

техно infotecs
2019 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



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

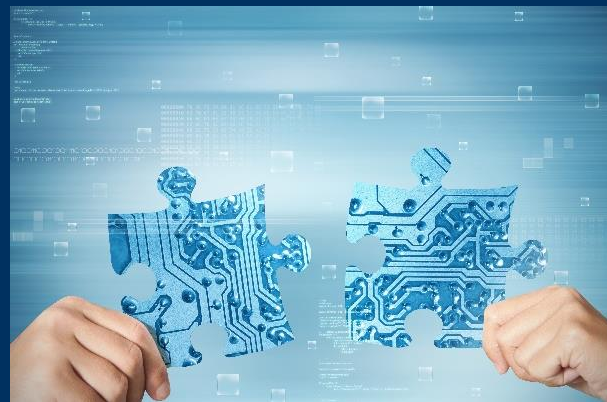
Что имеем сейчас

- 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

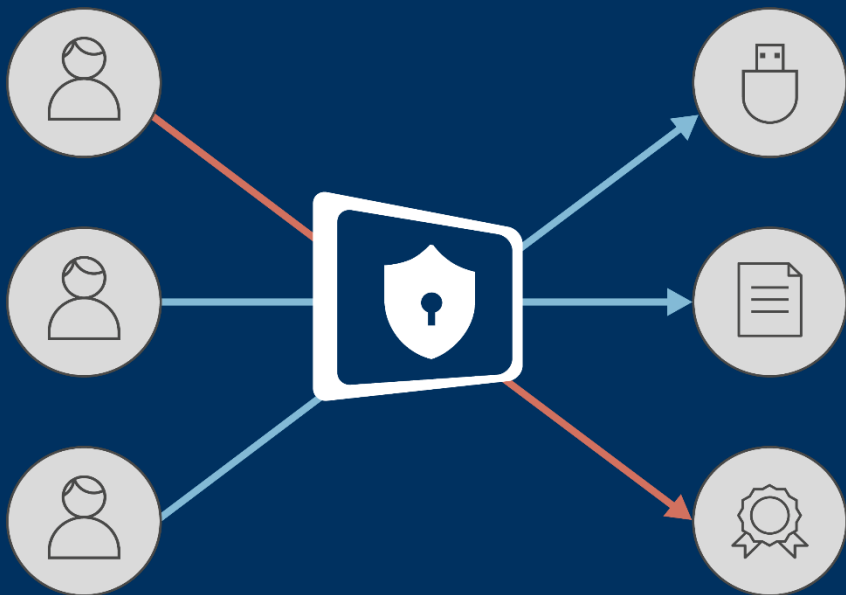
Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации. Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями)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



Ключевая функциональность

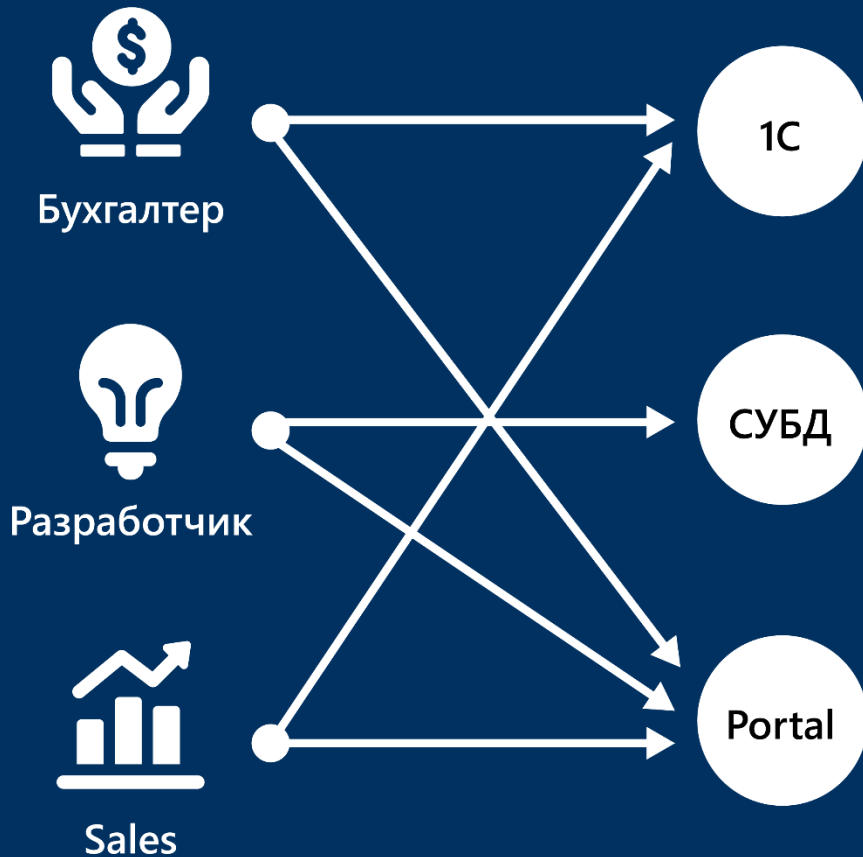


- Двухфакторная аутентификация пользователей
- Поддержка USB-токенов и смарт-карт:
 - JaCarta ГОСТ
 - JaCarta PKI
 - JaCarta LT
 - Rutoken S
 - Rutoken Lite
 - Rutoken ЭЦП



Дискреционный контроль
доступа пользователей

Разграничительная политика на основе
матрицы доступа



Мандатный контроль
доступа пользователей
и процессов

Разграничительная политика
на основе меток безопасности

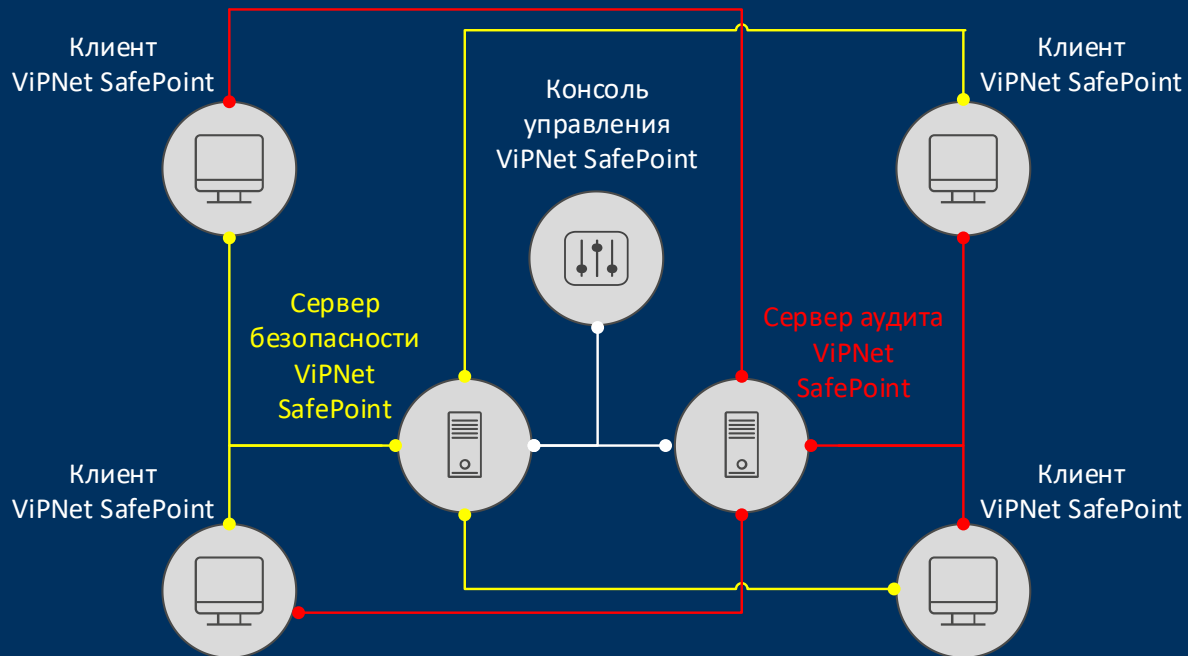
Замкнутая программная среда

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



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

The screenshot displays the VIPNet SafePoint management console. The main window, titled "Сервер ViPNet SafePoint", shows a tree view of clients under "Клиенты". A client named "Infotecs" with IP 127.0.0.1 is selected. The "Настройки" (Settings) tab is active, showing client status and system information.

Client Settings:

- Состояние клиента: Редактируются настройки клиента. Подождите.
- Операционная система: Microsoft Windows 7 Enterprise Edition x64 Service Pack 1 (build 7601)
- Версия клиента: 1.0.0.126

A secondary window, "Управление настройками клиента 'Новый клиент, IP: 127.0.0.1'", is open, showing a list of users and their access levels. The left sidebar contains navigation options like "Учетные записи", "Управление олицетворени...", "Субъекты доступа", "Профили", and "Управление доступом к статичным объектам ФС".

| Имя | Домен | Уровень доступа |
|-----------------|--------------|-----------------|
| система | NT AUTHORITY | |
| Гость | WIN7X64IDSHS | |
| Администратор | WIN7X64IDSHS | |
| root | WIN7X64IDSHS | |
| NETWORK SERVICE | NT AUTHORITY | |
| LOCAL SERVICE | NT AUTHORITY | |

Создание правила доступа

Управление настройками клиента "Новый клиент, IP: 127.0.0.1"

Профиль: Программисты

Правила доступа для выбранного профиля

| Тип | Объект файлово | Режим доступа | Режим аудита |
|-----|----------------|---------------|--------------|
| ★ | * | +Ц+Э+И+У+П | ----- |

Добавить новое правило

C:\Program Files (x86)

Режим доступа

| | | | | |
|-----------------|---|---|--|--|
| Чтение: | <input checked="" type="checkbox"/> Разрешить | <input type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать чтение локально | <input checked="" type="checkbox"/> Фиксировать чтение на сервере аудита |
| Запись: | <input type="checkbox"/> Разрешить | <input checked="" type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать запись локально | <input checked="" type="checkbox"/> Фиксировать запись на сервере аудита |
| Исполнение: | <input checked="" type="checkbox"/> Разрешить | <input type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать исполнение локально | <input checked="" type="checkbox"/> Фиксировать исполнение на сервере аудита |
| Удаление: | <input type="checkbox"/> Разрешить | <input checked="" type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать удаление локально | <input checked="" type="checkbox"/> Фиксировать удаление на сервере аудита |
| Переименование: | <input type="checkbox"/> Разрешить | <input checked="" type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать переименование локально | <input checked="" type="checkbox"/> Фиксировать переименование на сервере аудита |

Настройка разрешённых процессов

Сервер VIPNet SafePoint

Файл Запуск Помощь

Клиенты

Настройки Процессы

Управление настройками клиента "Новый клиент, IP: 127.0.0.1"

Файл Помощь

Управление устройствами

- Устройства
- Правила подключения
- Управление доступом к буферу обмена
- Управление внедрением кода или данных
- Очистка ОЗУ
- Управление процессами
 - Разрешенные процессы**
 - Обязательные процессы
 - Расписание работы
- Контроль целостности
- Файловая система

| Тип | Процесс | Режим аудита |
|-------|---------------------|--------------|
| Папка | %SystemRoot% | - :- |
| Папка | %ProgramFiles% | - :- |
| Папка | %ProgramFiles(x86)% | - :- |

Общие действия

- Завершать неразрешенные процессы

Общий аудит

- Фиксировать события старта/завершения запрещенного процесса локально
- Фиксировать события автозавершения запрещенного процесса локально
- Фиксировать события о старте/завершении запрещенного процесса на сервер аудита
- Фиксировать события автозавершения запрещенного процесса на сервер аудита

Дискреционное управление доступом

Управление настройками клиента "Новый клиент, IP: 127.0.0.1"

Файл Помощь

Профили

Управление доступом к статичным объектам ФС

Объекты

Правила доступа

Правила перенаправления

Гарантированное удаление

Управление доступом к создаваемым файлам

Аудит доступа к объектам

Дискреционное управление

Мандатное управление

Гарантированное удаление

Ограничение доступа

Управление прямым доступом к дискам

Устройства

Субъект осуществляет: Субъект-создатель Режим доступа Режим аудита

Добавление нового правила

Выберите субъектов осуществляющих доступ:

- службы SafePoint
- программы SafePoint
- Программисты

Выберите субъектов создателей:

- система
- службы
- службы SafePoint
- программы SafePoint

Режимы доступа и аудита

| | | | | |
|-----------------|---|---|--|--|
| Чтение: | <input type="checkbox"/> Разрешить | <input checked="" type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать чтение локально | <input checked="" type="checkbox"/> Фиксировать чтение на сервере аудита |
| Запись: | <input type="checkbox"/> Разрешить | <input checked="" type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать запись локально | <input checked="" type="checkbox"/> Фиксировать запись на сервере аудита |
| Удаление: | <input type="checkbox"/> Разрешить | <input checked="" type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать удаление локально | <input checked="" type="checkbox"/> Фиксировать удаление на сервере аудита |
| Переименование: | <input type="checkbox"/> Разрешить | <input checked="" type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать переименование локально | <input checked="" type="checkbox"/> Фиксировать переименование на сервере аудита |
| Исполнение: | <input checked="" type="checkbox"/> Разрешить | <input type="checkbox"/> Запретить | <input type="checkbox"/> Фиксировать исполнение локально | <input checked="" type="checkbox"/> Фиксировать исполнение на сервере аудита |

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





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

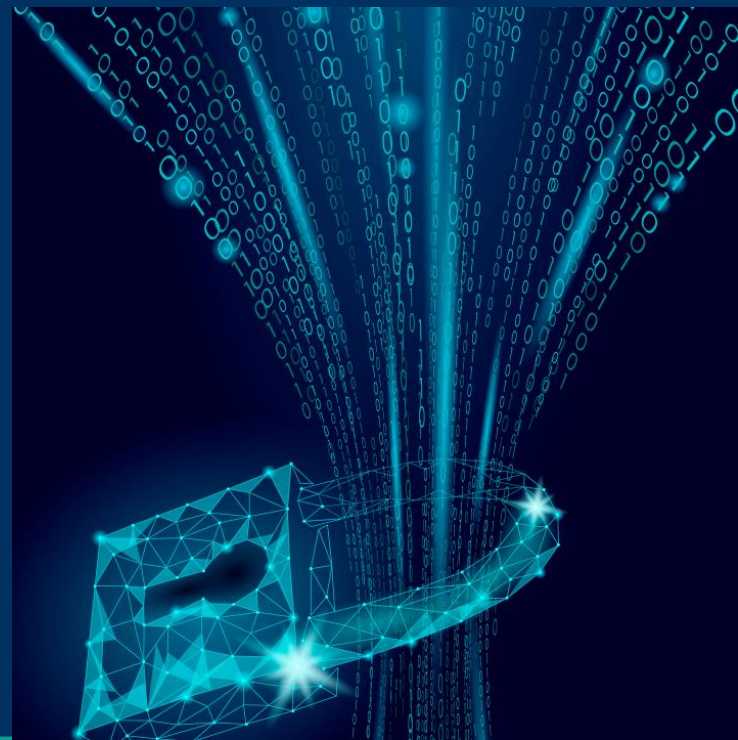
Блокируем

- Подозрительный сетевой трафик
- Атакующие хосты



Межсетевое экранирование

- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие предустановленных 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

WHITELIST

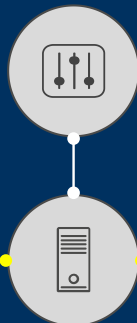
BLACKLIST

ViPNet Endpoint Protection



ViPNet Endpoint Protection

Консоль
управления



Сервер
ViPNet
Endpoint
Protection

ViPNet Endpoint Protection



ViPNet Endpoint Protection

Архитектура ViPNet Endpoint Protection

- Клиент
- Сервер
- Консоль управления

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

| Время | Personal Firewall | Application Control | HIPS |
|----------|-------------------|---------------------|------|
| 16:02:00 | 0 | 0 | 75 |
| 16:03:00 | 0 | 0 | 75 |
| 16:04:00 | 0 | 0 | 75 |
| 16:05:00 | 0 | 0 | 75 |
| 16:06:00 | 0 | 0 | 75 |
| 16:07:00 | 0 | 0 | 75 |
| 16:08:00 | 0 | 0 | 75 |
| 16:09:00 | 0 | 0 | 75 |
| 16:10:00 | 0 | 0 | 75 |
| 16:11:00 | 0 | 0 | 75 |
| 16:12:00 | 0 | 0 | 75 |
| 16:13:00 | 0 | 0 | 75 |
| 16:14:00 | 0 | 0 | 75 |
| 16:15:00 | 0 | 0 | 75 |
| 16:16:00 | 0 | 0 | 35 |

© 2019, ОАО "ИнфоТекС" Версия ПО: 1.0.2.59775

Выбор режима работы

The screenshot displays the 'Режимы работы' (Operating Modes) section of the ViPNet Endpoint Protection Server. The interface is divided into three main columns: 'Персональный межсетевой экран' (Personal Firewall), 'Контроль приложений' (Application Control), and 'Обнаружение и предотвращение вторжений' (Intrusion Detection and Prevention). Each column contains several modes with icons and brief descriptions. A left sidebar provides navigation options like 'Общие', 'Группы', and 'Режимы работы'.

ViPNet Endpoint Protection Server | Администратор

← Назад к Endpoint Protection

Основное
Общие
Группы
Режимы работы

Средства
Межсетевой экран
Контроль приложений
Обнаружение и предотвращение вторжений

Режимы работы

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.

Контроль приложений

- Черный список - Блокировать**
Новые приложения заносятся в черный список, любая его активность блокируется.
- Черный список - Уведомлять** ✓
Новые приложения заносятся в черный список, любая его активность блокируется. Приложение помечается маркером для оповещения пользов...
- Белый список - Уведомлять**
Новые приложения заносятся в белый список, приложению разрешен запуск, активность определяется правилами доступа к файлам, реест...
- Белый список - Разрешать**
Новые приложения заносятся в белый список, приложению разрешен запуск, активность определяется правилами доступа к файлам, реест...
- Отключен**
Контроль приложений отключен и не вляет на активность приложений.

Обнаружение и предотвращение вторжений

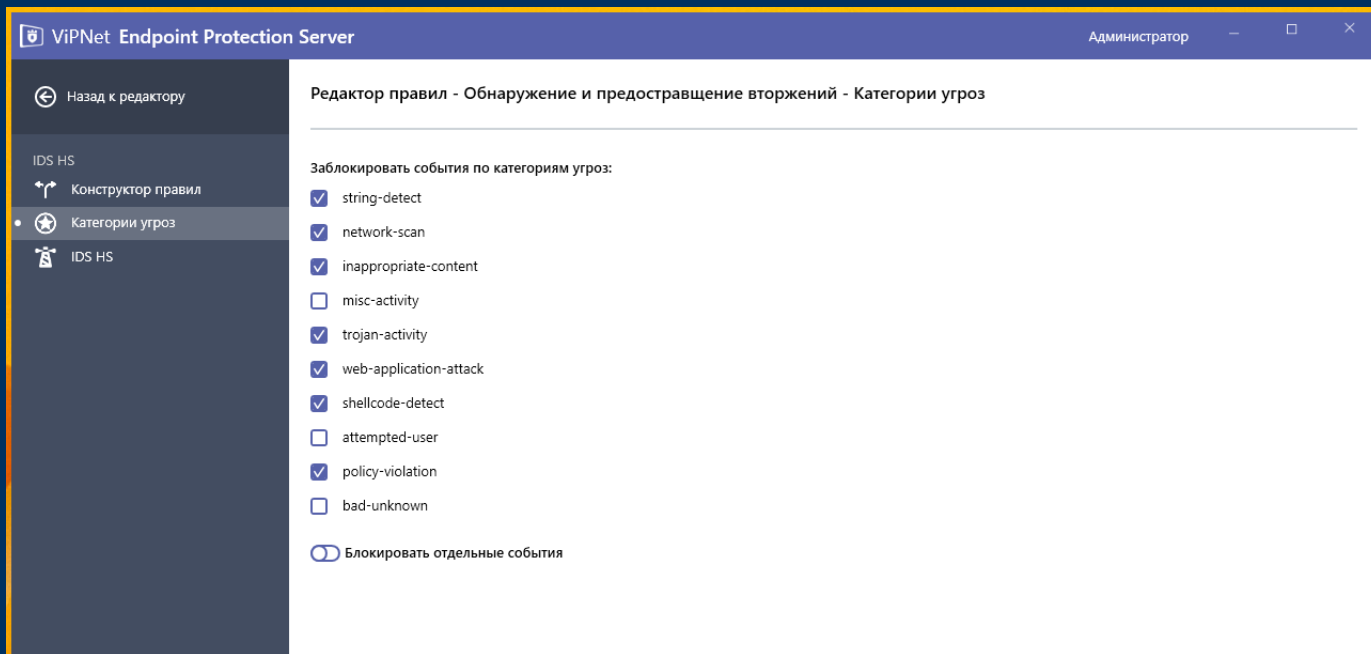
- Усиленный**
Используется полный набор правил. Может приводить к снижению производительности компьютера.
- Базовый** ✓
Используется оптимальный набор правил, обеспечивающий защиту в большинстве случаев.
- Минимальный**
Используется минимальный набор правил, защищающих от наиболее критичных атак.
- Отключен**
HIPS полностью выключен и не влияет на работу компьютера.

Чёрные и белые списки

The screenshot displays the 'ViPNet Endpoint Protection Server' interface. The title bar shows 'Администратор'. The left sidebar contains navigation options: 'Назад к редактору', 'Контроль' (with sub-item 'Запуск приложений'), and 'Защита' (with sub-item 'Правила доступа'). The main content area is titled 'Контроль приложений - Запуск приложений'. Below the title, there is a descriptive text: 'Приложения, которым разрешен запуск. Активность определяется правилами доступа к файлам, реестру, процессам.' Below this, there are tabs for 'Белый список' and 'Черный список'. A search bar with the placeholder 'Найти' and a magnifying glass icon is present, along with '+ Добавить' and a trash icon. A table lists applications under the 'Доверенные' (Trusted) category. Each row includes a checkbox, a toggle switch, and the application path.

| Программа |
|--|
| <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> c:\Windows*,* |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\Internet Explorer\iexplore.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\Internet Explorer\ieddiagcmd.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\7-Zip\7zFM.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\Registrar Registry Manger\rr.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\File Shredder\Shredder.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\Windows Mail\wab.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\Windows Mail\wabmig.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\Windows NT\Accessories\WORDPAD.EXE |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files\Notepad++\notepad++.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files (x86)\Windows Media Player\wmplayer.exe |
| <input type="checkbox"/> <input checked="" type="checkbox"/> C:\Program Files (x86)\Google\Chrome\Application\chrome.exe |

Обнаружение и предотвращение



The screenshot shows the 'VIPNet Endpoint Protection Server' interface. The title bar indicates the user is an administrator. The main window is titled 'Редактор правил - Обнаружение и предотвращение вторжений - Категории угроз'. On the left, a navigation pane shows 'Категории угроз' selected. The main area is titled 'Заблокировать события по категориям угроз:' and contains a list of threat categories with checkboxes:

- string-detect
- network-scan
- inappropriate-content
- misc-activity
- trojan-activity
- web-application-attack
- shellcode-detect
- attempted-user
- policy-violation
- bad-unknown

At the bottom, there is a radio button option: **Блокировать отдельные события**

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



ТЕХНО infotecs
2019 Фест

Спасибо
за внимание!