



# ViPNet EndPoint Protection for Linux

Руководство администратора

Версия продукта: 1.8.0

© АО «ИнфоТеКС», 2026

ФРКЕ.00238-01 32 02

Версия продукта: 1.8.0

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

Все условия эксплуатации и ограничения на использование ViPNet EPP приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet EPP.

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: [infotecs.ru](http://infotecs.ru)

Служба поддержки: [hotline@infotecs.ru](mailto:hotline@infotecs.ru)

# Содержание

|                                                                                               |           |
|-----------------------------------------------------------------------------------------------|-----------|
| <b>Введение.....</b>                                                                          | <b>8</b>  |
| О документе.....                                                                              | 9         |
| Соглашения документа.....                                                                     | 9         |
| О программном комплексе .....                                                                 | 10        |
| Требования к установке ViPNet EPP Сервер .....                                                | 12        |
| Требования к компьютеру пользователя для подключения к веб-интерфейсу ViPNet EPP Сервер ..... | 12        |
| Требования к установке ViPNet EPP Агент.....                                                  | 13        |
| Совместимость со сторонним программным обеспечением.....                                      | 15        |
| Комплект поставки.....                                                                        | 15        |
| Обратная связь.....                                                                           | 17        |
| <br><b>Глава 1. Общие сведения .....</b>                                                      | <b>18</b> |
| Основные функции .....                                                                        | 19        |
| Модели управления и принципы работы .....                                                     | 21        |
| Межсетевой экран.....                                                                         | 24        |
| Сетевой доступ с нулевым доверием (ZTNA) .....                                                | 30        |
| Схема фильтрации трафика при интеграции с ViPNet Client 5.....                                | 32        |
| Обнаружение и предотвращение вторжений .....                                                  | 36        |
| Обнаружение вторжений.....                                                                    | 36        |
| Предотвращение сетевых вторжений .....                                                        | 38        |
| Обнаружение аномалий с помощью критериев.....                                                 | 40        |
| Политика безопасности .....                                                                   | 41        |
| Уровни событий информационной безопасности.....                                               | 43        |
| Ролевая модель.....                                                                           | 44        |
| Отслеживание работы антивирусов.....                                                          | 45        |
| Лицензирование.....                                                                           | 47        |
| <br><b>Глава 2. Ввод в эксплуатацию.....</b>                                                  | <b>49</b> |
| Порядок ввода в эксплуатацию ViPNet EPP с агентами под управлением сервера .....              | 50        |
| Порядок ввода в эксплуатацию ViPNet EPP с автономными агентами .....                          | 52        |
| Установка, обновление, восстановление и удаление .....                                        | 53        |
| Подготовка к установке ViPNet EPP.....                                                        | 53        |
| Подготовка СУБД PostgreSQL на компьютере с ViPNet EPP Сервер .....                            | 54        |
| Установка ViPNet EPP Сервер .....                                                             | 55        |

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| Установка компонентов ViPNet EPP Сервер на один компьютер .....         | 55        |
| Установка компонентов ViPNet EPP Сервер на разные компьютеры .....      | 57        |
| Развёртывание инфраструктуры открытых ключей .....                      | 59        |
| Установка ViPNet EPP Агент .....                                        | 60        |
| Восстановление или удаление компонентов ViPNet EPP Сервер .....         | 63        |
| Восстановление или удаление ViPNet EPP Агент .....                      | 64        |
| Обновление .....                                                        | 64        |
| Порядок обновления ViPNet EPP версии 1.5.2 и выше до версии 1.8.0 ..... | 64        |
| Обновление ViPNet EPP Сервер .....                                      | 65        |
| Обновление ViPNet EPP Агент .....                                       | 66        |
| <b>Глава 3. Управление в ViPNet EPP Сервер .....</b>                    | <b>67</b> |
| Подключение к веб-интерфейсу ViPNet EPP Сервер .....                    | 68        |
| Интерфейс ViPNet EPP Сервер .....                                       | 70        |
| Установка и активация лицензии .....                                    | 72        |
| Управление защищаемыми узлами и группами .....                          | 73        |
| Подключение защищаемых узлов .....                                      | 73        |
| Настройка автоматического подключения защищаемых узлов .....            | 75        |
| Управление группами защищаемых узлов .....                              | 75        |
| Управление защищаемыми узлами группы .....                              | 77        |
| Управление политиками безопасности .....                                | 80        |
| Загрузка базы правил .....                                              | 83        |
| Автоматическая загрузка обновлений базы правил .....                    | 83        |
| Загрузка обновления базы правил вручную .....                           | 84        |
| Назначение политики группе узлов .....                                  | 87        |
| Порядок настройки политики .....                                        | 87        |
| Режимы модулей защиты .....                                             | 88        |
| Источник получения правил межсетевого экрана .....                      | 89        |
| Импорт данных из другой политики .....                                  | 89        |
| Правила фильтрации межсетевого экрана .....                             | 91        |
| Правила обнаружение вторжений .....                                     | 97        |
| Правила предотвращения вторжений .....                                  | 117       |
| Правила ZTNA .....                                                      | 125       |
| Правила контроля приложений .....                                       | 130       |
| Удаление политики .....                                                 | 144       |
| Настройка критериев обнаружения аномалий .....                          | 145       |
| Работа с журналами .....                                                | 146       |
| Критичные события агентов (Инфопанель) .....                            | 146       |
| Журналы событий .....                                                   | 149       |

|                                                                        |            |
|------------------------------------------------------------------------|------------|
| Журналы аудита .....                                                   | 151        |
| Запрос журнала регистрации трафика с ViPNet EPP Агент .....            | 152        |
| Администрирование ViPNet EPP Сервер.....                               | 155        |
| Управление рабочими серверами.....                                     | 155        |
| Добавление рабочего сервера на сервер управления .....                 | 155        |
| Просмотр и настройки параметров рабочих серверов.....                  | 155        |
| Удаление рабочего сервера .....                                        | 159        |
| Настройка параметров сервера управления .....                          | 159        |
| Настройка параметров защищаемых узлов.....                             | 163        |
| Управление учетными записями .....                                     | 164        |
| Требования к имени и паролю учетной записи.....                        | 166        |
| Проверка работоспособности и контроль целостности .....                | 166        |
| Диагностические журналы .....                                          | 168        |
| Обновление лицензии .....                                              | 168        |
| Интеграция с внешними системами.....                                   | 170        |
| Передача уведомлений по электронной почте .....                        | 170        |
| Подключение к почтовому серверу .....                                  | 171        |
| Передача событий информационной безопасности в сторонние системы ..... | 172        |
| Передача событий в сторонние системы по протоколу UDP.....             | 172        |
| Передача событий в ViPNet TIAS .....                                   | 173        |
| Выбор защищаемых узлов при настройке передачи событий.....             | 173        |
| <b>Глава 4. Локальное управление в ViPNet EPP Агент.....</b>           | <b>176</b> |
| Способы управления.....                                                | 177        |
| Управление с помощью графической консоли управления.....               | 178        |
| Подключение к ViPNet EPP Агент .....                                   | 178        |
| Интерфейс ViPNet EPP Агент.....                                        | 180        |
| Установка и активация лицензии .....                                   | 181        |
| Управление базой правил.....                                           | 182        |
| Загрузка и обновление базы правил .....                                | 182        |
| Распространение настроек модулей защиты на другие агенты .....         | 185        |
| Просмотр и настройка режимов работы модулей защиты .....               | 185        |
| Управление фильтрацией трафика.....                                    | 187        |
| Настройка пользовательских сетевых фильтров .....                      | 187        |
| Настройка пользовательских справочников .....                          | 190        |
| Управление обнаружением и предотвращением вторжений .....              | 193        |
| Просмотр и настройка правил обнаружения вторжений (HIDS) .....         | 194        |
| Просмотр и настройка сетевых правил предотвращения вторжений (HIPS)... | 199        |
| Настройка критериев обнаружения аномалий .....                         | 201        |

|                                                                                        |         |
|----------------------------------------------------------------------------------------|---------|
| Мониторинг .....                                                                       | 201     |
| Журнал событий .....                                                                   | 202     |
| Журнал активных соединений.....                                                        | 204     |
| Журнал трафика.....                                                                    | 205     |
| Администрирование ViPNet EPP Агент .....                                               | 208     |
| Управление учетными записями.....                                                      | 208     |
| Журнал аудита .....                                                                    | 210     |
| Просмотр и настройка параметров работы.....                                            | 212     |
| Проверка работоспособности .....                                                       | 215     |
| Просмотр сведений о программе и лицензии .....                                         | 217     |
| Уведомления об изменении настроек модулей защиты и обновлении<br>ViPNet SafeBoot ..... | 218     |
| Управление с помощью командного интерпретатора .....                                   | 220     |
| Подключение к ViPNet EPP Агент .....                                                   | 220     |
| Интерфейс командного интерпретатора .....                                              | 221     |
| Управление фильтрацией трафика.....                                                    | 222     |
| Просмотр и выбор режима работы .....                                                   | 223     |
| Просмотр журнала трафика .....                                                         | 223     |
| Просмотр активных соединений.....                                                      | 225     |
| Настройка пользовательских фильтров .....                                              | 226     |
| Настройка пользовательских справочников .....                                          | 228     |
| Просмотр статуса выполнения политики ZTNA.....                                         | 231     |
| Управление обнаружением и предотвращением вторжений .....                              | 232     |
| Журнал аудита.....                                                                     | 232     |
| Администрирование ViPNet EPP Агент .....                                               | 234     |
| Просмотр и управление параметрами работы .....                                         | 234     |
| Проверка работоспособности .....                                                       | 236     |
| Просмотр версии используемой базы правил .....                                         | 237     |
| Просмотр и изменение адреса ViPNet EPP Сервер .....                                    | 237     |
| Управление учетными записями.....                                                      | 238     |
| Требования к имени и паролю учетной записи.....                                        | 239     |
| Запуск и остановка ViPNet EPP Агент.....                                               | 240     |
| <br>Приложение А. Полномочия пользователей.....                                        | <br>241 |
| <br>Приложение В. Типы и идентификаторы правил.....                                    | <br>244 |
| <br>Приложение С. Структура CEF-сообщения .....                                        | <br>249 |

|                                                                                             |            |
|---------------------------------------------------------------------------------------------|------------|
| <b>Приложение D. Возможные неполадки .....</b>                                              | <b>264</b> |
| Потеряна связь с защищаемым узлом.....                                                      | 264        |
| В Kaspersky Endpoint Security Linux слишком большое количество проверяемых<br>объектов..... | 264        |
| Ошибка при обновлении ViPNet EPP Сервер на версию 1.8.0.....                                | 265        |
| <b>Приложение E. Термины и сокращения.....</b>                                              | <b>266</b> |



# Введение

|                         |    |
|-------------------------|----|
| О документе             | 9  |
| О программном комплексе | 10 |
| Обратная связь          | 17 |

# О документе

Документ поможет вам установить, настроить и использовать компоненты программного комплекса ViPNet EndPoint Protection for Linux (далее — ViPNet EPP), предназначенные для работы в ОС GNU/Linux.

Документ предназначен для администраторов информационной безопасности организаций.

Что нового в ViPNet EPP версии 1.8.0 см. в документе «ViPNet EPP for Windows. Руководство администратора».

## Соглашения документа

| Обозначение     | Описание                                                                   |
|-----------------|----------------------------------------------------------------------------|
| Название        | Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки          |
| Клавиша+Клавиша | Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую |
| Меню > Команда  | Последовательность элементов или действий                                  |
| Код             | Имя файла, путь, фрагмент кода или команда в командной строке              |



**Примечание.** В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

Обозначения при описании команд в документе:

- Команды, которые могут быть выполнены только в режиме администратора, выделены красным цветом:  
`команда`
- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки:  
`команда <параметр>`
- Необязательные параметры или ключевые слова заключены в квадратные скобки:  
`команда <обязательный параметр> [необязательный параметр]`
- Если можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:  
`команда {вариант-1 | вариант-2}`

# О программном комплексе

ViPNet EPP предназначен для комплексной защиты персональных компьютеров пользователей и корпоративных серверов организаций от различных [угроз безопасности информации](#) путем идентификации [событий информационной безопасности](#) и реагирования на угрозы на основе анализа событий.

ViPNet EPP включает:

- Компоненты для установки в ОС GNU/Linux:
  - Клиентский компонент — ViPNet EPP Агент for Linux (далее — ViPNet EPP Агент или агент). Устанавливается на персональные компьютеры и корпоративные серверы — [защищаемые узлы](#). Идентифицирует события информационной безопасности и обеспечивает безопасность информации с помощью модулей защиты:
    - [Межсетевой экран](#). Выполняет фильтрацию IP-трафика и блокирует нежелательную сетевую активность.
    - Обнаружение вторжений (см. [Обнаружение и предотвращение вторжений](#)). Обнаруживает сетевые атаки и атаки уровня защищаемого узла.
    - Предотвращение вторжений (см. [Предотвращение сетевых вторжений](#)). Обнаруживает и блокирует сетевые атаки на защищаемом узле.
    - Сетевой доступ с нулевым доверием ZTNA (см. [Сетевой доступ с нулевым доверием \(ZTNA\)](#)). Позволяет на защищаемых узлах с установленной программой ViPNet Client 5 контролировать доступ к ресурсам защищенной [сети ViPNet](#) и разрешать его только при условии выполнения правил, заданных для защищаемых узлов (далее — политика ZTNA). На защищаемых узлах без ViPNet Client 5 выполняется только отслеживание невыполнения политики ZTNA.

Полный список и описание модулей защиты см. в главе [Общие сведения](#).
- Серверный компонент — ViPNet EPP Сервер for Linux (далее — ViPNet EPP Сервер или сервер). Состоит из:
  - ViPNet EPP Сервер управления (далее — сервер управления) — обеспечивает централизованное управление агентами на защищаемых узлах и управление ViPNet EPP Рабочий сервер. Управление агентами выполняется через ViPNet EPP Рабочий сервер.  
Сервер управления может быть только один.
  - ViPNet EPP Рабочий сервер (далее — рабочий сервер) — непосредственно взаимодействует с агентами на защищаемых узлах, которые он обслуживает, и обеспечивает:
    - Пересылку данных между сервером управления и агентами, включая отправку базы правил (политики безопасности).
    - Сбор и хранение событий информационной безопасности, полученных от агентов.

- Передачу зарегистрированных событий информационной безопасности в сторонние системы мониторинга и анализа (SIEM, ViPNet TIAS и другие) и отправку по электронной почте.

- Клиентский и серверный компоненты для установки в ОС Windows (далее — ViPNet EPP Агент for Windows и ViPNet EPP Сервер for Windows). Подробно об использовании этих компонентов см. в документе «ViPNet EPP for Windows. Руководство администратора».

К ViPNet EPP Сервер for Linux могут быть подключены для управления ViPNet EPP Агент for Windows и ViPNet EPP Агент for Linux.

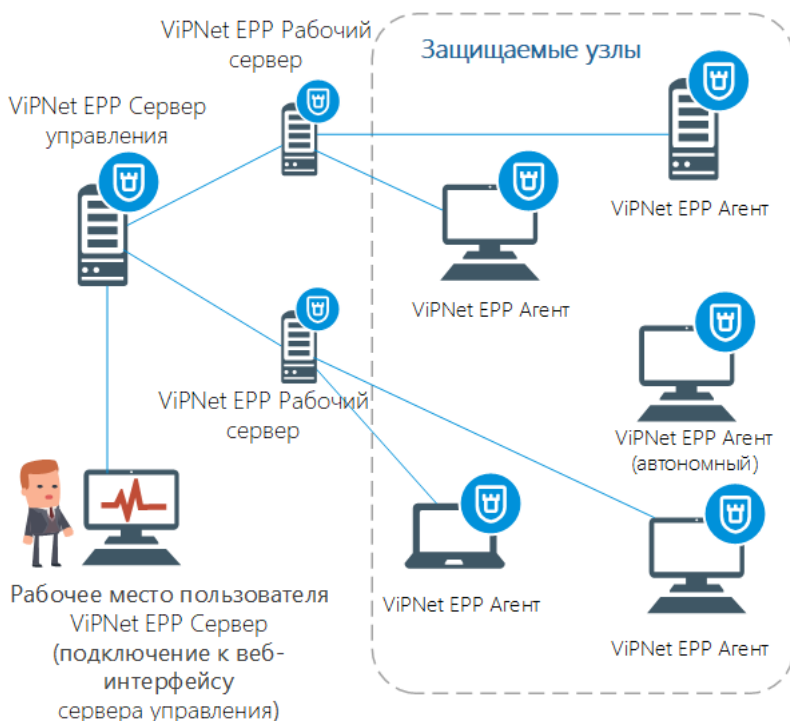


Рисунок 1. Компоненты ViPNet EPP на примере схемы с двумя рабочими серверами

ViPNet EPP Агент может работать в нескольких моделях управления:

- Под управлением ViPNet EPP Сервер (далее — ViPNet EPP Агент под управлением сервера).
- Автономно (далее — автономный ViPNet EPP Агент).

Модель управления ViPNet EPP Агент определяется лицензией. Подробнее о [моделях управления и принципах работы ViPNet EPP](#).

Список основных функций компонентов ViPNet EPP for Linux см. в разделе [Основные функции](#).

## Требования к установке ViPNet EPP Сервер

Требования к компьютеру, предназначенному для установки сервера управления или рабочего сервера:

- Процессор — x86-совместимый, количество физических ядер 4 и более, тактовая частота — не менее 3.2 ГГц.
- Объем оперативной памяти — не менее 16 Гбайт.
- Свободное место на диске (рекомендуется твердотельный накопитель) — не менее 500 Гбайт.
- Сетевой адаптер.
- Операционная система (64-разрядная): Astra Linux Special Edition 1.8.2.7 БЮЛЛЕТЕНЬ № 2025-0411SE18 (оперативное обновление 1.8.2).
- Графический интерфейс пользователя операционной системы: Fly-wm.
- СУБД PostgreSQL версии 15.12-astra.se1 (защищенная версия в основном репозитории на установочном диске ОС Astra Linux).
- Apache2 версии 2.4.62-3astra.se1 (защищенная версия в основном репозитории на установочном диске ОС Astra Linux).

## Требования к компьютеру пользователя для подключения к веб-интерфейсу ViPNet EPP Сервер

Для подключения к веб-интерфейсу ViPNet EPP Сервер на компьютере пользователя должен быть установлен один из поддерживаемых браузеров:

- Google Chrome версии 142.0 и выше.  
Системные требования к ОС и аппаратному обеспечению приведены на [сайте производителя](#).
- Mozilla Firefox версии 115.0 и выше.  
Системные требования к ОС и аппаратному обеспечению приведены на [сайте производителя](#).
- Яндекс Браузер версии 25.10 и выше.  
Системные требования к ОС и аппаратному обеспечению приведены на [сайте производителя](#).

Общие рекомендации для подготовки компьютера, с которого будет выполняться управление через веб-интерфейс:

- Установите последний пакет обновлений для ОС.
- Синхронизируйте системное время ОС и ViPNet EPP.
- В настройках браузера разрешите использование Cookie и протокола TLS версии 1.3.
- Установите разрешение экрана не менее 1366x768 пикселей.

## Требования к установке ViPNet EPP Агент

Требования к компьютеру, предназначенному для установки агента:

- Процессор — x86-совместимый, количество физических ядер 2 и более, тактовая частота — не менее 3.2 ГГц.
- Объем оперативной памяти — не менее 4 Гбайт.
- Свободное место в корневом разделе жесткого диска — не менее 5 Гбайт.
- Сетевой адаптер.
- Операционная система GNU/Linux (64-разрядная) одного из следующих дистрибутивов:
  - Astra Linux Special Edition 1.8.3.8, ядро Linux 6.12.34-1-generic #astra1+ci3;
  - Astra Linux Special Edition 1.8.3.8, ядро Linux 6.1.141-1-generic #astra1+ci7;
  - Astra Linux Special Edition 1.8.2.7, ядро Linux 6.12.11-1-generic #astra1+ci18;
  - Astra Linux Special Edition 1.8.1.12, ядро Linux 6.1.90-1-generic #astra2+ci15;
  - Astra Linux Special Edition 1.7.8.6, ядро Linux 6.1.141-1-generic #astra1+ci38;
  - Astra Linux Special Edition 1.7.8.6, ядро Linux 5.15.0-142-generic #astra1+ci172;

Использование режима замкнутой программной среды (ЗПС) поддерживается во всех Astra Linux Special Edition, кроме Astra Linux Special Edition «Опел».

- Альт СП Рабочая станция релиз 10.2.1, ядро Linux 6.12.28-6.12-alt0.ci10f.2;
- Альт Рабочая станция 10.4, ядро Linux 6.1.115-un-def-alt1;
- РЕД ОС 8.0 «Муром» Рабочая станция, сертифицированная редакция, ядро Linux 6.12.37-1.red80.x86\_64;
- РЕД ОС 7.3 «Муром» Рабочая станция, сертифицированная редакция, ядро Linux 6.1.148-1.el7.3.x86\_64;
- РЕД ОС 7.3 «Муром» Рабочая станция, сертифицированная редакция, ядро Linux 5.15.178-1.el7.3.x86\_64;
- РЕД ОС 7.3 «Муром» Рабочая станция, сертифицированная редакция, ядро Linux 6.1.110-1.el7.3.x86\_64;

- РЕД ОС 8.0.2 «Муром» Рабочая станция, стандартная редакция, ядро Linux 6.12.37-1.red80.x86\_64;
- РЕД ОС 8.0.2 «Муром» Рабочая станция, стандартная редакция, ядро Linux 6.6.76-1.red80.x86\_64;
- РЕД ОС 8.0 «Муром» Рабочая станция, стандартная редакция, ядро Linux 6.6.6-1.red80.x86\_64;
- РЕД ОС 7.3.6 «Муром» Рабочая станция, стандартная редакция, ядро Linux 6.1.148-1.el7.3.x86\_64;
- РЕД ОС 7.3.6 «Муром» Рабочая станция, стандартная редакция, ядро Linux 5.15.178-1.el7.3.x86\_64;
- РЕД ОС 8.0 «Муром» Рабочая станция, сертифицированная редакция, ядро Linux 6.12.56-1.red80.x86\_64;
- AlterOS 9.6 Agile Phoenix, ядро Linux 6.6.101-1.el9.alteros.x86\_64;
- Debian Linux 12.11 (bookworm), ядро Linux 6.1.0-35-amd64;
- Debian Linux 12.5 (bookworm), ядро Linux 6.1.0-18-amd64.



**Внимание!** При использовании других ядер ОС ViPNet EPP может работать с ограничениями.

---

- Для операционной системы должны быть установлены пакеты:
  - РЕД ОС — xcb-util-cursor.
  - Альт — libxcbutil-cursor.
  - Debian Linux:
    - libxcb-cursor0;
    - libxcb-xinerama0;
    - iptables — установите командой `apt-get install iptables`;
    - gnome-shell-extension-top-icons-plus — установите командой `sudo apt install gnome-shell-extension-top-icons-plus`.
- Графический интерфейс пользователя операционной системы:
  - Для ОС Astra Linux — Fly-wm.
  - Для ОС РЕД ОС, Альт — MATE.
  - Для ОС Debian Linux — GNOME.

# Совместимость со сторонним программным обеспечением

ViPNet EPP for Linux совместим со следующим программным обеспечением:

- Передает события информационной безопасности в ViPNet TIAS версий 3.10, 3.11.
- Может использоваться на защищаемых узлах совместно с [ViPNet SafePoint](#) версий 1.7.0, 1.8.0 (для ОС Linux).
- Может использоваться на защищаемых узлах совместно с [ViPNet Client 4U](#) версии 4.8.0, [ViPNet Client 5](#) версий 5.0, 5.1 (для ОС Linux).



**Внимание!** При использовании ViPNet Client 4U на защищаемом узле не будут применяться фильтры политик безопасности из ViPNet Policy Manager (или ViPNet Prime Policy Management) для фильтрации IP-трафика открытой сети и исключения ZTNA. Номер версии ViPNet Client 5, в которой будет поддержана функция передачи состояния для ZTNA, см. в документации ViPNet Client 5 после выпуска официальной версии ViPNet Client 5.

- На защищаемых узлах с ViPNet Client 5 могут использоваться фильтры политик безопасности:
  - из ViPNet Policy Manager версии 4.5 и ViPNet Administrator версии 4.6.11;
  - из ViPNet Prime Policy Management версии 1.9 и ViPNet Prime версии 1.9.11.
- На защищаемых узлах отслеживается работа антивирусного программного обеспечения (далее — антивирусов):
  - Kaspersky Endpoint Security версий 12.2.0–2412, 12.3.0–1162.
  - Dr.Web Desktop Security Suite версий 11.1, 11.1 в исполнении 2.

## Комплект поставки

В комплект поставки ViPNet EPP входят компоненты для установки в ОС Windows и ОС GNU/Linux:

- Установочные файлы для развертывания в ОС Windows:
  - ViPNet EPP Сервер и ViPNet EPP Серверная консоль — `ViPNetEppServerSetup_x64_RU_1.x.x.xxxx.msi`.
  - ViPNet EPP Агент — `ViPNetEppSetup_x64_RU_1.x.x.xxxx.msi`.
  - Microsoft .NET Desktop Runtime версии 8.0.11 — `windowsdesktop-runtime-8.0.11-win-x64.exe`.
  - СУБД PostgreSQL версии 14 — `postgresql-14.17-1-windows-x64.exe`.
  - Microsoft Visual C++ 2015–2022 Redistributable Package x64 — `VC_redist.x64.exe`.

- Установочные пакеты для развертывания в ОС GNU/Linux:
  - ViPNet EPP Сервер в составе:
    - `epp2-common-components_x86-64_1.x.x.xxxx.deb`;
    - `epp2-main-server_x86-64_1.x.x.xxxx.deb`;
    - `epp2-worker-server_x86-64_1.x.x.xxxx.deb`.
  - ViPNet EPP Агент для:
    - ОС Debian, Astra Linux — `EPP_x86-64_RU_1.x.x-xxxx.deb`;
    - ОС Ред ОС, Альт Рабочая станция, AlterOS — `EPP_x86-64_RU_1.x.x-xxxx.rpm`.
  - Открытый ключ `infotecs_pub.key`, необходимый для работы ViPNet EPP Агент в режиме замкнутой программной среды для поддерживаемых ОС Astra Linux Special Edition.
  - Файлы с базой системных правил в формате ZIP для автономных ViPNet EPP Агент, развернутых в ОС Windows и ОС GNU/Linux.
- PDF-файлы документации:
  - «ViPNet EPP for Linux. Руководство администратора».
  - «ViPNet EPP for Windows. Руководство администратора».
  - «ViPNet EPP. Руководство пользователя».
  - «ViPNet EPP. Сторонние лицензии».

# Обратная связь

## Контактная информация

- Единый многоканальный телефон:  
+7 (495) 737-6192,  
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: [hotline@infotecs.ru](mailto:hotline@infotecs.ru).  
Форма для обращения в службу поддержки через сайт.  
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: [soft@infotecs.ru](mailto:soft@infotecs.ru).

## Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу [security-notifications@infotecs.ru](mailto:security-notifications@infotecs.ru). Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется [политикой ответственного разглашения](#).

# 1

## Общие сведения

|                                            |    |
|--------------------------------------------|----|
| Основные функции                           | 19 |
| Модели управления и принципы работы        | 21 |
| Межсетевой экран                           | 24 |
| Обнаружение и предотвращение вторжений     | 36 |
| Политика безопасности                      | 41 |
| Уровни событий информационной безопасности | 43 |
| Ролевая модель                             | 44 |
| Отслеживание работы антивирусов            | 45 |
| Лицензирование                             | 47 |

# Основные функции

Основные функции ViPNet EPP for Linux:

- Фильтрация IP-трафика защищаемого узла (см. [Межсетевой экран](#)).
- Контроль доступа к ресурсам защищенной сети ViPNet с помощью технологии сетевого доступа с нулевым доверием (ZTNA) (см. [Сетевой доступ с нулевым доверием \(ZTNA\)](#)).
- Обнаружение угроз безопасности информации, которые могут свидетельствовать об атаках внутри защищаемого узла или сетевых атаках (см. [Обнаружение вторжений](#)).
- Предотвращение сетевых угроз безопасности информации (см. [Предотвращение сетевых вторжений](#)).
- Контроль аномальной активности защищаемого узла с помощью критериев (см. [Обнаружение аномалий с помощью критериев](#)).
- Управление доверенной загрузкой (ViPNet SafeBoot) на защищаемых узлах. Для использования этой функции защищаемые узлы с ОС GNU/Linux должны быть подключены к ViPNet EPP Сервер for Windows, поскольку управление доступно только в ViPNet EPP Сервер for Windows (см. в документе «ViPNet EPP for Windows. Руководство администратора», раздел «Управление доверенной загрузкой»).

Функции мониторинга и оповещения ViPNet EPP:

- Отслеживание работы антивирусов Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite и блокировка трафика в случае вирусной угрозы (см. [Отслеживание работы антивирусов](#)).
- Регистрация событий информационной безопасности защищаемого узла в журнале событий ViPNet EPP Агент.
- Консолидация событий информационной безопасности защищаемых узлов в ViPNet EPP Сервер и визуализация сводки критичных событий на инфопанели (см. [Критичные события агентов \(Инфопанель\)](#)).
- Оповещение о событиях информационной безопасности по электронной почте (см. [Передача уведомлений по электронной почте](#)). Настройка доступна в ViPNet EPP Сервер.
- Передача событий информационной безопасности в сторонние SIEM-системы и ViPNet TIAS (см. [Передача событий информационной безопасности в сторонние системы](#)). Настройка доступна в ViPNet EPP Сервер.

Служебные функции ViPNet EPP:

- Обновление базы системных правил (см. [Политика безопасности](#)).
- [Управление учетными записями](#) и разграничение полномочий пользователей (см. [Ролевая модель](#)).
- [Управление защищаемыми узлами и группами](#).
- [Управление рабочими серверами](#).

- Регистрация действий пользователей в журналах аудита ViPNet EPP Сервер (см. [Журналы аудита](#)) и ViPNet EPP Агент (см. [Журнал аудита](#)).
- Проверка работоспособности ViPNet EPP Сервер (см. [Проверка работоспособности и контроль целостности](#)) и ViPNet EPP Агент (см. [Проверка работоспособности](#)).

# Модели управления и принципы работы

## Работа ViPNet EPP Агент под управлением ViPNet EPP Сервер

Защищаемые узлы с ViPNet EPP Агент подключаются к ViPNet EPP Сервер. ViPNet EPP Агент for Windows и ViPNet EPP Агент for Linux могут быть подключены к ViPNet EPP Сервер for Linux или к ViPNet EPP Сервер for Windows.

**Внимание!** В ViPNet EPP Сервер for Linux не поддерживаются функции управления ViPNet EPP Агент:



- Управление параметрами сканирования AntiMalware и запуск сканирования.
- Обнаружение аномалий с помощью поведенческого анализа.
- Управление ViPNet SafeBoot.

Управление настройками и модулями защиты ViPNet EPP Агент, а также получение сведений о зарегистрированных событиях и состоянии защищаемых узлов, выполняется централизованно в ViPNet EPP Серверная консоль for Windows (или в веб-интерфейсе ViPNet EPP Сервер for Linux).

Схема, иллюстрирующая принцип работы ViPNet EPP с ViPNet EPP Агент под управлением ViPNet EPP Сервер, приведена на рисунке ниже.

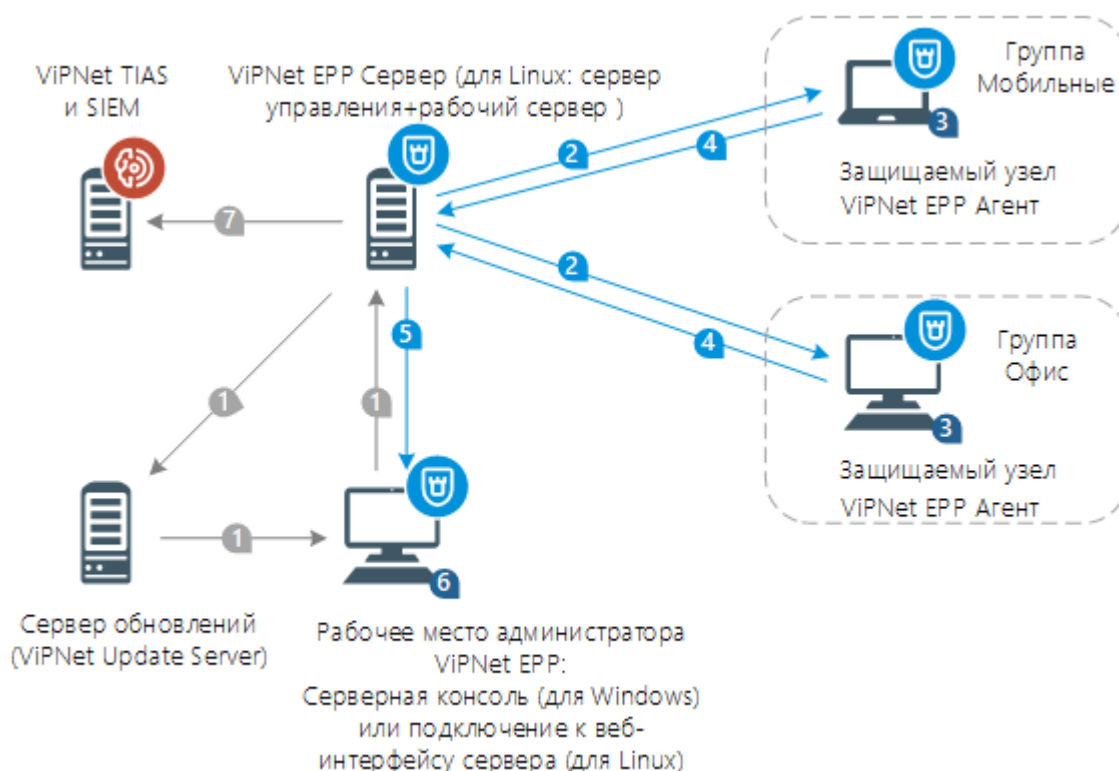


Рисунок 2. Работа ViPNet EPP Агент под управлением ViPNet EPP Сервер

Взаимодействие и работа происходит в следующем порядке:

- 1 Администратор ViPNet EPP настраивает автоматическую загрузку обновлений [базы системных правил](#) (далее — база правил) с сервера обновлений ИнфоТеКС [ViPNet Update Server](#) (далее — сервер обновлений) на ViPNet EPP Сервер или вручную скачивает с сервера обновлений последнюю версию базы правил и загружает ее в ViPNet EPP Сервер.
- 2 Администратор ViPNet EPP подключает защищаемые узлы к серверу, размещая их в группы. Администратор указывает модули защиты, которые будут работать на узле, и назначает базу правил (политику безопасности) на группы защищаемых узлов. При необходимости дополнительно настраивает базу правил (политику безопасности).
- 3 ViPNet EPP Агент применяет базу правил (политику безопасности) для защиты узла и идентификации событий информационной безопасности на защищаемом узле. В случае идентификации, событие регистрируется в журнале с одним из уровней (см. [Уровни событий информационной безопасности](#)), определяющим степень опасности.
- 4 Сведения о событиях информационной безопасности защищаемого узла передаются в ViPNet EPP Сервер.
- 5 ViPNet EPP Сервер в режиме, близком к реальному времени, консолидирует в журнале событий сведения, полученные от защищаемых узлов, и обнаруживает аномальную локальную и сетевую активность.
- 6 Администратор ViPNet EPP просматривает журнал событий ViPNet EPP Сервер, содержащий сведения о событиях информационной безопасности всех защищаемых узлов и создает на их основе новые [политики безопасности](#).
- 7 При необходимости администратор ViPNet EPP настраивает передачу зарегистрированных событий информационной безопасности в сторонние системы мониторинга и анализа — [SIEM](#) и ViPNet TIAS — для выявления [инцидентов информационной безопасности](#).

## Автономная работа ViPNet EPP Агент

Защищаемые узлы с ViPNet EPP Агент работают и настраиваются без подключения к ViPNet EPP Сервер. Настройка каждого автономного ViPNet EPP Агент выполняется индивидуально в локальной консоли управления. Возможен перевод автономного ViPNet EPP Агент на работу под управлением ViPNet EPP Сервер (см. [Перевод автономного ViPNet EPP Агент под управление ViPNet EPP Сервер](#)). Обратный перевод возможен только через удаление и повторную установку ViPNet EPP Агент.

Схема, иллюстрирующая принцип работы ViPNet EPP с автономными ViPNet EPP Агент, приведена на рисунке ниже.

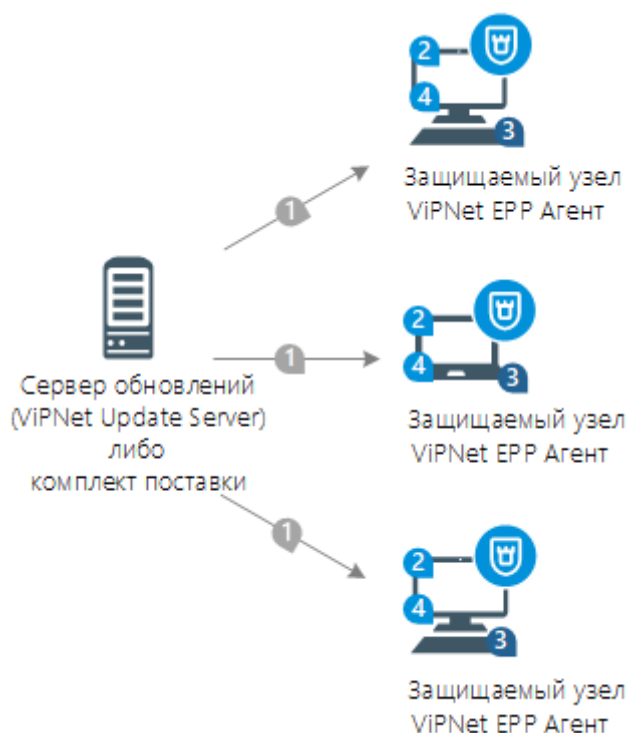


Рисунок 3. Автономная работа ViPNet EPP Агент

Настройка и работа происходит в следующем порядке:

- 1 Администратор ViPNet EPP Агент загружает на каждый защищаемый узел с ViPNet EPP Агент базу правил из комплекта поставки, либо при наличии подписки на обновление, вручную выгруженную с сервера обновлений ИнфоТеКС [ViPNet Update Server](#) (далее — сервер обновлений) последнюю версию [базы правил](#).
- 2 Администратор ViPNet EPP Агент при необходимости дополнительно настраивает базу правил на каждом защищаемом узле или настраивает ее на одном из защищаемых узлов, экспортирует, а затем импортирует на другие защищаемые узлы.
- 3 ViPNet EPP Агент применяет базу правил для защиты узла и идентификации событий информационной безопасности на защищаемом узле и обнаруживает аномальную локальную и сетевую активность. В случае идентификации, событие регистрируется в журнале событий с одним из уровней (см. [Уровни событий информационной безопасности](#)), определяющим степень опасности.
- 4 Администратор ViPNet EPP Агент просматривает на каждом защищаемом узле журнал событий, содержащий сведения о событиях информационной безопасности защищаемого узла и создает на их основе новые [политики безопасности](#).

# Межсетевой экран

Модуль защиты Межсетевой экран ViPNet EPP Агент выполняет фильтрацию IP-пакетов на защищаемом узле.

При установке ViPNet EPP Агент на компьютере с ViPNet Client 5 межсетевой экран ViPNet EPP Агент будет выполнять фильтрацию IP-трафика открытой сети. На компьютере с ViPNet Client 4U или ViPNet Client 5 межсетевой экран ViPNet EPP Агент может использоваться также для создания пользовательских фильтров защищенной сети для фильтрации IP-трафика между узлами [сети ViPNet](#).

Требования к программе ViPNet Client 5 (ViPNet Client 4U), совместимой с ViPNet EPP, см. в разделе Совместимость ViPNet EPP со сторонним программным обеспечением (см. [Совместимость со сторонним программным обеспечением](#)).

Результат фильтрации IP-пакетов открытой сети зависит от выбранного режима работы и действия сетевых фильтров межсетевого экрана. Служебный IP-трафик ViPNet EPP, необходимый для взаимодействия ViPNet EPP Агент с ViPNet EPP Сервер, в открытой сети всегда пропускается.

Сетевые фильтры разделены на три категории:

- **Фильтры политик безопасности** — основные фильтры IP-трафика на защищаемом узле:
  - Создаются в ViPNet EPP Сервер и действуют в пределах одной политики безопасности (см. [Политика безопасности](#)). Передаются с сервера на защищаемые узлы, подключенные к серверу, в политике безопасности и определяют общие для этих узлов параметры фильтрации. В автономном ViPNet EPP Агент фильтры политик безопасности из ViPNet EPP Сервер недоступны.
  - Если на защищаемом узле установлена программа ViPNet Client 5, ViPNet EPP Агент сможет получать фильтры политик безопасности из ViPNet Policy Manager (или ViPNet Prime Policy Management) для фильтрации IP-трафика открытой сети. Источник получения фильтров политик безопасности, которые будет использовать ViPNet EPP Агент, [настраивается в ViPNet EPP Сервер](#).

В автономном ViPNet EPP Агент фильтры политик безопасности из ViPNet Policy Manager или ViPNet Prime Policy Management начнут использоваться сразу после получения.

При получении фильтры из ViPNet Policy Manager (ViPNet Prime Policy Management) автоматически импортируются в ViPNet EPP Агент. Результаты импорта фильтров доступны в журнале аудита. При возникновении ошибок импорта в журнале аудита зафиксированы события с указанием проблемных фильтров.

Изменить или удалить фильтры политик безопасности на защищаемом узле невозможно.

- **Пользовательские фильтры** — создаются пользователем на защищаемом узле для учета особенностей фильтрации:
  - Фильтры открытой сети — для фильтрации IP-трафика защищаемого узла. Если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5, будет фильтроваться IP-трафик открытой сети, не относящийся к трафику сети ViPNet.

- Фильтры защищенной сети ViPNet — доступны только на защищаемом узле с установленной программой ViPNet Client 4U или ViPNet Client 5, для фильтрации трафика защищенной сети между своим узлом и узлами сети ViPNet, с которыми есть связь в программе ViPNet Client. Целесообразно использовать фильтры защищенной сети только для блокирования IP-трафика, поскольку заблокированный политиками безопасности ViPNet Client IP-трафик разрешить фильтрами защищенной сети ViPNet нельзя. Например, вы можете создать фильтр блокировки IP-трафика от своего узла к другому узлу из списка доступных узлов сети ViPNet.

В автономном ViPNet EPP Агент все сетевые фильтры, загружаемые из базы правил, попадают в категорию пользовательских фильтров. Пользовательские фильтры могут быть также загружены при импорте базы правил с другого защищаемого узла. При экспорте базы правил экспортируются только фильтры открытой сети.

Пользовательские фильтры можно изменять и удалять на защищаемом узле.

- **Системный фильтр** — фильтры по умолчанию, заданы в политике безопасности и в зависимости от режима определяют действия с IP-пакетом, если не сработал ни один из фильтров политик безопасности или пользовательских фильтров открытой сети. Если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5, фильтры по умолчанию будут применяться к IP-трафику открытой сети.

Изменить фильтры по умолчанию на защищаемом узле и на ViPNet EPP Сервер невозможно.

Параметры сетевого фильтра:

- Протоколы сетевого, транспортного уровней модели OSI.
- IP-адреса источника и назначения протоколов IPv4 и IPv6.
- Номера портов транспортных протоколов TCP и UDP, коды/типы сообщений ICMP.
- Команды прикладного протокола HTTP (OPTIONS, GET, HEAD, POST, PUT, PATCH, DELETE, TRACE, CONNECT) и типы файлов мобильного кода (JavaScript, PDF).
- Расписание.

При совпадении параметров, заданных в сетевом фильтре, с одноименными параметрами IP-пакета в период времени, указанный в расписании, фильтр срабатывает с одним из действий:

-  **Блокировать** — IP-пакет блокируется.
-  **Разрешить** — IP-пакет пропускается.

Для упрощения задания параметров сетевых фильтров используются справочники, каждый из которых объединяет несколько объектов одного типа:

- **Протоколы** — содержат любую комбинацию сетевых, транспортных протоколов, а также их параметров.
- **Адреса открытой сети** — содержат различные комбинации IPv4- либо IPv6-адресов или их диапазонов.

- **Узлы сети ViPNet** — справочник доступен только на защищаемом узле с установленной программой ViPNet Client 4U или ViPNet Client 5. Содержит сетевые узлы, с которыми есть связь в программе ViPNet Client 4U или ViPNet Client 5.

Предустановленные справочники:

- **Мой компьютер** — IP-адреса сетевых интерфейсов защищаемого узла.  
Выбор этого справочника в сетевом фильтре в качестве адреса источника будет означать исходящий трафик, а в качестве адреса назначения — входящий.
- **Другие компьютеры** — любые IP-адреса, кроме **Мой компьютер**.
- **Другие компьютеры VPN** — справочник доступен на защищаемом узле с установленной программой ViPNet Client 4U или ViPNet Client 5 и относится к типу **Справочники ViPNet**. Содержит все имена сетевых узлов сети ViPNet, с которыми есть связь в программе ViPNet Client 4U или ViPNet Client 5, кроме **Мой компьютер**.
- **Расписания** — содержат любую комбинацию параметров, определяющих время применения сетевого фильтра.

Также в справочнике могут быть заданы исключения, состоящие из того же набора объектов.

Справочники, используемые в фильтрах политик безопасности, являются глобальными. Они передаются в ViPNet EPP Агент в составе политики безопасности и не могут быть изменены. Справочники, используемые в пользовательских фильтрах — пользовательские справочники — настраиваются локально на защищаемом узле. Если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5, доступно создание пользовательских справочников адресов сети ViPNet.



**Внимание!** Исключения, заданные в любом справочнике сетевого фильтра с запрещенными командами протокола HTTP или запрещенными типами файлов мобильного кода, будут игнорироваться при фильтрации трафика ViPNet EPP Агент.

---

Режимы работы межсетевого экрана ViPNet EPP Агент:

- **Полная блокировка трафика** — это режим максимальной защиты узла, при котором блокируются любые входящие и исходящие соединения открытой сети. Защищаемый узел полностью отключен от открытой сети.
- **Публичная сеть (Усиленный)** — в этом режиме блокируются все входящие и исходящие соединения открытой сети, кроме разрешенных фильтрами политик безопасности. Режим рекомендуется использовать при работе в общественной сети. Режим доступен только для ViPNet EPP Агент под управлением сервера.
- **Частная сеть (Базовый)** — в этом режиме по умолчанию блокируются все входящие и исходящие соединения, кроме разрешенных фильтрами политик безопасности и пользовательскими фильтрами. Режим рекомендуется использовать при работе в частной сети, например, из дома.

- **Корпоративная сеть (Пользовательский)**— в этом режиме по умолчанию пропускаются все исходящие и входящие соединения открытой сети, кроме соединений, запрещенных пользовательскими фильтрами. Режим рекомендуется использовать при работе в сети с относительно низким уровнем угроз безопасности.
- **Отключено** — в этом режиме межсетевого экран отключен и не влияет на сетевой трафик.

В ViPNet EPP Сервер при настройке политики безопасности (см. [Политика безопасности](#)) режимы работы можно изменять. Режим работы передается на ViPNet EPP Агент защищаемого узла централизованно в составе политики безопасности. Для учета особенностей фильтрации IP-пакетов на защищаемом узле режим работы межсетевого экрана ViPNet EPP Агент можно изменить локально. Обновление политики безопасности может изменить этот режим.

Таблица 1. Применение сетевых фильтров в зависимости от режима работы межсетевого экрана ViPNet EPP Агент

| Режим работы              | Фильтры политик безопасности | Пользовательские фильтры открытой сети | Действие фильтров по умолчанию (системных фильтров)                                               |
|---------------------------|------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------|
| Полная блокировка трафика | Не применяются               | Не применяются                         |  Блокировать   |
| Публичная сеть            | Применяются                  | Не применяются                         |  Блокировать |
| Частная сеть              | Применяются                  | Применяются                            |  Блокировать |
| Корпоративная сеть        | Не применяются               | Применяются                            |  Разрешить   |
| Отключено                 | Не применяются               | Не применяются                         | Не применяются                                                                                    |

Для каждого режима работы настраивается свой список сетевых фильтров. Сетевые фильтры применяются последовательно до первого срабатывания: **Фильтры политик безопасности > Пользовательские фильтры > Системный фильтр**.

Все входящие и исходящие IP-пакеты проходят проверку в соответствии с режимом работы и сетевыми фильтрами:

- В режиме **Полная блокировка трафика** IP-пакет блокируется.
- В режимах **Публичная сеть**, **Частная сеть** и **Корпоративная сеть**:
  - Если IP-пакет был пропущен в соответствии с одним из этих режимом работы и сработал один из фильтров этого режима работы, то IP-пакет пропускается или блокируется в соответствии с действием фильтра.
  - Если IP-пакет был пропущен сетевым фильтром, для пропуска ответных IP-пакетов в рамках текущего соединения должен быть настроен соответствующий сетевой фильтр.
  - Если ни один из фильтров не сработал, IP-пакет блокируется или пропускается в соответствии с фильтром по умолчанию этого режима работы.

- Если в IP-пакет инкапсулированы данные протокола HTTP, сетевой фильтр, в параметрах которого указан протокол HTTP, будет применяться в последнюю очередь.
- В режиме **Отключено** IP-пакет пропускается.

Такой способ фильтрации IP-пакетов обеспечивает высокий уровень безопасности, разрешая соединения только с нужными узлами по заданным протоколам и портам.

Результаты применения фильтров фиксируются в [журнале трафика](#).

Схема фильтрации IP-трафика для защищаемых узлов (IP-трафика открытой сети — для защищаемых узлов с ViPNet Client 4U или ViPNet Client 5) приведена на рисунке ниже.

Общую схему фильтрации ViPNet EPP Агент входящего и исходящего IP-трафика на защищаемом узле с установленной программой ViPNet Client 5 (ViPNet Client 4U) см. в разделе [Схема фильтрации трафика при интеграции с ViPNet Client 5](#).

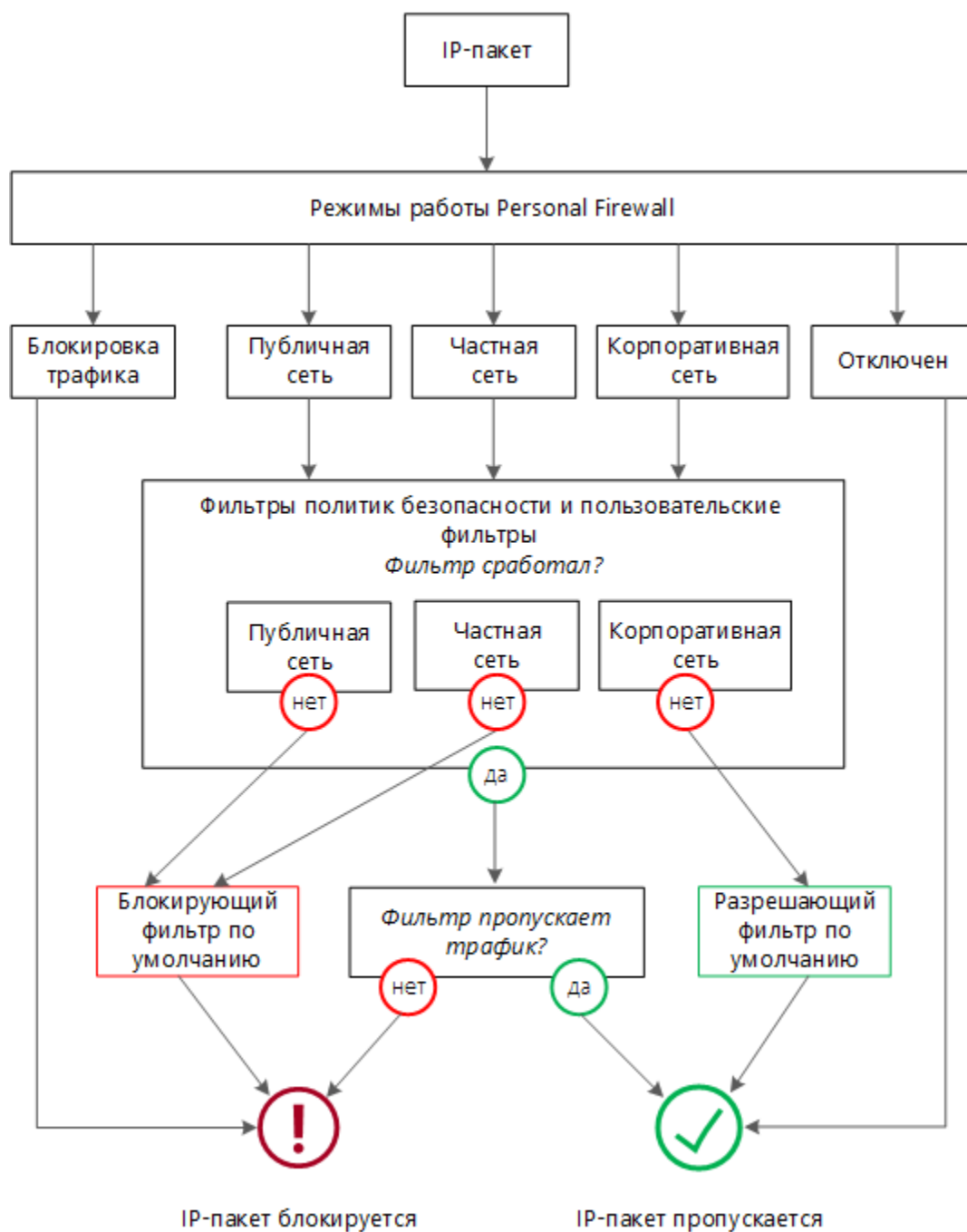


Рисунок 4. Схема фильтрации IP-трафика открытой сети

# Сетевой доступ с нулевым доверием (ZTNA)

Технология сетевого доступа с нулевым доверием в ViPNet EPP Агент реализована модулем защиты ZTNA. Для использования модуля ZTNA (далее — ZTNA) на защищаемом узле лицензия ViPNet EPP (см. [Лицензирование](#)) должна содержать разрешение на использование модуля [Межсетевой экран](#). ZTNA работает только в ViPNet EPP Агент под управлением сервера.

Технология сетевого доступа с нулевым доверием позволяет на всех защищаемых узлах, подключенных к ViPNet EPP Сервер, отслеживать выполнение политик ZTNA, заданных для защищаемых узлов. На защищаемых узлах с установленной программой ViPNet Client 5 (ViPNet Client 4U) также контролируется доступ к ресурсам защищенной [сети ViPNet](#). В результате доступ разрешается только при условии выполнения на защищаемом узле политики ZTNA. Для блокирования доступа к ресурсам защищенной [сети ViPNet](#) на защищаемых узлах должен быть включен модуль Межсетевой экран.

Требования к программе ViPNet Client 5 (ViPNet Client 4U), совместимой с ViPNet EPP, см. в разделе Совместимость ViPNet EPP со сторонним программным обеспечением (см. [Совместимость со сторонним программным обеспечением](#)).

Политика ZTNA настраивается в ViPNet EPP Сервер и отправляется в ViPNet EPP Агент в составе политики безопасности. Из ViPNet Policy Manager (или ViPNet Prime Policy Management) могут быть получены исключения ZTNA со списком узлов сети ViPNet, которые будут доступны на защищаемом узле даже при невыполнении политики ZTNA (например, с целью получить необходимые данные для выполнения политик). Если ViPNet EPP Сервер является узлом защищенной сети ViPNet, в ViPNet Policy Manager (ViPNet Prime Policy Management) необходимо добавить ViPNet EPP Сервер в исключения (см. документацию к продукту ViPNet Policy Manager (ViPNet Prime Policy Management)).

В ViPNet EPP Агент доступен только просмотр статуса выполнения политики ZTNA.

На защищаемом узле с установленной программой ViPNet Client 5 при попытке получить доступ к ресурсу защищенной сети ViPNet запускается проверка соответствия параметров защищаемого узла настроенной политике ZTNA, в случае невыполнения политики доступ к защищенной сети ViPNet будет заблокирован и отобразится уведомление о блокировке. Данные о заблокированном трафике будут доступны в [журнале трафика](#).

Если на защищаемом узле из ViPNet Policy Manager (ViPNet Prime Policy Management) были получены данные об исключениях ZTNA, при невыполнении политики ZTNA соответствующая часть ресурсов защищенной сети ViPNet останутся доступными.

Схему применения ZTNA и фильтрации IP-пакетов ViPNet EPP Агент на защищаемом узле с установленной программой ViPNet Client 5 см. в разделе [Схема фильтрации трафика при интеграции с ViPNet Client 5](#).

Пользователь ViPNet EPP Агент может посмотреть статус выполнения политики ZTNA, где указаны:

- один из статусов: политика не назначена, политика выполняется или политика не выполняется;
- список ресурсов защищенной сети ViPNet, которые останутся доступными при невыполнении политики (при наличии);

- в случае невыполнения политики — название правила, которое стало причиной блокирования доступа.

Политики ZTNA задаются набором правил отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux. В ViPNet EPP Сервер [Правила ZTNA](#) можно использовать правила из базы правил и добавить собственные правила.

В базе правил добавлены правила для антивирусов (по умолчанию выключены):

- Наличие работающего антивируса Kaspersky Antivirus — после включения проверяет, что на защищаемом узле установлен и запущен Kaspersky Antivirus с актуальными базами.
- Наличие работающего антивируса Dr.Web Antivirus — после включения проверяет, что на защищаемом узле установлен и запущен Dr.Web Antivirus с актуальными базами.

Для каждой ОС можно включить только одно из правил. Чтобы правило применялось на защищаемых узлах, должны быть включены проверки актуальности баз антивируса и другие параметры, заданные для правил (по умолчанию включены). По умолчанию базы правил антивирусов считаются актуальными 2 дня.

При настройке любых правил для защищаемых узлов с ОС Windows доступно добавление проверок по следующим параметрам:

- Список программного обеспечения, которое должно или не должно быть установлено на защищаемом узле. Проверяться будет только программное обеспечение из списка программ и компонентов Windows.
- Список процессов, которые должны или не должны быть запущены на защищаемом узле.
- Список служб, которые должны или не должны выполняться на защищаемом узле.
- Список файлов, которые должны или не должны присутствовать на защищаемом узле.
- Список путей к ключам реестра, которые должны или не должны существовать на защищаемом узле. Для целочисленных и строковых значений ключей могут быть заданы дополнительные критерии проверки.

При настройке любых правил для защищаемых узлов с ОС GNU/Linux доступно добавление проверок по следующим параметрам:

- Список служб systemd, которые должны или не должны выполняться на защищаемом узле.
- Список файлов, которые должны или не должны присутствовать на защищаемом узле.
- Список модулей ядра ОС, которые должны или не должны быть загружены на защищаемом узле.
- Список версий ядра ОС, которые должны или не должны использоваться на защищаемом узле. Могут быть заданы различные критерии сравнения: больше, меньше, равно и прочие.

# Схема фильтрации трафика при интеграции с ViPNet Client 5

Фильтрация IP-трафика ViPNet EPP Агент на защищаемом узле с установленной программой [ViPNet Client 5](#) выполняется по следующим принципам:

- Для трафика открытой сети применяются фильтры политик безопасности, пользовательские фильтры открытой сети, фильтры по умолчанию, а также блокировка активных соединений приложений.
- Для трафика защищенной сети ViPNet применяются политики ZTNA (см. [Сетевой доступ с нулевым доверием \(ZTNA\)](#)), пользовательские фильтры защищенной сети ViPNet, а также блокировка активных соединений приложений.
- Запрещающие правила имеют приоритет:
  - Если в ViPNet Client 5 определенный трафик защищенной сети ViPNet заблокирован фильтрами политики безопасности, а в ViPNet EPP Агент этот же трафик разрешен, будет действовать правило блокировки трафика из ViPNet Client 5.
  - Если в ViPNet EPP Агент задан пользовательский фильтр защищенной сети ViPNet для блокировки определенного трафика, а в ViPNet Client 5 этот же трафик разрешен, будет действовать правило блокировки трафика из ViPNet EPP Агент. Например, если в ViPNet EPP Агент заблокирован 53 порт для всех исходящих соединений защищенной сети, то и защищенные DNS-серверы будут недоступны, даже если в ViPNet Client 5 не задано никаких блокировок.



**Примечание.** Сетевые фильтры открытой и защищенной сети, содержащие контентную фильтрацию HTTP-трафика, будут применяться на этапах 2, 4, 5 (см. схемы ниже).

---

- Служебный трафик ViPNet EPP всегда пропускается в открытой сети. Служебный IP-трафик ViPNet EPP, необходимый для взаимодействия ViPNet EPP Агент с ViPNet EPP Сервер, в открытой сети всегда пропускается. В защищенной сети может потребоваться дополнительная настройка ViPNet Client 5 (см. документацию к ViPNet Policy Manager (ViPNet Prime Policy Management)).

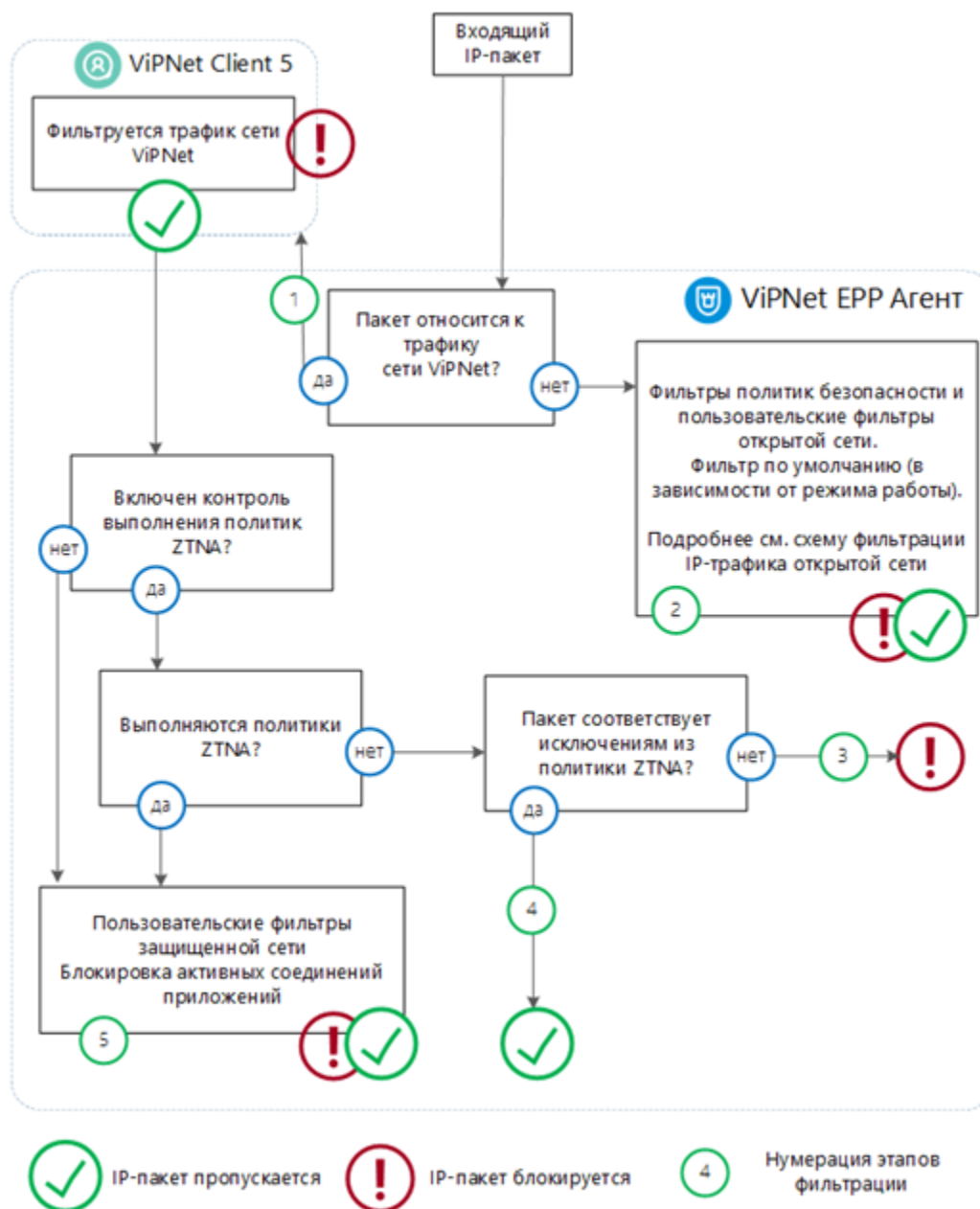


Рисунок 5. Фильтрация входящего трафика



3 Системный фильтр **Невыполнение политик ZTNA**.

4 Сетевой фильтр **Исключение по пропуску трафика (ZTNA)**.

5 Сетевой фильтр из списка пользовательских фильтров защищенной сети.

Сетевой фильтр **Блокировка сетевых соединений приложения** (только в ViPNet EPP Агент for Linux).

Сетевой фильтр **Правило фильтрации HTTP-контента**.

Системный фильтр **Пропуск VPN трафика пользователя (нешифрованный)** — это событие регистрируется, если не сработали предыдущие фильтры этапа.

6 Системный фильтр **Пропуск трафика VPN сети (шифрованный)**.

Описание фильтров см. в разделе [Журнал трафика](#).

# Обнаружение и предотвращение вторжений

Функции обнаружения и предотвращения вторжений ViPNet EPP Агент реализованы несколькими методами:

- Применение правил обнаружения вторжений на основе сигнатур наиболее распространенных угроз и правил предотвращения вторжений, входящие в состав политики безопасности (базы правил (см. [Политика безопасности](#))). Реализовано в модулях:

- Обнаружение вторжений (HIDS) — обнаруживает вторжения с помощью правил сигнатурного анализа (см. [Обнаружение вторжений](#)).

С целью обнаружения вторжений в непрерывном режиме модуль HIDS всегда активен. Остановка его работы недоступна.

- Предотвращение вторжений (HIPS) — предотвращает [сетевые вторжения](#), выявленные правилами сигнатурного анализа, с помощью правил предотвращения вторжений.

Правила обнаружения и предотвращения вторжений настраиваются на ViPNet EPP Сервер и передаются на ViPNet EPP Агент защищаемого узла централизованно в составе политики безопасности. В автономном ViPNet EPP Агент настройки выполняются локально.

- Применение методов обнаружения аномалий с помощью критериев (см. [Обнаружение аномалий с помощью критериев](#)).

Критерии обнаружения аномалий настраиваются в ViPNet EPP Сервер. В автономном ViPNet EPP Агент настройки критериев обнаружения аномалий выполняются локально.

Совместное применение сигнатурного анализа и критериев обнаружения аномалий позволяет получить целостное представление о событиях информационной безопасности всех защищаемых узлов.

## Обнаружение вторжений

Для обнаружения вторжений в ViPNet EPP Агент применяется сигнатурный анализ, основанный на применении правил обнаружения событий информационной безопасности — правил обнаружения вторжений (HIDS). Правила обнаружения вторжений формируются на основе сигнатур наиболее распространенных угроз и включают правила, применяемые на сетевом и локальном уровнях.

На сетевом уровне сигнатурный анализ реализован с помощью правил обнаружения сетевых атак. Эти правила содержат сигнатуры, позволяющие обнаружить сетевую атаку по конкретным, свойственным ей признакам. В случае наличия аналогичного активного правила предотвращения вторжения (правила HIPS), атака будет заблокирована этим правилом (см. [Предотвращение сетевых вторжений](#)).

Пример обнаружения атаки на сетевом уровне приведен на рисунке ниже:

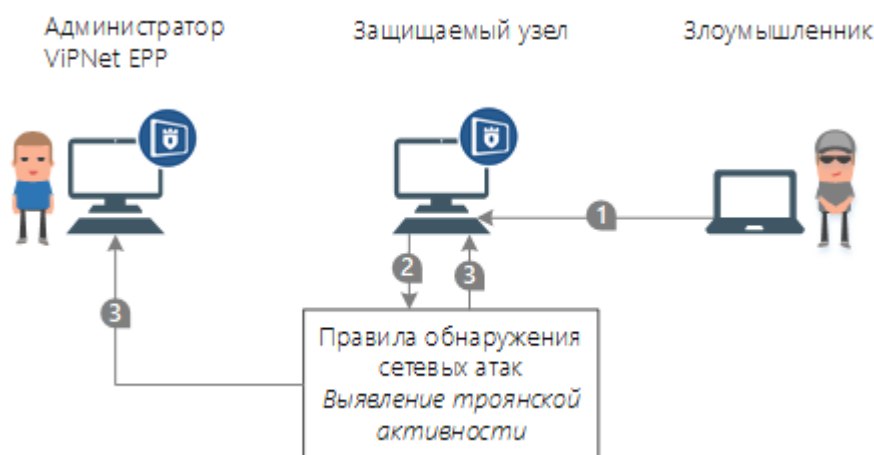


Рисунок 7. Обнаружение атаки на сетевом уровне

- 1 Злоумышленник получил удаленный доступ к одному из защищаемых узлов и запустил троянскую программу.
- 2 При анализе трафика с помощью правил обнаружения сетевых атак сработало одно из правил, идентифицировавшее активность троянской программы — сетевую атаку.



**Примечание.** Если сработало аналогичное правило предотвращения вторжения (правило HIPS), атака будет не только выявлена, но и сразу заблокирована (см. рисунок в разделе [Предотвращение сетевых вторжений](#)).

- 3 Сведения о сетевой атаке (событие информационной безопасности) регистрируется в журналах событий ViPNet EPP Агент и ViPNet EPP Сервер.

На локальном уровне сигнатурный анализ реализован с помощью узловых правил. К узловым правилам относятся, например, правила анализа событий в журналах приложений и служб. Эти правила содержат сигнатуры для анализа событий, зарегистрированных средствами ОС, позволяющие обнаружить атаку на защищаемом узле. Анализироваться будут только те журналы событий, которые указаны для отслеживания в настройках правил обнаружения вторжений (HIDS) (см. [Порядок настройки политики](#)). Для анализа событий используются:

- Декодеры — набор правил для первичного анализа событий, происходящих на защищаемом узле. Применяются для анализа некоторых видов событий перед применением правил анализа. Декодеры могут анализировать такие события, как изменения файловой системы, попытки входа в систему, управление учетными записями (например, строки в журналах событий ОС). Декодер извлекает информацию, которая нужна для дальнейшего анализа события. На следующем этапе эта информация обрабатывается с помощью правил анализа.
- Правила анализа — набор правил для идентификации событий, происходящих на защищаемом узле. С помощью правил анализа информация о событии разбирается детально. Например, правила могут содержать идентификаторы для присвоения событию уровня, по которому можно классифицировать критичность обнаруженной угрозы безопасности информации.

Правила анализа определяют, какие события могут считаться атакой, в результате чего ViPNet EPP идентифицируется событие информационной безопасности.

Пример обнаружения атаки на локальном уровне на основе анализа событий в журналах ОС приведен на рисунке ниже.

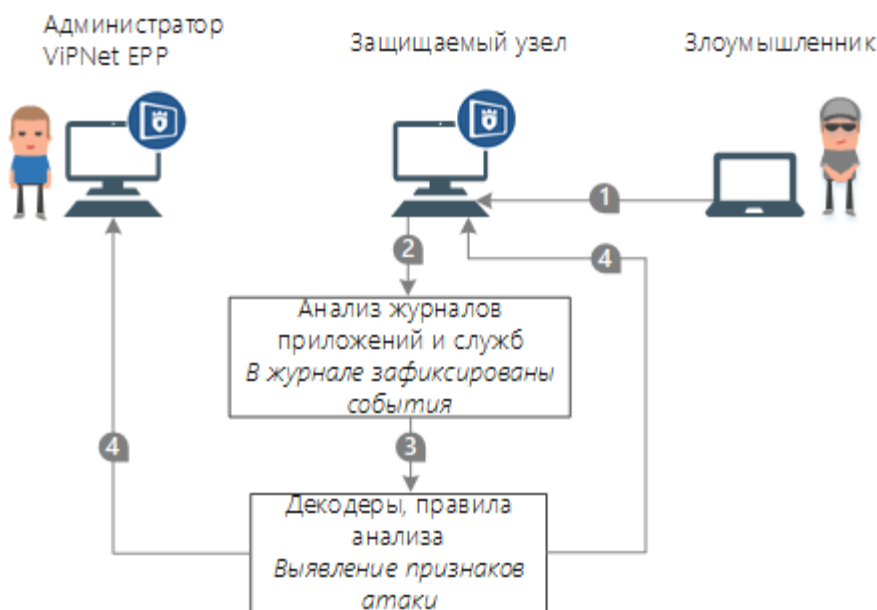


Рисунок 8. Обнаружение атаки на локальном уровне

- 1 Злоумышленник получил удаленный доступ к защищаемому узлу и изменил критически важный системный файл.
- 2 ViPNet EPP Агент выполнена проверка, что в журнале событий приложений и служб зафиксированы события для анализа.
- 3 С помощью правил анализа (декодера) идентифицированы изменения системного файла на защищаемом узле.
- 4 Сведения об атаке на локальном уровне (событие информационной безопасности) регистрируются в журналах событий ViPNet EPP Агент и ViPNet EPP Сервер.

Таким образом, на основе правил обнаружения вторжений (HIDS) ViPNet EPP Агент анализирует трафик, а также изменения на защищаемом узле. При срабатывании правил обнаружения вторжений (HIDS) идентифицируется событие информационной безопасности, содержащее сведения о сетевой атаке или зафиксированном отклонении от нормального поведения.

## Предотвращение сетевых вторжений

Для блокирования сетевой активности применяются правила предотвращения вторжений — [сетевые правила \(HIPS\)](#).

Пример предотвращения сетевой атаки приведен на рисунке ниже.

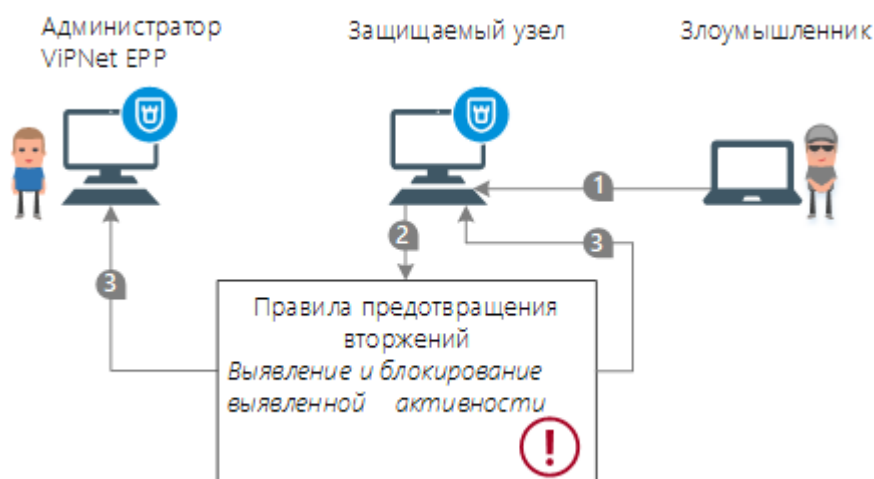


Рисунок 9. Предотвращение сетевой атаки

- 1 Злоумышленник получил удаленный доступ к одному из защищаемых узлов и запустил троянскую программу.
- 2 При анализе трафика сработало одно из правил предотвращения вторжений (сетевое правило HIPS). Правило выявило и заблокировало активность троянской программы — сетевую атаку, разорвав сетевое соединение.
- 3 Событие блокирования сетевой атаки регистрируется в журналах событий ViPNet EPP Агент и ViPNet EPP Сервер.

В зависимости от используемого набора правил предотвращения сетевых атак предотвращение вторжений работает в одном из режимов:

- **Усиленный** — используется полный набор правил предотвращения сетевых атак, что может привести к снижению производительности компьютера защищаемого узла.
- **Оптимальный (Базовый)** — используется оптимальный набор правил, обеспечивающий защиту в большинстве случаев.
- **Минимальный** — используется минимальный набор правил, защищающих от наиболее критичных атак.
- **Отключен** — предотвращение вторжений выключено и не влияет на работу защищаемого узла.

Режим работы передается на ViPNet EPP Агент защищаемого узла централизованно в составе политики безопасности (базы правил). Для учета особенностей обнаружения сетевых атак на защищаемом узле режим работы предотвращения вторжений ViPNet EPP Агент можно изменить локально. Обновление базы правил может изменить этот режим.

# Обнаружение аномалий с помощью критериев

События информационной безопасности защищаемого узла, идентифицированные с помощью правил обнаружения вторжений (HIDS), свидетельствуют об изменении локальной (состояние объектов операционной системы) и сетевой активности. Вы можете задать критерии обнаружения аномалий, указав в них списки правил обнаружения вторжений (HIDS) определенного типа и временной интервал, в котором активность не является нормой. Заданные критерии являются общими для всех защищаемых узлов под управлением сервера, начинают действовать сразу после создания, а обнаружение аномалий с их помощью выполняется в режиме, близком к реальному времени.

Например, вы можете задать проверку сетевой активности в определенный временной интервал и выявить сетевую активность в несвойственные для нее часы. В этом случае администратор ViPNet EPP может блокировать аномальную сетевую активность — создать блокирующий сетевой фильтр персонального межсетевого экрана ViPNet EPP Агент.

# Политика безопасности

Политика безопасности — совокупность настроек модулей, системных и пользовательских правил, регулирующая безопасность защищаемых узлов. На основе политики безопасности ViPNet EPP Агент обнаруживает и предотвращает угрозы информационной безопасности на защищаемых узлах. Политика безопасности создается и настраивается пользователями в ViPNet EPP Сервер (см. [Управление политиками безопасности](#)) на основе базы правил, формируемой специалистами ИнфоТеКС. База правил регулярно обновляется на сервере обновлений. Для своевременного выявления новых типов угроз информационной безопасности необходимо регулярно загружать обновление базы правил в ViPNet EPP.

Политика безопасности ViPNet EPP, содержит:

- [Межсетевой экран](#):
  - Фильтры политик безопасности (правила фильтрации).
  - Справочники протоколов, расписаний, адресов и сетей.
  - Режим работы межсетевого экрана.
- Контроль приложений (только для защищаемых узлов с ОС Windows):
  - Списки контроля приложений.
  - Правила доступа приложений к объектам ОС Windows.
  - Режим работы контроля приложений.

Подробнее о модуле защиты см. документ «ViPNet EPP for Windows. Руководство администратора» раздел «Контроль приложений».

- [Обнаружение и предотвращение вторжений](#):
  - Правила обнаружения вторжений (правила HIDS).
  - Правила предотвращения вторжений (правила HIPS).
  - Режим работы модуля предотвращения вторжений.
  - Веб-фильтры (только для защищаемых узлов с ОС Windows). Подробнее см. документ «ViPNet EPP for Windows. Руководство администратора» раздел «Блокировка доступа к вредоносным веб-ресурсам».
  - Бесфайловые атаки (только для защищаемых узлов с ОС Windows). Подробнее см. документ «ViPNet EPP for Windows. Руководство администратора» раздел «Обнаружение и предотвращение бесфайловых атак».
- [Сетевой доступ с нулевым доверием \(ZTNA\)](#).

Возможности работы с политикой безопасности зависят от модели управления ViPNet EPP:

- Работа ViPNet EPP Агент под управлением ViPNet EPP Сервер.

При работе ViPNet EPP Агент под управлением ViPNet EPP Сервер база правил загружается с сервера обновлений (см. [Модели управления и принципы работы](#)) в ViPNet EPP Сервер

вручную или автоматически. После загрузки базы правил для учета особенностей защиты администратор может вносить изменения в сформированную политику безопасности. Изменения можно сохранять в той же политике или создавать новую политику.

Чтобы после загрузки с сервера обновлений новой базы правил и создания новой политики, внесенные администратором изменения не были потеряны, доступен импорт пользовательских настроек модулей защиты из других политик безопасности.

Политика безопасности назначается на группы защищаемых узлов, после чего автоматически отправляется на защищаемые узлы. До тех пор, пока на группу, в которую входит защищаемый узел, не назначена политика, в ViPNet EPP Агент этого узла защита отключена.

При необходимости на защищаемом узле можно создать и добавить в текущую политику безопасности ViPNet EPP Агент пользовательские настройки модулей защиты ViPNet EPP:

- Межсетевой экран:
  - Пользовательские фильтры.
  - Справочники протоколов, расписаний, адресов и сетей для пользовательских фильтров.
  - Режим работы межсетевого экрана.
- Обнаружения и предотвращения вторжений:
  - Режим работы модуля предотвращения вторжений.

При назначении новой политики безопасности пользовательские настройки, добавленные в ViPNet EPP Агент защищаемого узла, сохраняются. Серверные настройки имеют приоритет над пользовательскими.

- Автономная работа ViPNet EPP Агент.

При автономной работе ViPNet EPP Агент база правил загружается из комплекта поставки или с сервера обновлений (см. [Модели управления и принципы работы](#)) в ViPNet EPP Агент вручную. Для учета особенностей защиты, настройки в базе правил можно изменить в каждом ViPNet EPP Агент.

До тех пор, пока на защищаемый узел не загружена база правил, защита отключена.

При необходимости на защищаемом узле можно создать и добавить в текущую базу правил ViPNet EPP Агент пользовательские настройки модулей защиты ViPNet EPP, кроме настроек ZTNA.

# Уровни событий информационной безопасности

Уровень события информационной безопасности определяется степенью опасности, в зависимости от которой требуется принятие мер реагирования разной срочности:

-  **Критическое** — наиболее опасное событие, угрожающее работоспособности защищаемого узла. Требуется принятия экстренных мер.
-  **Опасное** — событие средней степени опасности; может привести к сбоям в работе защищаемого узла. Требуется решения проблемы в рабочем порядке.
-  **Важное** — событие может косвенно свидетельствовать о вредоносной активности на защищаемом узле. Требуется решения проблемы в рабочем порядке.
-  **Информационное** — событие носит уведомительный характер; мер реагирования не требует.

Для защищаемого узла отслеживается его состояние, которое определяется по уровню наиболее опасных событий, зарегистрированных на нем за время отслеживания.

# Ролевая модель

Управление ViPNet EPP реализовано по ролевой модели доступа. Роль определяет полномочия пользователя и назначается при создании соответствующей учетной записи (см. [Управление учетными записями](#)). Кратко полномочия пользователей в соответствии с назначенной ролью приведены в таблице ниже, подробнее — в приложении (см. [Полномочия пользователей](#)).

Таблица 2. Полномочия пользователей ViPNet EPP for Linux

| Роль                 | Полномочия пользователей                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Администратор        | Роль назначается учетной записи, созданной в ViPNet EPP Сервер.<br>Обеспечивает доступ ко всем функциям ViPNet EPP Сервер и ViPNet EPP Агент.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Администратор агента | Роль назначается учетной записи, созданной в ViPNet EPP Агент.<br>Обеспечивает доступ ко всем функциям ViPNet EPP Агент.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Аудитор              | Роль назначается учетной записи, созданной в ViPNet EPP Сервер. Доступен просмотр инфопанели, журналов событий и журналов аудита ViPNet EPP Сервер и ViPNet EPP Агент.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Аудитор агента       | Роль назначается учетной записи, созданной в ViPNet EPP Агент. Доступны: <ul style="list-style-type: none"><li>• выбор режимов модулей защиты;</li><li>• просмотр инфопанели;</li><li>• просмотр критериев обнаружения аномалий (только в автономном ViPNet EPP Агент);</li><li>• просмотр журналов событий и журнала аудита;</li><li>• просмотр списков правил модулей защиты;</li><li>• просмотр статуса ZTNA (только в ViPNet EPP Агент под управлением сервера);</li><li>• просмотр результатов самотестирования;</li><li>• просмотр информации о лицензии и о ViPNet EPP Агент.</li></ul> |
| Пользователь агента  | Роль назначается учетной записи, созданной в ViPNet EPP Агент.<br>Доступны: <ul style="list-style-type: none"><li>• просмотр инфопанели;</li><li>• просмотр журнала событий;</li><li>• просмотр ZTNA (только в ViPNet EPP Агент под управлением сервера).</li></ul>                                                                                                                                                                                                                                                                                                                            |



**Примечание.** Учетные записи с ролями Администратор ViPNet EPP и Аудитор ViPNet EPP при авторизации в ViPNet EPP Агент получают те же полномочия, что и учетные записи с ролями Администратор агента и Аудитор агента.

# Отслеживание работы антивирусов

ViPNet EPP позволяет отслеживать работу антивирусного программного обеспечения Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite (см. [Совместимость со сторонним программным обеспечением](#)) (далее — антивирусов), установленного на защищаемых узлах.

Для отслеживания работы антивирусов на защищаемом узле лицензия ViPNet EPP (см. [Лицензирование](#)) должна содержать разрешение на использование модулей [Personal Firewall](#) и [HIDS](#).

События обнаружения вирусов отслеживаются в ViPNet EPP Агент правилами обнаружения событий информационной безопасности — [правилами HIDS](#). Если настроены правила, события обнаружения вирусов регистрируются в журнале событий и передаются в ViPNet EPP Сервер.



**Внимание!** Для отслеживания работы антивируса Kaspersky Endpoint Security на защищаемом узле с установленной ОС РЕД ОС 7.3.4 необходимо отключить SELinux.

---

При обнаружении антивирусом угрозы или при отключении (отсутствии) антивируса ViPNet EPP Агент полностью блокирует трафик сети (трафик открытой сети — на защищаемом узле с установленной программой ViPNet Client 4U (только в ОС Linux) или ViPNet Client 5). Для этого в настройках ViPNet EPP Сервер для агентов должно быть включено отслеживание работы антивируса (см. [Настройка параметров защищаемых узлов](#)). Отслеживание возможно, если персональный межсетевой экран ViPNet EPP Агент работает в одном из режимов:

- Публичная сеть.
- Частная сеть.
- Корпоративная сеть.

Если на защищаемом узле включено отслеживание работы антивируса:

- Проверяется статус антивируса:
  - Если антивирус работает — режим работы персонального меж сетевого экрана ViPNet EPP Агент не изменяется.
  - Если антивирус остановлен или не установлен — персональный межсетевой экран ViPNet EPP Агент переключается в режим **Полная блокировка трафика**, весь открытый сетевой трафик защищаемого узла, кроме трафика между ViPNet EPP Агент и ViPNet EPP Сервер, блокируется.
  - При возобновлении работы антивируса персональный межсетевой экран ViPNet EPP Агент автоматически переключается в режим, установленный до включения отслеживания, при условии, что режим **Полная блокировка трафика** не был установлен пользователем вручную.

- Проверяются события журнала антивируса.

Если антивирус обнаружил вредоносный объект, персональный межсетевой экран ViPNet EPP Агент переключается в режим **Полная блокировка трафика** — весь сетевой трафик защищаемого узла, кроме трафика между ViPNet EPP Агент и ViPNet EPP Сервер, блокируется. Чтобы разблокировать трафик, необходимо переключить режим персонального межсетевого экрана вручную или через назначение новой версии базы правил.

После выключения отслеживания работы антивируса (см. [Настройка параметров защищаемых узлов](#)) режим работы персонального межсетевого экрана ViPNet EPP Агент определяется следующим образом:

- Если режим **Полная блокировка трафика** устанавливался автоматически и не изменялся администратором ViPNet EPP (вручную или назначением базы правил), то возвращается режим работы, который был до включения отслеживания.
- Если администратор ViPNet EPP установил режим вручную или назначением базы правил, то этот режим работы останется после отключения отслеживания.

# Лицензирование

Лицензия ViPNet EPP дает право на легальное использование ViPNet EPP и поддержку производителем. Для приобретения лицензии обратитесь в ИнфоТеКС (см. [Обратная связь](#)).

Лицензия состоит из файла формата `itcslic` и PDF-файла с информацией об учетной записи для доступа к [серверу обновлений](#).

Лицензия определяет способ работы ViPNet EPP Агент:

- Серверная лицензия — ViPNet EPP Агент работает под управлением ViPNet EPP Сервер.

Лицензия устанавливается и активируется в ViPNet EPP Сервер и автоматически рассылается на подключенные к серверу ViPNet EPP Агент.

Лицензия определяет:

- Операционную систему, на которой будет работать ViPNet EPP Сервер (ОС Windows или Linux).
- Максимальное количество ViPNet EPP Агент, которые разрешено подключить к ViPNet EPP Сервер.
- Срок подписки на обновление базы правил, в течение которого предоставляется доступ к серверу обновлений и доступно скачивание баз правил.
- Доступные модули ViPNet EPP, которые можно подключить для защищаемых узлов, и срок их активности. Набор доступных модулей определяется при покупке ViPNet EPP.

Лицензия должна быть установлена при первом подключении к ViPNet EPP Сервер и активирована для подтверждения подлинности (см. [Установка и активация лицензии](#)). При подключении защищаемого узла к ViPNet EPP Сервер администратору необходимо указать, какие модули должны быть доступны на узле. ViPNet EPP Агент защищаемого узла получает лицензию, в которой указаны доступные модули (см. [Просмотр сведений о программе и лицензии](#)), после подключения к ViPNet EPP Сервер. На защищаемом узле будут работать только разрешенные модули.

- Автономная лицензия — ViPNet EPP Агент работает автономно без ViPNet EPP Сервер.

Лицензия устанавливается и активируется в ViPNet EPP Агент. Для каждого ViPNet EPP Агент должна быть отдельная лицензия.

Лицензия определяет:

- Срок подписки на обновление базы правил, в течение которого предоставляется доступ к серверу обновлений и доступно скачивание баз правил.
- Доступные модули ViPNet EPP и срок их активности. Выбрать набор доступных модулей при покупке ViPNet EPP нельзя.

Лицензия должна быть установлена при первом подключении к ViPNet EPP Агент и активирована для подтверждения подлинности. На защищаемом узле будут работать только доступные модули. Список доступных модулей изменить нельзя. При переходе автономного

ViPNet EPP Агент под управление сервера, ViPNet EPP Агент начнет использовать серверную лицензию.

Лицензия может быть бессрочной или иметь срок действия. Для расширения возможностей или продления срока действия лицензии обратитесь в компанию [ИнфоТеКС](#).

Если лицензия не установлена, не активирована или истек срок ее действия — ViPNet EPP будет работать с ограничениями:

- Модули отключены и не влияют на работу защищаемых узлов. Включить модули невозможно. Защита на узлах отключена.
- Загрузка баз правил недоступна.
- Подключить новые защищаемые узлы невозможно (только для ViPNet EPP Сервер).

В случае истечения срока действия лицензии или при повреждении лицензии указанные выше ограничения вступают в силу через 7 дней включительно после даты истечения или повреждения. Если лицензия была повреждена, вы можете повторно загрузить и активировать лицензию в течение всего срока её действия (см. [Установка и активация лицензии](#)).

За 14 дней до истечения лицензии или подписки на обновление базы правил в ViPNet EPP появляется предупреждение об этом.

# 2

## Ввод в эксплуатацию

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| Порядок ввода в эксплуатацию ViPNet EPP с агентами под управлением сервера | 50 |
| Порядок ввода в эксплуатацию ViPNet EPP с автономными агентами             | 52 |
| Установка, обновление, восстановление и удаление                           | 53 |

# Порядок ввода в эксплуатацию ViPNet EPP с агентами под управлением сервера

| Действие                                                                                                                                                                                                               | Ссылки                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Подготовьтесь к установке ViPNet EPP.<br>На компьютере для установки сервера управления подготовьте СУБД PostgreSQL                                                                           | <a href="#">Подготовка к установке ViPNet EPP</a><br><a href="#">Подготовка СУБД PostgreSQL на компьютере с ViPNet EPP Сервер</a>                                                                                                                                       |
| <input type="checkbox"/> Установите компоненты ViPNet EPP Сервер (сервер управления и рабочий сервер) на один компьютер или на разные. При необходимости разверните несколько рабочих серверов                         | <a href="#">Установка ViPNet EPP Сервер</a><br><a href="#">Развёртывание инфраструктуры открытых ключей</a>                                                                                                                                                             |
| <input type="checkbox"/> Подключитесь к веб-интерфейсу ViPNet EPP Сервер, установите и активируйте лицензию                                                                                                            | <a href="#">Подключение к веб-интерфейсу ViPNet EPP Сервер</a><br><a href="#">Установка и активация лицензии</a>                                                                                                                                                        |
| <input type="checkbox"/> Подключите рабочий сервер к серверу управления                                                                                                                                                | <a href="#">Добавление рабочего сервера на сервер управления</a><br><a href="#">Установка компонентов ViPNet EPP Сервер на один компьютер или Установка компонентов ViPNet EPP Сервер на разные компьютеры</a><br><a href="#">раздел «Подключение рабочего сервера»</a> |
| <input type="checkbox"/> Установите ViPNet EPP Агент на компьютеры корпоративной сети с ОС GNU/Linux,, настройте сетевой сенсор и укажите IP-адрес ViPNet EPP Сервер (рабочего сервера) для работы под его управлением | <a href="#">Установка ViPNet EPP Агент</a>                                                                                                                                                                                                                              |
| <input type="checkbox"/> Если требуется, установите ViPNet EPP Агент на компьютеры корпоративной сети с ОС Windows, при установке выберите способ работы под управлением сервера                                       | <a href="#">См. документ «ViPNet EPP for Windows. Руководство администратора» раздел «Установка ViPNet EPP Агент»</a>                                                                                                                                                   |
| <input type="checkbox"/> Подключитесь к веб-интерфейсу ViPNet EPP Сервер и подключите защищаемые узлы с ViPNet EPP Агент к ViPNet EPP Сервер                                                                           | <a href="#">Подключение защищаемых узлов</a>                                                                                                                                                                                                                            |
| <input type="checkbox"/> Настройте автоматическую загрузку обновлений базы правил с сервера обновлений или загрузите вручную                                                                                           | <a href="#">Загрузка базы правил</a>                                                                                                                                                                                                                                    |

| Действие                                                            | Ссылки                                           |
|---------------------------------------------------------------------|--------------------------------------------------|
| <input type="checkbox"/> Настройте политику безопасности            | <a href="#">Порядок настройки политики</a>       |
| <input type="checkbox"/> Назначьте политику группе защищаемых узлов | <a href="#">Назначение политики группе узлов</a> |

# Порядок ввода в эксплуатацию ViPNet EPP с автономными агентами

| Действие                                                                                                                                                                                | Ссылки                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Подготовьтесь к установке ViPNet EPP                                                                                                                           | <a href="#">Подготовка к установке ViPNet EPP</a>                                                                                                                                                                                                       |
| <input type="checkbox"/> Установите ViPNet EPP Агент на компьютеры корпоративной сети с ОС GNU/Linux и настройте сетевой сенсор, шаг подключения к ViPNet EPP Сервер выполнять не нужно | <a href="#">Установка ViPNet EPP Агент</a>                                                                                                                                                                                                              |
| <input type="checkbox"/> На каждом агенте в графической консоли управления установите и активируйте лицензию                                                                            | <a href="#">Подключение к ViPNet EPP Агент</a><br><a href="#">Установка и активация лицензии</a>                                                                                                                                                        |
| <input type="checkbox"/> На каждый агент в графической консоли управления загрузите базу правил                                                                                         | <a href="#">Загрузка и обновление базы правил</a>                                                                                                                                                                                                       |
| <input type="checkbox"/> На каждом агенте настройте параметры работы или оставьте параметры по умолчанию                                                                                | <a href="#">Просмотр и настройка параметров работы</a>                                                                                                                                                                                                  |
| <input type="checkbox"/> На каждом агенте настройте модули защиты или оставьте параметры из базы правил                                                                                 | <a href="#">Просмотр и настройка режимов работы модулей защиты</a><br><a href="#">Управление фильтрацией трафика</a><br><a href="#">Управление обнаружением и предотвращением вторжений</a><br><a href="#">Настройка критериев обнаружения аномалий</a> |

# Установка, обновление, восстановление и удаление

## Подготовка к установке ViPNet EPP

Действия со значком  нужно выполнять только при вводе в эксплуатацию ViPNet EPP с агентами, работающими под управлением сервера.

Перед установкой ViPNet EPP на компьютеры с ОС GNU/Linux:

- 1 Убедитесь, что компьютеры и их программное обеспечение отвечают требованиям к компонентам:

-  [Требования к установке сервера управления и рабочего сервера.](#)



**Совет.** В целях безопасности рекомендуем на компьютере, предназначенном для установки ViPNet EPP Сервер, использовать только учётные записи с правами администратора ОС GNU/Linux.

---

- [Требования к установке агента.](#)
- 2  На компьютерах должны быть разрешены входящие и исходящие соединения по TCP-портам:
    - 25014 — для связи рабочего сервера и агентов с ОС Linux.
    - 25010 — для связи рабочего сервера и агентов с ОС Windows.
    - 25016 — для связи рабочего сервера и сервера управления.
    - 443 — для доступа сервера управления к серверу обновлений и для подключения к веб-интерфейсу сервера.
  - 3  На компьютере, где будет установлен ViPNet EPP Сервер или любой из его компонентов, [подготовьте к работе СУБД PostgreSQL.](#)
  - 4  На компьютере, где будет установлен сервер управления, [разверните инфраструктуру открытых ключей.](#)
  - 5  Уточните IP-адрес (в формате IPv4) или доменное имя компьютера, предназначенного для установки ViPNet EPP Сервер. Адрес ViPNet EPP Сервер понадобится при установке агентов.
  - 6 Если на компьютерах, где будет устанавливаться ViPNet EPP Агент, используется сторонний межсетевой экран, выключите его. Отключите также межсетевой экран, встроенный в ОС.  
Использование ViPNet EPP Агент одновременно с другими межсетевыми экранами может привести к конфликтам правил фильтрации.

- 7 Если на компьютерах установлены ViPNet Client или ViPNet Personal Firewall, удалите их. Для работы в защищенной сети ViPNet совместно с ViPNet EPP можно использовать ViPNet Client 4U или ViPNet Client 5, совместимой с ViPNet EPP версии (см. [Совместимость со сторонним программным обеспечением](#)). Если программа ViPNet Client 4U или ViPNet Client 5 уже установлена, удалять не нужно.
- 8 Если на компьютерах установлен ViPNet IDS HS Агент, удалите его.

## Подготовка СУБД PostgreSQL на компьютере с ViPNet EPP Сервер

Перед установкой ViPNet EPP Сервер на компьютере, где будет установлен компонент сервер управления, подготовьте СУБД PostgreSQL:

- 1 Проверьте, что на компьютере установлен PostgreSQL версии 15.12. Если PostgreSQL не установлен, установите его:
  - 1.1 Подключите установочный диск Astra Linux Special Edition 1.8.2.7 БЮЛЛЕТЕНЬ № 2025-0411SE18 (оперативное обновление 1.8.2).
  - 1.2 Подключите `cdrom` в качестве локального репозитория:

```
sudo apt-cdrom add
```
  - 1.3 Обновите индекс и списки пакетов в подключённом репозитории:

```
sudo apt update
```
  - 1.4 Установите из подключённого репозитория PostgreSQL 15.12-astra.se1:

```
sudo apt install postgresql-15
```
- 2 Проверьте, что мандатный контроль целостности выключен:

```
sudo astra-mic-control status
```
- 3 Если мандатный контроль целостности включён:
  - 3.1 Выключите его на время настройки учётной записи СУБД:

```
sudo astra-mic-control disable
```
  - 3.2 Перезагрузите компьютер.
- 4 Создайте и настройте учётную запись СУБД для работы ViPNet EPP Сервер:



**Внимание!** Пароль учётной записи должен содержать только буквы, цифры, пробелы (но не в начале и в конце) и символы из списка: `!@%^&*(){}<>, .?~:;-_+``

---

- 4.1 Выполните последовательно команды:

```
sudo -u postgres psql
CREATE USER endpoint_protection WITH PASSWORD '<пароль учетной записи>' SUPERUSER;
exit
```

- 4.2 Добавьте созданному пользователю `endpoint_protection` возможность авторизации по паролю. Для этого выполните команду:

```
sudo nano /etc/postgresql/15/main/pg_hba.conf
```

и в файле `/etc/postgresql/15/main/pg_hba.conf` в разделе `#IPv4 local connections` добавьте строку:

```
host      all                                endpoint_protection  127.0.0.1/32        scram-sha-256
```

```
host      all                                endpoint_protection  127.0.0.1/32        scram-sha-256
```

Рисунок 10. Добавление пользователю возможности авторизации по паролю

- 4.3 Проверьте, что в файле `/etc/parsec/mswitch.conf` для параметра `zero_if_notfound` установлено значение `yes`.

```
# Return zero data instead of ENOENT/ENDATA in the absence of record
zero_if_notfound: yes
```

Рисунок 11. Проверка параметра `zero_if_notfound`

- 4.4 Перезапустите службу PostgreSQL:

```
sudo systemctl restart postgresql
```

- 5 Если перед настройки учётной записи СУБД вы выключили мандатный контроль целостности:

- 5.1 Включите его:

```
sudo astra-mic-control enable
```

- 5.2 Перезагрузите компьютер.



**Совет.** В целях безопасности рекомендуем ограничить возможность удаленного подключения к СУБД PostgreSQL. Для этого в файле `postgresql.conf` замените строку `listen_addresses = '*'` на `listen_addresses = 'localhost'`.

## Установка ViPNet EPP Сервер

Вы можете установить и настроить компоненты ViPNet EPP Сервер (сервер управления и рабочий сервер):

- [на один компьютер](#);
- [разные компьютеры](#), например, если рабочих серверов будет несколько.

### Установка компонентов ViPNet EPP Сервер на один компьютер

- 1 Убедитесь, что установлена и подготовлена к работе СУБД PostgreSQL 15.

- 2 Установите ПО веб-сервера Apache2:

```
sudo apt install apache2
```

- 3 Перейдите в каталог с установочными пакетами компонентов ViPNet EPP Сервер:

```
cd /<расположение каталога>/<каталог>
```

#### 4 Последовательно выполните команды установки пакетов:

```
sudo dpkg -i ./epp2-common-components_x86-64_1.x.x.xxxx.deb
sudo dpkg -i ./epp2-main-server_x86-64_1.x.x.xxxx.deb
sudo dpkg -i ./epp2-worker-server_x86-64_1.x.x.xxxx.deb
```

#### 5 Настройте параметры, создайте и инициализируйте базу данных, запустите службы для сервера управления и рабочего сервера, последовательно выполнив команды:

##### 5.1 Для сервера управления:

```
sudo /opt/epp2/bin/utility database-configure --server=main-server
--password='<пароль пользователя endpoint_protection>'
sudo /opt/epp2/bin/utility database-initialize --server=main-server
```

##### 5.2 Для рабочего сервера:

```
sudo /opt/epp2/bin/utility database-configure --server=epp-worker-server
--password='<пароль пользователя endpoint_protection>'
sudo /opt/epp2/bin/utility database-initialize --server=epp-worker-server
```

#### 6 Настройте конфигурацию ПО веб-сервера Apache2:

```
sudo /opt/epp2/bin/utility configure-apache --web-server-name="<доменное имя или
IP-адрес веб-сервера>"
```

#### 7 Для установления TLS-соединения между сервером управления и браузером:

- [Разверните инфраструктуру открытых ключей.](#)
- Если инфраструктура открытых ключей уже развёрнута, переместите цепочку сертификатов `epp_certificate.pem` и ключи сертификата сервера управления `epp_keypair.pem` в каталог `/opt/epp2/certs`:  

```
sudo mv epp_certificate.pem epp_keypair.pem /opt/epp2/certs
```



**Внимание!** Самостоятельно следите за сроком действия и своевременно обновляйте сертификаты и соответствующие ключи. Для обновления повторите шаги по [развёртыванию инфраструктуры открытых ключей](#).

---

#### 8 Перезапустите веб-сервер Apache2:

```
sudo systemctl restart apache2.service
```

#### 9 Перезапустите службу PostgreSQL:

```
sudo systemctl restart postgresql
```

#### 10 Проверьте состояние служб сервера управления и рабочего сервера, последовательно выполнив команды:

```
sudo systemctl status epp2-main-server.service
sudo systemctl status epp2-worker-server.service
```

#### 11 Настройте права доступа:

##### 11.1 Смените владельца папок `/opt/epp2/frontend` и `/opt/epp2/certs/epp_*`:

```
sudo chown -R www-data:www-data /opt/epp2/frontend
```

```
sudo chown -R www-data:www-data /opt/epp2/certs/epp_*
```

## 11.2 Ограничьте права доступа к файлу только для владельца и группы:

```
sudo chmod o-rwx /opt/epp2/certs/epp_*
```

```
sudo chmod gu+rw /opt/epp2/certs/epp_*
```

## 12 Подключитесь к веб-интерфейсу ViPNet EPP Сервер, установите и активируйте лицензию (см. [Установка и активация лицензии](#)).

### Подключение рабочего сервера

1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер и добавьте рабочий сервер (см. [Добавление рабочего сервера на сервер управления](#)). При добавлении рабочего сервера ему присвоится идентификатор.

2 На компьютере рабочего сервера добавьте идентификатор в конфигурационные файлы:

#### 2.1 В файле /opt/epp2/etc/worker\_server\_guid.conf раскомментируйте строку

worker\_server\_guid и укажите значение идентификатора:

```
worker_server_guid = {<Идентификатор рабочего сервера>}
```

#### 2.2 В файле /opt/epp2/etc/main\_server\_info.conf раскомментируйте строку address:

```
[*main_server*]
```

```
address = 127.0.0.1:25016
```

```
[*end*]
```

#### 2.3 Перезапустите службу рабочего сервера:

```
sudo systemctl restart epp2-worker-server.service
```

В результате рабочий сервер будет включен в работу. Убедитесь, что в веб-интерфейсе ViPNet EPP Сервер в разделе  **Серверы безопасности** > **Рабочие серверы** для рабочего сервера отображается статус **Активен** и указано недавнее время последней активности.

## Установка компонентов ViPNet EPP Сервер на разные компьютеры

### Установка сервера управления

1 Убедитесь, что установлена и подготовлена к работе СУБД PostgreSQL 15.

2 Установите ПО веб-сервера Apache2:

```
sudo apt install apache2
```

3 Перейдите в каталог с установочными пакетами сервера управления:

```
cd /<расположение каталога>/<каталог>
```

4 Установите пакеты сервера управления:

#### 4.1 Выполните последовательно команды установки пакетов:

```
sudo dpkg -i ./epp2-common-components_x86-64_1.x.x.xxxx.deb
```

```
sudo dpkg -i ./epp2-main-server_x86-64_1.x.x.xxxx.deb
```

#### 4.2 Настройте параметры базы данных сервера управления:

```
sudo /opt/epp2/bin/utility database-configure --server=main-server  
--password='<пароль пользователя endpoint_protection>'
```

#### 4.3 Выполните инициализацию базы данных и запустите службу сервера управления:

```
sudo /opt/epp2/bin/utility database-initialize --server=main-server
```

#### 4.4 Проверьте состояние службы сервера управления:

```
sudo systemctl status epp2-main-server.service
```

### 5 Настройте конфигурацию ПО веб-сервера Apache2:

```
sudo /opt/epp2/bin/utility configure-apache --web-server-name="<доменное имя или  
IP-адрес веб-сервера>"
```

### 6 Для установления TLS-соединения между сервером управления и браузером:

- [Разверните инфраструктуру открытых ключей.](#)
- Если инфраструктура открытых ключей уже развёрнута, переместите цепочку сертификатов `epp_certificate.pem` и ключи сертификата сервера управления `epp_keypair.pem` в каталог `/opt/epp2/certs`:  

```
sudo mv epp_certificate.pem epp_keypair.pem /opt/epp2/certs
```



**Внимание!** Самостоятельно следите за сроком действия и своевременно обновляйте сертификаты и соответствующие ключи. Для обновления повторите шаги по развёртыванию инфраструктуры открытых ключей.

---

### 7 Настройте права доступа:

#### 7.1 Смените владельца папок `/opt/epp2/frontend` и `/opt/epp2/certs/epp_*`:

```
sudo chown -R www-data:www-data /opt/epp2/frontend  
sudo chown -R www-data:www-data /opt/epp2/certs/epp_*
```

#### 7.2 Ограничьте права доступа к файлу только для владельца и группы:

```
sudo chmod o-rwx /opt/epp2/certs/epp_*  
sudo chmod gu+rw /opt/epp2/certs/epp_*
```

### 8 Подключитесь к веб-интерфейсу ViPNet EPP Сервер, установите и активируйте лицензию (см. [Установка и активация лицензии](#)).

## Установка рабочего сервера

#### 1 [Установите и подготовьте к работе СУБД PostgreSQL 15.](#)

#### 2 Перейдите в каталог с установочными пакетами рабочего сервера:

```
cd /<расположение каталога>/<каталог>
```

#### 3 Установите пакеты рабочего сервера:

##### 3.1 Последовательно выполните команды установки пакетов:

```
sudo dpkg -i ./epp2-common-components_x86-64_1.x.x.xxxx.deb
sudo dpkg -i ./epp2-worker-server_x86-64_1.x.x.xxxx.deb
```

### 3.2 Настройте параметры базы данных рабочего сервера:

```
sudo /opt/epp2/bin/utility database-configure --server=epp-worker-server
--password='<пароль пользователя endpoint_protection>'
```

### 3.3 Инициализируйте базу данных и запустите службу рабочего сервера:

```
sudo /opt/epp2/bin/utility database-initialize --server=epp-worker-server
```

### 3.4 Проверьте состояние службы рабочего сервера:

```
sudo systemctl status epp2-worker-server.service
```

## Подключение рабочего сервера

1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер и добавьте рабочий сервер (см. [Добавление рабочего сервера на сервер управления](#)). При добавлении рабочего сервера ему присвоится идентификатор.

2 На компьютере рабочего сервера добавьте идентификатор в конфигурационные файлы:

#### 2.1 В файле /opt/epp2/etc/worker\_server\_guid.conf раскомментируйте строку

worker\_server\_guid и укажите значение идентификатора:

```
worker_server_guid = {Идентификатор рабочего сервера>}
```

#### 2.2 В файле /opt/epp2/etc/main\_server\_info.conf раскомментируйте строку address и укажите адрес и порт (по умолчанию 25016) сервера управления:

```
[*main_server*]
address = <IP-адрес сервера управления>:25016
[*end*]
```

#### 2.3 Перезапустите службу рабочего сервера:

```
sudo systemctl restart epp2-worker-server.service
```

В результате рабочий сервер будет включен в работу. Убедитесь, что в веб-интерфейсе ViPNet EPP Сервер в разделе  **Серверы безопасности** > **Рабочие серверы** для рабочего сервера отображается статус **Активен** и указано недавнее время последней активности.

## Развёртывание инфраструктуры открытых ключей

Для установления TLS-соединения между сервером управления и браузером разверните инфраструктуру открытых ключей на компьютере с сервером управления:

### 1 Создайте самоподписанный корневой сертификат и соответствующий закрытый ключ:

```
openssl req -newkey rsa:<длина ключа CA> -x509 -subj "/CN=Root CA" -addext
"basicConstraints=critical,CA:TRUE" -days <срок действия> -noenc -keyout <ключ
CA>.pem -out <имя файла сертификата>.pem
```

где:

- <длина ключа CA> — длина закрытого ключа корневого сертификата в битах (не менее 4096 бит);
- <срок действия> — срок действия корневого сертификата в днях (рекомендуется 7300 дней);
- <ключ CA> — имя файла закрытого ключа корневого сертификата;
- <сертификат CA> — имя файла корневого сертификата.

## 2 Создайте запрос на сертификат сервера управления и соответствующий закрытый ключ:

- если подключение к серверу будет выполняться по IP-адресу:

```
openssl req -newkey rsa:<длина ключа EPP> -subj "/CN=<IP-адрес>" -addext
"basicConstraints=critical,CA:FALSE" -noenc -keyout epp_keypair.pem -out
server_csr.pem -addext "subjectAltName = IP:<IP-адрес>"
```

- если подключение к серверу будет выполняться по доменному имени:

```
openssl req -newkey rsa:<длина ключа EPP> -subj "/CN=<доменное имя>" -addext
"basicConstraints=critical,CA:FALSE" -noenc -keyout epp_keypair.pem -out
server_csr.pem -addext "subjectAltName = DNS:<доменное имя>"
```

где <длина ключа EPP> — длина закрытого ключа сертификата сервера управления в битах (не менее 4096 бит).

## 3 Создайте сертификат сервера управления:

```
openssl x509 -req -in server_csr.pem -copy_extensions copyall -CA <сертификат CA>.pem
-CAkey <ключ CA>.pem -days <срок действия сертификата СУ> -out epp-crt.pem
```

где <срок действия сертификата СУ> — срок действия сертификата сервера управления в днях (рекомендуется 1825 дней).

## 4 Создайте цепочку сертификатов — последовательно выполните команды:

```
cat epp-crt.pem > epp_certificate.pem

cat <сертификат CA>.pem >> epp_certificate.pem
```

## 5 Установите корневой сертификат в хранилище сертификатов — последовательно выполните команды:

```
sudo openssl x509 -in <сертификат CA>.pem -inform PEM -out
/usr/local/share/ca-certificates/local_ca_cert.crt

sudo update-ca-certificates -v
```

## 6 Переместите цепочку сертификатов epp\_certificate.pem и ключи сертификата сервера управления epp\_keypair.pem в каталог /opt/epp2/certs:

```
sudo mv epp_certificate.pem epp_keypair.pem /opt/epp2/certs
```

## 7 Перезапустите веб-сервер Apache2:

```
sudo systemctl restart apache2.service
```

# Установка ViPNet EPP Агент

Перед установкой ViPNet EPP Агент:

- 1 Убедитесь, что выполнена подготовка к установке (см. [Подготовка к установке ViPNet EPP](#)).
- 2 Проверьте, что на компьютере включены сетевые интерфейсы компьютера, которые необходимо контролировать ViPNet EPP Агент.
- 3 Настройте часы реального времени (RTC) в соответствии с системными часами с помощью команды: `sudo hwclock -w`



**Примечание.** Если вы устанавливаете ViPNet EPP Агент на ОС Astra Linux Special Edition и планируете включить режим замкнутой программной среды, используйте открытый ключ `infotecs_pub.key`, входящий в комплект поставки ViPNet EPP (см. [Комплект поставки](#)), и следуйте [инструкциям справочного центра Astra Linux](#). Перед установкой измените имя файла с открытым ключом на `ИнфоТеКС_pub.gpg`.

Чтобы установить ViPNet EPP Агент:

- 1 Перейдите в каталог с установочным пакетом ViPNet EPP Агент с помощью команды:  
`cd /<расположение каталога>/<каталог>`
- 2 Запустите установку. В зависимости от установочного пакета выполните одну из команд:

- Для DEB-пакета:

- `sudo dpkg -i ./EPP_x86-64_RU_1.x.x-xxxx.deb`

- Для RPM-пакета:

- `sudo rpm -i ./EPP_x86-64_RU_1.x.x-xxxx.rpm`

Дождитесь окончания установки. В результате установки ViPNet EPP Агент будет настроен работать автономно.

- 3 Проверьте состояние службы агента, выполнив команду:

```
sudo systemctl status epp_supervisor.service
```

После установки ViPNet EPP Агент:

- 1 Настройте сетевой сенсор ViPNet EPP Агент в файле `suricata.yaml`:

- Отключите `DCERPC` для транспортного протокола `UDP`.
- Настройте параметр `stream.reassembly.depth` для `SMB`.

По умолчанию файл `suricata.yaml` расположен в `/opt/epp-agent/suricata/etc/suricata`.

Для настройки откройте файл `suricata.yaml` и добавьте в секции `dcerpc` и `smb` строки, отмеченные красным цветом:

```
app-layer:
  protocols:
    dcerpc:
      enabled: yes
      udp:
        enabled: no
```

```
.....
smb:
  enabled: yes
  stream-depth: 1mb
  detection-ports:
  dp: 139, 445
```

## 2 Перезапустите сетевой сенсор ViPNet EPP Агент с помощью команды:

```
sudo systemctl restart epp_supervisor
```

После установки ViPNet EPP Агент будет работать автономно. Чтобы ViPNet EPP Агент работал под управлением ViPNet EPP Сервер, выполните настройку одним из способов:

- Подключитесь к ViPNet EPP Агент и настройте работу под управлением сервера (см. [Перевод автономного ViPNet EPP Агент под управление ViPNet EPP Сервер](#)).
- В консоли ViPNet EPP Агент укажите IP-адрес ViPNet EPP Сервер (рабочего сервера) с помощью команды:

```
/opt/epp-agent/bin/epp_mc_cli --login=admin server set-address <IP-адрес ViPNet EPP
Сервер (рабочего сервера)>
```

В запросе **Password** введите пароль `admin`. В результате запрос на подключение к ViPNet EPP Сервер отправится автоматически.

По умолчанию ViPNet EPP Агент контролирует все сетевые интерфейсы, включенные на момент его запуска. Если требуется ограничить список контролируемых сетевых интерфейсов, в консоли ViPNet EPP Агент:



**Примечание.** Ограничение списка сетевых интерфейсов работает только для модуля [HIDS](#) и [HIPS](#).

---

## 1 Выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=admin agent set-net-interfaces <имя
интерфейса>[, <имя интерфейса 2>...],
```

указав имена интерфейсов, которые необходимо контролировать.

## 2 В запросе **Password** введите пароль `admin`.

## 3 Перезагрузите компьютер.

# Восстановление или удаление компонентов ViPNet EPP Сервер

## Восстановление компонентов ViPNet EPP Сервер

Чтобы восстановить работоспособность ViPNet EPP Сервер, например, при выявлении модификации программного кода, выполните повторную установку компонентов ViPNet EPP Сервер:

- Если компоненты ViPNet EPP Сервер установлены на одном компьютере:

```
sudo dpkg -i ./epp2-common-components_x86-64_1.x.x.xxxx.deb
sudo dpkg -i ./epp2-main-server_x86-64_1.x.x.xxxx.deb
sudo dpkg -i ./epp2-worker-server_x86-64_1.x.x.xxxx.deb
```
- Если компоненты ViPNet EPP Сервер установлены на разных компьютерах:
  - Переустановите пакеты сервера управления:

```
sudo dpkg -i ./epp2-common-components_x86-64_1.x.x.xxxx.deb
sudo dpkg -i ./epp2-main-server_x86-64_1.x.x.xxxx.deb
```
  - Переустановите пакеты рабочего сервера:

```
sudo dpkg -i ./epp2-common-components_x86-64_1.x.x.xxxx.deb
sudo dpkg -i ./epp2-worker-server_x86-64_1.x.x.xxxx.deb
```

После завершения восстановления компонентов перезагрузите компьютер.

## Удаление компонентов ViPNet EPP Сервер

- Если компоненты ViPNet EPP Сервер установлены на одном компьютере:

```
sudo dpkg -r epp2-worker-server
sudo dpkg -r epp2-main-server
sudo dpkg -r epp2-common-components
```
- Если компоненты ViPNet EPP Сервер установлены на разных компьютерах:
  - Удалите сервер управления:

```
sudo dpkg -r epp2-main-server
sudo dpkg -r epp2-common-components
```
  - Удалите рабочий сервер:

```
sudo dpkg -r epp2-worker-server
sudo dpkg -r epp2-common-components
```

# Восстановление или удаление ViPNet EPP Агент

Чтобы восстановить работоспособность ViPNet EPP Агент, например, при выявлении модификации программного кода, выполните повторную установку ViPNet EPP Агент. В зависимости от типа пакета, который был установлен, выполните одну из команд:

- Для DEB-пакета:

```
sudo dpkg -i ./EPP_x86-64_RU_1.x.x-xxxx.deb
```

- Для RPM-пакета:

```
sudo rpm --reinstall ./EPP_x86-64_RU_1.x.x-xxxx.rpm
```

Чтобы удалить ViPNet EPP Агент, в зависимости от типа пакета, который был установлен, выполните одну из команд:

- Для DEB-пакета:

```
sudo dpkg -r endpoint-protection-agent
```

- Для RPM-пакета:

```
sudo rpm -e endpoint-protection-agent
```

## Обновление

### Порядок обновления ViPNet EPP версии 1.5.2 и выше до версии 1.8.0



**Внимание!** Обновление ViPNet EPP до версии 1.8.0 возможно только с версии 1.7.1.

Если вы используете ViPNet EPP версии 1.5.2, обновите версии ViPNet EPP последовательно по схеме: 1.5.2 -> 1.6.0 -> 1.7.0 -> 1.7.1 -> 1.8.0.

Для получения обновления ViPNet EPP до промежуточных версий обратитесь в [ИнфоТеКС](#). При обновлении следуйте указаниям раздела «Обновление» документа «ViPNet EPP for Linux. Руководство администратора» для той версии, на которую обновляете.

Порядок обновления компонентов ViPNet EPP версии 1.7.1 до версии 1.8.0:

- 1 Обновите ViPNet EPP Сервер.
- 2 Обновите все ViPNet EPP Агент (см. [Обновление ViPNet EPP Агент](#)) и настройте сетевой сенсор ViPNet EPP Агент аналогично настройкам при установке (см. [Установка ViPNet EPP Агент](#)).

После обновления сервера и агентов до версии 1.8.0:

- Журнал событий (на сервере), журнал самотестирования начнет вестись заново.
- В журнале критичных событий сохраняются данные за последние 2 недели.

- При первом подключении пользователей к серверу и агентам потребуется сменить пароли учетных записей.

## Обновление ViPNet EPP Сервер



**Внимание!** Обновление ViPNet EPP Сервер 1.8.0 на более ранние версии запрещено. В случае такого обновления работоспособность ViPNet EPP может быть нарушена.

Чтобы обновить ViPNet EPP Сервер (сервер управления и рабочий сервер):

### 1 Подготовьте резервные копии баз данных сервера управления и рабочего сервера:

#### 1.1 Отключите службы сервера управления и рабочего сервера и их автозапуск после перезагрузки:

```
sudo systemctl stop epp2-main-server.service epp2-worker-server.service
sudo systemctl disable epp2-main-server.service epp2-worker-server.service
```

#### 1.2 Создайте резервную копию базы данных сервера управления:

```
pg_dump -U endpoint_protection -h localhost -d epp_server_kldfn -F p -b -f <путь к каталогу>main_server_dump.sql
```

где <путь к каталогу> — путь к каталогу для сохранения резервной копии.

При выполнении команды введите пароль пользователя `endpoint_protection`.

#### 1.3 Создайте резервную копию базы данных сервера рабочего сервера:

```
pg_dump -U endpoint_protection -h localhost -d epp_worker_server_jhbfr -F p -b -f <путь к каталогу>worker_server_dump.sql
```

При выполнении команды введите пароль пользователя `endpoint_protection`.

### 2 Выполните миграцию Astra Linux Special Edition 1.7.4 на оперативное обновление Astra Linux Special Edition 1.8.2.

В процессе миграции Astra Linux Special Edition будет обновлен PostgreSQL до версии 15.12.

### 3 Запустите службу PostgreSQL и включите автозагрузку — последовательно выполните команды:

```
sudo systemctl start postgresql
sudo systemctl enable postgresql
```

### 4 Повторите [подготовку к работе СУБД PostgreSQL](#). При создании учётной записи задайте тот же пароль пользователя `endpoint_protection`, что и в предыдущей версии ViPNet EPP Сервер.

### 5 Восстановите базы данных сервера управления и рабочего сервера из резервных копий — последовательно выполните команды:

```
createdb -U endpoint_protection -h localhost epp_server_kldfn
createdb -U endpoint_protection -h localhost epp_worker_server_jhbfr
psql -U endpoint_protection -d epp_server_kldfn -f <путь к каталогу>main_server_dump.sql -h localhost
```

```
psql -U endpoint_protection -d epp_worker_server_jhbfr -f <путь к каталогу>worker_server_dump.sql -h localhost
```

где <путь к каталогу> — путь к каталогу с резервными копиями.

## 6 Установите компоненты ViPNet EPP Сервер.

## Обновление ViPNet EPP Агент

Чтобы обновить ViPNet EPP Агент:

### 1 Перейдите в каталог с установочным пакетом ViPNet EPP Агент с помощью команды:

```
cd /<расположение каталога>/<каталог>
```

### 2 Запустите обновление. В зависимости от установочного пакета выполните одну из команд:

#### ○ Для DEB-пакета:

- `sudo dpkg -i ./EPP_x86-64_RU_1.x.x-xxxx.deb`

#### ○ Для RPM-пакета:

- `sudo rpm -U ./EPP_x86-64_RU_1.x.x-xxxx.rpm`

Дождитесь окончания установки.

### 3 Проверьте состояние службы агента, выполнив команду:

```
sudo systemctl status epp_supervisor.service
```

# 3

## Управление в ViPNet EPP Сервер

|                                                |     |
|------------------------------------------------|-----|
| Подключение к веб-интерфейсу ViPNet EPP Сервер | 68  |
| Интерфейс ViPNet EPP Сервер                    | 70  |
| Установка и активация лицензии                 | 72  |
| Управление защищаемыми узлами и группами       | 73  |
| Управление политиками безопасности             | 80  |
| Настройка критериев обнаружения аномалий       | 145 |
| Работа с журналами                             | 146 |
| Администрирование ViPNet EPP Сервер            | 155 |
| Интеграция с внешними системами                | 170 |

# Подключение к веб-интерфейсу ViPNet EPP Сервер

Перед первым подключением к веб-интерфейсу ViPNet EPP Сервер установите корневой сертификат \*.pem, созданный при подготовке к установке ViPNet EPP (см. [Развёртывание инфраструктуры открытых ключей](#)):

- в ОС Linux — в используемый браузер;
- в ОС Windows — в хранилище **Доверенные корневые центры сертификации**.

---

**Внимание!** При первом подключении к веб-интерфейсу ViPNet EPP Сервер:



- 1 Войдите с учетной записью администратора ViPNet EPP по умолчанию: имя пользователя — admin, пароль — admin.
- 2 Смените пароль администратора ViPNet EPP по умолчанию (см. [Управление учетными записями](#)).

---

К веб-интерфейсу могут одновременно подключаться до 5 пользователей с разными учетными записями. Если изменения нескольких пользователей затрагивают один и тот же объект, для этого объекта будут применены изменения пользователя, сохранившего свои изменения первым. Параллельные сеансы работы с ViPNet EPP Сервер через веб-интерфейс пользователя с одной и той же учетной записью запрещены.

Чтобы подключиться к веб-интерфейсу ViPNet EPP Сервер:

- 1 Запустите браузер и в адресной строке введите: `https://<IP-адрес сервера управления ViPNet EPP Сервер>`
- 2 Введите ваши имя учетной записи и пароль.
- 3 Нажмите **Войти**.



---

**Внимание!** Если вы три раза подряд введете неверные данные учетной записи, возможность подключения к ViPNet EPP Сервер для этой учетной записи будет заблокирована на три минуты.

---

При успешной аутентификации и авторизации откроется страница веб-интерфейса ViPNet EPP Сервер, на которой будут доступны действия согласно вашим полномочиям (см. [Ролевая модель](#)).

Чтобы завершить работу с веб-интерфейсом авторизованного пользователя, на панели заголовка в меню авторизованного пользователя выберите **Выйти**. В результате текущий сеанс работы пользователя будет завершен.

Текущий сеанс работы пользователя завершится автоматически, если в веб-интерфейсе отсутствовала активность пользователя в течение 24 часов. Для возобновления сеанса работы пользователя потребуется повторная аутентификация.

# Интерфейс ViPNet EPP Сервер

На рисунке ниже представлено главное окно ViPNet EPP Сервер в режиме администратора ViPNet EPP.

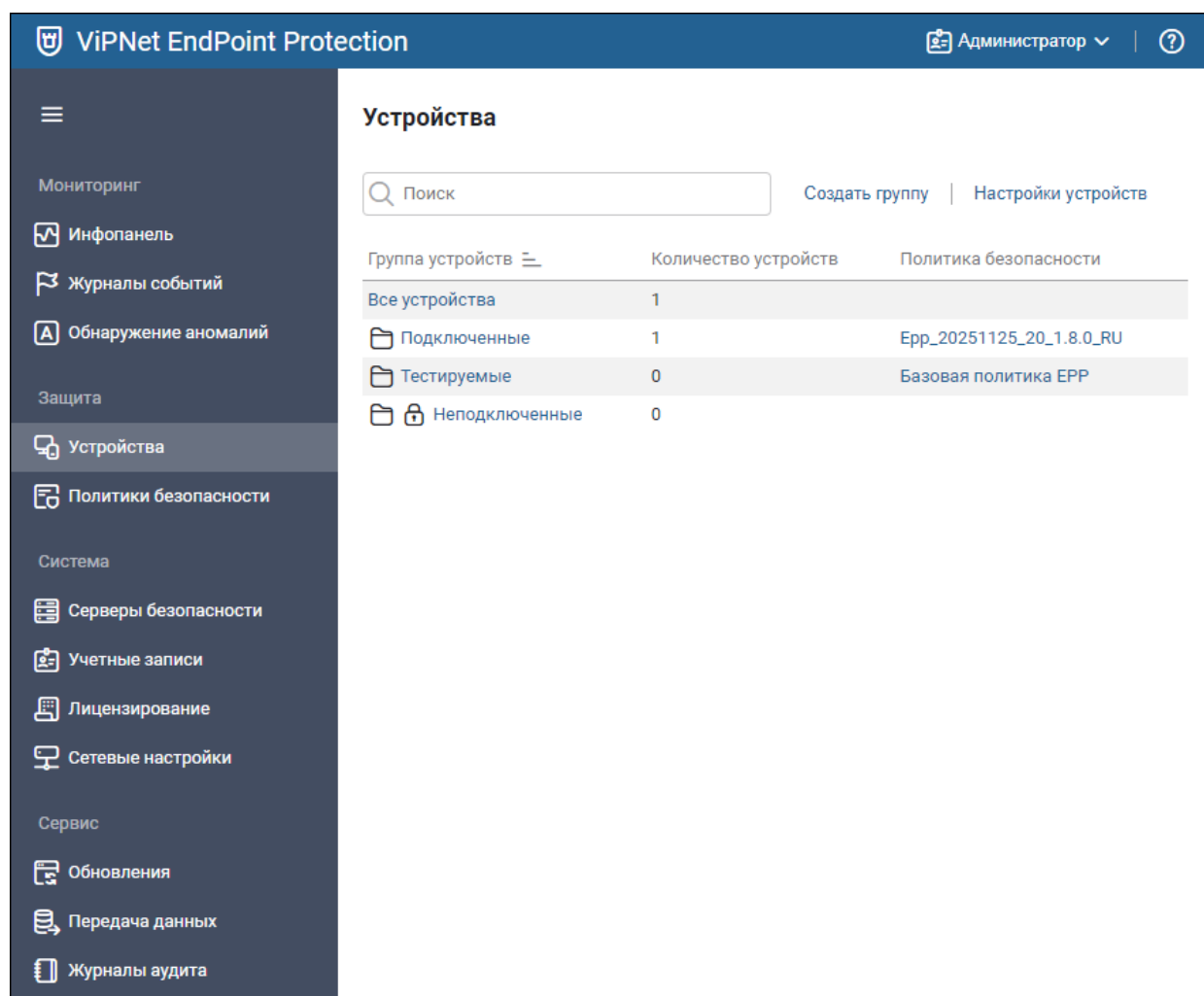


Рисунок 12. Главное окно ViPNet EPP Сервер в режиме администратора ViPNet EPP

Панель слева содержит разделы настройки ViPNet EPP и просмотра результатов его работы:

- **Инфопанель** — просмотр критичных событий журнала регистрации событий защищаемых узлов в режиме, близком к реальному времени. Настройка параметров критичных событий для регистрации в журнале (см. [Критичные события агентов \(Инфопанель\)](#)).
- **Журналы событий** — запрос и просмотр журналов событий информационной безопасности с защищаемых узлов за заданный период времени (см. [Журналы событий](#)).
- **Обнаружение аномалий** — настройка правил (критериев) обнаружения аномалий (см. [Настройка критериев обнаружения аномалий](#)).

-  **Устройства** — подключение защищаемых узлов, назначение базы правил группам узлов, управление группами узлов и просмотр состояния узлов (см. [Управление защищаемыми узлами и группами](#)).
-  **Политики безопасности** — загрузка базы правил и настройка политик безопасности (см. [Загрузка базы правил](#)).
-  **Серверы безопасности** — настройки серверов безопасности (см. [Настройка параметров сервера управления](#)), управление рабочими серверами.
-  **Учетные записи** — управление учетными записями ViPNet EPP Сервер: создание, редактирование, удаление (см. [Управление учетными записями](#)).
-  **Лицензирование** — [установка и активация лицензии](#), [обновление лицензии](#).
-  **Сетевые настройки** — настройка подключения к почтовому серверу (см. [Подключение к почтовому серверу](#)).
-  **Обновления** — настройка подключения к серверу обновлений и настройка автоматической загрузки обновлений (см. [Автоматическая загрузка обновлений базы правил](#)).
-  **Передача данных** — интеграция с внешними системами:
  - Передача событий по электронной почте (см. [Передача уведомлений по электронной почте](#)).
  - Передача событий в ViPNet TIAS или сторонние системы мониторинга (см. [Передача событий информационной безопасности в сторонние системы](#)).
-  **Журналы аудита** — просмотр журналов аудита сервера управления и рабочих серверов (см. [Журналы аудита](#)).

Панель заголовка:

-  **О программе** — версия программного обеспечения ViPNet EPP, контактные данные ИнфоТеКС, текст лицензионного соглашения.
-  **имя авторизованного пользователя** — завершение работы с веб-интерфейсом ViPNet EPP Сервер текущего пользователя.

# Установка и активация лицензии

При первом подключении к веб-интерфейсу ViPNet EPP Сервер необходимо установить и активировать лицензию ViPNet EPP:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Лицензирование** и нажмите **Установить лицензию**.
- 3 Выберите файл лицензии формата `itcslic`.



**Внимание!** Лицензия должна быть выпущена для работы ViPNet EPP Сервер в ОС GNU/Linux. Лицензия, выпущенная для ViPNet EPP Сервер for Windows, не установится.

---

- 4 Просмотрите информацию о составе лицензии и сроке действия, для установки лицензии нажмите **Установить**.

Дождитесь установки лицензии.

- 5 Нажмите **Активировать** и активируйте лицензию одним из способов:
  - Автоматически (необходим доступ к интернету) — выберите **Автоматически** и нажмите **Активировать**.
  - По электронной почте (с помощью запроса на активацию):

5.1.1 Выберите **По электронной почте** и нажмите **Далее**.

5.1.2 Чтобы создать письмо с запросом на активацию в установленном у вас почтовом клиенте, нажмите **Создать письмо с запросом**.

5.1.3 Чтобы отправить письмо с другого компьютера, нажмите **Скачать файл запроса** и сохраните запрос в файл.

5.1.4 Отправьте письмо с файлом запроса на электронный адрес [reg@infotecs.ru](mailto:reg@infotecs.ru).

Дождитесь ответного письма — в нем будет указан код регистрации для активации ViPNet EPP.

5.1.5 Введите код регистрации в одноименном поле.

5.1.6 Нажмите **Активировать**.

При успешной активации появится сообщение о завершении активации. Нажмите **Готово**.

В разделе  **Лицензирование** отобразится информация о лицензии и в строке **Статус** появится



**Активирована.**

# Управление защищаемыми узлами и группами

## Подключение защищаемых узлов

Защищаемые узлы, которыми планируется управлять с помощью ViPNet EPP Сервер, необходимо подключить к ViPNet EPP Сервер. При подключении к серверу защищаемым узлам распределяется лицензия для включения на узлах модулей защиты и отслеживания событий информационной безопасности с ViPNet EPP Сервер.

После установки и настройки ViPNet EPP Агент защищаемого узла автоматически отправляет на ViPNet EPP Сервер запрос на подключение. Защищаемый узел, от которого поступил запрос, отображается на сервере в разделе  **Устройства** в служебной группе **Неподключенные**. Для подключения к серверу защищаемый узел необходимо перенести в пользовательскую группу на сервере, указав модули защиты, которые будут доступны на узлах. Не рекомендуем добавлять более 500 узлов в одну группу. Это может привести к большой нагрузке на сервер и замедлению работы компьютера.

Для включения на защищаемом узле выбранных модулей защиты назначьте его пользовательской группе политику безопасности (см. [Назначение политики группе узлов](#)). Если политика уже была назначена группе, модули защиты включатся на защищаемом узле автоматически после перемещения в группу и получения политики.

В ViPNet EPP предусмотрены служебные и пользовательские группы узлов:

- Служебные группы:
  - **Неподключенные** — группа узлов, от которых пришел запрос на подключение.
  - **Все устройства** — группа всех узлов (подключенные и неподключенные к серверу).

Служебные группы невозможно удалить, а также назначить им политику безопасности.

- Пользовательская предустановленная группа: **Подключенные**.

Администратор ViPNet EPP Сервер может создавать новые пользовательские группы узлов (см. [Управление группами защищаемых узлов](#)). Пользовательские группы можно удалять и назначать им политику.

Если на защищаемые узлы будут назначаться разные политики безопасности, перед подключением защищаемых узлов создайте необходимые группы для распределения в них устройств (см. [Управление группами защищаемых узлов](#)).

Вы можете настроить автоматическое подключение защищаемых узлов к ViPNet EPP Сервер (см. [Настройка автоматического подключения защищаемых узлов](#)).

Чтобы подключить один или несколько защищаемых узлов:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Устройства** > **Неподключенные**.
- 3 Выберите одно или несколько устройств, которые необходимо подключить к ViPNet EPP Сервер. Несколько устройств выберите флажками.

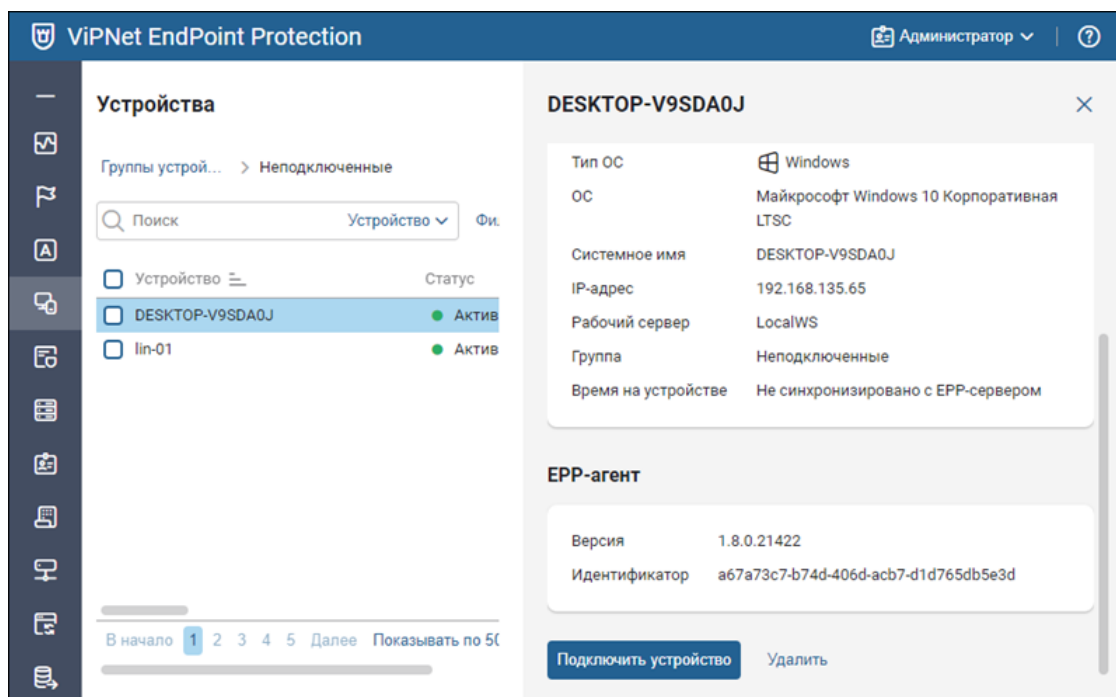


Рисунок 13. Подключение защищаемых узлов

- 4 На панели справа нажмите **Подключить устройство**. Если выбрано несколько устройств, на панели сверху нажмите **Подключить**.
- 5 Выберите пользовательскую группу для перемещения в нее узлов.
- 6 Чтобы время на узле было синхронизировано со временем ViPNet EPP Сервер, выберите **Синхронизировать время на устройстве с EPP-сервером**.
- 7 Выберите флажками модули защиты, которые должны быть доступны на узлах. Список модулей зависит от лицензии ViPNet EPP (см. [Лицензирование](#)). **Контроль приложений** выбирайте только для узлов с ОС Windows.
- 8 Нажмите **Подключить**.

После подключения защищаемых узлов на пользовательские группы узлов необходимо назначать политики, если они еще не назначены (см. [Назначение политики группе узлов](#)).

# Настройка автоматического подключения защищаемых узлов

Чтобы не подключать защищаемые узлы к ViPNet EPP Сервер вручную, вы можете настроить автоматическое подключение защищаемых узлов. По умолчанию автоматическое подключение выключено. При включении автоматического подключения нужно выбрать:

- Пользовательскую группу ViPNet EPP Сервер, в которую будут автоматически перемещаться защищаемые узлы, приславшие запросы на подключение. Выбранная пользовательская группа в разделе  **Устройства** будет отмечена значком .
- Модули защиты, которые будут доступны на узлах.

Автоматически подключаться к ViPNet EPP Сервер и перемещаться в выбранную при настройке пользовательскую группу будут только те защищаемые узлы, которые прислали запросы на подключение после включения автоматического подключения.

Для успешного автоматического подключения защищаемых узлов необходимо наличие свободных лицензий для всех выбранных модулей ViPNet EPP. Если закончились свободные лицензии хотя бы на один модуль ViPNet EPP, автоматическое подключение защищаемых узлов выполняться не будет. При этом защищаемые узлы, приславшие запрос на подключение, отобразятся в группе **Неподключенные**, откуда их можно будет подключить вручную (см. [Подключение защищаемых узлов](#)).

Чтобы включить автоматическое подключение новых защищаемых узлов:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Устройства** > **Настройки устройств**.
- 3 В разделе **Автоподключение** выберите **Автоматически подключать новые устройства к EPP-серверу**, в списке выберите группу для добавления новых узлов и укажите модули защиты.
- 4 Нажмите **Сохранить**.

Для включения на защищаемом узле выбранных модулей защиты назначьте выбранной пользовательской группе политику (см. [Назначение политики группе узлов](#)). Если политика уже назначена группе, модули защиты включатся на защищаемом узле автоматически после перемещения в группу и получения политики.

## Управление группами защищаемых узлов

Для управления группами доступны:

- Просмотр списка групп.
- Создание новой группы.

- Изменение имени группы.
- Удаление группы.
- Назначение новой политики группе.
- Отзыв политики с группы. В результате отзыва политики узлы группы станут незащищенными.

Вы можете управлять группами защищаемых узлов и просматривать сведения о них:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Устройства** и просмотрите сведения о группах. Для групп в списке отображаются:
  - **Группа устройств** — название группы. Группа будет отмечена значком ★, если для нее настроено автоматическое подключение защищаемых узлов.
  - **Количество устройств** — количество устройств в группе.
  - **Политика безопасности** — название политики, назначенной для группы.
- 3 Чтобы посмотреть список всех защищаемых узлов, выберите группу **Все устройства**.
- 4 Чтобы создать новую группу:
  - 4.1 Нажмите **Создать группу** и введите название новой группы.
  - 4.2 Вы можете сразу назначить новой группе политику безопасности, если она уже была создана (см. [Управление политиками безопасности](#)). Для этого в списке **Политика безопасности** выберите политику по названию и номеру.



**Примечание.** Политику безопасности можно назначить и позднее (см. [Назначение политики группе узлов](#)).

---

- 4.3 Нажмите **Создать**.
- 5 Чтобы найти группу узлов, в поле поиска  введите имя группы или ее часть.
- 6 Чтобы изменить название группы, выберите строку группы, на панели справа нажмите  и введите новое название. Нажмите **Сохранить**.
- 7 Чтобы удалить группу, выберите строку группы, на панели справа нажмите  и подтвердите удаление.



**Примечание.** Группа доступна для удаления, если в ней нет защищаемых узлов.

---

- 8 Чтобы назначить другую политику на группу, выберите строку группы, на панели справа нажмите **Назначить новую политику**, выберите политику и нажмите **Назначить**.

- 9 Чтобы отозвать назначенную политику с группы, выберите строку группы, на панели справа нажмите **Отозвать политику** и подтвердите отзыв.

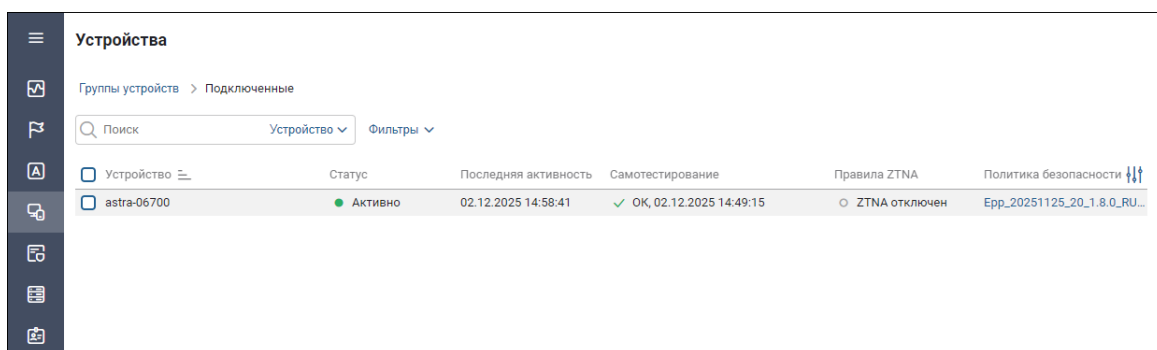
## Управление защищаемыми узлами группы

Для управления защищаемыми узлами доступны:

- Просмотр списка узлов.
- Просмотр свойств выбранного узла.
- Изменение настроек узла: имени, группы подключения, синхронизации времени с сервером и модулей безопасности, доступных на узле.
- Отключение узла от сервера. В результате модули защиты узла будут отключены и узел станет незащищенным.
- Удаление узла. Удалить можно только неподключенный узел.

Вы можете управлять защищаемыми узлами группы и просматривать сведения о них:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Устройства**:
  - Чтобы посмотреть список всех подключенных и не подключенных защищаемых узлов, выберите группу **Все устройства**.
  - Чтобы посмотреть список еще не подключенных узлов, выберите группу **Неподключенные**.
  - Чтобы просмотреть список подключенных защищаемых узлов в определенной группе, выберите пользовательскую группу, например группу **Подключенные**.



| Устройства                                                                          |         |                      |                           |                 |                             |
|-------------------------------------------------------------------------------------|---------|----------------------|---------------------------|-----------------|-----------------------------|
| Группы устройств > Подключенные                                                     |         |                      |                           |                 |                             |
| <input type="text" value="Поиск"/> <span>Устройство ▾</span> <span>Фильтры ▾</span> |         |                      |                           |                 |                             |
| Устройство                                                                          | Статус  | Последняя активность | Самотестирование          | Правила ZTNA    | Политика безопасности       |
| <input type="checkbox"/> astra-06700                                                | Активно | 02.12.2025 14:58:41  | ✓ ОК, 02.12.2025 14:49:15 | ○ ZTNA отключен | Epp_20251125_20_1.8.0_RU... |

Рисунок 14. Список защищаемых узлов в группе

Для подключенного защищаемого узла в списке в табличном виде отображаются:

- **Устройство** — название защищаемого узла.
- **Группа** — группа, в которую входит защищаемый узел. Отображается только при просмотре узлов в группе **Все устройства**.

- **Статус** — активность узла: **Активно**, **Неактивно**, **Неизвестно**. Узел активен, если он регулярно обменивается данными с ViPNet EPP Сервер. Если в течение периода времени, определяемого параметром **Период обмена данными с EPP-сервером**, обмена данными не происходит, защищаемый узел считается неактивным. Это означает, что связь с узлом потеряна, и события на узле не отслеживаются. Если статус определить не удалось, будет отображено **Неизвестно**.
- **Последняя активность** — время последнего обмена данными с сервером.
- **Самотестирование** — результат последнего самотестирования:
  - ОК — проблем не обнаружено.
  - Проблема — выявлены проблемы. Подробности вы можете посмотреть на панели справа на вкладке **Самотестирование**.
  - Неизвестно — не удалось получить данных о самотестировании.
- **Правила ZTNA** — статус выполнения [правил ZTNA](#).
- **Политика безопасности** — название политики безопасности, используемой на узле.
- **Режимы модулей EPP**:
  - Из политики — на узле используются режимы работы модулей защиты, заданные в политике.
  - Локальные — режимы работы модулей защиты изменены на защищаемом узле.
- **Системное имя, IP-адрес** защищаемого узла.
- **Тип ОС**:
  -  — защищаемые узлы с ОС Windows.
  -  — защищаемые узлы с ОС GNU/Linux.
- **Операционная система** — операционная система, установленная на узле.
- **Модули EPP** — модули защиты ViPNet EPP, доступные на узле:
  -  — Межсетевой экран.
  -  — Обнаружение вторжений.
  -  — Предотвращение вторжений.
  -  — Контроль приложений.
- **Версия EPP-агента** — номер версии ViPNet EPP Агент, установленной на защищаемом узле.
- **Рабочий сервер** — название рабочего сервера, который обслуживает защищаемый узел.

Вы можете настраивать видимость столбцов таблицы списка защищаемых узлов. По умолчанию отображаются все столбцы. Для настройки справа нажмите  и снимите флажки столбцов, которые нужно скрыть.

- Чтобы в списке узлов найти определенный узел, в поле поиска  справа выберите характеристику узла, по которому будете искать и введите ключевое слово для поиска. По умолчанию поиск выполняется по названию узла (устройства).
- Чтобы просмотреть подробные сведения об определенном подключенном узле, найдите этот узел в списке и выберите его — на панели справа будут отображены вкладки:
  - **Общее** — информация о защищаемом узле (аналогично данным при просмотре списка узлов).
  - **Самотестирование** — информация о последней проверке работоспособности узла: дата и время, результат проверки (см. [Проверка работоспособности](#)). Периодичность проверки работоспособности узла определяется параметром **Период самотестирования** (см. [Настройка параметров защищаемых узлов](#)).
  - **События:**
    - Чтобы просмотреть на инфопанели в режиме реального времени журнал критичных событий, зарегистрированных на узлах, нажмите **Перейти к мониторингу**.
    - Чтобы просмотреть журнал событий узла за определенный период и с определенными характеристиками событий, нажмите **Запросить журнал** и настройте критерии поиска (см. [Журналы событий](#)).
  - **Трафик** — создание и просмотр отчетов журнала трафика узла (см. [Запрос журнала регистрации трафика с ViPNet EPP Агент](#)).
- Чтобы в списке узлов выбрать узлы по их характеристикам, используйте фильтры: нажмите **Фильтр** и выберите из списков критерии фильтрации.
- Чтобы изменить настройки подключенного узла, выберите его и на панели справа сверху нажмите . Измените имя узла, выберите другую группу, измените настройку синхронизации времени с сервером и укажите доступные модули безопасности аналогично действиям при подключении узла (см. [Подключение защищаемых узлов](#)). Нажмите **Сохранить**.
- Чтобы временно отключить узел от ViPNet EPP Сервер (прекратить отслеживание событий узла), выберите его — на панели справа сверху нажмите  > **Отключить от EPP-сервера** и подтвердите отключение — узел будет перемещен в группу **Неподключенные**. Временно отключенные узлы можно удалить с ViPNet EPP Сервер.
- Чтобы удалить узел с ViPNet EPP Сервер, в группе **Неподключенные** выберите его флажком, на панели сверху нажмите  и подтвердите удаление узла.

# Управление политиками безопасности

После установки ViPNet EPP Сервер содержит базовую политику EPP, сформированную на основе встроенной базы правил. Для своевременного выявления новых угроз безопасности информации необходимо обновлять базу правил с сервера обновлений сразу после установки ViPNet EPP Сервер и далее обновлять регулярно. Вы можете настроить автоматическое обновление базы правил или загружать вручную (см. [Загрузка базы правил](#)).

После загрузки обновления базы правил в ViPNet EPP Сервер, на ее основе формируется новая версия политики безопасности.

Политика безопасности назначается группе узлов (см. [Назначение политики группе узлов](#)) и применяется ко всем защищаемым узлам группы.

Для применения на защищаемых узлах политику нужно назначать группам узлов (см. [Назначение политики группе узлов](#)).

Доступны следующие действия с политиками безопасности:

- Просмотр списка политик и данных об определенной политике.
- Загрузка обновлений баз правил (см. [Загрузка базы правил](#)).
- Настройка политики и создание новой политики на основе существующей (см. [Порядок настройки политики](#)).
- Удаление неиспользуемых политик (см. [Удаление политики](#)).

Не рекомендуем хранить на сервере более 225 политик безопасности. Это может привести к большой нагрузке на сервер и замедлению работы компьютера. Регулярно удаляйте ненужные политики (см. [Удаление политики](#)).

Чтобы просмотреть список политик ViPNet EPP Сервер и найти нужную политику:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  Политики безопасности.

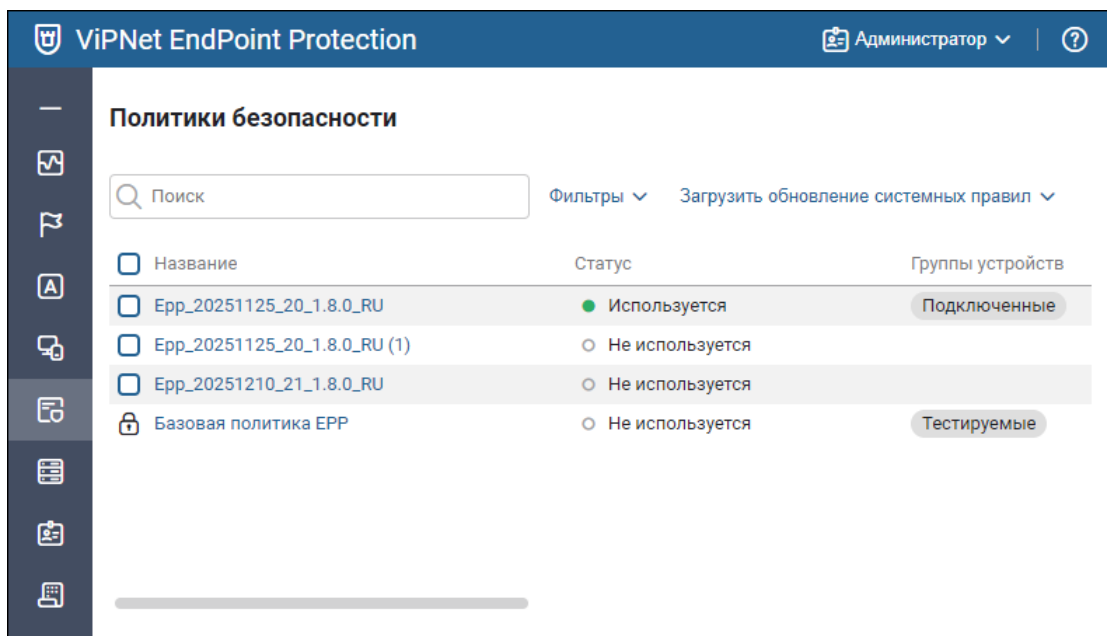


Рисунок 15. Список политик безопасности ViPNet EPP Сервер

- В строке поиска  введите часть названия политики или воспользуйтесь фильтром по статусам.

Чтобы просмотреть сведения об определенной политике, в списке политик выберите строку с политикой.

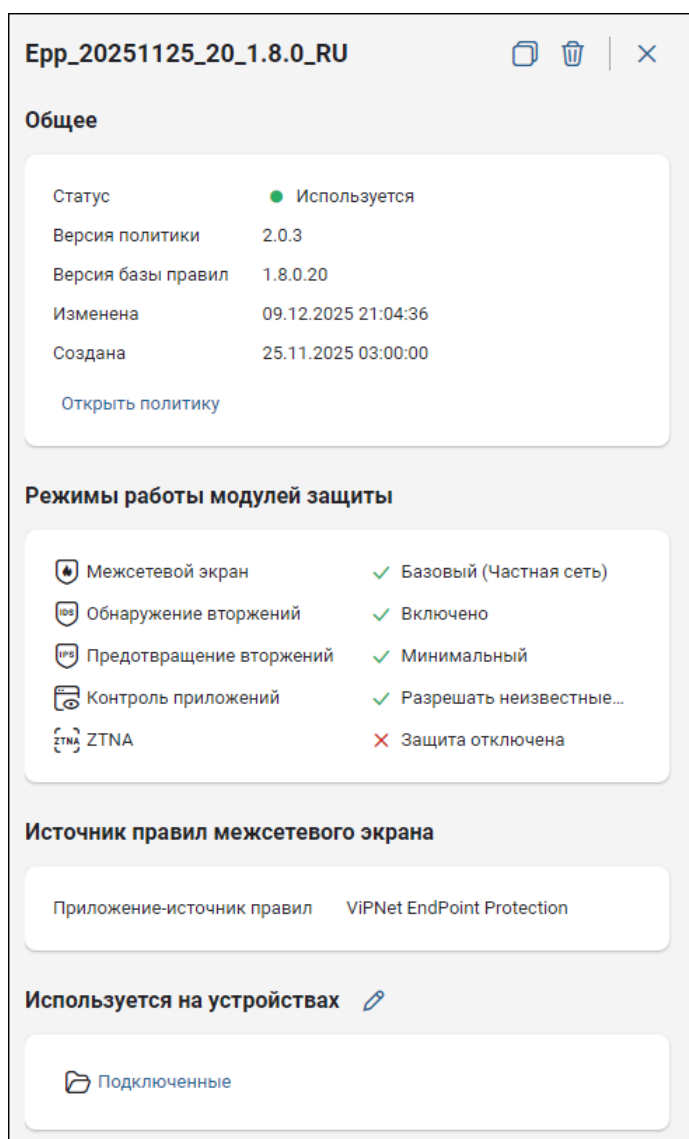


Рисунок 16. Сведения о политике безопасности

На панели справа отображаются сведения о политике:

- **Статус:**
  - **Используется** — применяется на защищаемых узлах групп.
  - **Отзывается** — политика уже не назначена никаким группам узлов, но есть узлы, на которых эта политика еще используется, например, защищаемый узел неактивен и на него еще не загружена новая назначенная ему политика.
  - **Не используется** — не применяется ни на одном защищаемом узле.
- Версия политики, версия базы правил, дата изменения политики, дата создания базы правил.
- **Режимы работы модулей защиты.**
- **Источник правил межсетевого экрана** — ViPNet EndPoint Protection или ViPNet Prime, ViPNet Policy Manager.

- **Используется на устройствах** — список групп защищаемых узлов, на которые назначена политика.

Чтобы отфильтровать список политик по статусу использования, нажмите **Фильтры** и выберите критерии фильтрации — используется, не используется или отзывается.

## Загрузка базы правил

Варианты загрузки обновлений базы правил в ViPNet EPP Сервер:

- автоматически с заданным периодом (рекомендуем использовать этот вариант) (см. [Автоматическая загрузка обновлений базы правил](#));
- вручную (см. [Загрузка обновления базы правил вручную](#)).

## Автоматическая загрузка обновлений базы правил

ViPNet EPP поддерживает автоматическую загрузку обновлений базы правил с [сервера обновлений](#). После загрузки лицензии режим автоматической загрузки обновлений баз правил будет включен, обновление будет проверяться каждые 24 часа. Вы можете изменить эти параметры.

Для настройки автоматической загрузки вам могут потребоваться:

- Имя и пароль учетной записи пользователя для подключения к серверу обновлений, указанные в PDF-файле лицензии. По умолчанию эти данные автоматически загружаются в ViPNet EPP Сервер при установке лицензии.
- Адрес сервера обновлений, если он отличается от установленного по умолчанию. Адрес указан в PDF-файле лицензии. Адрес сервера обновлений по умолчанию автоматически загружается в ViPNet EPP Сервер при установке лицензии.
- Если на сервере управления интернет доступен через прокси-сервер, потребуется предварительно на компьютере с сервером управления настроить параметры доступа к прокси-серверу: адрес и порт прокси-сервера, имя и пароль пользователя (при их наличии). Пример настройки для HTTP-прокси:

В файле `/etc/environment` укажите:

- Если на прокси-сервере есть аутентификация пользователя:

```
https_proxy="http[s]://<имя пользователя>:<пароль пользователя>@<адрес прокси-сервера>:<порт прокси-сервера>"
```

Например, `https_proxy="http://test_user:test_password@192.168.120.152:3128"`

- Если на прокси-сервере аутентификации пользователя нет:

```
https_proxy="http[s]://<адрес прокси-сервера>:<порт прокси-сервера>"
```

Например, `https_proxy="http://192.168.120.152:3128"`

После изменения файла необходимо перезагрузить компьютер.



**Совет.** При совместной работе ViPNet EPP Сервер и ViPNet EPP Агент на защищаемом узле рекомендуется переместить этот узел в отдельную пользовательскую группу и назначить на нее политику, в которой правила межсетевого экрана не блокируют трафик между ViPNet EPP Сервер и сервером обновлений.

Чтобы настроить автоматическую загрузку обновлений:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Обновления**.
- 3 Включите  **Автоматическая загрузка обновлений**.
- 4 Чтобы изменить периодичность проверки обновлений базы правил, в разделе **Автоматическая загрузка обновлений** нажмите  и укажите период от 12 часов до 1 месяца.
- 5 В разделе **Настройка подключения к серверу обновлений** нажмите .
- 6 Если в PDF-файле лицензии указан адрес сервера обновлений, отличный от установленного по умолчанию (`https://updateids.infotecs.ru`), задайте его.
- 7 Если была установлена лицензия, имя учетной записи пользователя и пароль для подключения к серверу обновлений уже указаны в соответствующих полях. Если имя учетной записи пользователя и пароль автоматически не добавились, вручную введите имя учетной записи и пароль, указанные в PDF-файле лицензии.
- 8 Для проверки подключения к серверу обновлений нажмите **Проверить подключение**. Если были выявлены проблемы подключения, раздел  **Обновления** будет отмечен желтым маркером .
- 9 Чтобы вернуть измененные параметры к значениям по умолчанию, нажмите **По умолчанию**.
- 10 Нажмите **Сохранить**.

## Загрузка обновления базы правил вручную

Вы можете загружать базу правил в ViPNet EPP Сервер вручную, например, если автоматическая загрузка выключена или требуется в определенное время загрузить и отправить обновление. При загрузке обновления базы правил в ViPNet EPP Сервер проверяется электронная подпись базы правил.

Доступна загрузка:

- Из файла. Предварительно с сервера обновлений необходимо скачать файл архива обновления базы правил (формата ZIP) и файл электронной подписи (формата SIG). База правил должна быть совместима с установленной у вас версией ViPNet EPP.
- Непосредственно с сервера обновлений (только при наличии там новой версии базы правил, совместимой с используемой у вас версией ViPNet EPP). Предварительно должно быть настроено подключение к серверу обновлений (см. [Автоматическая загрузка обновлений базы правил](#)).

Чтобы с сервера обновлений скачать файлы архива обновления базы правил и электронной подписи:

- 1 В браузере введите `https://updateids.infotecs.ru`.
- 2 Введите имя и пароль своей учетной записи для входа на сервер обновлений.



**Примечание.** Имя и пароль учетной записи для входа на сервер обновлений указаны в PDF-файле лицензии на ViPNet EPP.

---

- 3 Выберите  **ViPNet EndPoint Protection > Базы правил.**
- 4 В списке обновлений найдите последнее по дате создания обновление базы правил, совместимое с используемой у вас версией ViPNet EPP:



**Примечание.** Последнее обновление базы правил содержит актуальные настройки и правила, поэтому более ранние обновления базы правил скачивать не требуется.

---

- 4.1 Щелкните файл обновления. Файл с обновлением будет сохранен на компьютер.
- 4.2 Щелкните файл электронной подписи. Файл с электронной подписью будет сохранен на компьютер.

| VIPNet Update Server                      |                        |                 |               |                |                                  |
|-------------------------------------------|------------------------|-----------------|---------------|----------------|----------------------------------|
| Обновления для VIPNet EndPoint Protection |                        |                 |               |                |                                  |
| Базы правил                               |                        |                 |               |                |                                  |
| Поиск обновления                          | С любой датой создания | Любая версия ПО | 56 обновлений |                |                                  |
| Файл обновления                           | Версия                 | Дата создания   | Размер        | Совместимые... | Электронная подпись              |
| Epp_20251113_12_1...                      | 12                     | 13.11.2025      | 14.53 М...    | 1.7.2          | Epp_20251113_12_1.7.2_EN.zip.sig |
| Epp_20251110_97_1...                      | 97                     | 10.11.2025      | 24.66 М...    | 1.6            | Epp_20251110_97_1.6_RU.zip.sig   |
| Epp_20251110_69_1...                      | 69                     | 10.11.2025      | 14.78 М...    | 1.7            | Epp_20251110_69_1.7_RU.zip.sig   |
| Epp_20251110_48_1...                      | 48                     | 10.11.2025      | 14.73 М...    | 1.7.1          | Epp_20251110_48_1.7.1_RU.zip.sig |
| Epp_20251110_19_1...                      | 19                     | 10.11.2025      | 14.73 М...    | 1.8.0          | Epp_20251110_19_1.8.0_RU.zip.sig |
| Epp_20251110_104_1...                     | 104                    | 10.11.2025      | 6.33 Мб...    | 1.5            | Epp_20251110_104_1.5_RU.zip.sig  |
| Epp_20251028_11_1.7...                    | 11                     | 28.10.2025      | 14.49 Мб...   | 1.7.2          | Epp_20251028_11_1.7.2_EN.zip.sig |

Рисунок 17. Главная страница сервера обновлений ViPNet Update Server

Чтобы загрузить в ViPNet EPP Сервер обновление базы правил:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  Политики безопасности.
- 3 На панели сверху выберите **Загрузить обновление системных правил > Из файла**.
- 4 Выберите файл обновления базы правил и файл электронной подписи, которые вы скачали с сервера обновления.
- 5 Нажмите **Загрузить**.

После успешной проверки подписи база правил отобразится в списке политик безопасности.

Чтобы вручную проверить и при наличии загрузить обновление базы правил в ViPNet EPP Сервер непосредственно с сервера обновлений:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  Политики безопасности.
- 3 На панели сверху выберите **Загрузить обновление системных правил > С сервера обновлений**.

Если подходящая база правил будет найдена, она загрузится и отобразится в списке политик безопасности.

# Назначение политики группе узлов

Чтобы ViPNet EPP Агент обнаруживал и предотвращал угрозы безопасности информации на защищаемых узлах, назначьте политику безопасности группам, в которые входят эти узлы. Вы можете назначить политики двумя способами:

- Выбрать группы устройств и указать политику.
- При редактировании политики выбрать группы устройств (см. [Порядок настройки политики](#)).

Чтобы назначить политику первым способом:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Устройства**.
- 3 В списке групп выберите строку с группой, на которую нужно назначить политику.
- 4 На панели справа в разделе **Политика безопасности** нажмите **Назначить**, выберите политику по названию и номеру, нажмите **Назначить**.

В результате политика будет отправлена на защищаемые узлы из группы. На странице **Устройства** в списке групп для выбранной группы появится название назначенной политики.

Вы можете изменить политику, для этого нажмите **Назначить новую политику** и выберите политику.

## Порядок настройки политики



**Примечание.** Настройкой политики безопасности должен заниматься аналитик информационной безопасности с компетенциями в области сетевых технологий, знаниями принципов создания правил для систем обнаружения вторжений и опытом расследования инцидентов информационной безопасности.

### Общий порядок настройки политики безопасности

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Политики безопасности**.
- 3 В списке политик щелкните название политики, которую нужно настроить.
- 4 В разделе  **Основное** посмотрите текущие настройки.
- 5 Чтобы изменить название политики, в разделе **Общее** нажмите , введите название и нажмите **Сохранить**.

- 6 Чтобы назначить или изменить используемую политику группам устройств, в разделе **Используется на устройствах** нажмите , выберите флажками одну или несколько групп устройств для назначения им политики и нажмите **Сохранить**.
- 7 Выполните настройки в соответствии с разделами:
- Выбор режимов модулей защиты (см. [Режимы модулей защиты](#)). Чтобы на защищаемом узле работали правила модулей защиты, настроенные в политике, модули защиты должны быть включены.
  - Настройка источника получения правил межсетевого экрана (см. [Источник получения правил межсетевого экрана](#)).
  - [Импорт данных из другой политики](#).
  - Настройка правил (сетевых фильтров) и справочников межсетевого экрана (см. [Правила фильтрации межсетевого экрана](#)).
  - Настройка правил обнаружения вторжений (см. [Правила обнаружения вторжений](#)).
  - Настройка правил предотвращения вторжений (см. [Правила предотвращения вторжений](#)).
  - Настройка правил ZTNA (см. [Правила ZTNA](#)).
  - Настройка правил запуска и активности приложений (только для защищаемых узлов с ОС Windows) (см. [Правила контроля приложений](#)).
- 8 Чтобы сохранить изменения в настраиваемой политике, нажмите **Сохранить**. Подтвердите сохранение. Если политика уже была назначена устройствам, на устройства будет отправлено обновление.
- 9 Чтобы сохранить изменения в новой политике, нажмите **Сохранить как новую политику**. Подтвердите сохранение. Будет создана новая версия политики. Если редактируемая политика уже была назначена устройствам, устройствам будет назначена новая версия политики. На устройства будет отправлено обновление.

## Режимы модулей защиты

Вы можете изменить режимы работы модулей защиты в политике, заданные по умолчанию (см. [Политика безопасности](#)), в соответствии с политикой информационной безопасности вашей организации. Правила модулей защиты будут работать только при включенных модулях.

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Основное**.
- 2 В разделе **Режимы работы модулей защиты** нажмите .
- 3 Чтобы изменить режим работы модуля защиты, включите  его и в списке выберите режим. Для модуля ZTNA режимы не предусмотрены. Его можно только включить или отключить.
- 4 Чтобы отключить работу модуля защиты, выключите  его. Если модуль защиты отключен, режимы не действуют.

- 5 Нажмите **Сохранить**.
- 6 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Источник получения правил межсетевого экрана

На защищаемом узле в ViPNet EPP Агент в качестве фильтров политик безопасности открытой сети могут использоваться правила межсетевого экрана, полученные из одного из следующих источников (см. [Межсетевой экран](#)):

- ViPNet EPP Сервер;
- ViPNet Prime или ViPNet Policy Manager.

По умолчанию в ViPNet EPP Агент используются правила, полученные из ViPNet EPP Сервер. Вы можете изменить источник получения правил. После смены источника получения правил межсетевого экрана на ViPNet Prime (ViPNet Policy Manager) в ViPNet EPP Агент будут игнорироваться правила межсетевого экрана ViPNet EPP Сервер независимо от наличия правил ViPNet Prime (ViPNet Policy Manager).

Чтобы изменить источник получения правил в ViPNet EPP Агент на ViPNet Prime (ViPNet Policy Manager):

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Основное**.
- 2 В разделе **Источник правил межсетевого экрана** нажмите .
- 3 В списке **Приложение-источник правил** выберите **ViPNet Prime, ViPNet Policy Manager**.
- 4 Нажмите **Сохранить**.
- 5 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

Чтобы снова перейти на использование правил, полученных из ViPNet EPP Сервер, в списке **Приложение-источник правил** выберите **ViPNet EndPoint Protection**.

## Импорт данных из другой политики

Если вы настраиваете новую версию политики, но часть правил и параметров вы уже настраивали ранее в другой политике, вы можете импортировать эти данные, чтобы не настраивать повторно.

Доступен импорт правил и параметров для межсетевого экрана, предотвращения вторжений (только веб-фильтры), контроля приложений и ZTNA. Вы можете настроить для каждого модуля, какие данные нужно импортировать.

При импорте пользовательских правил выполняется проверка на дубликаты. Дубликаты не импортируются. Правила с одинаковыми названиями импортируются с переименованием.

Если вы выберете импорт всех правил, исходные правила полностью заменятся на импортируемые.

Чтобы импортировать данные из другой политики:

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Основное**.
- 2 Раскройте разделе **Импорт данных из другой политики** и нажмите **Импортировать**.
- 3 В списке **Политика-источник данных** выберите политику, откуда требуется импортировать данные.
- 4 Укажите импортируемые данные для каждого модуля. Для этого в разделе модуля нажмите  и выберите данные. Нажмите **Сохранить**.

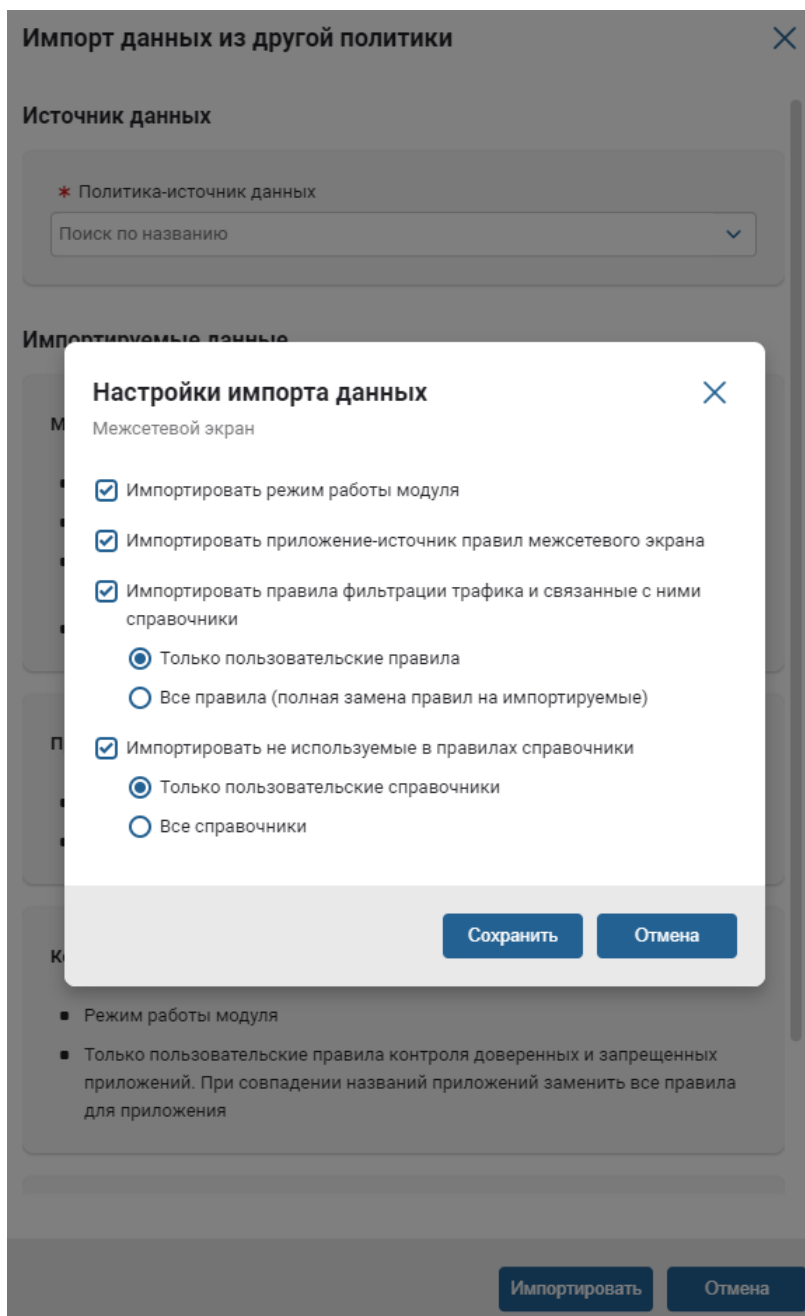


Рисунок 18. Настройка импортируемых данных

- 5 Нажмите **Импортировать**.
- 6 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Правила фильтрации межсетевого экрана

Правила фильтрации межсетевого экрана (фильтры политик безопасности (см. [Межсетевой экран](#))) применяются для обработки IP-пакетов сетевого трафика межсетевым экраном ViPNet EPP Агент.

Фильтры действуют в режимах публичной (усиленный) и частной сети (базовый) политики, в которой они были созданы или изменены.

Для настройки правил фильтрации доступны:

- Создание правила.
- Изменение порядка применения правил.
- Изменение параметров уже созданных правил.
- Удаление правил.
- Настройка справочников.

## Общий порядок управления правилами фильтрации межсетевого экрана

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Межсетевой экран > Правила фильтрации**.
- 2 На панели вверху выберите один из режимов — **Усиленный** (Публичная сеть) или **Базовый** (Частная сеть).
- 3 Просмотрите текущий список правил. Для каждого правила в списке отображаются параметры фильтрации IP-пакетов:
  - Состояние — состояние правила: включено или выключено.
  - Правило — название правила.
  - Действие — фильтр пропускает  **Пропускать** или блокирует  **Блокировать** IP-пакеты с заданными настройками.
  - Версия IP — версия IP-протокола: IP v4 или IP v6.
  - Источник и Назначение — отправители и получатели IP-пакетов.
  - Протоколы — протоколы передачи IP-пакетов.
  - Расписание — время действия правила.
  - Режим — в каких режимах действует правило.
  -  — наличие такого значка для правила означает, что правило было создано или изменено пользователем.
- 4 Выполните действия в соответствии с описанием ниже.
- 5 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Создание правила фильтрации

1 В разделе выбранного режима **Усиленный** (Публичная сеть) или **Базовый** (Частная сеть) на панели вверху выберите **Создать правило** > версия IP-протокола в правиле (IPv4 или IPv6) и настройте правило:

- Выберите  **Правило включено**.
- Введите название правила.
- Выберите действие правила:  **Пропускать** или  **Блокировать**.
- Выберите режимы, в которых будет использоваться правило. Вы можете создать правило как для одного режима, так и сразу для двух — **Усиленный** (Публичная сеть) или **Базовый** (Частная сеть).
- Чтобы задать адреса источников, в разделе **Источники** нажмите  и укажите адреса отправителей IP-пакетов. По умолчанию правило будет применяться к IP-пакетам с любыми адресами отправителя в формате выбранной версии IP-протокола. Для выбора определенных IP-адресов отправителей, на основании которых будет срабатывать правило:
  - Выберите справочники адресов из списка.



**Внимание!** В составе одного правила не следует использовать справочники **Мой компьютер** и **Другие компьютеры** одновременно с другими справочниками.

---

- Добавьте новый справочник адресов. Нажмите **Добавить адреса** и укажите IP-адреса для справочника адресов. В результате созданный справочник адресов будет выбран для правила.
- Нажмите **Сохранить**.
- Чтобы задать адреса назначений, в разделе **Назначения** нажмите  и укажите адреса получателей IP-пакетов. По умолчанию фильтр будет применяться к IP-пакетам с любыми адресами получателей в формате выбранной версии IP-протокола. Для выбора определенных IP-адресов получателей, на основании которых будет срабатывать фильтр, выполните такие же действия, как для адресов источников.
- Чтобы задать протоколы, в разделе **Протоколы** нажмите  и укажите протоколы передачи пакетов. По умолчанию фильтр будет применяться к IP-пакетам, передаваемым по всем протоколам. Для выбора определенных протоколов, на основании которых будет срабатывать фильтр:
  - Выберите справочники протоколов из списка.
  - Добавьте новый справочник протоколов. Нажмите **Добавить протоколы**, укажите протоколы и их параметры для создания справочника. В результате созданный справочник протоколов будет выбран для фильтра.
  - Нажмите **Сохранить**.

- Чтобы задать расписание, в разделе **Расписание** нажмите  и укажите расписание применения фильтра. По умолчанию фильтр будет применяться всегда. Для выбора определенного времени применения:
  - Выберите справочники расписания из списка.
  - Добавьте новый справочник расписания. Нажмите **Добавить расписание**, укажите параметры для создания справочника и нажмите **Создать**. В результате созданный справочник расписания будет выбран для правила.
  - Нажмите **Сохранить**.
- Нажмите **Создать**.

В результате для указанных режимов в разделе **Межсетевой экран** будет создано правило фильтрации, отмеченное признаком .

## Изменение порядка применения правил

Правила применяются в списке последовательно, сверху вниз, до первого срабатывания. Чтобы изменить порядок применения:

- 1 В разделе выбранного режима **Усиленный** (Публичная сеть) или **Базовый** (Частная сеть) в списке правил выберите флажками одно или несколько правил, порядок применения которых необходимо изменить.
- 2 На панели сверху нажмите  или  для перемещения выбранных правил в списке.

## Изменение параметров правил

- 1 В разделе выбранного режима **Усиленный** (Публичная сеть) или **Базовый** (Частная сеть) в списке выберите правило или предварительно на панели сверху воспользуйтесь поиском  по названию правила.
- 2 На панели справа посмотрите сведения о правиле. В разделе **Общее** вы можете изменить активность правила.
- 3 Чтобы внести изменения в другие параметры правила, сверху справа нажмите  и внесите необходимые изменения аналогично созданию правила (см. выше).
- 4 Нажмите **Сохранить**.

## Удаление фильтров

- 1 В разделе выбранного режима **Усиленный** (Публичная сеть) или **Базовый** (Частная сеть) в списке правил выберите флажками правила.
- 2 На панели сверху нажмите .

3 Подтвердите удаление.

## Настройка справочников

Справочники позволяют упростить процессы создания и изменения правил фильтрации межсетевого экрана.

Чтобы создать справочник:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Политики безопасности**.
- 3 В списке политик щелкните название политики, которую нужно настроить.
- 4 Выберите  **Межсетевой экран > Справочники**.
- 5 Выберите вкладку вида справочника и настройте справочники в соответствии с описанием в разделе:
  - [Адреса](#).
  - [Протоколы](#).
  - [Расписания](#).

Чтобы посмотреть и изменить справочник:

- 1 Выберите вкладку вида справочника и выберите строку справочника в списке или предварительно на панели вверху воспользуйтесь поиском  по названию справочника.
- 2 На панели справа просмотрите параметры справочника и применение в правилах.
- 3 Чтобы изменить справочник, вверху справа нажмите  и внесите необходимые изменения аналогично созданию справочника определенного типа (см. выше).
- 4 Нажмите **Сохранить**.

Чтобы удалить справочник, на вкладке типа справочника выберите строку справочника в списке и на панели справа нажмите . Чтобы удалить сразу несколько справочников, выберите их флажками и на панели вверху нажмите . В результате справочники будут удалены, если они не используются в сетевых фильтрах.

### *Адреса*

На вкладке **Адреса** просмотрите существующие справочники адресов и создайте новый:

- 1 Выберите **Создать справочник > версия IP-протокола (IPv4 или IPv6) > Адреса**.
- 2 Введите название справочника.

- 3 Введите IP-адреса в составе справочника и исключения из справочника в разделах **Состав** и **Исключения** в зависимости от выбранной версии IP-протокола:
- Если был выбран IPv4-адрес, введите адрес, подсеть или диапазон адресов в формате IPv4. При указании диапазона IP-адресов разделяйте начальное и конечное значение диапазона дефисом. Например, 192.168.0.1-192.168.0.100. Для указания диапазона адресов вы можете использовать маски подсети, например, 192.168.0.0/24 или 192.168.0.0/255.255.255.0.
  - Если был выбран IPv6-адрес, введите адрес, подсеть или диапазон адресов в формате IPv6, например, 2001:db80:0000:a000:c000:d000:b000:e2f0, 2001:0DB8::/32.



**Примечание.** При указании нескольких IP-адресов, подсетей или диапазонов IP-адресов разделяйте их запятой, точкой с запятой или вводите значение с новой строки.

---

#### 4 Нажмите **Создать**.

### Протоколы

На вкладке **Протоколы** просмотрите существующие справочники протоколов и создайте новый:

- 1 Выберите **Создать справочник** > версия IP-протокола (**IPv4** или **IPv6**) > **Протоколы**.
- 2 Введите название справочника.
- 3 Добавьте протоколы в состав справочника и в исключения из справочника в разделах **Состав** и **Исключения** и настройте параметры в зависимости от выбранной версии IP-протокола и выбранного протокола. В справочник вы можете добавить один или несколько протоколов:
  - Чтобы добавить в состав справочника все протоколы, выберите **Добавить** > **Любой из: TCP, UDP, ICMPv4**. В этом случае возможность добавить в состав справочника конкретные протоколы будет недоступна. Вы можете выбрать исключения из справочника.
  - Выберите **Добавить** > **TCP** и настройте:
    - Введите порты или диапазон портов источника, назначения. При указании диапазона портов разделяйте начальное и конечное значение диапазона дефисом.
    - Укажите команды протокола HTTP, которые должны быть запрещены.
    - Укажите типы файлов, в виде которых должна быть запрещена передача мобильного кода.
  - Выберите **Добавить** > **UDP** и введите порты или диапазон портов источника, назначения. При указании диапазона портов разделяйте начальное и конечное значение диапазона дефисом.
  - Если был выбран IPv4-адрес, выберите **Добавить** > **ICMPv4**, выберите в списке тип ICMPv4-сообщений и при необходимости код сообщения.
  - Если был выбран IPv6-адрес, выберите **Добавить** > **ICMPv6**, выберите в списке нужный тип ICMPv6-сообщений и при необходимости код сообщения.

- Чтобы удалить добавленные протоколы, в разделе с названием протокола справа нажмите .

4 Нажмите **Создать**.

### Расписания

На вкладке **Расписания** просмотрите существующие справочники расписаний и создайте новый:

- 1 Выберите **Создать справочник > Расписание**.
- 2 Введите название справочника.
- 3 Добавьте расписания в разделах **Состав** и **Исключения**. В справочник вы можете добавить одно или несколько расписаний, но только одного типа (либо по дням недели, либо по периоду):
  - Чтобы справочник работал всегда, выберите **Добавить > Всегда**. В этом случае возможность добавить в состав справочника расписания с конкретным временем будет недоступна. Вы можете выбрать исключения из справочника.
  - Чтобы добавить определенные дни недели и время применения фильтра, выберите **Добавить > Дни недели** и укажите данные.
  - Чтобы добавить период применения фильтра, выберите **Добавить > Период** и укажите данные.
  - Чтобы удалить добавленные протоколы, в разделе с названием протокола справа нажмите .

4 Нажмите **Добавить**.

## Правила обнаружение вторжений

**Правила обнаружения вторжений (HIDS)** актуальной версии политики выявляют широкий спектр угроз безопасности информации. Вы можете дополнительно настроить существующие правила, а также создать новые.

Чтобы настроить правила обнаружения вторжений:

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Обнаружение вторжений**.
- 2 Выберите вкладку операционной системы, которая установлена на защищаемых узлах.
- 3 При выборе **ОС Windows** настройте правила отслеживания следующих объектов:
  - Приложения и файлы:
    - [Анализ журналов](#).
    - [Мониторинг файлов](#).
    - [Расчет контрольных сумм файлов](#).

- Бесфайловые атаки, RemSec:
  - [Обнаружение бесфайловых атак.](#)
  - [Обнаружение вредоносной активности RemSec](#)
- Мониторинг сетевой активности:
  - [Обнаружение сетевых атак.](#)
  - [TLS-инспекция.](#)
- Мониторинг системы:
  - [Команды мониторинга системы.](#)
  - [Мониторинг установки ПО.](#)
  - [Мониторинг установки системных обновлений.](#)
- Политика аудита:
  - [Аудит защищаемых узлов.](#)

#### 4 При выборе ОС Linux настройте правила следующих типов:

- Приложения и файлы:
  - [Анализ журналов приложений и служб.](#)
  - [Мониторинг файлов.](#)
  - [Расчет контрольных сумм файлов.](#)
- Мониторинг сетевой активности:
  - [Обнаружение сетевых атак.](#)

#### 5 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Анализ журналов

ViPNet EPP в соответствии с правилами анализа позволяет обнаруживать изменения в журналах:

- событий Windows на защищаемых узлах с ОС Windows (см. [Анализ журналов событий Windows](#));
- приложений и служб на защищаемых узлах с ОС Windows и ОС GNU/Linux (см. [Анализ журналов приложений и служб](#)).

Список анализируемых журналов содержится в настройках. Вы можете настроить параметры работы правил анализа журналов и добавить дополнительные журналы для анализа, а также внести изменения в тексты декодеров и правил анализа для обнаружения других локальных угроз, например, обнаружения событий антивирусов или контроль реестра Windows:

- [Настройка декодера.](#)
- [Настройка правил анализа.](#)

## Анализ журналов событий Windows

ViPNet EPP позволяет обнаруживать изменения в журналах событий ОС Windows (Приложение, Безопасность, Система и другие) на защищаемых узлах. По умолчанию отслеживаются изменения в журналах, указанных в политике. Вы можете просматривать и изменять список анализируемых журналов.

Чтобы изменить настройки отслеживания изменений в журналах ОС Windows:

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows**.
- 2 В разделе **Приложения и файлы** раскройте **Анализ журналов**.
- 3 Включите  **Анализ журналов событий Windows** и раскройте настройку. Будет отображен список отслеживаемых журналов.
- 4 Чтобы добавить новый журнал в список для отслеживания, нажмите **Добавить журнал**, введите название журнала или путь и название журнала и нажмите **Добавить**.
- 5 Чтобы изменить путь отслеживания журнала из списка отслеживания:
  - 5.1 Выберите журнал или предварительно воспользуйтесь поиском  по пути или названию журнала, справа от названия журнала выберите  > **Изменить**.
  - 5.2 Введите новый путь и название журнала, нажмите **Сохранить**.
- 6 Чтобы исключить журнал из списка отслеживания, выберите журнал и справа от названия журнала выберите  > **Удалить**. Подтвердите удаление.

Чтобы отключить отслеживание изменений в журналах событий Windows, выключите  **Анализ журналов событий Windows**.

## Анализ журналов приложений и служб

ViPNet EPP позволяет обнаруживать изменения в журналах приложений и служб на защищаемых узлах с ОС Windows и ОС GNU/Linux. По умолчанию отслеживаются изменения в журналах, указанных в политике. Вы можете просматривать и изменять период анализа журналов (только для узлов с ОС Windows) и список анализируемых журналов.

Настройки выполняются отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

В настройках для защищаемых узлов с ОС GNU/Linux, если анализ журналов приложений и служб отключен, также будут отключены мониторинг файлов и расчет контрольных сумм файлов.

Чтобы просмотреть и настроить параметры отслеживания изменений в журналах приложений и служб на защищаемых узлах с ОС Windows или ОС GNU/Linux:

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows** или **ОС Linux**.
- 2 Если выбрана вкладка **ОС Windows**, в разделе **Приложения и файлы** раскройте **Анализ журналов**.

- 3 Включите  **Анализ журналов приложений и служб** и раскройте настройку. Будет отображен список отслеживаемых журналов и служб.
- 4 Если выбрана вкладка **ОС Windows**, чтобы изменить период анализа журналов, в разделе **Общее** нажмите  и укажите значение из диапазона 60–120 секунд. Рекомендуемое значение — 60 секунд. При изменении этого параметра учитывайте, что чем меньше значение вы укажете, тем больше будет нагрузка на ViPNet EPP Сервер и ViPNet EPP Агент. Нажмите **Сохранить**.
- 5 Чтобы добавить новый журнал в список для отслеживания, в разделе **Журналы для анализа** нажмите **Добавить журнал**, введите путь к файлу с журналом и нажмите **Добавить**.
- 6 Чтобы изменить путь отслеживания журнала из списка отслеживания, в разделе **Журналы для анализа**:
  - 6.1 Выберите журнал или предварительно воспользуйтесь поиском  по пути к файлу журнала, справа от названия журнала выберите  > **Изменить**.
  - 6.2 Введите новый путь к файлу с журналом и нажмите **Сохранить**.
- 7 Чтобы исключить журнал из списка отслеживания, в разделе **Журналы для анализа** выберите журнал и справа от названия журнала выберите  > **Удалить**.

Чтобы отключить отслеживание изменений в журналах приложений и служб на вкладке **ОС Windows** или **ОС Linux**:

- 1 Выключите  **Анализ журналов приложений и служб**.
- 2 Если выбрана вкладка **ОС Linux** и были включены **Мониторинг файлов** или **Расчет контрольных сумм**, появится сообщение об их отключении. Подтвердите отключение, чтобы анализ журналов приложений и служб отключился.

### *Настройка декодера*

Для первичного анализа ряда изменений, происходящих на защищаемом узле, в ViPNet EPP используются декодеры. Декодер предварительно обрабатывает журналы перед их анализом правилами. Настройки декодера находятся в файле `decoder.xml`. Текст настроек соответствует синтаксису **OSSEC**. Вы можете просмотреть настройки и внести в них изменения.

Настройки выполняются отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows** или **ОС Linux**.
- 2 Если выбрана вкладка **ОС Windows**, в разделе **Приложения и файлы** раскройте **Анализ журналов**.
- 3 Если выбрана вкладка **ОС Linux**, в разделе **Приложения и файлы** раскройте **Анализ журналов приложений и служб**.
- 4 Раскройте **Декодер журналов**.
- 5 Чтобы внести изменения в настройки декодера:

- 5.1 Справа от файла `decoder.xml` выберите  > **Изменить**.
- 5.2 В поле **Регулярные выражения** внесите новые настройки или отредактируйте уже существующие строго в соответствии с синтаксисом OSSEC. Синтаксис и логика вносимых данных не проверяется.
- 5.3 Нажмите **Сохранить**.

### Настройка правил анализа

Для детального разбора информации от декодеров для идентификации событий, происходящих на защищаемом узле, в ViPNet EPP используются правила анализа.

По умолчанию используются правила анализа из политики, записанные в файлы:

- `EventRules.xml` — правила для защищаемых узлов с ОС Windows.
- `ids_rules.xml` — правила для защищаемых узлов с ОС GNU/Linux.

Текст правил соответствует синтаксису [OSSEC](#). Вы можете скачать файлы, чтобы просмотреть тексты правил и внести изменения.



**Примечание.** При редактировании и добавлении правил используйте идентификаторы правил строго в соответствии с диапазонами идентификаторов из таблицы [Типы и идентификаторы правил](#).

---

Отредактированные файлы вы сможете загрузить в политику вместо файлов по умолчанию, предварительно удалив их.

Настройки выполняются отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows** или **ОС Linux**.
- 2 Если выбрана вкладка **ОС Windows**, в разделе **Приложения и файлы** раскройте **Анализ журналов**.
- 3 Если выбрана вкладка **ОС Linux**, в разделе **Приложения и файлы** раскройте **Анализ журналов приложений и служб**.
- 4 Раскройте **Правила анализа журналов**.
- 5 Чтобы внести изменения в правила анализа:
  - 5.1 Справа от **Правила анализа журналов** выберите  > **Скачать**. Файл с правилами анализа (`EventRules.xml` или `ids_rules.xml`) будет сохранен на компьютер в папку **Загрузки**.
  - 5.2 Откройте файл с правилами в текстовом редакторе, внесите новые правила анализа или отредактируйте уже существующие строго в соответствии с синтаксисом OSSEC. Сохраните файл.
  - 5.3 Справа от **Правила анализа журналов** выберите  > **Удалить**. Подтвердите удаление.

- 5.4 Нажмите **Загрузить правила** и выберите сохраненный файл с правилами анализа. Новые правила анализа будут загружены в политику.

## Мониторинг файлов

ViPNet EPP позволяет обнаруживать изменения в файлах на защищаемых узлах с ОС Windows и ОС GNU/Linux. Отслеживаются процессы изменения, создания и удаления файлов по заданным путям. Вы можете изменять параметры отслеживания и список отслеживаемых путей.

Настройки выполняются отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

Чтобы отслеживание изменений в файлах работало на защищаемых узлах с ОС GNU/Linux, должен быть включен **Анализ журналов приложений и служб**.

Чтобы просмотреть и настроить параметры мониторинга файлов на защищаемых узлах с ОС Windows или ОС GNU/Linux:

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows** или **ОС Linux**.
- 2 В разделе **Приложения и файлы** включите  **Мониторинг файлов**.
- 3 Если выбрана вкладка **ОС Linux** и не был включен **Анализ журналов приложений и служб**, появится уведомление о необходимости включить анализ журналов приложений и служб. Нажмите **Включить**.
- 4 Раскройте **Мониторинг файлов**. Будет отображен список отслеживаемых путей к файлам и параметры отслеживания.
- 5 Чтобы добавить новое правило отслеживания, нажмите **Добавить путь**:
  - 5.1 В поле **Путь до файла** укажите путь отслеживания изменений файлов.
  - 5.2 Если нужно отслеживать все вложенные папки в случае их наличия, выберите **Рекурсия**.



**Примечание.** На защищаемых узлах с ОС GNU/Linux вложенные папки, созданные с помощью команды `mkdir -p`, отслеживаться не будут, если папки более высокого уровня не были созданы до запуска команды.

---

- 5.3 Укажите маску имени файла, по которой будет происходить поиск изменяемых файлов. Это необязательный параметр.

В пути до файла и в маске могут использоваться символы:

- ? — любой допустимый символ.
- \* — любой набор допустимых символов, в том числе пустой.



**Внимание!** Не рекомендуется задавать в качестве отслеживаемых папки, занимающие большую часть дискового пространства. Это может привести к замедлению работы компьютера.

---

5.4 Если по указанной маске нужно исключать отслеживание файлов, выберите **Исключать по маске**.

5.5 Выберите операции, которые нужно отслеживать: **Создание, Изменение, Удаление**.

5.6 Нажмите **Добавить**.

6 Чтобы изменить правило отслеживания файлов из списка:

6.1 Выберите строку с правилом или предварительно воспользуйтесь поиском , в конце строки выберите  > **Изменить**.

6.2 Измените параметры и нажмите **Сохранить**.

7 Чтобы удалить правило, выберите строку с правилом и в конце строки выберите  > **Удалить**. Подтвердите удаление.

Чтобы отключить отслеживание изменений файлов на вкладке **OC Windows** или **OC Linux**, выключите  **Мониторинг файлов**.

## Расчет контрольных сумм файлов

ViPNet EPP позволяет отслеживать на защищаемых узлах с ОС Windows и GNU/Linux создание новых файлов и вычислять их контрольные суммы по одному из алгоритмов: MD5, SHA256 или SpamSum. Вы можете включать и отключать работу правил, изменять параметры отслеживания и список отслеживаемых путей.

Настройки выполняются отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

Чтобы отслеживание изменений файлов и расчет контрольных сумм работали на защищаемых узлах с ОС GNU/Linux, должен быть включен **Анализ журналов приложений и служб**.

Чтобы просмотреть параметры, включить и настроить отслеживание создания новых файлов и вычисление их контрольных сумм на защищаемых узлах с ОС Windows или ОС GNU/Linux:

1 На странице **Обнаружение вторжений** выберите вкладку **OC Windows** или **OC Linux**.

2 В разделе **Приложения и файлы** включите  **Расчет контрольных сумм файлов**.

3 Если выбрана вкладка **OC Linux** и не был включен **Анализ журналов приложений и служб**, появится уведомление о необходимости включить анализ журналов приложений и служб. Нажмите **Включить**.

4 Раскройте **Расчет контрольных сумм файлов**. Будет отображен список отслеживаемых путей к файлам, исключений из отслеживания и алгоритмы расчета контрольных сумм (если они уже были настроены).

5 Чтобы добавить новое правило расчета контрольных сумм, нажмите **Добавить путь**:

5.1 Если выбрана вкладка **OC Windows**:

5.1.1 В поле **Путь до файла** укажите путь отслеживания создаваемых файлов.

5.1.2 В поле **Исключение** укажите название или путь и название файла, по которым файлы будут исключаться из списка для расчета контрольной суммы. Это необязательный параметр.

В пути до файла и в исключении могут использоваться символы:

- ? — любой допустимый символ.
- \* — любой набор допустимых символов, в том числе пустой.

5.2 Если выбрана вкладка **ОС Linux**:

5.2.1 В поле **Путь до файла** укажите путь отслеживания создаваемых файлов.

5.2.2 Если нужно отслеживать все вложенные папки в случае их наличия, выберите **Рекурсия**.



**Примечание.** На защищаемых узлах с ОС GNU/Linux вложенные папки, созданные с помощью команды `mkdir -p`, отслеживаться не будут, если папки более высокого уровня не были созданы до запуска команды.

---

5.2.3 Укажите маску имени файла, по которой будет происходить поиск создаваемых файлов. Это необязательный параметр.

В пути до файла и в маске могут использоваться символы:

- ? — любой допустимый символ.
- \* — любой набор допустимых символов, в том числе пустой.

Сверка на наличие новых папок, удовлетворяющих настроенным маскам, будет выполняться каждые 60 секунд.

5.2.4 Если по указанной маске нужно исключать отслеживание файлов, выберите **Исключать по маске**.

5.3 Выберите алгоритм вычисления контрольной суммы: **MD5, SHA256, SpamSum**.



**Примечание.** Для алгоритма SpamSum максимальный размер отслеживаемых файлов ограничен значением 100 Мбайт.

---

5.4 Нажмите **Добавить**.

6 Чтобы изменить правило расчета контрольных сумм из списка:

6.1 Выберите строку с правилом или предварительно воспользуйтесь поиском , в конце строки выберите  > **Изменить**.

6.2 Измените параметры и нажмите **Сохранить**.

7 Чтобы удалить правило, выберите строку с правилом и в конце строки выберите  > **Удалить**. Подтвердите удаление.

Чтобы отключить отслеживание создания новых файлов и вычисления их контрольных сумм на вкладке **OC Windows** или **OC Linux** выключите  **Расчет контрольных сумм файлов**.

## Обнаружение бесфайловых атак

ViPNet EPP позволяет обнаруживать бесфайловые атаки на защищаемых узлах с ОС Windows, выполняемых с помощью методов по классификации MITRE ATT&CK®. Вы можете включать и отключать работу правил, изменять период сканирования процессов на защищаемом узле.

После применения на защищаемом узле политики с настройками бесфайловых атак, чтобы изменения вступили в действие, необходимо перезагрузить защищаемый узел в случаях:

- Если вы включили хотя бы одно правило для бесфайловых атак в разделах **Обнаружение вторжений** или **Предотвращение вторжений**, а ранее все правила в этих разделах были отключены.
- Если вы отключили все правила обнаружения и предотвращения бесфайловых атак в этих разделах, а ранее хотя бы одно правило было включено.

В остальных случаях перезагрузка не требуется.

Чтобы просмотреть параметры, включить и настроить обнаружение бесфайловых атак:

- 1 На странице **Обнаружение вторжений** выберите вкладку **OC Windows**.
- 2 В разделе **Бесфайловые атаки**, RemSec включите  **Обнаружение бесфайловых атак**.
- 3 Чтобы настроить период сканирования ViPNet EPP Агент процессов на защищаемом узле, справа нажмите  :
  - 3.1 Укажите значение периода от 1 до 1440 минут. Рекомендуемое значение — 10 минут. Можно задать значение в минутах, секундах или часах.
  - 3.2 Чтобы в журнале событий не отображались информационные события сканирования процессов, в результате которого не были обнаружены потенциальные атаки, снимите флажок **Регистрировать событие сканирования в журнале**.
  - 3.3 Нажмите **Сохранить**.

При срабатывании правила обнаружения бесфайловых атак (только для событий **Обнаружение Keylogging**) вы можете настроить блокировку атаки с помощью правил предотвращения атак (HIPS).

Чтобы отключить отслеживание бесфайловых атак, на вкладке **OC Windows** выключите  **Обнаружение бесфайловых атак**.

## Обнаружение вредоносной активности RemSec

ViPNet EPP позволяет обнаруживать вредоносную активность RemSec на защищаемых узлах с ОС Windows. Вы можете включать и отключать отслеживание.

Чтобы включить обнаружение вредоносной активности RemSec:

- 1 На странице **Обнаружение вторжений** выберите вкладку **OC Windows**.
- 2 В разделе **Бесфайловые атаки, RemSec** включите  **Обнаружение вредоносной активности RemSec**.

Чтобы отключить отслеживание бесфайловых атак, на вкладке **OC Windows** выключите  **Обнаружение вредоносной активности RemSec**.

## Обнаружение сетевых атак

ViPNet EPP позволяет контролировать входящий и исходящий трафик защищаемого узла с ОС Windows и GNU/Linux и обнаруживать потенциально опасную сетевую активность с помощью правил обнаружения сетевых атак. В случае наличия аналогичного активного правила предотвращения сетевых атак, потенциально опасная сетевая активность будет обнаружена и заблокирована правилом предотвращения вторжений (HIPS).

Вы можете включать и отключать обнаружение сетевых атак, добавлять новые правила, изменять и удалять существующие.

Тексты правил обнаружения сетевых атак написаны в соответствии с синтаксисом [Suricata](#).



**Внимание!** При создании и изменении правил избегайте применения функций трансформации содержимого: `to_lowercase`, `to_uppercase`, `strip_whitespace`, `compress_whitespace`, `dotprefix`, `header_lowercase`, `strip_pseudo_headers`, `url_decode`, `xor`.

Настройки выполняются отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

Чтобы просмотреть правила, включить обнаружение и настроить правила обнаружения сетевых атак на защищаемых узлах с ОС Windows или ОС GNU/Linux:

- 1 На странице **Обнаружение вторжений** выберите вкладку **OC Windows** или **OC Linux**.
- 2 В разделе **Мониторинг сетевой активности** включите  **Обнаружение сетевых атак** и раскройте настройку. Будет отображен список правил обнаружения сетевых атак с указанием идентификаторов правил.
- 3 Чтобы добавить новые правила, нажмите **Добавить правила**:
  - 3.1 Внесите тексты новых правил строго в соответствии с синтаксисом Suricata. Вносите каждое правило с новой строки. Синтаксис и логика вносимых данных не проверяется.
  - 3.2 Укажите действие при совпадении идентификаторов:
    - **Не добавлять дубликаты правил** — при совпадении идентификаторов новое правило не будет добавлено в политику.

- **Перезаписать существующие правила** — при совпадении идентификаторов новое правило добавится в политику вместо существующего. Это действие установлено по умолчанию.

### 3.3 Нажмите **Добавить**.

4 Чтобы изменить существующее правило из списка:

4.1 Выберите правило или предварительно воспользуйтесь поиском  по названию или идентификатору правила, справа от названия правила выберите  > **Изменить**.

4.2 Внесите изменения в текст правила по аналогии с созданием правила и нажмите **Сохранить**.

5 Чтобы удалить правило из списка, выберите правило и справа от названия выберите  > **Удалить**. Чтобы удалить сразу несколько правил, выберите их флажками, нажмите  и подтвердите удаление.

Чтобы отключить отслеживание сетевой активности на защищаемом узле, на вкладке **OC Windows** или **OC Linux** выключите  **Обнаружение сетевых атак**.

## TLS-инспекция

ViPNet EPP с помощью функции TLS-инспекции позволяет расшифровывать HTTPS-трафик на защищаемых узлах с ОС Windows для возможности проверки его правилами предотвращения вторжений (HIPS), сетевыми правилами обнаружения вторжений и веб-фильтрами. Вы можете включать и отключать TLS-инспекцию.

По умолчанию TLS-инспекция выключена. Контролировать будет только HTTP-трафик.

Чтобы включить TLS-инспекцию:

- 1 На странице **Обнаружение вторжений** выберите вкладку **OC Windows**.
- 2 В разделе **Мониторинг сетевой активности** включите  **TLS-инспекция**.

## Команды мониторинга системы

В ViPNet EPP для отслеживания истории изменений состояния защищаемых узлов с ОС Windows можно настроить периодический запуск команд мониторинга и сравнения результатов.

Вы можете включать или выключать использование команд мониторинга, настраивать период запуска команд и уровень регистрируемых событий, настраивать команды мониторинга.

Таблица 3. Команды мониторинга состояния защищаемого узла, которые можно настроить

| Назначение команды                                                  | Команда                                                                                                                                                                     |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Получение общей сетевой информации по TCP-соединениям               | <code>netstat -nabop tcp</code>                                                                                                                                             |
| Получение сетевой информации по TCP-соединениям по слушающим портам | <code>netstat -nabop tcp   findstr LISTENING</code>                                                                                                                         |
| Получение общей сетевой информации по UDP-соединениям               | <code>netstat -nabop udp</code>                                                                                                                                             |
| Разрешение доменного имени                                          | <code>nslookup &lt;имя домена&gt; &lt;IP DNS-сервера&gt;</code> , где <IP DNS-сервера> — необязательный параметр, без него используется IP-адрес сервера по умолчанию       |
| Разрешение IP-адреса                                                | <code>nslookup -q=ptr &lt;IP&gt; &lt;IP DNS-сервера&gt;</code> , где <IP DNS-сервера> — необязательный параметр, без него используется IP-адрес сервера по умолчанию        |
| Получение списка почтовых серверов домена                           | <code>nslookup -q=mx &lt;имя домена&gt; &lt;IP DNS-сервера&gt;</code> , где <IP DNS-сервера> — необязательный параметр, без него используется IP-адрес сервера по умолчанию |
| Получение списка авторитетных DNS-серверов домена                   | <code>nslookup -q=ns &lt;имя домена&gt; &lt;IP DNS-сервера&gt;</code> , где <IP DNS-сервера> — необязательный параметр, без него используется IP-адрес сервера по умолчанию |
| Получение списка контроллеров домена Active Directory               | <code>nslookup -type=srv _ldap._tcp.&lt;имя домена&gt;   findstr "internet address"</code>                                                                                  |
| Список подключенных общих сетевых ресурсов                          | <code>net use</code>                                                                                                                                                        |
| Получение данных по общим ресурсам                                  | <code>wmic share</code>                                                                                                                                                     |
| Список дисковых устройств                                           | <code>wmic diskdrive get Model,Description,Status</code>                                                                                                                    |
| Список сетевых интерфейсов                                          | <code>wmic nic get Name,NetEnabled</code>                                                                                                                                   |
| Список установленного программного обеспечения                      | <code>wmic product get Name,Version,Vendor</code>                                                                                                                           |
| Список автозагрузки                                                 | <code>wmic startup get Name,Location,User</code>                                                                                                                            |
| Список драйверов                                                    | <code>driverquery</code>                                                                                                                                                    |
| Текущие пользовательские сессии                                     | <code>query session</code>                                                                                                                                                  |
| Проверка сетевого соединения                                        | <code>ping &lt;IP-адрес узла&gt;</code>                                                                                                                                     |
| Таблица маршрутизации IPv4                                          | <code>route print -4</code>                                                                                                                                                 |
| Таблица маршрутизации IPv6                                          | <code>route print -6</code>                                                                                                                                                 |
| Трассировка маршрута                                                | <code>tracert -d &lt;IP-адрес&gt;</code>                                                                                                                                    |

Чтобы включить использование команд мониторинга, добавить команды и настроить параметры:

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows**.
- 2 В разделе **Мониторинг системы** включите  **Команды мониторинга системы**.
- 3 Раскройте **Команды мониторинга системы**. Будут отображены настройки и список отслеживаемых команд (если уже задан).
- 4 Чтобы настроить параметры использования команд мониторинга, в разделе **Общее** нажмите  :
  - 4.1 Укажите значение периода запуска команд в диапазоне от 1 минуты до 31 дня.  
Рекомендуемое значение — 1 минута. Можно задать значение в минутах, секундах, часах или днях.
  - 4.2 Выберите уровень, который будет присваиваться событиям, регистрируемым в результате выполнения команд. Можно выбрать: **Информационное**, **Важное**, **Опасное**, **Критическое**.  
Значение по умолчанию — **Информационное**.
  - 4.3 Нажмите **Сохранить**.
- 5 Чтобы настроить команды, нажмите **Задать**:
  - 5.1 Введите команду из списка доступных команд, с помощью которой будет отслеживаться состояние защищаемых узлов.
  - 5.2 Чтобы предыдущий результат выполнения команды сравнивался с текущим и отображалась разница, включите **Сравнивать новый результат с предыдущим (дельта)**.
  - 5.3 Вы можете настроить сравнение результатов, содержащие только определенные данные. Для этого задайте маску: в поле **Маска для сравнения результатов** укажите критерии, по которым будут отфильтрованы результаты. Например, чтобы сравнивались результаты выполнения команды `ping 127.0.0.1`, имеющие период запуска 60 секунд, в поле **Маска для сравнения результатов** задайте величину этого периода — 60.
  - 5.4 Нажмите **Добавить**.

Чтобы отключить отслеживание состояния защищаемых узлов с помощью команд мониторинга, выключите  **Команды мониторинга системы**.

## Мониторинг установки ПО

ViPNet EPP позволяет отслеживать установку нового программного обеспечения на защищаемых узлах с ОС Windows. Вы можете включать или выключать мониторинг установки ПО, настраивать период мониторинга и уровень регистрируемых событий.

Чтобы включить и настроить мониторинг:

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows**.
- 2 В разделе **Мониторинг системы** включите  **Мониторинг установки ПО**.
- 3 Раскройте **Мониторинг установки ПО**. Просмотрите настройки.

4 Чтобы настроить параметры мониторинга нажмите  :

- 4.1 Укажите значение периода мониторинга в диапазоне от 100 секунд до 31 дня.  
Рекомендуемое значение — 10 минут. Можно задать значение в минутах, секундах, часах или днях.
- 4.2 Выберите уровень, который будет присваиваться событиям, регистрируемым в результате мониторинга при установке ПО. Можно выбрать: **Информационное**, **Важное**, **Опасное**, **Критическое**. Значение по умолчанию — **Информационное**.
- 4.3 Нажмите **Сохранить**.

Чтобы отключить отслеживание установки нового программного обеспечения, выключите  **Мониторинг установки ПО**.

## Мониторинг установки системных обновлений

ViPNet EPP позволяет отслеживать установку системных обновлений ОС Windows на защищаемых узлах. Вы можете включать или выключать мониторинг установки системных обновлений, настраивать период мониторинга, уровень регистрируемых событий и версии системных обновлений для мониторинга.

Чтобы включить и настроить мониторинг:

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows**.
- 2 В разделе **Мониторинг системы** включите  **Мониторинг установки системных обновлений**.
- 3 Раскройте **Мониторинг установки системных обновлений**. Просмотрите настройки.
- 4 Чтобы настроить параметры мониторинга и версии системных обновлений, нажмите  :
  - 4.1 Укажите значение периода мониторинга в диапазоне от 100 секунд до 31 дня.  
Рекомендуемое значение — 12 часов. Можно задать значение в минутах, секундах, часах или днях.
  - 4.2 Укажите версии системных обновлений Windows, установку которых нужно отслеживать.  
Например, KB2669970, KB4338825. После ввода каждого значения нажимайте Enter.
  - 4.3 Выберите уровень, который будет присваиваться событиям, регистрируемым в результате обнаружения отсутствия установки системных обновлений из списка. Можно выбрать: **Информационное**, **Важное**, **Опасное**, **Критическое**. Значение по умолчанию — **Критическое**.
  - 4.4 Нажмите **Сохранить**.

В результате при обнаружении отсутствия на защищаемом узле установленного системного обновления ОС Windows из заданного списка в журнале событий ViPNet EPP Агент будет регистрироваться событие, содержащее перечень отсутствующих обновлений.

Чтобы отключить отслеживание установки системных обновлений, выключите  **Мониторинг установки системных обновлений**.

## Аудит защищаемых узлов

ViPNet EPP позволяет настраивать политику аудита для защищаемых узлов с ОС Windows. Политика аудита определяет, какие типы событий ОС Windows должна записывать в журнал безопасности Windows на защищаемом узле.

Вы можете включать или выключать аудит защищаемых узлов, просматривать и настраивать политику аудита для различных категорий объектов ОС.



**Внимание!** При выключении аудита защищаемых узлов будут сброшены все настройки политик аудита для всех категорий объектов. После следующего включения аудита потребуются полная повторная настройка политик аудита.

Чтобы просмотреть и настроить политику аудита:

- 1 На странице **Обнаружение вторжений** выберите вкладку **ОС Windows**.
- 2 В разделе **Политика аудита** включите  **Аудит защищаемых узлов**.
- 3 Настройте политики, выбирая категории:



**Примечание.** Чем больше будет задано отслеживаемых папок, разделов реестра и чем больше вложенных отслеживаемых объектов в политике аудита, тем будет выше нагрузка на процессор при применении политики на защищаемом узле.

- **Аутентификация** — политика аудита аутентификации пользователей.
- **Управление учетными записями** — политика аудита управления учетными записями.
- **Реестр** — политика аудита изменений в реестре.
- **Файловая система** — политика аудита изменений в файловой системе.
- **Прочие типы событий** — политика аудита для отслеживания других типов событий.

## Политика аудита аутентификации пользователей

Чтобы настроить политику аудита для событий аутентификации пользователей в ОС Windows:

- 1 В разделе **Политика аудита** раскройте **Аутентификация**. Будут отображены настройки типов аудируемых событий (если заданы).
- 2 Справа от **Аутентификация** нажмите  и выберите, какие события аутентификации пользователей Windows должны отслеживаться на защищаемых узлах.

| Типы аудируемых событий              | Успех                               | Отказ                               |
|--------------------------------------|-------------------------------------|-------------------------------------|
| Проверка учетных данных              | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Вход в систему                       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Выход из системы                     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Другие события входа и выхода        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Служба проверки подлинности Kerberos | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Операции с билетами службы Kerberos  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Специальный вход                     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Сохранить Отмена

Рисунок 19. Настройка политик аудита для событий аутентификации пользователей

### 3 Нажмите Сохранить.

#### Политика аудита управления учетными записями

Аудит будет проводиться только при успешном достижении результата выполнения скрипта Powershell.

Чтобы настроить политику аудита для событий управления учетными записями в ОС Windows:

- 1 В разделе **Политика аудита** раскройте **Управление учетными записями**. Будут отображены настройки типов аудируемых событий (если заданы).
- 2 Справа от **Управление учетными записями** нажмите  и выберите, какие события управления учетными записями пользователей Windows должны отслеживаться на защищаемых узлах.

Аудит проводится только при успешном выполнении скрипта Powershell.

Типы аудируемых событий

- ☒ Управление группой безопасности
- ☒ Управление учетной записью компьютера
- ☒ Управление учетными записями

Сохранить Отмена

Рисунок 20. Настройка политик аудита управления учетными записями

3 Нажмите **Сохранить**.

### Политика аудита изменений в реестре

Чтобы настроить политику аудита для событий управления разделами реестра в ОС Windows:

- 1 В разделе **Политика аудита** раскройте **Реестр**. Будут отображены настройки типов аудируемых событий (если заданы).
- 2 Нажмите **Настроить** или **Добавить аудируемый путь** и укажите путь реестра и операции, которые будут отслеживаться на защищаемых узлах:

**Добавление аудируемого пути реестра**

\* Аудируемый путь реестра

HKEY\_LOCAL\_MACHINE\SOFTWARE

Раздел и подразделы

Исключения (каждый путь с новой строки)

\* Отслеживаемые операции

- ☒ Задание значения
- ☐ Запись DAC
- ☐ Запрос значения
- ☐ Перечисление подразделов
- ☐ Полный доступ
- ☐ Смена владельца
- ☒ Создание подразделов
- ☐ Создание связи
- ☐ Уведомление
- ☒ Удаление
- ☐ Чтение разрешений

Добавить Отмена

Рисунок 21. Настройка политик аудита для отслеживания изменений в реестре

2.1 Укажите путь к разделу реестра для аудирования.



**Примечание.** Если требуется отслеживать подразделы в `HKEY_CURRENT_USER`, вместо `HKEY_CURRENT_USER` указывайте `HKEY_USERS\<идентификатор конкретного пользователя>`. Например, вместо `HKEY_CURRENT_USER\Console` может быть указано `HKEY_USERS\S-1-5-19\Console`

- 2.2 В списке выберите область применения политики (к разделам и подразделам, только разделам или только подразделам).
  - 2.3 Укажите исключения — пути к подразделам реестра из раздела, указанного на шаге 2.1, для которых политика применяться не будет. После ввода каждого пути нажимайте Enter.
  - 2.4 Выберите операции с разделом реестра, которые будут отслеживаться.
  - 2.5 Нажмите **Добавить**.
- 3 Повторите шаг 2, 2.1-2.5 для добавления всех необходимых аудируемых путей.

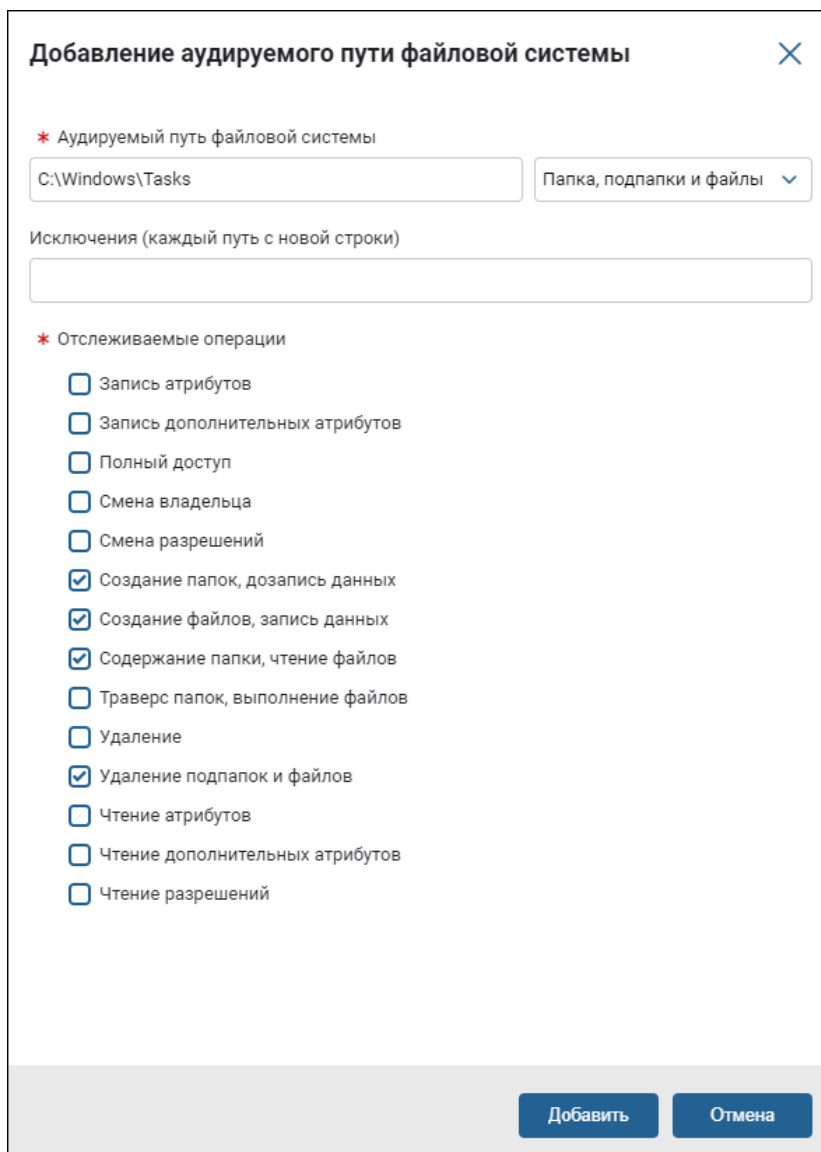
Чтобы изменить или удалить добавленные аудируемые пути:

- 1 Выберите аудируемый путь или предварительно воспользуйтесь поиском .
- 2 Справа от названия аудируемого пути выберите  > **Изменить** или  > **Удалить**.
- 3 Внесите изменения или подтвердите удаление.

#### *Политика аудита изменений в файловой системе*

Чтобы настроить политику аудита для событий управления объектами файловой системы в ОС Windows — файлов и папок:

- 1 В разделе **Политика аудита** раскройте **Файловая система**. Будут отображены настройки типов аудируемых событий (если заданы).
- 2 Нажмите **Настроить** или **Добавить аудируемый путь** и укажите, какой путь к файлам и события управления реестром должны отслеживаться на защищаемых узлах:



**Добавление аудируемого пути файловой системы**

\* Аудируемый путь файловой системы

C:\Windows\Tasks Папка, подпапки и файлы

Исключения (каждый путь с новой строки)

\* Отслеживаемые операции

- ☐ Запись атрибутов
- ☐ Запись дополнительных атрибутов
- ☐ Полный доступ
- ☐ Смена владельца
- ☐ Смена разрешений
- ☒ Создание папок, дозапись данных
- ☒ Создание файлов, запись данных
- ☒ Содержание папки, чтение файлов
- ☐ Траверс папок, выполнение файлов
- ☐ Удаление
- ☒ Удаление подпапок и файлов
- ☐ Чтение атрибутов
- ☐ Чтение дополнительных атрибутов
- ☐ Чтение разрешений

Добавить Отмена

Рисунок 22. Настройка политик аудита для отслеживания изменений в файловой системе

- 2.1 Укажите путь к папке для аудирования.
  - 2.2 В списке выберите область применения политики (к папкам, подпапкам и файлам, к папкам и файлам в ней).
  - 2.3 Укажите исключения — подпапки папки, указанной на шаге 2.1, для которых политика применяться не будет. После ввода каждой подпапки нажимайте Enter.
  - 2.4 Выберите операции с файловой системой, которые будут отслеживаться.
  - 2.5 Нажмите **Добавить**.
- 3 Повторите шаг 2 для добавления всех необходимых аудируемых путей.

Чтобы изменить или удалить добавленные аудируемые пути:

- 1 Выберите аудируемый путь или предварительно воспользуйтесь поиском ,

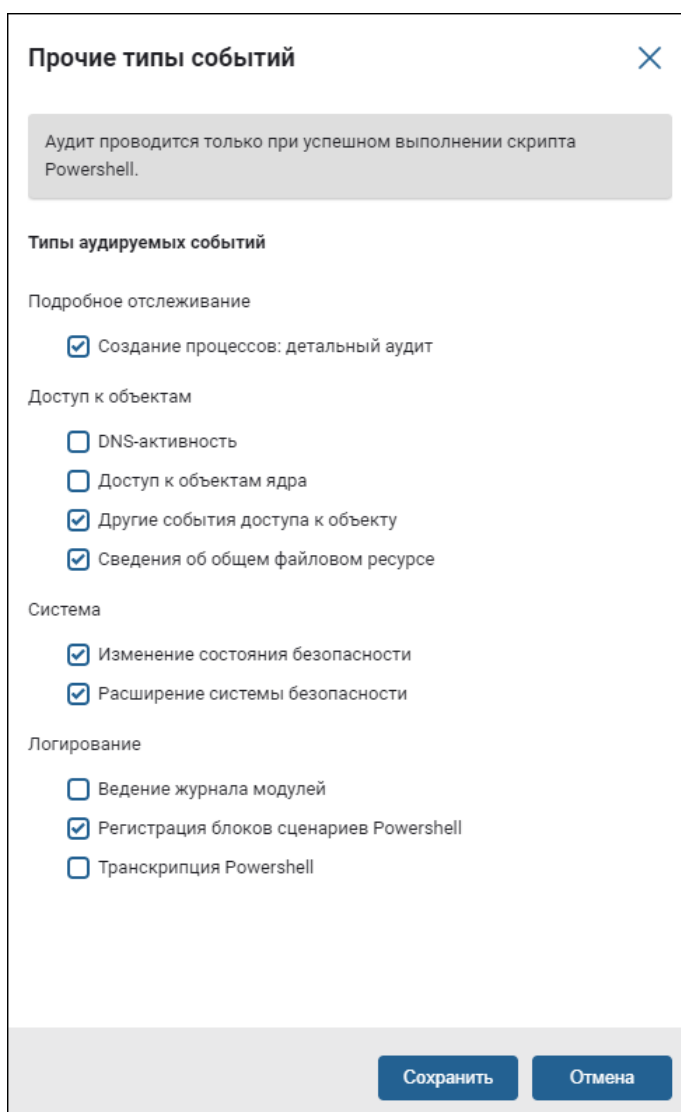
- 2 Справа от названия аудируемого пути выберите  > **Изменить** или  > **Удалить**.
- 3 Внесите изменения или подтвердите удаление.

### *Другие события аудита*

Аудит будет проводиться только при успешном достижении результата выполнения скрипта Powershell.

Чтобы настроить политику аудита для прочих событий управления объектами в ОС Windows:

- 1 В разделе **Политика аудита** раскройте **Прочие типы событий**. Будет отображен список аудируемых событий (если заданы).
- 2 Справа от **Прочие типы событий** нажмите  и выберите аудируемые события разных типов, которые будут отслеживаться на защищаемых узлах.



**Прочие типы событий**

Аудит проводится только при успешном выполнении скрипта Powershell.

**Типы аудируемых событий**

Подробное отслеживание

- ☒ Создание процессов: детальный аудит

Доступ к объектам

- ☐ DNS-активность
- ☐ Доступ к объектам ядра
- ☒ Другие события доступа к объекту
- ☒ Сведения об общем файловом ресурсе

Система

- ☒ Изменение состояния безопасности
- ☒ Расширение системы безопасности

Логирование

- ☐ Ведение журнала модулей
- ☒ Регистрация блоков сценариев Powershell
- ☐ Транскрипция Powershell

**Сохранить** **Отмена**

Рисунок 23. Настройка дополнительных политик аудита

- 3 Нажмите **Сохранить**.

## Правила предотвращения вторжений

Правила предотвращения вторжений (см. [Обнаружение и предотвращение вторжений](#)) позволяют настроить:

- Блокирование сетевой активности.
- Блокирование бесфайловых атак (см. [Предотвращение бесфайловых атак](#)) (только на защищаемых узлах с ОС Windows):
- Блокирование доступа к вредоносным-веб ресурсам (см. [Настройка веб-фильтров](#)) (только на защищаемых узлах с ОС Windows).

### Настройка сетевых правил

В политике безопасности содержатся предустановленные [сетевые правила](#) для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux, а также для каждого из режимов работы модуля предотвращения вторжений: усиленного, оптимального и минимального. Вы можете просматривать и настраивать сетевые правила. Для каждого из режимов вы можете настроить свой набор правил.

Для настройки сетевых правил доступны:

- Создание правил.
- Изменение параметров уже созданных правил.
- Удаление правил.

Сетевые правила написаны в соответствии с синтаксисом [Suricata](#). Вы можете создать новые правила или изменить уже существующие путем написания или редактирования текста правил.

При написании правил учитывайте, что в ViPNet EPP Агент применяются сетевые правила только с действиями правил:

- `drop` ( **Блокировать**) — IP-пакет блокируется сетевым фильтром межсетевого экрана ViPNet EPP Агент.
- `alert` ( **Уведомлять**) — срабатывание сетевого правила регистрируется в журнале ViPNet EPP Агент.



**Внимание!** При создании и изменении правил избегайте применения функций трансформации содержимого: `to_lowercase`, `to_uppercase`, `strip_whitespace`, `compress_whitespace`, `dotprefix`, `header_lowercase`, `strip_pseudo_headers`, `url_decode`, `xor`.

---

## Общий порядок просмотра и управления сетевыми правилами

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Предотвращение вторжений > Сетевые правила**.
- 2 На панели сверху выберите операционную систему защищаемых узлов, для которых вы хотите просмотреть правила:
  -  — защищаемые узлы с ОС Windows.
  -  — защищаемые узлы с ОС GNU/Linux.
- 3 На панели сверху выберите один из режимов предотвращения вторжений — **Усиленный**, **Оптимальный** или **Минимальный**. Отобразится список сетевых правил, настроенных для выбранного режима.

Для каждого правила в списке отображаются параметры:

  - ОС — значок операционной системы защищаемых узлов, в которой работает правило.
  - Идентификатор — идентификатор правила из диапазона сетевых правил (см. [Типы и идентификаторы правил](#)).
  - Название правила.
  - Протокол, адрес и порт источника, направление, адрес и порт назначения — параметры трафика для определения источника и направления атаки. Направление трафика:
    -  — от источника к назначению;
    -  — двунаправленный.
  - Действие — действие правила:  **Блокировать** или  **Уведомлять**.
  - Режим — в каких режимах применяется правило.
- 4 Чтобы просмотреть подробные сведения о правиле, выберите его в списке или предварительно на панели сверху воспользуйтесь поиском  по идентификатору и названию. Просмотрите параметры и текст правила на панели справа.
- 5 Внесите изменения в соответствии с описанием ниже.
- 6 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Создание сетевого правила

- 1 На вкладке **Сетевые правила** на панели сверху нажмите **Добавить правила >** операционная система, в которой будет действовать правило (**Для ОС Windows** или **Для ОС Linux**).
- 2 Выберите режимы, в которых будут применяться правила.
- 3 Выберите действия, при совпадении идентификаторов правил (SID):

- **Не добавлять дубликаты правил** — если идентификаторы новых правил совпадают с существующими правилами, новые правила не будут добавлены.
  - **Перезаписать существующие правила** — при совпадении идентификаторов новых правил с существующими правилами новые правила будут добавлены вместо существующих. Это значение установлено по умолчанию.
- 4 Введите текст правил строго в соответствии с синтаксисом Suricata. Логика и текст правил не проверяется. Текст правил может содержать не более 70000 символов.
  - 5 Нажмите **Добавить**.

### Изменение параметров уже созданных правил

- 1 На вкладке **Сетевые правила** на панели сверху выберите операционную систему и режим.
- 2 В списке правил выберите правило.
- 3 На панели справа сверху нажмите  и внесите необходимые изменения аналогично добавлению правил (см. выше).
- 4 Нажмите **Сохранить**.

### Удаление правил

- 1 На вкладке **Сетевые правила** на панели сверху выберите операционную систему и режим.
- 2 В списке правил выберите флажками правила.
- 3 На панели сверху нажмите .
- 4 Подтвердите удаление.

### Настройка веб-фильтров

Веб-фильтры применяются только на защищаемых узлах с ОС Windows. Подробнее о принципе работы веб-фильтров см. в документе «ViPNet EPP for Windows. Руководство администратора» в разделе «Блокировка доступа к вредоносным веб-ресурсам». Политика безопасности содержит предустановленные веб-фильтры.

Для настройки веб-фильтров доступно:

- Создание веб-фильтров.
- Изменение ранее созданных веб-фильтров, включая предустановленные, кроме фильтра **Прочие сайты**.
- Изменение порядка применения веб-фильтров.
- Удаление веб-фильтров.

Адреса контролируемых веб-ресурсов задаются в виде IP-адресов, доменных имен и URL-адресов и загружаются в веб-фильтры в текстовых файлах формата CSV. Для каждого вида адресов используется отдельный файл.

Перед созданием или изменением веб-фильтров подготовьте CSV-файлы с адресами веб-ресурсов. Вы можете скачать CSV-файлы из ранее созданных веб-фильтров, чтобы просмотреть и внести изменения, или создать новые CSV-файлы. При подготовке CSV-файлов соблюдайте требования:

- Для адресов каждого вида необходимо подготовить отдельный файл.
- Каждый адрес в файле задавайте с новой строки.
- Адреса не должны дублироваться.
- Требования к формату для каждого вида адреса:
  - IP-адреса, только в формате IPv4, например `98.144.73.193`. Использовать маски нельзя.
  - Доменные имена, например `ach2.xyz`. При задании доменных имен вы можете использовать маски:
    - `\*` — любая последовательность символов;
    - `\?` — любой один символ.

При задании маски `\*` в начале доменного имени, например `\*ach2.xyz`, в блокирующем веб-фильтре будут блокироваться все поддомены `ach2.xyz`: `test.ach2.xyz`, `test1.test.ach2.xyz` и так далее.



**Внимание!** Использование масок в конце доменного имени в зависимости от действия веб-фильтра приведет к блокировке или разрешению всех веб-ресурсов.

---

- URL-адреса, например `http://wasjar.dynu.net`. При задании URL-адресов:
  - В качестве хоста можно использовать доменное имя или IP-адрес в формате IPv4, например `http://198.144.73.193`.
  - Можно использовать те же маски, что и для доменных имен (`\*` и `\?`).
  - Если символы `*` и `?` входят в состав реального URL-адреса, не добавляйте `\`.



**Примечание.** Если в браузере защищаемого узла какой-либо веб-ресурс уже открывался (например, `www.vsport.com`), после добавления блокирующего веб-фильтра по неполному URL-адресу этого веб-ресурса (например, `vsport.com\`), при следующей попытке открыть этот ресурс доступ может остаться не заблокирован. Это связано с тем, что в браузере уже есть информация о реальном адресе веб-ресурса.

---

Подготовленные CSV-файлы вы сможете загрузить при создании нового фильтра или при изменении существующих вместо ранее добавленных файлов, предварительно удалив их.

## Общий порядок управления веб-фильтрами

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Предотвращение вторжений > Веб-фильтры (Windows)**.
- 2 Просмотрите текущий список веб-фильтров. Для каждого фильтра в списке отображаются:
  - № — порядковый номер фильтра. Все фильтры из списка применяются по порядку.
  - Состояние фильтра — включено или выключено.
  - Название фильтра.
  - Действие — разрешает  **Разрешить** или блокирует  **Блокировать** доступ к настроенным веб-адресам.
  - IP-адреса, Домены, URL-адреса — количество контролируемых фильтром веб-адресов каждого типа.
  - Регистрация события — значок  означает, что при срабатывании фильтра в журнале событий будут регистрироваться события. Если значка нет, события регистрироваться не будут.
  -  — наличие такого значка для фильтра означает, что фильтр был создан или изменен пользователем.
- 3 Чтобы просмотреть сведения о веб-фильтре или просмотреть файлы с адресами веб-ресурсов, загруженные в веб-фильтр:
  - 3.1 Выберите фильтр в списке или предварительно на панели вверху воспользуйтесь поиском  по названию фильтра.
  - 3.2 На панели справа посмотрите сведения о фильтре.
  - 3.3 Чтобы скачать файлы с адресами веб-ресурсов, вверху справа нажмите .
  - 3.4 В разделе **Веб-ресурсы** справа от названия каждого вида загруженных адресов веб-ресурсов нажмите .CSV-файлы с адресами будут сохранены на компьютер в папку **Загрузки**:
  - ips.csv с IP-адресами;
  - urls.csv с URL-адресами;
  - domains.csv с доменными именами.
- 4 Создайте, измените веб-фильтр, измените порядок применения фильтров, временно отключите или удалите ненужные фильтры в соответствии с описанием ниже.
- 5 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Создание веб-фильтра

- 1 На вкладке **Веб-фильтры (Windows)** на панели сверху нажмите **Создать фильтр**.
- 2 Выберите  **Фильтр включен**.
- 3 Введите название фильтра.
- 4 Выберите действие фильтра при срабатывании:  **Разрешать** доступ к веб-ресурсу или  **Блокировать** доступ к веб-ресурсу.
- 5 Чтобы при срабатывании фильтра в журнале событий регистрировались события, выберите **Регистрировать событие срабатывания фильтра в журнале**.
- 6 Чтобы добавить адреса веб-ресурсов из подготовленных файлов формата `csv`, в разделе **Веб-ресурсы** в меню **Загрузить из файла** выберите название типа веб-ресурсов (**IP-адреса**, **Доменные имена** или **URL-адреса**).
  - 6.1 Выберите подготовленный CSV-файл с веб-ресурсами выбранного типа.
  - 6.2 Нажмите **Загрузить**. Дубликаты и не соответствующие формату данные не будут загружены.
- 7 Загрузите все необходимые типы адресов веб-ресурсов в соответствии с шагом 6. Для каждого типа адресов веб-ресурсов вы можете загрузить только один файл.
- 8 Нажмите **Создать**.

## Изменение параметров веб-фильтров

- 1 На вкладке **Веб-фильтры (Windows)** в списке выберите фильтр.
- 2 На панели справа в разделе **Общее** вы можете изменить активность фильтра.
- 3 Чтобы внести изменения в другие параметры фильтра, сверху справа нажмите  и внесите необходимые изменения аналогично созданию фильтра (см. выше).
- 4 Чтобы внести изменения в адреса веб-ресурсов, ранее загруженных в фильтр, в разделе **Веб-ресурсы**:
  - 4.1 Скачайте CSV-файлы с адресами веб-ресурсов в соответствии с шагом 3 общего порядка управления (см. выше).
  - 4.2 В текстовом редакторе внесите изменения в файлы или создайте новые CSV-файлы строго в соответствии с требованиями к формату (см. выше).
  - 4.3 Удалите загруженные файлы с адресами веб-ресурсов, которые нужно изменить. Для этого справа от названия вида загруженных адресов веб-ресурсов нажмите .
  - 4.4 Загрузите подготовленные на шаге 2 CSV-файлы, выполнив действия из шага 6-7 сценария создания веб-фильтра.
- 5 Нажмите **Сохранить**.

## Изменение порядка применения веб-фильтров

Веб-фильтры применяются в списке последовательно, сверху вниз в соответствии с нумерацией, до первого срабатывания. Чтобы изменить порядок применения:

- 1 В списке веб-фильтров выберите флажками фильтры, порядок применения которых необходимо изменить.
- 2 На панели сверху нажмите  или  для перемещения выбранных фильтров в списке.

## Удаление веб-фильтров

- 1 В списке веб-фильтров выберите флажками фильтры, которые необходимо удалить.
- 2 На панели сверху нажмите  **Удалить** и подтвердите удаление.

## Предотвращение бесфайловых атак

ViPNet EPP позволяет предотвращать следующие виды бесфайловых атак на защищаемых узлах с ОС Windows:

- Атак с целью получения адресов функций в модулях ядра ОС Windows.
- Атаки типа Hollowing и Doppelganging.
- Атаки типа Keylogging, выявленные правилами обнаружения для бесфайловых атак (см. [Обнаружение бесфайловых атак](#)).

Подробнее о принципе работы предотвращения бесфайловых атак см. в документе «ViPNet EPP for Windows. Руководство администратора» в разделе «Обнаружение и предотвращение бесфайловых атак».

Вы можете включать и отключать предотвращение бесфайловых атак типа Hollowing и Doppelganging и атак с целью получения адресов функций в модулях ядра ОС Windows.

Для предотвращения бесфайловых атак, относящиеся к методу Keylogging, проводимые злоумышленником с помощью вызова функции ОС Windows `SetWindowsHookEx`, вы можете настраивать правила реагирования на хуки (hook).

После применения на защищаемом узле политики с настройками бесфайловых атак, чтобы изменения вступили в действие, необходимо перезагрузить защищаемый узел в случаях:

- Если вы включили хотя бы одно правило для бесфайловых атак в разделах **Обнаружение вторжений** или **Предотвращение вторжений**, а ранее все правила в этих разделах были отключены.
- Если вы отключили все правила обнаружения и предотвращения бесфайловых атак в этих разделах, а ранее хотя бы одно правило было включено.

В остальных случаях перезагрузка не требуется.

Чтобы настроить правила предотвращения бесфайловых атак:

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Предотвращение вторжений > Бесфайловые атаки (Windows)**.
- 2 Чтобы включить правила предотвращения бесфайловых атак, относящиеся к методам Process Hollowing и Process Doppelganging, включите  **Предотвращение атак типа Hollowing и Doppelganging**.
- 3 Чтобы включить правила обнаружения и блокирования бесфайловых атак, связанных с получением адресов функций в модулях ядра Windows, включите  **Предотвращение получения адресов функций в модулях ядра Windows**.
- 4 Чтобы создать правило реагирования на хуки, в одноименном разделе нажмите **Создать правило**.
- 5 Выберите  **Правило включено**.
- 6 Введите название правила.
- 7 Выберите тип отслеживаемых хуков:
  - **Клавиатура** — контроль сообщений от клавиатуры.
  - **Мышь** — контроль сообщений от мыши.
  - **Окна** — контроль событий от окон.
  - **Прочее** — контроль прочих системных сообщений.
- 8 Определите действие правила:
  -  **Блокировать** — при срабатывании правила атака будет заблокирована.
  -  **Разрешать** — при срабатывании правила блокировки не будет.
- 9 Укажите путь к отслеживаемому процессу. По умолчанию поле пустое. Вы можете указать маску для отслеживания нескольких процессов (см. [Особенности задания и использования правил доступа](#)) или полный путь к определенному процессу. Например, маска `C:\Windows\System32\*.exe` или полный путь `C:\Windows\explorer.exe`. Для указания любого процесса введите символ `*`.
- 10 Укажите путь к отслеживаемому модулю, который может быть внедрен в процесс. По умолчанию установлен символ `*`, что означает отслеживание любых внедренных модулей. Аналогично процессам вы можете указать маску для отслеживания нескольких модулей (см. [Особенности задания и использования правил доступа](#)) или полный путь к определенному модулю.
- 11 Чтобы события фиксировались в журнале событий, выберите **Регистрировать событие срабатывания правила в журнале**.
- 12 Нажмите **Создать**.
- 13 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Изменение параметров правил реагирования на хуки

- 1 В списке правил реагирования на хуки выберите правило.
- 2 На панели справа вы можете изменить активность правила.
- 3 Чтобы внести изменения в другие параметры фильтра, вверху справа нажмите  и внесите необходимые изменения аналогично созданию правила (см. выше).
- 4 Нажмите **Сохранить**.

## Изменение порядка применения правил реагирования на хуки

Правила применяются в списке последовательно, сверху вниз в соответствии с нумерацией, до первого срабатывания. Чтобы изменить порядок применения:

- 1 В списке правил реагирования на хуки выберите флажками правила, порядок применения которых необходимо изменить.
- 2 На панели вверху нажмите  или  для перемещения выбранных правил в списке.

## Удаление правил реагирования на хуки

- 1 В списке правил реагирования на хуки выберите флажками правила, которые необходимо удалить.
- 2 На панели вверху нажмите  **Удалить** и подтвердите удаление.

## Правила ZTNA

Выполнение правил политики ZTNA (см. [Сетевой доступ с нулевым доверием \(ZTNA\)](#)) будет отслеживаться на всех защищаемых узлах, если включен модуль ZTNA. Если на защищаемом узле установлена программа ViPNet Client 5 и включен модуль **Межсетевой экран** (см. [Режимы модулей защиты](#)), будет также контролироваться доступ к ресурсам защищенной [сети ViPNet](#). По умолчанию модуль ZTNA выключен. Для использования правил ZTNA включите модуль **ZTNA** (см. [Режимы модулей защиты](#)).

Правила ZTNA действуют в пределах одной политики. По умолчанию политика уже содержит ряд правил для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

Для управления правилами ZTNA доступны:

- Добавление и настройка новых правил.
- Настройка правил для антивирусов, периода проверки наличия обновления базы антивируса.
- Изменение параметров уже добавленных правил, включение и отключение правил.
- Удаление правил. Правила для антивирусов удалить нельзя.

## Общий порядок просмотра и управления правилами ZTNA

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **ZTNA**.
- 2 На панели сверху выберите операционную систему защищаемых узлов, для которых вы хотите просмотреть правила:
  -  — защищаемые узлы с ОС Windows.
  -  — защищаемые узлы с ОС GNU/Linux.

Для каждого правила в списке отображаются параметры:

- **ОС** — значок операционной системы защищаемых узлов, в которой работает правило.
  - **Состояние** — включено или отключено правило.
  - **Правило** — название правила.
  - **Действие** — действие правила:  **Пропускать**.
  - **Типы условий** — список условий, которые настроены в правиле и будут проверяться на защищаемом узле.
  -  — наличие такого значка для правила означает, что правило было создано или изменено пользователем.
- 3 Чтобы просмотреть подробные сведения о правиле, выберите его в списке или предварительно на панели сверху воспользуйтесь поиском  по названию. Просмотрите сведения параметры и условия срабатывания правила на панели справа.
  - 4 Внесите необходимые изменения в соответствии со сценариями ниже или добавьте и настройте новые правила ZTNA.
  - 5 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Настройка правил для антивирусов

- 1 Выберите одно из правил **Наличие работающего антивируса Kaspersky Antivirus** или **Наличие работающего антивируса Dr.Web Antivirus** и на панели справа включите его  **Правило включено**. Можно включить только одно из правил для каждой ОС.
- 2 На панели справа сверху нажмите . Проверьте условия срабатывания правила.
- 3 При необходимости измените название правила.

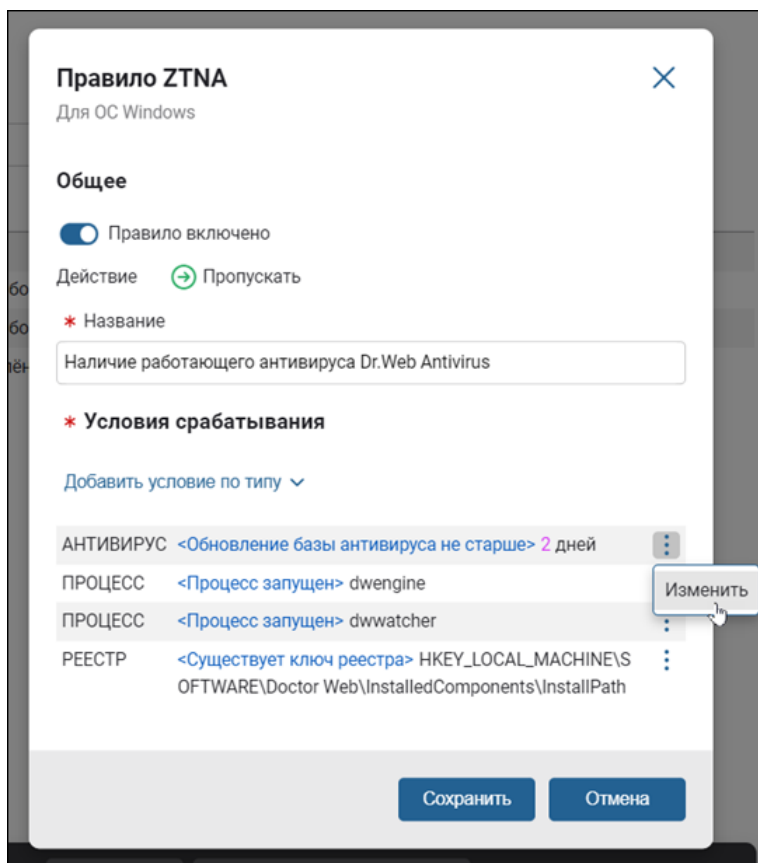


Рисунок 24. Настройка правила ZTNA для антивируса

- 4 Чтобы изменить условие срабатывания **Антивирус** и настроить период проверки наличия обновления базы антивируса на защищаемых узлах, справа от условия выберите > **Изменить**.
- 5 Укажите период времени в днях, через который нужно проверять актуальность базы антивируса. Может принимать значение из диапазона 1–30. По умолчанию установлен период 2 дня.
- 6 Нажмите **Добавить**.
- 7 Чтобы изменить другие условия срабатывания правила для антивируса, справа от условия выберите > **Изменить**, и настройте параметры аналогично описанию в сценарии добавления и настройки правил.
- 8 Чтобы удалить условия срабатывания правила для антивируса, справа от условия выберите > **Удалить**. Условие **Антивирус** удалить нельзя.
- 9 Чтобы добавить новые условия срабатывания правила, в списке **Добавить условия по типу** выберите тип условия и настройте параметры аналогично описанию в сценарии добавления и настройки правил. Нажмите **Добавить**.
- 10 Нажмите **Сохранить**.

## Изменение параметров ранее добавленных правил

- 1 Чтобы изменить активность правила, выберите правило и на панели справа включите  **Правило включено** или выключите  **Правило отключено**. Чтобы включить или выключить сразу несколько правил, выберите их флажками и на панели сверху нажмите **Включить** или **Отключить**.
- 2 Чтобы изменить параметры выбранного правила, на панели справа сверху нажмите  . Проверьте условия срабатывания правила.
- 3 Измените название.
- 4 Чтобы изменить добавленные условия срабатывания правила, справа от условия выберите  > **Изменить**, и настройте параметры аналогично описанию в сценарии добавления и настройки правил.
- 5 Чтобы удалить условия срабатывания правила, справа от условия выберите  > **Удалить**.
- 6 Чтобы добавить новые условия срабатывания правила, в списке **Добавить условия по типу** выберите тип условия и настройте параметры аналогично описанию в сценарии добавления и настройки правил. Нажмите **Добавить**.
- 7 Нажмите **Сохранить**.

## Удаление ранее добавленных правил

Выберите правило в списке, на панели справа сверху нажмите  и подтвердите удаление. Чтобы удалить сразу несколько правил, выберите их флажками и на панели сверху нажмите .

## Создание и настройка правил

- 1 Чтобы добавить новое правило, на странице **ZTNA** нажмите **Создать правило** > **ОС**, в которой будет действовать правило (**Для ОС Windows** или **Для ОС Linux**).
- 2 Убедитесь, что  **Правило включено**.
- 3 Введите название правила.
- 4 Чтобы настроить условия срабатывания правила, в списке **Добавить условия по типу** выберите тип условия и настройте параметры:
  - 4.1 При настройке для защищаемых узлов с ОС Windows:
    - При выборе **Программное обеспечение** введите название программного обеспечения и выберите условие срабатывания правила: указанное ПО должно быть на защищаемом узле **Установлено** или **Не установлено**. Название ПО должно совпадать с названием в **Программы и компоненты Windows**.
    - При выборе **Процесс** введите имя процесса и выберите условие срабатывания правила: указанный процесс должен быть на защищаемом узле **Запущен** или **Не**

запущен. Имя процесса должно совпадать с именем в **Диспетчер задач > Подробности**, но указывается без расширения.

- При выборе **Реестр** введите путь к ключу или параметру реестра и задайте условие срабатывания правила. Путь должен содержать не более 256 символов. Можно использовать полное и сокращенное название ключей корневого уровня реестра, например, `HKLM\SOFTWARE\test\paramtest`, за исключением `HKKEY_CURRENT_USER` (`HKCU`). Вместо `HKKEY_CURRENT_USER` (`HKCU`) следует указывать `HKKEY_USERS` (или `HKU`) и идентификатор конкретного пользователя. При задании условий соблюдайте правила:
  - **Существует или Не существует.** Условия можно задавать для любых типов значений реестра. В этом случае путь должен быть указан до параметра реестра.
  - **Равно или Не равно.** Условия можно задавать только для целочисленных и строковых значений параметров реестра. В этом случае путь должен быть указан до параметра реестра. После выбора условия укажите значение для сравнения в десятичной системе счисления.
  - **Содержит или Не содержит.** Условия можно задавать только для строковых значений параметров реестра. В этом случае путь должен быть указан до параметра реестра. После выбора условия укажите значение для сравнения.
  - **Меньше, Больше, Меньше или равно, Больше или равно.** Условия можно задавать для целочисленных значений параметров реестра. В этом случае путь должен быть указан до параметра реестра. После выбора условия укажите значение для сравнения в десятичной системе счисления.
- При выборе **Служба** введите имя службы и выберите условие срабатывания правила: указанная служба на защищаемом узле **Выполняется** или **Не выполняется**. Имя службы должно совпадать с именем в **Службы** (`services.msc`).
- При выборе **Файлы** введите полный путь к файлу, например, `C:\Program Files\Test\test.exe`. Допускается также указание сетевого пути к файлу, например `\\Server\Test\test.exe`. Путь должен содержать не более 1000 символов.

Выберите условие срабатывания правила: указанный файл на защищаемом узле **Существует** или **Не существует**.

#### 4.2 При настройке для защищаемых узлов с ОС GNU/Linux:

- При выборе **Версия ядра** укажите условие срабатывания правила (**Равно, Не равно, Меньше, Больше, Меньше или равно, Больше или равно**) и введите версию ядра для сравнения в формате `A.B.C`, например `1.4.8`. Версии ядра сравниваются только по первым трем цифрам номера.
- При выборе **Модуль ядра** введите имя модуля ядра и выберите условие срабатывания правила: указанный модуль ядра на защищаемом узле **Загружен** или **Не загружен**. Список всех модулей для текущего ядра можно посмотреть, выполнив команду:

```
find /lib/modules/$(uname -r) -name <имя>.ko
```

Просмотр загруженных модулей:

```
lsmod
```

- При выборе **Служба systemd** введите имя службы `systemd` и выберите условие срабатывания правила: указанная служба на защищаемом узле **Выполняется** или **Не выполняется**.

Список всех служб можно посмотреть, выполнив команду:

```
systemctl list-units --type=service
```

Имя службы нужно указывать в формате `name.service`, как оно отображается в списке всех служб.

- При выборе **Файлы** введите путь к файлу, например `/home/user/test.txt`. Путь должен содержать не более 1000 символов. Выберите условие срабатывания правила: указанный файл на защищаемом узле **Существует** или **Не существует**.

5 Нажмите **Добавить**.

6 Добавьте все необходимые условия срабатывания правила в соответствии с шагами 4-5.

Все созданные условия добавятся в раздел **Условия срабатывания**.

7 Нажмите **Сохранить**.

## Правила контроля приложений

Правила контроля приложений применяются только на защищаемых узлах с ОС Windows.

Подробнее о принципе работы контроля приложений см. в документе «ViPNet EPP for Windows. Руководство администратора» в разделе «Контроль приложений».

Чтобы настроить правило контроля приложения:

- 1 Добавьте приложение в политику и настройте для него правило запуска (см. [Правила запуска приложений](#)).
- 2 Определите активность приложения правилами доступа к системе для этого приложения (см. [Правила доступа приложений](#)) или используйте [правила доступа по умолчанию](#).

Вы можете добавлять приложения в один из списков доверия:

- **Доверенные** (белый список) — приложению из этого списка разрешен запуск в любом режиме работы модуля **Контроль приложений**, если правило разрешения запуска приложения включено (применяется). Если правило запуска не применяется, запуск приложения будет разрешен только в режиме **Разрешать неизвестные**. Приложения списка распределяются по группам. По умолчанию список содержит группы:
  - **Доверенные** — предустановленная системная группа. Активность приложений из этой группы не ограничена правилами доступа. Приложениям разрешено взаимодействие с объектами ОС Windows. Изменение правил доступа и удаление этой группы недоступно.
  - **Слабое доверие** и **Частичное доверие** — предустановленные пользовательские группы. Активность приложений из этих групп определяется правилами доступа к системе. Правила доступа можно изменять. Группы можно удалять.

Вы можете создать другие пользовательские доверенные группы, добавить в них приложения и настроить правила доступа.

- **Запрещенные** (черный список) — приложению из этого списка запрещен запуск в любом режиме работы модуля **Контроль приложений**, если правило блокировки запуска приложения включено (применяется). Если правило запуска не применяется, запуск приложения будет запрещен только в режиме **Запрещать неизвестные**. В этом списке группы не используются.

Для правил запуска и правил доступа вы можете настроить регистрации событий в журнале событий при срабатывании правила.

Правила контроля приложений применяются последовательно, сверху вниз в соответствии с нумерацией. Вы можете перемещать приложения между списками и группами, изменять порядок применения правил для групп и правил в группах, а также изменять порядок применения правил доступа для каждого приложения.

## Общий порядок управления правилами контроля приложений

- 1 На странице настройки политики (см. [Порядок настройки политики](#)) выберите  **Контроль приложений**.
- 2 На панели вверху выберите список доверия — **Доверенные** или **Запрещенные**.
- 3 Просмотрите текущий список групп и приложений. Для просмотра приложений в списке **Доверенные** раскройте группы приложений.

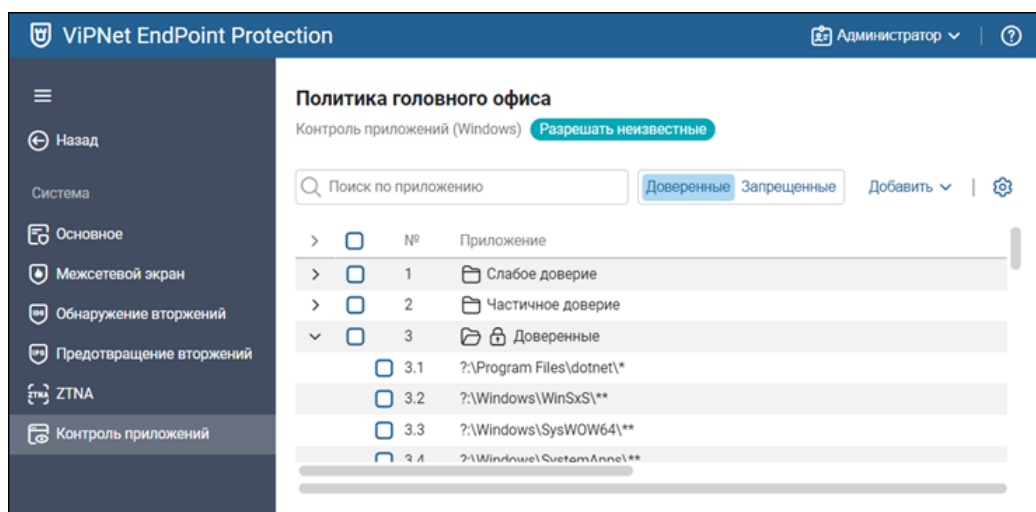


Рисунок 25. Просмотр списка контроля приложений

Для каждой группы и приложения в списке отображаются параметры:

- **№** — порядковый номер применения правил группы приложения и правил приложений в группе. Отображается только для списка **Доверенные**. Все правила из списка применяются по порядку, начиная с 1.
- **Приложение** — название приложения (группы).
- **Правило запуска** —  применяется или  не применяется правило разрешения запуска (в списке **Доверенные**) или запрета запуска (в списке **Запрещенные**).

- **Регистрация события запуска** — наличие значка  означает, что при срабатывании правила запуска приложения в журнале будут регистрироваться события. Если значка нет, события регистрироваться не будут.
-  — наличие такого значка означает, что правило запуска для приложения было создано или изменено пользователем.

4 Выполните действия по настройке правил в соответствии с описанием:

- [Настройка правил запуска приложений.](#)
- [Настройка правил доступа приложений.](#)
- [Настройка порядка применения правил.](#)
- [Настройка контроля доступа к сетевым папкам.](#)
- [Добавление групп доверенных приложений и настройка правил доступа приложений по умолчанию.](#)

5 Чтобы политика была сохранена и отправлена назначенным защищаемым узлам, сохраните изменения (см. [Порядок настройки политики](#)). Рекомендуем сохранять политику только после внесения в нее всех необходимых изменений.

## Правила запуска приложений

При добавлении приложения создается правило запуска. Вы можете изменять параметры добавленных приложений, включать, выключать правила запуска и удалять приложения.

Чтобы добавить приложение и настроить правило запуска:

- 1 Чтобы добавить приложение в список **Доверенные**, на странице **Контроль приложений (Windows)** нажмите **Добавить** > **Доверенное приложение**:
  - 1.1 Укажите путь к приложению, такой же, как на защищаемом узле.



**Примечание.** В поле **Приложение** вы можете использовать маску имен файлов для выбора группы приложений в папке и вложенных папках (см. [Особенности задания и использования правил доступа](#)).

---

- 1.1 Выберите группу доверенных приложений в списке для размещения в нее приложения.
- 1.2 Чтобы при запуске приложения регистрировалось событие в журнале, выберите **Регистрировать событие запуска приложения**.



**Примечание.** Обратите внимание, что при включении опции регистрации событий для часто запускаемых приложений может увеличиться потребление ресурсов компьютера и замедлиться работа других приложений. Будьте аккуратны при включении опции для таких приложений. В этом случае рекомендуем оставлять регистрацию событий включенным на срок не более одних суток.

### 1.3 Настройте правило запуска:

- Чтобы запуск приложения был разрешен в любом режиме работы модуля контроля приложений, выберите  **Применяется**.
- Чтобы запуск приложения был разрешен только в режиме **Разрешать неизвестные**, выберите  **Не применяется**.

### 1.4 Нажмите **Добавить**.

В результате приложение и правило запуска для него будет добавлено в список выбранной группы. Для приложения будут применяться правила доступа к системе по умолчанию, [настроенные для группы](#). Чтобы настроить правила доступа (см. [Правила доступа приложений](#)) именно для этого приложения, в уведомлении о добавлении приложения щелкните **настроить правила доступа**. Вы можете настроить правила доступа и позднее (см. [Правила доступа приложений](#)).

## 2 Чтобы добавить приложение в список **Запрещенные**, на странице **Контроль приложений (Windows)** нажмите **Добавить** > **Запрещенное приложение**.

### 2.1 Укажите путь к приложению, такой же, как на защищаемом узле.



**Примечание.** В поле **Выберите путь к приложению** вы можете использовать маску имен файлов для выбора группы приложений в папке и вложенных папках (см. [Особенности задания и использования правил доступа](#)).

### 2.2 Чтобы при попытке запуска приложения регистрировалось событие в журнале, выберите **Регистрировать событие запуска приложения**.

### 2.3 Настройте правило блокировки запуска:

- Чтобы запуск приложения был запрещен в любом режиме работы модуля контроля приложений, выберите  **Применяется**.
- Чтобы запуск приложения был запрещен только в режиме **Разрешать неизвестные**, выберите  **Не применяется**. Обратите внимание, что в режиме **Разрешать неизвестные** запуск будет разрешен.

### 2.4 Нажмите **Добавить**.

Если добавлены правила для нескольких приложений, настройте порядок применения правил (см. [Настройка порядка применения правил](#)).

Чтобы изменить параметры приложения или правила запуска приложения:

- 1 На странице **Контроль приложений (Windows)** выберите **Доверенные**.
- 2 Выберите приложение в списке или предварительно на панели сверху воспользуйтесь поиском  по названию приложения. На панели справа посмотрите сведения о настройках правил приложения.
- 3 Вверху справа нажмите  и внесите изменения в разделе **Общее** по аналогии с шагами сценария добавления правила.
- 4 Нажмите **Сохранить**.

Чтобы удалить приложения:

- 1 На странице **Контроль приложений (Windows)** выберите **Доверенные**.
- 2 Выберите флажками одно или несколько приложений в списке, которые необходимо удалить.
- 3 На панели сверху нажмите  **Удалить** и подтвердите удаление.

### *Правила доступа приложений*

Правила доступа определяют активность приложения из списка **Доверенные**: перечень разрешенных операций с объектами ОС Windows. Для каждой операции можно настроить регистрацию события в журнале.



**Совет.** При включении опции регистрации событий в правилах часто запускаемых приложений может увеличиться потребление ресурсов компьютера и замедлиться работа других приложений. Будьте аккуратны при включении регистрации событий в правилах доступа для часто запускаемых приложений. Рекомендуем оставлять опцию включенной на срок не более одних суток.

При указании в правилах доступа путей к объектам учитывайте особенности их настройки (см. [Особенности задания и использования правил доступа](#)).

Вы можете добавить одно или несколько правил доступа для каждого вида объектов и настроить порядок применения правил. Правила можно отключать и изменять.

Если правила доступа для приложения не настроить, будут использоваться [правила доступа по умолчанию для группы, в которую добавлено приложение](#).

Чтобы добавить правила доступа для приложения:

- 1 На странице **Контроль приложений (Windows)** выберите **Доверенные**.
- 2 Выберите приложение в списке или предварительно на панели сверху воспользуйтесь поиском  по названию приложения. На панели справа посмотрите сведения о настройках правил приложения.
- 3 Вверху справа нажмите .

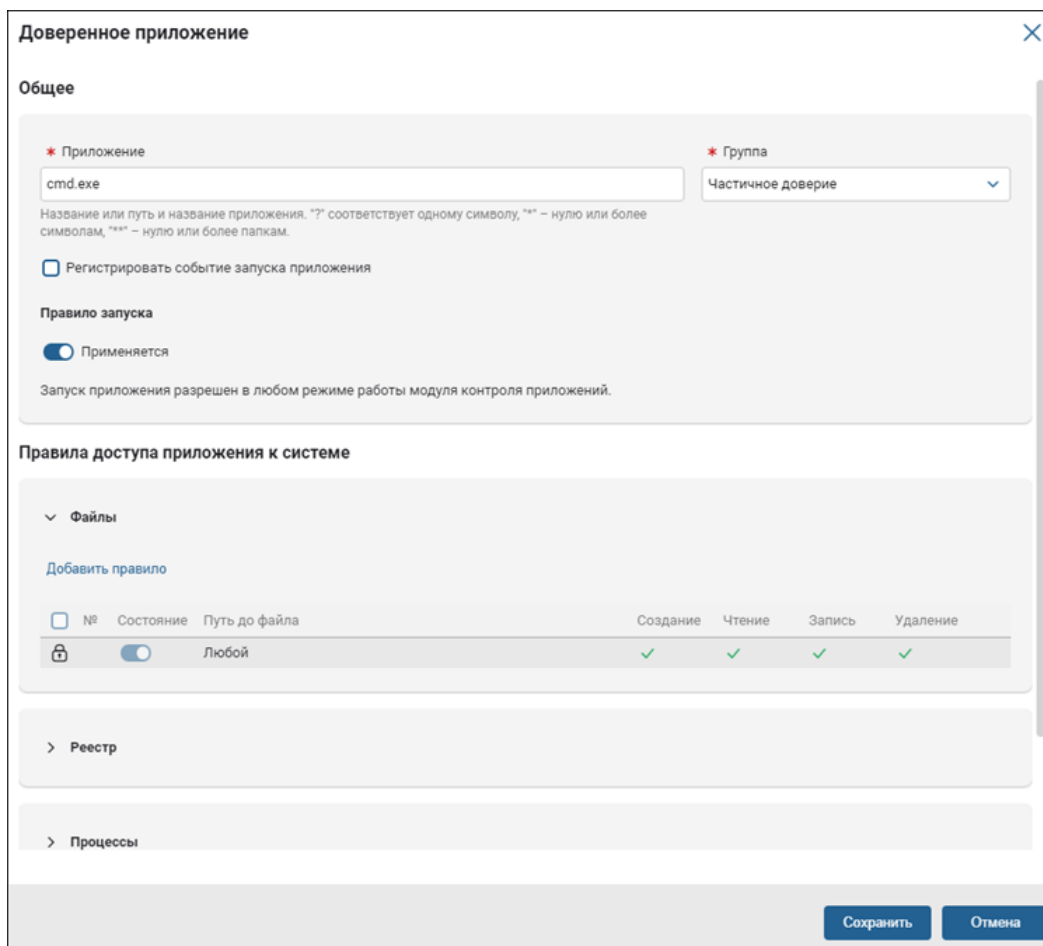


Рисунок 26. Настройка правил доступа приложения

- 4 Чтобы создать правило доступа приложения к файлам, раскройте раздел **Файлы** и нажмите **Добавить правило**.
  - 4.1 Выберите  **Правило включено**.
  - 4.2 Укажите путь к файлу, такой же, как на защищаемом узле.
  - 4.3 Выберите в списках **Создание**, **Чтение**, **Запись** и **Удаление** разрешение или запрет для операций с файлом или группами файлов.
  - 4.4 Чтобы при срабатывании правила в журнал записывались события, для каждой операции выберите **Регистрировать событие**.

**Создание правила доступа приложения к файлу**

☒ Правило включено

\* Путь до файла

C:\Windows\winhlp32.exe

"?" соответствует одному символу, "\*" – нулю или более символам, "\*\*" – нулю или более папкам.

**Доступ приложения к файлу**

\* Создание

✗ Запретить ☒ Регистрировать событие

\* Чтение

✓ Разрешить ☒ Регистрировать событие

\* Запись

✗ Запретить ☒ Регистрировать событие

\* Удаление

✗ Запретить ☐ Регистрировать событие

Создать Отмена

Рисунок 27. Создание правила доступа к файлу

#### 4.5 Нажмите **Создать**.

- 5 Чтобы добавить несколько правил доступа к файлам, повторите шаг 4.
- 6 Если добавлено несколько правил доступа к файлам, настройте порядок применения правил (см. [Настройка порядка применения правил](#)).
- 7 Чтобы создать правила доступа приложения к ветви реестра, раскройте раздел **Реестр** и нажмите **Добавить правило**.
  - 7.1 Выберите ☒ **Правило включено**.
  - 7.2 Укажите путь к ветви реестра такой же, как на защищаемом узле.
  - 7.3 Выберите в списках **Создание**, **Чтение**, **Запись** и **Удаление** разрешение или запрет для операций с указанной ветвью реестра.
  - 7.4 Чтобы при срабатывании правила в журнал записывались события, для каждой операции выберите **Регистрировать событие**.
  - 7.5 Нажмите **Создать**.
- 8 Чтобы создать несколько правил доступа к ветвям реестра, повторите шаг 7.
- 9 Если добавлено несколько правил доступа к ветвям реестра, настройте порядок применения правил (см. [Настройка порядка применения правил](#)).

10 Чтобы создать правила доступа приложения к процессам, раскройте раздел **Процессы** и нажмите **Добавить правило**.

10.1 Выберите  **Правило включено**.

10.2 Укажите путь к исполняемому файлу процесса такой же, как на защищаемом узле.

10.3 Выберите в списке **Запуск** разрешать или запрещать запуск указанного процесса.

10.4 Чтобы при срабатывании правила в журнал записывались события, выберите **Регистрировать событие**.

10.5 Нажмите **Создать**.

11 Чтобы создать несколько правил доступа к процессам, повторите шаг 10.

12 Если добавлено несколько правил доступа к процессам, настройте порядок применения правил (см. [Настройка порядка применения правил](#)).

13 Чтобы создать правила доступа для запуска приложения с помощью определенных параметров командной строки, раскройте раздел **Команды** и нажмите **Добавить правило**.

13.1 Выберите  **Правило включено**.

13.2 Укажите параметр командной строки.

13.3 Выберите в списке **Запуск** разрешать или запрещать использование параметра для запуска приложения.

13.4 Чтобы при срабатывании правила в журнал записывались события, выберите **Регистрировать событие**.

13.5 Нажмите **Создать**.

14 Чтобы создать несколько правил доступа к параметрам командной строки, повторите шаг 13.

15 Если добавлено несколько правил доступа к параметрам командной строки, настройте порядок применения правил (см. [Настройка порядка применения правил](#)).

16 Нажмите **Сохранить**.

Чтобы отключить, изменить или удалить существующее правило доступа для приложения:

1 На странице **Контроль приложений (Windows)** выберите **Доверенные**.

2 Выберите приложение в списке или предварительно на панели сверху воспользуйтесь поиском  по названию приложения. На панели справа посмотрите сведения о настройках правил приложения.

3 Сверху справа нажмите .

4 Раскройте нужный раздел (**Файлы**, **Реестр**, **Процессы**, **Команды**) и для правила, которое вы собираетесь отключить, изменить или удалить.

4.1 Чтобы отключить правило, в столбце **Состояние** выберите .

4.2 Чтобы внести изменения в правило, справа выберите  > **Изменить** и в окне настройки правила доступа установите параметры по аналогии с шагами предыдущего сценария.

4.3 Чтобы удалить правило, справа выберите  > **Удалить** и подтвердите удаление.

5 Нажмите **Сохранить**.

## Настройка порядка применения правил

Правила контроля приложений применяются последовательно, сверху вниз в соответствии с нумерацией. Правила доступа каждого приложения применяются из списка последовательно до первого срабатывания. Если ни одно из правил доступа не сработало, применяются правила доступа по умолчанию для группы этого приложения. Вы можете изменить последовательность приложений (групп приложений) или правил доступа для каждого приложения.

Чтобы изменить порядок приложений или групп приложений для применения правил доступа:

- 1 На странице **Контроль приложений (Windows)** выберите **Доверенные**.
- 2 Выберите объекты, порядок применения которых вы хотите изменить:
  - Выберите флажками одну или несколько групп приложений.
  - Раскройте одну или несколько групп приложений и выберите флажками одно или несколько приложений.
- 3 На панели сверху нажмите  или  для перемещения выбранных объектов в списке.

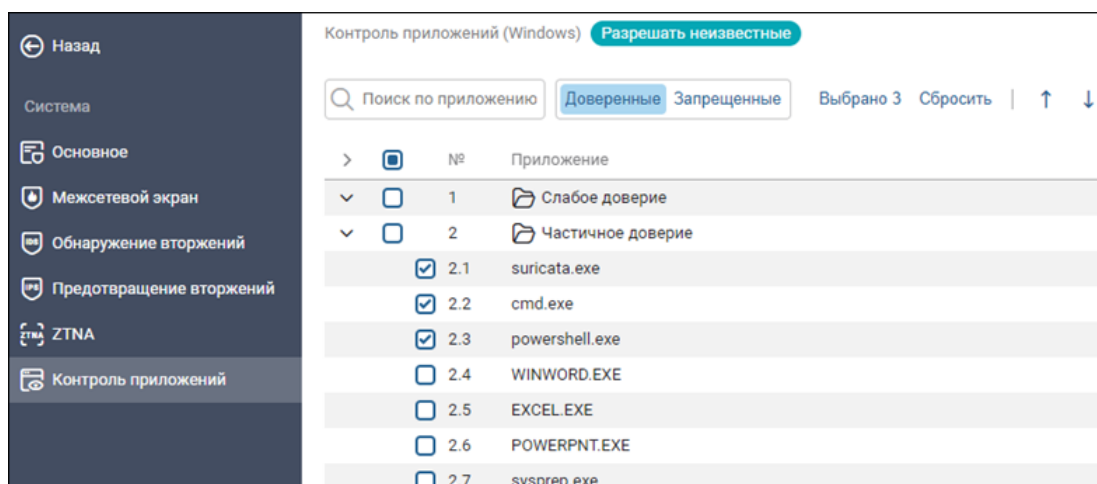


Рисунок 28. Изменение порядка применения выбранных приложений

Чтобы изменить порядок применения правил доступа для выбранного приложения:

- 1 На странице **Контроль приложений (Windows)** выберите **Доверенные**.
- 2 Выберите приложение в списке или предварительно на панели сверху воспользуйтесь поиском  по названию приложения.
- 3 На панели справа сверху нажмите .

- 4 Раскройте раздел, например **Процессы** и выберите флажками одно или несколько правил доступа, порядок применения которых вы хотите изменить.
- 5 Нажмите **↑** или **↓** для перемещения выбранных правил в списке.

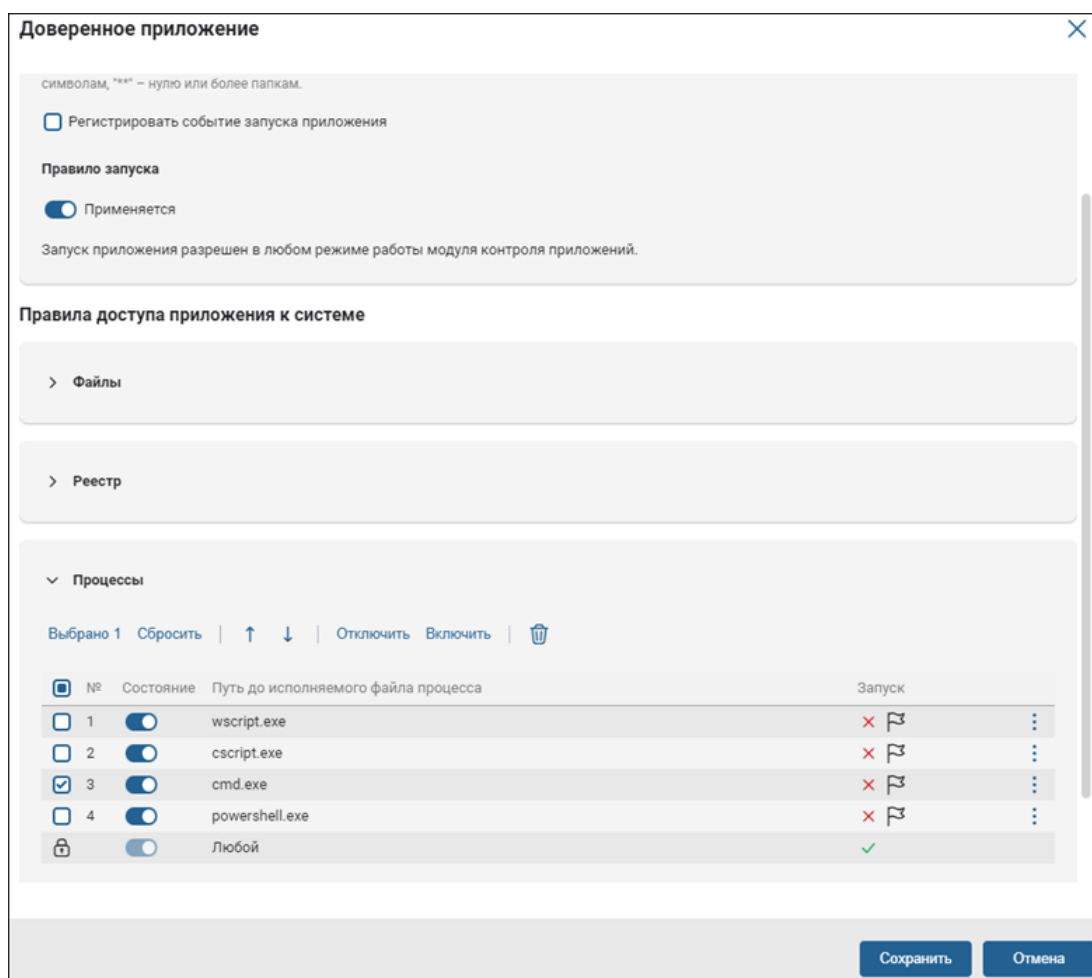


Рисунок 29. Изменение порядка применения правил доступа приложения

- 6 Нажмите **Сохранить**.

## Настройка контроля доступа к сетевым папкам

Иногда контроль доступа приложений к файлам может вызывать на защищаемых узлах замедление работы с файлами, расположенными на сетевых дисках (например, при обращении пользователя к большому количеству файлов небольшого размера). При возникновении такой проблемы для более быстрой работы с сетевыми файлами вы можете отключить контроль обращений к сетевым папкам. В результате файлы и папки, расположенные на сетевых дисках, перестанут контролироваться ViPNet EPP. Отключение контроля обращений к сетевым папкам повлияет только на работу правил доступа к файлам. Контроль запуска приложений и остальные правила доступа (для реестра, процессов и параметров командной строки) продолжат работать в полном объеме.



**Совет.** Рекомендуем не отключать контроль обращений к сетевым папкам без крайней необходимости.

---

Чтобы отключить контроль обращений к сетевым папкам:

- 1 На странице **Контроль приложений (Windows)** на панели инструментов нажмите .
- 2 Отключите **Контролировать доступ доверенных приложений к файлам в сетевых папках**.
- 3 Нажмите **Сохранить**.

Чтобы в ViPNet EPP Агент сетевые папки снова контролировались, включите **Контролировать доступ доверенных приложений к файлам в сетевых папках**.

### Добавление групп доверенных приложений и настройка правил доступа приложений по умолчанию

Вы можете настраивать правила доступа по умолчанию для пользовательских групп доверенных приложений, как предустановленных (кроме группы **Доверенные**), так и для созданных пользователем. Правила доступа по умолчанию применяются для всех приложений группы в случае, если ни одно из правил доступа приложения не сработало или правила доступа для приложения не задавались. Правила доступа по умолчанию для предустановленных групп определены в политике.

Чтобы добавить пользовательскую группу доверенных приложений и настроить для нее правила доступа по умолчанию:

- 1 На странице **Контроль приложений (Windows)** нажмите **Добавить > Группу доверенных приложений**.

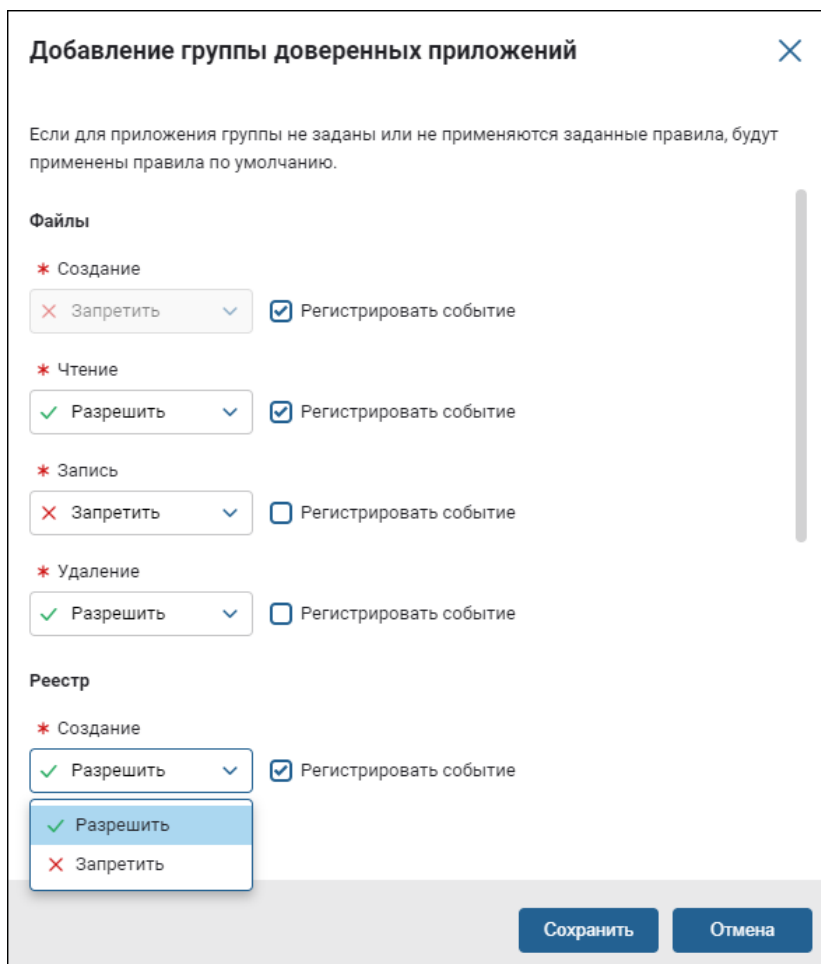


Рисунок 30. Настройка правил доступа по умолчанию для группы

- 2 Введите название группы.
- 3 Настройте правила доступа приложений к системе по умолчанию: В разделах **Файлы**, **Реестр**, **Процессы** и **Команды** настройте разрешения и запреты для операций с одноименными объектами операционной системы. Для этого в каждом разделе для каждой операции в списке выберите **Разрешить** или **Запретить**.

Чтобы при срабатывании правила доступа в журнал записывалось событие, для операции выберите **Регистрировать событие**.

- 4 Нажмите **Добавить**.

Чтобы изменить правила доступа по умолчанию для уже добавленных групп:

- 1 На странице **Контроль приложений (Windows)** выберите группу, например **Частичное доверие**.
- 2 На панели справа посмотрите настройки группы и правила доступа к системе, настроенные по умолчанию.
- 3 На панели справа сверху нажмите  и настройте разрешения и запреты аналогично сценарию настройки при добавлении группы (см. выше).

## Особенности задания и использования правил доступа

### Использование масок в правилах

Использование маски в правилах позволяет выбрать группу объектов файловой системы (папка, файл) или реестра (ключ, параметр) ОС Windows. В маске используются символы, допустимые в именах объектов, а также специальные символы:

- ? — любой допустимый символ.
- \* — любой набор допустимых символов, в том числе пустой; соответствует объектам одного уровня (папка, ключ, файл, параметр).
- \*\* — любой набор допустимых символов, в том числе пустой; соответствует:
  - для маски объектов файловой системы — частям путей к объектам (папка и файл) определенного уровня, включая объекты уровней, расположенных выше.
  - для маски объектов реестра — частям ветвей к объектам (ключ, параметр) определенного уровня, включая объекты уровней, расположенных выше.
- \ и / — разделители частей пути или ветви.

Особенности синтаксиса маски:

- Разделители \ и / равнозначны.
- После \*\* необходимо указывать разделитель, например \*\*\\*.txt.

Примеры масок объектов файловой системы. Например, на диске C: расположены следующие объекты:

- 1 C:\aaa\bbb\ccc\ddd.txt
- 2 C:\aaa\ddd.txt
- 3 C:\aaa\bbb\ddd.txt
- 4 C:\bbb\aaa\bbb\ccc.txt
- 5 C:\bbb\ccc.txt

Маска C:\\*\*\\*.txt соответствует всем объектам.

Маска C:\aaa\\*\*\\*.txt соответствует объектам 1 — 3.

Маска C:\aaa\\*.txt соответствует объекту 2.

Маска C:\\*\*\bbb\\*.txt соответствует объектам 3 — 5.

Маска C:\\*\\*.txt соответствует объектам 2 и 5.

### Использование переменных ViPNet EPP в правилах доступа к файлам

При задании путей в правилах доступа к файлам вы можете использовать системные переменные среды ОС Windows, созданные от имени пользователя System, такие как:

- `%EPP_AGENT_ROOT%` — путь к папке с исполняемыми файлами ViPNet EPP Агент. Принимает значение, заданное в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\epcontrol\Parameters\InstalledFrom`.
- `%EPP_SERVER_ROOT%` — путь к папке с исполняемыми файлами ViPNet EPP Сервер. Переменная определена, если ViPNet EPP Агент и ViPNet EPP Сервер установлены на одном компьютере. Принимает значение, заданное в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EppServer\ImagePath`.
- `%SYSTEMDRIVE%` — имя диска, содержащего корневую папку ОС Windows.
- `%SYSTEMROOT%` — корневая папка ОС Windows.

Например, в правиле доступа вместо `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection Server\EppServer.exe` укажите `%EPP_SERVER_ROOT%`.

## Особенности правил доступа к файлам, запрещающих удаление

Некоторые программы передают удаление файлов на уровень системных процессов, например, процессу `dllhost.exe`. Учитывайте такое поведение при создании правил доступа к файлам, которые блокируют удаление.

Из-за особенностей работы файловой системы ОС Windows, запрет удаления файлов возможен только при одновременном запрете записи. Запрет записи допускается устанавливать и без запрета удаления, но не наоборот.

## Особенности правил доступа к реестру

Приложения, работающие с реестром ОС Windows, например `regedit.exe`, сразу открывают реестр с правами «на запись». Учитывайте такое поведение при создании правил доступа к реестру, которые запрещают запись в ветвь реестра.

## Запуск дочерних процессов приложения

На запускаемые дочерние процессы приложения, помимо правил доступа, действуют глобальные и пользовательские списки (черный и белый), а также режим работы ViPNet EPP Агент.

Например, если приложение `App_1` находится в пользовательском черном списке, а приложению `App_2` из пользовательского белого списка разрешено запускать приложение `App_1` исходя из правил доступа к процессам, то запуск приложения `App_1` будет запрещен на основе пользовательского черного списка.

## Особенности правил доступа к файлам для приложения notepad++

Если требуется запретить чтение файла с помощью текстового редактора notepad++, то в правилах доступа к этому файлу необходимо установить запрет не только на чтение, но и на удаление этого файла. Иначе, ввиду особенности работы notepad++, при открытии на чтение файл может быть удален.

## Особенности правил доступа для параметров командной строки

При создании и настройке правил доступа для параметров командной строки необходимо учитывать следующие особенности:

- Несколько параметров командной строки необходимо заключать в двойные кавычки, например, `ipconfig "/renew EL*"`.
- В параметре командной строки запрещено использовать `&`.
- Значение параметра не может быть пустым. Используйте `*`, если необходимо указать, что параметр может быть любым, в том числе отсутствовать.

## Удаление политики

Вы можете удалять политики, например, устаревшие и неиспользуемые. К удалению доступны политики, которые не назначены ни одной группе.

Чтобы удалить политику:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Политики безопасности**.
- 3 В списке выберите флажками политики для удаления.
- 4 На панели сверху нажмите  и подтвердите удаление.

# Настройка критериев обнаружения аномалий

Правила обнаружения аномалий позволяют контролировать локальную и сетевую активность на защищаемых узлах в течение заданного времени. Для этого администратор ViPNet EPP задает временной интервал, для которого локальная или сетевая активность нетипична. Например, в нерабочее время на защищаемых узлах файлы, как правило, не изменяются, активность пользователей в сети интернет отсутствует. При активности в указанные часы регистрируется аномалия. Правило обнаружения аномалии задается идентификаторами правил (см. [Типы и идентификаторы правил](#)), а также временным интервалом.

Чтобы настроить правило обнаружения аномалий:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Обнаружение аномалий**.
- 3 Для добавления нового правила нажмите **Создать правило**.
  - 3.1 Введите название правила.
  - 3.2 В поле **Идентификаторы событий** укажите через запятую идентификаторы правил в диапазоне от 10000 до 7999999, при срабатывании которых должна регистрироваться аномалия.
  - 3.3 В полях **Период аномального возникновения событий** укажите границы временного интервала, в котором срабатывание указанных правил считается нетипичным.

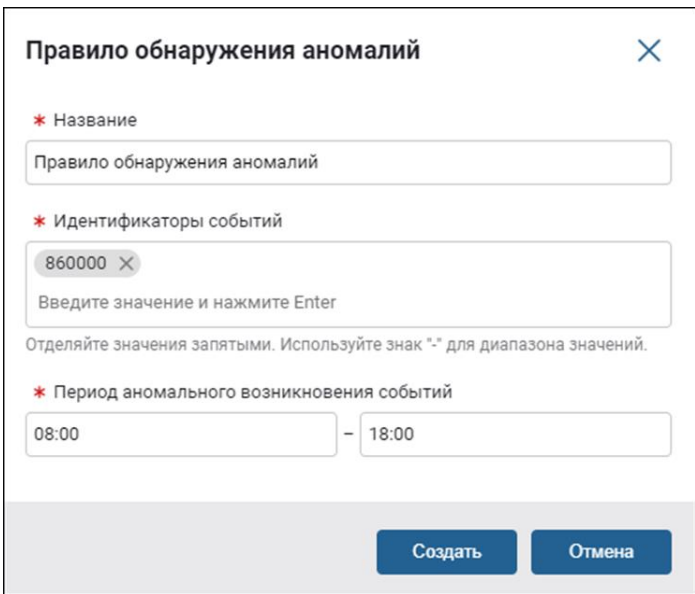


Рисунок 31. Создание правила обнаружения аномалий

- 4 Нажмите **Создать**.

# Работа с журналами

В ViPNet EPP Сервер ведутся журналы:

- Журнал критичных событий информационной безопасности защищаемых узлов (см. [Критичные события агентов \(Инфопанель\)](#)).
- Журнал аудита действий пользователей (см. [Журналы аудита](#)).

В ViPNet EPP Рабочий сервер ведется журнал всех событий подключенных к нему защищаемых узлов. В ViPNet EPP Сервер управления вы можете запросить эти журналы (см. [Журналы событий](#)).

При переполнении журналов в соответствии с параметрами хранения выполняется автоматическая ротация событий и журналов (см. [Настройка параметров сервера управления](#)).

## Критичные события агентов (Инфопанель)

ViPNet EPP консолидирует события информационной безопасности подключенных защищаемых узлов в журнале событий ViPNet EPP Сервер в режиме, близком к реальному времени. По умолчанию на ViPNet EPP Сервере регистрируются только критические события всех подключенных защищаемых узлов. Администратор может настроить регистрацию событий в журнале по своим критериям, выбрав уровни событий, идентификаторы правил и защищаемые узлы.

Вы можете просмотреть журнал критичных событий на инфопанели:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора или аудитора.
- 2 Выберите **Мониторинг** >  **Инфопанель**.

Каждая запись о событии в журнале содержит:

- Цветовой индикатор уровня события:
  -  — критическое.
  -  — опасное.
  -  — важное.
  -  — информационное.
- **Время** — дата и время регистрации события (UTC+3).
- **Событие** — текстовое описание события.
- **Количество** —
  - для защищаемых устройств с ОС Windows — количество повторений события на защищаемом узле каждые 200 мс. Повторные события определяются по одинаковому идентификатору сработавшего правила.

- для защищаемых устройств с ОС Linux — количество зарегистрированных событий сработавшим правилом.
- **Устройство** — имя защищаемого узла, на котором зарегистрировано событие.
- **Группа устройств** — группа устройств, к которой относится защищаемый узел.
- **Модуль защиты** — модуль защиты, к которому относится сработавшее правило:
  - Межсетевой экран.
  - Обнаружение вторжений.
  - Предотвращение вторжений.
  - Контроль приложений.

3 Для поиска событий в журнале используйте фильтры:

3.1 Выберите по какому полю найти элемент: **Устройство** или **Событие**, в поле поиска  введите ключевое слово.

3.2 Выберите или нажмите  и укажите промежуток времени, в течение которого происходили искомые события.

3.3 Нажмите **Фильтры** и задайте параметры фильтрации:

- Чтобы в журнале отображались только аномальные события, выберите **Только аномальные события**.
- Выберите типы событий.
- Выберите группу устройств.

3.4 Нажмите **Применить**.

4 Для обновления списка событий вручную сверху нажмите .

5 Чтобы удалить события с сервера, выберите флажками события, на панели сверху нажмите  и подтвердите удаление.

Чтобы просмотреть сведения о событии, щелкните название события в выбранной строке.

### Сервис был запущен

✕

|                       |                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------|
| Уровень события       | ● Важное                                                                                                |
| Дата и время          | 04.12.2025 12:36:36 (UTC+3)                                                                             |
| Количество            | 1                                                                                                       |
| Тип события           | SystemActivityLinux                                                                                     |
| Модуль защиты         |  Обнаружение вторжений |
| Устройство            | <a href="#">astra-06700</a>                                                                             |
| Группа устройств      | Подключенные                                                                                            |
| Идентификатор правила | 870023                                                                                                  |
| Политика              | Epp_20251125_20_1.8.0_RU (2.0.0)                                                                        |

**Текст события**

Dec 4 14:36:36 astra-06700 systemd[1]: Starting apt-daily.service - Daily apt download activities...

**Сработавшее правило**

```
<rule id="870023" level="2"><program_name>systemd</program_name><regex ignorecase="true">(Started|Starting)(?!.*\bEndpoint\s+Protection\b).*</regex><description>Сервис был запущен</description><info><link/><techniques/><capec/><cwe/><cve/></info></rule>
```

[Удалить с сервера](#)

Заккрыть

Рисунок 32. Подробная информация о событии на защищаемом узле

Чтобы изменить критерии регистрации событий в журнал, отображаемый на инфопанели:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора или аудитора.
- 2 Выберите **Мониторинг** >  **Инфопанель**.
- 3 На панели сверху нажмите .
- 4 Задайте критерии:
  - **События устройств** — выберите защищаемые узлы или группы защищаемых узлов, для которых нужно сохранять в журнале сервера зарегистрированные события. Подробнее о выборе устройств в ViPNet EPP см. [Выбор защищаемых узлов при настройке передачи событий](#).
  - Чтобы в журнале регистрировались только аномальные события, выберите **Только события с признаком аномальности**.
  - **Уровень события** — информационное, важное, опасное и критическое. Укажите уровни событий, зарегистрированных на защищаемых узлах, которые должны регистрироваться в журнале сервера.

- **Тип события** — укажите модули защиты или идентификаторы правил на защищаемых узлах, при срабатывании которых в журнале сервера будут регистрироваться события.

#### 5 Нажмите **Сохранить**.

В результате в журнале критичных событий начнут регистрироваться события в соответствии с заданными настройками. Все события, зарегистрированные при предыдущих настройках, останутся в журнале и будут доступны для просмотра.

## Журналы событий

Вы можете запрашивать данные журнала событий информационной безопасности с подключенных защищаемых узлов за заданный период времени. Защищаемые узлы должны быть в активном состоянии.

Запрос формируется на основе заданных параметров: уровней событий, идентификаторов правил, списка защищаемых узлов и периода времени, за который нужны данные журнала событий с указанных узлов.

В результате каждого запроса формируется журнал событий информационной безопасности в соответствии с заданными параметрами. Запрашиваемые события защищаемых узлов хранятся на рабочих серверах, а формируемые журналы сохраняются на ViPNet EPP Сервер управления и доступны к просмотру. Можно временно приостанавливать формирование журналов и удалять.

Чтобы запросить журнал событий информационной безопасности агентов за определенный период:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора или аудитора.
- 2 Выберите **Мониторинг** >  **Журналы событий**.
- 3 Нажмите **Запросить журнал**.
- 4 Задайте параметры запроса:
  - Период времени, за который в журнал должны попасть данные о событиях.
  - Название журнала.
  - **События устройств** — выберите защищаемые узлы или группы защищаемых узлов, для которых нужно сохранять в журнале сервера зарегистрированные события. Подробнее о выборе устройств в ViPNet EPP см. [Выбор защищаемых узлов при настройке передачи событий](#).
  - Чтобы в журнале отображались только аномальные события, выберите **Только события с признаком аномальности**.
  - **Уровень события** — информационное, важное, опасное и критическое. Укажите уровни событий, зарегистрированных на защищаемых узлах, которые должны регистрироваться в журнале сервера.

- **Тип события** — укажите модули защиты или идентификаторы правил на защищаемых узлах, при срабатывании которых в журнале сервера будут регистрироваться события.

## 5 Нажмите **Сохранить**.

В результате на странице **Журналы событий** отобразится новый отчет в соответствии с заданными настройками.

Вы можете остановить запрос, для этого щелкните строку журнала со статусом **Формируется** и на правой боковой панели в разделе **Общие** нажмите **Приостановить формирование**.

Чтобы продолжить выполнение запроса, щелкните строку журнала со статусом **Формирование приостановлено** и на правой боковой панели в разделе **Общие** нажмите **Возобновить формирование**.

### Журналы событий

Поиск по названию журнала

| <input type="checkbox"/> Журнал                            | Период событий (UTC+3)  | Статус журнала | События |
|------------------------------------------------------------|-------------------------|----------------|---------|
| <input type="checkbox"/> За 3-4.12                         | 03.12.2025 – 04.12.2025 | ● Сформирован  | 6 108   |
| <input type="checkbox"/> Все события, кроме информационных | 03.12.2025 – 04.12.2025 | ● Сформирован  | 6 123   |
| <input type="checkbox"/> Все события, кроме информационных | 03.12.2025 – 04.12.2025 | ● Сформирован  | 6 124   |
| <input type="checkbox"/> Все события, кроме информационных | 03.12.2025 – 04.12.2025 | ● Сформирован  | 5 921   |

### Все события, кроме информационных

#### Общие

Статус журнала

● Сформирован

Начало формирования

04.12.2025 16:58:42

Окончание формирования

04.12.2025 17:15:40

События

5 921

Автоудаление журнала ?

Разрешено

Открыть журнал

#### Параметры событий

Период событий

03.12.2025 16:57:58 – 04.12.2025

Типы событий

Все типы событий

Уровни событий

Важное, Опасное, Критическое

Аномальность

Не учитывается

#### Устройства

☒ Подключенные

☒ Тестируемые

Рисунок 33. Журналы событий информационной безопасности защищаемых узлов

Чтобы просмотреть журнал:

- 1 Откройте выполненный запрос:
  - 1.1 Щелкните строку журнала со статусом **Сформирован**.
  - 1.2 На правой боковой панели в разделе **Общие** нажмите **Открыть журнал**.
- 2 Записи о событиях отображаются в том же формате, что и на инфопанели в журнале критичных событий агентов (см. [Критичные события агентов \(Инфопанель\)](#)).
- 3 Чтобы просмотреть сведения о событии, щелкните строку с событием.

Чтобы удалить ненужные журналы:

- 1 Выберите флажками отчеты для удаления.
- 2 На панели сверху нажмите  и подтвердите удаление.

По умолчанию, журналы событий по запросу хранятся в системе 45 дней. Вы можете изменить срок хранения журнала (см. [Настройка параметров сервера управления](#)).

## Журналы аудита

В журнале аудита ViPNet EPP Сервер регистрируются события, вызванные действиями пользователей, а также системные события ViPNet EPP Сервер.

Вы можете просматривать журналы аудита отдельно для сервера управления и рабочих серверов. Для сервера управления доступна настройка типов событий, которые необходимо регистрировать в журнале аудита (см. [Настройка параметров сервера управления](#)). По умолчанию регистрируются все типы событий.

Чтобы просмотреть журнал аудита сервера управления:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер от имени администратора или аудитора.
- 2 Выберите  **Журналы аудита** и перейдите на вкладку **Журнал сервера управления**.

Каждая запись в журнале содержит:

- **Дата и время** — дата и время, когда событие зарегистрировано.



**Примечание.** Для периодических событий, например, события **Запуск самотестирования сервера**, время между регистрациями событий отсчитывается от момента завершения действия из предыдущего события. В связи с чем время между регистрациями периодических событий может быть больше заданного периода времени для действия из события.

- **События** — название события.
- **Инициатор:**
  - Система (например, системное событие «Запуск самотестирования сервера управления»).
  - Администраторы, аудиторы (например, аутентификация администратора на ViPNet EPP Сервер).
- **Результат** — действие, вызвавшее событие успешно (● **Успех**) или неудачно (● **Неуспех**).
- **Описание** — краткая информация о событии.

Чтобы просмотреть журнал аудита рабочего сервера:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора или аудитора.

- 2 Выберите  **Журналы аудита** и перейдите на вкладку **Журнал рабочих серверов**.
- 3 Настройте фильтры отображаемых событий:
  - 3.1 Нажмите **Настроить фильтры событий**.
  - 3.2 Выберите рабочий сервер для просмотра событий аудита. Рабочий сервер должен быть в активном состоянии.
  - 3.3 Укажите период времени. В журнале отобразятся события только за этот период.
  - 3.4 Выберите результаты событий. В журнале отобразятся события только с выбранными результатами. Вы можете не выбирать результат, тогда в журнале отобразятся события с любым результатом.
  - 3.5 Нажмите **Применить**.

Записи о событиях отображаются в том же формате, что и в журнале аудита сервера управления.

## Запрос журнала регистрации трафика с ViPNet EPP Агент

Администратор ViPNet EPP Сервер может запрашивать данные журнала регистрации трафика с подключенных защищаемых узлов за заданный период времени. Запрос данных доступен только для защищаемых узлов, на которых при подключении к ViPNet EPP Сервер была разрешена работа модуля [Межсетевой экран](#). Защищаемые узлы должны быть в активном состоянии.

Запрос формируется для выбранного защищаемого узла на основе заданных параметров:

- период времени, за который нужны данные журнала трафика;
- действие сработавших правил фильтрации (блокирует или пропускает IP-пакеты).

По умолчанию будут запрашиваться данные обо всех зарегистрированных событиях за последние сутки.

В результате каждого запроса формируется отчет, содержащий события журнала трафика защищаемого узла в соответствии с параметрами поиска. Отчеты сохраняются в ViPNet EPP Сервер и доступны к детальному просмотру. По умолчанию срок хранения каждого отчета составляет 30 дней с момента создания, после чего отчет удаляется. Администратор ViPNet EPP Сервер может изменить срок хранения отчетов о трафике (см. [Настройка параметров сервера управления](#)). Отчеты можно удалить и вручную.

Чтобы запросить данные журнала трафика с подключенного защищаемого узла:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Устройства**.
- 3 Найдите защищаемый узел в списке и выберите его.

- 4 На панели справа выберите вкладку **Трафик**.
- 5 Нажмите **Запросить журнал**, укажите период времени, за который нужен отчет, и действие правил фильтрации трафика.
- 6 Нажмите **Запросить** и дождитесь создания отчета. Отчет будет создан, когда пропадет значок ⌄ рядом с датой запроса.

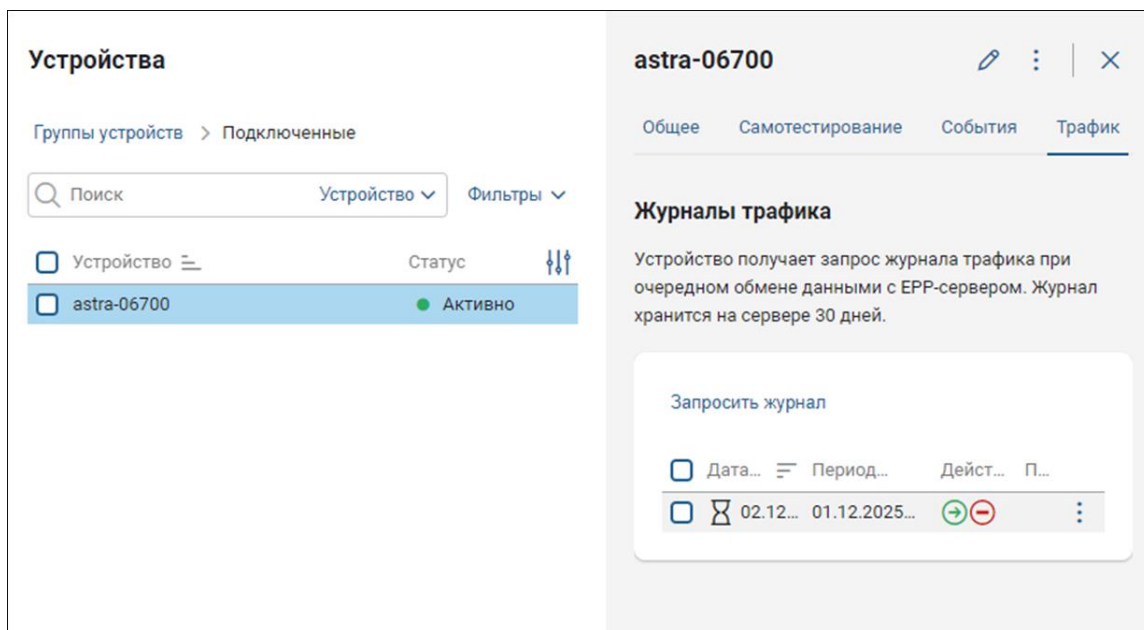


Рисунок 34. Запрос данных журнала трафика с защищаемого узла

Чтобы просмотреть отчеты о трафике с выбранного защищаемого узла:

- 1 На панели справа на вкладке **Трафик** для каждого отчета отображаются:
  - **Дата запроса.**
  - **Период трафика** — временной период, за который был запрошен отчет о трафике.
  - **Действие правил**, по которым зарегистрировался трафик.
  - **Пакеты** — количество зарегистрированных IP-пакетов.
- 2 Для просмотра подробной информации в отчете щелкните период трафика и просмотрите данные о событиях.

Каждая запись о событии содержит:

- **Время последнего пакета** — дата и время регистрации последнего IP-пакета с одинаковыми характеристиками.
- **Сеть** — к какой сети относится сетевой фильтр:
  - **Защищенная сеть** — зарегистрировано фильтром защищенной сети ViPNet (только если установлена программа ViPNet Client 5).
  - **Открытая сеть** — зарегистрировано фильтром открытой сети.
- **Направление** — направление трафика (Входящий, Исходящий).

- **Действие правила** — **Блокировать** или **Пропускать**.
- IP-адреса и порты источника и назначения, протокол передачи.
- **Пакеты** — количество зарегистрированных однотипных IP-пакетов за указанный период времени.
- **Сработавшее правило** — правило, по срабатыванию которого было зарегистрировано событие:
  - Сетевой фильтр из списка фильтров для режимов работы.
  - Служебный трафик EndPoint — всегда разрешенный трафик, необходимый для взаимодействия ViPNet EPP Агент с ViPNet EPP Сервер.
  - Правило фильтрации HTTP-контента — трафик, зарегистрированный фильтром контента HTTP.
  - Фильтры только для защищаемых узлов с ViPNet Client 5:
    - Пропуск трафика VPN сети (шифрованный) — входящий и исходящий шифрованный VPN трафик (сети ViPNet).
    - Пропуск VPN трафика пользователя (нешифрованный) — входящий и исходящий нешифрованный VPN трафик (сети ViPNet).
    - Невыполнение политик ZTNA — трафик заблокирован из-за невыполнения политик ZTNA.
    - Исключение по пропуску трафика ZTNA — политика ZTNA не выполнена, но трафик был пропущен из-за наличия исключения из политик.

Вы можете отсортировать записи отчета по любому из указанных параметров.

- 3 Чтобы найти определенные события, в поле поиска  введите часть адреса источника или назначения IP-пакета, уточните период времени и воспользуйтесь фильтром поиска **Фильтры** по сети, направлению, действию правила.
- 4 Чтобы просмотреть дату и время регистрации каждого IP-пакета события, выберите событие и щелкните количество пакетов в поле **Пакеты**.

Чтобы удалить отчеты о трафике с выбранного защищаемого узла, например устаревшие, на панели справа на вкладке **Трафик** выберите отчеты флажками и на панели сверху нажмите  . Подтвердите удаление.

# Администрирование ViPNet EPP Сервер

## Управление рабочими серверами

### Добавление рабочего сервера на сервер управления

Для начала работы ViPNet EPP Сервер должен быть подключен к серверу управления хотя бы один рабочий сервер. Вы можете подключить один или несколько рабочих серверов. Перед подключением добавьте рабочий сервер на сервер управления и скопируйте присвоенный ему идентификатор.

Чтобы добавить рабочий сервер на сервер управления:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора (см. [Подключение к веб-интерфейсу ViPNet EPP Сервер](#)).
- 2 Выберите  **Серверы безопасности > Рабочие серверы**.
- 3 На панели сверху нажмите **Добавить сервер**, укажите имя и описание рабочего сервера. Длина имени не должна превышать 100 символов.
- 4 Нажмите **Добавить**.

Сервер отобразится на вкладке **Рабочие серверы** в статусе **Не подключен**.

Чтобы скопировать идентификатор рабочего сервера, выберите сервер и на панели справа в разделе **Общее** скопируйте идентификатор.

Чтобы включить сервер в работу, настройте подключение на компьютере рабочего сервера (см. [Установка ViPNet EPP Сервер](#)).

### Просмотр и настройки параметров рабочих серверов

После добавления рабочих серверов вы можете просматривать и настраивать параметры серверов:

- Период самотестирования рабочего сервера.
- Параметры хранения журналов событий, полученных с защищаемых устройств: сроки хранения и максимальное количество событий от одного устройства.
- Параметры хранения событий рабочего сервера в журнале аудита: сроки хранения и максимальное количество событий аудита сервера.

Настройки можно задать как сразу для всех подключенных рабочих серверов (настройки по умолчанию), так и отдельно для каждого. После добавления рабочего сервера на него действуют настройки по умолчанию.

При переполнении журналов в соответствии с параметрами хранения автоматически удаляются:

- События с истекшим сроком хранения.
- Все наиболее старые события, превышающие максимальное количество хранимых событий, а также еще 25% наиболее старых событий на момент проверки.

Информация о переполнении журнала и удалении событий фиксируется в журнале аудита.

Чтобы просмотреть и настроить параметры рабочих серверов:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора (см. [Подключение к веб-интерфейсу ViPNet EPP Сервер](#)).
- 2 Выберите  **Серверы безопасности > Рабочие серверы**.

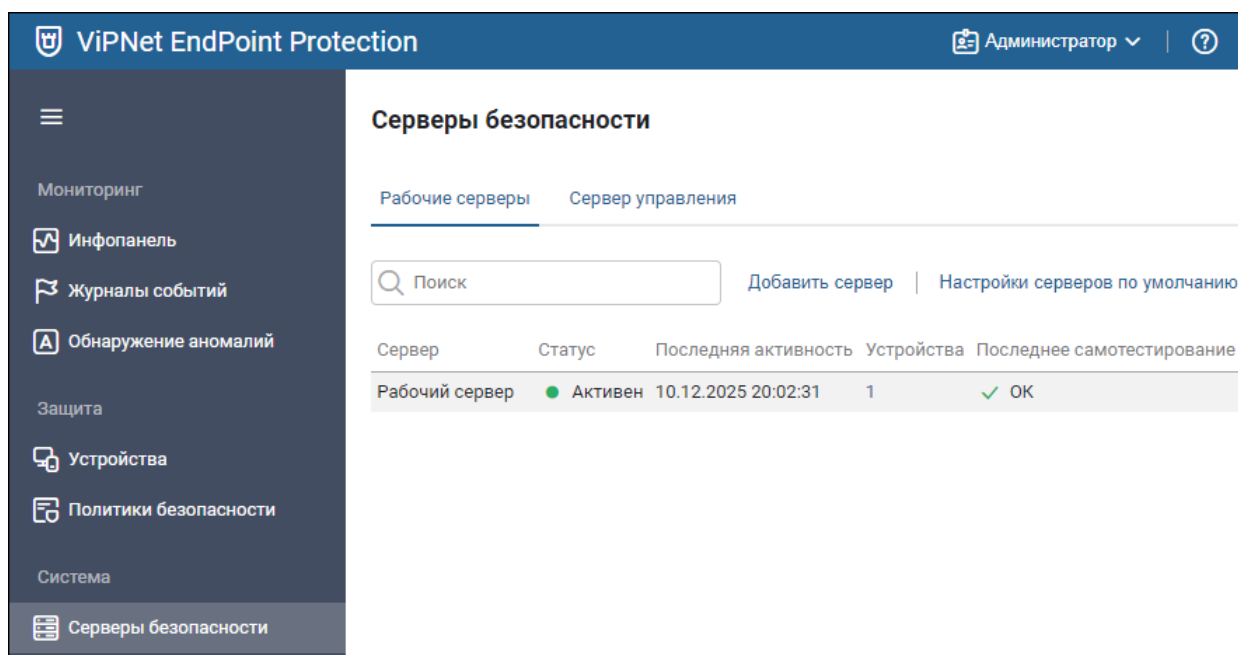


Рисунок 35. Просмотр списка рабочих серверов

Для рабочих серверов в списке отображаются:

- **Сервер** — название сервера.
- **Статус**:
  -  **Не подключен** — рабочий сервер еще не подключен к серверу управления.
  -  **Активен** — рабочий сервер подключен.
  -  **Нет связи** — рабочий сервер был подключен, но в настоящий момент недоступен. Связь с рабочим сервером потеряна, данные от подключенных защищаемых узлов не поступают.

- **Последняя активность** — время последней активности сервера.
- **Устройства** — количество подключенных защищаемых узлов.
- **Последнее самотестирование** — результаты последнего самотестирования рабочего сервера:
  - **ОК** — проблем не обнаружено.
  - **Проблема** — выявлены проблемы. Чтобы посмотреть перечень проблем, выберите сервер и посмотрите на панели справа в разделе **Самотестирование** (см. [Проверка работоспособности и контроль целостности](#)).

3 Чтобы посмотреть и изменить настройки по умолчанию для рабочих серверов:

3.1 На панели сверху нажмите **Настройки серверов по умолчанию**. Вы можете изменить:

- **Период самотестирования** — промежуток времени, через который проверяется работоспособность рабочего сервера (см. [Проверка работоспособности и контроль целостности](#)). Можно задать в минутах, секундах или часах. Рекомендуемое значение — 10 минут. Может принимать значение из диапазона 20 секунд–24 часа.
- Параметры хранения событий устройств:
  - **Срок хранения событий, дни** — события, зарегистрированные ранее указанного срока, удаляются из журнала событий в ViPNet EPP Сервер. Рекомендуемое значение — 45 дней. Может принимать значение из диапазона 1–400 дней.
  - **Максимальное количество событий одного устройства** — максимальное число записей, которое может храниться в журнале событий в ViPNet EPP Сервер для каждого защищаемого узла. Рекомендуемое значение — 50000. Может принимать значение из диапазона 1–100000.
- Параметры хранения событий аудита сервера:
  - **Срок хранения событий, дни** — события, зарегистрированные ранее указанного срока, удаляются из журнала аудита рабочего сервера. Рекомендуемое значение — 45 дней. Может принимать значение из диапазона 1–400 дней.
  - **Максимальное количество событий** — максимальное число записей, которое может храниться в журнале аудита рабочего сервера в ViPNet EPP Сервер. Рекомендуемое значение — 50000. Может принимать значение из диапазона 1–100000.

Для возврата измененных параметров сервера к значениям по умолчанию нажмите **По умолчанию**.

3.2 Если настройки были изменены, нажмите **Сохранить**.

Настройки по умолчанию применяются ко всем рабочим серверам, в параметрах которых включено **Использовать настройки по умолчанию**.

4 Чтобы найти сервер, в поле **Поиск** введите ключевое слово.

5 Чтобы посмотреть настройки определенного сервера, выберите его, на правой панели будут отображены разделы:

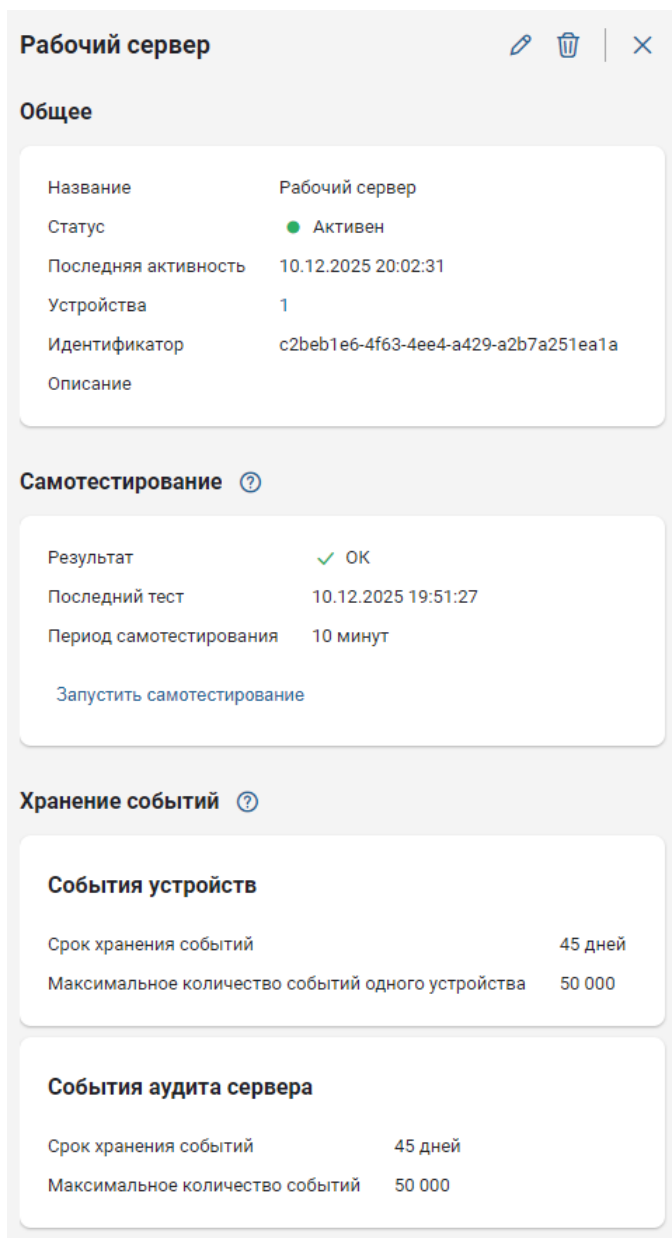


Рисунок 36. Просмотр настроек рабочего сервера

- **Общее** — название и идентификатор сервера, данные о статусе подключения, последней активности и количестве подключенных устройств.
- **Самотестирование** — период самотестирования и результат последнего самотестирования (если оно было).
- **Хранение событий** — параметры хранения событий защищаемых устройств и событий аудита рабочего сервера.

6 Чтобы изменить настройки выбранного сервера:

6.1 На правой панели нажмите  .

6.2 Измените название и описание сервера.

- 6.3 Чтобы изменить параметры самотестирования и хранения событий, для соответствующей группы параметров выключите **Использовать настройки по умолчанию** и внесите изменения в соответствии с описанием на шаге 3.

Нажмите **Сохранить**.

## Удаление рабочего сервера

Если к рабочему серверу не подключены защищаемые узлы, вы можете его удалить.

- 1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора (см. [Подключение к веб-интерфейсу ViPNet EPP Сервер](#)).
- 2 Выберите  **Серверы безопасности > Рабочие серверы**.
- 3 Выберите сервер и на правой панели нажмите .
- 4 Для подтверждения удаления выбранного сервера нажмите **Удалить**.

## Настройка параметров сервера управления

Вы можете просматривать и настраивать параметры сервера управления:

- Идентификатор (только просмотр).
- Период самотестирования сервера.
- Параметры журнала аудита:
  - Сроки хранения и максимальное количество событий аудита.
  - Типы регистрируемых событий.
- Параметры хранения событий и журналов, полученных с защищаемых устройств:
  - Срок хранения и максимальное количество событий в журнале критичных событий (раздел **Инфопанель**).
  - Срок хранения журналов событий, запрошенных с защищаемых устройств (раздел **Журналы событий**).
  - Срок хранения журналов трафика, запрошенных с защищаемых устройств.

При переполнении журналов в соответствии с параметрами хранения автоматически удаляются:

- События и журналы с истекшим сроком хранения.
- Все наиболее старые события, превышающие максимальное количество хранимых событий, а также еще 25% наиболее старых событий на момент проверки.

Информация о переполнении журнала и удалении событий фиксируется в журнале аудита.

Чтобы просмотреть и настроить параметры сервера управления:

- 1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора (см. [Подключение к веб-интерфейсу ViPNet EPP Сервер](#)).
- 2 Выберите  **Серверы безопасности > Сервер управления**.
- 3 Просмотрите заданные настройки.
- 4 Чтобы настроить параметры, в разделе с необходимыми параметрами нажмите , внесите изменения и нажмите **Сохранить**.

Вы можете изменять:

- В разделе **Самотестирование**:
  - **Период самотестирования** — промежуток времени, через который проверяется работоспособность сервера управления (см. [Проверка работоспособности и контроль целостности](#)). Можно задать в минутах, секундах или часах. Рекомендуемое значение — 10 минут. Может принимать значение из диапазона 20 секунд–24 часа.
- В разделе **Журнал аудита**:
  - **Срок хранения событий, дни** — события, зарегистрированные ранее указанного срока, удаляются из журнала аудита сервера управления. Рекомендуемое значение — 45 дней. Может принимать значение из диапазона 1–400 дней.
  - **Максимальное количество событий** — максимальное число записей, которое может храниться в журнале аудита сервера управления. Рекомендуемое значение — 50000. Может принимать значение из диапазона 1–100000.

- **Типы событий** — типы событий, которые будут регистрироваться в журнале аудита сервера управления. По умолчанию регистрируются события всех типов:

Журнал аудита

Хранение событий

\* Срок хранения событий, дни

45

От 1 до 400 дней.

\* Максимальное количество событий

50000

От 1 до 100 000.

Типы событий

\* Регистрировать в журнале аудита события следующих типов

▼

☑ Все типы событий

>

☑ Журнал аудита

>

☑ Самотестирование

>

☑ Операции с учетными записями

>

☑ Операции с политикой

>

☑ Действия с устройствами

>

☑ Операции с критериями обнаружения аномалий

>

☑ Операции с группами устройств

>

☑ Лицензирование

>

☑ Действия с РС

>

☑ Изменение системных настроек

>

☑ Действия с избранными правилами

>

☑ Операции с журналом критичных событий

>

☑ Операции с отчётами

>

☑ Регистрируются всегда

По умолчанию

Сохранить

Отмена

Рисунок 37. Типы регистрируемых событий

ViPNet EndPoint Protection for Linux. Руководство администратора | 161

Вы можете отключить регистрацию событий одного, нескольких или сразу всех типов, кроме обязательных событий, которые регистрируются всегда:

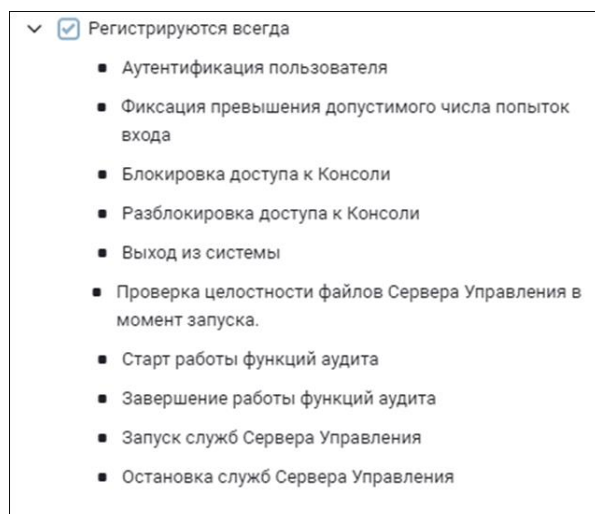


Рисунок 38. События, регистрируемые всегда

- Чтобы просмотреть список событий, раскройте список с названием типа событий.
- Выключите типы событий, которые не должны регистрироваться в журнале.
- Чтобы включить или выключить регистрацию сразу всех типов событий, включите или выключите **Все типы событий**. Флажок с типа обязательных событий **Регистрируются всегда** снять нельзя.
- В разделе **Хранение данных, полученных от устройств**:
  - Для событий, полученных в режиме реального времени (журнал критичных событий в разделе **Инфопанель**):
    - **Срок хранения событий, дни** — события, зарегистрированные ранее указанного срока, удаляются из журнала критичных событий. Рекомендуемое значение — 45 дней. Может принимать значение из диапазона 1–400 дней.
    - **Максимальное количество событий** — максимальное число записей, которое может храниться в журнале критичных событий. Рекомендуемое значение — 50000. Может принимать значение из диапазона 1–100000.
  - Для журналов событий, сформированных по запросу (в разделе **Журналы событий**)
    - **Срок хранения журнала, дни** — журналы, сформированные ранее указанного срока, удаляются из журналов событий. Рекомендуемое значение — 45 дней. Может принимать значение из диапазона 1–400 дней.
  - Для журналов трафика, запрошенных с защищаемых узлов:
    - **Срок хранения журнала, дни** — журналы, запрошенные ранее указанного срока, удаляются из журналов трафика. Рекомендуемое значение — 30 дней. Может принимать значение из диапазона 1–400 дней.

Для возврата измененных параметров сервера к значениям по умолчанию нажмите **По умолчанию**.

# Настройка параметров защищаемых узлов

Вы можете просматривать и настраивать параметры ViPNet EPP Агент, которые будут применяться на защищаемых узлах:

- Период самотестирования ViPNet EPP Агент.
- Период обмена данными между ViPNet EPP Сервер и ViPNet EPP Агент.
- Отслеживание работы антивирусов на защищаемых узлах (см. [Отслеживание работы антивирусов](#)).
- Параметры хранения событий в журналах в ViPNet EPP Агент (журнале событий, журнале трафика и журнале аудита):
  - Срок хранения и максимальное количество записей в каждом журнале.
  - Количество удаляемых записей при достижении максимума.
- Автоматическое подключение новых защищаемых узлов (см. [Настройка автоматического подключения защищаемых узлов](#)).

При переполнении журналов в ViPNet EPP Агент в соответствии с параметрами хранения автоматически удаляются из каждого журнала:

- Записи с истекшим сроком хранения.
- Наиболее старые записи журнала в количестве, указанном в настройках, превышающие максимальное количество хранимых событий.

Также при уменьшении объема свободного места на диске компьютера с ViPNet EPP Агент до 3 Гбайт из каждого журнала удаляются наиболее старые события в количестве  $n^3$ , где  $n$  — значение параметра **Количество удаляемых записей при достижении максимума**.

Информация о переполнении журнала и удалении событий фиксируется в журнале аудита.

Чтобы просмотреть и изменить параметры защищаемых узлов:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Устройства** и на панели сверху нажмите **Настройки устройств**.
- 3 Просмотрите заданные настройки. Вы можете изменить:
  - **Период самотестирования** — промежуток времени, через который автоматически выполняется проверка работоспособности ViPNet EPP Агент (см. [Проверка работоспособности](#)). Можно задать в минутах, секундах или часах. Рекомендуемое значение — 10 минут, но должно быть больше периода обмена данными с EPP-сервером. Может принимать значение из диапазона 20 секунд–24 часа.
  - **Период обмена данными с EPP-сервером** — промежуток времени, через который происходит опрос защищаемых узлов о зарегистрированных событиях информационной безопасности и результатах самотестирования. Можно задать в минутах, секундах или

часах. Рекомендуемое значение — 20 секунд. Может принимать значение из диапазона 20 секунд–24 часа.

- **Следить за антивирусом** — контроль работы антивирусов Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite на защищаемом узле. Если слежение включено, ViPNet EPP Агент может блокировать сетевой трафик защищаемого узла (см. [Отслеживание работы антивирусов](#)). По умолчанию слежение за антивирусом отключено.



**Внимание!** Если на защищаемом узле не установлены Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite, при включении отслеживания работы антивирусов весь сетевой трафик этого узла, кроме трафика между ViPNet EPP Агент и ViPNet EPP Сервер, будет заблокирован.

---

- Параметры хранения записей в журналах (журнале событий, журнале трафика, журнале аудита):
  - **Срок хранения записей, дни** — записи, зарегистрированные ранее указанного срока, удаляются из журналов в ViPNet EPP Агент. Рекомендуемое значение — 45 дней. Может принимать значение из диапазона 1–400 дней.
  - **Максимальное количество записей в каждом журнале** — максимальное число записей, которое может храниться в каждом из журналов в ViPNet EPP Агент. Рекомендуемое значение — 50000. Может принимать значение из диапазона 1–100000.
  - **Количество записей, удаляемых при достижении максимума** — количество записей, которое удаляется из каждого журнала в случае достижения максимального количества хранимых записей. Рекомендуемое значение — 10000. Может принимать значение из диапазона 1–99999, но должно быть меньше максимального числа записей.
- Автоматическое подключение новых защищаемых узлов (см. [Настройка автоматического подключения защищаемых узлов](#))

Для возврата измененных параметров сервера к значениям по умолчанию нажмите **По умолчанию**.

- 4 Если настройки были изменены, нажмите **Сохранить**.

## Управление учетными записями

При установке ViPNet EPP Сервер автоматически создается учетная запись администратора ViPNet EPP (см. [Ролевая модель](#)). Она позволяет подключаться к веб-интерфейсу ViPNet EPP Сервер и выполнять любые настройки, включая создание новых учетных записей и изменение существующих.

Администратор может просматривать, добавлять учетные записи, изменять пароль и удалять учетные записи.

Учетные записи с ролью администратора или аудитора, созданные в ViPNet EPP Сервер, могут быть использованы для подключения к ViPNet EPP Сервер и локально к ViPNet EPP Агент, подключенному к серверу. Для этого после создания учетной записи выполняется синхронизация данных с агентом. Дополнительные учетные записи в ViPNet EPP Агент не отображаются.

С целью смены пароля, вы можете заменить учетную запись администратора или аудитора, созданную локально в ViPNet EPP Агент, на учетную запись, созданную в ViPNet EPP Сервер. Для этого создайте в ViPNet EPP Сервер учетную запись с таким же именем и ролью, что и в ViPNet EPP Агент, и задайте для нее другой пароль. После синхронизации данных подключиться к ViPNet EPP Агент с этой учетной записью можно будет только используя пароль, заданный в ViPNet EPP Сервер. Чтобы в ViPNet EPP Агент для этой учетной записи начал использоваться прежний пароль, удалите аналогичную учетную запись с ViPNet EPP Сервер.

Чтобы просмотреть список учетных записей ViPNet EPP Сервер:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Учетные записи**.

Чтобы на странице **Учетные записи** отсортировать список учетных записей по имени учетной записи, роли или имени пользователя, щелкните соответствующий заголовок таблицы.

Чтобы создать новую учетную запись:

- 1 На странице **Учетные записи** на панели сверху нажмите **Создать учетную запись**.
- 2 В окне **Создание учетной записи**:
  - 2.1 Укажите:
    - **Имя учетной записи**, с помощью которой пользователь будет подключаться к веб-интерфейсу.
    - **Пользователь** — имя пользователя, которое будет отображаться в веб-интерфейсе.
    - **Роль** — полномочия учетной записи: администратор, аудитор (см. [Ролевая модель](#)).
    - **Пароль** — пароль пользователя в соответствии с требованиями (см. [Требования к имени и паролю учетной записи](#)). Чтобы скопировать пароль, справа нажмите .



**Примечание.** Вы можете выключить **Запретить использование ненадежных паролей** и указать любой пароль, но в целях безопасности использовать простые пароли не рекомендуется.

---

## 2.2 Нажмите **Создать**.

Чтобы изменить параметры существующей учетной записи (имя пользователя, имя учетной записи, пароль):

- 1 На странице **Учетные записи** выберите учетную запись в списке.

- 2 Справа нажмите  > **Изменить**. Внесите изменения.
- 3 Нажмите **Сохранить**.

Чтобы удалить учетную запись:

- 1 На странице **Учетные записи** выберите учетную запись в списке. Удаление единственной учетной записи администратора недоступно.
- 2 Справа нажмите  > **Удалить** и подтвердите удаление.

## Требования к имени и паролю учетной записи

При создании имени учетной записи разрешено использовать:

- прописные буквы латинского алфавита от A до Z;
- строчные буквы латинского алфавита от a до z;
- десятичные цифры от 0 до 9;
- символы !@#\$%^&\*()\_+=;:'",.<>/?\|`~[]{}.

Имя учетной записи должно начинаться с прописной или строчной буквы и не должно содержать пробелы. Максимальная длина имени учетной записи — 32 символа.

При создании или изменении пароля учетной записи, стойкого к попыткам подбора, соблюдайте требования:

- Минимальная длина — 8 символов.
- Максимальная длина — 32 символа.
- Любые идущие подряд три символа пароля не должны совпадать с частью имени учетной записи.
- Один и тот же символ не должен встречаться более двух раз.
- В пароле должны одновременно присутствовать символы четырех категорий:
  - прописные буквы латинского алфавита от A до Z;
  - строчные буквы латинского алфавита от a до z;
  - десятичные цифры от 0 до 9;
  - символы !@#\$%^&\*()\_+=;:'",.<>/?\|`~[]{}.

## Проверка работоспособности и контроль целостности

Для контроля работоспособности в ViPNet EPP Сервер выполняются:

- Контроль целостности критичных файлов ПО ViPNet EPP. Выполняется при старте компонентов ViPNet EPP Сервер (сервера управления и рабочих серверов) и периодически в процессе работы. При обнаружении нарушения целостности сервера управления, подключение к ViPNet EPP Сервер будет невозможно. При нарушении целостности рабочего сервера, будет невозможен его запуск. Данные о нарушении целостности также будут записаны в служебные диагностические журналы. При возникновении ошибок целостности важных файлов ПО ViPNet EPP Сервер становится неработоспособным. Для восстановления работоспособности выполните восстановление ViPNet EPP Сервер (см. [Восстановление или удаление компонентов ViPNet EPP Сервер](#)).
- Контроль целостности журналов аудита, журналов событий, целостность базы данных. Выполняется при самотестировании ViPNet EPP.

Самотестирование выполняется отдельно для сервера управления и для рабочих серверов. Самотестирование запускается автоматически при запуске программы и периодически по расписанию (по умолчанию — каждые 10 минут). Периодичность запуска самотестирования можно изменять.

Администратор ViPNet EPP может запустить самотестирование вручную.

Запуск, завершение и результаты самотестирования регистрируются в журнале аудита ViPNet EPP Сервер (см. [Журналы аудита](#)).

Если в результате самотестирования были выявлены проблемы, раздел  **Серверы безопасности** будет отмечен желтым маркером .

Администратору доступен просмотр отчета о результатах последнего самотестирования:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Чтобы посмотреть отчет для сервера управления, выберите  **Серверы безопасности > Сервер управления**.
- 3 Чтобы посмотреть отчет для рабочего сервера, выберите  **Серверы безопасности > Рабочие серверы**, выберите рабочий сервер.

Отчет отображается в разделе **Самотестирование** и содержит:

- Результат:
  - **ОК** — проблем не обнаружено.
  - **Проблема** — выявлены проблемы. Выше будет перечислен перечень проблем.
- Дата и время проведения самотестирования.

Чтобы запустить самотестирование сервера управления или рабочего сервера вручную:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Чтобы запустить самотестирование сервера управления, выберите  **Серверы безопасности > Сервер управления** и в разделе **Самотестирование** нажмите **Запустить самотестирование**.

3 Чтобы запустить самотестирование рабочего сервера, выберите  **Серверы безопасности > Рабочие серверы:**

3.1 Выберите рабочий сервер. Сервер должен быть в активном статусе.

3.2 На правой панели в разделе **Самотестирование** нажмите **Запустить самотестирование**.

После завершения самотестирования появится уведомление о результате. Последние результаты самотестирования отобразятся в разделе **Самотестирование**.

---

**Внимание!** Если целостность журнала аудита нарушена, например в случае аппаратного сбоя:



- 1 Остановите службы сервера.
- 2 Удалите испорченную базу данных.
- 3 Выполните настройку параметров и инициализацию базы данных ViPNet EPP Сервер, как [при установке](#).
- 4 Перезапустите службы сервера управления и рабочего сервера, последовательно выполнив команды:

```
sudo systemctl restart epp2-main-server.service  
sudo systemctl restart epp2-worker-server.service
```

---

## Диагностические журналы

В процессе работы в ViPNet EPP ведутся диагностические журналы, где сохраняется информация о работе модулей и подсистем ViPNet EPP. Диагностические журналы позволяют специалистам ИнфоТеКС разбираться в причинах неполадок в работе ПО ViPNet EPP.

Диагностические журналы сохраняются в `/opt/epp2/log/`.

## Обновление лицензии

В некоторых случаях необходимо обновить существующую лицензию, например для продления срока действия лицензии или увеличения количества защищаемых узлов. Для получения новой лицензии следует обратиться в ИнфоТеКС (см. [Обратная связь](#)).

После получения лицензии обновите ее:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Лицензирование** и нажмите **Установить другую лицензию**.
- 3 Выберите файл новой лицензии формата `itcslic`.
- 4 Просмотрите новую лицензию и нажмите **Установить**.

После обновления на странице **Лицензирование** отобразится информация о новых параметрах лицензии.



**Внимание!** Убедитесь в том, что установлены параметры новой лицензии, например изменился срок действия лицензии или увеличилось число защищаемых узлов.

---

- 5 Если потребуется, выполните активацию новой лицензии аналогично сценарию установки и активации лицензии (см. [Установка и активация лицензии](#)).

# Интеграция с внешними системами

## Передача уведомлений по электронной почте

ViPNet EPP поддерживает передачу уведомлений о зарегистрированных событиях на защищаемых узлах по электронной почте. Например, вы можете оповещать сотрудников, ответственных за информационную безопасность подразделений, к которым относятся защищаемые узлы.

Взаимодействие с внешними системами происходит через рабочий сервер.

По умолчанию передача событий отключена.

Чтобы настроить уведомления о событиях по электронной почте:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 [Настройте подключение ViPNet EPP к почтовому серверу, рассылающему уведомления.](#)
- 3 Выберите  **Передача данных.**
- 4 На вкладке **Электронная почта** включите  **Передача событий устройств на электронную почту.**

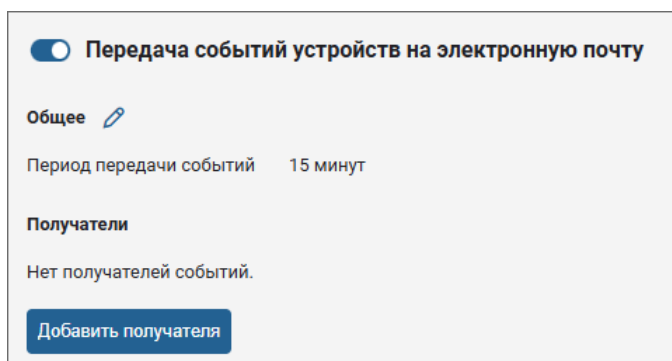


Рисунок 39. Настройка передачи уведомлений по электронной почте

- 5 Настройте период рассылки уведомлений по электронной почте:
  - 5.1 Нажмите  в разделе **Общее.**
  - 5.2 В поле **Период отправки сообщений, минуты** укажите период (рекомендуется — 15 минут).
  - 5.3 Нажмите **Сохранить.**
- 6 Добавьте получателя уведомления:
  - 6.1 Нажмите **Добавить получателя** в разделе **Получатели.**

6.2 Введите адрес электронной почты получателя.

6.3 Выберите устройства или группы защищаемых узлов, при регистрации событий на которых необходимо оповещать получателя.

6.4 Выберите флажками уровни и типы событий, при регистрации которых необходимо оповещать получателя.

6.5 Нажмите **Добавить**.

Вы можете добавить несколько получателей и указать для них разные устройства и параметры событий.

Чтобы изменить данные о получателе, нажмите  и выберите **Изменить**.

Чтобы удалить получателя из списка, нажмите  и выберите **Удалить**.

Если вы отключите  передачу событий по электронной почте, ViPNet EPP сохранит текущие настройки передачи.

## Подключение к почтовому серверу

Уведомления о событиях по электронной почте рассылает почтовый сервер, поэтому необходимо настроить подключение рабочего сервера к нему:

6.1 Выберите  **Сетевые настройки**.

6.2 В разделе **Подключение к почтовому серверу** нажмите **Настроить**.

6.3 В полях **Адрес SMTP-сервера** и **Порт** укажите адрес и порт (по умолчанию — 587) почтового сервера.

6.4 В полях **Учетная запись** и **Пароль** укажите параметры доступа к электронному почтовому ящику, от имени которого будет осуществляться рассылка уведомлений.

6.5 В поле **Электронная почта отправителя** укажите электронный адрес, от имени которого будет осуществляться рассылка уведомлений.

6.6 Для защищенной передачи уведомлений по криптографическим протоколам SSL/TLS выберите **Использовать TLS-соединение**.

6.7 Чтобы проверить правильность введенных данных, отправьте тестовое письмо. Для этого в поле **Электронная почта получателя** введите электронный адрес и нажмите **Отправить сообщение**.

Почтовый сервер отправит тестовое сообщение на указанный адрес получателя от имени указанного адреса отправителя.

6.8 Нажмите **Сохранить**.

Чтобы удалить соединение рабочего сервера с почтовым сервером, в настройках подключения нажмите **Сбросить**. При этом ViPNet EPP остановит передачу уведомлений по электронной почте, даже если она включена.

# Передача событий информационной безопасности в сторонние системы

В ViPNet EPP поддерживается передача зарегистрированных событий информационной безопасности в сторонние системы мониторинга и анализа ([SIEM](#), ViPNet TIAS и другие) с помощью прикладного протокола [Syslog](#). События передаются в виде текстовых CEF-сообщений (см. [Структура CEF-сообщения](#)). В зависимости от транспортного протокола, используемого в Syslog, вы можете настроить передачу событий в сторонние системы:

- По протоколу UDP — [в любую стороннюю систему, поддерживающую протокол UDP, и ViPNet TIAS](#).
- По протоколу TCP — [только в ViPNet TIAS](#) любой из актуальных версий (см. [Совместимость со сторонним программным обеспечением](#)).

События могут передаваться в две сторонние системы по протоколам UDP и TCP одновременно. Например, вы можете настроить передачу событий в разные системы в зависимости от типов правил.

В ViPNet EPP Сервер for Linux взаимодействие с внешними системами происходит через рабочий сервер.

По умолчанию передача событий отключена.

## Передача событий в сторонние системы по протоколу UDP

Чтобы настроить передачу событий в стороннюю систему по протоколу UDP:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора.
- 2 Выберите  **Передача данных**.
- 3 На вкладке **Syslog** включите  **Передача событий по протоколу Syslog**.
- 4 Нажмите **Настроить**.
- 5 Укажите IP-адрес и UDP-порт сервера Syslog.
- 6 Чтобы проверить доступность сервера Syslog, нажмите **Проверить соединение**. Тестовое сообщение будет отправлено на сервер Syslog.
- 7 [Выберите устройства или группы защищаемых узлов](#), при регистрации событий на которых необходимо оповещать получателя.
- 8 Выберите флажками уровни и типы событий, при регистрации которых необходимо оповещать получателя.
- 9 Нажмите **Сохранить**.
- 10 [Скопируйте идентификатор ViPNet EPP Сервер](#). Сообщите администратору сторонней системы IP-адрес и идентификатор ViPNet EPP Сервер.

Вы можете изменить настройки передачи. Для этого нажмите  напротив заголовка **Передача событий по протоколу Syslog**.

Если вы отключите  передачу событий, ViPNet EPP сохранит текущие настройки передачи.

## Передача событий в ViPNet TIAS

Чтобы настроить передачу событий в ViPNet TIAS по протоколу TCP:

- 1 Подключитесь к веб-интерфейсу ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
- 2 Выберите  **Передача данных**.
- 3 На вкладке **TIAS** включите  **Передача событий на сервер ViPNet TIAS**.
- 4 Укажите IP-адрес сервера ViPNet TIAS.



**Внимание!** По умолчанию сервер ViPNet TIAS использует TCP-порт 34349. Не изменяйте его без указания администратора ViPNet TIAS.

- 5 Чтобы проверить доступность сервера ViPNet TIAS, нажмите **Проверить соединение**. Тестовое сообщение будет отправлено на сервер Syslog.
- 6 Выберите устройства или группы защищаемых узлов, при регистрации событий на которых необходимо оповещать получателя.
- 7 Выберите флажками уровни и типы событий, при регистрации которых необходимо оповещать получателя.
- 8 Нажмите **Сохранить**.
- 9 Скопируйте идентификатор ViPNet EPP Сервер (рабочего сервера). Сообщите администратору ViPNet TIAS IP-адрес и идентификатор ViPNet EPP Сервер.

Вы можете изменить настройки передачи. Для этого нажмите  напротив заголовка **Передача событий на сервер ViPNet TIAS**.

Если вы отключите  передачу событий, ViPNet EPP сохранит текущие настройки передачи.

## Выбор защищаемых узлов при настройке передачи событий

ViPNet EPP оповещает только о событиях на тех устройствах, которые были указаны при настройке передачи данных. Вы можете указать как конкретные устройства, так и группы защищаемых узлов. Для этого при настройке передачи событий:

- 1 Нажмите  в разделе **События устройств**.

2 Чтобы оповещать о событиях на всех защищаемых узлах, выберите **Все подключенные устройства**.

3 Чтобы оповещать о событиях на некоторых узлах:

3.1 Выберите **Выбранные устройства**.

В списке отображаются все группы защищаемых узлов.

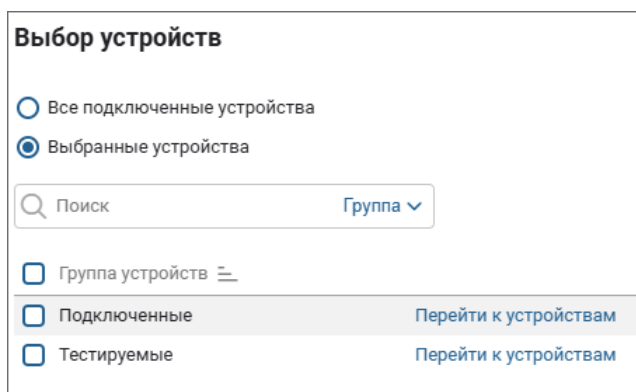


Рисунок 40. Выбор устройств

3.2 Чтобы выбрать группу защищаемых узлов, отметьте флажком ее в списке.

При этом ViPNet EPP будет оповещать о событиях на всех узлах из этой группы.

Вы можете найти группу по ее имени. Для этого в  поле для поиска выберите **Группа** и начните вводить имя группы.

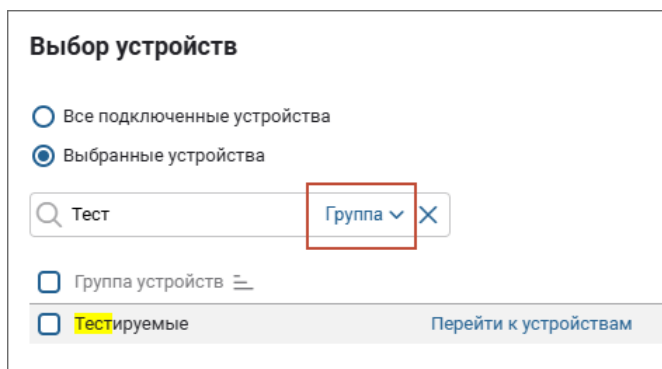
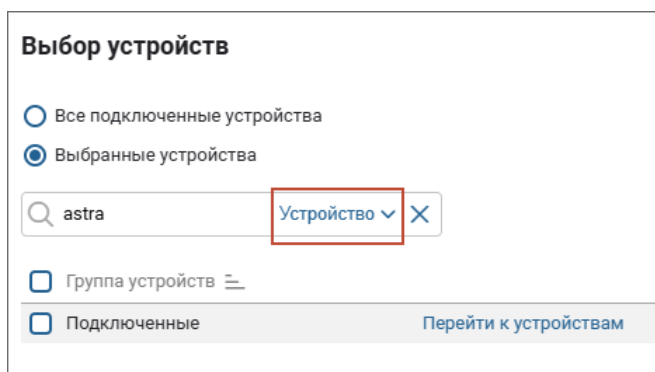


Рисунок 41. Поиск группы защищаемых узлов по имени

3.3 Чтобы выбрать защищаемый узел:

3.3.1 Нажмите **Перейти к устройствам** в строке группы, к которой относится узел.

Если вы не знаете к какой группе относится узел, воспользуйтесь поиском. Для этого в  поле для поиска выберите **Устройство** и начните вводить имя устройства. Результатом будет группа, к которой относится защищаемый узел.



**Выбор устройств**

☐ Все подключенные устройства

☒ Выбранные устройства

**Устройство** 

☐ Группа устройств 

☒ Подключенные [Перейти к устройствам](#)

Рисунок 42. Поиск защищаемого узла по его имени

3.3.2 Найдите устройство в списке и отметьте его флажком.

3.3.3 Нажмите **Сохранить**.

4 Нажмите **Сохранить**.

# 4

## Локальное управление в ViPNet EPP Агент

|                                                     |     |
|-----------------------------------------------------|-----|
| Способы управления                                  | 177 |
| Управление с помощью графической консоли управления | 178 |
| Управление с помощью командного интерпретатора      | 220 |

# Способы управления

Для локального управления в ViPNet EPP Агент предусмотрены следующие средства:

- [Графическая консоль](#) — основное средство локального управления ViPNet EPP Агент.
- [Командный интерпретатор](#) — вспомогательное средство управления. Вы можете использовать его для изменения [списка контролируемых сетевых интерфейсов](#). В командном интерпретаторе недоступна часть возможностей графической консоли:
  - Для агента под управлением сервера недоступны:
    - Настройка типов регистрируемых событий в журнале аудита.
    - Просмотр журнала событий обнаружения и предотвращения вторжений.
    - Блокирование и разблокирование трафика из журнала трафика.
  - Для автономного агента недоступны:
    - Загрузка и активация лицензии.
    - Загрузка и экспорт базы правил.
    - Управление правилами обнаружения вторжений (HIDS).
    - Управление сетевыми правилами предотвращения вторжений (HIDS).
    - Настройка критериев обнаружения аномалий.
    - Настройка параметров работы агента.
    - Просмотр журнала событий обнаружения и предотвращения вторжений.
    - Блокирование и разблокирование трафика из журнала трафика.

# Управление с помощью графической консоли управления

## Подключение к ViPNet EPP Агент

ViPNet EPP Агент запускается автоматически при загрузке ОС. Чтобы подключиться к ViPNet EPP Агент и запустить графическую консоль управления:

- 1 В меню **Пуск** начните вводить **ViPNet EndPoint Protection** и запустите найденную программу.



**Примечание.** Графическую консоль управления можно также запустить из командной строки, для этого выполните команду: `/opt/epp-agent/bin/epp_gui`

---

- 2 В окне аутентификации введите параметры входа в ViPNet EPP Агент:
  - Введите имя пользователя и пароль вашей учетной записи.  
При первом запуске после установки ViPNet EPP Агент войдите с учетной записью администратора агента по умолчанию: имя учетной записи — `admin`, пароль — `admin`.
  - Чтобы при последующем запуске ViPNet EPP Агент не вводить имя пользователя и пароль учетной записи, выберите **Запомнить меня**.

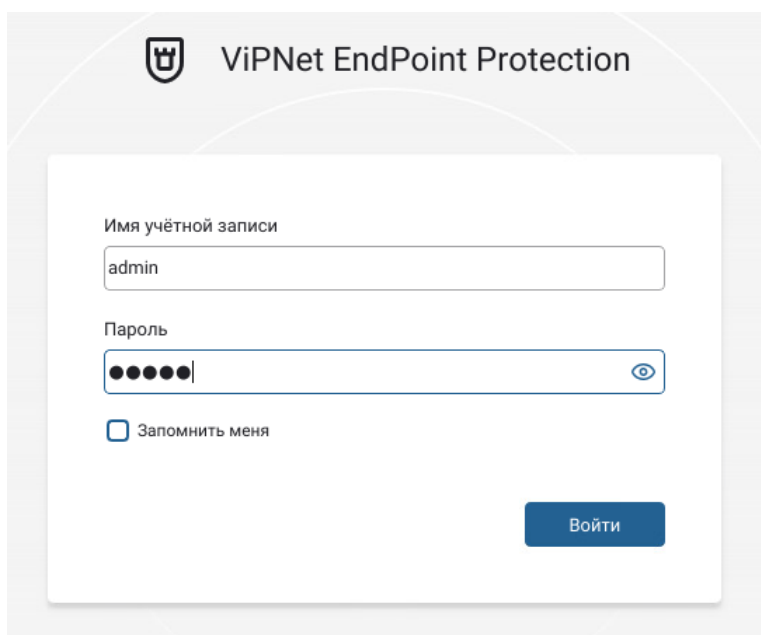


Рисунок 43. Подключение к ViPNet EPP Агент

- 3 Нажмите **Войти**.



**Внимание!** Если вы три раза подряд введете неверные данные учетной записи, возможность входа в ViPNet EPP Агент будет заблокирована на три минуты.

---

- 4 При первом подключении пользователя смените пароль учетной записи. Для этого в окне **Смена пароля учетной записи** введите новый пароль пользователя в соответствии с требованиями (см. [Требования к имени и паролю учетной записи](#)). Новый пароль должен отличаться от предыдущего.
- 



**Примечание.** Вы можете выбрать **Не применять требования к сложности пароля** и указать любой пароль, отличающийся от предыдущего, но в целях безопасности использовать простые пароли не рекомендуется.

---

Нажмите **Готово**.

- 5 При первом запуске после установки ознакомьтесь с лицензионным соглашением. В случае согласия выберите **Принимаю условия лицензионного соглашения** и нажмите **Продолжить**.

При успешной аутентификации в главном окне ViPNet EPP Агент пользователю будут доступны действия согласно его полномочиям (см. [Полномочия пользователей](#)).

При первом запуске защита будет отключена, в зависимости от способа работы ViPNet EPP Агент:

- Для ViPNet EPP Агент под управлением сервера — до подключения к ViPNet EPP Сервер, получения лицензии и получения базы правил (см. [Подключение защищаемых узлов](#)).
- Для автономного ViPNet EPP Агент — до загрузки и активации лицензии и загрузки базы правил.

# Интерфейс ViPNet EPP Агент

На рисунке ниже в качестве примера представлено главное окно ViPNet EPP Агент под управлением сервера пользователя с максимальными полномочиями администратора агента.

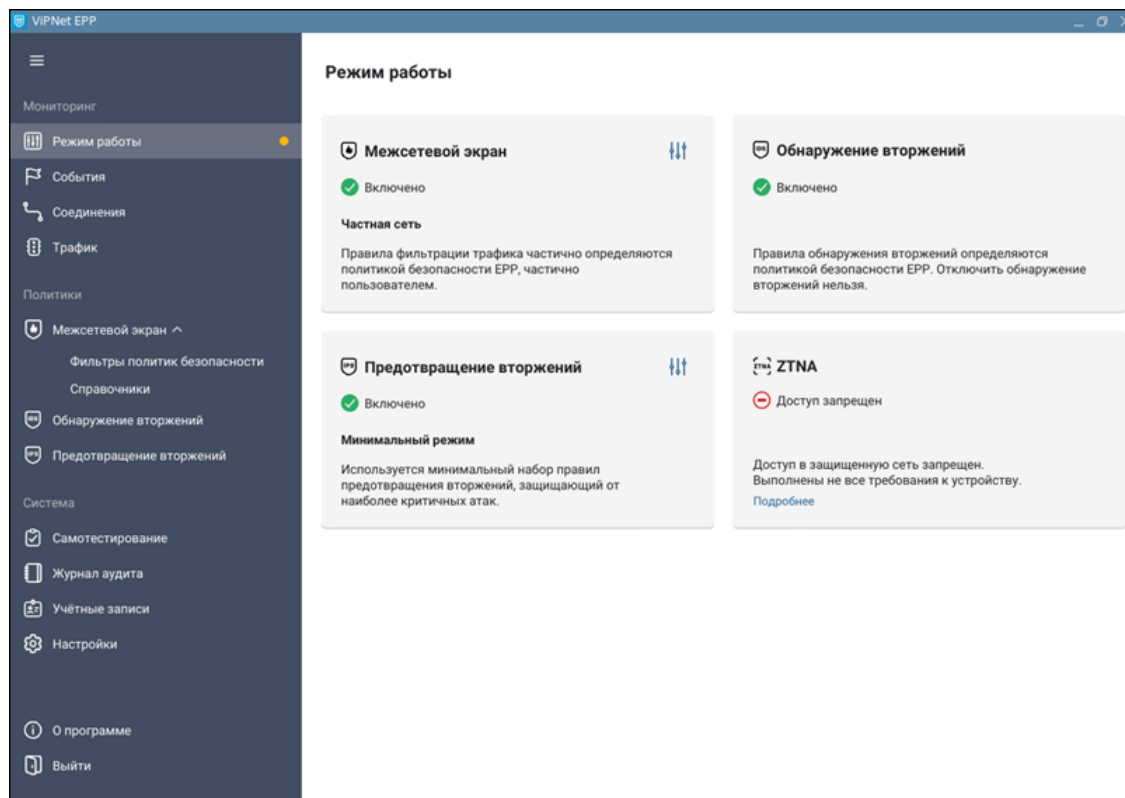


Рисунок 44. Главное окно ViPNet EPP Агент под управлением сервера

Для оптимального отображения интерфейса установите разрешение экрана не менее 1440 на 900 пикселей.

Панель слева содержит разделы настройки ViPNet EPP Агент и просмотра результатов его работы:

-  **Режимы работы** — [просмотр и настройка режимов работы модулей защиты](#).
-  **События** — просмотр зарегистрированных событий на защищаемом узле (см. [Журнал событий](#)).
-  **Соединения** — просмотр журнала активных соединений защищаемого узла (см. [Журнал активных соединений](#)).
-  **Трафик** — просмотр журнала регистрации трафика (см. [Журнал трафика](#)).
-  **Межсетевой экран** — управление фильтрацией трафика на защищаемом узле (см. [Управление фильтрацией трафика](#)).
-  **Обнаружение вторжений** — управление обнаружением вторжений на защищаемом узле (см. [Просмотр и настройка правил обнаружения вторжений \(HIDS\)](#)).

-  **Предотвращение вторжений** — управление предотвращением вторжений на защищаемом узле (см. [Просмотр и настройка сетевых правил предотвращения вторжений \(HIPS\)](#)).
-  **Обнаружение аномалий** — доступно только в автономном ViPNet EPP Агент. [Настройка критериев обнаружения аномалий](#).
-  **Импорт и экспорт базы правил** — доступно только в автономном ViPNet EPP Агент. Загрузка и выгрузка базы правил (см. [Управление базой правил](#)).
-  **Самотестирование** — проверка работоспособности ViPNet EPP Агент (см. [Проверка работоспособности](#)).
-  **Журнал аудита** — просмотр журнала аудита ViPNet EPP Агент (см. [Журнал аудита](#)).
-  **Учетные записи** — управление учетными записями ViPNet EPP Агент (см. [Управление учетными записями](#)).
-  **Настройки** — просмотр и настройка параметров работы ViPNet EPP Агент (см. [Просмотр и настройка параметров работы](#)).
-  **О программе** — версия программного обеспечения ViPNet EPP, контактные данные ИнфоТеКС, состояние лицензии и текст лицензионного соглашения (см. [Просмотр сведений о программе и лицензии](#)). Для автономного ViPNet EPP Агента — [установка и активация лицензии](#).
-  **Выйти** — завершение сеанса работы с ViPNet EPP Агент.

## Установка и активация лицензии

Установка и активация лицензии доступны только в автономном ViPNet EPP Агент.

При первом подключении к автономному ViPNet EPP Агент необходимо установить и активировать лицензию ViPNet EPP:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **О программе > Лицензия**.
- 3 Нажмите **Загрузить лицензию**, выберите файл лицензии формата `itcslic` и нажмите **Загрузить**.  
  
После загрузки лицензии на вкладке отобразится информация о лицензии. Статус лицензии: **Лицензия не активирована**. Тип лицензии: **Автономная**.
- 4 Нажмите **Активировать лицензию** и активируйте лицензию одним из способов:
  - Онлайн-активация (необходим доступ в интернет) — выберите **Онлайн** и нажмите **Далее**.
  - С помощью запроса на активацию:

4.1.1 Выберите **Без доступа к сети интернет** > **Скачать файл с запросом на активацию**.

4.1.2 Нажмите **Скачать файл с запросом** и сохраните файл запроса. Нажмите **Заккрыть**.

4.1.3 Отправьте письмо с файлом запроса на электронный адрес [reg@infotecs.ru](mailto:reg@infotecs.ru).

Дождитесь ответного письма — в нем будет указан регистрационный код для активации ViPNet EPP.

4.1.4 Нажмите **Активировать лицензию** и выберите **Без доступа к сети интернет** > **Ввести код регистрации и активировать**.

4.1.5 В окне **Активация лицензии** введите код регистрации из ответного письма, нажмите **Активировать лицензию**.

4.1.6 Нажмите **Заккрыть**.

При успешной активации в строке **Статус** появится **Лицензия активирована**.

## Управление базой правил

Управление базой правил доступно только в автономном ViPNet EPP Агент.

### Загрузка и обновление базы правил

Чтобы в автономном ViPNet EPP Агент были включены модули защиты, должна быть загружена база правил. По умолчанию после установки ViPNet EPP Агент база правил не загружена. Вы можете загрузить ее только вручную из следующих источников:

- из комплекта поставки;
- с сервера обновлений, предварительно скачав базу правил с сервера обновлений (при наличии подписки на обновление базы правил);
- экспортированную с другого автономного ViPNet EPP Агент for Linux. Загрузка базы правил, экспортированной с автономного ViPNet EPP Агент for Windows, недоступна.

ViPNet EPP Агент может использовать только одну базу правил. Вы можете обновить установленную базу правил, загрузив новую базу правил и указав правила обновления параметров установленной базы правил.



**Совет.** Для скачивания обновлений базы правил с сервера обновлений рекомендуется использовать выделенный компьютер с доступом в интернет, не подключенный к защищаемой сети; перенос файла обновления базы правил на компьютер ViPNet EPP Серверная консоль следует выполнять с помощью USB-носителя.

---

Чтобы с сервера обновлений скачать файл с архивом обновления базы правил и сохранить на USB-носитель:

- 1 На компьютере с доступом к интернету запустите веб-браузер и в адресной строке введите `https://updateids.infotecs.ru`.
- 2 Введите имя и пароль своей учетной записи для входа на сервер обновлений.

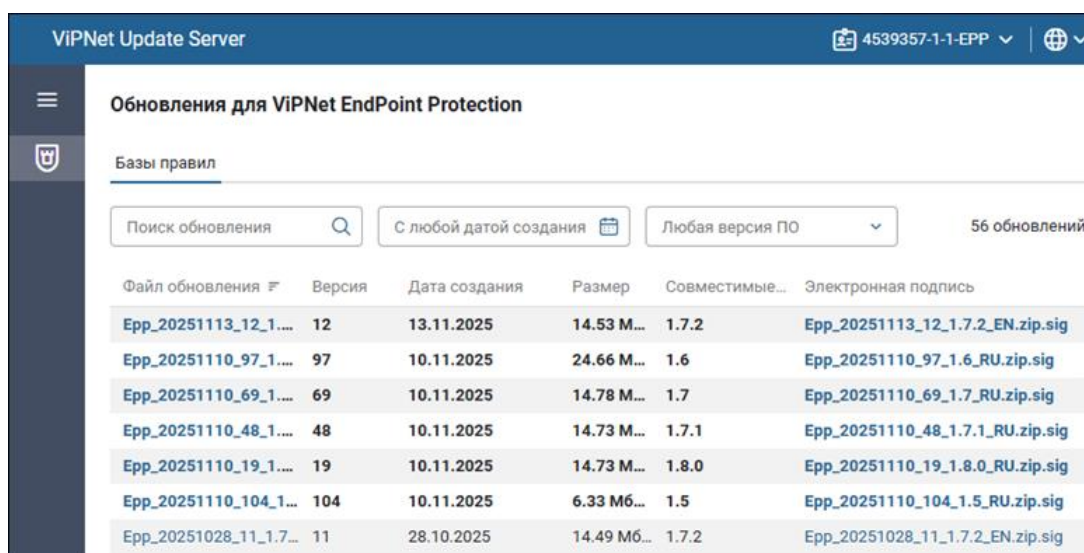


**Примечание.** Имя и пароль учетной записи для входа на сервер обновлений указаны в PDF-файле лицензии на ViPNet EPP.

- 3 Выберите  **ViPNet EndPoint Protection > Базы правил.**
- 4 В списке обновлений найдите последнее по дате создания обновление базы правил, совместимое с используемой у вас версией ViPNet EPP.
- 5 Щелкните файл обновления в одноименном столбце. Файл с обновлением будет сохранен на компьютер.



**Примечание.** Последнее обновление базы правил содержит актуальные настройки и правила, поэтому более ранние обновления базы правил скачивать не требуется.



| Файл обновления        | Версия | Дата создания | Размер      | Совместимые... | Электронная подпись              |
|------------------------|--------|---------------|-------------|----------------|----------------------------------|
| Epp_20251113_12_1...   | 12     | 13.11.2025    | 14.53 М...  | 1.7.2          | Epp_20251113_12_1.7.2_EN.zip.sig |
| Epp_20251110_97_1...   | 97     | 10.11.2025    | 24.66 М...  | 1.6            | Epp_20251110_97_1.6_RU.zip.sig   |
| Epp_20251110_69_1...   | 69     | 10.11.2025    | 14.78 М...  | 1.7            | Epp_20251110_69_1.7_RU.zip.sig   |
| Epp_20251110_48_1...   | 48     | 10.11.2025    | 14.73 М...  | 1.7.1          | Epp_20251110_48_1.7.1_RU.zip.sig |
| Epp_20251110_19_1...   | 19     | 10.11.2025    | 14.73 М...  | 1.8.0          | Epp_20251110_19_1.8.0_RU.zip.sig |
| Epp_20251110_104_1...  | 104    | 10.11.2025    | 6.33 Мб...  | 1.5            | Epp_20251110_104_1.5_RU.zip.sig  |
| Epp_20251028_11_1.7... | 11     | 28.10.2025    | 14.49 Мб... | 1.7.2          | Epp_20251028_11_1.7.2_EN.zip.sig |

Рисунок 45. Главная страница сервера обновлений ViPNet Update Server

- 6 Скопируйте файл с архивом обновления на USB-носитель.

Чтобы загрузить в ViPNet EPP Агент базу правил:

- 1 Подключите к компьютеру USB-носитель с архивом обновления базы правил.
- 2 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 3 Выберите  **Импорт и экспорт базы правил.**
- 4 Если база правил загружается впервые:

4.1 Нажмите **Загрузить базу правил** и выберите на USB-носителе файл с архивом обновления базы правил. База правил должна быть совместима с установленной у вас версией ViPNet EPP.

4.2 Нажмите **Загрузить**.

4.3 Дождитесь завершения импорта базы правил. Нажмите **Заккрыть**.

5 Если в ViPNet EPP Агент уже была загружена база правил:

5.1 Нажмите **Загрузить новую базу правил** и выберите на USB-носителе файл с архивом обновления базы правил. База правил должна быть совместима с установленной у вас версией ViPNet EPP.

5.2 В разделе **Настройки загрузки** укажите, какие параметры установленной базы правил нужно заменить параметрами загружаемой базы правил, а какие параметры оставить без изменения:

- Для режимов работы модулей, правил обнаружения вторжений, правил предотвращения вторжений, настроек агента выберите: заменить или не загружать из новой базы правил.
- Для сетевых фильтров и справочников межсетевого экрана выберите:
  - Заменить, не загружать из новой базы правил, добавить новые сетевые фильтры после существующих или добавить новые сетевые фильтры до существующих, в зависимости от приоритета.
  - Загружать ли новые справочники, не используемые в импортируемых сетевых фильтрах. Справочники, используемые в импортируемых сетевых фильтрах, импортируются всегда.
- Для правил обнаружения аномалий выберите: заменить, добавить новые правила после существующих или не загружать настройки из новой базы правил.

5.3 Нажмите **Загрузить**.

5.4 Дождитесь завершения импорта базы правил. Нажмите **Заккрыть**.

После успешного импорта информация о базе правил отобразится на странице **Импорт и экспорт базы правил**:

- Версия базы правил.
- Дата и время создания и изменения базы правил.
- Источник получения базы правил (комплект поставки или сервер обновлений).

Если база правил была отредактирована пользователем, дополнительно будет указано — **отредактированная**.

- Имя файла обновления.

## Распространение настроек модулей защиты на другие агенты

Если модули защиты и параметры работы нескольких агентов должны быть настроены однотипно, вы можете выполнить настройки на одном агенте и распространить их на другие агенты:

- 1 На одном из защищаемых компьютеров [загрузите базу правил](#) и настройте модули защиты:
  - [Управление фильтрацией трафика](#).
  - [Управление обнаружением и предотвращением вторжений](#).
  - Настройка критериев обнаружения аномалий (автономный агент) (см. [Настройка критериев обнаружения аномалий](#)).
- 2 Настройте параметры работы (см. [Просмотр и настройка параметров работы](#)).
- 3 Экспортируйте базу правил с агента.
- 4 Загрузите экспортированную базу правил на другие агенты.

### Экспорт базы правил

Вы можете экспортировать настроенную базу правил с автономного ViPNet EPP Агент, например для последующего импорта на другие автономные ViPNet EPP Агент.

По умолчанию база правил экспортируется в архив `ViPNet_EPP_AgentLin_RuleBase_v<номер версии базы правил>_<дата экспорта>.zip`.

Чтобы экспортировать базу правил с ViPNet EPP Агент:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Импорт и экспорт базы правил**.
- 3 Нажмите **Скачать базу правил**, укажите папку сохранения и имя файла архива базы правил в формате ZIP. Нажмите **Открыть**.
- 4 Дождитесь завершения экспорта базы правил. Нажмите **Заккрыть**.

## Просмотр и настройка режимов работы модулей защиты

Вы можете отслеживать на защищаемом узле режимы работы модулей защиты:

- [межсетевого экрана](#);
- [обнаружения вторжений](#);
- [предотвращения вторжений](#);
- [политики ZTNA](#) (только при работе ViPNet EPP Агент под управлением сервера).

Для учета особенностей фильтрации IP-пакетов и предотвращения вторжений на защищаемом узле режимы работы можно изменить. Обнаружение вторжений работает всегда, изменить режим работы или отключить его нельзя.



**Примечание.** Мы не рекомендуем отключать предотвращение вторжений.

---

При автономной работе ViPNet EPP Агент режим межсетевого экрана **Публичная сеть** не используется и не отображается.

Для политики ZTNA доступен только просмотр статуса выполнения. При невыполнении политики ZTNA доступен просмотр списка правил, которым не соответствует защищаемый узел.

Чтобы просматривать и управлять режимами работы модулей защиты:

**1** Подключитесь к ViPNet EPP Агент:

- для просмотра — с любыми полномочиями;
- для управления — с полномочиями администратора или аудитора агента.

**2** Выберите  **Режим работы.**

**3** Просмотрите режимы работы модулей защиты на виджетах. Модули защиты могут быть отмечены индикаторами:

-  **Включено** — модуль защиты работает в соответствии с указанным режимом.  
Для виджета ZTNA индикатор означает, что защищаемый узел прошел проверку в соответствии со всеми правилами политики ZTNA, заданными на сервере. Если на защищаемом узле установлена программа ViPNet Client 5 (ViPNet Client 4U), доступ к защищенной сети ViPNet будет разрешен.
-  **Отключено** — модуль защиты отключен и никак не влияет на защищаемый узел.  
Если отключен межсетевой экран, на защищаемом узле с ViPNet Client 5 (ViPNet Client 4U) не будет блокироваться доступ к защищенной сети ViPNet при невыполнении политики ZTNA. При отключении межсетевого экрана в ViPNet EPP Агент под управлением сервера проверка выполнения настроенной политики ZTNA будет продолжена, при этом на защищаемом узле с ViPNet Client 5 (ViPNet Client 4U) не будет блокироваться доступ к защищенной сети ViPNet при невыполнении политики ZTNA.
-  **Не выполняется** — только для виджета ZTNA. Защищаемый узел не прошел проверку по заданным правилам политики ZTNA. Нажмите **Подробнее**, чтобы посмотреть правила, параметрам которых не соответствует защищаемый узел. Если на защищаемом узле установлена программа ViPNet Client 5 (ViPNet Client 4U) и включен межсетевой экран, доступ к ресурсам защищенной сети ViPNet будет заблокирован или ограничен.

При наличии данных об исключениях из политики ZTNA, в списке будут перечислены узлы защищенной сети ViPNet, к которым доступ сохранен.

Данные о заблокированном трафике можно найти в [журнале трафика](#) по названию фильтра **Невыполнение политик ZTNA**.

- 4 Чтобы сменить режим работы межсетевого экрана или предотвращения вторжений, на виджете с названием модуля защиты нажмите :

4.1 Убедитесь, что модуль защиты включен  и выберите режим работы.

4.2 Чтобы отключить модуль защиты, выберите . Если модуль защиты отключен, режимы не действуют.

При отключении межсетевого экрана в ViPNet EPP Агент под управлением сервера будут отключены также проверки выполнения политики ZTNA.

При отключении предотвращения вторжений сетевые правила HIPS применяться не будут.

4.3 Нажмите **Сохранить**.

Чтобы посмотреть режимы работы в области уведомлений панели задач ОС GNU/Linux, щелкните значок ViPNet EPP Агент.

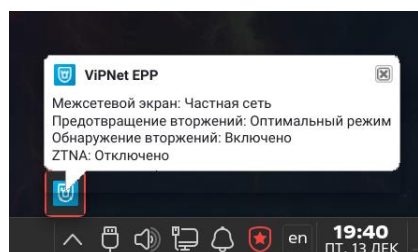


Рисунок 46. Просмотр режимов работы в области уведомлений

## Управление фильтрацией трафика

### Настройка пользовательских сетевых фильтров

Сетевые фильтры межсетевого экрана ViPNet EPP Агент (см. [Межсетевой экран](#)) применяются на защищаемом узле для обработки IP-пакетов трафика. Для настройки на защищаемом узле доступны только сетевые фильтры из раздела **Пользовательские фильтры**. Для учета особенностей фильтрации IP-пакетов на защищаемом узле вы можете для режимов частной и корпоративной сетей изменять, удалять существующие фильтры и добавлять новые.

Если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5, вы можете создать пользовательские сетевые фильтры защищенной сети ViPNet.

Чтобы создать и настроить пользовательский сетевой фильтр открытой сети (не относящегося к защищенной сети ViPNet):

- 1 Подключитесь к ViPNet EPP Агент с учетной записью администратора агента.

- 2 Выберите  **Межсетевой экран** > **Фильтры политик безопасности**.
- 3 Выберите вкладку режима (**Частная сеть** или **Корпоративная сеть**), в котором будет использоваться создаваемый фильтр.
- 4 Выберите **Создать фильтр** > версия IP-протокола в фильтре (**IPv4** или **IPv6**) и настройте фильтр:

---

**Примечание.** Если вы будете настраивать фильтры для IPv6-адресов, для их корректной работы:



- 1 Создайте справочник протоколов ICMPv6 с перечислением всех типов сообщений, необходимых для NDP-протокола (133-137).
- 2 Создайте разрешающий фильтр на основе созданного справочника.
- 3 Включите этот фильтр и переместите его в самое начало. Он должен быть выше всех остальных фильтров по приоритету..

- 
- Выберите  **Фильтр включен**.
  - Введите название фильтра.
  - Выберите действие фильтра:  **Пропускать** или  **Блокировать**.
  - Выберите режимы, в которых будет использоваться фильтр. Вы можете создать фильтр как для одного режима, так и сразу для двух — **Частная сеть** и **Корпоративная сеть**.
  - Чтобы задать адреса источников, в разделе **Источники** нажмите  и укажите адреса отправителей IP-пакетов. По умолчанию фильтр будет применяться к IP-пакетам с любыми адресами отправителя в формате выбранной версии IP-протокола. Для выбора определенных IP-адресов отправителей, на основании которых будет срабатывать фильтр:
    - Выберите справочники адресов из списка.



---

**Внимание!** В составе одного правила не следует использовать справочники **Мой компьютер** и **Другие компьютеры** одновременно с другими справочниками.

---

- Добавьте новый справочник адресов. Нажмите **Добавить адреса** и укажите IP-адреса для справочника адресов. В результате созданный справочник адресов будет выбран для фильтра.
- Нажмите **Сохранить**.
- Чтобы задать адреса назначений, в разделе **Назначения** нажмите  и укажите адреса получателей IP-пакетов. По умолчанию фильтр будет применяться к IP-пакетам с любыми адресами получателей в формате выбранной версии IP-протокола. Для выбора определенных IP-адресов получателей, на основании которых будет срабатывать фильтр, выполните такие же действия, как для адресов источников.
- Чтобы задать протоколы, в разделе **Протоколы** нажмите  и укажите протоколы передачи пакетов. По умолчанию фильтр будет применяться к IP-пакетам, передаваемым

по всем протоколам. Для выбора определенных протоколов, на основании которых будет срабатывать фильтр:

- Выберите справочники протоколов из списка.
  - Добавьте новый справочник протоколов. Нажмите **Добавить протоколы**, укажите протоколы и их параметры для создания справочника. В результате созданный справочник протоколов будет выбран для фильтра.
  - Нажмите **Сохранить**.
- Чтобы задать расписание, в разделе **Расписание** нажмите  и укажите расписание применения фильтра. По умолчанию фильтр будет применяться всегда. Для выбора определенного времени применения:
    - Выберите справочники расписания из списка.
    - Добавьте новый справочник расписания. Нажмите **Добавить расписание**, укажите параметры для создания справочника. В результате созданный справочник расписания будет выбран для фильтра.
    - Нажмите **Сохранить**.
  - Нажмите **Создать**.

В результате для указанных режимов в разделе **Пользовательские фильтры** будет создан сетевой фильтр с типом фильтра **Открытой сети**.

Чтобы создать и настроить пользовательский сетевой фильтр для защищенного трафика сети ViPNet, на странице **Фильтры политик безопасности**:

- 1 Выберите вкладку режима (**Частная сеть** или **Корпоративная сеть**), в котором будет использоваться создаваемый фильтр.
- 2 Выберите **Создать фильтр сети ViPNet**. Этот пункт доступен для выбора, если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5. Настройте фильтр:
  - Выберите  **Фильтр включен**.
  - Введите название фильтра.
  - Выберите действие фильтра:  **Пропускать** или  **Блокировать**.
  - Выберите режимы, в которых будет использоваться фильтр. Вы можете создать фильтр как для одного режима, так и сразу для двух — **Частная сеть** и **Корпоративная сеть**.
  - Задайте параметры фильтра аналогично настройкам для сетевого фильтра открытой сети (см. выше). При задании адресов источников и назначения будут использоваться **Справочники узлов сети ViPNet**.
  - Нажмите **Создать**.

В результате для указанных режимов в разделе **Пользовательские фильтры** будет создан сетевой фильтр с типом фильтра **Сети ViPNet**.

Задайте порядок применения пользовательских фильтров в каждом из режимов (**Частная сеть** и/или **Корпоративная сеть**) с помощью  и .

Чтобы посмотреть и изменить параметры пользовательского фильтра, на странице **Фильтры политик безопасности**:

- 1 Выберите вкладку режима (**Частная сеть** или **Корпоративная сеть**).
- 2 В списке пользовательских фильтров выберите строку фильтра или предварительно на панеливерху воспользуйтесь поиском  по названию фильтра.
- 3 На панели справа посмотрите сведения о фильтре и в разделе **Основное** вы можете изменить активность фильтра.
- 4 Чтобы внести изменения в другие параметры фильтра, вверху справа нажмите  и внесите необходимые изменения аналогично созданию фильтра (см. выше).
- 5 Нажмите **Сохранить**.

Чтобы удалить пользовательские фильтры, на странице **Фильтры политик безопасности**:

- 1 Выберите вкладку режима (**Частная сеть** или **Корпоративная сеть**).
- 2 В списке пользовательских фильтров выберите флажками нужные фильтры.
- 3 На панели вверху нажмите .
- 4 Подтвердите удаление.

## Настройка пользовательских справочников

При создании и изменении пользовательских фильтров применяются пользовательские и системные справочники. Системные справочники устанавливаются и обновляются на защищаемом узле вместе с ViPNet EPP Агент. Системные справочники недоступны для редактирования и удаления. Чтобы добавить пользовательские справочники:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Межсетевой экран > Справочники**.
- 3 Выберите вкладку типа справочника и настройте справочники в соответствии с описанием в разделе:
  - [Адреса открытой сети](#).
  - Узлы сети ViPNet (см. [Справочники узлов сети ViPNet](#)). Вкладка отображается, если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5.
  - [Протоколы](#).
  - [Расписания](#).

Чтобы посмотреть и изменить пользовательский справочник:

- 1 Выберите вкладку типа справочника и выберите строку пользовательского справочника в списке или предварительно на панели сверху воспользуйтесь поиском  по названию справочника.
- 2 На панели справа на вкладке **Основные** просмотрите параметры справочника и применение в сетевых фильтрах.
- 3 Чтобы изменить справочник, сверху справа нажмите  и внесите необходимые изменения аналогично созданию справочника определенного типа (см. выше).
- 4 Нажмите **Сохранить**.

Чтобы удалить пользовательский справочник, на вкладке типа справочника выберите строку пользовательского справочника в списке и на панели справа нажмите . Чтобы удалить сразу несколько справочников, выберите их флажками и на панели сверху нажмите . В результате справочники будут удалены, если они не используются в сетевых фильтрах.

## Адреса открытой сети

На вкладке **Адреса открытой сети**:

- 1 Выберите **Добавить адреса** > версия IP-протокола (**IPv4** или **IPv6**).
- 2 Введите название справочника.
- 3 Введите IP-адреса в составе справочника и исключения из справочника в разделах **Состав** и **Исключения** в зависимости от выбранной версии IP-протокола:
  - Если был выбран IPv4-адрес, введите адрес, подсеть или диапазон адресов в формате IPv4. При указании диапазона IP-адресов разделяйте начальное и конечное значение диапазона дефисом. Например, 192.168.0.1-192.168.0.100. Для указания подсети вы можете использовать маски подсети, например, 192.168.0.0/24 или 192.168.0.0/255.255.255.0.
  - Если был выбран IPv6-адрес, введите адрес, подсеть или диапазон адресов в формате IPv6, например 2001:db80:0000:a000:c000:d000:b000:e2f0, 2001:0db8::/32.



**Примечание.** При указании нескольких IP-адресов или диапазонов IP-адресов разделяйте их запятой, точкой с запятой или вводите значение с новой строки

---

- 4 Нажмите **Добавить**.

## Справочники узлов сети ViPNet

Если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5, доступно создание пользовательских справочников адресов сети ViPNet, которые можно использовать при

создании пользовательских сетевых фильтров для защищенной сети ViPNet (см. [Настройка пользовательских фильтров](#)).

На вкладке **Узлы сети ViPNet**:

- 1 Выберите **Добавить узлы**.
- 2 Введите название справочника.
- 3 Выберите флажками один или несколько сетевых узлов ViPNet. В списке сетевых узлов отображаются только узлы, с которыми есть связь в программе ViPNet Client 4U или ViPNet Client 5.
- 4 Нажмите **Добавить**.

## Протоколы

На вкладке **Протоколы**:

- 1 Выберите **Добавить протоколы** > версия IP-протокола (**IPv4** или **IPv6**).
- 2 Введите название справочника.
- 3 Добавьте протоколы в состав справочника и в исключения из справочника в разделах **Состав** и **Исключения** и настройте параметры в зависимости от выбранной версии IP-протокола и выбранного протокола. В справочник вы можете добавить один или несколько протоколов:
  - Чтобы добавить в состав справочника все протоколы, выберите **Добавить** > **Любой**. В этом случае возможность добавить в состав справочника конкретные протоколы будет недоступна. Вы можете выбрать исключения из справочника.
  - Выберите **Добавить** > **TCP** и настройте:
    - Введите порты или диапазон портов источника, назначения. При указании диапазона портов разделяйте начальное и конечное значение диапазона дефисом.
    - Укажите запрещенные методы HTTP-запроса.
    - Укажите типы файлов, в виде которых должна быть запрещена передача мобильного кода.
  - Выберите **Добавить** > **UDP** и введите порты или диапазон портов источника, назначения. При указании диапазона портов разделяйте начальное и конечное значение диапазона дефисом.
  - Если был выбран IPv4-адрес, выберите **Добавить** > **ICMPv4**, выберите в списке тип ICMPv4-сообщений и при необходимости код сообщения.
  - Если был выбран IPv6-адрес, выберите **Добавить** > **ICMPv6**, выберите в списке нужный тип ICMPv6-сообщений и при необходимости код сообщения.
  - Чтобы удалить добавленные протоколы, в разделе с названием протокола справа нажмите .
- 4 Нажмите **Добавить**.

## Расписания

На вкладке **Расписания**:

- 1 Выберите **Добавить расписание**.
- 2 Введите название справочника.
- 3 Добавьте расписания в разделах **Состав** и **Исключения**. В справочник вы можете добавить одно или несколько расписаний, но только одного типа (либо по дням недели, либо по периоду):
  - Чтобы справочник работал всегда, выберите **Добавить > Всегда**. В этом случае возможность добавить в состав справочника расписания с конкретным временем будет недоступна. Вы можете выбрать исключения из справочника.
  - Чтобы добавить определенные дни недели и время применения фильтра, выберите **Добавить > Дни недели** и укажите данные.
  - Чтобы добавить период применения фильтра, выберите **Добавить > Период** и укажите данные.
  - Чтобы удалить добавленные протоколы, в разделе с названием протокола справа нажмите .
- 4 Нажмите **Добавить**.

## Управление обнаружением и предотвращением вторжений



**Совет.** Для исключения возможного большого потребления ресурсов компьютера рекомендуем отключить обработку протокола DNS в файле настроек сетевого сенсора `suricata.yaml`.

---

По умолчанию файл `suricata.yaml` расположен в папке:

- В ОС Windows — `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection\Suricata\etc`.
- В ОС Linux — `/opt/epp-agent/suricata/etc/suricata`.

Чтобы отключить обработку протокола DNS, откройте файл `suricata.yaml` и в разделе `app-layer: protocols:` для протокола `dns`: замените параметры `yes` на `no` в следующих строках:

```
app-layer:
.....
  protocols:
.....
```

```
dns:
  tcp:
    enabled: no
    detection-ports:
      dp: 53
  udp:
    enabled: no
    detection-ports:
      dp: 53
```

## Просмотр и настройка правил обнаружения вторжений (HIDS)

Правила HIDS применяются ViPNet EPP Агент для обнаружения вторжений (см. [Обнаружение вторжений](#)). Возможность настройки правил HIDS зависит от способа работы ViPNet EPP Агент:

- При работе под управлением ViPNet EPP Сервер (см. [Подключение защищаемых узлов](#)) правила HIDS настраиваются на сервере и передаются в составе базы правил на ViPNet EPP Агент. В ViPNet EPP Агент вы можете только просматривать статус и параметры применения групп правил HIDS.
- При автономной работе ViPNet EPP Агент доступна настройка правил HIDS.

Чтобы просмотреть или настроить правила обнаружения вторжений:

- 1 Подключитесь к ViPNet EPP Агент:
  - для просмотра правил — с полномочиями администратора или аудитора агента.
  - для настройки правил — с полномочиями администратора агента.
- 2 Выберите  **Обнаружение вторжений**.
- 3 Выберите вкладку с названием типа правил обнаружения вторжений и в зависимости от способа работы ViPNet EPP Агент:
  - Если ViPNet EPP Агент работает автономно, просмотрите и настройте правила HIDS, выбрав группу правил в соответствии с разделами:
    - [Анализ журналов приложений и служб](#).
    - [Мониторинг файлов](#).
    - [Расчет контрольных сумм файлов](#).
    - [Обнаружение сетевых атак](#).
  - Если ViPNet EPP Агент работает под управлением ViPNet EPP Сервер, посмотрите статусы применения групп правил HIDS. Выбранные  группы правил HIDS применяются ViPNet EPP Агент для обнаружения вторжений на защищаемом узле. Чтобы посмотреть

параметры, в разделе с названием группы правил справа нажмите . Описание параметров см. в соответствующих разделах выше.

## Анализ журналов приложений и служб

ViPNet EPP позволяет обнаруживать изменения в журналах приложений и служб на защищаемых узлах. Отслеживаются изменения в журналах, указанных в политике. Доступен просмотр и изменение частоты проверки журналов и списка отслеживаемых журналов. Если отслеживание журналов приложений и служб отключено, также будет отключено отслеживание файлов и расчет контрольных сумм файлов.

Для первичного анализа ряда изменений, происходящих на защищаемом узле, используются декодеры. Правила декодера находятся в файле `decoder.xml`. Текст правил соответствует синтаксису [OSSEC](#).

Для детального разбора информации от декодеров используются правила анализа. Правила анализа находятся в файле `ids_rules.xml`. Текст правил соответствует синтаксису [OSSEC](#).

Чтобы просмотреть и настроить правила и параметры отслеживания изменений в журналах приложений и служб:

- 1 На странице **Обнаружение вторжений** выберите вкладку **Приложения и службы**.
- 2 Включите  **Анализ журналов приложений и служб** и справа нажмите . Будет отображен список отслеживаемых журналов и служб.
- 3 Чтобы добавить новый журнал в список для отслеживания, в разделе **Журналы для анализа** нажмите **Добавить**, введите путь к файлу с журналом и нажмите **Добавить**.
- 4 Чтобы изменить путь отслеживания журнала из списка отслеживания, в разделе **Журналы для анализа**:
  - 4.1 Выберите журнал или предварительно воспользуйтесь поиском  по пути к файлу журнала, справа от названия нужного журнала выберите  > **Изменить**.
  - 4.2 Введите новый путь к файлу с журналом и нажмите **Сохранить**.
- 5 Чтобы исключить журнал из списка отслеживания, в разделе **Журналы для анализа** выберите журнал и справа от названия нужного журнала выберите  > **Удалить**.
- 6 Чтобы внести изменения в правила анализа в разделе **Файлы правил анализа**:
  - 6.1 Справа от файла `ids_rules.xml` выберите  > **Изменить**.
  - 6.2 Внесите новые правила анализа или отредактируйте уже существующие в соответствии с синтаксисом [OSSEC](#).
  - 6.3 Нажмите **Сохранить**.
- 7 Чтобы внести изменения в правила декодеров в разделе **Декодер**:
  - 7.1 Справа от файла `decoder.xml` выберите  > **Изменить**.

7.2 Внесите новые правила или отредактируйте уже существующие в соответствии с синтаксисом OSSEC.

7.3 Нажмите **Сохранить**.

8 Нажмите **Сохранить**.

Чтобы отключить отслеживание изменений в журналах приложений и служб:

- 1 На вкладке **Приложения и службы** выключите  **Анализ журналов приложений и служб**.
- 2 Подтвердите отключение мониторинга файлов и расчета контрольных сумм.

## Мониторинг файлов

ViPNet EPP позволяет обнаруживать изменения в файлах на защищаемых узлах. Отслеживаются процессы изменения, создания и удаления файлов по указанным путям. Чтобы отслеживание изменений в файлах можно было включить, должен быть включен **Анализ журналов приложений и служб**.

Чтобы просмотреть и настроить правила отслеживания файлов:

- 1 На странице **Обнаружение вторжений** выберите вкладку **Файлы**.
- 2 Проверьте, что включен **анализ журналов приложений и служб**. Если анализ журналов приложений и служб не будет включен, вы не сможете включить мониторинг файлов.
- 3 Включите  **Мониторинг файлов** и справа нажмите . Будет отображен список правил отслеживания файлов. Параметры правил отмечены значками:
  - ● — параметр используется для отслеживания.
  - ○ — параметр не используется для отслеживания.
- 4 Чтобы добавить новое правило отслеживания, нажмите **Создать**:
  - 4.1 В поле **Путь** укажите путь отслеживания изменяемых файлов.
  - 4.2 Если нужно отслеживать все вложенные папки в случае их наличия, выберите **Учитывать вложенные папки (рекурсия)**.



**Примечание.** Вложенные папки, созданные с помощью команды `mkdir -p`, отслеживаться не будут, если папки более высокого уровня не были созданы до запуска команды.

---

- 4.3 Укажите маску, по которой будет происходить поиск изменяемых файлов. В маске могут использоваться символы:
  - ? — любой допустимый символ.
  - \* — любой набор допустимых символов, в том числе пустой.



**Внимание!** Не рекомендуется задавать в качестве отслеживаемых папки, занимающие большую часть дискового пространства. Это может привести к замедлению работы компьютера.

- 4.4 Если по указанной маске нужно исключать отслеживание файлов, выберите **Исключать по маске**.
- 4.5 Выберите процессы, которые нужно отслеживать: **Создание, Изменение, Удаление**.
- 4.6 Нажмите **Сохранить**.
- 5 Чтобы изменить правило отслеживания файлов из списка:
  - 5.1 Выберите строку с правилом или предварительно воспользуйтесь поиском , в конце строки выберите  > **Изменить**.
  - 5.2 Измените параметры и нажмите **Сохранить**.
- 6 Чтобы удалить правило, выберите строку с правилом и в конце строки выберите  > **Удалить**. Подтвердите удаление.

Чтобы отключить отслеживание изменений файлов на вкладке **Файлы** выключите  **Мониторинг файлов**.

## Расчет контрольных сумм файлов

ViPNet EPP позволяет отслеживать на защищаемых узлах создание новых файлов и вычислять их контрольные суммы по одному из алгоритмов: MD5, SHA256 или SpamSum. Чтобы расчет контрольных сумм можно было включить, должен быть включен **Анализ журналов приложений и служб**.

Чтобы посмотреть и настроить правила расчета контрольных сумм файлов:

- 1 На странице **Обнаружение вторжений** выберите вкладку **Файлы**.
- 2 Проверьте, что включен **анализ журналов приложений и служб**. Если анализ журналов приложений и служб не будет включен, вы не сможете включить мониторинг файлов.
- 3 Включите  **Расчет контрольных сумм файлов** и справа нажмите . Будет отображен список правил (если они уже были настроены). Параметры правил отмечены значками:
  - ● — параметр используется для отслеживания.
  - ○ — параметр не используется для отслеживания.
- 4 Чтобы добавить новое правило расчета контрольных сумм, нажмите **Создать правило** и:
  - 4.1 В поле **Путь** укажите путь отслеживания создаваемых файлов.
  - 4.2 Если нужно отслеживать все вложенные папки в случае их наличия, выберите **Учитывать вложенные папки (рекурсия)**.



**Примечание.** Вложенные папки, созданные с помощью команды `mkdir -p`, отслеживаться не будут, если папки более высокого уровня не были созданы до запуска команды.

4.3 Укажите маску, по которой будет происходить поиск создаваемых файлов. В маске могут использоваться символы:

- ? — любой допустимый символ.
- \* — любой набор допустимых символов, в том числе пустой.

Сверка на наличие новых папок, удовлетворяющих настроенным шаблонам, будет выполняться каждые 60 секунд.

4.4 Если по указанной маске нужно исключать отслеживание файлов, выберите **Исключать по маске**.

4.5 Выберите алгоритм вычисления контрольной суммы: **MD5, SHA256, SpamSum**.



**Примечание.** Для алгоритма SpamSum максимальный размер отслеживаемых файлов ограничен значением 100 Мбайт.

4.6 Нажмите **Сохранить**.

5 Чтобы изменить правило расчета контрольных сумм из списка:

5.1 Выберите строку с правилом или предварительно воспользуйтесь поиском , в конце строки выберите  > **Изменить**.

5.2 Измените параметры и нажмите **Сохранить**.

6 Чтобы удалить правило, выберите строку с правилом и в конце строки выберите  > **Удалить**. Подтвердите удаление.

В результате при создании новых файлов по указанным путям и с заданными параметрами в журнале событий будет регистрироваться событие расчета контрольной суммы.

Чтобы отключить отслеживание создания новых файлов и вычисления их контрольных сумм на вкладке **Файлы** выключите  **Расчет контрольных сумм файлов**.

## Обнаружение сетевых атак

ViPNet EPP позволяет контролировать входящий и исходящий трафик защищаемого узла и обнаруживать потенциально опасную сетевую активность с помощью правил обнаружения сетевых атак. В случае наличия аналогичного активного правила предотвращения сетевых атак, потенциально опасная сетевая активность будет обнаружена и заблокирована правилом HIPS.

Тексты правил обнаружения сетевых атак написаны в соответствии с синтаксисом [Suricata](#) и содержатся в файле.



**Внимание!** При создании и изменении правил избегайте применения функций трансформации содержимого: `to_lowercase`, `to_uppercase`, `strip_whitespace`, `compress_whitespace`, `dotprefix`, `header_lowercase`, `strip_pseudo_headers`, `url_decode`, `xor`.

Чтобы просмотреть и настроить правила обнаружения сетевых атак:

- 1 На странице **Обнаружение вторжений** выберите вкладку **Сетевая активность**.
- 2 Включите  **Обнаружение сетевых атак** и справа нажмите . Будет отображен файл правил отслеживания сетевых атак.
- 3 Внесите новые правила или измените уже существующие в соответствии с синтаксисом Suricata.
- 4 Нажмите **Сохранить**.

Чтобы отключить отслеживание сетевой активности на защищаемом узле, на вкладке **Сетевая активность** выключите  **Обнаружение сетевых атак**.

## Просмотр и настройка сетевых правил предотвращения вторжений (HIPS)

Сетевые правила HIPS применяются ViPNet EPP Агент для [предотвращения вторжений](#). Политика безопасности содержит предустановленные [правила HIPS](#) для защищаемых узлов для каждого из режимов работы обнаружения и предотвращения вторжений: усиленного, оптимального и минимального. Возможность настройки правил HIPS зависит от способа работы ViPNet EPP Агент:

- При работе под управлением ViPNet EPP Сервер (см. [Подключение защищаемых узлов](#)) правила HIPS настраиваются на сервере и передаются в составе политики безопасности на ViPNet EPP Агент. В ViPNet EPP Агент вы можете только просматривать список правил HIPS.
- При автономной работе ViPNet EPP Агент доступна настройка правил HIPS.

Правила HIPS для защищаемых узлов содержатся в файле и написаны в соответствии с синтаксисом [Suricata](#). Изменения можно внести путем редактирования файла, строго соблюдая синтаксис Suricata. При написании правил учитывайте, что в ViPNet EPP Агент применяются правила HIPS только с действиями правил:

- `drop` ( **Блокировать**) — IP-пакет блокируется сетевым фильтром HIPS межсетевого экрана ViPNet EPP Агент.
- `alert` ( **Уведомлять**) — срабатывание правила HIPS регистрируется в журнале ViPNet EPP Агент.



**Внимание!** При создании и изменении правил избегайте применения функций трансформации содержимого: `to_lowercase`, `to_uppercase`, `strip_whitespace`, `compress_whitespace`, `dotprefix`, `header_lowercase`, `strip_pseudo_headers`, `url_decode`, `xor`.

Чтобы просмотреть списки или настроить сетевые правила HIPS:

- 1 Подключитесь к ViPNet EPP Агент:
  - для просмотра правил — с полномочиями администратора или аудитора агента.
  - для настройки правил — с полномочиями администратора агента.
- 2 Выберите  **Предотвращение вторжений**.
- 3 Выберите вкладку режима работы:
  - **Усиленный режим.**
  - **Оптимальный режим.**
  - **Минимальный режим.**

Отобразится список сетевых правил HIPS, настроенных для выбранного режима. В списке для каждого правила отображаются параметры: идентификатор, название, состояние правила (**Включено** или **Отключено**), адреса и порты источника и назначения, протокол, направление и действие ( **Блокировать** или  **Уведомлять**).
- 4 Чтобы просмотреть подробные сведения о правиле HIPS, выберите его в списке или предварительно на панели сверху воспользуйтесь поиском  по параметрам фильтра. Просмотрите сведения на панели справа.
- 5 При автономной работе ViPNet EPP Агент:
  - 5.1 Чтобы изменить активность правила, на панели справа в разделе **Основное** выберите  **Правило включено** или  **Правило выключено**.
  - 5.2 Чтобы внести изменения в параметры правила, сверху справа нажмите  и внесите необходимые изменения в текст правила. Нажмите **Сохранить**.
  - 5.3 Чтобы добавить новое правило, на панели сверху нажмите **Редактировать файл правил** и добавьте текст правила в соответствии с синтаксисом правил Suricata. Нажмите **Сохранить**.

Чтобы удалить правило, на странице **Предотвращение вторжений**:

- 1 Выберите вкладку режима.
- 2 В списке правил выберите правило.
- 3 На панели справа нажмите .
- 4 Подтвердите удаление.

## Настройка критериев обнаружения аномалий

Отображение и настройка критериев обнаружения аномалий доступна только в автономном ViPNet EPP Агент.

Критерии обнаружения аномалий позволяют контролировать локальную и сетевую активность на защищаемых узлах в течение заданного времени (см. [Обнаружение аномалий с помощью критериев](#)). Критерий обнаружения аномалии задается типом правил HIDS и идентификаторами определенных правил этого типа (см. [Типы и идентификаторы правил](#)), а также временным интервалом.

Чтобы настроить критерии обнаружения аномалий:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента или аудитора агента (только для просмотра).
- 2 Выберите  **Обнаружение аномалий**.
- 3 Для добавления нового критерия обнаружения аномалий нажмите **Создать правило**.
- 4 В окне **Правило обнаружения аномалий** укажите:
  - 4.1 Выберите название критерия из списка.
  - 4.2 Укажите через запятую идентификаторы правил HIDS для выбранного критерия. Идентификаторы правил можно посмотреть в подсказке для поля ввода идентификатора или в журнале событий в столбце **Идентификатор правила**.
  - 4.3 Укажите период аномального возникновения событий, в котором активность считается нетипичной.
- 5 Нажмите **Создать**.

## Мониторинг

В ViPNet EPP Агент ведутся журналы:

- Журнал событий информационной безопасности (см. [Журнал событий](#)).
- Журнал аудита действий пользователей (см. [Журнал аудита](#)).
- Журналы модулей защиты:
  - [Журнал активных соединений](#).
  - [Журнал трафика](#).

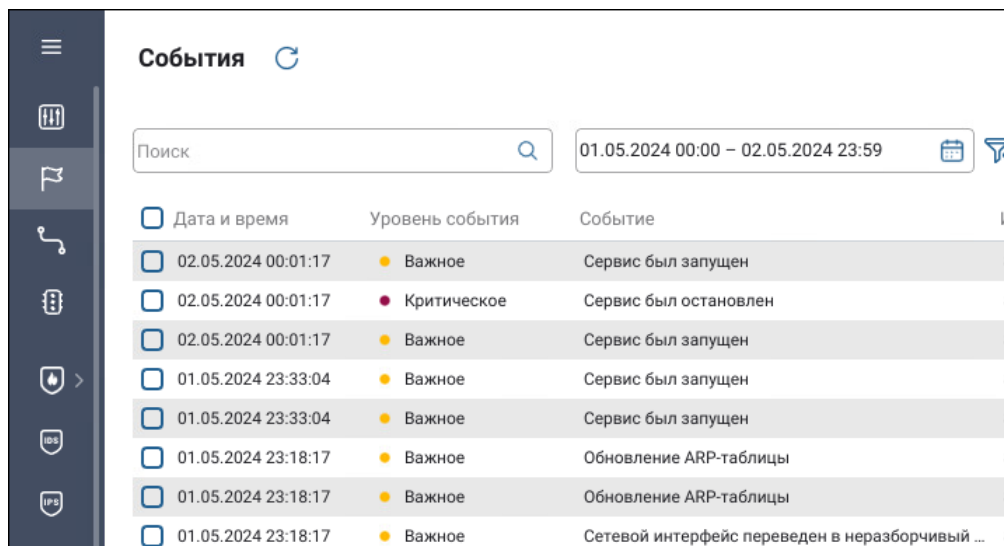
При переполнении журналов (журнала событий, журнала трафика и журнала аудита) в соответствии с параметрами работы выполняется автоматическая ротация событий и журналов (см. [Просмотр и настройка параметров работы](#)).

## Журнал событий

События информационной безопасности, идентифицированные всеми модулями защиты ViPNet EPP Агент, регистрируются в журнале событий ViPNet EPP Агент. Вы можете просматривать и удалять события.

Чтобы просмотреть журнал событий ViPNet EPP Агент и выполнить возможные действия:

- 1 Войдите в ViPNet EPP Агент с полномочиями администратора или аудитора агента.
- 2 Выберите  **События**.



| Дата и время        | Уровень события | Событие                                         | Идентификатор |
|---------------------|-----------------|-------------------------------------------------|---------------|
| 02.05.2024 00:01:17 | Важное          | Сервис был запущен                              | 8             |
| 02.05.2024 00:01:17 | Критическое     | Сервис был остановлен                           | 8             |
| 02.05.2024 00:01:17 | Важное          | Сервис был запущен                              | 8             |
| 01.05.2024 23:33:04 | Важное          | Сервис был запущен                              | 8             |
| 01.05.2024 23:33:04 | Важное          | Сервис был запущен                              | 8             |
| 01.05.2024 23:18:17 | Важное          | Обновление ARP-таблицы                          | 8             |
| 01.05.2024 23:18:17 | Важное          | Обновление ARP-таблицы                          | 8             |
| 01.05.2024 23:18:17 | Важное          | Сетевой интерфейс переведен в неразборчивый ... | 8             |

Рисунок 47. Журнал событий ViPNet EPP Агент



**Примечание.** По умолчанию отображается информация обо всех зарегистрированных событиях за текущие и предыдущие сутки.

Каждая запись о событии в журнале содержит:

- **Дата и время** — дата и время обнаружения.



**Внимание!** Если одно и тоже событие, зарегистрированное модулем обнаружения вторжений, произошло несколько раз за одну секунду, в журнале событий отобразится только одно событие.

- Цветовой индикатор и название уровня события:

-  — критическое.
-  — опасное.
-  — важное.
-  — информационное.

- **Событие** — описание события.
- **Идентификатор правила** — идентификатор правила, при срабатывании которого зарегистрировано событие (см. [Типы и идентификаторы правил](#)).
- **Тип правила и Категория угрозы** — к какому типу правил относится сработавшее правило (см. [Типы и идентификаторы правил](#)).
- **Версия базы правил** — политика безопасности (база правил), в которой находится сработавшее правило.
- **Модуль** — модуль защиты, к которому относится сработавшее правило.



**Примечание.** При работе ViPNet EPP Агент под управлением ViPNet EPP Сервер события информационной безопасности защищаемого узла пересылаются в ViPNet EPP Сервер. До тех пор, пока событие не доставлено в ViPNet EPP Сервер, строка с описанием события в журнале будет выделена **жирным шрифтом**.

- 3 Чтобы просмотреть сведения о событии, выберите строку с событием в журнале — на панели справа будут отображены сведения о сработавшем правиле и подробные сведения о событии. По умолчанию отображаются только важные сведения о событии в удобном для чтения виде. Для просмотра полных сведений о событии выберите **Показывать в виде текста события**.

Чтобы скопировать сведения в буфер обмена, нажмите

- 4 Для поиска событий в журнале используйте фильтры:

4.1 В поле поиска введите ключевое слово и нажмите .

4.2 Нажмите и укажите промежуток времени, в течение которого происходили искомые события.

4.3 Нажмите и задайте параметры фильтрации:

- Чтобы отобразить события, зарегистрированные заданными критериями аномалий, выберите **Только аномальные события** (доступно только для автономного ViPNet EPP Агент).
- Выберите **Только не доставленные на сервер ViPNet EPP события**, чтобы отобразить такие события (доступно только при работе ViPNet EPP Агент под управлением ViPNet EPP Сервер).
- Выберите флажками уровни, события которых нужно отобразить.
- Выберите модули, события которых нужно отобразить.
- Выберите тип правил, с помощью которых были идентифицированы события.

4.4 Нажмите **Применить**.

- 5 Чтобы обновить журнал, вверху нажмите .

- 6 Чтобы удалить события, выберите их флажками, на панели вверху нажмите и подтвердите удаление.

## Журнал активных соединений

Межсетевой экран ViPNet EPP Агент отслеживает сетевую активность приложений защищаемого узла. Вы можете просмотреть приложения, которые в настоящий момент работают с сетевыми ресурсами — имеют активные соединения, и параметры соединений в журнале активных соединений межсетевого экрана ViPNet EPP Агент. При обнаружении подозрительной сетевой активности приложений вы можете заблокировать их.



**Примечание.** Приложение можно заблокировать, если межсетевой экран ViPNet EPP Агент работает в одном из режимов: **Частная сеть** или **Корпоративная сеть**.

---

Чтобы в журнале активных соединений просмотреть список приложений, работающих с сетевыми ресурсами, и при необходимости заблокировать их:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.
- 2 Выберите  **Соединения**.
- 3 Чтобы найти соединение, в поле поиска введите название приложения и нажмите .
- 4 Для просмотра параметров соединения (протокола, локального и удаленного адресов) на вкладке **Активные** раскройте приложение.
- 5 Чтобы обновить журнал, сверху нажмите .
- 6 Чтобы разорвать соединение и заблокировать приложение:
  - 6.1 Справа от названия нужного приложения выберите  > **Заблокировать соединение**.
  - 6.2 Укажите режимы межсетевого экрана, в которых приложение должно быть заблокировано (**Корпоративная сеть** или **Частная сеть**) и нажмите **Заблокировать**.
  - 6.3 Нажмите **Заккрыть**. В результате данные о заблокированном приложении будут удалены со вкладки **Активные** и отобразятся на вкладке **Заблокированные**.

Чтобы разблокировать приложение — разрешить сетевую активность:

- 1 На странице **Соединения** > **Заблокированные** справа от названия нужного приложения выберите  > **Разблокировать соединение**.
- 2 Если соединение было заблокировано только в одном режиме, подтвердите разблокирование.
- 3 Если соединение было заблокировано в нескольких режимах, укажите режимы межсетевого экрана, в которых приложение нужно разблокировать (**Корпоративная сеть** или **Частная сеть**) и нажмите **Разблокировать**.
- 4 Нажмите **Заккрыть**.

## Журнал трафика

В межсетевом экране ViPNet EPP Агент ведется журнал регистрации трафика, проходящего через защищаемый узел. Вы можете на основе различных параметров поиска сформировать отчет о заблокированных и разрешенных IP-пакетах, а также просмотреть время регистрации каждого IP-пакета. Отчеты позволяют контролировать прохождение IP-пакетов и при необходимости на основе событий журнала создавать дополнительные блокирующие либо разрешающие пользовательские фильтры. Создание фильтров на основе событий будет недоступно, если событие зарегистрировано для защищенного трафика сети ViPNet



**Примечание.** Не рекомендуется создавать пользовательские фильтры на события журнала трафика, которые были зарегистрированы в результате срабатывания фильтров политик безопасности. Если событие зарегистрировано при срабатывании фильтра политик безопасности, созданный на его основе фильтр работать не будет, поскольку фильтры политик безопасности имеют наивысший приоритет.

Чтобы просмотреть журнал регистрации трафика меж сетевого экрана ViPNet EPP Агент:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.
- 2 Выберите  **Трафик**.



**Примечание.** По умолчанию отображается информация обо всех зарегистрированных IP-пакетах за последние сутки.

Каждая запись о событии в журнале содержит:

- **Дата и время** — дату и время регистрации последнего однотипного IP-пакета (с одинаковыми характеристиками: направлением, действием, адресами и портами источника и назначения, протоколом).
- **Направление** — направление пакетов (входящие IP-пакеты, исходящие IP-пакеты).
- **Действие** — разрешенные IP-пакеты ( **Пропускать**) или заблокированные ( **Блокировать**).
- **Адрес и порт источника, Адрес и порт назначения, Протокол передачи.**
- **Пакеты** — количество зарегистрированных однотипных IP-пакетов за указанный период времени.
- **Фильтр** — сетевой или системный фильтр, по срабатыванию которого было зарегистрировано событие:
  - Сетевой фильтр из списка фильтров политик безопасности для режимов работы.
  - Служебный трафик EndPoint — всегда разрешенный трафик, необходимый для взаимодействия ViPNet EPP Агент с ViPNet EPP Сервер.
  - Правило фильтрации HTTP-контента — трафик, зарегистрированный фильтром контента HTTP.

- Блокировка сетевых соединений приложения — трафик, заблокированный фильтром активных соединений приложений.
- Фильтры только для защищаемых узлов с ViPNet Client 4U или ViPNet Client 5:
  - Пропуск трафика VPN сети (шифрованный) — входящий и исходящий шифрованный VPN трафик (сети ViPNet).
  - Пропуск VPN трафика пользователя (нешифрованный) — входящий и исходящий нешифрованный VPN трафик (сети ViPNet).
  - Невыполнение политик ZTNA — трафик заблокирован из-за невыполнения политик ZTNA.
  - Исключение по пропуску трафика ZTNA — политика ZTNA не выполнена, но трафик был пропущен из-за наличия исключения из политик.

Вы можете отсортировать записи журнала по любому из указанных параметров.

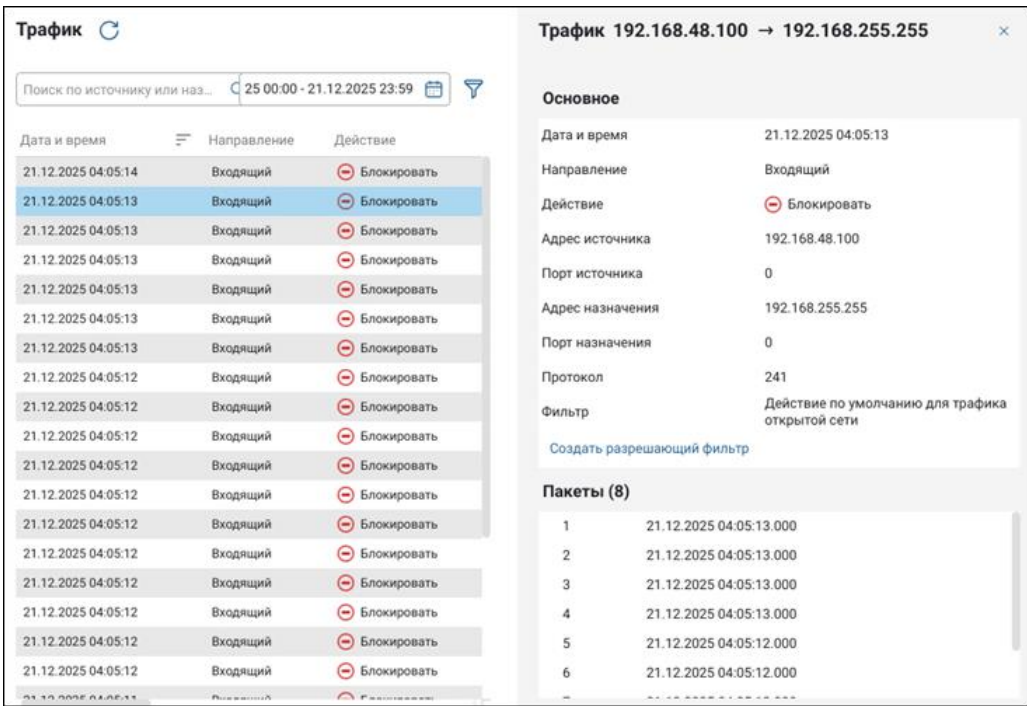
### 3 Чтобы найти определенные события:

3.1 В поле поиска введите часть адреса источника или назначения IP-пакета и нажмите .

3.2 Нажмите  и укажите промежуток времени, в течение которого происходили искомые события.

3.3 Нажмите  и задайте параметры фильтрации: направление трафика, действие фильтра, протокол передачи и название сетевого фильтра.

### 4 Чтобы просмотреть дату и время регистрации каждого IP-пакета события, выберите событие и на панели справа посмотрите данные.



**Трафик**

Поиск по источнику или наз... 25 00:00 - 21.12.2025 23:59

| Дата и время        | Направление | Действие    |
|---------------------|-------------|-------------|
| 21.12.2025 04:05:14 | Входящий    | Блокировать |
| 21.12.2025 04:05:13 | Входящий    | Блокировать |
| 21.12.2025 04:05:13 | Входящий    | Блокировать |
| 21.12.2025 04:05:13 | Входящий    | Блокировать |
| 21.12.2025 04:05:13 | Входящий    | Блокировать |
| 21.12.2025 04:05:13 | Входящий    | Блокировать |
| 21.12.2025 04:05:13 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |
| 21.12.2025 04:05:12 | Входящий    | Блокировать |

**Трафик 192.168.48.100 → 192.168.255.255**

**Основное**

|                  |                                                 |
|------------------|-------------------------------------------------|
| Дата и время     | 21.12.2025 04:05:13                             |
| Направление      | Входящий                                        |
| Действие         | Блокировать                                     |
| Адрес источника  | 192.168.48.100                                  |
| Порт источника   | 0                                               |
| Адрес назначения | 192.168.255.255                                 |
| Порт назначения  | 0                                               |
| Протокол         | 241                                             |
| Фильтр           | Действие по умолчанию для трафика открытой сети |

[Создать разрешающий фильтр](#)

**Пакеты (8)**

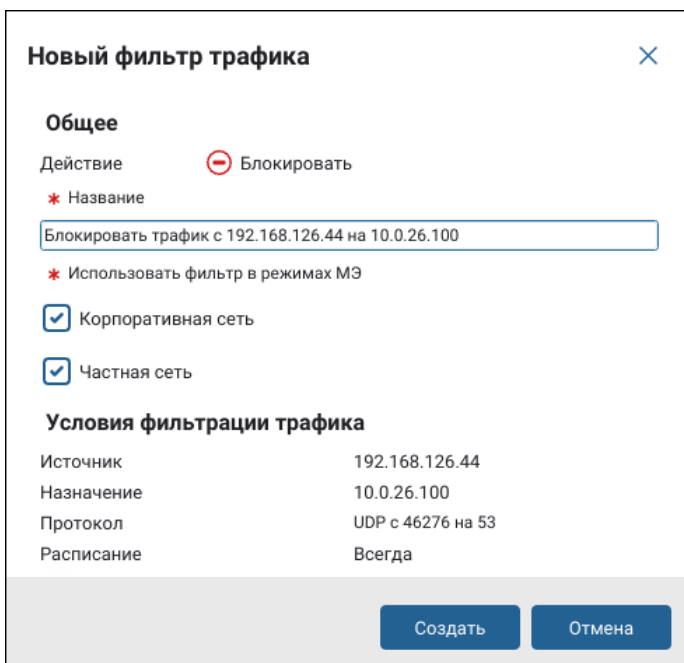
|   |                         |
|---|-------------------------|
| 1 | 21.12.2025 04:05:13.000 |
| 2 | 21.12.2025 04:05:13.000 |
| 3 | 21.12.2025 04:05:13.000 |
| 4 | 21.12.2025 04:05:13.000 |
| 5 | 21.12.2025 04:05:12.000 |
| 6 | 21.12.2025 04:05:12.000 |

Рисунок 48. Просмотр даты и времени регистрации каждого IP-пакета события

### 5 Чтобы обновить журнал, вверху нажмите .

Чтобы на основе зарегистрированного события создать блокирующий или разрешающий пользовательский фильтр:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Трафик**.
- 3 Выполните одно из действий:
  - Чтобы заблокировать ранее разрешенный пользовательскими фильтрами трафик, выберите событие (с параметрами разрешенного трафика, который вы хотите заблокировать) и на панели справа нажмите **Создать запрещающий фильтр**.
  - Чтобы разрешить ранее заблокированный пользовательскими фильтрами трафик, выберите событие (с параметрами заблокированного трафика, который вы хотите разрешить) и на панели справа нажмите **Создать разрешающий фильтр**. Если трафик был заблокирован в разделе **Соединения**, перед созданием разрешающего фильтра необходимо разблокировать соединение соответствующего приложения.
- 4 В окне создания блокирующего или разрешающего фильтра:
  - 4.1 Укажите наименование фильтра.
  - 4.2 Выберите режимы, в которых будет применяться фильтр.



**Новый фильтр трафика**

**Общее**

Действие  Блокировать

\* Название

Блокировать трафик с 192.168.126.44 на 10.0.26.100

\* Использовать фильтр в режимах МЭ

☒ Корпоративная сеть

☒ Частная сеть

**Условия фильтрации трафика**

|            |                   |
|------------|-------------------|
| Источник   | 192.168.126.44    |
| Назначение | 10.0.26.100       |
| Протокол   | UDP с 46276 на 53 |
| Расписание | Всегда            |

**Создать** **Отмена**

Рисунок 49. Создание пользовательского блокирующего фильтра

#### 4.3 Нажмите **Создать**.

Фильтр отобразится на странице частной или корпоративной сети, в зависимости от режима, в котором будут применяться фильтры.

Если трафик был заблокирован в разделе **Соединения**, перед созданием разрешающего фильтра необходимо разблокировать соединение.

#### 4.4 Нажмите **Заккрыть**.



**Примечание.** Если для события журнала трафика ранее создавался пользовательский фильтр с противоположным действием, такой фильтр необходимо либо удалить, либо выключить, либо изменить порядок применения.

## Администрирование ViPNet EPP Агент

### Управление учетными записями

При установке ViPNet EPP Агент автоматически создается учетная запись администратора агента.

**Примечание.** Только для ViPNet EPP Агент под управлением сервера.

Учетные записи, созданные в ViPNet EPP Сервер, с ролями Администратор ViPNet EPP и Аудитор ViPNet EPP (см. [Полномочия пользователей](#)) синхронизируются с учетными записями ViPNet EPP Агент. Эти учетные записи не отображаются в списке учетных записей ViPNet EPP Агент, но с их помощью вы можете авторизоваться и получить те же полномочия, что и для учетных записей с ролями Администратор агента и Аудитор агента.



Администратор в ViPNet EPP Сервер может сменить пароль учетным записям с ролями Администратор агента и Аудитор агента, созданным ViPNet EPP Агент, путем создания аналогичных учетных записей в ViPNet EPP Сервер. При подключении к ViPNet EPP Агент с этими учетными записями вы сможете авторизоваться только с помощью пароля, заданного в ViPNet EPP Сервер. При удалении этих учетных записей на сервере в ViPNet EPP Агент снова будет использоваться пароль учетной записи, созданной в ViPNet EPP Агент.

Чтобы создать новые учетные записи и отредактировать существующие:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Учетные записи**.
- 3 Чтобы создать новую учетную запись:
  - 3.1 На панели сверху нажмите **Создать учетную запись**.
  - 3.2 В окне **Учетная запись** укажите:
    - Имя учетной записи в соответствии с [требованиями](#).
    - Имя пользователя, например фамилия и имя.
    - Роль учетной записи: администратор, аудитор, пользователь (см. [Ролевая модель](#)).
    - Пароль — пароль пользователя в соответствии с [требованиями](#).



**Примечание.** Вы можете выбрать **Не применять требования к сложности пароля** и в поле **Пароль** указать любой пароль, но в целях безопасности использовать простые пароли не рекомендуется.

### 3.3 Нажмите **Создать**.

- 4 Для поиска учетных записей на основе их ролей (администратор, аудитор и пользователь) используйте фильтр:

4.1 Нажмите .

4.2 Выберите роль учетных записей.

4.3 Нажмите **Применить**.

- 5 Для поиска учетных записей по имени в поле поиска введите часть имени или имя целиком и нажмите .

- 6 Чтобы изменить пароль существующей учетной записи:

6.1 На странице **Учетные записи** выберите учетную запись в списке.

6.2 На панели справа нажмите **Сменить пароль** и укажите новый пароль аналогично созданию новой учетной записи.

6.3 Нажмите **Сохранить**.

- 7 Чтобы изменить параметры существующей учетной записи (имя пользователя и роль):

7.1 На странице **Учетные записи** выберите учетную запись в списке.

7.2 На панели справа нажмите  и укажите новые имя пользователя и роль.

7.3 Нажмите **Сохранить**.

Чтобы удалить учетную запись:

- 1 На странице **Учетные записи** выберите учетную запись в списке.

- 2 На панели справа нажмите  и подтвердите удаление.

## Требования к имени и паролю учетной записи

При создании имени учетной записи разрешено использовать:

- прописные буквы латинского алфавита от **A** до **Z**;
- строчные буквы латинского алфавита от **a** до **z**;
- десятичные цифры от **0** до **9**;

Имя учетной записи должно начинаться с прописной или строчной букв латинского алфавита и не должно содержать пробелы. Максимальная длина имени учетной записи — 32 символа.

При создании или изменении пароля учетной записи, стойкого к попыткам подбора, соблюдайте требования:

- Минимальная длина — 8 символов.
- Максимальная длина — 32 символа.
- Любые идущие подряд три символа пароля не должны совпадать с частью имени учетной записи.
- Один и тот же символ не должен встречаться более двух раз.
- В пароле должны одновременно присутствовать символы четырех категорий:
  - прописные буквы латинского алфавита от A до Z;
  - строчные буквы латинского алфавита от a до z;
  - десятичные цифры от 0 до 9;
  - символы !@#\$%^&\*()\_+=;:'",.<>/?\|`~[]{}.

## Журнал аудита

События, вызванные действиями пользователей ViPNet EPP Агент, а также системные события и результаты самотестирования ViPNet EPP Агент регистрируются в журнале аудита ViPNet EPP Агент.

Чтобы просмотреть журнал аудита ViPNet EPP Агент:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.
- 2 Выберите  **Журнал аудита**.

Отобразится список зарегистрированных событий аудита. Каждая запись о событии в журнале содержит:

- **Дата и время** — дата и время, когда событие произошло.
- **Результат** — успех или ошибка.
- **Событие** — название события.
- **Детали** — описание события (при наличии).
- **Инициатор**:
  - Система (например, системные события «Запуск службы» или «Запуск самотестирования агента»).
  - Администраторы, аудиторы и пользователи ViPNet EPP Агент (например, аутентификация администратора на ViPNet EPP Агент).



**Примечание.** Если аутентификация в ViPNet EPP Агент выполнена с учетной записью, имеющей полномочия администратора или аудитора ViPNet EPP, либо учетные данные администратора или аудитора ViPNet EPP Агент совпадают с учетными данными администратора или аудитора ViPNet EPP, в поле **Инициатор** кроме роли и имени будет отображаться — Администратор сервера или Аудитор сервера. Например, Администратор (admin) Администратор сервера.

○ **Получатель:**

- ViPNet EPP Агент и служба сетевого сенсора ViPNet EPP.
- Администраторы, аудиторы и пользователи ViPNet EPP Агент. Для некоторых событий поле может быть пустым.

**3 Для поиска событий в журнале используйте фильтр:**

**3.1** В поле поиска введите ключевое слово и нажмите .

**3.2** Нажмите  и укажите промежуток времени, в течение которого происходили искомые события.

**3.3** Нажмите  и задайте параметры фильтрации: по результату, инициатору, получателю, событию.

**3.4** Нажмите **Применить**.

**4** Чтобы обновить журнал, вверху нажмите .

## Настройка типов регистрируемых событий в журнале аудита

В ViPNet EPP Агент вы можете выбрать типы событий, которые будут регистрироваться в журнале аудита. По умолчанию регистрируются события всех типов:

- Вход/Выход пользователей.
- Лицензия.
- Регистрируются всегда.
- Операции с базой правил.
- Операции с журналами.
- Операции с учетными записями.
- Управление правилами модулей.
- Управление правилами обнаружения аномалий.
- Установка режимов работы модулей.
- Функционирование EPP Агента.

Вы можете отключить регистрацию событий одного, нескольких или сразу всех типов, кроме обязательных событий, которые регистрируются всегда:

- Запуск самотестирования агента.

- Завершение самотестирования агента.
- Обнаружено повреждение журнала аудита.
- Обнаружено повреждение журнала трафика.
- Обнаружено повреждение журнала событий.

Чтобы настроить типы событий, которые будут регистрироваться в журнале аудита:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Настройки**.
- 3 В разделе **Настройки Агента** справа нажмите .
- 4 В разделе **Типы регистрируемых событий**:
  - 4.1 Чтобы просмотреть список событий, раскройте список с названием типа событий.
  - 4.2 Снимите флажки типов событий, которые не должны регистрироваться в журнале.
  - 4.3 Чтобы снять или установить флажки сразу со всех типов событий, снимите или установите флажок **Все типы событий**. Флажок с типа обязательных событий **Регистрируются всегда** снять нельзя.
  - 4.4 Нажмите **Сохранить**.

## Просмотр и настройка параметров работы

После установки параметры работы ViPNet EPP Агент заданы по умолчанию. Возможность настройки параметров зависит от способа работы ViPNet EPP Агент:

- При работе под управлением ViPNet EPP Сервер (см. [Подключение защищаемых узлов](#)) на ViPNet EPP Агент передаются глобальные параметры работы, заданные на сервере (см. [Настройка параметров защищаемых узлов](#)). В ViPNet EPP Агент вы можете изменить типы регистрируемых событий аудита (см. [Настройка типов регистрируемых событий в журнале аудита](#)), адрес и порт ViPNet EPP Сервер (см. [Изменение адреса ViPNet EPP Сервер](#)). Все остальные параметры доступны только для просмотра.
- При автономной работе в ViPNet EPP Агент доступна настройка всех параметров работы агента. Также доступен перевод ViPNet EPP Агент под управление ViPNet EPP Сервер (см. [Перевод автономного ViPNet EPP Агент под управление ViPNet EPP Сервер](#)).

При переполнении журналов в ViPNet EPP Агент (журнала событий, журнала трафика и журнала аудита) в соответствии с настроенными параметрами автоматически удаляются из каждого журнала:

- Записи с истекшим сроком хранения.
- Наиболее старые записи журнала в количестве, указанном в настройках, превышающие максимальное количество хранимых событий.

Также при уменьшении объема свободного места на диске компьютера с ViPNet EPP Агент до 3 Гбайт из каждого журнала удаляются наиболее старые события в количестве  $N^3$ , где  $N$  — значение параметра **Число записей, удаляемых при достижении максимума**.

Информация о переполнении журнала и удалении событий фиксируется в журнале аудита (см. [Журнал аудита](#)).

Чтобы посмотреть или настроить параметры работы:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Настройки**.
- 3 Настройте типы регистрируемых событий аудита (см. [Настройка типов регистрируемых событий в журнале аудита](#)).
- 4 При работе под управлением ViPNet EPP Сервер, настройте адрес и порт ViPNet EPP Сервер (см. [Изменение адреса ViPNet EPP Сервер](#)) и просмотрите настройки параметров в разделе **Настройки Агента**.
- 5 При работе в автономном режиме, в разделе **Настройки Агента** посмотрите и настройте параметры. Чтобы настроить параметры, нажмите  и задайте:
  - **Период самотестирования** — промежуток времени, через который происходит автоматическая проверка работоспособности ViPNet EPP Агент (см. [Проверка работоспособности](#)). Рекомендуемое значение — 10 минут.
  - **Следить за антивирусом** — контроль работы антивирусов Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite на защищаемом узле. Если слежение включено (установлен флажок), ViPNet EPP Агент может блокировать сетевой трафик защищаемого узла (см. [Отслеживание работы антивирусов](#)). По умолчанию слежение за антивирусом отключено.



**Внимание!** Если на защищаемом узле не установлены Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite, при включении отслеживания работы антивирусов весь сетевой трафик этого узла, кроме трафика между ViPNet EPP Агент и ViPNet EPP Сервер, будет заблокирован.

---

- **Срок хранения записей журнала (дней)** — записи, зарегистрированные ранее указанного срока, удаляются из журналов (событий, аудита, трафика) в ViPNet EPP Агент. Рекомендуемое значение — 30 дней. Может принимать значение из диапазона 1–400 дней.
- **Максимальное число записей** — максимальное число записей, которое может храниться в каждом из журналов (событий, аудита, трафика) в ViPNet EPP Агент. Рекомендуемое значение — 50000. Может принимать значение из диапазона 1–100000.
- **Число записей, удаляемых при достижении максимума** — количество записей, которое удаляется из каждого журнала (событий, аудита, трафика) в ViPNet EPP Агент в случае достижения максимального количества хранимых записей. Рекомендуемое значение —

1000. Может принимать значение из диапазона 1–9999, но должно быть меньше максимального числа записей.

- Для возврата измененных параметров агента к значениям по умолчанию нажмите **По умолчанию**.

Нажмите **Сохранить**.

## Перевод автономного ViPNet EPP Агент под управление ViPNet EPP Сервер

Перевод автономного ViPNet EPP Агент под управление ViPNet EPP Сервер может потребоваться:

- Для настройки работы под управлением ViPNet EPP Сервер сразу после установки ViPNet EPP Агент.
- Если ViPNet EPP Агент уже работает в автономном режиме и в сети установлен ViPNet EPP Сервер, вы можете перевести ViPNet EPP Агент под управление ViPNet EPP Сервер.

После подключения к ViPNet EPP Сервер и получения от него политики безопасности в ViPNet EPP Агент будут заменены данными с ViPNet EPP Сервер:

- Лицензия (см. [Лицензирование](#)).
- Параметры агента (см. [Настройка параметров защищаемых узлов](#)).
- Фильтры политик безопасности, глобальные справочники.
- Все правила обнаружения вторжений (HIDS).
- Критерии обнаружения аномалий.
- Режимы работы.
- Все правила предотвращения вторжений (HIPS).

После перехода ViPNet EPP Агент под управление сервера, вернуться в автономный режим работы будет невозможно. Потребуется повторная установка ViPNet EPP Агент.

Чтобы ViPNet EPP Агент в автономном режиме перевести под управление ViPNet EPP Сервер:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Настройки**.
- 3 В разделе **Работа под управлением ViPNet EPP Сервера** нажмите **Настроить подключение**.
- 4 Выберите **Работать под управлением ViPNet EPP Сервера** и укажите адрес сервера (рабочего сервера) и порт (по умолчанию — 25014).
- 5 Нажмите **Сохранить**.

В результате переход ViPNet EPP Агент под управление ViPNet EPP Сервер будет выполнен после обработки запроса на подключение на сервере.

## Изменение адреса ViPNet EPP Сервер

В случае работы ViPNet EPP Агент под управлением сервера, при изменении адресного пространства сети, в которой уже используется ViPNet EPP, может потребоваться изменение адреса (IP-адреса или доменного имени) ViPNet EPP Сервер (рабочего сервера) и номера порта в настройках ViPNet EPP Агент.

Чтобы изменить адрес и номер порта ViPNet EPP Сервер:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Настройки**.
- 3 В разделе **Работа под управлением ViPNet EPP Сервера** справа нажмите .
- 4 Укажите новые значения адреса сервера и номера порта.
- 5 Нажмите **Сохранить**.

## Проверка работоспособности

Для контроля работоспособности в ViPNet EPP Агент выполняется:

- Контроль целостности критичных файлов ПО ViPNet EPP. Выполняется при старте программы и периодически в процессе работы программы. При возникновении ошибок целостности важных файлов ПО ViPNet EPP Агент становится неработоспособным. Данные о неработоспособности будут записаны в служебный диагностический журнал. Для восстановления работоспособности см. раздел Восстановление или удаление ViPNet EPP Агент.
- Контроль целостности журналов аудита. Выполняется при старте ПО ViPNet EPP и по расписанию (см. [Настройка параметров защищаемых узлов](#)) в рамках самотестирования (по умолчанию — каждые 600 секунд).

Администратор может запустить самотестирование ViPNet EPP Агент вручную.

В ходе самотестирования проверяется и отображается:

- Дата и время проведения самотестирования.
- Версия ViPNet EPP Агент.
- Работоспособность сетевого сенсора ViPNet EPP — работает или остановлен.
- Состояние подключения к ViPNet EPP Сервер (только если в ViPNet EPP Агент задана настройка работы под управлением сервера):
  - Сервер не задан — настройки подключения к ViPNet EPP Сервер не заданы.
  - Ожидает подключения — находится в группе **Неподключенные** ViPNet EPP Сервер.
  - Подключен — перемещен из группы **Неподключенные** в одну из пользовательских групп ViPNet EPP Сервер.
  - Удален — не посылает запросы на подключение к ViPNet EPP Сервер.
  - Ошибка — проверка состояния подключения завершилась ошибкой.

- Состояние подключения к базе данных ViPNet EPP Агент — завершено успешно или завершено с ошибкой.
- Целостность журнала аудита, целостность журнала трафика, целостность журнала событий — нарушена или не нарушена.

Если целостность одного или нескольких журналов нарушена:

- Текущий журнал, целостность которого нарушена, будет сохранен в каталоге установки ViPNet EPP Агент в файлах:
  - o `/etc/epp-agent/audit_journal.db.backup` — журнал аудита;
  - o `/etc/epp-agent/traffic_journal.db.backup` — журнал трафика;
  - o `/etc/epp-agent/events_journal.db.backup` — журнал событий.
- Из текущего журнала, целостность которого нарушена, будут удалены все события, кроме события о нарушении целостности, и регистрируется следующее событие о восстановлении работоспособности после нарушения целостности соответствующего журнала.
- Дата и время обновления базы правил, версия базы правил.
- Актуальность базы правил — актуальная, устарела или отсутствует (только для ViPNet EPP Агент под управлением сервера).
- Режимы работы предотвращения вторжений и межсетевого экрана — из базы правил (политики), отключен или локальный (изменен администратором агента). Отображаются только для ViPNet EPP Агент под управлением сервера.

Результаты самотестирования, выполненного автоматически или вручную, регистрируются в журнале аудита (см. [Журнал аудита](#)) и журнале самотестирования ViPNet EPP Агент (см. [Журнал самотестирования](#)) и передаются в ViPNet EPP Сервер (только для ViPNet EPP Агент под управлением сервера).

Если в результате самотестирования были выявлены проблемы, раздел  **Самотестирование** будет отмечен желтым маркером .

Чтобы запустить самотестирование ViPNet EPP Агент:

- 1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
- 2 Выберите  **Самотестирование > Самотестирование**.
- 3 Нажмите **Запустить сейчас** и дождитесь результатов.

Результаты самотестирования отобразятся на вкладке **Самотестирование**.

## Журнал самотестирования

Результаты самотестирования, выполненного автоматически или вручную, регистрируются в журнале аудита (см. [Журнал аудита](#)), а также дублируются в журнал самотестирования ViPNet EPP Агент.

Чтобы просмотреть журнал самотестирования ViPNet EPP Агент:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.

2 Выберите  **Самотестирование > Журнал**.

Отобразится список зарегистрированных событий запуска и завершения самотестирования. Каждая запись о событии в журнале содержит:

- **Дата и время** — дата и время, когда событие произошло.
- **Результат** — успех или ошибка.
- **Событие** — название события.
- **Инициатор**:
  - Система (для самотестирования, запущенного автоматически по расписанию).
  - Администратор ViPNet EPP Агент (для самотестирования, запущенного вручную администратором).

3 Для поиска событий в журнале используйте фильтр:

3.1 Нажмите  и укажите промежуток времени, в течение которого происходили искомые события.

3.2 Нажмите  и задайте параметры фильтрации: по результату, инициатору, событию.

3.3 Нажмите **Сохранить**.

4 Чтобы обновить журнал, на панели сверху нажмите .

## Диагностические журналы

Диагностические журналы сохраняются в папке `/var/log/epp-agent/`.

Уровень детализации диагностических журналов можно изменить в [командном интерпретаторе ViPNet EPP Агент](#).

## Просмотр сведений о программе и лицензии

Чтобы просмотреть сведения о программе, лицензии ViPNet EPP Агент и ознакомиться с лицензионным соглашением на использование ViPNet EPP:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.

2 Выберите  **О программе > Основное** и посмотрите сведения о ViPNet EPP Агент:

- Версии ПО и базы правил.
- Контактная информация ИнфоТеКС.

3 Выберите вкладку **Лицензия** и посмотрите сведения о лицензии ViPNet EPP Агент:

- Статус лицензии: не загружена, не активирована, активирована, истек срок действия.
- Срок действия — дата окончания действия лицензии или бессрочная лицензия.
- Срок действия подписки на обновление базы правил.
- Идентификатор.
- Тип лицензии: автономная или лицензия сервера.
- Состав лицензии: список доступных модулей и срок действия лицензии на них.

4 Для ознакомления с лицензионным соглашением на использование ViPNet EPP выберите вкладку **Лицензионное соглашение**.

## Уведомления об изменении настроек модулей защиты и обновлении ViPNet SafeBoot

На защищаемом узле могут появляться всплывающие уведомления в области уведомлений панели задач ОС GNU/Linux:

- о смене статуса выполнения политики ZTNA;
- о полученном обновлении ViPNet SafeBoot и более длительной следующей загрузке компьютера из-за применения обновления (появляется только если ViPNet SafeBoot было установлено ранее и ViPNet EPP Агент под управлением сервера for Windows).

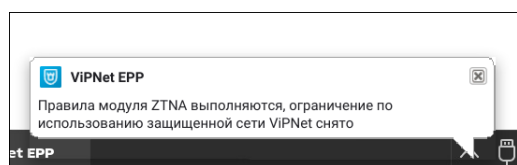


Рисунок 50. Пример уведомления о смене статуса выполнения политики ZTNA

Чтобы появлялись уведомления на защищаемом узле с ОС Debian Linux 12 (bookworm):

1 Пропишите репозитории в `/etc/apt/sources.list`:

```
deb http://deb.debian.org/debian bookworm main contrib non-free non-free-firmware
deb-src http://deb.debian.org/debian bookworm main contrib non-free non-free-firmware
deb http://deb.debian.org/debian-security/ bookworm-security main contrib non-free non-free-firmware
deb-src http://deb.debian.org/debian-security/ bookworm-security main contrib non-free non-free-firmware
deb http://deb.debian.org/debian bookworm-updates main contrib non-free non-free-firmware
deb-src http://deb.debian.org/debian bookworm-updates main contrib non-free non-free-firmware
```

2 В командной строке выполните команду:

```
sudo apt update
```

3 Установите пакет `gnome-shell-extension-top-icons-plus` с помощью команды:

```
sudo apt install gnome-shell-extension-top-icons-plus
```

- 4 Перезагрузите компьютер.
- 5 В меню приложений выберите **Расширения** и включите расширение **TopIcons Plus**.

# Управление с помощью командного интерпретатора

## Подключение к ViPNet EPP Агент



**Совет.** В целях безопасности рекомендуем подключаться к ViPNet EPP Агент и выполнять команды в командном интерпретаторе только пользователям с правами суперпользователя ОС GNU/Linux, чтобы непривилегированные пользователи ОС не смогли сохранить в истории ОС введенные команды с аутентификационными данными пользователей ViPNet EPP.

Чтобы подключиться к ViPNet EPP Агент и выполнить команду управления:

**1** Выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя> <команда управления>
```

где <команда управления> — команда из списка групп команд, доступных для управления ViPNet EPP Агент в командном интерпретаторе, см. в разделе [Интерфейс командного интерпретатора](#).

**2** В запросе **Password** введите пароль пользователя. При вводе пароль не отображается.

При установке ViPNet EPP Агент была создана учетная запись администратора агента с параметрами: имя пользователя — `admin`, пароль — `admin`. При первом запуске ViPNet EPP Агент используйте эту учетную запись. Рекомендуем сразу же сменить пароль по умолчанию (см. [Управление учетными записями](#)).



**Внимание!** Если вы три раза подряд введете неверные данные учетной записи, возможность аутентификации и запуска команд в командном интерпретаторе ViPNet EPP Агент будет заблокирована на три минуты.

При успешной аутентификации пользователю будут доступны действия согласно его полномочиям (см. [Полномочия пользователей](#)).



**Примечание.** При выполнении любой команды в командном интерпретаторе необходимы вызов утилиты управления ViPNet EPP Агент `epp_mc_cli` и аутентификация пользователя. В дальнейшем описании выполнения команд упоминание ввода пароля пользователя в запросе **Password** будет опущено для краткости.

# Интерфейс командного интерпретатора

В [командном интерпретаторе](#) используются текстовые команды и параметры, состоящие из латинских и специальных символов. Команды разделяются пробелами.

Для облегчения работы в интерпретаторе предусмотрено:

- Контекстная справка

Контекстная справка позволяет просмотреть информацию о командах и параметрах, ввод которых возможен в текущей ситуации. Контекстная справка вызывается с помощью ввода «-h» или «--help».

- Сочетания клавиш

Командный интерпретатор поддерживает стандартные сочетания клавиш, перечисленные в таблице ниже.

Таблица 4. Поддерживаемые интерпретатором сочетания клавиш

| Сочетание клавиш | Действие                                |
|------------------|-----------------------------------------|
| Ctrl+U           | стереть все от начала строки до курсора |
| Ctrl+K           | стереть все от курсора до конца строки  |
| Ctrl+A           | перейти в начало строки                 |
| Ctrl+E           | перейти в конец строки                  |
| Ctrl+B           | перейти на один символ назад            |
| Ctrl+F           | перейти на один символ вперед           |
| Ctrl+H           | стереть символ за курсором              |
| Ctrl+W           | стереть слово перед курсором            |

Редактирование команд доступно обычным способом: стирать символы клавишей **Backspace** или **Delete**, перемещаться по тексту с помощью клавиш со стрелками влево и вправо. Все введенные в текущем сеансе работы командного интерпретатора команды запоминаются. Для повторного ввода команд из истории используйте клавиши со стрелками вниз и вверх.

При выполнении каждой команды в командном интерпретаторе необходим вызов утилиты управления ViPNet EPP Агент `epp_mc_cli` и аутентификация пользователя (см. [Подключение к ViPNet EPP Агент](#)). Для вызова контекстной справки аутентификация пользователя не требуется.

Чтобы просмотреть список всех доступных групп команд, выполните команду вызова контекстной справки:

```
/opt/epp-agent/bin/epp_mc_cli -h
```

Группы команд управления ViPNet EPP Агент:

- `rulebase` — работа с базой правил (см. [Просмотр версии используемой базы правил](#));
- `audit-journal` — работа с журналом аудита (см. [Журнал аудита](#));

- `pfw` — настройка межсетевого экрана (см. [Управление фильтрацией трафика](#));
- `hips` — [управление обнаружением и предотвращением вторжений](#);
- `server` — настройка параметров подключения к ViPNet EPP Сервер (см. [Просмотр и изменение адреса ViPNet EPP Сервер](#));
- `users` — [управление учетными записями](#);
- `agent` — настройки параметров ViPNet EPP Агент (см. [Просмотр и управление параметрами работы](#)).
- `ztna` — [просмотр статуса выполнения политики ZTNA](#). Недоступно для автономного ViPNet EPP Агент.

Чтобы просмотреть список доступных команд для одной из групп команд управления, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli <наименование группы команд управления> -h
```

Для выполнения всех команд (кроме контекстной справки) служба ViPNet EPP Агент `epp_supervisor.service` должен быть запущен.

## Управление фильтрацией трафика

Для настройки межсетевого экрана предназначены команды группы `pfw`:

```
Usage: pfw [OPTIONS] SUBCOMMAND

Options:
  -h, --help          Print this help message and exit

Subcommands:
  get-mode             get pfw mode
  set-mode             set pfw mode
  traffic-journal      traffic journal submodule
  active-connections  active connections submodule
  schedule-collection  schedule collection submodule
  address-collection  address collection submodule
  protocol-collection  protocol collection submodule
  rules               rules submodule
```

Рисунок 51. Синтаксис и список команд группы `pfw`

- `get-mode` — просмотр текущего режима работы;
- `set-mode` — изменение режима работы;
- `traffic-journal` — просмотр журнала трафика и его параметров;
- `active-connections` — просмотр активных соединений;
- `schedule-collection` — управление пользовательскими справочниками расписаний;
- `address-collection` — управление пользовательскими справочниками адресов и сетей;
- `protocol-collection` — управление пользовательскими справочниками протоколов;

- `rules` — управление пользовательскими фильтрами.

## Просмотр и выбор режима работы

Чтобы посмотреть текущий режим работы межсетевого экрана ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора, аудитора или пользователя агента> pfw get-mode
```

Список обозначений режимов:

- `block` — Полная блокировка трафика.
- `public` — Публичная сеть.
- `private` — Частная сеть.
- `protected` — Корпоративная сеть.
- `off` — Отключен.

Чтобы изменить режим работы межсетевого экрана ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора, аудитора агента> pfw set-mode {block|public|private|protected|off},
```

указав в параметрах команды значение нужного режима из перечисленных вариантов.

## Просмотр журнала трафика

При переполнении журнала трафика в соответствии с параметрами работы выполняется автоматическая ротация событий и журналов (см. [Просмотр и настройка параметров работы](#)).

Чтобы посмотреть параметры хранения журнала трафика, полученные с сервера, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора> pfw traffic-journal show-config
```

В результате отобразятся: максимальное число записей в журнале; количество записей, удаляемых при достижении максимального значения записей и срок хранения записей журнала в днях.

Чтобы посмотреть журнал регистрации трафика межсетевого экрана ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора или аудитора агента> pfw traffic-journal show
```

В результате отобразится список записей журнала. Каждая запись будет содержать:

- **packet count** — количество зарегистрированных однотипных IP-пакетов за указанный период времени.

- **packet info:**
  - **mode** — режим, при котором были зарегистрированы пакеты.
  - **action** — действие, выполненное с пакетом.
  - **rule** — тип фильтра.
  - **protocol** — протокол, по которому были переданы пакеты.
  - **source** — источник пакета (IP-адрес, порт).
  - **destination** — назначение пакета (IP-адрес, порт).
  - **time point** — дата и время каждого зарегистрированного однотипного пакета.

Чтобы в журнале регистрации трафика межсетевого экрана ViPNet EPP Агент найти определенные события, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора или аудитора агента> pfw traffic-journal show [--time-format=<формат даты и времени>]
[--time-order={undefined|ascending|descending}] [--from-time=<дата и время начала интервала поиска>]
[--to-time=<дата и время окончания интервала поиска>]
[--protocol={tcp|udp|icmp|icmpv6}] [--action={drop|accept|ask}]
[--mode={block|public|private|protected}] [--rule-type={pfw|default|appc}]
```

и укажите нужные параметры фильтра поиска:

- `[--time-format=<формат даты и времени>]` — формат ввода даты и времени в параметрах `from-time` и `to-time`. Требуется указывать только для изменения формата ввода по умолчанию. По умолчанию используется формат `%m-%d-%YT%H:%M:%S`:
  - `%m` — месяц;
  - `%d` — день;
  - `%Y` — год;
  - `%H` — часы;
  - `%M` — минуты;
  - `%S` — секунды.
- `[--time-order={undefined|ascending|descending}]` — формат сортировки событий:
  - `undefined` — не сортировать события.
  - `ascending` — сортировать по времени последнего пакета в группе пакетов.
  - `descending` — сортировать по времени последнего пакета в группе пакетов в порядке убывания.
- `[--from-time=<дата и время начала интервала поиска>]` — дата и время начала интервала поиска событий в формате `time-format`, например `--from-time=09-20-2021T10:12:14`.
- `[--to-time=<дата и время окончания интервала поиска>]` — дата и время окончания интервала поиска событий в формате `time-format`.
- `[--protocol={tcp|udp|icmp|icmpv6}]` — протокол, по которому передаются IP-пакеты.

- `[--action={drop|accept}]` — действие, выполненное с пакетом в результате срабатывания сетевого фильтра:
  - `drop` — заблокирован.
  - `accept` — разрешен.
- `[--mode={block|public|private|protected}]` — режим, в котором был применен сетевой фильтр.
- `[--rule-type={rules_pfw|rules_default|appc}]` — тип фильтра:
  - `rules_pfw` — фильтры политик безопасности.
  - `rules_default` — фильтры по умолчанию.
  - `appc` — правила блокировки соединений.

## Просмотр активных соединений

Межсетевой экран ViPNet EPP Агент отслеживает сетевую активность приложений защищаемого узла. Вы можете просмотреть приложения, которые в настоящий момент работают с сетевыми ресурсами — имеют активные соединения, и параметры соединений в журнале активных соединений межсетевого экрана ViPNet EPP Агент. При обнаружении подозрительной сетевой активности приложений вы можете заблокировать исходящий трафик этих приложений.

Чтобы просмотреть список приложений, работающих с сетевыми ресурсами, в журнале активных соединений ViPNet EPP Агент выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора или аудитора агента> pfw active-connections show
```

Чтобы заблокировать приложение, работающее с сетевыми ресурсами, и создать пользовательский блокирующий фильтр в указанном режиме работы, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>
pfw active-connections block --path=<абсолютный путь к приложению>
--mode={private|protected},
```

указав в параметре `--mode` значение режима из перечисленных вариантов, в котором будет создан блокирующий фильтр. Фильтры могут быть созданы только в режимах **Частная сеть** (`private`) и **Корпоративная сеть** (`protected`).

Чтобы просмотреть все заблокированные приложения, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента
или аудитора агента> pfw active-connections show-blocked
```

Чтобы разблокировать приложение и удалить пользовательский блокирующий фильтр, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
pfw active-connections unblock --path=<абсолютный путь к приложению>  
--mode={public|private|protected},
```

указав в параметре `--mode` значение нужного режима из перечисленных вариантов, в котором был создан блокирующий фильтр.

## Настройка пользовательских фильтров

Для учета особенностей фильтрации IP-пакетов на защищаемых узлах можно создавать пользовательские фильтры для режимов частной и корпоративной сетей. Для настройки пользовательских фильтров межсетевого экрана предназначены команды подгруппы `rules` группы `pfw`:

- `show` — просмотр списка пользовательских фильтров;
- `delete` — удаление пользовательского фильтра;
- `add` — добавление пользовательского фильтра;
- `disable` — отключение пользовательского фильтра;
- `enable` — включение пользовательского фильтра;
- `up` — переместить пользовательский фильтр в списке на одну позицию вверх;
- `down` — переместить пользовательский фильтр в списке на одну позицию вниз;

Чтобы посмотреть список пользовательских фильтров, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора или  
аудитора агента> pfw rules show
```

В результате фильтры отобразятся в порядке их применения. Для каждого фильтра будут отображены: название фильтра, идентификатор фильтра (ID) и параметры фильтра.

Чтобы добавить пользовательский фильтр, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
pfw rules add --name=<название фильтра> --action={drop|accept} --mode={private|protected}  
[--ip-version={4|6}] [--src-addr=<идентификатор справочника адресов>]  
[--dst-addr=<идентификатор справочника адресов>] [--protocols=<идентификатор  
справочника протоколов>] [--schedules=<идентификатор справочника расписаний>],
```

указав нужные параметры фильтра:

- `--name=<название фильтра>` — введите название создаваемого пользовательского фильтра.
- `--action={drop|accept}` — действие фильтра при срабатывании:
  - `drop` — блокировать IP-пакеты.
  - `accept` — пропускать IP-пакеты.
- `--mode={private|protected}` — режим, в котором будет создан фильтр.

- `[--ip-version={4|6}]` — версия IP-протокола:
  - 4 — IP v4, значение используется по умолчанию, если параметр не задавать.
  - 6 — IP v6.
- `[--src-addr=<идентификатор справочника адресов>]` — адреса отправителей IP-пакетов. Укажите идентификатор (ID) нужного справочника. Если параметр не задавать, фильтр будет применяться к IP-пакетам с любыми адресами отправителя.
- `[--dst-addr=<идентификатор справочника адресов>]` — адреса получателей IP-пакетов. Укажите идентификатор (ID) нужного справочника. Если параметр не задавать, фильтр будет применяться к IP-пакетам с любыми адресами получателя.
- `[--protocols=<идентификатор справочника протоколов>]` — протоколы передачи пакетов. Укажите идентификатор (ID) нужного справочника. Если параметр не задавать, фильтр будет применяться к IP-пакетам, передаваемым по всем протоколам.
- `[--schedules=<идентификатор справочника расписаний>]` — справочники расписаний. Укажите идентификатор (ID) нужного справочника. Если параметр не задавать, фильтр будет действовать постоянно.

Идентификаторы справочников вы можете посмотреть с помощью команды просмотра справочников (см. [Настройка пользовательских справочников](#)).

Чтобы задать порядок применения пользовательских фильтров, перемещайте созданные фильтры вверх или вниз:

- Чтобы переместить фильтр вверх, выполните команду:
 

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw rules up <идентификатор фильтра (ID)>
```
- Чтобы переместить фильтр вниз, выполните команду:
 

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw rules down <идентификатор фильтра (ID)>
```

Чтобы временно отключить созданный пользовательский фильтр, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw rules disable <идентификатор фильтра (ID)>
```

Чтобы снова включить созданный пользовательский фильтр, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw rules enable <идентификатор фильтра (ID)>
```

Чтобы удалить созданный пользовательский фильтр, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw rules delete <идентификатор фильтра (ID)>
```

## Настройка пользовательских справочников

При создании и изменении пользовательских фильтров применяются пользовательские справочники протоколов, адресов и сетей, расписаний. Справочники позволяют упростить процессы создания и изменения сетевых фильтров. Справочники устанавливаются и обновляются на защищаемом узле вместе с ViPNet EPP Агент. Вы можете добавлять новые справочники.

Если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5, применяются также пользовательские справочники адресов сети ViPNet, которые можно использовать при создании пользовательских сетевых фильтров для защищенной сети ViPNet.

Просмотр пользовательских справочников:

- Чтобы просмотреть все пользовательские справочники протоколов, выполните команду:  

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента или аудитора агента> pfw protocol-collection show
```
- Чтобы просмотреть все пользовательские справочники адресов и сетей, выполните команду:  

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента или аудитора агента> pfw address-collection show
```
- Чтобы просмотреть все пользовательские справочники расписаний, выполните команду:  

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента или аудитора агента> pfw schedule-collection show
```
- Чтобы просмотреть пользовательские справочники адресов сети ViPNet, выполните команду:  

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента или аудитора агента> pfw address-collection vpn-list-show
```

Удаление пользовательских справочников:

- Чтобы удалить пользовательский справочник протоколов, выполните команду:  

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw protocol-collection delete <идентификатор справочника (ID)>
```
- Чтобы удалить пользовательский справочник адресов и сетей, выполните команду:  

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw address-collection delete <идентификатор справочника (ID)>
```
- Чтобы удалить пользовательский справочник расписаний, выполните команду:  

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> pfw schedule-collection delete <идентификатор справочника (ID)>
```

Добавление новых справочников:

- [Добавление справочника протоколов.](#)
- [Добавление справочников адресов и сетей.](#)
- [Добавление справочника расписаний.](#)

## Добавление справочника протоколов

Чтобы добавить пользовательский справочник протоколов, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
pfw protocol-collection add --name=<название справочника> [--ip-version={4|6}]  
[--tcp-ports=<номера портов1>,<номера портов2>,...<номера портовN>] [--udp-ports=<номера  
портов1>,<номера портов2>,...<номера портовN>] [--icmps=<тип и код сообщения1>,<тип и код  
сообщения2>,...<тип и код сообщенияN>] [--except-tcp-ports=<номера портов1>,<номера  
портов2>,...<номера портовN>] [--except-udp-ports=<номера портов1>,<номера  
портов2>,...<номера портовN>] [--except-icmps=<тип и код сообщения1>,<тип и код  
сообщения2>,...<тип и код сообщенияN>],
```

указав нужные параметры справочника:

- `--name=<название справочника>` — введите название создаваемого справочника.
- `--ip-version={4|6}` — версия IP-протокола:
  - 4 — IP v4.
  - 6 — IP v6.
- `--tcp-ports=<номера портов>` — задайте один или несколько номеров TCP-портов источника и назначения. Формат задания `<номера портов>`:
  - `<номер порта>-` — порт источника.
  - `-<номер порта>` — порт назначения.
  - `<номер порта1>-<номер порта2>` — порт источника и порт назначения.
  - `<номер порта1>:<номер порта2>-` — диапазон портов источника.
  - `-<номер порта1>:<номер порта2>-` — диапазон портов назначения.
  - `<номер порта1>:<номер порта2>-<номер порта3>:<номер порта4>` — диапазоны портов источника и назначения.
- `--udp-ports=<номера портов>` — задайте один или несколько номеров UDP-портов источника и назначения. Формат задания `<номера портов>` такой же, как для `--tcp-ports` (см. выше).
- `--icmps=<тип и код сообщения1>,<тип и код сообщения2>,...<тип и код сообщенияN>` — задайте один или несколько типов и кодов ICMP-сообщений, разделяя значения запятыми. Формат задания `<тип и код сообщения>`:
  - `<тип сообщения>[/<код сообщения>]` — укажите тип и при необходимости код ICMP-сообщения.
- `--except-tcp-ports=<номера портов>` — задайте номера TCP-портов, которые будут исключены из справочника. Формат задания `<номера портовN>` такой же, как для `--tcp-ports` (см. выше).
- `--except-udp-ports=<номера портов>` — задайте номера UDP-портов, которые будут исключены из справочника. Формат задания `<номера портовN>` такой же, как для `--udp-ports` (см. выше).

- `[--except-icmps=<тип и код сообщения1>,<тип и код сообщения2>,...<тип и код сообщенияN>]` — задайте типы и коды ICMP-сообщений, которые будут исключены из справочника. Формат задания `<тип и код сообщенияN>` такой же, как для `--icmps` (см. выше).

## Добавление справочников адресов и сетей

Если на защищаемом узле установлена программа ViPNet Client 4U или ViPNet Client 5, доступно создание пользовательских справочников адресов сети ViPNet, которые можно использовать при создании пользовательских сетевых фильтров для трафика защищенной сети ViPNet (см. [Настройка пользовательских фильтров](#)).

Чтобы добавить пользовательский справочник адресов и сетей, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>
pfw address-collection add --name=<название справочника> [--type={ip|vpn}]
[--ip-version={4|6}] [--addr=<IP-адреса>] [--except-addr=<IP-адреса>]
[--vpn-nodes=<идентификаторы сетевых узлов ViPNet>],
```

указав нужные параметры справочника:

- `--name=<название справочника>` — введите название создаваемого справочника.
- `[--type={ip|vpn}]` — тип создаваемого справочника:
  - `ip` — обычный пользовательский справочник, значение используется по умолчанию, если параметр не задавать.
  - `vpn` — пользовательских справочников адресов сети ViPNet.
- `[--ip-version={4|6}]` — версия IP-протокола.
- `[--addr=<IP-адреса>]` — задайте один или несколько IP-адресов в одном из следующих форматов:
  - `<IP-адрес>` — один IP-адрес.
  - `<IP-адрес1>,<IP-адрес2>,...<IP-адресN>` — несколько IP-адресов.
  - `<IP-адрес1>-<IP-адрес2>` — диапазон IP-адресов.
  - `<IP-адрес>/<Маска подсети>` — подсеть. Например, `68.21.12.34/255.255.252.0`.
  - `<IP-адрес>/<Маска подсети в формате CIDR>` — подсеть. Например, `192.168.201.1/24`.
- `[--except-addr=<IP-адреса>]` — задайте IP-адреса, которые будут исключены из справочника. Формат задания `<IP-адреса>` такой же, как для `--addr` (см. выше).
- `[--vpn-nodes=<идентификаторы сетевых узлов ViPNet>]` — этот параметр нужно использовать для создания пользовательских справочников адресов сети ViPNet. Задайте идентификаторы сетевых узлов ViPNet в формате:
  - `<идентификатор сетевого узла ViPNet>` — один сетевой узел ViPNet.
  - `<идентификатор сетевого узла ViPNet1>,<идентификатор сетевого узла ViPNet2>,...<идентификатор сетевого узла ViPNetN>` — несколько сетевых узлов ViPNet.

## Добавление справочника расписаний

Чтобы добавить пользовательский справочник расписаний, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
pfw schedule-collection add --name=<название справочника> [--weekdays=<дни недели>]  
[--date-range=<диапазон дат>] [--daytime-range=<диапазон времени>]  
[--except-weekdays=<дни недели>] [--except-date-range=<диапазон дат>]  
[--except-daytime-range=<диапазон времени>],
```

указав нужные параметры справочника:

- `--name=<название справочника>` — введите название создаваемого справочника.
- `[--weekdays=<дни недели>]` — выполнять действие в указанные дни недели. Для указания дней недели используйте цифры от 1 до 7, что соответствует дням с понедельника по воскресенье. Укажите один или несколько дней недели, разделяя запятой. Например, `--weekdays=1,3,5`
- `[--date-range=<диапазон дат>]` — выполнять действие в указанный диапазон дат. Формат задания `<диапазон дат>`: `dd.mm.yyyy:dd.mm.yyyy`. Например, `--date-range=01.12.2021:25.12.2021`
- `[--daytime-range=<диапазон времени>]` — выполнять действие в указанный диапазон времени. Формат задания `<диапазон времени>`: `HH:MM:SS-HH:MM:SS`. Например, `--daytime-range=08:00:00-22:20:00`
- `[--except-weekdays=<дни недели>]` — задайте дни недели, которые будут исключены из справочника. Формат задания такой же, как для `--weekdays` (см. выше).
- `[--except-date-range=<диапазон дат>]` — задайте диапазон дат, который будет исключен из справочника. Формат задания такой же, как для `--date-range` (см. выше).
- `[--except-daytime-range=<диапазон времени>]` — задайте диапазон времени, который будет исключен из справочника. Формат задания такой же, как для `--daytime-range` (см. выше).

## Просмотр статуса выполнения политики ZTNA

Политики ZTNA (см. [Сетевой доступ с нулевым доверием \(ZTNA\)](#)) для группы защищаемых узлов устанавливаются централизованно при назначении на группу базы правил.

Для работы с политиками ZTNA предназначены команда группы `ztna: show` — просмотр статуса выполнения политики ZTNA.

Чтобы посмотреть статус выполнения политики ZTNA, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора,  
аудитора или пользователя агента> ztna show
```

В результате отобразится один статусов:

- **on, acceptable** — защищаемый узел прошел проверку в соответствии со всеми заданными правилами политики ZTNA.

- **on, not acceptable** — защищаемый узел не прошел проверку по заданным правилам политики ZTNA. В списке будут перечислены правила, параметрам которого не соответствует защищаемый узел.
- **off** — политики ZTNA выключены.

Подробнее о статусах см. в разделе [Просмотр и настройка режимов работы модулей защиты](#).

## Управление обнаружением и предотвращением вторжений

Для управления обнаружением и предотвращением вторжений ViPNet EPP Агент предназначены команды группы `hips`:

- `get-mode` — просмотр текущего режима работы;
- `set-mode` — изменение режима работы.

Чтобы посмотреть текущий режим работы обнаружения и предотвращения вторжений ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора, аудитора или пользователя агента> hips get-mode
```

Список обозначений режимов:

- `high` — Усиленный.
- `medium` — Базовый.
- `low` — Минимальный.
- `off` — Отключен.

Чтобы изменить режим работы обнаружения и предотвращения вторжений ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора, аудитора или пользователя агента> hips set-mode {off|low|medium|high},
```

указав в параметрах команды значение нужного режима из перечисленных вариантов.

## Журнал аудита

События, вызванные действиями пользователей ViPNet EPP Агент, а также системные события и результаты самотестирования ViPNet EPP Агент регистрируются в журнале аудита ViPNet EPP Агент.

При переполнении журнала аудита в соответствии с параметрами работы выполняется автоматическая ротация событий и журналов (см. [Просмотр и настройка параметров работы](#)).

Для работы с журналом аудита предназначены команды группы `audit-journal`:

- `show-config` — просмотр настроек журнала аудита;
- `list-types` — отображение полного списка событий аудита, которые могут быть зарегистрированы в журнале аудита.
- `show` — просмотр журнала аудита.

Чтобы посмотреть [параметры хранения журнала аудита, полученные с сервера](#), выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
audit-journal show-config
```

В результате отобразятся: максимальное число записей в журнале; количество записей, удаляемых при достижении максимального значения записей и срок хранения записей журнала в днях.

Чтобы посмотреть журнал аудита ViPNet EPP Агент за последние сутки, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора или  
аудитора агента> audit-journal show
```

В результате отобразится список записей журнала. Каждая запись будет содержать:

- **time** — дата и время, когда событие зарегистрировано.
- **status** — действие, вызвавшее событие, успешно (success) или не успешно (fail).
- **type** — название события.
- **requester** — инициатор действия (система, пользователи).
- **receiver** — на что или кого направлено действие (пользователи, устройства).
- **info** — подробная информация о событии (при наличии).

Чтобы посмотреть список всех существующих в ViPNet EPP событий аудита, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора или  
аудитора агента> audit-journal list-types
```

Отобразится пронумерованный список событий. Номера событий можно использовать для поиска определенных событий, зарегистрированных в журнале аудита.

Чтобы в журнале аудита ViPNet EPP Агент найти определенные события, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора или  
аудитора агента> audit-journal show [--types=<номер события>] [--time-format=<формат даты  
и времени>] [--from-time=<дата и время начала интервала поиска>] [--to-time=<дата и время  
окончания интервала поиска>] [--status={fail|success}],
```

указав нужные параметры фильтра поиска (порядок параметров может быть любым):

- `[--types=<номер события>]` — задайте номер события аудита для поиска в журнале. Номер события выбирается из списка, который выводится с помощью вышеописанной команды `list-types`. Вы можете указать только один номер. Например, `--type=1`.
- `[--time-format=<формат даты и времени>]` — формат ввода даты и времени в параметрах `from-time` и `to-time`. Требуется указывать только для изменения формата ввода по умолчанию. По умолчанию используется формат `%m-%d-%YT%H:%M:%S`
- `[--from-time=<дата и время начала интервала поиска>]` — дата и время начала интервала поиска событий в формате `time-format`, например `--from-time=09-20-2021T10:12:14`.
- `[--to-time=<дата и время окончания интервала поиска>]` — дата и время окончания интервала поиска событий в формате `time-format`.
- `[--status={fail|success}]` — статус завершения действия в событии:
  - `fail` — ошибка.
  - `success` — успех.

# Администрирование ViPNet EPP Агент

## Просмотр и управление параметрами работы

Для просмотра и управления параметрами работы ViPNet EPP Агент предназначены команды группы `agent`.

- `version` — просмотр номера версии ViPNet EPP Агент;
- `show-license` — просмотр информации о лицензии ViPNet EPP;
- `show-settings` — просмотр всех параметров работы ViPNet EPP Агент;



**Примечание.** Команды `get-log-level` и `set-log-level` могут потребоваться при сбоях в работе ViPNet EPP Агент для формирования диагностического журнала (см. [Диагностические журналы](#)) с уровнем детализации, запрошенным специалистами ИнфоТекС.

---

- `get-log-level` — просмотр установленного уровня детализации журнала для диагностики работы ViPNet EPP Агент;
- `set-log-level` — изменение уровня детализации журнала для диагностики работы ViPNet EPP Агент;
- `get-net-interfaces` — просмотр списка контролируемых сетевых интерфейсов;
- `set-net-interfaces` — изменение списка контролируемых сетевых интерфейсов;

- `self-check` — проверка работоспособности ViPNet EPP Агент (см. [Проверка работоспособности](#)).

Чтобы посмотреть номер версии ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента, аудитора агента или пользователя агента> agent version
```

Чтобы посмотреть информацию о лицензии ViPNet EPP, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента или аудитора агента> agent show-license
```

Чтобы посмотреть настройки параметров работы ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> agent show-settings
```

Чтобы посмотреть установленный уровень детализации информации в служебном журнале для диагностики работы ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> agent get-log-level
```

Чтобы изменить уровень детализации записываемой информации в служебные журналы для диагностики работы ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> agent set-log-level --level={trace|debug|info|warning|error|fatal}
```

указав в параметре `level` уровень детализации, запрошенный специалистами ИнфоТеКС. Затем перезапустите службу `epp_supervisor.service` (см. [Запуск и остановка ViPNet EPP Агент](#)).

Чтобы посмотреть список контролируемых сетевых интерфейсов, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> agent get-net-interfaces
```

Чтобы изменить контролируемые сетевые интерфейсы, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> agent set-net-interfaces <имя интерфейса>[,<имя интерфейса 2>...],
```

указав имена нужных интерфейсов. Затем перезапустите службу `epp_supervisor.service` (см. [Запуск и остановка ViPNet EPP Агент](#)).

## Проверка работоспособности

Для проверки работоспособности ViPNet EPP Агент предназначено самотестирование. Кроме автоматического самотестирования, которое выполняется по расписанию (см. [Настройка параметров защищаемых узлов](#)), администратор может запустить самотестирование ViPNet EPP Агент вручную.

В ходе самотестирования проверяется и фиксируется:

- Целостность журнала аудита (**Audit journal integrity**), целостность журнала трафика (**PFW traffic journal integrity**), целостность журнала событий (**Events journal integrity**) — нарушена (broken) или не нарушена (not violated).

Если целостность одного или нескольких журналов нарушена:

- Текущий журнал, целостность которого нарушена, будет сохранен в каталоге установки ViPNet EPP Агент в файлах:
  - `/etc/epp-agent/audit_journal.db.backup` — журнал аудита;
  - `/etc/epp-agent/traffic_journal.db.backup` — журнал трафика;
  - `/etc/epp-agent/events_journal.db.backup` — журнал событий.
- Из текущего журнала, целостность которого нарушена, будут удалены все события и зарегистрируется первое событие о восстановлении работоспособности после нарушения целостности соответствующего журнала:
  - **audit journal corrupted** — в журнале аудита;
  - **pfw traffic journal corrupted** — в журнале трафика.
- Дата и время обновления базы правил, версия базы правил (**Current rule version** и **Current rule received**).
- Состояние подключения к базе данных ViPNet EPP Агент (**DB connected**) — завершено успешно (success) или завершено с ошибкой.
- Версия ViPNet EPP Агент (**EPP agent version**).
- Режимы работы обнаружения и предотвращения вторжений (**HIPS mode different from server**) и межсетевого экрана (**PFW mode different from server**) — установлены из базы правил сервера (yes) или локально администратором агента (no).
- Дата и время проведения самотестирования (**Self-test time**).
- Состояние подключения к ViPNet EPP Сервер (**Server connection state**):
  - Ожидает подключения (request) — находится в группе **Запросы на подключение ViPNet EPP Сервер**.
  - Подключен (active) — перемещен из группы **Запросы на подключение** в одну из пользовательских групп ViPNet EPP Сервер.
  - Удален (delete) — не посылает запросы на подключение к ViPNet EPP Сервер.

Результаты самотестирования, выполненного автоматически или вручную, регистрируются в журнале аудита ViPNet EPP Агент (см. [Журнал аудита](#)) и передаются на ViPNet EPP Сервер.

Чтобы запустить самотестирование ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
agent self-check
```

## Просмотр версии используемой базы правил

Чтобы посмотреть номер версии базы правил, используемой в ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента,  
аудитора агента или пользователя агента> rulebase show
```



**Примечание.** При выполнении команды сразу после обновления базы правил, отобразятся старая и новая базы правил. После применения новой базы правил, старая версия базы правил отображаться не будет.

---

## Просмотр и изменение адреса ViPNet EPP Сервер

При изменении адресного пространства сети, в которой уже используется ViPNet EPP, может потребоваться изменение адреса (IP-адреса или доменного имени) ViPNet EPP Сервер и номера порта в настройках ViPNet EPP Агент. Для просмотра и изменения адреса ViPNet EPP Сервер предназначены команды группы `server`:

Чтобы посмотреть текущий адрес ViPNet EPP Сервер, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
server get-address
```

Чтобы изменить адрес ViPNet EPP Сервер, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
server set-address <IP-адрес или доменное имя>
```

Чтобы посмотреть номер используемого порта ViPNet EPP Сервер, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
server get-port
```

Чтобы изменить номер используемого порта ViPNet EPP Сервер, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
server set-port <номер порта>
```

## Управление учетными записями

При установке ViPNet EPP Агент автоматически создается учетная запись администратора агента. Для создания новых учетных записей и редактирования существующих предназначены команды группы `users`.

- `add-user` — добавление новой учетной записи;
- `show-user` — просмотр данных об учетной записи;
- `show-users` — просмотр информации обо всех учетных записях;
- `remove-user` — удаление учетной записи;
- `update-password` — изменение пароля учетной записи.

Чтобы добавить учетную запись ViPNet EPP Агент:

### 1 Выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> users add-user --login=<имя учетной записи> --role={administrator|auditor|user} --name=<имя пользователя> [--easy-password]
```

и укажите нужные параметры:

- в параметре `role` укажите нужную роль:
  - `administrator` — администратор агента;
  - `auditor` — аудитор агента;
  - `user` — пользователь агента.
- чтобы задать простой пароль, не соответствующий требованиям к паролям, укажите `--easy-password`

В целях безопасности использовать простые пароли не рекомендуется.

- 2 В запросе **Password** введите пароль текущего пользователя. При вводе пароль не отображается.
- 3 В запросе **New user password** введите пароль новой учетной записи [в соответствии с требованиями](#). Если указан параметр `--easy-password`, введите любой пароль. При вводе пароль не отображается.
- 4 В запросе **Confirm new user password** подтвердите пароль новой учетной записи. При вводе пароль не отображается.

Чтобы просмотреть данные учетной записи ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> users show-user --login=<имя пользователя учетной записи>
```

Чтобы просмотреть данные обо всех учетных записях ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> users show-users
```

Чтобы удалить учетную запись ViPNet EPP Агент, выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента>  
users remove-user --login=<имя пользователя учетной записи>
```

Чтобы сменить пароль учетной записи ViPNet EPP Агент:

1 Выполните команду:

```
/opt/epp-agent/bin/epp_mc_cli --login=<имя пользователя с правами администратора агента> users update-password [--easy-password]
```

укажите `--easy-password`, чтобы сменить пароль на простой, не соответствующий требованиям к паролям. В целях безопасности использовать простые пароли не рекомендуется.

2 В запросе **Password** введите пароль текущего пользователя. При вводе пароль не отображается.

3 В запросе **New password** введите новый пароль учетной записи пользователя **в соответствии с требованиями**. Если указан параметр `--easy-password`, введите любой пароль. При вводе пароль не отображается.

4 В запросе **Confirm new password** подтвердите новый пароль учетной записи пользователя. При вводе пароль не отображается.

## Требования к имени и паролю учетной записи

При создании в командном интерпретаторе ViPNet EPP Агент имени учетной записи разрешено использовать:

- прописные буквы латинского алфавита от **A** до **Z**;
- строчные буквы латинского алфавита от **a** до **z**;
- десятичные цифры от **0** до **9**;

Имя учетной записи должно начинаться с прописной или строчной букв латинского алфавита и не должно содержать пробелы и символы, не принадлежащие к вышеуказанному алфавитно-цифровому набору. Максимальная длина имени учетной записи — 32 символа.

При создании или изменении пароля учетной записи, стойкого к попыткам подбора, соблюдайте требования:

- Минимальная длина — 8 символов.
- Максимальная длина — 32 символа.
- Любые идущие подряд три символа пароля не должны совпадать с частью имени учетной записи.
- Один и тот же символ не должен встречаться более двух раз.
- В пароле должны одновременно присутствовать символы четырех категорий:

- прописные буквы латинского алфавита от A до Z;
- строчные буквы латинского алфавита от a до z;
- десятичные цифры от 0 до 9;
- пробел и символы, не принадлежащие к алфавитно-цифровому набору (кроме одинарной кавычки '): !@#\$%^&\*()\_+=;: ", .<>/?\|`~[]{}.

## Запуск и остановка ViPNet EPP Агент

Чтобы перезапустить службу ViPNet EPP Агент, выполните команду:

```
sudo systemctl restart epp_supervisor.service
```

Чтобы остановить службу ViPNet EPP Агент, выполните команду:

```
sudo systemctl stop epp_supervisor.service
```

Чтобы запустить службу ViPNet EPP Агент, выполните команду:

```
sudo systemctl start epp_supervisor.service
```



# Полномочия пользователей

Полный список полномочий пользователей ViPNet EPP Сервер приведен в таблице ниже.

Таблица 5. Полномочия пользователей ViPNet EPP Сервер в соответствии с назначенной ролью

| Полномочия пользователя                                                                     | Администратор | Аудитор |
|---------------------------------------------------------------------------------------------|---------------|---------|
| Управление рабочими серверами                                                               | +             | -       |
| Просмотр информации о лицензии ViPNet EPP                                                   | +             | +       |
| Установка и активация лицензии ViPNet EPP                                                   | +             | -       |
| Управление защищаемыми устройствами и группами                                              | +             | -       |
| Управление учетными записями ViPNet EPP Сервер                                              | +             | -       |
| Изменение собственного пароля. Аудитору доступна смена пароля только при первом подключении | +             | +       |
| Настройка параметров системы, конфигурации ViPNet EPP Агент и ViPNet EPP Сервер             | +             | -       |
| Управление базами правил и политиками безопасности                                          | +             | -       |
| Настройка правил обнаружения аномалий                                                       | +             | -       |
| Просмотр журнала критичных событий устройств (Инфопанель)                                   | +             | +       |
| Настройка получения критичных событий с устройств                                           | +             | -       |
| Запрос журнала событий с устройств и работа с журналом                                      | +             | +       |
| Просмотр журнала аудита ViPNet EPP Сервер (сервера управления и рабочих                     | +             | +       |

серверов)

|                                                                                                             |   |   |
|-------------------------------------------------------------------------------------------------------------|---|---|
| Проверка работоспособности ViPNet EPP Сервер: запуск самотестирования сервера управления и рабочих серверов | + | - |
|-------------------------------------------------------------------------------------------------------------|---|---|

Полный список полномочий пользователей ViPNet EPP Агент приведен в таблице ниже.

Таблица 6. Полномочия пользователей ViPNet EPP Агент в соответствии с назначенной ролью

| Полномочия пользователя                                                                                                                                                           | Администратор | Аудитор | Пользователь |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------|--------------|
| Управление учетными записями ViPNet EPP Агент                                                                                                                                     | +             | -       | -            |
| Просмотр и редактирование настроек ViPNet EPP Агент                                                                                                                               | +             | -       | -            |
| Изменение адреса ViPNet EPP Сервер (IP-адреса и TCP-порта)                                                                                                                        | +             | -       | -            |
| Просмотр статуса выполнения политики ZTNA и списка узлов защищенной сети ViPNet, доступных при невыполнении политики (доступно только в ViPNet EPP Агент под управлением сервера) | +             | +       | +            |
| Удаление событий                                                                                                                                                                  | +             | -       | -            |
| Просмотр журнала аудита ViPNet EPP Агент                                                                                                                                          | +             | +       | -            |
| Настройка параметров журнала аудита ViPNet EPP Агент                                                                                                                              | +             | -       | -            |
| Просмотр сведений о лицензии                                                                                                                                                      | +             | +       | -            |
| Проверка работоспособности ViPNet EPP Агент (запуск самотестирования)                                                                                                             | +             | -       | -            |
| Просмотр версии ViPNet EPP Агент, версии базы правил и результатов самотестирования                                                                                               | +             | +       | -            |
| Установка и активация лицензии ViPNet EPP Агент (доступно только в автономном ViPNet EPP Агент)                                                                                   | +             | -       | -            |
| Просмотр уведомлений ViPNet EPP на панели уведомлений ОС GNU/Linux                                                                                                                | +             | +       | +            |
| Импорт и экспорт базы правил (доступно только в автономном ViPNet EPP Агент)                                                                                                      | +             | -       | -            |
| <b>Межсетевой экран PFW</b>                                                                                                                                                       |               |         |              |
| Изменение режима работа PFW                                                                                                                                                       | +             | +       | -            |
| Просмотр сетевых фильтров                                                                                                                                                         | +             | +       | -            |
| Управление пользовательскими сетевыми фильтрами                                                                                                                                   | +             | -       | -            |
| Просмотр активных соединений на защищаемом узле и просмотр заблокированных приложений                                                                                             | +             | +       | -            |
| Просмотр журнала трафика PFW                                                                                                                                                      | +             | +       | -            |

|                                                                                            |   |   |   |
|--------------------------------------------------------------------------------------------|---|---|---|
| Настройка пользовательских справочников адресов и сетей PFW                                | + | - | - |
| Настройка пользовательских справочников протоколов PFW                                     | + | - | - |
| Просмотр пользовательских справочников PFW                                                 | + | + | - |
| Настройка пользовательских справочников расписаний PFW                                     | + | - | - |
| Настройка справочников ViPNet                                                              | + | - | - |
| <b>Обнаружение и предотвращение вторжений HIPS/HIDS</b>                                    |   |   |   |
| Изменение режима работы HIPS                                                               | + | + | - |
| Просмотр журнала событий HIPS/HIDS                                                         | + | + | + |
| Просмотр сетевых правил HIPS                                                               | + | + | - |
| Управление сетевыми правилами HIPS (доступно только в автономном ViPNet EPP Агент)         | + | - | - |
| Просмотр критериев обнаружения аномалий                                                    | + | + | - |
| Управление критериями обнаружения аномалий (доступно только в автономном ViPNet EPP Агент) | + | - | - |
| Просмотр правил HIDS                                                                       | + | + | - |
| Управление правилами HIDS (доступно только в автономном ViPNet EPP Агент)                  | + | - | - |

# В

## Типы и идентификаторы правил

Таблица 7. Типы и идентификаторы правил

| Диапазон идентификаторов правил | Тип правил в журнале и в критериях обнаружения аномалий | Тип правил в базе правил | Тип правил при передаче по CEF                                              | Модуль                  | Примечание                                              |
|---------------------------------|---------------------------------------------------------|--------------------------|-----------------------------------------------------------------------------|-------------------------|---------------------------------------------------------|
| 100000–199999                   | Контроль реестра (Windows)                              | Правила анализа          | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux) |                         | Правила HIDS для мониторинга событий реестра            |
| 200000–209999<br>210001–299999  | Контроль файлов (Windows)                               | Правила анализа          | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux) | Обнаружение атак (HIDS) | Правила HIDS для мониторинга изменений файловой системы |
| 210000                          | Контроль файлов (Windows)                               | Мониторинг файлов        | Мониторинг файлов (в Windows)<br>Операции с файлами (в Linux)               |                         | Правила HIDS для мониторинга файлов                     |

| Диапазон<br>идентифика-<br>торов<br>правил | Тип правил в<br>журнале и в<br>критериях<br>обнаружения<br>аномалий | Тип правил в<br>базе правил                                                                                                           | Тип правил при<br>передаче по CEF                                                                                                                                                                                                                                                                     | Модуль | Примечание                                              |
|--------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------------------------------------------|
| 860000–869999                              | Изменение файловой системы (Linux)                                  | 860000–860015,<br>860020–869999 – правила анализа<br>860016 – получение контрольной суммы файлов<br>860017–860019 – мониторинг файлов | 860000–860015,<br>860020–869999 – правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)<br>860016 – получение контрольной суммы файлов (в Windows)<br>Расчет контрольных сумм файлов (в Linux)<br>860017–860019 – мониторинг файлов (в Windows)<br>Операции с файлами (в Linux) |        | Правила HIDS для мониторинга изменений файловой системы |
| 300000–379999                              | Контроль процессов (Windows)                                        | Правила анализа                                                                                                                       | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)                                                                                                                                                                                                                           |        | Правила HIDS для контроля активности процессов          |
| 380000–399999                              | Обнаружение бесфайловых атак (Windows)                              | Обнаружение бесфайловых атак                                                                                                          | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)                                                                                                                                                                                                                           |        | Правила HIDS для обнаружения бесфайловых атак           |
| 400000–499999                              | Системная активность (Windows)                                      | Правила анализа<br>Анализ журнала событий Windows                                                                                     | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)                                                                                                                                                                                                                           |        | Правила HIDS для контроля системной активности          |

| Диапазон идентификации правил | Тип правил в журнале и в критериях обнаружения аномалий | Тип правил в базе правил                          | Тип правил при передаче по CEF                                                   | Модуль | Примечание                                                                  |
|-------------------------------|---------------------------------------------------------|---------------------------------------------------|----------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------|
| 870000–879999                 | Системная активность (Linux)                            | Правила анализа                                   | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)      |        | Правила HIDS для контроля системной активности                              |
| 500000–599999                 | Логины пользователей (Windows)                          | Правила анализа<br>Анализ журнала событий Windows | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)      |        | Правила HIDS для контроля аутентификации пользователей                      |
| 880000–889999                 | Логины с учетной записью (Linux)                        | Правила анализа                                   | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)      |        | Правила HIDS для контроля аутентификации пользователей                      |
| 600000–699999                 | Изменения учетных записей (Windows)                     | Правила анализа<br>Анализ журнала событий Windows | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)      |        | Правила HIDS для контроля изменения учетных записей и групп учетных записей |
| 890000–899999                 | Изменения учетных записей (Linux)                       | Правила анализа                                   | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)      |        |                                                                             |
| 700000–749999                 | Выполняемые команды (Windows)                           | Команды мониторинга системы                       | Выполняемые команды (в Windows)<br>Команды мониторинга системы Windows (в Linux) |        | Правила HIDS для контроля за выполнением команд                             |
| 839999–859999                 | Выполняемые команды (Linux)                             | Команды мониторинга                               | Выполняемые команды                                                              |        |                                                                             |

| Диапазон идентификации правил | Тип правил в журнале и в критериях обнаружения аномалий | Тип правил в базе правил системы                    | Тип правил при передаче по CEF                                                                    | Модуль | Примечание                                                              |
|-------------------------------|---------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------------------|
| 750000–779999                 | Контроль установки приложений (Windows)                 | Мониторинг устанавливаемого ПО                      | Обнаружение установки ПО (в Windows)<br>Установка ПО (в Linux)                                    |        | Правила HIDS для контроля за установкой нового программного обеспечения |
| 780000–789999                 | Обнаружение системных обновлений (Windows)              | Мониторинг системных обновлений                     | Статус пакетов обновления Windows (в Windows)<br>Установка системных обновлений Windows (в Linux) |        | Правила HIDS для контроля за установкой обновлений Windows              |
| 790000–799999                 | Мониторинг вредоносных файлов (Windows)                 | Получение контрольной суммы файлов                  | Получение контрольных сумм файлов (в Windows)<br>Расчет контрольных сумм файлов (в Linux)         |        | Правила HIDS для контроля за хэш-суммами файлов                         |
| 800000–839998                 | Журнал приложений (Windows)                             | Анализ журналов приложений и служб                  | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)                       |        | Правила HIDS для контроля за журналами приложений                       |
| 900000–999999                 | Обнаружение вредоносной активности RemSec (Windows)     | Обнаружение вредоносной активности RemSec (Windows) | Правила обнаружения локальных атак (в Windows)<br>Локальные атаки (в Linux)                       |        | Правила HIDS для обнаружения RemSec                                     |
| 2000000–4000000               | Правила обнаружения сетевых атак (Windows/Linux)        | Правила обнаружения сетевых атак                    | Правила обнаружения сетевых атак (в Windows)<br>Сетевые атаки (в Linux)                           |        | Сетевые правила HIDS защищаемого узла                                   |

| Диапазон идентификации правил | Тип правил в журнале и в критериях обнаружения аномалий | Тип правил в базе правил         | Тип правил при передаче по CEF                                          | Модуль                          | Примечание                                                                                         |
|-------------------------------|---------------------------------------------------------|----------------------------------|-------------------------------------------------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------|
| 2000000–4000000               | Правила предотвращения сетевых атак (Windows/Linux)     | Правила обнаружения сетевых атак | Правила обнаружения сетевых атак (в Windows)<br>Сетевые атаки (в Linux) | HIPS                            | Правила HIPS защищаемого узла                                                                      |
| 4000001–409999                | —                                                       | —                                | — (в Windows)<br>Межсетевой экран (в Linux)                             | Межсетевой экран (PFW)          | Фильтры политик безопасности, задаваемые в базе правил (политике безопасности) в ViPNet EPP Сервер |
| 4100000–419999                | —                                                       | —                                | — (в Windows)<br>Межсетевой экран (в Linux)                             |                                 | Пользовательские фильтры, задаваемые в ViPNet EPP Агент защищаемого узла                           |
| 4950000–499999                | —                                                       | —                                | — (в Windows)<br>Межсетевой экран (в Linux)                             |                                 | Сетевые фильтры блокирования контента                                                              |
| 5000000–519999                | Контроль активности приложений (Windows)                | —                                | Контроль приложений                                                     | Контроль приложений (AppC)      | Черный и белый списки                                                                              |
| 5200000–539999                | Контроль доступа приложений к файлам (Windows)          | —                                | Контроль приложений                                                     |                                 | Правила доступа к файлам                                                                           |
| 5400000–559999                | Контроль доступа приложений к реестру (Windows)         | —                                | Контроль приложений                                                     |                                 | Правила доступа к ветвям реестра                                                                   |
| 6380000–6381999               | —                                                       | —                                | —                                                                       | Предотвращение вторжений (HIPS) | Правила для бесфайлового HIPS                                                                      |
| 6382000–6383999               | Контроль доступа к веб-ресурсам (Windows)               | —                                | —                                                                       | Предотвращение вторжений (HIPS) | Веб-фильтрация                                                                                     |



# Структура CEF-сообщения

В приложении приведены структура [CEF-сообщения](#) и описания поддерживаемых в ViPNet EPP полей и ключей расширения. В CEF-сообщении используется кодировка UTF-8.

Структура CEF-сообщения:

[Дата и время] [Источник] [Заголовок] [Расширение], где:

- [Дата и время] — дата и время создания CEF-сообщения в соответствии с системным временем ViPNet EPP Сервер в формате: Месяц Число Час:Минута:Секунда.Миллисекунда. Например, Dec 13 10:15:13.999.
- [Источник] — источник CEF-сообщения — [EPP-Server](#).
- [Заголовок] — заголовок CEF-сообщения, состоящий из полей:

CEF: [Version] | [Device Vendor] | [Device Product] | [Device Version] | [Device Event Class ID или Signature ID] | [Name] | [Severity] |

Все поля заголовка являются обязательными. Поля заголовка отделяются друг от друга символом |. Последнее поле заголовка также отделено от поля расширения символом |. Описание полей заголовка CEF-сообщения представлено в таблице ниже.

Таблица 8. Описание полей заголовка CEF-сообщения

| Поле               | Описание                                                                 |
|--------------------|--------------------------------------------------------------------------|
| Version            | Текущая версия формата CEF — 0                                           |
| Device Vendor      | Наименование производителя ViPNet EPP — <a href="#">infotecs</a>         |
| Device Product     | Наименование продукта — <a href="#">EPP</a>                              |
| Device Version     | Версия ViPNet EPP в формате: X.Y.Z. Например, <a href="#">1.1.3.3036</a> |
| Device Event Class | Уникальный идентификатор класса события в одном из следующих форматов:   |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID           | <ul style="list-style-type: none"> <li>Формат для сетевых событий (Device Event Class ID):</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| или          | [Номер типа правила] : [Идентификатор правила] : [Версия правила], где:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Signature ID | <p>[Номер типа правила] — номер, который идентифицирует метод обнаружения угрозы. Для сигнатурных правил параметр имеет постоянное значение — 1.</p> <p>[Идентификатор правила] — уникальный номер, присваиваемый каждому правилу для идентификации события.</p> <p>[Версия правила] — номер версии правила.</p> <p>Значения [Идентификатор правила] и [Версия правила] прописаны для каждого правила в базе правил.</p> <p>Например, Device Event Class ID может содержать значение — 1:2100366:4</p> <ul style="list-style-type: none"> <li>Формат других событий (Signature ID):</li> </ul> <p>[Идентификатор правила]</p> <p>Например, Signature ID может содержать значение — 190001</p> <p>Идентификатор правила зависит от вида правил. Распределение идентификаторов правил для различных видов правил см. ниже в таблице «Зависимость обязательных ключей и распределение поддерживаемых дополнительных ключей».</p> |

|          |                                                                                                                                                                                                                                                                                  |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name     | Описание события. Например, — <a href="#">Изменение журнала приложений</a>                                                                                                                                                                                                       |
| Severity | <p>Уровень события:</p> <ul style="list-style-type: none"> <li>0 — информационное событие (в TIAS — низкий).</li> <li>4 — важное событие (в TIAS — средний).</li> <li>6 — опасное событие (в TIAS — высокий).</li> <li>10 — критическое событие (в TIAS — критичный).</li> </ul> |

- [Расширение] — набор пар ключ-значение:

[ключ]=[значение] [ключ]=[значение] . . . [ключ]=[значение]

Расширение может содержать произвольное количество пар ключ-значение, разделенных пробелами. Часть ключей расширения являются обязательными. Состав дополнительных ключей определяется идентификатором правила. Обязательные ключи расширения (пары ключ-значение) записываются в CEF-сообщение в первую очередь, а затем записываются дополнительные ключи. Перечень и описание поддерживаемых в ViPNet EPP обязательных ключей приведены в таблице ниже.



**Внимание!** Длина CEF-сообщения, для передачи которого используется транспортный протокол UDP, не может превышать 65000 байт. Если при формировании CEF-сообщения его длина достигнет 65000 байт, оставшиеся пары ключ-значение будут отброшены.

Таблица 9. Общие ключи поля расширения

| Ключ                        | Описание ключа                                                                                                                                                                                                    | Пример значения ключа или поддерживаемые ключи                                                                                                                                                                                                                                                                                        |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Обязательные ключи</b>   |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                       |
| protocolVersion             | Спецификация CEF-TIAS, поддерживаемая TIAS                                                                                                                                                                        | 1.0                                                                                                                                                                                                                                                                                                                                   |
| eventType                   | Тип события: узловое (host) или сетевое (net)                                                                                                                                                                     | Например, net                                                                                                                                                                                                                                                                                                                         |
| agentId                     | Идентификатор устройства, на котором зарегистрировано событие                                                                                                                                                     | Например, ef52ce22-3356-4db5-a767-a0cd42f80f5d                                                                                                                                                                                                                                                                                        |
| eventId                     | Идентификатор события во внутренней базе данных ViPNet EPP Сервер                                                                                                                                                 | Например, 5445                                                                                                                                                                                                                                                                                                                        |
| sensorExternalId            | Идентификатор ViPNet EPP Сервера, к которому подключен устройство (для ОС Linux — идентификатор Сервера управления)                                                                                               | Например, 74451b40-2ace-4b0e-8c3f-f846b62c6f96                                                                                                                                                                                                                                                                                        |
| agentIp                     | IP-адрес защищаемого узла; допустимые значения IP v4                                                                                                                                                              | Например, localhost или 192.169.147.140                                                                                                                                                                                                                                                                                               |
| rt                          | Метка времени регистрации события, равная количеству миллисекунд, прошедших с 1 января 1970г. до даты события. Дата события — это дата и время получения события (от ViPNet EPP Агент) на ViPNet EPP Сервер в UTC | Например, 1523013338106                                                                                                                                                                                                                                                                                                               |
| threatSourceCat             | Категория источника угроз                                                                                                                                                                                         | Поддерживаемые ключи — RegeditControl; FileControl; ProcessControl; SystemActivity; LoginControl; UserChangesControl; InstallAppControl; AppControl; NetAgentRules; CommandControl; InstallKbControl<br><br>Описание ключей см. ниже в таблице «Зависимость обязательных ключей и распределение поддерживаемых дополнительных ключей» |
| sensorModule                | Модуль ViPNet EPP, идентифицировавший событие                                                                                                                                                                     | Поддерживаемые ключи — AppC; HIDS; HIPS; PFW                                                                                                                                                                                                                                                                                          |
| <b>Необязательные ключи</b> |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                       |

|                         |                                                                                                |                                                                                                                                                                                                 |
|-------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cnt                     | Количество срабатываний правила, в результате которых зарегистрировано событие                 | Например, 17                                                                                                                                                                                    |
| anomaly                 | Аномальное событие; обнаружено с помощью критерия                                              | 1                                                                                                                                                                                               |
| agentMac                | Мас-адрес сетевого адаптера компьютера защищаемого узла                                        | Например, 10:FF:FF:FF:FF:FF                                                                                                                                                                     |
| ThreatCat               | Категория типа угроз                                                                           | Например, RegeditControl                                                                                                                                                                        |
| deviceFacility          | Источник события                                                                               | Поддерживаемые ключи — eventlog; applog; snort; command_control; newsoft; integritycontrol; update_kb; suricata<br>Описание ключей см. ниже в таблице «Описание значений ключа deviceFacility». |
| agentName               | Название защищаемого узла, заданное в ViPNet EPP Сервер                                        | Например, Agent5, MSK-1111                                                                                                                                                                      |
| sensorExternalWorkingId | Идентификатор ViPNet EPP Рабочего Сервера, к которому подключен защищаемый узел (для ОС Linux) | Например, 6f9619ff-1111-dddd-3333-00cf4fc964ff                                                                                                                                                  |
| hostName                | Имя компьютера защищаемого узла, на котором зарегистрировано событие                           |                                                                                                                                                                                                 |

При настройке передачи CEF-сообщений администратор ViPNet EPP может выбрать, события с каким источником (*deviceFacility*) необходимо отправлять. Для ViPNet EPP Сервер данная настройка заключается в выборе типов правил (для ViPNet EPP Сервер управления — в выборе типов события), при срабатывании которых будут отправляться CEF-сообщения. Перечень и описание значений ключа источника событий (*deviceFacility*), а также распределение по видам правил, настраиваемым в ViPNet EPP Серверная консоль (только для ОС Windows), приведены в таблице ниже.

Таблица 10. Описание значений ключа *deviceFacility*

| Значения ключа <i>deviceFacility</i> | Описание                                                                                                            |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| applog                               | События, связанные с обнаружением изменений в журналах приложений и служб                                           |
| command_control                      | События, связанные с обнаружением изменений состояния контролируемых узлов с помощью выполнения определенных команд |
| eventlog                             | События, связанные с обнаружением изменений в журнале событий                                                       |

| Значения ключа deviceFacility | Описание                                                                                       |
|-------------------------------|------------------------------------------------------------------------------------------------|
| integritycontrol              | События, связанные с отслеживанием создания новых файлов и подсчетом контрольной суммы для них |
| newsoft                       | События, связанные с обнаружением нового ПО                                                    |
| snort                         | События, связанные с обнаружением сетевых атак                                                 |
| suricata                      | События, связанные с обнаружением сетевых атак                                                 |
| update_kb                     | События, связанные с отслеживанием установки системных обновлений ОС Windows                   |

В зависимости от значения ключа источника событий (`deviceFacility`) расширение может содержать различные значения ключа категории событий (`threatSourceCat`). Перечень и описание значений ключа категории событий (`threatSourceCat`) приведены в таблице ниже.

Таблица 11. Описание значений ключа `threatSourceCat`

| Значения ключа threatSourceCat | Описание                                                                                                 |
|--------------------------------|----------------------------------------------------------------------------------------------------------|
| AppControl                     | Контроль приложений                                                                                      |
| CommandControl                 | Контроль выполняемых команд                                                                              |
| FileControl                    | Контроль файла                                                                                           |
| InstallAppControl              | Контроль установки приложений                                                                            |
| InstallKbControl               | Мониторинг системных обновлений                                                                          |
| LoginControl                   | Имена учетных записей пользователей                                                                      |
| NetAgentRules                  | Сетевая активность                                                                                       |
| ProcessControl                 | Контроль процессов                                                                                       |
| RegeditControl                 | Контроль реестра                                                                                         |
| SystemActivity                 | Системная активность                                                                                     |
| unknown                        | Неизвестный источник. Используется для событий, не относящихся ни к одному из известных источников угроз |
| UserChangesControl             | Изменения учетных записей                                                                                |

Для некоторых значений ключа `deviceFacility` значение ключа `threatSourceCat` определяется в зависимости от значения идентификатора правила и типа правил. Идентификатор правила зависит от типа правил. Для каждого типа правил выделен определенный диапазон идентификаторов правил.

Состав дополнительных ключей расширения определяется в зависимости от значения идентификатора правила, типа правила и значения ключа `deviceFacility`.

Зависимость между диапазоном идентификаторов правил, типом правил, ключами `deviceFacility` и `threatSourceCat`, а также распределение поддерживаемых наиболее важных дополнительных ключей приведено в таблице ниже.



**Внимание!** В таблице приведен список возможных важных дополнительных ключей для каждого диапазона идентификаторов правил. В CEF-сообщении могут присутствовать не все перечисленные ключи, а также ключи, не приведенные в данной таблице. Также часть значений ключей имеет максимальную длину и будет обрезана при ее достижении.

Таблица 12. Зависимость обязательных ключей и распределение поддерживаемых дополнительных ключей

| Диапазон идентификаторов в правил | Тип правил                   | Значения ключа <code>deviceFacility</code> | Поддерживаемые значения ключа <code>threatSourceCat</code> | Поддерживаемые дополнительные ключи                                                                                                     |
|-----------------------------------|------------------------------|--------------------------------------------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 100000-199999                     | Контроль реестра             | eventlog                                   | RegeditControl                                             | RegistryKey;<br>RegistryNewValue;<br>RegistryOldValue;<br>RegistryOperationType;<br>RegistryPath;<br>sntdom;<br>sproc;<br>suid<br>suser |
| 200000-299999                     | Контроль файлов              | eventlog                                   | FileControl                                                | filePath;<br>FileOperationType;<br>message<br>sntdom;<br>sproc;<br>suid;<br>suser                                                       |
| 300000-379999                     | Контроль процессов           | eventlog                                   | ProcessControl                                             | CommandLine;<br>ParentProcessName;<br>message<br>sntdom;<br>sproc;<br>suid;<br>suser                                                    |
| 380000-399999                     | Обнаружение бесфайловых атак |                                            | ProcessControl                                             | sproc;<br>suser                                                                                                                         |

|               |                         |          |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|-------------------------|----------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 400000-499999 | Системная<br>активность | eventlog | SystemActivity | filePath;<br>AuthenticationPackageName;<br>DeviceName;<br>DnsServerIpAddress;<br>DomainQueryName;<br>DomainQueryType;<br>KasperskyEventType;<br>KasperskyResult;<br>KasperskyResultName;<br>KasperskyResultType;<br>KasperThreatSever;<br>NewSD;<br>NotificationPackageName;<br>ObjectName;<br>OldSD;<br>SecurityPackageName;<br>ServiceAccount;<br>ServiceAlias;<br>ServiceFileName;<br>ServiceStartType;<br>ServiceStartTypeNewValue;<br>ServiceStartTypeOldValue;<br>ServiceType;<br>SoftName;<br>TaskCommand;<br>TaskName;<br>WindowCaption;<br>WindowMsg;<br>reasonDescription;<br>sntdom;<br>sourceServiceName;<br>sproc;<br>src;<br>suid;<br>suser<br>virusName |
| 500000-599999 | Логины<br>пользователей | eventlog | LoginControl   | dntdom;<br>duid;<br>duser;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|               |                                          |                      |                        |                                                                                                                                 |
|---------------|------------------------------------------|----------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|               |                                          |                      |                        | AuthType;<br>LogOnType;<br>SessionName;<br>tgtOpt;<br>reasonDescription;<br>shost;<br>sntdom;<br>spt;<br>src;<br>suid;<br>suser |
| 600000-699999 | Изменения<br>учетных<br>записей          | eventlog             | UserChangesCo<br>ntrol | dntdom;<br>duid;<br>duser;<br>SidUserGroup;<br>UserGroup;<br>sntdom;<br>suid<br>suser                                           |
| 700000-749999 | Команды<br>мониторинга                   | command_c<br>ontrol  | CommandCont<br>roll    | executedCommands                                                                                                                |
| 750000-779999 | Контроль<br>установки<br>приложений      | newsoft              | InstallAppContr<br>ol  | SoftName;<br>SoftPublisher;<br>SoftVersion                                                                                      |
| 780000-789999 | Мониторинг<br>системных<br>обновлений    | update_kb            | InstallKbContro<br>l   | Updates                                                                                                                         |
| 790000-799999 | Получение<br>контрольной<br>суммы файлов | integritycon<br>trol | SystemActivity         | filePath;<br>FileHash;<br>FileHashType                                                                                          |
| 800000-839998 | Журнал<br>приложений                     | applog               | AppControl             | message                                                                                                                         |
| 839999-859999 | Команды<br>мониторинга<br>ОС *nix        | command_c<br>ontrol  | CommandCont<br>roll    | executedCommands                                                                                                                |
| 860000-869999 | Контроль<br>файлов ОС *nix               | eventlog             | FileControl            | message                                                                                                                         |

|                 |                                           |                    |                    |                                                        |
|-----------------|-------------------------------------------|--------------------|--------------------|--------------------------------------------------------|
| 870000-879999   | Системная активность ОС *nix              | eventlog           | SystemActivity     | message                                                |
| 880000-889999   | Логины пользователей ОС *nix              | eventlog           | LoginControl       | message                                                |
| 890000-899999   | Изменения учетных записей ОС *nix         | eventlog           | UserChangesControl | message                                                |
| 900000-999999   | Обнаружение вредоносной активности RemSec | applog             | AppControl         | reasonDescription;<br>filePath                         |
| 2000000-4000000 | Правила обнаружения сетевых атак          | snort,<br>suricata | NetAgentRules      | dpt;<br>dst;<br>transportProto;<br>spt;<br>src         |
| 4950000-4999999 | Сетевая активность                        | suricata           | NetAgentRules      | dpt;<br>dst;<br>transportProto;<br>spt;<br>src;<br>cnt |
| 5000000-5199999 | Контроль активности приложений            |                    | AppControl         | cnt;<br>data                                           |
| 5200000-5399999 | Контроль доступа приложений к файлам      |                    | FileControl        | cnt;<br>data                                           |
| 5400000-5599999 | Контроль доступа приложений к реестру     |                    | RegeditControl     | cnt;<br>data                                           |

Перечень и описание поддерживаемых дополнительных ключей приведены в таблице ниже.

Таблица 13. Список дополнительных ключей расширения

| Ключ | Описание ключа | Пример значения ключа |
|------|----------------|-----------------------|
| cnt  | Количество     | 10                    |

|                           |                                                   |                                                                                                                                    |
|---------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| data                      | Данные в текстовом формате JSON                   | [<br>{<br>"app_path": "",<br>//Приложение/путь к приложению<br>"reg_path": "", //Путь к ветке реестра<br>},<br>]                   |
| reasonDescription         | Описание вредоносной активности                   | Обнаружен PoC CVE-2020-0986                                                                                                        |
| dntdom                    | Домен целевой учетной записи                      | DESKTOP-EQSPQ7H<br>duid=S-1-5-21-3343134865-3529847183-3180321194-1002                                                             |
| dpt                       | Порт назначения                                   | 22                                                                                                                                 |
| dst                       | Адрес назначения                                  | 192.168.2.130                                                                                                                      |
| duid                      | Идентификатор целевой учетной записи пользователя | S-1-5-21-3343134865-3529847183-3180321194-1002                                                                                     |
| duser                     | Целевая учетная запись пользователя               | Ivanov                                                                                                                             |
| filePath                  | Полный путь к файлу                               | C:\Windows\WinSxS\wow64_microsoft-windows-security-spp-clienttext_31bf3856ad364e35_10.0.16299.15_none_fa07cc1956a42a62\sppcext.dll |
| AuthenticationPackageName | Наименование пакета аутентификации                | "MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0"                                                                                        |
| AuthType                  | Способ аутентификации                             | User_1                                                                                                                             |
| CommandLine               | Параметры командной строки                        | net user chop 123 /add                                                                                                             |
| DeviceName                | Имя сетевого адаптера                             | Ethernet_1                                                                                                                         |
| DnsServerIpAddress        | IP-адрес DNS-сервера                              | 192.168.0.7                                                                                                                        |
| DomainQueryName           | Запрашиваемый домен                               | Access denied                                                                                                                      |
| DomainQueryType           | Тип запроса                                       | Programm                                                                                                                           |
| FileHash                  | Значение контрольной суммы файла                  | D41D8CD98F00B204E9800998ECF8427E                                                                                                   |
| FileHashType              | Алгоритм подсчета контрольной суммы файла         | MD5                                                                                                                                |
| FileOperationType         | Тип операции                                      | удаление/переименование файла                                                                                                      |
| KasperskyEventType        | Тип события обнаружения вируса                    | Непонятное                                                                                                                         |

|                          |                                         |                                                                                                                           |
|--------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| KasperskyResult          | Описание вируса                         | Добавление_нового_объекта                                                                                                 |
| KasperskyResultName      | Название вируса                         | Зеленая папка                                                                                                             |
| KasperskyResultType      | Тип вируса                              | Добавление                                                                                                                |
| KasperThreatSever        | Степень угрозы<br>обнаруженного вируса  | Минимальная                                                                                                               |
| LogOnType                | Тип входа                               | user                                                                                                                      |
| NotificationPackageName  | Наименование пакета<br>уведомлений      | "WDIGEST"                                                                                                                 |
| ObjectName               | Имя объекта                             | Папка                                                                                                                     |
| ParentProcessName        | Имя родительского<br>процесса           | C:\Windows\System32\svchost.exe                                                                                           |
| RegistryKey              | Имя ключа                               | ProxyServer                                                                                                               |
| RegistryOldValue         | Старое значение ключа                   | 127.0.0.1:8                                                                                                               |
| RegistryNewValue         | Новое значение ключа                    | 127.0.0.1:800                                                                                                             |
| RegistryOperationType    | Тип операции                            | изменение ключа реестра                                                                                                   |
| RegistryPath             | Раздел реестра                          | \REGISTRY\USER\S-1-5-21-3343134865-3529847183-3180321194-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings |
| SecurityPackageName      | Наименование пакета<br>безопасности     | "Kerberos"                                                                                                                |
| ServiceAccount           | Учетная запись службы                   | LocalSystem                                                                                                               |
| ServiceAlias             | Псевдоним службы                        | TrustedInstaller                                                                                                          |
| ServiceFileName          | Полный путь к образу<br>службы          | "C:\Program Files\Zabbix Agent\zabbix_agentd.exe"                                                                         |
| ServiceStartType         | Тип запуска службы                      | auto start                                                                                                                |
| ServiceStartTypeNewValue | Тип запуска службы<br>(новое значение)  | Автоматически                                                                                                             |
| ServiceStartTypeOldValue | Тип запуска службы<br>(старое значение) | Вручную                                                                                                                   |
| ServiceType              | Тип службы                              | user mode service                                                                                                         |
| SessionName              | Имя сессии                              | user                                                                                                                      |
| SidUserGroup             | Идентификатор целевой<br>группы         | S-1-5-21-3457937927-2839227994-823803824-2104                                                                             |
| SoftName                 | Наименование ПО                         | AIDA64 Extreme v5.75                                                                                                      |
| SoftPublisher            | Издатель ПО                             | FinalWire Ltd.                                                                                                            |

|                   |                                                   |                                                                                                                                                                                              |
|-------------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SoftVersion       | Версия ПО                                         | 5.75                                                                                                                                                                                         |
| TaskCommand       | Полный путь к образу задачи                       | C:\Windows\system32\MRT.exe                                                                                                                                                                  |
| TaskName          | Имя задачи                                        | \Microsoft\Windows\RemovalTools\MRT_ERROR_HB                                                                                                                                                 |
| TgtOpt            | Параметры TGT                                     | 0x40810010                                                                                                                                                                                   |
| Updates           | Названия системных обновлений                     | KB1234567                                                                                                                                                                                    |
| UserGroup         | Целевая группа                                    | AccountOperators                                                                                                                                                                             |
| WindowCaption     | Заголовок всплывающего окна                       | test-Win64-Shipping.exe - Точка входа не найдена                                                                                                                                             |
| WindowMsg         | Сообщение                                         | Точка входа в процедуру GetUserDefaultGeoName не найдена в библиотеке DLL<br>D:\test\test-Win64-Shipping.exe                                                                                 |
| message           | Сообщение                                         | postgres - "C:/Program Files (x86)/PostgreSQL/bin/postgres.exe"<br>"--forkbackend" "4084"                                                                                                    |
| executedCommands  | Выполняемые команды                               | Обмен пакетами с 127.0.0.1 по с 32 байтами данных:<br><br>Превышен интервал ожидания для запроса.<br><br>...<br><br>Пакетов: отправлено = 4, получено = 0, потеряно = 4<br><br>(100% потерь) |
| transportProto    | Протокол передачи данных                          | ICMP                                                                                                                                                                                         |
| reasonDescription | Причина                                           | disallowed_source_ip                                                                                                                                                                         |
| shost             | Имя источника                                     | User_1                                                                                                                                                                                       |
| sid               | Идентификатор Snort события в формате gid:sid:rev | gid:1000001; sid:1; rev:1                                                                                                                                                                    |
| sntdom            | Домен активной учетной записи пользователя        | DESKTOP-EQSPQ7H                                                                                                                                                                              |
| sourceServiceName | Имя службы                                        | Установщик модулей Windows                                                                                                                                                                   |
| sproc             | Имя процесса                                      | C:\Windows\ImmersiveControlPanel\SystemSettings.exe                                                                                                                                          |
| spt               | Номер порта источника                             | 50855                                                                                                                                                                                        |
| src               | IP-адрес источника                                | 192.168.2.129                                                                                                                                                                                |

|           |                                                    |                                                |
|-----------|----------------------------------------------------|------------------------------------------------|
| suid      | Идентификатор активной учетной записи пользователя | S-1-5-21-3343134865-3529847183-3180321194-1001 |
| suser     | Активная учетная запись пользователя               | Petrov                                         |
| virusName | Имя вредоносного объекта                           | Троянская программа                            |

Примеры CEF-сообщений для некоторых категорий событий приведены в таблице ниже.

Таблица 14. Примеры CEF-сообщений по категории события

| Категория события (threatSourceCat) | Пример CEF-сообщения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AppControl                          | <pre> Mar 16 12:46:23.135 EPP-Server CEF:0 infotecs EPP 1.0.0.0 900150 DMALocker: Обнаружен шифровальщик DMALocker 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=AppControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=applog ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 reasonDescription=DMALocker: Обнаружен шифровальщик DMALocker filePath=C:\\Program Files\\ESET\\ESET Security\\Modules\\em002_64\\48838\\em002_64.dll </pre>                                                                                                                                                                                                                                                                                                                                                                                          |
| CommandControl                      | <pre> Mar 16 12:46:23.135 EPP-Server CEF:0 infotecs EPP 1.0.0.0 700002 ping 127.0.0.1 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=CommandControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=command_control ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 executedCommands=Обмен пакетами с 127.0.0.1 по с 32 байтами данных:  Ответ от 127.0.0.1: число байт\=32 время&lt;1мс TTL\=128 Ответ от 127.0.0.1: число байт\=32 время&lt;1мс TTL\=128 Ответ от 127.0.0.1: число байт\=32 время&lt;1мс TTL\=128 Ответ от 127.0.0.1: число байт\=32 время&lt;1мс TTL\=128  Статистика Ping для 127.0.0.1:     Пакетов: отправлено \= 4, получено \= 4, потеряно \= 0     (0% потерь) Приблизительное время приема-передачи в мс:     Минимальное \= 0мсек, Максимальное \= 0 мсек, Среднее \= 0 мсек  C:\\WINDOWS\\system32&gt; </pre> |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileControl       | <pre> Mar 16 12:46:23.135 EPP-Server CEF:0 infotecs EPP 1.0.0.0 200002 Добавление в автозагрузку через каталоги файловой системы 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=FileControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=eventlog ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 filePath=C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\StartUp\\APC UPS Status.lnk sproc=D:\\SOFT\\PCPE_3.1.0.exe FileOperationType=%%4417 %%4418 suser=Peter.P sntdom=infotecs-NT suid=S-1-5-21-1128627858-1011171821-2048475684-25584 </pre> |
| InstallAppControl | <pre> Mar 16 12:46:23.135 EPP-Server CEF:0 infotecs EPP 1.0.0.0 800000 Изменение журнала приложений 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=AppControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=applog ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 message=2021-03-23 23:18:49.2207 WARN IDSHS.Analyzer.Processors.Implementations.Analysis Processor Failed to decode event 'Целостность журнала аудита - не нарушена - True'.  </pre>                                                                                                        |
| InstallKbControl  | <pre> Mar 16 12:46:23.135 EPP-Server CEF:0 infotecs EPP 1.0.0.0 780000 Мониторинг системных обновлений 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=InstallKbControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=update_kb ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 Updates=KB4601048 </pre>                                                                                                                                                                                                                                                        |
| LoginControl      | <pre> Mar 16 12:46:23.135 EPP-Server CEF:0 infotecs EPP 1.0.0.0 500009 Сетевой вход в систему 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=LoginControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=eventlog ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 duser=UFA-W0325\$ dntdom=infotecs-NT LogOnType=3 AuthType=Kerberos shost=- src=- duid=S-1-5-18 spt=- </pre>                                                                                                                                                                                   |
| NetAgentRules     | <pre> Mar 16 12:46:23.135 EPP-Server CEF:0 infotecs EPP 1.0.0.0 1:3098816:4 AM EXPLOIT Possible Mikrotik RouterOS 6.41.3-6.46.5 SMB Server DoS 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=NetAgentRules rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=snort ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 src=10.0.109.136 spt=53805 dst=10.0.109.71 dpt=445 transportProto=TCP </pre>                                                                                                                                                                   |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ProcessControl     | <p>Mar 16 12:46:23.135 EPP-Server</p> <p>CEF:0 infotecs EPP 1.0.0.0 380007 Portable Executable Injection 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=ProcessControl rt=1615898783135 cnt=1 HostName=Peter.P PC ThreatCat=privilege_escalation agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 suser=NT AUTHORITY\\NETWORK SERVICE sproc=C:\\Program Files\\Far2\\Far.exe</p>                                                                                                                                                                                                                                           |
| RegeditControl     | <p>Mar 16 12:46:23.135 EPP-Server</p> <p>CEF:0 infotecs EPP 1.0.0.0 100016 Изменение типа запуска службы (peectp) 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=RegeditControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=eventlog ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 RegistryPath=\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\Services\\FD ResPub\\ServiceData RegistryKey=FirstStart sproc=C:\\Windows\\System32\\svchost.exe RegistryOperationType=%%1905 RegistryOldValue=%%1800 RegistryNewValue=%%1800 suser=LOCAL SERVICE sntdom=NT AUTHORITY suid=S-1-5-19</p> |
| SystemActivity     | <p>Mar 16 12:46:23.135 EPP-Server</p> <p>CEF:0 infotecs EPP 1.0.0.0 400025 Создание службы с учетной записью SYSTEM 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=SystemActivity rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=eventlog ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 sourceServiceName=WinDivert1.3 ServiceFileName=C:\\Program Files\\infotecs\\ViPNet EndPoint Protection\\WinDivert64.sys ServiceType=0x1 ServiceStartType=3 ServiceAccount=LocalSystem suser=UFA-W0325\$ sntdom=infotecs-NT suid=S-1-5-18</p>                                                   |
| UserChangesControl | <p>Mar 16 12:46:23.135 EPP-Server</p> <p>CEF:0 infotecs EPP 1.0.0.0 890004 Изменение пароля пользователя 10 sensorExternalId=6D23F512-F1D4-42A2-9902-AD478CD6192A AgentId=9E48FAEE-08B3-47E0-8BA6-A8C1F900518E eventId=1234567890 SensorModule=hids threatSourceCat=UserChangesControl rt=1615898783135 cnt=1 HostName=Peter.P PC deviceFacility=eventlog ThreatCat=persistence agentIp=11.0.10.12 agentMac=00:0D:60:AF:1B:61 Anomaly=1 message=Mar 23 19:08:58 CentOS7 passwd: pam_unix(passwd:chauthtok): password changed for test</p>                                                                                                                                                                                                     |



# Возможные неполадки

## Потеряна связь с защищаемым узлом

Если связь с защищаемым узлом пропала, это означает, что на нем, возможно, перестал работать ViPNet EPP Агент, включая встроенные модули защиты.

Состояние защищаемых узлов можно отслеживать в ViPNet EPP Сервер (см. [Управление защищаемыми узлами группы](#)). Если вы заметили, что защищаемый узел неактивен, а причина заключается в работе ViPNet EPP Агент — перезагрузите компьютер защищаемого узла. После перезагрузки работа ViPNet EPP Агент будет восстановлена.

## В Kaspersky Endpoint Security Linux слишком большое количество проверяемых объектов

Если при совместной работе ViPNet EPP и Kaspersky Endpoint Security в Kaspersky Endpoint Security в модуле **Защита от файловых угроз** наблюдается слишком большое количество проверяемых объектов, исключите из антивирусной проверки следующие файлы:

- `/var/log/epp-agent/ossec.log`
- `/etc/epp-agent/traffic_journal.db`

Рекомендации по настройке исключений из антивирусной проверки см. в документации к Kaspersky Endpoint Security для Linux.

# Ошибка при обновлении ViPNet EPP Сервер на версию 1.8.0

При обновлении ViPNet EPP Сервер на версию 1.8.0 может возникнуть ошибка: «Повторяющееся значение ключа нарушает ограничение уникальности».

Чтобы обновить ViPNet EPP Сервер:

- 1 Средствами PostgreSQL удалите критерии обнаружения аномалий, у которых одинаковые типы правил (одинаковые значения в столбце `method`):
  - 1.1 В таблице `anomaly_detection_rules` базы данных `epp_server_kldfn`.
  - 1.2 В таблице `anomaly_detection_rules` базы данных `epp_worker_server_jhbfr`.
- 2 [Обновите ПО](#).



# Термины и сокращения

## CEF (Common Event Format)

Открытый текстовый формат описания событий. Позволяет агрегировать события различных типов сетевых устройств и приложений в едином формате.

## HIDS

Модуль, реализующий функции обнаружения вторжений; объект лицензирования ViPNet EPP.

## HIPS

Модуль, реализующий функции предотвращения вторжений; объект лицензирования ViPNet EPP.

## Personal Firewall

Модуль, реализующий функции персонального межсетевого экрана; объект лицензирования ViPNet EPP.

## SIEM (Security Information and Event Management)

Система управления событиями информационной безопасности, предназначенная для сбора сообщений, поступающих от различных источников (системы обнаружения вторжений, межсетевые экраны, антивирусные средства, сетевые устройства, операционные системы, различные приложения и т.п.), и их анализа с целью выявления отклонений от норм информационной безопасности по заданным критериям.

## Syslog

Прикладной протокол передачи и регистрации текстовых сообщений в IP-сетях; использует один из транспортных протоколов: TCP или UDP. Позволяет организовать сбор и хранение сообщений от распределенных источников в едином хранилище. Применяется для передачи событий ядра операционной системы, прикладного программного обеспечения, системных служб и других.

## ViPNet Client

Программа ViPNet Client 4U (ViPNet Client 5) предназначены для защиты IP-трафика на компьютерах с ОС Windows или GNU/Linux путем шифрования IP-пакетов.

## ViPNet SafePoint

Программный комплекс ViPNet SafePoint предназначен для защиты компьютеров с операционными системами семейства Microsoft Windows и Linux от несанкционированного доступа к информации.

ViPNet SafePoint обеспечивает защиту на уровне ядра ОС от следующих угроз:

- Внутренних угроз — компьютерных атак со стороны внутренних пользователей, обрабатывающих данные в информационной системе, а также привилегированных пользователей, выполняющих задачи администрирования в информационной системе.
- Внешних угроз — компьютерных атак (в том числе целевых атак) со стороны злоумышленников.

## ViPNet Update Server

Публичный веб-сервис, предоставляющий пользователям ViPNet EPP доступ к обновлениям баз правил, баз Malware detection и других экспертных данных.

## Zero Trust Network Access (ZTNA)

Технология сетевого доступа с нулевым доверием, основанная на принципах модели безопасности "Zero Trust", при которой каждый пользователь, устройство и сетевой ресурс перед получением доступа к ресурсам внутренней сети подвергаются проверке на основе детализированных правил контроля доступа. ZTNA позволяет повысить безопасность и защиту сетевых ресурсов.

## Аномалия

Отклонение от ожидаемой локальной (изменение состояния объектов операционной системы) и сетевой активности защищаемого узла. Аномалия обнаруживается при анализе событий информационной безопасности двумя методами:

- С помощью критериев обнаружения аномалий.
- С помощью поведенческого анализа (только в ОС Windows).

## База правил

Набор предустановленных параметров и правил работы модулей защиты ViPNet EPP: персонального межсетевого экрана, контроля приложений, обнаружения и предотвращения вторжений, ZTNA. Обновления базы правил регулярно публикуются на [сервере обновлений](#).

## Безопасность информации

Состояние информации, обрабатываемой в информационной системе, при котором сохраняется её конфиденциальность, целостность и доступность.

## Глобальные правила HIPS

Правила формируются на ViPNet EPP Сервер и действуют в пределах одной [базы правил](#); правила невозможно изменить на [защищаемом узле](#).

## Глобальные справочники

Справочники протоколов, адресов и расписаний формируются на ViPNet EPP Сервер и действуют в пределах одной [базы правил](#); справочники невозможно изменить на [защищаемом узле](#).

## Декодер

Анализатор [событий информационной безопасности](#), идентифицированных при изменениях на защищаемом узле: в реестре и файловой системе, при попытках входа и управления учетными записями.

## Защищаемый узел

Компьютер, на котором установлен ViPNet EPP Агент.

Синоним: узел.

## Злоумышленник

Физическое лицо (субъект), преднамеренно совершившее действия, следствием которых является нарушение [безопасности информации](#) на защищаемом узле.

Внутренний нарушитель находится на защищаемом узле, внешний — вне защищаемого узла.

## Инцидент информационной безопасности

Выявление нежелательных или неожиданных [событий информационной безопасности](#), с которыми связана значительная вероятность нарушения [безопасности информации](#).

## Командный интерпретатор

Командная оболочка, предназначенная для настройки ViPNet EPP Агент for Linux с помощью ряда специальных команд.

## Компьютерная атака

Целенаправленное воздействие на компьютер защищаемого узла, заключающееся в поиске и эксплуатации той или иной уязвимости, и т.о. реализации угрозы безопасности информации.

Синонимы: атака, вторжение.

## Критерий обнаружения аномалий

Временной интервал и список правил HIDS одного типа, для которых локальная или сетевая активность на защищаемом узле нетипична.

## Обнаружение и предотвращение вторжений

Модуль защиты ViPNet EPP Агент. Обнаруживает сетевые атаки и блокирует их с помощью персонального межсетевого экрана; реализовано модулями HIDS и HIPS.

## Персональный межсетевой экран

Модуль защиты ViPNet EPP Агент. Выполняет фильтрацию IP-пакетов сетевого трафика защищаемого узла с помощью сетевых фильтров; реализовано модулем PFW.

## Политика безопасности

Совокупность настроек модулей, системных и пользовательских правил, регулирующая безопасность защищаемых узлов.

## Пользовательские справочники

Справочники протоколов, адресов и расписаний, создаваемые на защищаемом узле для учета особенностей фильтрации. Обновление базы правил не влияет на пользовательские справочники.

## Пользовательские фильтры

[Сетевые фильтры](#), создаваемые на защищаемом узле для учета особенностей фильтрации. Обновление базы правил не влияет на пользовательские фильтры.

## Правила HIDS

Правила обнаружения событий информационной безопасности, основанные на сигнатурном методе анализа. Включают локальные и сетевые правила обнаружения атак.

## Правила анализа

Правила детального разбора информации о событии информационной безопасности, в том числе полученной от [декодера](#).

## Правила обнаружения сетевых атак

Правила отслеживания сетевой активности на защищаемом узле. Правила содержат [сигнатуры атак](#), позволяющие определить вредоносный сетевой трафик.

### Роль

Полномочия учетной записи пользователя по управлению и мониторингу ViPNet EPP Сервер и ViPNet EPP Агент.

### Сетевая атака

[Компьютерная атака](#) с использованием протоколов прикладного, транспортного и сетевого уровней модели передачи данных TCP/IP.

### Сетевой фильтр

Правило обработки IP-пакета сетевого трафика защищаемого узла персональным межсетевым экраном ViPNet EPP Агент на основании IP-адресов источника и получателя, протоколов, расписания. По типу действия различают блокирующие и разрешающие сетевые фильтры.

### Сетевые правила HIPS

Правила блокирования сетевой активности.

### Сеть ViPNet

Защищенная виртуальная частная сеть (VPN), построенная по технологии ViPNet, которая может быть развернута поверх локальных или глобальных сетей любой структуры. Трафик между узлами такой сети защищается с помощью шифрования на симметричных ключах. Ключи распределяются централизованно. Сеть ViPNet состоит из узлов, на которых установлено программное обеспечение ViPNet (шлюзы безопасности и клиенты).

### Сигнатура атаки

Признаки обнаружения компьютерной атаки, указанные в правиле обнаружения сетевых атак.

### Сигнатурный анализ

Метод выявления в потоке данных последовательности, которая определена как признак [вторжения](#), например сообщения об ошибках, записанные в журнал приложения. Метод реализован в модуле [HIDS](#).

### Событие информационной безопасности

Идентифицированное состояние информации, обрабатываемой на защищаемом узле, указывающее на возможное нарушение политики безопасности информации или возникновение

неизвестной ранее ситуации, которая может свидетельствовать о нарушении [безопасности информации](#).

### Справочник «Адреса и сети»

Совокупность однотипных объектов: содержит любую комбинацию IP v4- и IP v6 адресов или их диапазонов, используемых в [сетевых фильтрах](#).

### Справочник «Протоколы»

Совокупность однотипных объектов; содержит любую комбинацию сетевых, транспортных, и прикладных протоколов, а также их параметров, используемых в [сетевых фильтрах](#).

### Справочник «Расписания»

Совокупность однотипных объектов: содержит любую комбинацию параметров, определяющих время применения [сетевого фильтра](#).

### Угроза безопасности информации

Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения [безопасности информации](#).

### Уровень события

Степень серьезности [события информационной безопасности](#), в зависимости от которой требуется принятие мер реагирования разной срочности.

- Критическое.
- Опасное.
- Важное.
- Информационное.

### Устройство

[Защищаемый узел](#) как объект управления и мониторинга на ViPNet EPP Сервер.

### Уязвимость

Недостаток в программном или аппаратном обеспечении компьютера защищаемого узла, который делает возможным возникновение [угрозы безопасности информации](#).

### Фильтры по умолчанию

Предустановленные неизменяемые [сетевые фильтры](#).

## Фильтры политик безопасности

Сетевые фильтры, создаваемые на ViPNet EPP Сервер. Передаются на защищаемые узлы в составе базы правил; не могут быть изменены.