый семплом.
- Попытка DDoS-атаки (attempted-dos)**
События данной категории свидетельствуют о попытках DDoS-атаки.
- web-application-activity**
- Потенциально опасный трафик (bad-unknown)**
Правила обнаруживают обращения к подозрительным/вредоносным доменным именам, IP адресам. В базе данных «черных списков», используемые злоумышленниками для организации командных центров ботнетов, фишинговых писем, размещения вредоносного контента, проведении всевозможных атак и т.д.
- Неудачная попытка использования прав пользователя (unsuccessful-user)**
События данной категории обнаруживают попытки повышения привилегий, которые завершились неудачно.

По категориям угроз

Редактор правил - Обнаружение и предотвращение вторжений - Правила режима работы 'Усиление'

Глобальные

Найти

| <input type="checkbox"/> | Правило | Действие | Источник | Назначение |
|-------------------------------------|--------------------------|---------------|----------|------------|
| <input checked="" type="checkbox"/> | Правило HIPS SIG=3001565 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3001582 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004562 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004565 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004569 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004572 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004573 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004576 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004579 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004651 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004653 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004654 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004682 | ❗ Блокировать | Все | Все |
| <input type="checkbox"/> | Правило HIPS SIG=3004685 | ❗ Блокировать | Все | Все |

По правилам

Межсетевой экран

Несколько режимов работы
с предустановленными фильтрами
от производителя

Администратор имеет возможность
добавлять/изменять/удалять
фильтры в режимах работы
«Частная сеть» и «Публичная сеть»

Персональный межсетевой экран



Полная блокировка трафика

Блокируется любой входящий и исходящий трафик.



Публичная сеть

Подключение к общественной сети. Максимальная степень защиты, определяемая политикой безопасности.



Частная сеть

Подключение к частной сети. Пользователь может самостоятельно определять сетевые фильтры.



Защищенная сеть

Работа в защищенной сети. Пользователь самостоятельно определяет сетевые фильтры.



Отключен

Personal Firewall полностью отключен и не влияет на сетевой трафик.

Межсетевой экран

ViPNet EndPoint Protection Server Администратор

← Назад к редактору

Сетевые фильтры

- Публичная сеть
- Частная сеть
- Защищенная сеть

Справочники

- Протоколы
- Адреса и сети
- Расписания

Редактор правил - Персональный межсетевой экран - Фильтры режима работы 'Публичная сеть'

Поиск по названию фильтра... + Создать фильтр ↑ ↓

| Название фильтра | Статус | Действие | Протокол | Источник | Назначение |
|--|-------------------------------------|---------------|-----------------------|--------------------|---------------|
| <input type="checkbox"/> Фильтры политик безопасности | | | | | |
| <input type="checkbox"/> Веб-серфинг | <input checked="" type="checkbox"/> | ✓ Разрешить | DHCP; DNS; HTTP; HTTP | Все | Все |
| <input type="checkbox"/> Почта | <input checked="" type="checkbox"/> | ✓ Разрешить | IMAP; POP3; SMTP | Все | Все |
| <input type="checkbox"/> Доступ к частной сети | <input checked="" type="checkbox"/> | ✓ Разрешить | Все | Мой компьютер | Частная сеть |
| <input type="checkbox"/> Обращения из частной сети | <input checked="" type="checkbox"/> | ✓ Разрешить | Все | Частная сеть | Мой компьютер |
| <input type="checkbox"/> Доступ из корпоративной сети | <input checked="" type="checkbox"/> | ✓ Разрешить | Все | Корпоративная сеть | Мой компьютер |
| Фильтры по умолчанию | | | | | |
| <input checked="" type="checkbox"/> Действие по умолчанию | <input type="checkbox"/> | ! Блокировать | Все | Все | Все |

Создание фильтров аналогично PFW, но т.к. это делается на сервере, имеется возможность рассылки на группы агентов.

Контроль приложений

Возможность выбора режима работы Черного/Белого списка – с полной блокировкой или уведомлением о запуске

Контроль приложений



Черный список - Блокировать

Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий.



Черный список - Уведомлять

Любая активность приложения блокируется. Попытки запуска приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.



Белый список - Уведомлять

Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий и помечаются маркером для оповещения пользователя.



Белый список - Разрешать

Приложению разрешен запуск. Активности приложения фиксируются в журнале Событий.



Отключен

Контроль приложений отключен и не влияет на активность приложений.

Контроль приложений

Возможность формирования Белых и Чёрных списков.


































Редактор правил - Контроль приложений - Запуск приложений

[Белый список](#) [Чёрный список](#)

Приложения, которым разрешен запуск. Активность определяется правилами доступа к файлам, реестру, про...

Найти   [Добавить](#) | 

Глобальные

-  Слабое доверие
-  Частичное доверие
-  Доверенные
 -   C:\Windows\WinSxS*
 -   C:\Windows\SysWOW64*
 -   C:\Windows\SystemApps*
 -   C:\Windows\servicing*
 -   C:\Windows\Boot\PCAT*
 -   C:\Windows\ImmersiveControlPanel*
 -   C:\Windows\Microsoft.NET*
 -   C:\Windows\PrintDialog*
 -   C:\Windows\Speech\Common*
 -   C:\Windows\System32*
 -   C:\ProgramData\Microsoft\Windows Defender\Platform*
 -   C:\Program Files\Common Files\microsoft shared*
 -   C:\Program Files\InfoTeCS*
 -   C:\Program Files\internet explorer*
 -   C:\Program Files\PostgreSQL*

Контроль приложений

Правила доступа

Возможность создания правил доступа для приложений к следующим объектам:

- Файлам
- Реестру
- Процессам
- Командной строке

Контроль приложений - Правила доступа

Выберите приложение или группу приложений для которых вы хотите настроить правила доступа

Найти   Добавить |   

Глобальные ▾

- > Слабое доверие
- ▼ Частичное доверие
 - cmd.exe
 - powershell.exe
 - C:\Users*
 - C:\Windows\Temp*
 - C:\Windows\Tasks*
 - WINWORD.EXE
 - EXCEL.EXE
- > Доверенные

Правила доступа



Файлы Реестр Процессы Командная строка

Задайте правила доступа к реестру.

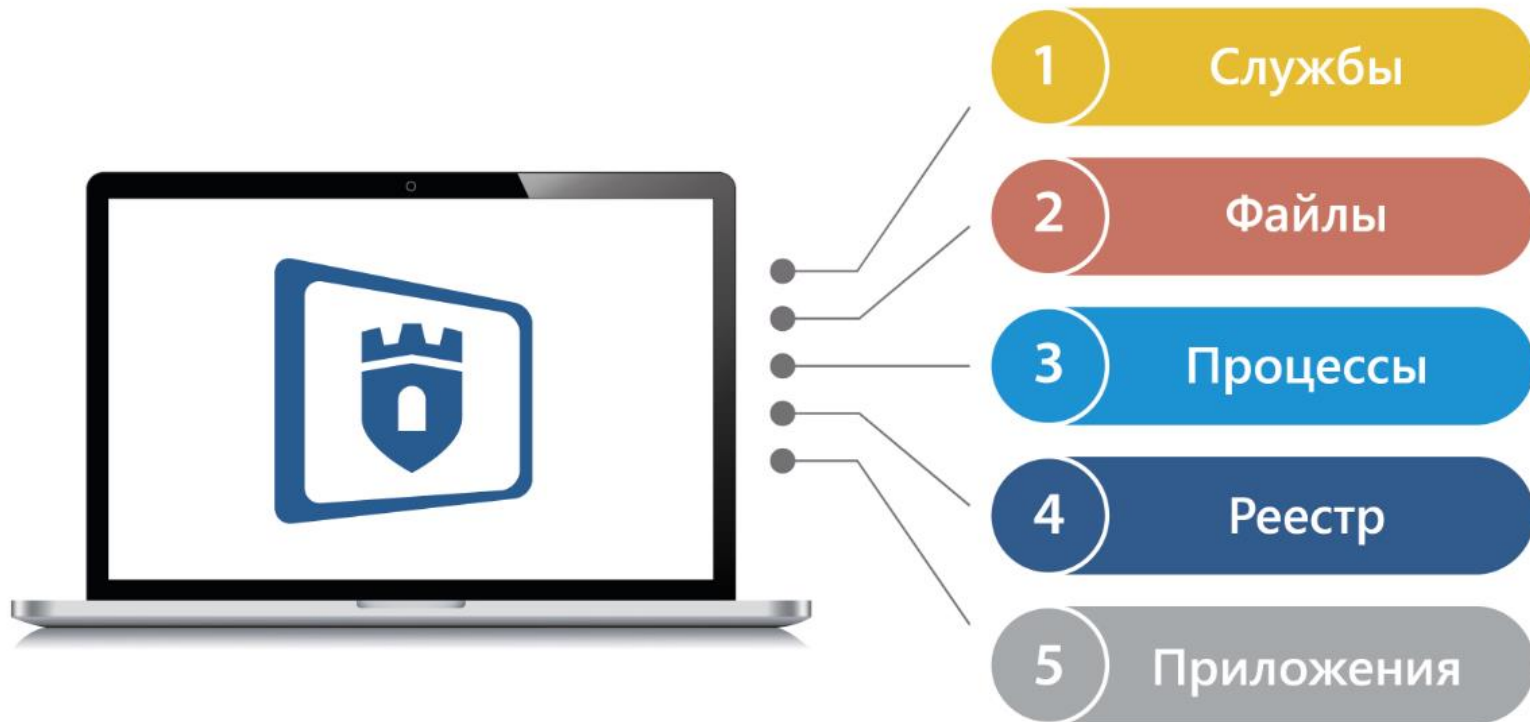
Правила применяются по порядку сверху вниз до пер

 Добавить правило |    

N Объекты Оп. Рек.

 1 По умолчанию 

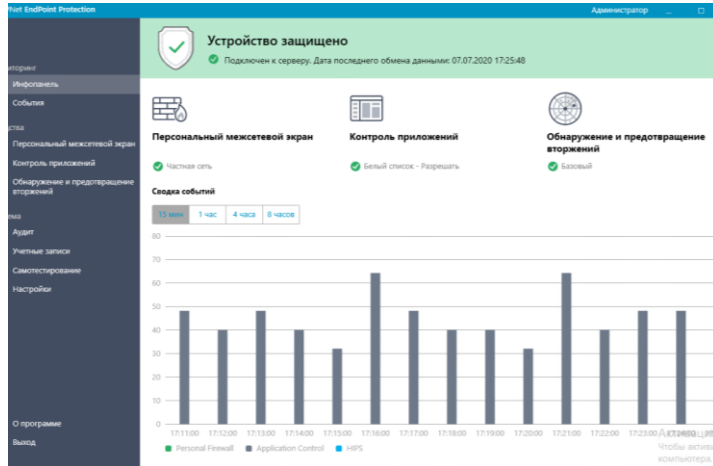
Полная защита



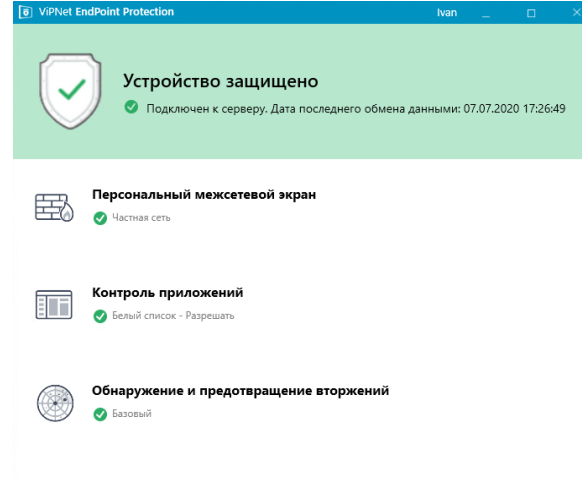
Это только кратко про сервер
ViPNet EndPoint Protection, а есть ещё...



А есть ещё агент...



... на котором администратор может локально изменять настройки...



... а доверенный пользователь только менять режим работы для себя

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

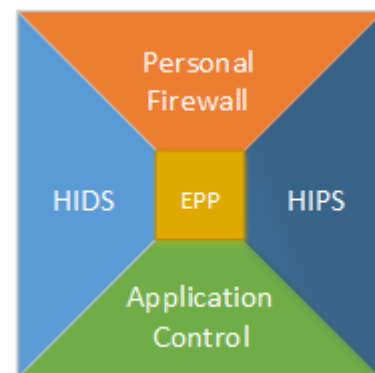
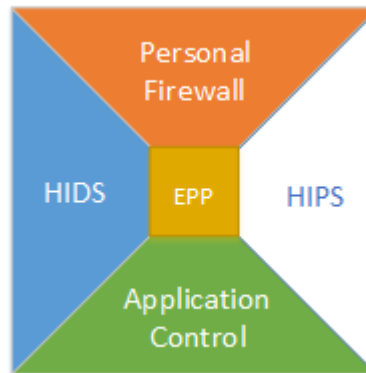
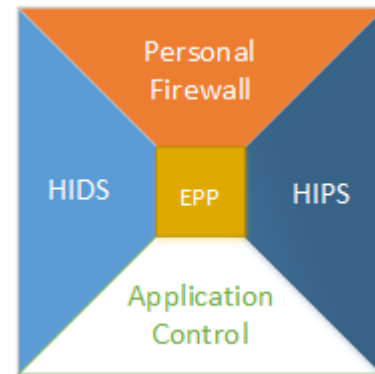
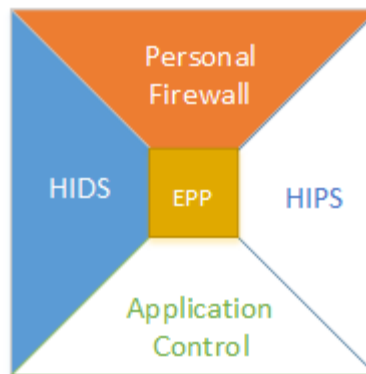


Продукт передан на сертификацию по линии
ФСТЭК России по требованиям к:

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

Модульный продукт

- Пользователь может сам выбрать нужный набор модулей в зависимости от имеющихся задач и бюджета



Лицензирование

Лицензия устанавливается на ViPNet EPP Сервер и определяет:

- МАХ-количество защищаемых узлов, которые разрешено подключить серверу.
- Срок скачивания баз правил и загрузки баз правил на ViPNet EPP Сервер.
- Максимальную версию ViPNet EPP Сервер, до которой возможно обновление.
- Вариант разрешенных модулей одинаковый для всех защищаемых узлов:
 - Personal Firewall + HIDS.
 - Personal Firewall + HIDS + HIPS.
 - Personal Firewall + HIDS + HIPS + Application Control.

ЛИЦЕНЗИЯ

| | |
|---------------------------------------|-----------------------|
| Состояние: | Лицензия активирована |
| Идентификатор лицензии: | 1818468/1/1-EPP |
| Дата окончания обновления баз правил: | 25.03.2021 |
| Дата окончания действия лицензии: | 02.10.2020 |

| ДОСТУПНЫЕ МОДУЛИ | ВСЕГО | ИСПОЛЬЗОВАНО | ОСТАЛОСЬ |
|---------------------|-------|--------------|----------|
| HIDS | 25 | 1 | 24 |
| Personal Firewall | 25 | 1 | 24 |
| Application Control | 25 | 1 | 24 |
| HIPS | 25 | 1 | 24 |

Что дальше?

- Агент для Linux:
 - Astra Linux Special Edition 1.6 релиз «Смоленск»
 - Ред ОС 7.2
 - АльтЛинукс 8 СП
- Возможность управления ViPNet SafeBoot
- Расширение возможностей модуля эвристики (аномальные запуски системных утилит, перехват системных вызовов, сканирование памяти для отслеживания code injection и fileless атак)
- WebControl
- Интеграция с ViPNet Client 4U





Вместо эпилога

Текущая концепция защиты рабочих станций



ViPNet SafeBoot

Доверие
к платформе
и обеспечение
доверенной
загрузки ОС

Разграничение
доступа
и защита
данных



ViPNet SafePoint



ViPNet Client 4U

Обеспечение
защищённых
коммуникаций

Защита
от внешних
атак
и угроз



ViPNet EndPoint
Protection

Вопросы?

Иван Кадыков,
руководитель направления

Ivan.Kadykov@infotecs.ru



Спасибо
за внимание!