

# VIPNet EndPoint Protection

Новое сертифицированное  
многофункциональное средство защиты  
рабочих станций сотрудников

Кадыков Иван

Руководитель продуктового направления

# «Данные» – самый важный актив компании

Любая информация/данные могут стать ценной добычей для злоумышленников.

А если не украдут, так испортят.



# Всё плохое, что есть в IT мире..



# Использование различных техник

- Классические техники – защитные механизмы, использующие сигнатуры (правила). Защищаем от того, что знаем и видели.
- Современные техники (modern) – эвристические, использующие математические модели и методы искусственного интеллекта. Защита от ранее неизвестных атак и зловредов, а так же бесфайловых атак



# Вот бы всё в одном «флаконе» получить

## Классический Endpoint Protection

- знаем, что ищем (антивирус). Блокируем, что знаем (МЭ + HIPS), контролируем подключение устройств

## Next Generation Endpoint Protection

- классический Endpoint + модули по обнаружению и противодействию современным угрозам (ransomware, fileless-атаки, never-before-seen attacks) – Sandbox, Appcontrol, Memory Protection...

## Endpoint Detection & Response

- NG EPP + возможность расследования инцидента и формирование реакции на инцидент (forensic)

# НАШЕ РЕШЕНИЕ



# VIPNet EndPoint Protection

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

## СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БИ00

### СЕРТИФИКАТ СООТВЕТСТВИЯ № 4666

Внесен в государственный реестр системы сертификации  
средств защиты информации по требованиям безопасности информации  
22 марта 2023 г.

Выдан: 22 марта 2023 г.  
Действителен до: 22 марта 2028 г.

Настоящий сертификат удостоверяет, что изделие **VIPNet EndPoint Protection**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции межсетевых экранов и системы обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) и задания по безопасности ФРКЕ.00238-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00238-01 30 01.

Сертификат выдан на основании технического заключения от 21.02.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией АНО «Институт инженерной физики» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 03.03.2023, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: АО «ИнфоТеКС»  
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX,  
комната 29  
Телефон: (495) 737-6192



# Сертифицировано!

- Межсетевой экран тип В класс 4
- Система обнаружения вторжений У4
- 4 класс ТДБ

Сертифицирована версия 1.5.1



# Меры прописаны в правилах пользования

На картинке представлена  
лишь часть мер прописанных  
в документе

Таблица 1 – Реализация ViPNet EPP мер по защите информации

№ п/п	Содержание меры по обеспечению безопасности в [1], [2] и ее условное обозначение	Содержание меры по обеспечению безопасности в [3], [7] и ее условное обозначение
1.	ИАФ.1* Идентификация и аутентификация пользователей, являющихся работниками оператора	ИАФ.1* Идентификация и аутентификация пользователей и ниншируемых ими процессов
2.	ИАФ.3* Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	ИАФ.3* Управление идентификаторами
3.	ИАФ.4* Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	ИАФ.4* Управление средствами аутентификации
4.	ИАФ.5* Защита обратной связи при вводе аутентификационной информации	В [3], [7] отсутствует соответствующая мера
5.	УПД.1* Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	УПД.1* Управление учетными записями пользователей
6.	УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	УПД.2 Реализация модели управления доступом
7.	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между	ЗИС.6 Управление сетевыми потоками

# Защитные механизмы

## Контроль приложений



# Обнаружение и предотвращение атак

Используем:

- Эвристический анализ
- Сигнатурный анализ

Следим за:

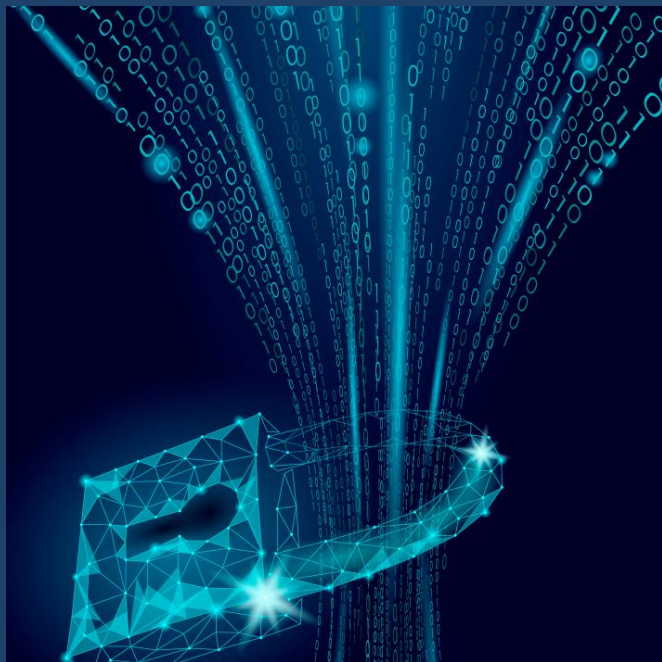
- Системными журналами Windows
- Журналами и логами приложений
- Изменениями в файловой системе и реестре
- Сетевым трафиком

Блокируем:

- Подозрительный сетевой трафик
- Атакующие хосты



# Межсетевое экранирование



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

# Контроль приложений

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



# Эвристический Antimalware движок

- Возможность сканирования исполняемых файлов и библиотек с целью выявления зловреда
- Эвристический Antimalware использует собственную модель построенную с помощью машинного обучения
- Модель постоянно обновляется в рамках подписки на БРП

# Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенной с помощью машинного обучения.

Выявляем различного рода аномалии, например:

- Аномальный вход в систему
- Аномалия в создании процесса
- Аномалия в создании задачи планировщику
- Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т.д.



# Обнаружение и предотвращение бесфайловых атак

Расширение возможностей модуля обнаружения и предотвращения вторжений

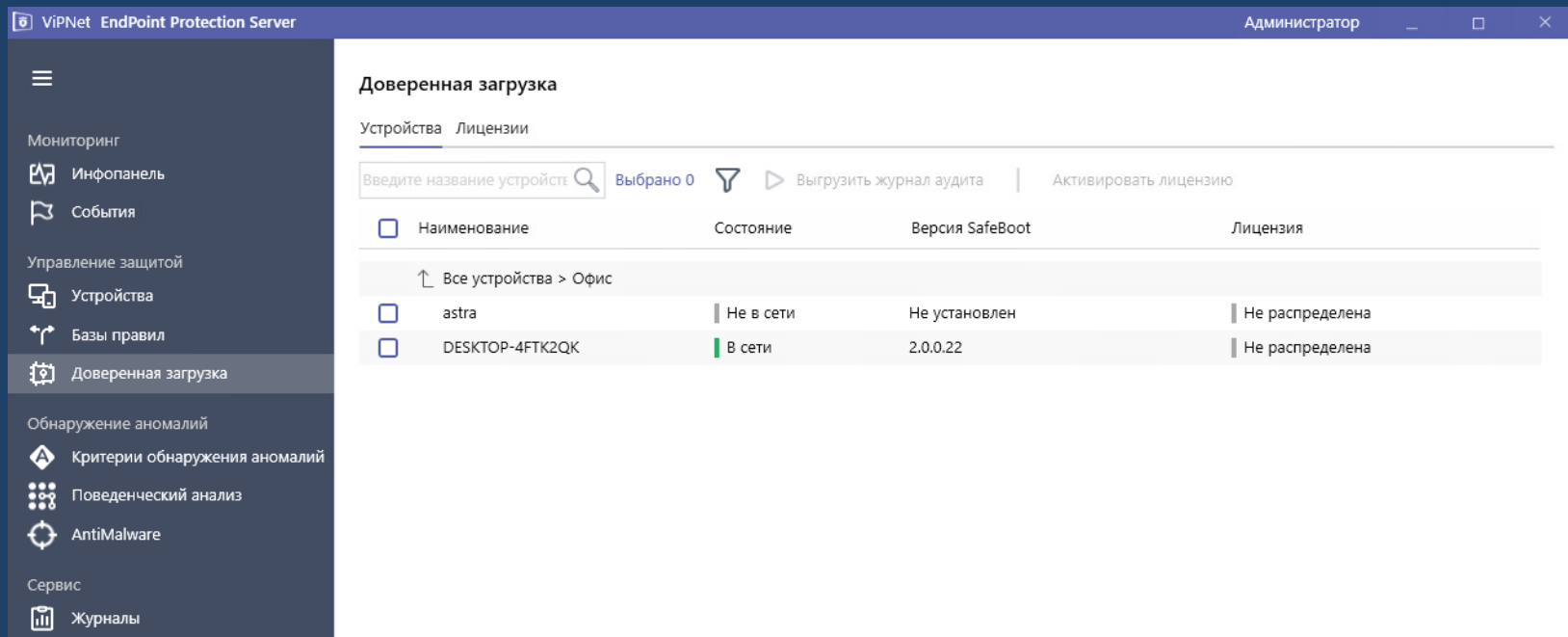
Отслеживаем техники Keylogging и Process injection

- Credential API Hooking (T1056.004)
- Process Hollowing (T1055.012)
- Process Doppelganging (T1055.013)
- Dynamic-link library injection (T1055.001)
- Portable Executable Injection (T1055.002)





# Управление ViPNet SafeBoot



ViPNet EndPoint Protection Server Администратор

### Доверенная загрузка

Устройства Лицензии

Введите название устройства 🔍 Выбрано 0 🔍 ▶ Выгрузить журнал аудита | Активировать лицензию

<input type="checkbox"/>	Наименование	Состояние	Версия SafeBoot	Лицензия
↑ Все устройства > Офис				
<input type="checkbox"/>	astra	Не в сети	Не установлен	Не распределена
<input type="checkbox"/>	DESKTOP-4FTK2QK	В сети	2.0.0.22	Не распределена

Передача событий в ViPNet TIAS

### Уровни передаваемых событий

Минимальный уровень событий: Информационное ▾

### Типы правил

- Обнаружение вторжений
  - Правила обнаружения локальных атак
  - Правила обнаружения сетевых атак
  - Выполняемые команды
  - Обнаружение установки ПО
  - Мониторинг файлов
  - Статус пакетов обновления Windows
  - Получение контрольных сумм файлов
- Персональный межсетевой экран
- Контроль приложений
- Предотвращение вторжений

### Сервер ViPNet TIAS

Адрес сервера ViPNet TIAS:  Порт:

Идентификатор ViPNet EPP Сервера:

# Интеграция с ViPNet TIAS

Возможность  
гранулированной передачи  
событий в ViPNet TIAS

# Другие варианты передачи данных

- электронная почта
- по syslog в формате cef

**Передача данных**

Электронная почта Active Directory Syslog TIAS

Использовать рассылку по электронной почте

**Настройки отправки оповещений**

Период отправки сообщений (минут):

Адрес отправителя:

**Почтовый сервер**

Почтовый сервер:  Порт:

Использовать SSL/TLS

**Авторизация**

Имя пользователя:

Пароль:

[Проверить настройки](#)

**Передача данных**

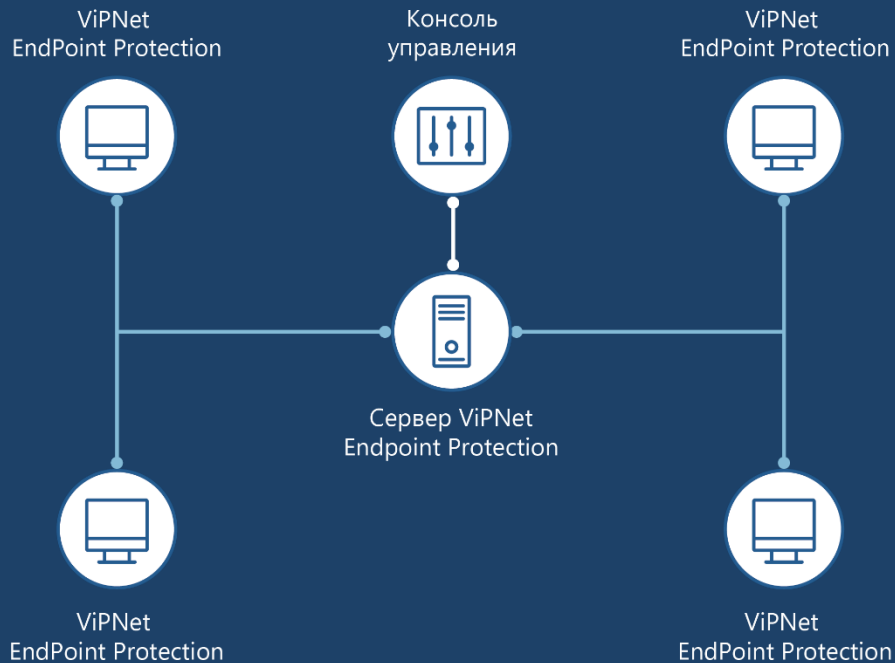
Электронная почта Active Directory Syslog TIAS

Передача событий в Syslog

**Уровни передаваемых событий**

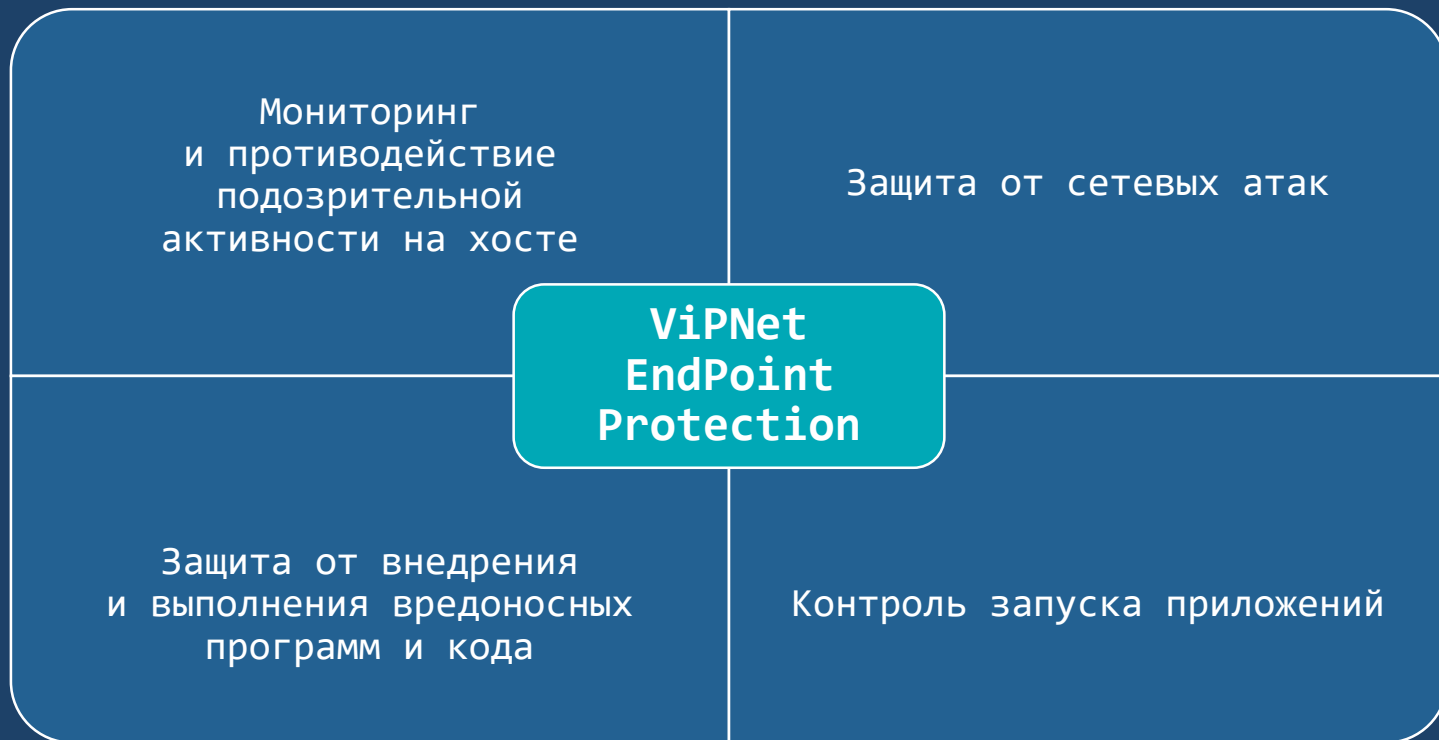
Минимальный уровень событий:

# Архитектура ViPNet EndPoint Protection



- Клиент
- Сервер
- Консоль управления

# Решаемые задачи



# Поддержка Linux

- Astra Linux Special Edition «Смоленск» 1.6 и 1.7
- РЕД ОС 7.3
- Альт Рабочая станция 8 СП
- Debian 11
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019



# 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

ЛИЦЕНЗИЯ				
Состояние:	Лицензия активирована			
Идентификатор лицензии:	2565538/1/1-EPP			
Дата окончания обновления баз правил:	08.12.2023			
Дата окончания действия лицензии:	08.12.2023			
ДОСТУПНЫЕ МОДУЛИ	ВСЕГО	ИСПОЛЬЗОВАНО	ОСТАЛОСЬ	АКТИВЕН ДО
HIDS	100	16	84	08.12.2023
Personal Firewall	100	16	84	08.12.2023
Application Control	100	16	84	08.12.2023
HIPS	100	16	84	08.12.2023
SafeBootMC	100	16	84	08.12.2023

# КРАТКИЙ ОБЗОР ИНТЕРФЕЙСА И ПРИНЦИПОВ РАБОТЫ



ViPNet EndPoint Protection Server | IvanK

### Информация

#### Персональный межсетевой экран

Режим	Хосты
Полная блокировка трафика	0
Публичная сеть	0
Частная сеть	5
Защищенная сеть	10
Сетевой экран отключен	2
Всего	17

#### Контроль приложений

Режим	Хосты
Блокировать	0
Разрешать	13
Отключен	4
Всего	17

#### Обнаружение и предотвращение вторжений

Режим	Хосты
Усиленный	0
Базовый	0
Минимальный	15
Отключен	2
Всего	17

#### Запросы на подключение

Всего запросов: **0**

Доступно лицензий: **84**

#### Актуальность баз правил

15 устройств с актуальными базами правил

2 устройств ожидают обновления

0 не назначено

#### Syslog

- ✓ Передача на IP 10.0.24.191:5000
- ✓ Последний обмен 10.04.2023 10:18:18

#### TIAS

- ✓ Передача на IP 10.0.24.164:34222
- ✓ Последний обмен 10.04.2023 10:18:18

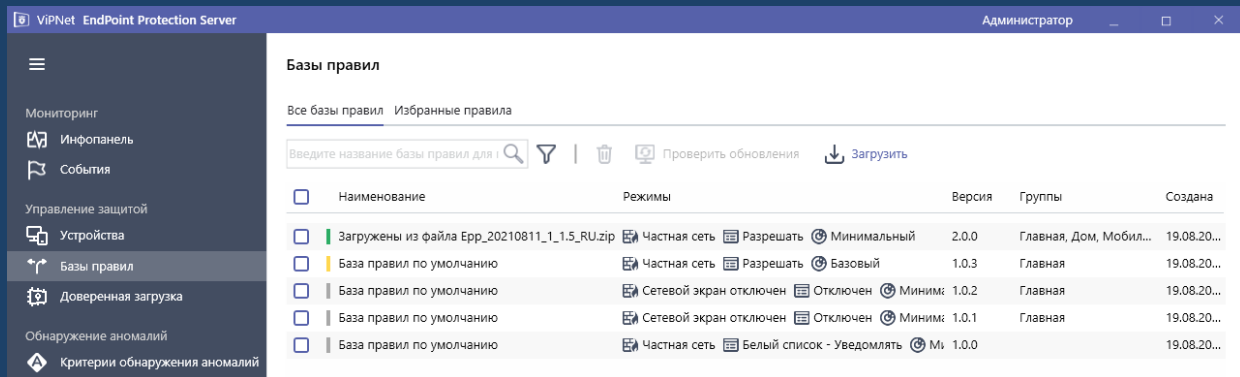
#### Сводка событий

15 мин | 1 час | 4 часа | 8 часов

Legend: Personal Firewall (green), Application Control (grey), HIPS (blue)

# Консоль управления сервером

# Работаем по правилам!



EndPoint Protection работает по БРП

## Состоит из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевого экрана
- Списков ПО для Черного и Белого списка
- Эвристического движка Anti-malware
- Движка обнаружения аномального поведения системных утилит

# Автоматическая загрузка БРП и избранные правила

Возможность автоматической загрузки БРП с сохранением ранее созданных правил.

## Параметры системы

Параметры Агента   Параметры Сервера   Обновление баз правил   Сервис

Использовать автоматическую загрузку обновлений баз правил

Дата и время последней проверки обновлений: неизвестно.

### Сервер обновления

Адрес сервера обновлений:

Имя пользователя:

Пароль:

### Прокси-сервер

Использовать прокси-сервер

Адрес сервера:

### Авторизация

С текущей учетной записью

С учетной записью

Имя пользователя:

Пароль:

Назад к EndPoint Protection
Сохранить Отмена

Основное

Сведения

**Режимы работы**

Средства

Персональный межсетевой экран

Контроль приложений

Обнаружение и предотвращение вторжений

### Редактор правил - 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

**Блокировать**

Запуск неизвестных приложений блокируется. Активность остальных приложений определяется правилами Контроля приложений.

**Разрешать** ✓

Запуск неизвестных приложений разрешен. Активность остальных приложений определяется правилами Контроля приложений.

**Отключен**

Контроль приложений отключен и не влияет на активность приложений.

#### 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 критических атак.

**Отключен**

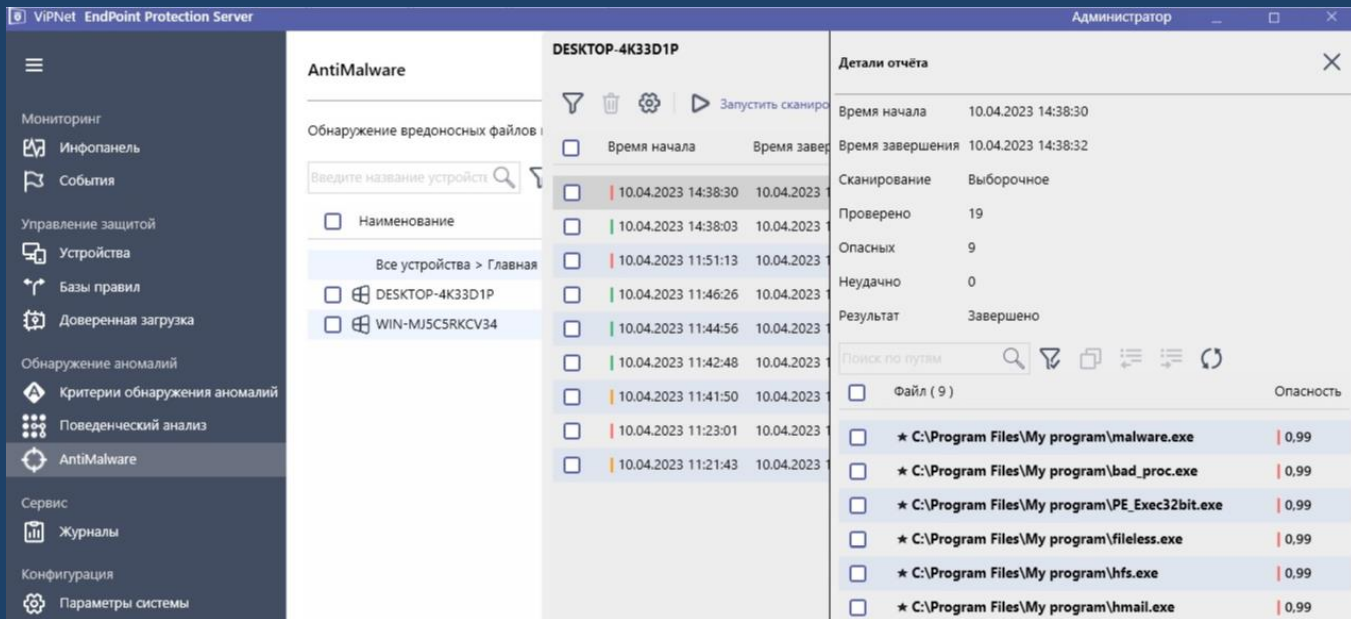
Модуль предотвращения вторжений полностью выключен и не влияет на работу компьютера.



# Настройки модулей — Режимы работы

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

28



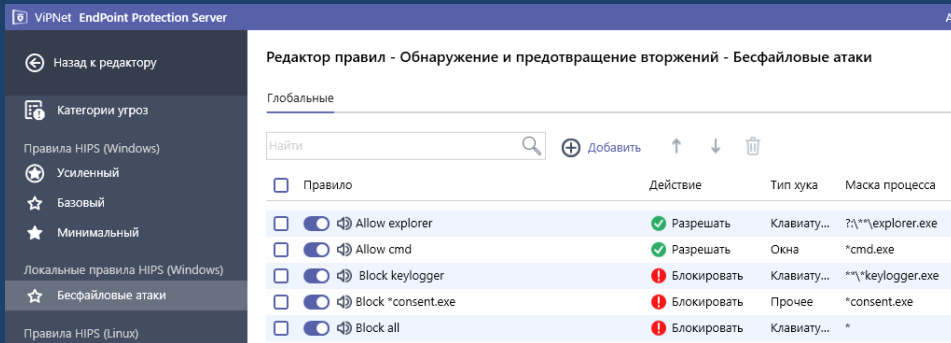
The screenshot shows the VIPNet EndPoint Protection Server interface. The main window displays the AntiMalware section for the device DESKTOP-4K33D1P. The interface is divided into several panes:

- Left Panel:** Navigation menu with categories like Мониторинг, Управление защитой, and Обнаружение аномалий. The AntiMalware section is currently selected.
- Center Panel:** A table showing the detection history for the device. The table has columns for 'Наименование', 'Время начала', and 'Время завершения'. The most recent entry is for the file 'C:\Program Files\My program\malware.exe' detected on 10.04.2023 at 14:38:30 with a risk score of 0.99.
- Right Panel (Детали отчёта):** A detailed report for the selected file. It shows the scan time (10.04.2023 14:38:30), the scan type (Выборочное), the number of files checked (19), and the number of dangerous files (9). The result is 'Завершено' (Completed).

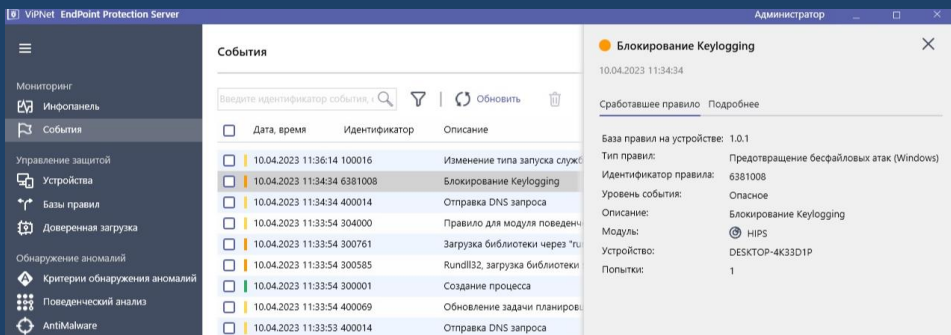
Наименование	Время начала	Время завершения	Опасность
C:\Program Files\My program\malware.exe	10.04.2023 14:38:30	10.04.2023 14:38:32	0,99
C:\Program Files\My program\bad_proc.exe	10.04.2023 14:38:03	10.04.2023 14:38:03	0,99
C:\Program Files\My program\PE_Exec32bit.exe	10.04.2023 11:51:13	10.04.2023 11:51:13	0,99
C:\Program Files\My program\fileless.exe	10.04.2023 11:46:26	10.04.2023 11:46:26	0,99
C:\Program Files\My program\hfs.exe	10.04.2023 11:44:56	10.04.2023 11:44:56	0,99
C:\Program Files\My program\hmail.exe	10.04.2023 11:42:48	10.04.2023 11:42:48	0,99
C:\Program Files\My program\hmail.exe	10.04.2023 11:41:50	10.04.2023 11:41:50	0,99
C:\Program Files\My program\hmail.exe	10.04.2023 11:23:01	10.04.2023 11:23:01	0,99
C:\Program Files\My program\hmail.exe	10.04.2023 11:21:43	10.04.2023 11:21:43	0,99

# Antimalware движок

- Эвристический подход
- Регулярное обновление в составе БРП



# Обнаружение и предотвращение бесфайловых атак



Входит в состав модуля «Обнаружения и предотвращения вторжений»

Видео-скриншот интерфейса VIPNet EndPoint Protection Server. В центре экрана отображается список событий, в котором выделено событие с идентификатором 7000101: "Аномальный запуск rundll32.exe". Справа от списка открыто всплывающее окно с подробными данными об этом событии, включая тип правила, описание, модуль и категорию.

Дата, время	Идентификатор	Описание
10.04.2023 14:21:39	400050	Регистрация доверенного процес...
10.04.2023 14:19:45	7000000	Аномальный вход в систему
10.04.2023 14:19:45	7000101	Аномальный запуск rundll32.exe
10.04.2023 14:19:44	304000	Правило для модуля поведенч...
10.04.2023 14:19:44	300001	Создание процесса
10.04.2023 14:19:44	400069	Обновление задачи планиров...
10.04.2023 14:05:59	500004	Вход в систему с полномочиям...
10.04.2023 14:05:59	500001	Интерактивный вход в систему
10.04.2023 14:05:59	400050	Регистрация доверенного процес...
10.04.2023 14:05:59	100016	Изменение типа запуска служб...
10.04.2023 14:05:59	100026	Удаление службы (реестр)
10.04.2023 14:04:52	400028	Изменен тип запуска службы
10.04.2023 14:04:52	100016	Изменение типа запуска служб...
10.04.2023 14:04:52	300761	Загрузка библиотеки через "tl...
10.04.2023 14:04:52	300585	rundll32, загрузка библиотеки
10.04.2023 14:04:52	304000	Правило для модуля поведенч...
10.04.2023 14:04:52	300001	Создание процесса
10.04.2023 14:04:52	300444	Возможный вредоносный арте...
10.04.2023 14:04:52	300489	Вредоносный артефакт: Исто...
10.04.2023 14:04:52	304000	Правило для модуля поведенч...
10.04.2023 14:04:52	300001	Создание процесса
10.04.2023 14:33:48	7000006	Аномалия в событии удаления
10.04.2023 14:33:48	7000005	Аномалия в событии создания
10.04.2023 14:31:48	7000004	Аномалия в событии создания

### Аномальный запуск rundll32.exe

10.04.2023 14:19:45

Сработавшее правило: Подробнее

Тип правил: Аномальная активность  
 Идентификатор правила: 7000101  
 Уровень события: Опасное  
 Превышение порога (IRE/RETH): 16.41/0.36  
 Описание: Аномальный запуск rundll32.exe  
 Модуль: Behavior Analytics  
 Устройство: WIN-MJ5C5RKC34  
 Попытки: 1

**Аномальное событие**  
 Отображать только важную информацию о событии

Дата: 08.03.2023 11:15:41  
 База правил на устройстве: 1.0.1  
 Тип правил: Контроль процессов (Windows)  
 Идентификатор правила: 304000  
 Уровень события: Важное  
 Описание: Правило для модуля поведенческого анализа  
 Модуль: HIDS  
 Попытки: 1  
 Категория: Подозрительная, потенциально опасная активность

Описание категории:  
 События данной категории могут свидетельствовать о компрометации системы либо указывать на факт компрометации, например: установка подозрительных служб/драйверов, изменение типа запуска служб, изменения в системном каталоге, изменения в группах пользователей, создание/удаление учетных записей, удаление важных файлов.

# Выявление аномалий

# ПЕРСПЕКТИВЫ РАЗВИТИЯ



# Планы на апрель-май

- Выпуск версии 1.5.2:
  - Поддержка новых «ядер» отечественных Linux
  - Bugfix
- Выполнение работ по Извещению по изменению



# Идёт активная работа



Параллельно разрабатывается релиз 1.6.

Главной целью релиза является – добавление новых защитных механизмов и интеграционные работы.

Подробнее дальше

# Межсетевое экранирование и работа с VipNet Clinet 4U

- Возможность управления фильтрами защищённой сети на хосте, через локальную консоль VipNet EndPoint Protection
- Организация ZTNA-политик:
  - Проверка хоста на наличие определённого ПО, полученных обновлений ПО и антивирусных баз и т.д.
  - Блокировка защищенной сети на устройстве при несоответствии устройства политикам ZTNA, информирование пользователя об этом



# Расширение возможностей по управлению ViPNet SafeBoot

- Централизованное обновление ViPNet SafeBoot из консоли ViPNet EPP Server
- Централизованная установка корневых сертификатов ViPNet SafeBoot из консоли ViPNet EPP Server
- Централизованное управление пользователями ViPNet SafeBoot из консоли ViPNet EPP Server

# А ещё будет!

- Модуль Safebrowsing
- Реализация SSL-инспекции на хосте
- Внедрение новых методик определения бесфайловых атак
- Реализация сервера под Linux
- Прочие улучшения





Спасибо за внимание!

Иван Кадыков

Руководитель продуктового направления

Ivan.Kadykov@infotecs.ru

---

Подписывайтесь на наши соцсети

---



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)