

ViPNet EndPoint Protection for Windows

Руководство администратора

Версия продукта: 1.8.0

infotecs

© АО «ИнфоТеКС», 2026

ФРКЕ.00238-01 32 01

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

Служба поддержки: hotline@infotecs.ru

Содержание

Введение ... **9**
О документе ... 10
Соглашения документа ... 10
О программном комплексе ... 11
Комплект поставки ... 12
Требования к установке ViPNet EPP Сервер ... 13
Требования к установке ViPNet EPP Серверная консоль ... 14
Требования к установке ViPNet EPP Агент ... 15
Совместимость с Oracle VM VirtualBox ... 16
Совместимость ViPNet EPP со сторонним программным обеспечением ... 16
Что нового в версии 1.8.0 ... 18
Обратная связь ... 20

Глава 1. Общие сведения ... **21**
Основные функции ... 22
Модели управления и принципы работы ... 24
Персональный межсетевой экран ... 27
Сетевой доступ с нулевым доверием (ZTNA) ... 33
Схема фильтрации трафика при интеграции с ViPNet Client 5 ... 35
Контроль приложений ... 39
Обнаружение признаков вредоносности в исполняемых файлах с помощью сканирования AntiMalware и блокировка опасных файлов ... 42
Обнаружение и предотвращение вторжений ... 43
Обнаружение вторжений ... 44
Предотвращение сетевых вторжений ... 46
Обнаружение и предотвращение бесфайловых атак ... 47
Блокировка доступа к вредоносным веб-ресурсам ... 48
Обнаружение аномалий с помощью критериев ... 49
Обнаружение аномалий с помощью поведенческого анализа ... 50
База правил (политика безопасности) ... 53
Уровни событий информационной безопасности ... 55
Ролевая модель ... 56
Управление доверенной загрузкой ... 58
Отслеживание работы антивирусов ... 59
Лицензирование ... 61

Глава 2. Ввод в эксплуатацию ... 63
Порядок ввода в эксплуатацию ViPNet EPP с агентами под управлением сервера ... 64
Порядок ввода в эксплуатацию ViPNet EPP с автономными агентами ... 66
Установка, обновление, восстановление и удаление ... 67
Подготовка к установке ViPNet EPP ... 67
Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль ... 68
Установка ViPNet EPP Серверная консоль ... 70
Установка ViPNet EPP Агент ... 71
Установка ViPNet EPP Агент вручную ... 72
Установка ViPNet EPP Агент с помощью групповых политик Active Directory ... 73
Восстановление или удаление ViPNet EPP Сервер и ViPNet EPP Серверная консоль ... 76
Восстановление или удаление ViPNet EPP Агент ... 77
Обновление ... 78
Порядок обновления ViPNet EPP версии 1.5.2 и выше до версии 1.8.0 ... 78
Порядок перехода с ViPNet EPP версии 1.5.1 или ниже на версию 1.8.0 ... 82

Глава 3. Управление в ViPNet EPP Сервер ... 84
Подключение к ViPNet EPP Сервер ... 85
Интерфейс ViPNet EPP Сервер ... 87
Установка и активация лицензии ... 89
Управление защищаемыми узлами и группами ... 90
Подключение защищаемых узлов ... 90
Настройка автоматического подключения защищаемых узлов ... 92
Импорт защищаемых узлов из домена Active Directory ... 93
Управление группами защищаемых узлов и просмотр сведений о группах ... 93
Управление защищаемыми узлами группы ... 94
Управление базами правил ... 98
Загрузка обновлений баз правил на ViPNet EPP Сервер ... 100
Автоматическая загрузка обновлений базы правил ... 100
Загрузка обновления базы правил вручную ... 103
Просмотр и удаление избранных правил ... 105
Настройка базы правил ... 107
Назначение базы правил группе узлов ... 107
Выбор режимов работы модулей защиты ... 108
Управление фильтрацией трафика ... 109
Настройка фильтров политик безопасности ... 109
Настройка справочников ... 115
Настройка источника получения фильтров политик безопасности ... 121

Управление политиками ZTNA ... 122
Добавление и настройка новых правил политики ZTNA ... 126
Управление запуском и активностью приложений ... 135
Управление запуском приложений ... 135
Настройка контроля обращений к сетевым папкам ... 143
Особенности задания и использования правил доступа ... 144
Изменение порядка применения правил доступа для приложений ... 146
Настройка правил доступа по умолчанию для группы приложений ... 148
Управление обнаружением и предотвращением вторжений ... 149
Настройка правил HIDS ... 149
Настройка правил HIPS ... 161
Настройка веб-фильтров ... 169
Настройка политик аудита ... 174
Управление ViPNet SafeBoot на защищаемых узлах ... 180
Порядок управления ... 180
Просмотр информации о версии и состоянии ViPNet SafeBoot на защищаемых узлах ... 182
Управление лицензиями ... 183
Загрузка лицензий ViPNet SafeBoot на ViPNet EPP Сервер ... 183
Просмотр информации о свободных лицензиях ViPNet SafeBoot ... 184
Распределение, отправка и активация лицензии ViPNet SafeBoot на защищаемых узлах ... 185
Выгрузка журнала аудита ViPNet SafeBoot с защищаемых узлов ... 186
Управление учетными записями пользователей ViPNet SafeBoot ... 186
Просмотр учетных записей на защищаемых узлах ... 187
Изменение параметров и блокировка учетной записи ... 187
Добавление новых учетных записей ... 189
Удаление учетных записей ... 190
Обновление ViPNet SafeBoot на защищаемых узлах ... 191
Загрузка и удаление обновлений на ViPNet EPP Сервер ... 194
Управление корневыми сертификатами и CRL ... 194
Просмотр информации о сертификатах на защищаемых узлах, выгрузка и удаление сертификатов ... 195
Установка корневых сертификатов и CRL ... 196
Настройка критериев обнаружения аномалий ... 198
Настройка модели нормальной активности защищаемого узла ... 199
Сканирование AntiMalware ... 202
Запуск сканирования вручную ... 203
Просмотр и обработка результатов сканирования ... 204

Просмотр и настройка параметров сканирования ... 208
Настройка расписания автоматического запуска сканирования ... 210
Работа с журналами ... 212
Журнал событий ... 212
Выявление ложных аномалий ... 218
Журнал аудита ... 219
Запрос журнала регистрации трафика с ViPNet EPP Агент ... 221
Администрирование ViPNet EPP Сервер ... 225
Управление учетными записями ... 225
Требования к имени и паролю учетной записи ... 225
Просмотр списка учетных записей ... 226
Создание учетной записи ... 226
Изменение учетной записи ... 227
Удаление учетной записи ... 227
Настройка параметров системы ... 227
Проверка работоспособности ... 230
Диагностические журналы ... 231
Обновление лицензии ... 231
Резервное копирование и восстановление конфигурации ... 232
Интеграция с внешними системами ... 234
Передача уведомлений по электронной почте ... 234
Подключение к домену Active Directory ... 236
Передача событий информационной безопасности в сторонние системы ... 236
Передача событий в сторонние системы по протоколу UDP ... 237
Передача событий в ViPNet TIAS ... 237

Глава 4. Локальное управление ViPNet EPP Агент ... 239
Подключение к ViPNet EPP Агент ... 240
Интерфейс ViPNet EPP Агент ... 241
Установка и активация лицензии ... 243
Управление базой правил ... 244
Загрузка и обновление базы правил ... 244
Распространение настроек средств защиты на другие агенты ... 246
Экспорт базы правил ... 247
Управление фильтрацией трафика ... 248
Выбор режима работы ... 248
Основные действия по управлению фильтрацией ... 248
Настройка пользовательских сетевых фильтров ... 249
Настройка пользовательских справочников ... 251

Настройка справочников ViPNet ... 252
Запрет входящих соединений ... 253
Работа с журналами персонального межсетевого экрана ... 254
Журнал активных соединений ... 254
Журнал трафика ... 255
Просмотр статуса выполнения политики ZTNA ... 259
Управление запуском и активностью приложений ... 260
Выбор режима работы контроля приложений ... 260
Просмотр списков контроля приложений ... 260
Управление пользовательскими списками приложений ... 262
Создание правил доступа приложения ... 264
Изменение порядка применения правил доступа для приложений ... 266
Настройка контроля обращений к сетевым папкам ... 268
Настройка правил доступа по умолчанию для группы приложений ... 268
Сканирование AntiMalware ... 269
Просмотр и обработка результатов сканирования AntiMalware ... 270
Журнал событий контроля приложений ... 272
Управление обнаружением и предотвращением вторжений ... 275
Выбор режима работы ... 275
Просмотр и настройка правил HIDS ... 276
Просмотр и настройка сетевых правил HIPS ... 276
Просмотр и настройка веб-фильтров ... 278
Управление пользовательскими правилами HIPS для бесфайловых атак ... 278
Политика аудита ... 279
Журнал событий обнаружения и предотвращения вторжений ... 280
Настройка критериев обнаружения аномалий ... 284
Работа с журналами ... 285
Журнал событий ... 285
Журнал аудита ... 288
Настройка типов регистрируемых событий в журнале аудита ... 290
Администрирование ViPNet EPP Агент ... 292
Управление учетными записями ... 292
Просмотр и настройка параметров работы ... 293
Перевод автономного ViPNet EPP Агент под управление ViPNet EPP Сервер ... 294
Изменение адреса ViPNet EPP Сервер ... 294
Настройка самозащиты ... 295
Проверка работоспособности ... 295
Диагностические журналы ... 297
Просмотр сведений о лицензии ... 297

Управление из области уведомлений панели задач ОС Windows ... 298
Уведомления о срабатывании модулей защиты и обновлении ViPNet SafeBoot ... 299

Приложение A. Полномочия пользователей ... 300

Приложение B. Типы и идентификаторы правил ... 304

Приложение C. Типы аномалий, обнаруживаемые с помощью поведенческого анализа ... 309

Приложение D. Структура CEF-сообщения ... 311

Приложение E. Возможные неполадки ... 326
В ViPNet EPP Сервер не приходит запрос на подключение от ViPNet EPP Агент ... 326
Ошибка подключения "Не удалось подключиться к сервису" ... 326
Потеряна связь с защищаемым узлом ... 327
Ошибка типа «синий экран» ОС Windows на компьютере защищаемого узла ... 327
Высокая загрузка процессора на компьютере защищаемого узла ... 327
На компьютере защищаемого узла с ОС Windows 10 сбрасываются приложения по умолчанию ... 328
Не работает блокировка драйвера ... 328
Не работает блокировка dll-библиотеки с помощью правила доступа к процессам ... 328
Проблемы при работе с MS Office 2010 x86 ... 328
Ошибка запуска Powershell после настройки политики аудита ... 329
Ошибка подключения при использовании приложений, создающих сетевые соединения по протоколу SSL/TLS ... 329
Ошибка подключения к базе данных при восстановлении ViPNet EPP Сервер ... 329
Ошибка «Служба EPP недоступна» ... 330
Не удается подключиться к удаленному Серверу ... 330

Приложение F. История версий ... 331
Что нового в версии 1.7.1 ... 331
Что нового в версии 1.7.0 ... 334
Что нового в версии 1.6.0 ... 336
Что нового в версии 1.5.2 ... 339

Приложение G. Термины и сокращения ... 340



Введение

О документе 10

О программном комплексе 11

Что нового в версии 1.8.0 18

Обратная связь 20

О документе

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

Документ предназначен для администраторов информационной безопасности организаций.

Соглашения документа

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приемы и хорошие практики
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.

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 Windows:
  - Клиентский компонент — ViPNet EPP Агент for Windows (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 основных модулей защиты:
    - Персональный межсетевой экран. Выполняет фильтрацию IP-трафика и блокирует нежелательную сетевую активность.
    - Контроль приложений. Управляет запуском и активностью приложений, а также их доступом к файлам, реестру ОС Windows, процессам и параметрам командной строки; предотвращает установку и запуск вредоносного программного обеспечения.
    - Обнаружение и предотвращение вторжений. Обнаруживает и блокирует сетевые атаки и атаки уровня защищаемого узла.
    - Сетевой доступ с нулевым доверием (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 Windows (далее ViPNet EPP Сервер или сервер). Обеспечивает:
    - Централизованное управление ViPNet EPP Агент на защищаемых узлах.
    - Консолидацию событий информационной безопасности защищаемых узлов и обнаружение среди них аномалий.

    Для управления в ViPNet EPP Сервер используется ViPNet EPP Серверная консоль, входящая в состав ViPNet EPP Сервер.
- Клиентский и серверный компоненты для установки в ОС GNU/Linux (далее — ViPNet EPP Агент for Linux и ViPNet EPP Сервер for Linux. Подробно об использовании этих компонентов см. в документе «ViPNet EPP for Linux. Руководство администратора».

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.

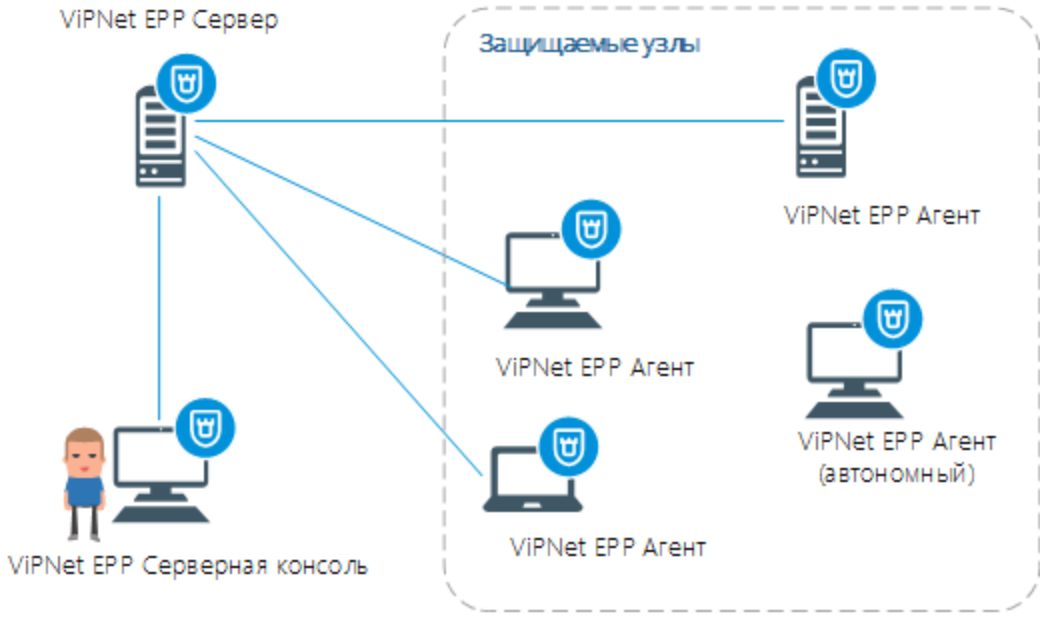


Рисунок 1. Компоненты ViPNet EPP

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

Список основных функций ViPNet EPP см. в разделе Основные функции.

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».

Требования к установке ViPNet EPP Сервер

Требования к компьютеру, предназначенному для установки ViPNet EPP Сервер и ViPNet EPP Серверная консоль:

- Процессор — x86-совместимый, количество физических ядер 4 и более, тактовая частота одного ядра — не менее 2.2 ГГц.
- Объем оперативной памяти — не менее 16 Гбайт.
- Свободное место на диске (рекомендуется твердотельный накопитель) — не менее 500 Гбайт. Рекомендуется твердотельный накопитель.
- Сетевой адаптер.
- Операционная система (64-разрядная):
  - Windows 11 LTSC 2024 Корпоративная версия 24H2;
  - Windows Server 2019 Standard и Datacenter версия 1809;
  - Windows Server 2022 Standard и Datacenter версия 21H2 EN.



Внимание! Для операционной системы необходимо установить последний накопительный пакет обновлений.

На компьютер должны быть установлены:

- Пакет платформы Microsoft .NET Desktop Runtime версии 8.0.11 (.NET 8) и последнее обновление системы безопасности платформы.
- Microsoft Visual C++ 2015–2022 Redistributable Package (x64).
- СУБД PostgreSQL версии 14.

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'`.

Эти компоненты входят в комплект поставки ViPNet EPP. Если компоненты не установлены, установите их перед установкой ViPNet EPP Сервер.

Требования к установке ViPNet EPP Серверная консоль

Требования к компьютеру, предназначенному для установки ViPNet EPP Серверная консоль:

- Процессор — x86-совместимый, количество физических ядер 2 и более, тактовая частота одного ядра — не менее 3.2 ГГц.
- Объем оперативной памяти — не менее 4 Гбайт.
- Свободное место на жестком диске — не менее 600 Мбайт.
- Сетевой адаптер.
- Операционная система (64-разрядная):
  - Windows 11 LTSC 2024 Корпоративная версия 24H2;
  - Windows Server 2019 Standard и Datacenter версия 1809;
  - Windows Server 2022 Standard и Datacenter версия 21H2 EN.

Внимание! Для операционной системы необходимо установить последний накопительный пакет обновлений.

На компьютер должны быть установлены:

- Пакет платформы Microsoft .NET Desktop Runtime версии 8.0.11 (.NET 8) и последнее обновление системы безопасности платформы.
- Microsoft Visual C++ 2015–2022 Redistributable Package (x64).
- СУБД PostgreSQL версии 14.

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'`.

Эти компоненты входят в комплект поставки ViPNet EPP. Если компоненты не установлены, установите их перед установкой ViPNet EPP Серверная консоль.

Требования к установке ViPNet EPP Агент

Требования к компьютеру, предназначенному для установки ViPNet EPP Агент Windows:

- Процессор — x86-совместимый, количество физических ядер 2 и более, тактовая частота одного ядра — не менее 3.2 ГГц.
- Объем оперативной памяти — не менее 4 Гбайт.
- Свободное место на жестком диске — не менее 5 Гбайт.
- Сетевой адаптер.
- Операционная система (64-разрядная):
  - Windows 10 LTSC Корпоративная версия 21H2;
  - Windows 11 Версия 25H2 Pro;
  - Windows 11 LTSC 2024 Корпоративная версия 24H2;
  - Windows Server 2019 Standard и Datacenter версия 1809;
  - Windows Server 2022 Standard и Datacenter версия 21H2;
  - Windows Server 2025 Standard и Datacenter версия 24H2.

Внимание! Для операционной системы необходимо установить последний накопительный пакет обновлений.

На компьютер должны быть установлены:

- Пакет платформы Microsoft .NET Desktop Runtime версии 8.0.11 (.NET 8) и последнее обновление системы безопасности платформы.
- Microsoft Visual C++ 2015–2022 Redistributable Package (x64).

Эти компоненты входят в комплект поставки ViPNet EPP Агент Windows. Если компоненты не установлены, установите их перед установкой ViPNet EPP Агент Windows.

Допускается установка ViPNet EPP Агент на один компьютер с ViPNet EPP Сервер.

Совместимость с Oracle VM VirtualBox

Если на компьютере с ViPNet EPP Агент также установлен Oracle VM VirtualBox, для сохранения работоспособности в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\scanmemdrv\Parameters\Dont Inject To` создайте параметры `REG_SZ` с произвольными именами ключей и со следующими значениями:

```
C:\Program Files\Oracle\VirtualBox\VirtualBoxVM.exe
C:\Program Files\Oracle\VirtualBox\VBoxSVC.exe
C:\Program Files\Oracle\VirtualBox\VBoxSDS.exe
C:\Program Files\Oracle\VirtualBox\VBoxNetDHCP.exe
C:\Program Files\Oracle\VirtualBox\VirtualBox.exe
C:\Program Files\Oracle\VirtualBox\VBoxNetNAT.exe
C:\Program Files\Oracle\VirtualBox\VBoxSDL.exe
```

Совместимость ViPNet EPP со сторонним программным обеспечением

ViPNet EPP for Windows, совместим со следующим программным обеспечением:

- Может передавать 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 Windows).

  Если на компьютерах предполагается совместная работа ViPNet EPP и ViPNet SafePoint, отключите (см. Выбор режимов работы модулей защиты) модуль контроль приложений ViPNet EPP.
- Может использоваться на защищаемых узлах совместно с ViPNet Client 5 версии 5.4 (для ОС Windows).

Внимание! 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;
  - из ViPNet Prime Policy Management версии и 1.9.
- Возможно управление ViPNet SafeBoot версий 2.1.2, 3.0.3, 3.2.0 и 3.2.1, установленным на защищаемых узлах.

- На защищаемых узлах отслеживается работа антивирусного программного обеспечения (далее — антивирусов):
  - Kaspersky Endpoint Security версий 12.8.0.505, 12.10.0.466 (для ОС Windows).
  - Dr.Web Desktop Security Suite версий 13.0.3, 13.0.5, 12.0 в исполнении 2 (для ОС Windows), Dr.Web Security Space версии 12.0 (для ОС Windows).

Что нового в версии 1.8.0

Изменения в предыдущих версиях см. в приложении История версий.

- **Реализован веб-сервер ViPNet EPP for Linux**

  ViPNet EPP Сервер for Linux теперь реализован как веб-серверное решение. Для управления ViPNet EPP Сервер for Linux используется веб-интерфейс, к которому пользователи подключаются со своих рабочих мест с помощью браузера по защищенному каналу TLS. Пользовательский интерфейс ViPNet EPP Сервер for Linux полностью переработан и имеет новый дизайн. ViPNet EPP Сервер for Linux поддерживает работу в ОС Astra Linux Special Edition 1.8.2.7 БЮЛЛЕТЕНЬ № 2025-0411SE18 (оперативное обновление 1.8.2).

  В состав ViPNet EPP Сервер for Linux входят компоненты: сервер управления и рабочий сервер. Доступно масштабирование ViPNet EPP Сервер for Linux, например при увеличении количества управляемых устройств, путем развертывания нескольких рабочих серверов для распределения нагрузки.

  Теперь к ViPNet EPP Сервер for Linux могут быть подключены для управления не только защищаемые узлы с ViPNet EPP Агент for Linux, но и с ViPNet EPP Агент for Windows. В ViPNet EPP Сервер for Linux не поддерживаются некоторые функции по управлению ViPNet EPP Агент: управление параметрами AntiMalware, управление ViPNet SafeBoot и проведение поведенческого анализа.

  Подробнее см. в документе «ViPNet EPP for Linux. Руководство администратора» в разделах «О программном комплексе», «Требования к установке ViPNet EPP Сервер».

- **Новые возможности в ViPNet EPP Сервер for Linux**

  В ViPNet EPP Сервер for Linux добавлены новые возможности управления:

  - Настройка автоматического подключения защищаемых узлов к ViPNet EPP Сервер for Linux.
  - Настройка автоматической загрузки обновлений базы правил.
  - Проверка электронной подписи при загрузке обновления базы правил в ViPNet EPP Сервер for Linux.
  - Настройка политики безопасности. Реализован редактор параметров и правил политики безопасности для защищаемых узлов с ViPNet EPP Агент for Windows и ViPNet EPP Агент for Linux. Политика безопасности формируется в ViPNet EPP Сервер for Linux на основе базы системных правил, загружаемой с сервера обновления.
  - Импорт данных из другой политики безопасности в процессе настройки политики.
  - Запрос журнала регистрации трафика с защищаемых узлов.
  - Передача уведомлений о зарегистрированных событиях по электронной почте.
  - Передача зарегистрированных событий в сторонние системы мониторинга и анализа (SIEM, ViPNet TIAS и другие) с помощью прикладного протокола Syslog.

- Доступ с учетными записями администратора и аудитора, созданными на сервере, к управлению в локальной консоли ViPNet EPP Агент.

Подробнее см. в документе «ViPNet EPP for Linux. Руководство администратора».

- **Изменения поддерживаемых ОС GNU/Linux для ViPNet EPP Агент**

  Реализована поддержка работы ViPNet EPP Агент в ОС AlterOS 9.6 Agile Phoenix. Изменен список поддерживаемых версий ОС Astra Linux, Альт, РЕД ОС и Debian Linux.

  Список всех номеров версий поддерживаемых ОС GNU/Linux см. в документе «ViPNet EPP for Linux. Руководство администратора» в разделе «Требования к установке ViPNet EPP Агент».

- **Изменения поддерживаемых ОС Windows для ViPNet EPP Сервер и ViPNet EPP Агент**

  Прекращена поддержка работы ViPNet EPP Сервер в ОС Windows 10. Изменен список поддерживаемых версий ОС Windows 11.

  Реализована поддержка работы ViPNet EPP Агент в ОС Windows Server 2025. Изменен список поддерживаемых версий ОС Windows 10, Windows 11.

  Список всех номеров версий поддерживаемых ОС Windows см. в разделах Требования к установке ViPNet EPP Сервер и Требования к установке ViPNet EPP Агент.

- **Обновление ViPNet EPP**

  Обновление ViPNet EPP до версии 1.8.0 возможно только с версии 1.7.1. Обновление с более старых версий должно выполняться по определенной схеме.

  Подробнее см. в разделе Порядок обновления ViPNet EPP версии 1.5.2 и выше до версии 1.8.0 и в документе «ViPNet EPP for Linux. Руководство администратора» в аналогичном разделе.

- **Запрет смены режимов работы модулей защиты в ViPNet EPP Агент для учетных записей с ролью Пользователь**

  Теперь при подключении к локальной консоли ViPNet EPP Агент с правами пользователя изменение режимов модулей защиты недоступно.

  Подробнее см. в разделе Полномочия пользователей и документе «ViPNet EPP. Руководство пользователя».

- **Проверка наличия установленных обновлений ОС Windows на защищаемых узлах под управлением ViPNet EPP Сервер for Windows**

  Теперь в ViPNet EPP Сервер for Windows в политике ZTNA для защищаемых узлов с ViPNet EPP Агент for Windows доступна настройка правил для проверки наличия установленных обновлений ОС Windows. Вы можете указать выпуск, версию и сборку ОС Windows для проверки и задать список обновлений, которые должны быть установлены на защищаемых узлах. При проверке, если хотя бы одно обновление не будет найдено среди установленных на защищаемом узле, политика ZTNA будет не выполнена.

  Подробнее см. в разделах Сетевой доступ с нулевым доверием (см. Сетевой доступ с нулевым доверием (ZTNA)) и Добавление и настройка новых правил политики ZTNA.

- **Исправление ошибок**

  Устранены ошибки, выявленные в процессе эксплуатации предыдущей версии.

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.

  Форма для обращения в службу поддержки через сайт.

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: 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. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется политикой ответственного разглашения.

1

Общие сведения

Основные функции 22

Модели управления и принципы работы 24

Персональный межсетевой экран 27

Контроль приложений 39

Обнаружение и предотвращение вторжений 43

База правил (политика безопасности) 53

Уровни событий информационной безопасности 55

Ролевая модель 56

Управление доверенной загрузкой 58

Отслеживание работы антивирусов 59

Лицензирование 61

Основные функции

Основные функции ViPNet EPP for Windows:

- Фильтрация IP-трафика защищаемого узла (см. Персональный 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)). Доступно только в ViPNet EPP с агентами под управлением сервера.
- Контроль установки, запуска и активности приложений защищаемого узла (см. Контроль приложений)*.
- Обнаружение признаков вредоносности в исполняемых файлах с помощью сканирования AntiMalware и блокировка опасных файлов*.
- 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).
- Обнаружение и предотвращение бесфайловых атак*.
- Блокировка доступа к вредоносным веб-ресурсам*.
- Контроль аномальной активности защищаемого узла:
  - С помощью критериев (см. Обнаружение аномалий с помощью критериев).
  - С помощью поведенческого анализа (см. Обнаружение аномалий с помощью поведенческого анализа)*. Доступно только в ViPNet EPP с агентами под управлением сервера.
- Управление доверенной загрузкой на защищаемых узлах. Доступно только в ViPNet EPP с агентами под управлением сервера.

Функции мониторинга и оповещения ViPNet EPP for Windows:

- 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.
- Отображение статусов защищаемого узла в ViPNet EPP Агент: защита отключена, пониженный статус защиты и устройство защищено (см. в документе «ViPNet EPP. Руководство пользователя»).
- Консолидация событий информационной безопасности защищаемых узлов в ViPNet EPP Сервер и визуализация сводки событий на инфопанели (см. Интерфейс ViPNet EPP Сервер).
- Оповещение о событиях информационной безопасности по электронной почте (см. Передача уведомлений по электронной почте). Настройка доступна только 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 только в ViPNet EPP Сервер.

Служебные функции ViPNet EPP for Windows:

- Обновление базы правил системных правил (см. База правил (политика безопасности)).
- Управление учетными записями и разграничение полномочий пользователей (см. Ролевая модель).
- Управление защищаемыми узлами (см. Управление защищаемыми узлами и группами).
- Регистрация действий пользователей в журналах аудита ViPNet EPP Сервер (см. Журнал аудита) и ViPNet EPP Агент (см. Журнал аудита).
- Проверка работоспособности ViPNet EPP Сервер (см. Проверка работоспособности) и ViPNet EPP Агент (см. Проверка работоспособности).
- Резервное копирование и восстановление конфигурации ViPNet EPP Сервер (см. Резервное копирование и восстановление конфигурации).



Примечание. * — в ViPNet EPP Сервер эти функции можно настроить только для защищаемых узлов с ViPNet EPP Агент for Windows, поскольку для защищаемых узлов с ViPNet EPP Агент for Linux функции недоступны.

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 Windows или к ViPNet EPP Сервер for Linux.

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.

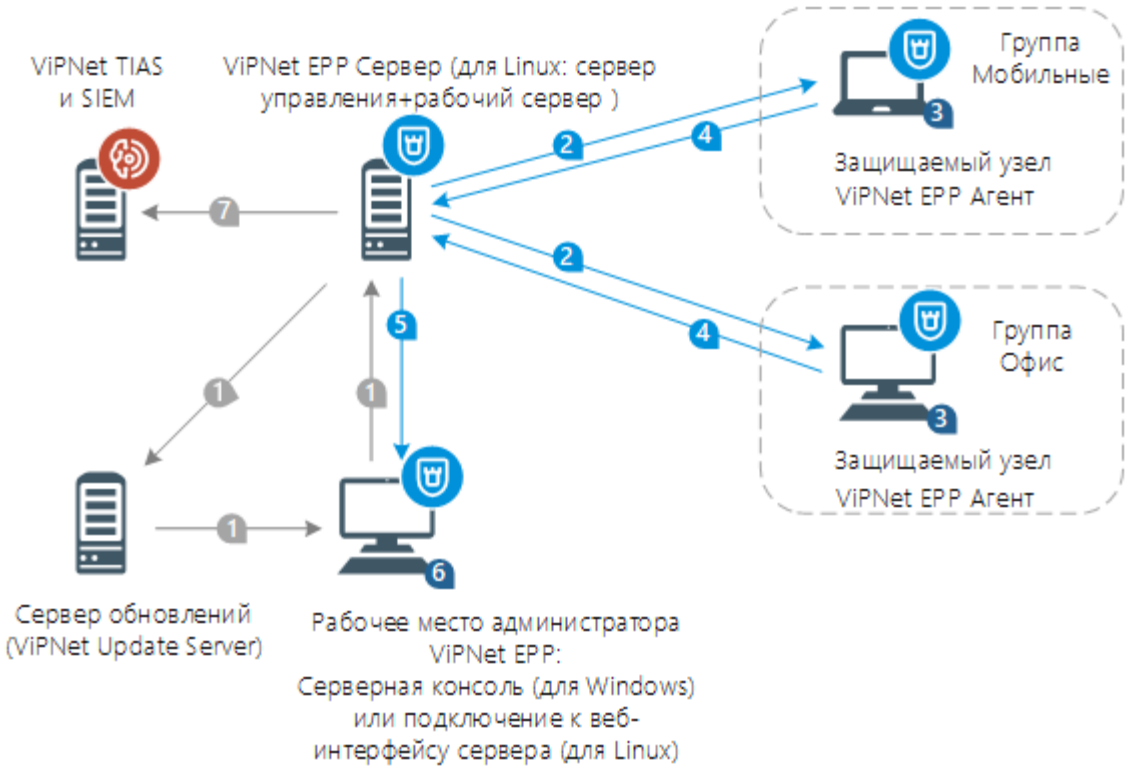


Рисунок 2. Работа ViPNet EPP Агент под управлением ViPNet EPP Сервер

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.

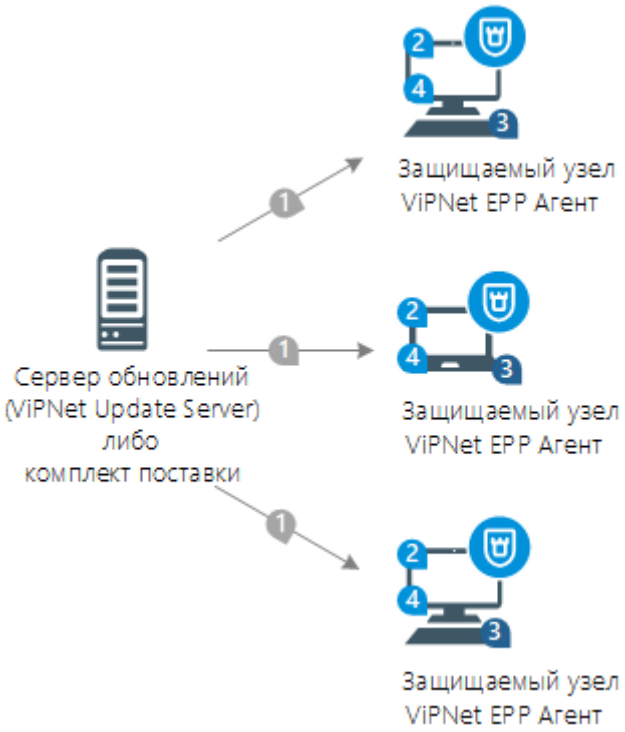


Рисунок 3. Автономная работа ViPNet EPP Агент

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.

Персональный межсетевой экран

Межсетевой экран ViPNet EPP Агент выполняет фильтрацию IP-пакетов на защищаемом узле и реализован модулем Personal Firewall.

При установке ViPNet EPP Агент на компьютере с установленной программой ViPNet Client 5 персональный межсетевой экран ViPNet EPP Агент будет выполнять фильтрацию IP-трафика открытой сети, а также может использоваться для создания пользовательских фильтров защищенной сети для фильтрации IP-трафика между узлами сети ViPNet.

Требования к программе ViPNet Client 5, совместимой с ViPNet EPP, см. в разделе Совместимость ViPNet EPP со сторонним программным обеспечением.

Результат фильтрации IP-пакетов открытой сети зависит от выбранного режима работы и действия сетевых фильтров персонального 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 базы правил (см. База правил (политика безопасности)). Передаются с сервера на защищаемые узлы, подключенные к серверу, в составе базы правил 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 все 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 зафиксируются 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 5, будет фильтроваться IP-трафик открытой сети, т.е. не относящийся к трафику сети ViPNet.

- Фильтры защищенной сети ViPNet — доступны только на защищаемом узле с установленной программой ViPNet Client 5, для фильтрации IP-трафика защищенной сети между своим узлом и узлами сети ViPNet, с которыми есть связь в программе ViPNet Client 5. Целесообразно использовать фильтры защищенной сети только для блокирования IP-трафика, поскольку заблокированный политиками безопасности ViPNet Client 5 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 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.

- **Фильтры по умолчанию** — заданы в базе правил 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 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 IP v4 и IP v6.
- 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 формат файлов мобильного кода (JavaScript, PDF) для контентной фильтрации HTTP-трафика.
- 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** — содержит любую комбинацию сетевых, транспортных протоколов, а также их параметров.
- **Адреса и сети** — содержит различные комбинации IP v4- либо IP v6-адресов или их диапазонов.

- **Справочники ViPNet** — доступен только на защищаемом узле с установленной программой ViPNet Client 5 и отображается в **Адреса и сети**. Содержит сетевые узлы сети ViPNet, с которыми на защищаемом узле есть связь в программе 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 IP-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 5 и относится к типу **Справочники ViPNet**. Содержит все имена сетевых узлов сети ViPNet, с которыми есть связь в программе 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, называются глобальными. Они передаются в ViPNet EPP Агент в составе базы правил 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 5, доступно создание пользовательских справочников 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 персонального 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** — 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** — в этом режиме по умолчанию блокируются все входящие и исходящие соединения открытой сети, кроме разрешенных фильтрами политик безопасности и пользовательскими фильтрами. Режим рекомендуется использовать при работе в частной сети, например, из дома.
- **Корпоративная сеть** — в этом режиме по умолчанию пропускаются все исходящие и входящие соединения, кроме запрещенных пользовательскими фильтрами. Режим

рекомендуется использовать при работе в сети с относительно низким уровнем угроз безопасности.

- **Отключено** — в этом режиме персональный межсетевой экран отключен и не влияет на сетевой трафик.

Режим работы передается в ViPNet EPP Агент защищаемого узла в составе базы правил. Для учета особенностей фильтрации IP-пакетов на защищаемом узле режим работы персонального межсетевого экрана ViPNet EPP Агент можно изменить локально. Обновление базы правил может изменить этот режим.

Если на защищаемом узле установлена программа ViPNet Client 5, режим работы будет действовать только на IP-трафик открытой сети.

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

Режим работы	Фильтры политик безопасности	Пользовательские фильтры открытой сети	Действие фильтров по умолчанию
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** > **Фильтры по умолчанию**.

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 сетевых фильтров этого режима работы, 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 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 см. в разделе Схема фильтрации трафика при интеграции с ViPNet Client 5.

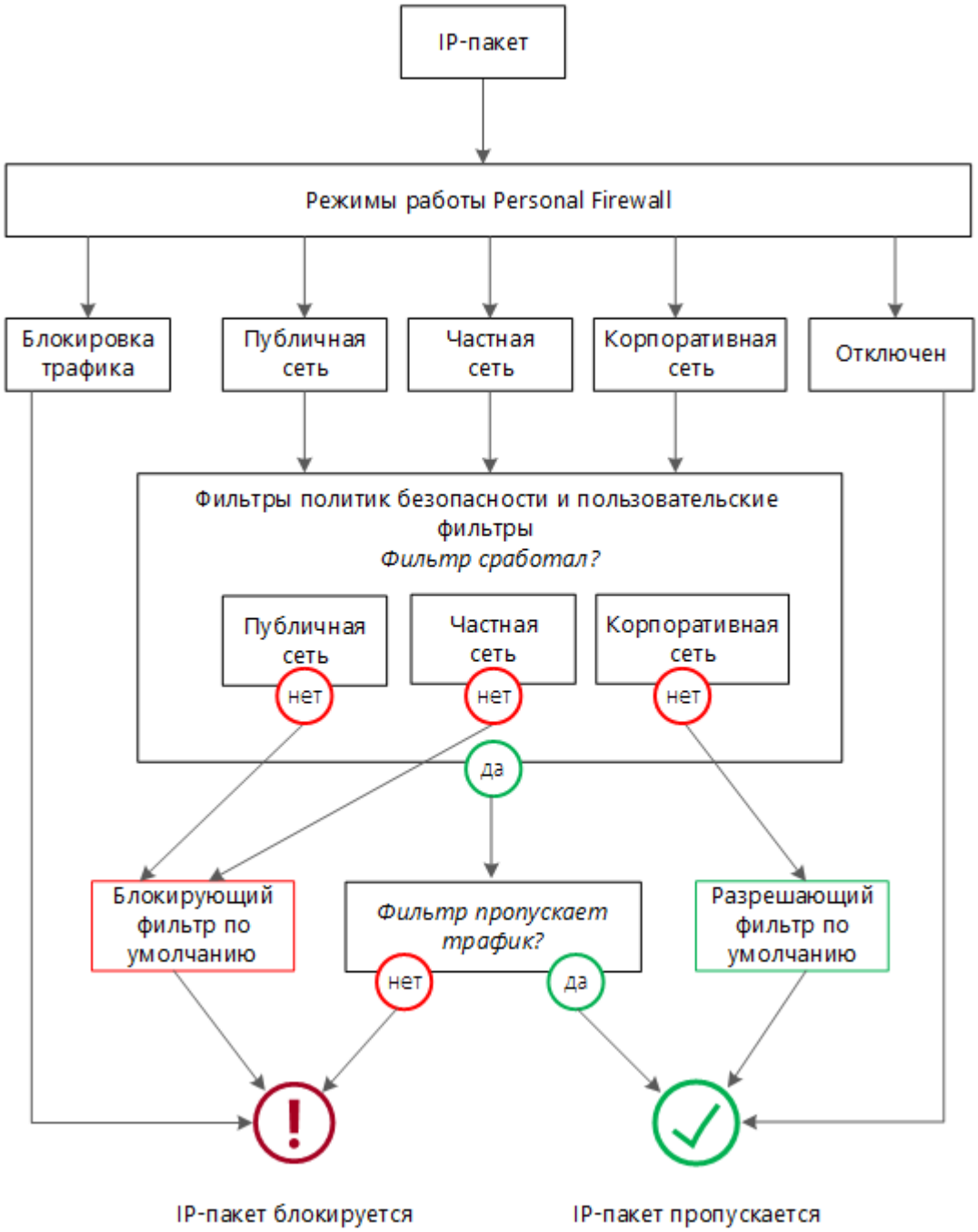


Рисунок 4. Схема фильтрации IP-трафика открытой сети

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 Персональный межсетевой экран. ZTNA работает только в ViPNet EPP Агент под управлением сервера.

Технология сетевого доступа с нулевым доверием позволяет отслеживать на всех защищаемых узлах, подключенных к ViPNet EPP Сервер, выполнение политик ZTNA, заданных для защищаемых узлов. На защищаемых узлах с установленной программой ViPNet Client 5 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 Персональный межсетевой экран.

Требования к программе ViPNet Client 5, совместимой с ViPNet EPP, см. в разделе Совместимость ViPNet EPP со сторонним программным обеспечением.

Политики ZTNA настраиваются в ViPNet EPP Сервер и отправляются в ViPNet EPP Агент в составе базы правил (политики безопасности). Из ViPNet Policy Manager (или ViPNet Prime Policy Management) могут быть получены исключения из политик 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).

В ViPNet EPP Агент доступен только просмотр статуса выполнения политик 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 Prime Policy Management (ViPNet Policy Manager) были получены данные об исключениях из ZTNA, при невыполнении политики ZTNA ресурсы защищенной сети ViPNet из списка исключений 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 Управление политиками 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 быть установлено или не установлено на защищаемом узле. Проверяться будет только программное обеспечение из списка программ и компонентов Windows.
- Список процессов, которые должны быть запущены или не запущены на защищаемом узле.
- Список служб, которые должны выполняться или не выполняться на защищаемом узле.
- Список файлов, которые должны присутствовать или отсутствовать на защищаемом узле.
- Список путей к ключам реестра, которые должны существовать или не существовать на защищаемом узле. Для целочисленных и строковых значений ключей могут быть заданы дополнительные критерии проверки.
- Список обновлений ОС Windows, которые должны быть установлены на защищаемом узле. Можно добавить вручную и из файла формата CSV, выгруженного из Windows Server Update Services.

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

- Список служб systemd, которые должны выполняться или не выполняться на защищаемом узле.
- Список файлов, которые должны присутствовать или отсутствовать на защищаемом узле.
- Список модулей ядра ОС, которые должны быть загружены или не загружены на защищаемом узле.
- Список версий ядра ОС, которые должны использоваться или не 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)).

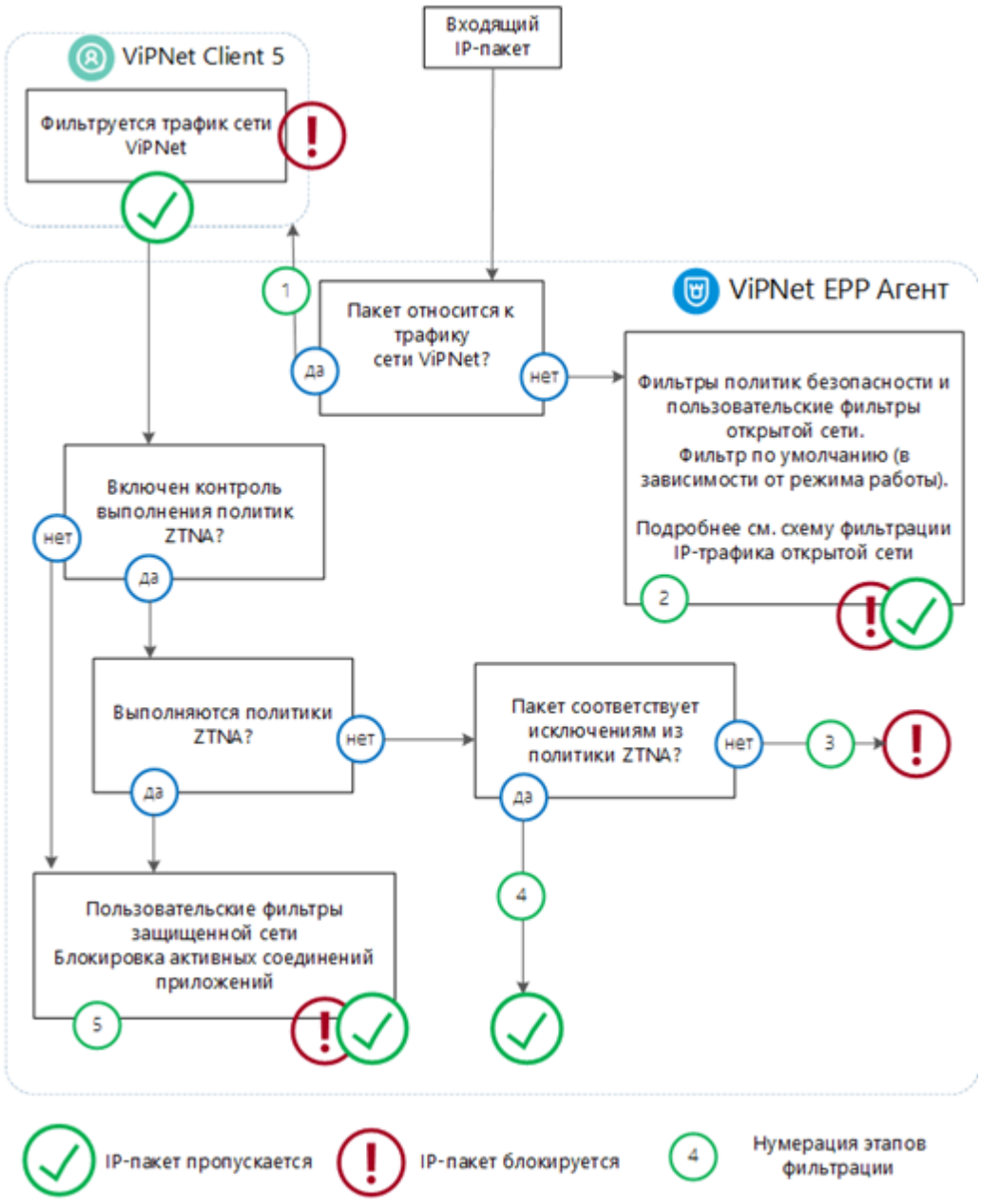


Рисунок 5. Фильтрация входящего трафика

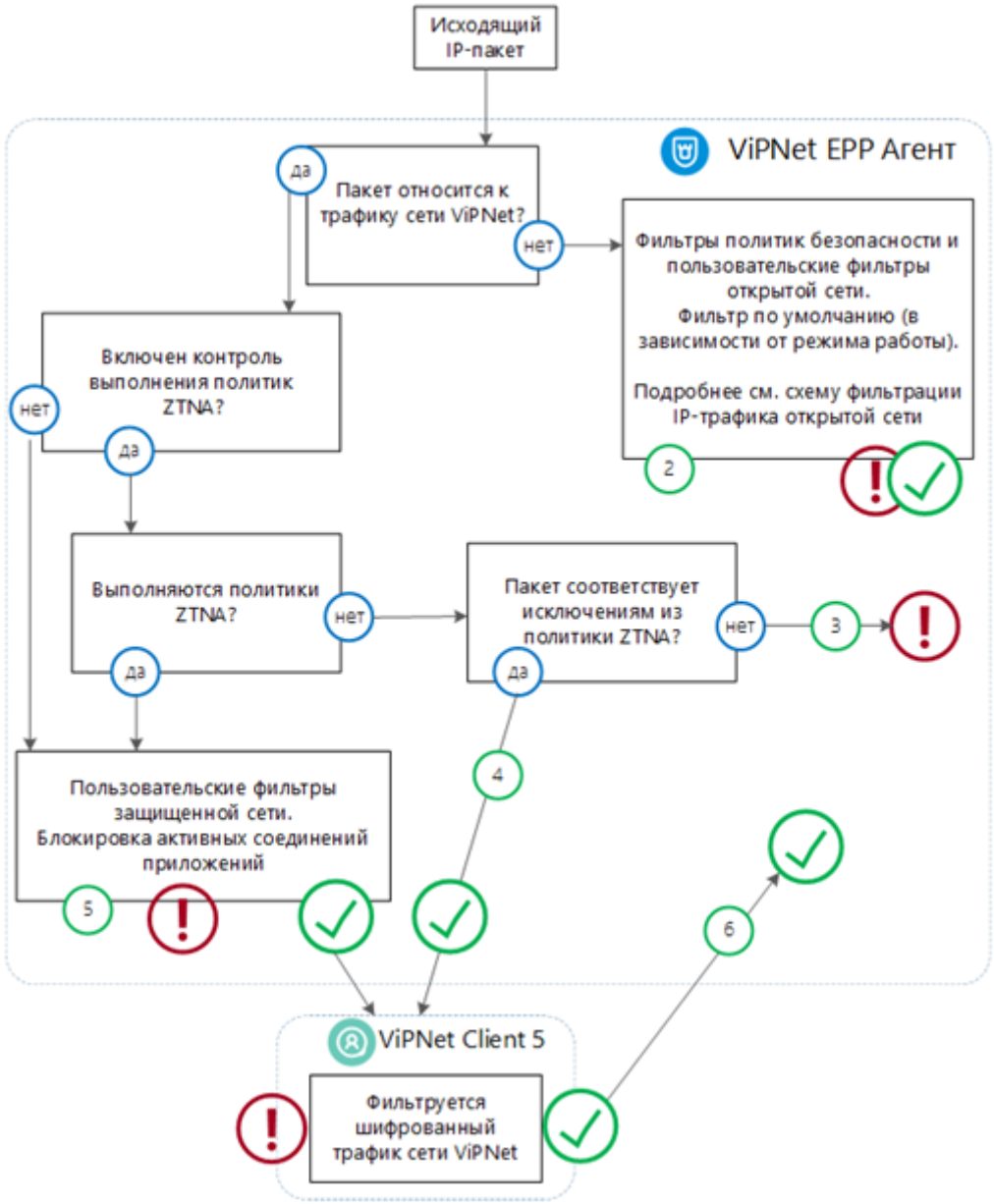


Рисунок 6. Фильтрация исходящего трафика

На каждом этапе фильтрации трафика в журнале трафика регистрируются события с названиями сработавших фильтров. При пропуске служебного трафика регистрируется событие с системным фильтром **Служебный трафик EndPoint**. Системные фильтры не отображаются в списке сетевых фильтров ViPNet EPP Агент.

Номера этапов фильтрации (на схемах выше) и фильтры, которые могут сработать на каждом этапе:

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

2 Сетевой фильтр из списка фильтров для режимов работы.

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

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

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.

Контроль приложений

Контроль приложений ViPNet EPP Агент for Windows позволяет на защищаемом узле:

- управлять установкой, запуском и активностью приложений;
- контролировать взаимодействие приложений с объектами ОС Windows (файлами, реестром, процессами) и запуск приложений с определенными параметрами командной строки;
- обнаруживать признаки вредоносности в исполняемых файлах в ОС Windows с помощью обучаемой модели AntiMalware (см. Обнаружение признаков вредоносности в исполняемых файлах с помощью сканирования AntiMalware и блокировка опасных файлов).

Контроль приложений ViPNet EPP Агент реализован модулем Application Control.

Установка, запуск и активность приложения настраивается в правиле запуска и зависит от его нахождения в списках контроля приложений (черном или белом) и заданного режима работы контроля приложений ViPNet EPP Агент:

- Запуск приложений из правил запуска черного списка запрещен.
- Запуск приложений из правил запуска белого списка разрешен, а их активность может быть ограничена правилами доступа.
- Запуск приложений, не входящих в черный и белый списки, определяется режимом работы.

Правила доступа определяют взаимодействие приложения из правила запуска с объектами ОС Windows и устанавливают:

- Для файлов:
  - Оповещение (регистрация срабатывания правила в журнале событий).
  - Разрешения на операции с файлом (создание, чтение, изменение, удаление).
- Для ветвей реестра:
  - Оповещение (регистрация срабатывания правила в журнале событий).
  - Разрешения на операции с ветвями реестра (создание, чтение, изменение, удаление).
- Для процессов:
  - Оповещение (регистрация срабатывания правила в журнале событий).
  - Разрешение на запуск процессов (разрешить или запретить).
- Для параметров командной строки:
  - Оповещение (регистрация срабатывания правила в журнале событий).
  - Разрешение на запуск приложения (разрешить или запретить) с указанными параметрами из командных интерпретаторов ОС Windows — PowerShell или cmd.

Белые и черные списки используются двух типов:

- **Глобальные** — создаются в ViPNet EPP Сервер и действуют в пределах одной базы правил (см. База правил (политика безопасности)). Глобальные черный и белый списки передаются на защищаемые узлы в составе базы правил. Изменить правила в глобальном списке на защищаемом узле невозможно. В автономном ViPNet EPP Агент списки этого типа не отображаются.
- **Пользовательские** — создаются и действуют локально на защищаемом узле. Обновление базы правил на защищаемом узле не изменяет правила в пользовательских списках.

Глобальные списки имеют приоритет над пользовательскими. Порядок применения списков контроля приложений: **Глобальный черный список** > **Пользовательский черный список** > **Глобальный белый список** > **Пользовательский белый список**.

Правила контроля приложений глобального и пользовательского списков могут входить в группы:

- **Доверенные** — предустановленная группа белого списка без возможности удаления. Активность приложений из этой группы не ограничена.

  При установке ViPNet EPP Агент в пользовательском белом списке в группе **Доверенные** автоматически создаются разрешающие правила для всех приложений, имеющихся на защищаемом узле. Правила для приложений, установленных на защищаемом узле нестандартным способом, не включаются в группу **Доверенные** автоматически. Чтобы активность таких приложений не ограничивалась, создайте для них разрешающее правило запуска вручную.

  Правила из группы **Доверенные** пользовательского белого списка могут быть перемещены в пользовательские группы или пользовательский черный список.
- **Пользовательские** — предустановленные группы белого списка **Частичное доверие** и **Слабое доверие**, а также группы, созданные пользователями. Группы можно удалять. Активность приложений из правил этих групп зависит от настройки правил доступа.

  Для вышеперечисленных групп приложений установлены правила доступа по умолчанию. Правила доступа по умолчанию для группы **Доверенные** изменить невозможно. Правила доступа по умолчанию пользовательских групп и правил запуска приложений в этих группах можно изменить.
- **Запрещенные** — приложение, добавленное при создании правила в эту группу, попадет в черный список, где активность приложения полностью запрещена.

Изменение параметров запуска и активности работающего приложения (добавление в список, изменение правил доступа) вступает в силу только после перезапуска этого приложения.

Режимы работы контроля приложений ViPNet EPP Агент:

- **Блокировать** — запуск приложений, не входящих в белый и черный списки, блокируется. Попытки запуска приложений фиксируются в журнале.
- **Разрешать** — запуск приложений, не входящих в белый и черный списки, разрешен.
- **Отключено** — контроль приложений отключен и не влияет на запуск приложений.

Режим работы передается в составе базы правил (см. База правил (политика безопасности)) (политики безопасности). Для учета особенностей запуска приложений на защищаемом узле

режим работы контроля приложений ViPNet EPP Агент можно изменить локально. Обновление базы правил может изменить этот режим.

Схема работы контроля приложений приведена на рисунке ниже.

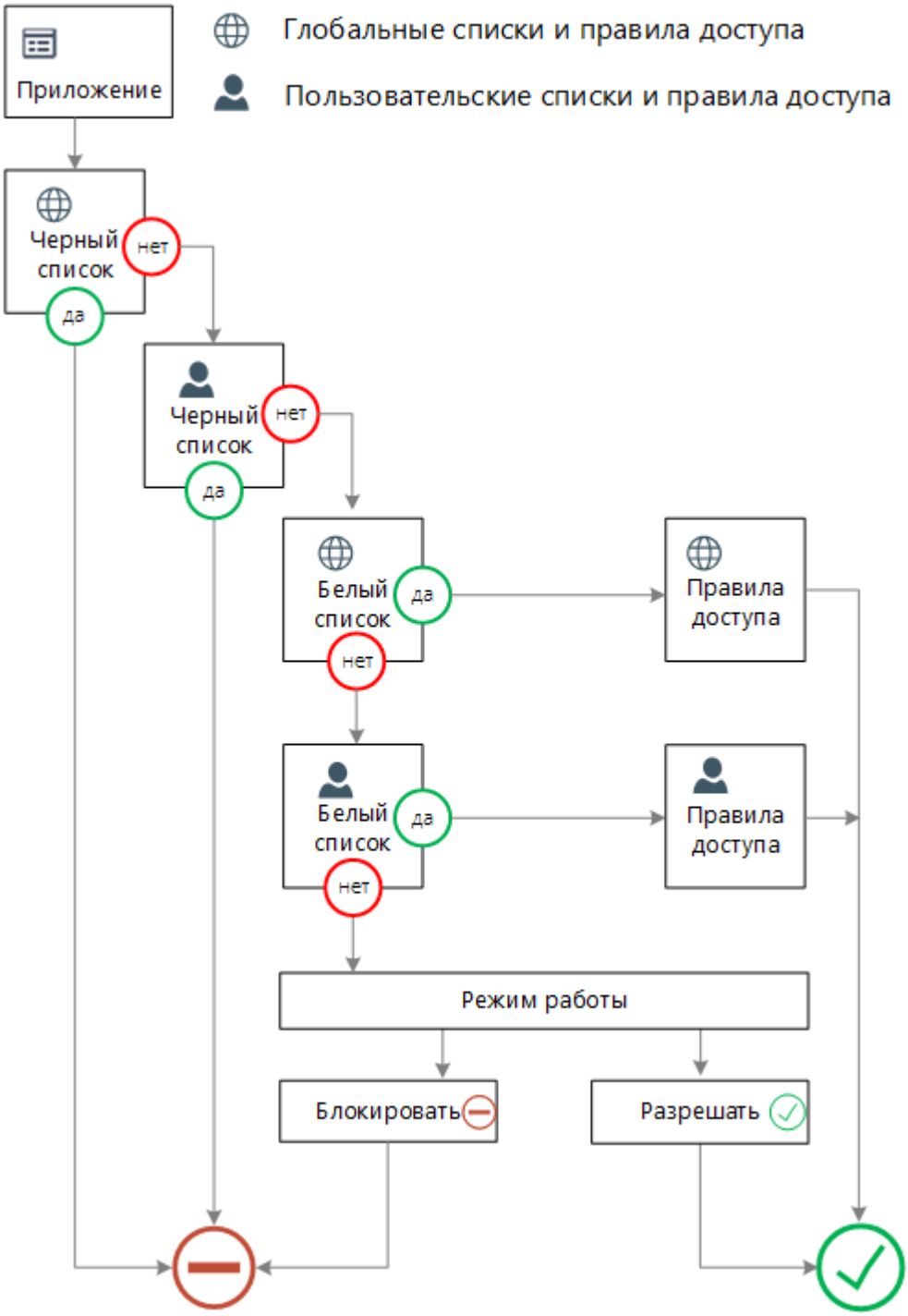


Рисунок 7. Схема работы контроля приложений ViPNet EPP Агент

Обнаружение признаков вредоносности в исполняемых файлах с помощью сканирования AntiMalware и блокировка опасных файлов



Внимание! В текущей версии ViPNet EPP данная функция реализована для экспериментальной эксплуатации.

Для поиска признаков вредоносного ПО в исполняемых файлах на защищаемых узлах с ViPNet EPP Агент for Windows используется механизм сканирования AntiMalware. Сканирование выполняется на основе модели AntiMalware, построенной с помощью машинного обучения. Параметры работы модели AntiMalware входят в состав базы правил и обновляются вместе с ней.

При сканировании проверяются все или выбранные файлы *.exe и *.dll и в результате для каждого файла вычисляется уровень опасности. Уровень опасности отображает вероятность того, что проверенный объект является вредоносным ПО. Уровень опасности может принимать значения от 0 (низкий уровень опасности) до 1 (критический уровень опасности). По умолчанию вероятности для уровней опасности распределены следующим образом:

- 0-0,39 — низкий уровень опасности. Проверенный объект с большой долей вероятности не является вредоносным ПО.
- 0,40-0,69 — средний уровень.
- 0,7-0,94 — высокий уровень.
- 0,95-1 — критический уровень. Проверенный объект с большой долей вероятности является вредоносным ПО.

По результатам проверки формируется отчет и на защищаемых узлах можно заблокировать потенциально опасные исполняемые файлы, добавив их в пользовательский черный список контроля приложений (см. Просмотр и обработка результатов сканирования AntiMalware).

Запуск сканирования доступен в ViPNet EPP Сервер (см. Сканирование AntiMalware) или непосредственно на защищаемом узле в ViPNet EPP Агент (см. Сканирование AntiMalware).

В ViPNet EPP Сервер доступна настройка автоматического сканирования по расписанию, а также настройка уровней опасности и автоматической блокировки потенциально опасных исполняемых файлов. Эти настройки доступны также в автономном ViPNet EPP Агент.

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 базы правил (см. База правил (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 и локальные вторжения, выявленные правилами сигнатурного анализа, с помощью правил предотвращения вторжений.
- Применение правил веб-фильтрации для блокирования доступа к вредоносным сайтам (см. Блокировка доступа к вредоносным веб-ресурсам), входящие в состав базы правил. Реализовано в модуле HIPS.
- Применение политик аудита Windows (см. Настройка политик аудита). Определяют, какие типы событий ОС Windows должна записывать в журнал безопасности Windows на защищаемом узле.

  Правила обнаружения и предотвращения вторжений, правила веб-фильтрации и политики аудита настраиваются в ViPNet EPP Сервер и передаются в ViPNet EPP Агент защищаемого узла централизованно в составе базы правил (политики безопасности). В автономном ViPNet EPP Агент настройки выполняются локально.
- Применение методов обнаружения аномалий:
  - С помощью критериев (см. Обнаружение аномалий с помощью критериев).
  - С помощью поведенческого анализа (см. Обнаружение аномалий с помощью поведенческого анализа), реализованного в модуле Behavior Analytics. Функция недоступна для защищаемых узлов с ViPNet EPP Linux Агент и автономных ViPNet EPP Агент.

  Критерии обнаружения аномалий и поведенческий анализ настраиваются в ViPNet EPP Сервер и передаются в ViPNet EPP Агент защищаемого узла централизованно. В автономном ViPNet EPP Агент настройки критериев обнаружения аномалий выполняются локально.

Совместное применение сигнатурного анализа, критериев обнаружения аномалий и поведенческого анализа 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 HIDS 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 сетевой атаки (правила HIPS), атака будет заблокирована этим правилом (см. Предотвращение сетевых вторжений).

Пример обнаружения атаки на сетевом уровне приведен на рисунке ниже:

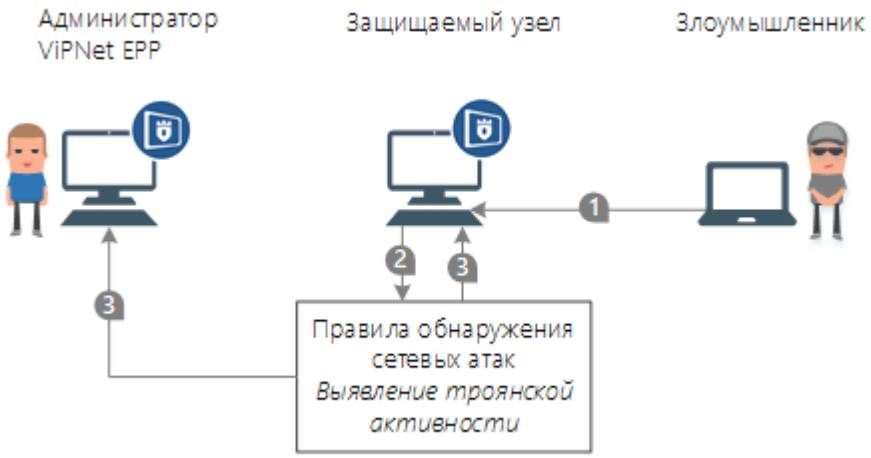


Рисунок 8. Обнаружение атаки на сетевом уровне

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 сетевой атаки (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 локальных правил. К локальным правилам относятся, например, правила анализа событий в журналах событий ОС Windows, 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 HIDS (см. Настройка правил HIDS). Для защищаемых узлов с ОС Windows типы событий, которые будут записываться в журналы событий ОС Windows, задаются в ViPNet EPP политиками аудита (см. Настройка политик аудита). 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 реестра, файловой системы, попытки входа в систему, управление учетными записями (например, строки в журналах событий ОС или изменения в параметре реестра). 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.

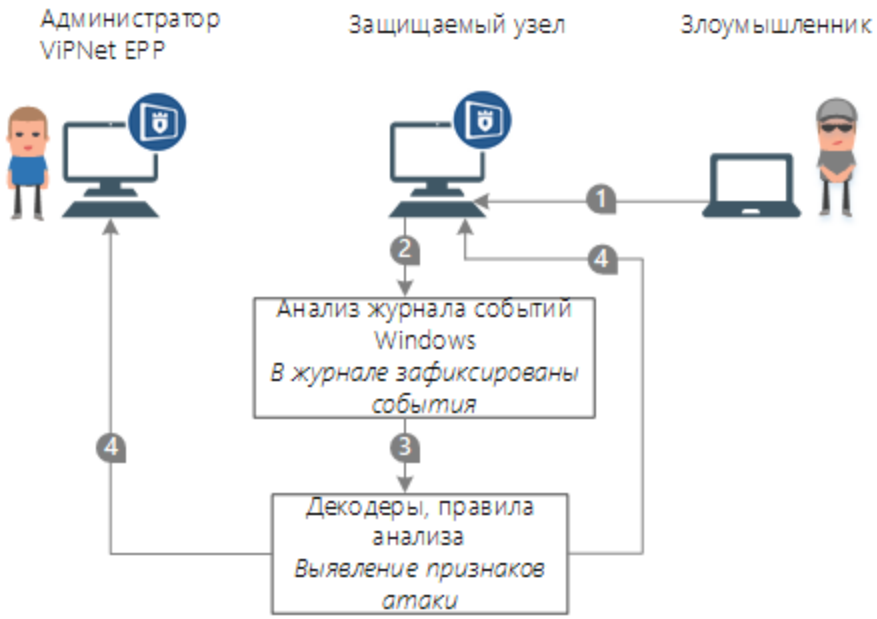


Рисунок 9. Обнаружение атаки на локальном уровне

1 Злоумышленник получил удаленный доступ к защищаемому узлу и изменил критически важный системный файл.

2 ViPNet EPP Агент выполнена проверка, что в журнале событий ОС Windows 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 HIDS ViPNet EPP Агент анализирует трафик, а также изменения на защищаемом узле. При срабатывании правил 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.

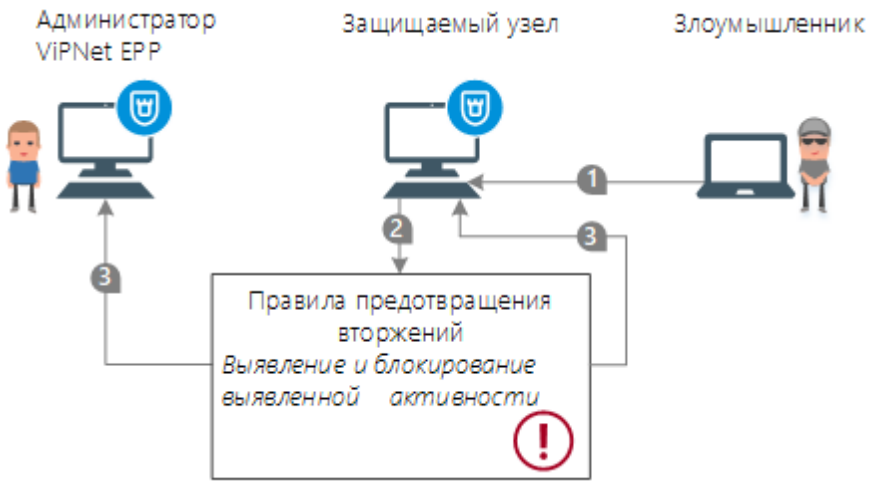


Рисунок 10. Предотвращение сетевой атаки

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.
- **Базовый** (**Оптимальный**) — используется оптимальный набор правил, обеспечивающий защиту в большинстве случаев.

- **Минимальный** — используется минимальный набор правил, защищающих от наиболее критичных атак.
- **Отключено** — предотвращение вторжений выключено.

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

Обнаружение и предотвращение бесфайловых атак

Функция недоступна для защищаемых узлов с ViPNet EPP Агент for Linux.

ViPNet EPP позволяет обнаруживать бесфайловые атаки на защищаемых узлах с ОС Windows, а также предотвращать некоторые из таких атак:

- Могут быть обнаружены бесфайловые атаки, выполняемые с помощью следующих методов по классификации MITRE ATT&CK®:
  - Credential API Hooking — замена стартового кода DLL-модуля для перехвата API-функции и подмены оригинального обработчика.
  - Process Hollowing — внедрение вредоносного кода в приостановленный процесс для обхода защиты процесса; применяется для выполнения вредоносного кода в адресном пространстве легитимного процесса.
  - Process Doppelganging — внедрение вредоносного кода в процесс с использованием отката NTFS-транзакции для обхода защиты процесса или повышения привилегий; применяется для выполнения вредоносного кода в адресном пространстве легитимного процесса.
  - Dynamic-link Library Injection — внедрение DLL-модуля в процесс для обхода защиты процесса или повышения привилегий; применяется для выполнения вредоносного кода в адресном пространстве легитимного процесса.
  - Portable Executable Injection — внедрение PE-файла в процесс для обхода защиты процесса или повышения привилегий; применяется для выполнения вредоносного кода в адресном пространстве легитимного процесса.
  - Keylogging — внедрение DLL-модуля в процесс для перехвата API-функций обработки данных нажатия клавиш клавиатуры, мыши и т.д.

  Бесфайловые атаки выявляются правилами HIDS, а именно правилами обнаружения бесфайловых атак (см. Обнаружение бесфайловых атак) при их включении.
- Могут быть предотвращены:
  - Бесфайловые атаки, относящиеся к методу Keylogging и проводимые злоумышленником с помощью вызова функции ОС Windows `SetWindowsHookEx`. Для проведения такой атаки

используется механизм перехвата событий (hook) для получения конфиденциальной информации с помощью внедренных в легитимные процессы вредоносных dll-модулей. Для выявления и дальнейшего блокирования таких атак необходимо настроить локальные правила предотвращения вторжений HIPS — правила для бесфайловых атак (см. Блокирование бесфайловых атак типа Keylogging).

Отслеживаются следующие типы hook: события клавиатуры, мыши, оконные сообщения (элементов управления, меню и т.д.) и прочие системные сообщения.

Например, злоумышленник запустил на защищаемом узле клавиатурный шпион (кейлогер) для получения конфиденциальной информации путем перехвата и записи всех действий пользователя с клавиатурой. В ViPNet EPP при анализе данных с помощью правил HIDS обнаружения бесфайловых атак сработало одно из правил, выявившее активность кейлогера — бесфайловую атаку по методу Keylogging. Администратор ViPNet EPP может заблокировать активность кейлогера — создать блокирующее правило HIPS для бесфайловых атак, указав в нем в качестве типа отслеживаемых hook события клавиатуры и данные об атаке из зарегистрированного события в результате сработавшего правила HIDS. Работа кейлогера будет заблокирована.

Также с использованием правил HIPS для бесфайловых атак можно сначала выявить все приложения (процессы), которые используют механизм перехвата событий (hook), а затем разрешить известные и полезные приложения и запретить все остальные для предотвращения утечки конфиденциальной информации.

- Бесфайловые атаки, относящихся к методам Process Hollowing и Process Doppelganging. Для выявления и блокирования этих атак необходимо включить в локальных правилах предотвращения вторжений HIPS — Предотвращение атак типа Hollowing и Doppelganging (см. Блокирование бесфайловых атак типа Hollowing и Doppelganging).
- Бесфайловые атаки, связанные с получением адресов функций или структур в модулях ядра ОС Windows (таких как `ntoskrnl.exe`, `hal.dll`, `win32k.sys`) из процессов прикладного уровня. Для выявления и блокирования этих атак необходимо включить в локальных правилах предотвращения вторжений HIPS — Предотвращение получения адресов функций в модулях ядра Windows (см. Блокирование бесфайловых атак с целью получения адресов функций в модулях ядра ОС Windows).

Блокировка доступа к вредоносным веб-ресурсам

Функция недоступна для защищаемых узлов с ViPNet EPP Агент for Linux.

ViPNet EPP Агент позволяет на защищаемых узлах с ОС Windows блокировать доступ к вредоносным сайтам — веб-ресурсам с вредоносным, фишинговым и спам содержимым. Для этого в ViPNet EPP Агент применяются веб-фильтры.

Кроме блокирования доступа к вредоносным сайтам на защищаемых узлах, веб-фильтры могут быть настроены, например:

- для разграничения доступа сотрудников разных отделов к веб-ресурсам;
- для оптимизации времени сотрудников за счет запрещения нецелевых сайтов.

При любой попытке получить доступ к сайту с защищаемого узла, доступ к которому заблокирован веб-фильтрами, отобразится предупреждение о блокировке.

Веб-фильтры настраиваются в ViPNet EPP Сервер и отправляются ViPNet EPP Агент в составе базы правил. В автономном ViPNet EPP Агент веб-фильтры загружаются из базы правил и настраиваются локально. Веб-фильтры разделены на категории:

- **Фильтры политик безопасности** — определяют параметры фильтрации для различных видов вредоносных сайтов. По умолчанию содержат следующие блокирующие веб-фильтры:
  - malware — содержит адреса веб-ресурсов, используемых различным вредоносным ПО;
  - phishing — содержит адреса фишинговых веб-ресурсов;
  - spam — содержит адреса веб-ресурсов для рассылки спама.

  Адреса веб-ресурсов заданы в виде IP-адресов, доменных имен и URL.

  Администратор может изменить веб-фильтры по умолчанию или добавить свои.
- **Фильтры по умолчанию** — содержит фильтр **Прочие сайты**, определяющий возможность доступа к веб-ресурсам, которых нет в фильтрах политик безопасности. По умолчанию доступ разрешен. Администратор может изменить действие фильтра по умолчанию и заблокировать все остальные веб-ресурсы. Удалить **Прочие сайты** нельзя.

Фильтрация выполняется по адресам веб-ресурсов, заданным в веб-фильтрах. Фильтр может разрешать или запрещать доступ к веб-ресурсу. При срабатывании фильтра доступ к веб-ресурсу блокируется либо разрешается, в зависимости от настройки.

На защищаемых узлах с ViPNet EPP Агент под управлением сервера изменение веб-фильтров недоступно.

Для работы веб-фильтров на защищаемых узлах модуль защиты **Обнаружение и предотвращение вторжений** должен быть включен — установлен один из режимов работы, кроме **Отключен** (см. Выбор режимов работы модулей защиты).

Веб-фильтры применяются последовательно до первого срабатывания. Проверка доступа к веб-ресурсам выполняется для любых источников обращений с защищаемого узла к веб-ресурсам, будь это, например, обращения пользователя, системы или приложений. По умолчанию контролируется HTTP и HTTPS-трафик. Для контроля HTTPS-трафика в правилах HIDS включена TLS-инспекция.

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.

Обнаружение аномалий с помощью поведенческого анализа



Внимание! В текущей версии ViPNet EPP данная функция реализована для экспериментальной эксплуатации и недоступна для защищаемых узлов с автономным ViPNet EPP Агент.

Поведенческий анализ позволяет обнаруживать аномалии определенных типов (см. Типы аномалий, обнаруживаемые с помощью поведенческого анализа). Процесс обнаружения аномалий состоит из трех взаимосвязанных стадий:

1. Первичное обучение — построение модели нормальной активности защищаемого узла с помощью машинного обучения.
2. Обнаружение — применение модели нормальной активности защищаемого узла для обнаружения аномалий.
3. Повторное обучение — построение новой модели нормальной активности защищаемого узла, выполняемое в двух случаях:
   - При выявлении администратором ViPNet EPP ложных аномалий среди обнаруженных.
   - Один раз в 30 дней для уточнения модели нормальной активности защищаемого узла.

Поведенческий анализ ViPNet EPP Агент for Windows реализован модулем Behavior Analytics.

На первой стадии, по завершении периода накопления событий информационной безопасности для первичного обучения, равного 30 дням, строится модель нормальной активности и вычисляются пороговые значения аномалий IRE_{th} каждого типа. Обучение проводится для каждого защищаемого узла, поэтому модели нормальной активности и пороговые значения IRE_{th} для разных защищаемых узлов различаются.

На второй стадии выполняется обнаружение аномалий — для новых событий информационной безопасности вычисляются текущие значения аномалий IRE, которые сравниваются с пороговыми значениями аномалий IRE_{th} данного типа. При превышении IRE над IRE_{th} регистрируется аномалия.

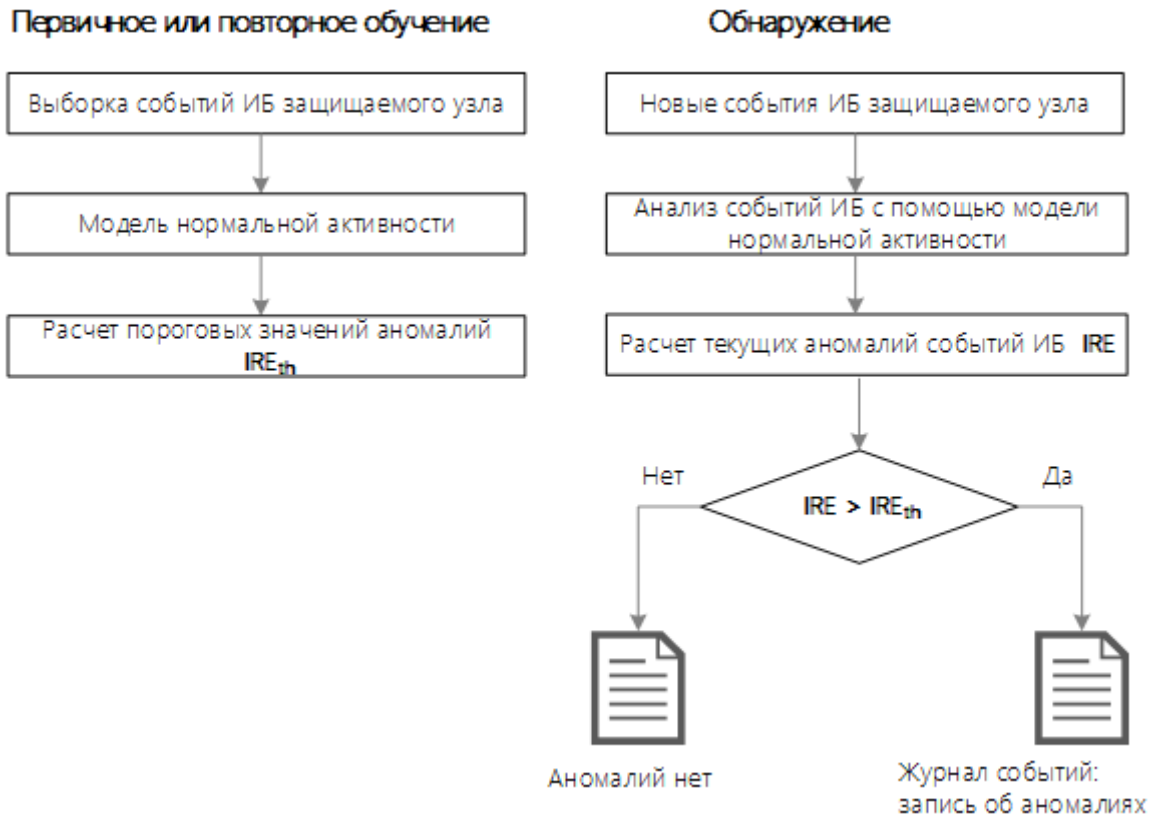


Рисунок 11. Стадии процесса обнаружения аномалий с помощью поведенческого анализа

В зависимости от степени превышения IRE над IRE_{th} в журнале ViPNet EPP Сервер регистрируется аномалия — событие модуля Behavior Analytics с определенным уровнем важности:

- **Критические**.
- **Опасные**.
- **Важные**.
- **Информационные**.

На третьей стадии администратор ViPNet EPP просматривает события модуля Behavior Analytics в журнале ViPNet EPP Сервер, определяет среди них ложные аномалии и запускает повторное обучение на защищаемых узлах, где обнаружены ложные аномалии. На время повторного обучения обнаружение аномалий выполняется с помощью модели нормальной активности защищаемого узла, построенной ранее. После завершения повторного обучения обнаружение аномалий выполняется с помощью новой модели нормальной активности.

На стадиях обучения (первичного и повторного) статус обучения модуля Behavior Analytics на защищаемом узле может принимать следующие значения:

- **Недостаточно данных для обучения** — первичное обучение недоступно, так как не завершился период накопления событий.
- **Требуется обучение** — завершился период накопления событий для первичного обучения или с момента последнего обучения прошло более 30 дней; администратор ViPNet EPP может запустить обучение.
- **Идет обучение** — идет первичное или повторное обучение.
- **Ошибка обучения** — первичное или повторное обучение прервано.
- **Обучен** – первичное или повторное обучение завершено.

База правил (политика безопасности)

База правил, на основе которой ViPNet EPP Агент обнаруживает и предотвращает угрозы информационной безопасности на защищаемых узлах, формируется специалистами ИнфоТеКС и регулярно обновляется на сервере обновлений. В ViPNet EPP база правил может быть дополнительно настроена и представляет собой политику безопасности — набор глобальных настроек и правил работы модулей защиты ViPNet EPP:

- Персональный межсетевой экран:
  - Фильтры политик безопасности.
  - Справочники протоколов, расписаний, адресов и сетей.
  - Режим работы персонального межсетевого экрана.
- Контроль приложений:
  - Списки контроля приложений (белый и черный).
  - Правила доступа приложений к объектам ОС Windows.
  - Режим работы контроля приложений.
  - Параметры модели AntiMalware для обнаружения признаков вредоносности в исполняемых файлах в ОС Windows.
- Обнаружение и предотвращение вторжений:
  - Правила обнаружения вторжений (правила HIDS).
  - Правила предотвращения вторжений (правила HIPS).
  - Режим работы обнаружения и предотвращения вторжений.
  - Веб-фильтры.
  - Политики аудита Windows.
- Сетевой доступ с нулевым доверием (ZTNA).

Возможности работы с базой правил (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. Для учета особенностей защиты, в базу правил администратором ViPNet EPP Сервер могут вноситься изменения, в результате чего будет создана новая версия базы правил (политики безопасности). Чтобы после загрузки с сервера обновлений новой базы правил, внесенные администратором изменения не были потеряны, доступен экспорт части глобальных настроек в избранное и последующий импорт в новую базу правил. В избранное

можно добавить: фильтры политик безопасности, правила доступа приложений, веб-фильтры и правила ZTNA.

База правил 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 база правил, в ViPNet EPP Агент этого узла защита отключена.

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

- Персональный межсетевой экран:
  - Пользовательские фильтры.
  - Справочники протоколов, расписаний, адресов и сетей для пользовательских фильтров.
  - Режим работы персонального межсетевого экрана.
- Контроль приложений:
  - Списки контроля приложений (белый и черный).
  - Правила доступа приложений к объектам ОС Windows.
  - Режим работы контроля приложений.
- Обнаружения и предотвращения вторжений:
  - Пользовательские правила HIPS для бесфайловых атак.
  - Режим работы обнаружения и предотвращения вторжений.

При назначении новой базы правил (или новой версии базы правил) пользовательские настройки, добавленные в ViPNet EPP Агент защищаемого узла, сохраняются.

- 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 (аналогично ViPNet EPP Агент под управлением ViPNet EPP Сервер, 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. Требует принятия экстренных мер.
- **Опасное** — событие средней степени опасности; может привести к сбоям в работе защищаемого узла. Требует решения проблемы в рабочем порядке.
- **Важное** — событие может косвенно свидетельствовать о вредоносной активности на защищаемом узле. Требует 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. Кратко полномочия пользователей в соответствии с назначенной ролью приведены в таблице ниже, подробнее — в приложении (см. Полномочия пользователей).

Таблица 2. Полномочия пользователей ViPNet EPP

Роль	Полномочия пользователей
Администратор ViPNet EPP	Роль назначается учетной записи, созданной в ViPNet EPP Сервер. Обеспечивает доступ ко всем функциям ViPNet EPP Сервер и ViPNet EPP Агент.
Администратор агента	Роль назначается учетной записи, созданной в ViPNet EPP Агент. Обеспечивает доступ ко всем функциям ViPNet EPP Агент.
Аудитор ViPNet EPP	Роль назначается учетной записи, созданной в ViPNet EPP Сервер. Доступен просмотр: • инфопанели; • журналов событий и аудита; • базы правил и лицензии ViPNet EPP Сервер и ViPNet EPP Агент. Роль обеспечивает доступ к ViPNet EPP Сервер и ViPNet EPP Агент
Аудитор агента	Роль назначается учетной записи, созданной в ViPNet EPP Агент. Доступны: • выбор режимов модулей защиты; • просмотр инфопанели; • просмотр критериев обнаружения аномалий (только в автономном ViPNet EPP Агент); • просмотр журналов событий и журнала аудита; • просмотр списков правил модулей защиты; • просмотр статуса ZTNA (только в ViPNet EPP Агент под управлением сервера); • просмотр результатов самотестирования; • просмотр информации о лицензии и о ViPNet EPP Агент.
Пользователь сервера	Роль назначается учетной записи, созданной в ViPNet EPP Сервер. Доступен просмотр: • журнала событий; • базы правил и лицензии ViPNet EPP Сервер.
Пользователь агента	Роль назначается учетной записи, созданной в ViPNet EPP Агент. Доступны: • просмотр инфопанели;

Роль	Полномочия пользователей
	• настройка оповещений по событиям безопасности; • просмотр журнала событий; • просмотр ZTNA (только в ViPNet EPP Агент под управлением сервера).



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.

Управление доверенной загрузкой

ViPNet EPP позволяет управлять программным комплексом «Программный модуль доверенной загрузки ViPNet SafeBoot» (далее — ViPNet SafeBoot), установленным на защищаемых узлах. Подробнее о возможностях ViPNet SafeBoot см. в документации к ViPNet SafeBoot. Для управления лицензия ViPNet EPP (см. Лицензирование) должна содержать разрешение на использование модуля SafeBootMC, а также максимальное количество доступных для управления узлов.

Версии ViPNet SafeBoot, доступные для управления, см. в разделе Совместимость ViPNet EPP со сторонним программным обеспечением.

Внимание! Из ViPNet EPP нельзя управлять ViPNet SafeBoot, работающим в бездисковом режиме.

В ViPNet EPP доступны следующие действия по управлению ViPNet SafeBoot на защищаемых узлах:

- Управление лицензиями ViPNet SafeBoot — распределение, отправка и активация лицензий.
- Управление учетными записями пользователей.

Примечание. В ViPNet EPP добавление учетных записей пользователей возможно только со способом аутентификации по паролю. Также недоступны:

- Настройка режима единого входа в ViPNet SafeBoot и в ОС — Single Sign-On.
- Смена типа аутентификации пользователя.
- Изменение пароля для учетной записи с типом аутентификации, отличным от аутентификации по паролю.
- Изменение минимальной и максимальной длины пароля.
- Изменение количества неудачных попыток ввода пароля.

- Управление корневыми сертификатами и списками отозванных сертификатов (далее — CRL).
- Обновление ViPNet SafeBoot.
- Выгрузка журнала аудита ViPNet SafeBoot.

Отслеживание работы антивирусов

ViPNet EPP позволяет отслеживать работу антивирусного программного обеспечения Kaspersky Endpoint Security или Dr.Web Enterprise Security Suite (см. Совместимость ViPNet EPP 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 (см. Отслеживание событий обнаружения вирусов).



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 системы). 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 межсетевого 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 системы) 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 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 64

Порядок ввода в эксплуатацию ViPNet EPP с автономными агентами 66

Установка, обновление, восстановление и удаление 67

Порядок ввода в эксплуатацию ViPNet EPP с агентами под управлением сервера

Таблица 3. Последовательность действий по вводу в эксплуатацию

	Действие	Ссылка
☐	Подготовьтесь к установке ViPNet EPP	Подготовка к установке ViPNet EPP
☐	Установите ViPNet EPP Сервер. Вместе с ViPNet EPP Сервер будет установлена ViPNet EPP Серверная консоль.	Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль
☐	Если планируется подключаться к ViPNet EPP Сервер с разных компьютеров, установите на них ViPNet EPP Серверная консоль (без компонента ViPNet EPP Сервер).	Установка ViPNet EPP Серверная консоль
☐	Установите ViPNet EPP Агент на компьютеры корпоративной сети с ОС Windows, при установке выберите способ работы под управлением сервера. Установите одним из способов: • С помощью групповых политик Active Directory • Вручную Для завершения установки настройте сетевой сенсор ViPNet EPP Агент	 Установка ViPNet EPP Агент с помощью групповых политик Active Directory Установка ViPNet EPP Агент вручную Установка ViPNet EPP Агент
☐	Если требуется, установите ViPNet EPP Агент на компьютеры корпоративной сети с ОС GNU/Linux и выберите способ работы под управлением сервера	См. документ «ViPNet EPP for Linux. Руководство администратора» раздел «Установка ViPNet EPP Агент»
☐	Подключитесь к ViPNet EPP Сервер, установите и активируйте лицензию	Подключение к ViPNet EPP Сервер Установка и активация лицензии
☐	Подключите защищаемые узлы к ViPNet EPP Сервер	Подключение защищаемых узлов
☐	Настройте автоматическую загрузку обновлений базы правил с сервера обновлений или загрузите вручную	Загрузка обновлений баз правил на ViPNet EPP Сервер

	Действие	Ссылка
☐	Настройте базу правил и назначьте ее группе защищаемых узлов	Настройка базы правил

Порядок ввода в эксплуатацию ViPNet EPP с автономными агентами

Таблица 4. Последовательность действий по вводу в эксплуатацию

	Действие	Ссылка
☐	Подготовьтесь к установке ViPNet EPP	Подготовка к установке ViPNet EPP
☐	Установите ViPNet EPP Агент на компьютеры корпоративной сети с ОС Windows, при установке выберите способ работы без управления сервера (автономный). Установите одним из способов:	
	• С помощью групповых политик Active Directory	Установка ViPNet EPP Агент с помощью групповых политик Active Directory
	• Вручную	Установка ViPNet EPP Агент вручную
	Для завершения установки настройте сетевой сенсор ViPNet EPP Агент	Установка ViPNet EPP Агент
☐	На каждый агент установите и активируйте лицензию	Подключение к ViPNet EPP Агент Установка и активация лицензии
☐	На каждый агент загрузите базу правил	Загрузка и обновление базы правил
☐	На каждом агенте настройте параметры работы или оставьте параметры по умолчанию	Просмотр и настройка параметров работы
☐	На каждом агенте настройте модули защиты	Управление фильтрацией трафика Управление запуском и активностью приложений Управление обнаружением и предотвращением вторжений Настройка критериев обнаружения аномалий

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:

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

- ✱ Требования к установке ViPNet EPP Сервер.
- ✱ Требования к установке ViPNet EPP Серверная консоль.
- Требования к установке ViPNet EPP Агент.



Совет. В целях безопасности рекомендуем на компьютерах, предназначенных для установки ViPNet EPP Сервер, использовать только учётные записи с правами администратора ОС Windows.

---

2 ✱ На компьютерах должны быть разрешены входящие и исходящие соединения по TCP-портам:

- 25010 — для связи ViPNet EPP Сервер и ViPNet EPP Агент.
- 25014 — для связи ViPNet EPP Сервер и ViPNet EPP Агент for Linux.
- 25001 — для связи ViPNet EPP Сервер и ViPNet EPP Серверная консоль.
- 443 — для доступа ViPNet EPP Сервер к серверу обновлений.

Список разрешенных портов можно посмотреть в **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности**.

3 ✱ Уточните IP-адрес (в формате IP v4) или доменное имя компьютера, предназначенного для установки ViPNet EPP Сервер. Этот параметр понадобится при установке ViPNet EPP Агент и ViPNet EPP Серверная консоль, если консоль будет устанавливаться отдельно от ViPNet EPP Сервер.

4 На компьютерах, где будет устанавливаться ViPNet EPP Агент:

4.1 Если используется сторонний межсетевой экран, выключите его.

4.2 Выключите межсетевой экран, встроенный в ОС.

Использование ViPNet EPP Агент одновременно с другими межсетевыми экранами может привести к конфликтам правил фильтрации.

5 Если на компьютерах установлены ViPNet Client версии 4.5 или ViPNet Personal Firewall версии 4.5, удалите их. Для работы в защищенной сети ViPNet совместно с ViPNet EPP можно использовать ViPNet Client 5 версии, совместимой с ViPNet EPP (см. Совместимость ViPNet EPP со сторонним программным обеспечением). Если ViPNet Client 5 уже установлен, удалять не нужно.

6 Если на компьютерах установлены компоненты ViPNet IDS HS (ViPNet IDS HS Сервер, ViPNet IDS HS Агент, ViPNet IDS HS Консоль управления):

6.1 При необходимости просмотра журнала событий ViPNet IDS HS Сервер за прошедший период создайте резервную копию конфигурации.

6.2 Удалите с компьютеров все компоненты ViPNet IDS HS.



Примечание. Чтобы позднее просмотреть журнал событий ViPNet IDS HS Сервер:

1 Установите ViPNet IDS HS Сервер на выделенный компьютер или виртуальную машину.

2 Переведите системное время компьютера или виртуальной машины на дату создания резервной копии конфигурации.

3 Восстановите конфигурацию ViPNet IDS HS Сервер из резервной копии.

7 Если на компьютере, где предполагается установка ViPNet EPP Сервер, установлен Kaspersky Endpoint Security (см. Совместимость ViPNet EPP со сторонним программным обеспечением), добавьте установочный файл ViPNet EPP Сервер и архив с базой правил в список исключений из проверки Kaspersky Endpoint Security.

Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль

При установке ViPNet EPP Сервер на компьютер также будет установлена ViPNet EPP Серверная консоль. Об установке только ViPNet EPP Серверная консоль см. раздел Установка ViPNet EPP Серверная консоль. Установить ViPNet EPP Сервер без ViPNet EPP Серверная консоль невозможно.

Чтобы установить ViPNet EPP Сервер и ViPNet EPP Серверная консоль:

1 Запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` и следуйте указаниям мастера установки.

Если произошел сбой установки, вы увидите сообщение об ошибке установки с указанием возможной причины. Устраните причины сбоя и запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` заново.

2 Ознакомьтесь с лицензионным соглашением. В случае согласия выберите **Я принимаю условия лицензионного соглашения**.

3 На странице **Компоненты продукта** проверьте, что выбраны все компоненты и нажмите **Далее**.

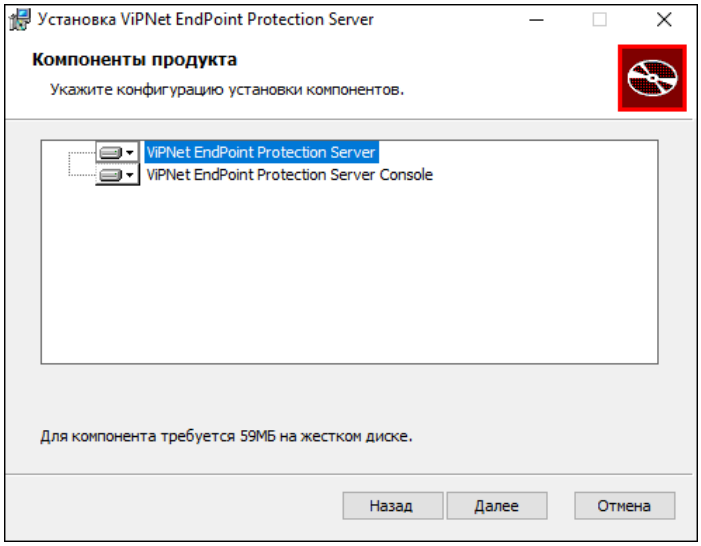


Рисунок 12. Устанавливаемые компоненты — ViPNet EPP Сервер и ViPNet EPP Серверная консоль

4 На странице **Настройка PostgreSQL** укажите параметры подключения к PostgreSQL:

- Порт подключения — оставьте значение по умолчанию (`5432`) или укажите другой порт.
- Имя учетной записи (по умолчанию — `postgres`) — укажите имя учетной записи `Superuser` в PostgreSQL.
- Пароль — введите пароль, который используется для учетной записи с правами `Superuser` в PostgreSQL.

5 Нажмите **Далее**.

6 Задайте параметры учетной записи для управления базой данных ViPNet EPP в PostgreSQL:

- Имя учетной записи `endpoint_protection` для управления базой данных — недоступно для изменения.
- Введите и подтвердите пароль учетной записи в соответствии с требованиями:
  - Длина пароля — от 8 до 31 символа.
  - Пароль должен содержать символы из каждой категории:
    - строчные буквы английского алфавита от `a` до `z`;
    - прописные буквы английского алфавита от `A` до `Z`;
    - цифры от `0` до `9`;
    - специальные символы `. ! @ # $ * () - _ + = ; : , / ? \ ` ~ [ ] { }`.
  - Пароль не должен содержать другие символы.

7 Нажмите **Далее**.

8 Измените папку установки ViPNet EPP Сервер или оставьте по умолчанию и нажмите **Далее**.



Внимание! Путь установки может содержать:

- прописные буквы латинского алфавита от `A` до `Z`;
- строчные буквы латинского алфавита от `a` до `z`;
- десятичные цифры от `0` до `9`;
- пробел;
- символы: `_-+.,:;$#@!~\(){}[]`. Символ `:` можно использовать только для указания диска.

При использовании других символов появится сообщение об ошибке и продолжение установки будет недоступно.

9 На странице **Все готово к установке ViPNet EndPoint Protection Server** нажмите **Установить**.

Дождитесь завершения установки.

10 На странице **Установка ViPNet EndPoint Protection Server завершена** нажмите **Готово**.

В результате на компьютер будет установлен ViPNet EPP Сервер и ViPNet EPP Серверная консоль. Учетная запись администратора ViPNet EPP по умолчанию: имя — `admin`, пароль — `admin`.



Внимание! Если вы установили ViPNet EPP Сервер или ViPNet EPP Серверная консоль на компьютер, где установлен ViPNet EPP Агент, добавьте правила запуска сервера и серверной консоли в пользовательский белый список ViPNet EPP Агент (см. Управление пользовательскими списками приложений). Иначе запуск сервера и серверной консоли может быть заблокирован.

Чтобы установить сервер ViPNet EPP Сервер на компьютер с уже установленной ViPNet EPP Серверная консоль:

1 Удалите ViPNet EPP Серверная консоль (см. Восстановление или удаление ViPNet EPP Сервер и ViPNet EPP Серверная консоль).

2 Перезапустите компьютер.

3 Установите ViPNet EPP Сервер и ViPNet EPP Серверная консоль согласно шагам предыдущего сценария.

Установка ViPNet EPP Серверная консоль

Если планируется подключаться к ViPNet EPP Сервер с разных компьютеров, установите ViPNet EPP Серверная консоль на эти компьютеры без компонента ViPNet EPP Сервер.

Установка ViPNet EPP Серверная консоль выполняется с помощью установочного файла ViPNet EPP Сервер.

Чтобы установить ViPNet EPP Серверная консоль:

1 Запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` и следуйте указаниям мастера установки.

   Если произошел сбой установки, вы увидите сообщение об ошибке установки с указанием возможной причины. Устраните причины сбоя и запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` заново.

2 Ознакомьтесь с лицензионным соглашением. В случае согласия выберите **Я принимаю условия лицензионного соглашения**.

3 На странице **Компоненты продукта** для компонента **ViPNet EndPoint Protection Server** в контекстном меню выберите **Компонент будет полностью недоступен** и нажмите **Далее**.

4 Измените папку установки ViPNet EPP Серверная консоль или оставьте по умолчанию и нажмите **Далее**.



Внимание! Требования к пути установки аналогичны требованиям при установке ViPNet EPP Сервер (см. Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль).

---

5 На странице **Все готово к установке ViPNet EndPoint Protection Server** нажмите **Установить**.

   Дождитесь завершения установки.

6 На странице **Установка ViPNet EndPoint Protection Server завершена** нажмите **Готово**.

В результате на компьютер будет установлена только ViPNet EPP Серверная консоль.

Установка ViPNet EPP Агент

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 папке `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection\Suricata\etc`.

   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:

```
net stop suricata & net start suricata
```



Примечание. После установки ViPNet EPP Агент брандмауэр Защитника Windows будет отключен — контроль и управление IP-трафиком защищаемого узла будет выполняться персональным межсетевым экраном ViPNet EPP Агент.

Установка ViPNet EPP Агент вручную

Чтобы установить ViPNet EPP Агент вручную:

1 Запустите установочный файл `ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi` и следуйте указаниям мастера установки.

Если какие-либо компоненты из необходимого программного обеспечения не были установлены, вы увидите сообщение об ошибке установки со списком установленных и требуемых к установке компонентов. Установите отсутствующие компоненты и запустите файл `ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi` заново.

2 Измените папку установки ViPNet EPP Агент или оставьте по умолчанию.



Внимание! Требования к пути установки аналогичны требованиям при установке ViPNet EPP Сервер (см. Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль).

3 Задайте имя, введите и подтвердите пароль учетной записи администратора агента (см. Требования к имени и паролю учетной записи) или оставьте значения, предложенные по умолчанию: имя — `admin`, пароль — `admin`.

4 Выберите способ работы ViPNet EPP Агент:

- Под управлением ViPNet EPP Сервер — выберите **Работа под управлением сервера**, укажите:
  - Для подключения к ViPNet EPP Сервер for Windows — IP-адрес или доменное имя ViPNet EPP Сервер for Windows.
  - Для подключения к ViPNet EPP Сервер for Linux — IP-адрес рабочего сервера.

    TCP-порт оставьте по умолчанию (`25010`).
- Автономный — снимите флажок **Работа под управлением сервера**.

5 На странице **Все готово к установке ViPNet EndPoint Protection Agent** нажмите **Установить**.

6 По завершении установки нажмите **Готово**.

7 Для перезагрузки компьютера нажмите **Да**.

В результате на компьютер будет установлен ViPNet EPP Агент. Настройте сетевой сенсор ViPNet EPP Агент.

Если был выбран режим под управлением сервера, запрос на подключение к ViPNet EPP Сервер отправится автоматически.

Установка ViPNet EPP Агент с помощью групповых политик Active Directory

Установка ViPNet EPP Агент в корпоративной сети с большим количеством компьютеров в ручном режиме может быть долгой и трудоемкой. В этом случае вы можете установить ViPNet EPP Агент удаленно с помощью групповых политик Active Directory.

Примечание. Подробнее об установке программного обеспечения с помощью групповых политик см. на сайте компании Microsoft.

Настройка параметров установки ViPNet EPP Агент с помощью групповых политик выполняется системным администратором домена на контроллере домена Active Directory.

Примечание. Описание пользовательского интерфейса создания объекта групповой политики и задания на установку ViPNet EPP Агент приведено на примере ОС Windows Server 2012 R2. Интерфейс других версий ОС Windows Server может незначительно отличаться.

Для установки ViPNet EPP Агент с помощью групповых политик:

1 Создайте точку распространения:

1.1 На контроллере домена в общей папке `Netlogon` создайте новую папку `EPP_Agent`.

1.2 Создайте файл `EPP_Agent.bat`, содержащий команды установки:

- Для установки ViPNet EPP Агент под управлением сервера:

```
@echo off

msiexec /q /i \\<Имя контроллера
домена>\NETLOGON\EPP_Agent\ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi
SERVER=<IP-адрес или доменное имя ViPNet EPP Сервер или IP-адрес рабочего
сервера> PORT=25010 LOGIN=<Имя пользователя администратора агента>
PASSWORD=<Пароль администратора агента> /norestart
```

где:

  - `PORT` — порт для подключения к ViPNet EPP Сервер;
  - `/norestart` — команда отмены перезагрузки.

- Для установки автономных ViPNet EPP Агент:

```
@echo off

msiexec /q /i \\<Имя контроллера
домена>\NETLOGON\EPP_Agent\ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi
SERVERSCHEME=0
```

1.3 Скопируйте файлы `EPP_Agent.bat` и `ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi` в папку `EPP_Agent`.

2 В домене Active Directory создайте одну или несколько групп, включающих компьютеры, на которых вы хотите установить или выполнить обновление ViPNet EPP Агент с помощью групповых политик. Параметры создаваемых групп оставьте по умолчанию.

3 Создайте новый объект групповой политики и свяжите его с доменом.

4 Добавьте группы компьютеров, созданные на шаге 2, к объекту групповой политики, созданному на шаге 3:

4.1 Откройте окно свойств объекта групповой политики.

4.2 На вкладке **Область** в разделе **Фильтры безопасности** нажмите **Добавить** и выберите необходимые группы.

5 Откройте окно редактирования объекта групповой политики и создайте задание на установку ViPNet EPP Агент. Для этого щелкните объект групповой политики правой кнопкой мыши и выберите **Изменить**.

6 Перейдите в раздел **Конфигурация компьютера** > **Настройка** > **Параметры панели управления** > **Назначенные задания**.

7 Щелкните **Назначенные задания** правой кнопкой мыши и выберите **Создать** > **Запланированная задача (Windows 7 и выше)**.

8 В окне **Новые свойства задачи (Windows 7 и выше)** на вкладке **Общие**:

8.1 В списке **Действие** выберите **Создать**.

8.2 В поле **Имя** укажите название задания.

8.3 Укажите имя учетной записи, с помощью которой задание будет выполняться:

8.3.1 В группе **Параметры безопасности** нажмите **Изменить пользователя или группу**.

8.3.2 В окне **Выбор: Пользователь или группа** нажмите **Дополнительно,** затем **Поиск** и в появившемся списке учетных записей выберите системную учетную запись `Система`.

8.3.3 Нажмите **OK**.

8.4 В окне выбора пользователя или группы нажмите **OK**.

В результате в поле **При выполнении задачи использовать следующую учетную запись пользователя** должна отобразиться учетная запись `NT AUTHORITY\System`.

Примечание. Вы можете использовать вместо системной учетной записи другую учетную запись с правами администратора. В этом случае после выбора учетной записи установите флажок **Выполнять вне зависимости от регистрации пользователя** и в появившемся окне введите пароль выбранной учетной записи. Учетная запись с правами администратора должна быть добавлена на компьютеры пользователей.

9 Установите флажок **Выполнить с наивысшими правами**.

10 В списке **Настроить для:** выберите **Windows Vista или Windows Server 2008**.

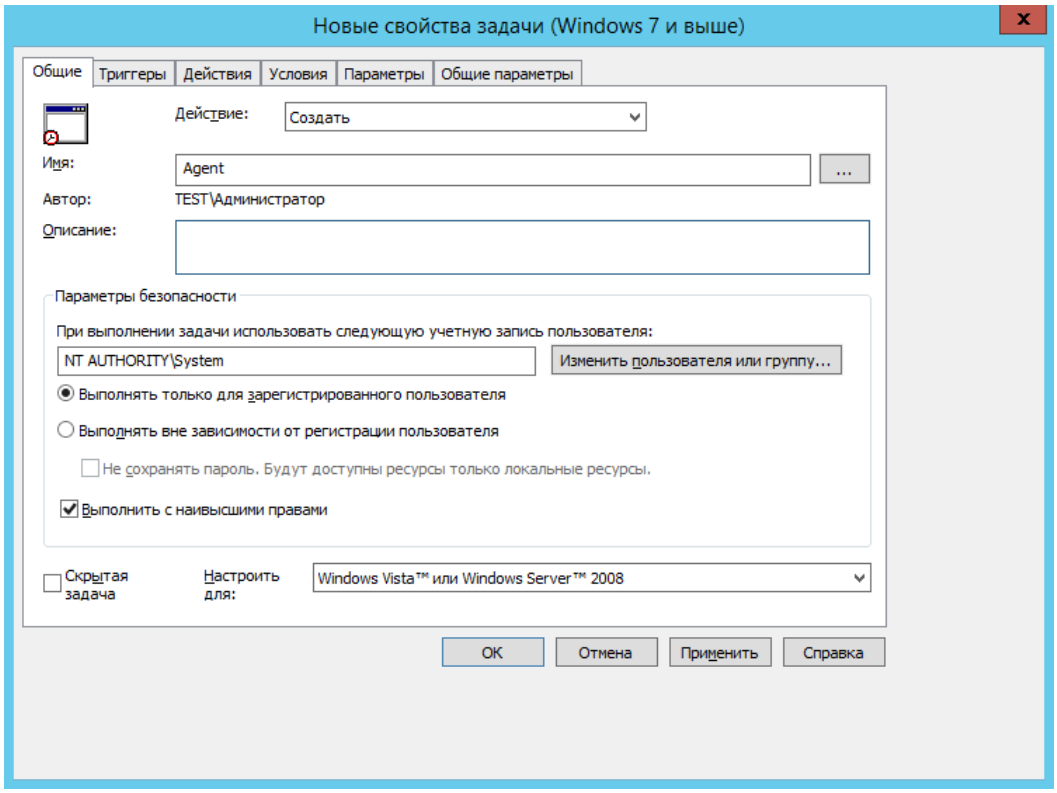


Рисунок 13. Настройка общих параметров и параметров безопасности задания на установку ViPNet EPP Агент

11 В окне **Новые свойства задачи** на вкладке **Триггеры** укажите необходимое условие для запуска выполнения задания (например, время начала выполнения задания и частоту его выполнения).

12 В окне **Новые свойства задачи** на вкладке **Действия** нажмите **Создать** и в окне **Новое действие**:

12.1 В списке **Действие** выберите **Запуск программы.**

В результате в поле **Программа или сценарий** укажите полный сетевой путь к файлу `EPP_Agent.bat`, созданному на шаге 1.2: `\\<Имя вашего контроллера домена>\NETLOGON\EPP_Agent\EPP_Agent.bat`.

12.2 Нажмите **OK**.

13 Сохраните созданное задание на установку. Нажмите **Применить**. Нажмите **OK**.

Задание на установку будет запущено при выполнении условия, указанного на вкладке **Триггеры** (шаг 11).

14 Для автоматической установки или обновления ViPNet EPP Агент перезагрузите компьютеры.



Примечание. Если на контроллере домена задан большой интервал времени для обновления групповых политик (по умолчанию — 90 минут), вы можете самостоятельно начать их немедленное обновление. Для этого воспользуйтесь консолью управления групповыми политиками GPMC. Затем начните перезагрузку компьютеров пользователей или попросите их самостоятельно перезагрузить компьютеры.

После перезагрузки компьютеров установка ViPNet EPP Агент на них будет запущена автоматически в фоновом режиме. После установки ViPNet EPP Агент запрос на подключение к ViPNet EPP Сервер отправится автоматически.

На защищаемых узлах настройте сетевой сенсор ViPNet EPP Агент.

Восстановление или удаление ViPNet EPP Сервер и ViPNet EPP Серверная консоль



Совет. Перед удалением ViPNet EPP Сервер и ViPNet EPP Серверная консоль рекомендуется создать резервную копию конфигурации ViPNet EPP Сервер (см. Резервное копирование и восстановление конфигурации). Это позволит быстро восстановить работоспособность в случаях сбоев или переустановки программного обеспечения.

Чтобы восстановить или удалить ViPNet EPP Сервер и ViPNet EPP Серверная консоль:

1 Запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi`.

2 На странице **Изменение, восстановление или удаление установки** выберите действие:

2.1 Для исправления ошибок в установке ViPNet EPP Сервер и ViPNet EPP Серверная консоль путем восстановления отсутствующих и поврежденных файлов, ярлыков и записей реестра нажмите **Восстановить**:

2.1.1 На странице готовности к восстановлению нажмите **Восстановить**.

2.1.2 Дождитесь окончания восстановления и нажмите **Готово**.

2.2 Для удаления ViPNet EPP Сервер и ViPNet EPP Серверная консоль нажмите **Удалить**:

2.2.1 На странице готовности к удалению нажмите **Удалить**.

2.2.2 Дождитесь окончания удаления и нажмите **Готово**.

Восстановление или удаление ViPNet EPP Агент

Чтобы восстановить ViPNet EPP Агент с помощью групповых политик Active Directory, выполните все шаги сценария установки (см. Установка ViPNet EPP Агент с помощью групповых политик Active Directory). При этом на шаге 1.2 создайте файл `EPP_Agent.bat`, содержащий команду:

```
@echo off
msiexec /q /i \\<Имя контроллера
домена>\NETLOGON\EPP_Agent\ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi REINSTALL=ALL
/norestart
```

Чтобы вручную восстановить ViPNet EPP Агент или удалить его:

1 Запустите файл `ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi` и следуйте указаниям мастера.

2 На странице **Изменение, восстановление или удаление установки** выберите нужное действие:

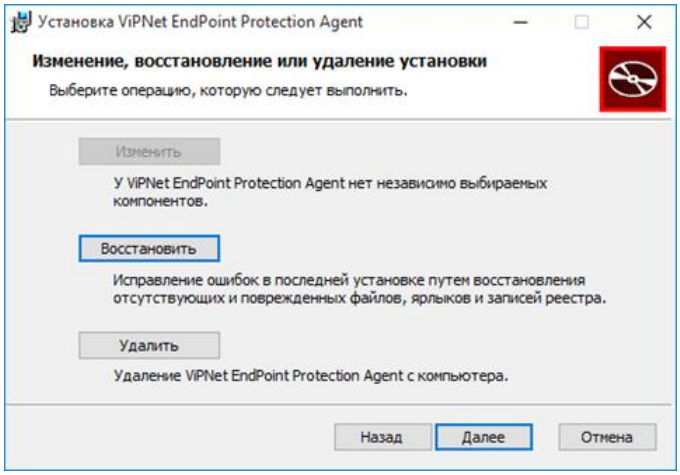


Рисунок 14. Восстановление или удаление ViPNet EPP Агент

2.1 Для исправления ошибок в установке ViPNet EPP Агент путем восстановления отсутствующих и поврежденных файлов, ярлыков и записей реестра нажмите **Восстановить**:

2.1.1 На странице готовности к восстановлению нажмите **Восстановить**.

2.1.2 Дождитесь окончания восстановления и нажмите **Готово**.

2.1.3 Для перезагрузки компьютера нажмите **Да**.

2.2 Для удаления ViPNet EPP Агент нажмите **Удалить**:

2.2.1 На странице готовности к удалению нажмите **Удалить**.

> **Примечание.** В процессе удаления могут появляться сообщения о необходимости закрыть различные приложения. Для продолжения удаления нажмите **Игнорировать** или **Пропустить**.

2.2.2 Дождитесь окончания удаления и нажмите **Готово**.

2.2.3 Для перезагрузки компьютера нажмите **Да**.

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 от 1.5.2 до 1.7.0, обновите версии ViPNet EPP последовательно по схеме: 1.5.2 -> 1.6.0 -> 1.7.0 -> 1.7.1 -> 1.8.0.

При последовательном обновлении 1.7.0 -> 1.7.1 -> 1.8.0 в связи с изменениями поддерживаемой версии PostgreSQL может потребоваться удаление и переустановка ViPNet EPP Сервер для получения возможности указания нового порта.

Для получения обновления ViPNet EPP до промежуточных версий обратитесь в ИнфоТеКС. При обновлении следуйте указаниям раздела о порядке обновления в документе «ViPNet EPP. Руководство администратора» для той версии, на которую обновляете.

Если вы используете версию 1.5.1 или ниже, для перехода на версию ViPNet EPP 1.8.0 выполните все шаги в соответствии с разделом Порядок перехода с ViPNet EPP версии 1.5.1 или ниже на версию 1.8.0.

Порядок обновления компонентов ViPNet EPP версии 1.7.1 до версии 1.8.0:

1. На компьютере с ViPNet EPP Сервер обновите версию СУБД PostgreSQL версии 14.13 до версии 14.17.
2. Обновите ViPNet EPP Сервер и ViPNet EPP Серверная консоль до версии 1.8.0 (см. Обновление ViPNet EPP Сервер и ViPNet EPP Серверная консоль). Если ViPNet EPP Сервер и ViPNet EPP Серверная консоль установлены на разных компьютерах, сначала обновите ViPNet EPP Сервер (см. Обновление ViPNet EPP Сервер и ViPNet EPP Серверная консоль), а затем ViPNet EPP Серверная консоль (см. Обновление ViPNet EPP Серверная консоль).
3. Чтобы получить базу правил для ViPNet EPP Агент версии 1.8.0, в ViPNet EPP Сервер запустите проверку обновления на сервере обновлений (см. Управление базами правил). Действие доступно только при наличии действующей подписки на обновления баз правил.
4. Обновите все ViPNet EPP Агент до версии 1.8.0 (см. Обновление ViPNet EPP Агент). Порядок обновления ViPNet EPP Агент на компьютерах с ОС GNU/Linux см. в документе «ViPNet EPP for Linux. Руководство администратора» в разделе «Установка и обновление ViPNet EPP Агент».
5. Настройте сетевой сенсор ViPNet EPP Агент.

После обновления сервера и агентов до версии 1.8.0:

- Журнал аудита и журнал самотестирования (только на агентах) начнет вестись заново.
- При первом подключении пользователей к серверу и агентам потребуется сменить пароли учетных записей.

Обновление СУБД PostgreSQL версии 14.13 до версии 14.17 на компьютере с ViPNet EPP Сервер

В рамках описания предполагается, что СУБД PostgreSQL версии 14.13 установлена в папку по умолчанию: `C:\Program Files\PostgreSQL\14`. Если у вас другая папка установки, в настройках вместо `C:\Program Files\PostgreSQL\14` используйте путь к папке установки СУБД PostgreSQL версии 14.13 на вашем компьютере.

Примечание. Если на компьютере установлен ViPNet EPP Агент, перед обновлением выключите контроль приложений (см. Выбор режима работы контроля приложений).

Перед обновлением ViPNet EPP Сервер обновите СУБД PostgreSQL версии 14.13 до версии 14.17 и подготовьте к работе:

1 Остановите службу ViPNet EPP Сервер:

1.1 Нажмите сочетание клавиш **Win+R**.

1.2 В поле **Открыть** введите `services.msc` и нажмите **OK**.

1.3 В списке **Службы (локальные)** дважды щёлкните по **ViPNet EPP Server**.

1.4 В поле **Тип запуска** выберите **Отключена**.

1.5 Нажмите **OK**.

1.6 Если на компьютере установлен ViPNet EPP Агент, отключите службу **ViPNet EPP Agent**.

1.7 Остановите службу **ViPNet EPP Server**.

2 Скопируйте расширения СУБД PostgreSQL версии 14.13 во временную папку:

2.1 Создайте временную папку, например: `C:\Temp`.

2.2 Перейдите в папку `C:\Program Files\PostgreSQL\14\share\extension`.

2.3 Скопируйте все файлы, включающие в название `partman`, в папку `C:\Temp`.

3 Удалите СУБД PostgreSQL версии 14.13.

4 Установите СУБД PostgreSQL версии 14.17. Для этого запустите установочный файл PostgreSQL из комплекта поставки ViPNet EPP и следуйте указаниям мастера:

4.1 На странице **Installation Directory** оставьте папку по умолчанию `C:\Program Files\PostgreSQL\14`.

4.2 На странице **Select Components** снимите флажок **Stack Builder**.

4.3 На странице **Data Directory** оставьте папку по умолчанию `C:\Program Files\PostgreSQL\14\data`.

4.4 На странице **Password** укажите такой же пароль учетной записи `postgres`, какой был для PostgreSQL версии 14.13.

4.5 На странице **Port** оставьте порт по умолчанию `5432`.

4.6 Дождитесь завершения установки PostgreSQL и на последней странице мастера нажмите **Finish**.

5 Перенесите расширения СУБД PostgreSQL версии 14.13 в версию 14.17 — скопируйте файлы из шага 2 в папку `C:\Program Files\PostgreSQL\14\share\extension`.

6 Установите Microsoft .NET Desktop Runtime версии 8.0.11. Для этого запустите установочный файл Microsoft .NET Desktop Runtime из комплекта поставки ViPNet EPP и следуйте указаниям мастера.

Обновление ViPNet EPP Сервер и ViPNet EPP Серверная консоль



Внимание! При обновлении ViPNet EPP Сервер необходимо наличие свободного места на диске по объему больше базы данных. При большом размере базы данных ViPNet EPP Сервер обновление может занять продолжительное время.

Перед запуском обновления рекомендуем убедиться, что завершены процессы сканирования AntiMalware (см. Сканирование AntiMalware) и построения модели поведенческого анализа (см. Настройка модели нормальной активности защищаемого узла), иначе после обновления данные по незавершенным процессам будут потеряны.

Чтобы обновить ViPNet EPP Сервер и ViPNet EPP Серверная консоль:

1 Запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` и следуйте указаниям мастера установки.

Если произошел сбой установки, вы увидите сообщение об ошибке установки с указанием возможной причины. Устраните причины сбоя и запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` заново.

2 Ознакомьтесь с лицензионным соглашением. В случае согласия выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

3 На странице **Все готово к установке ViPNet EndPoint Protection Server** нажмите **Установить**.

При появлении страницы мастера **Используемые файлы** со списком служб ViPNet EPP, которые не были остановлены, но используют файлы, нуждающиеся в обновлении, выберите **Закрыть приложения и попытаться перезапустить их**. Нажмите **OK**.

Дождитесь завершения установки.

4 На странице **Установка ViPNet EndPoint Protection Server завершена** нажмите **Готово**.

Перезагрузка компьютера не требуется.



Примечание. После обновления при первом подключении к серверу возможно появление ошибки подключения с сообщением о проведении подготовительной работы сервером. Это связано с техническими процессами после обновления. Подождите 1-2 минуты и повторите подключение к серверу.

Обновление ViPNet EPP Серверная консоль

Обновление ViPNet EPP Серверная консоль выполняется с помощью установочного файла ViPNet EPP Сервер.

Чтобы обновить ViPNet EPP Серверная консоль:

1 Запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` и следуйте указаниям мастера установки.

Если произошел сбой установки, вы увидите сообщение об ошибке установки с указанием возможной причины. Устраните причины сбоя и запустите файл `ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi` заново.

2 Ознакомьтесь с лицензионным соглашением. В случае согласия выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

3 На странице **Все готово к установке ViPNet EndPoint Protection Server** нажмите **Установить**.

Дождитесь завершения установки.

4 На странице **Установка ViPNet EndPoint Protection Server завершена** нажмите **Готово**.



Примечание. После обновления при первом подключении к серверу возможно появление ошибки подключения с сообщением о проведении подготовительной работы сервером. Это связано с техническими процессами после обновления. Подождите 1-2 минуты и повторите подключение к серверу.

Обновление ViPNet EPP Агент

Чтобы обновить ViPNet EPP Агент с помощью групповых политик Active Directory, выполните все шаги сценария установки (см. Установка ViPNet EPP Агент с помощью групповых политик Active Directory). При этом на шаге 1.2 создайте файл `EPP_Agent.bat`, содержащий команду:

```
@echo off
msiexec /q /i \\<Имя контроллера
домена>\NETLOGON\EPP_Agent\ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi /norestart
```

Чтобы обновить ViPNet EPP Агент вручную:

1 Запустите установочный файл `ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi` и следуйте указаниям мастера установки.

Если какие-либо компоненты из необходимого программного обеспечения не были установлены, вы увидите сообщение об ошибке установки со списком установленных и требуемых к установке компонентов. Установите отсутствующие компоненты и запустите файл `ViPNetEppSetup_x64_RU_x.x.x.xxxx.msi` заново.

2 На странице **Все готово к установке ViPNet EndPoint Protection Agent** нажмите **Установить**.

При появлении страницы мастера **Используемые файлы** со списком служб ViPNet EPP, которые не были остановлены, но используют файлы, нуждающиеся в обновлении, выберите **Закрыть приложения и попытаться перезапустить их**. Нажмите **OK**.

Дождитесь завершения установки.

3 На странице **Установка ViPNet EndPoint Protection Agent завершена** нажмите **Готово**.

4 Для перезагрузки компьютера нажмите **Да**.

Порядок перехода с ViPNet EPP версии 1.5.1 или ниже на версию 1.8.0

В связи с изменениями в программе установки ViPNet EPP версии 1.8.0 обновить ViPNet EPP версии 1.5.1 или ниже до версии 1.8.0 возможно только через удаление старой версии и установку новой. Для корректного перехода на версию 1.8.0 строго следуйте инструкциям ниже.

1 Обновите ViPNet EPP Сервер и ViPNet EPP Серверная консоль до версии 1.8.0:

1.1 Удалите установленную у вас версию ViPNet EPP Сервер версии 1.5.1 или ниже в соответствии с документацией к установленной версии.

1.2 Удалите папку установки ViPNet EPP Сервер (по умолчанию — `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection Server` и `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection Server Console`).

1.3 Удалите установленную СУБД PostgreSQL.

1.4 Подготовьтесь к установке ViPNet EPP Сервер (см. Подготовка к установке ViPNet EPP).

1.5 Установите ViPNet EPP Сервер и ViPNet EPP Серверная консоль версии 1.8.0 (см. Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль).

2 Если ViPNet EPP Серверная консоль установлена отдельно от ViPNet EPP Сервер, обновите ViPNet EPP Серверная консоль до версии 1.8.0:

2.1 Удалите установленную у вас версию ViPNet EPP Серверная консоль версии 1.5.1 или ниже в соответствии с документацией к установленной версии.

2.2 Удалите папку установки ViPNet EPP Серверная консоль (по умолчанию — `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection Server Console`).

2.3 Установите ViPNet EPP Серверная консоль версии 1.8.0 (см. Установка ViPNet EPP Серверная консоль).

3 Обновите ViPNet EPP Агент до версии 1.8.0 на всех компьютерах, где использовалась версия 1.5.1 или ниже. Для этого на каждом компьютере:

3.1 Удалите установленную версию ViPNet EPP Агент версии 1.5.1 или ниже в соответствии с документацией к установленной версии.

3.2 Удалите папку установки ViPNet EPP Агент (по умолчанию — `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection`).

3.3 Подготовьтесь к установке ViPNet EPP Агент (см. Подготовка к установке ViPNet EPP).

3.4 Установите ViPNet EPP Агент версии 1.8.0 (см. Установка ViPNet EPP Агент).

4 Подключите защищаемые узлы с ViPNet EPP Агент (из шага 3) к ViPNet EPP Сервер (см. Подключение защищаемых узлов).

5 Назначьте базу правил группе, в которую были добавлены защищаемые узлы с ViPNet EPP Агент (из шага 3), если база правил еще не назначена (см. Назначение базы правил группе узлов).

3

Управление в ViPNet EPP Сервер

Подключение к ViPNet EPP Сервер 85

Интерфейс ViPNet EPP Сервер 87

Установка и активация лицензии 89

Управление защищаемыми узлами и группами 90

Управление базами правил 98

Настройка базы правил 107

Управление ViPNet SafeBoot на защищаемых узлах 180

Настройка критериев обнаружения аномалий 198

Настройка модели нормальной активности защищаемого узла 199

Сканирование AntiMalware 202

Работа с журналами 212

Запрос журнала регистрации трафика с ViPNet EPP Агент 221

Администрирование ViPNet EPP Сервер 225

Интеграция с внешними системами 234

Подключение к ViPNet EPP Сервер

ViPNet EPP Сервер запускается автоматически при старте ОС Windows. Настройка ViPNet EPP Сервер выполняется с помощью ViPNet EPP Серверная консоль. Для успешного подключения к ViPNet EPP Сервер версии ViPNet EPP Сервер и ViPNet EPP Серверная консоль должны совпадать.

Внимание! Одновременное подключение к ViPNet EPP Сервер двух и более ViPNet EPP Серверная консоль с одной учетной записью запрещено.

Чтобы подключиться к ViPNet EPP Сервер:

1 В меню **Пуск** начните вводить **ViPNet EndPoint Protection Server Console** и запустите найденную программу.

2 Введите параметры входа в ViPNet EPP Сервер:

- В поле **Адрес сервера** введите доменное имя или IP-адрес компьютера в формате IP v4, на котором установлен ViPNet EPP Сервер. Если ViPNet EPP Серверная консоль и ViPNet EPP Сервер установлены на одном и том же компьютере, введите `localhost`.
- В полях **Имя учетной записи** и **Пароль** введите имя пользователя и пароль вашей учетной записи.

  При первом подключении к ViPNet EPP Сервер после установки войдите с учетной записью администратора ViPNet EPP по умолчанию: имя учетной записи — `admin`, пароль — `admin`.
- Чтобы при последующем подключении к ViPNet EPP Сервер не вводить имя пользователя и пароль учетной записи, выберите **Запомнить меня**.

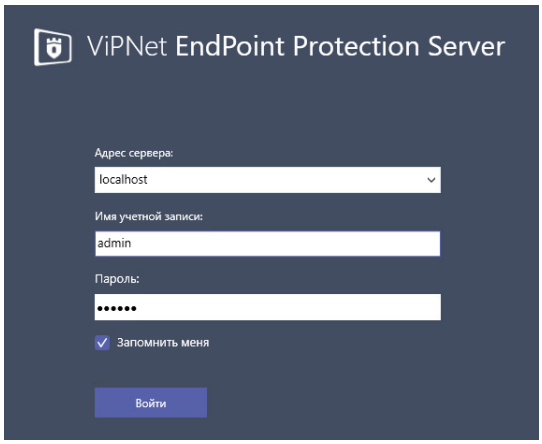


Рисунок 15. Подключение к ViPNet EPP Сервер

3 Нажмите **Войти**.



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

4 При первом подключении пользователя смените пароль учетной записи. Для этого в окне **Смена пароля** 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 **Использовать простой пароль** и указать любой пароль, отличающийся от предыдущего, но в целях безопасности использовать простые пароли не рекомендуется.

Нажмите **Готово**.

При успешной аутентификации откроется главное окно ViPNet EPP Сервер, в котором будут доступны действия по настройке согласно полномочиям вашей роли (см. Ролевая модель).

Интерфейс ViPNet EPP Сервер

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

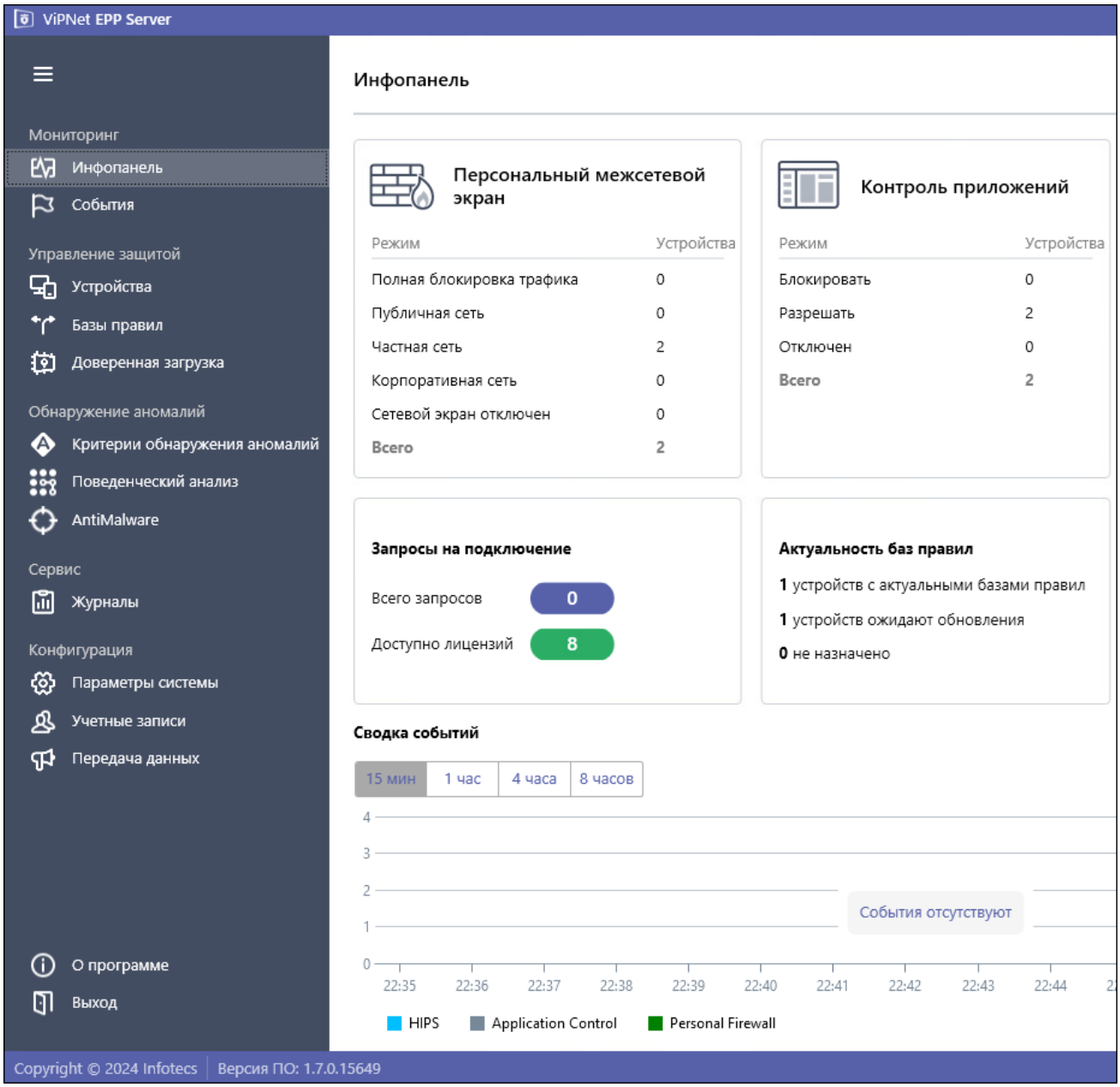


Рисунок 16. Главное окно ViPNet EPP Сервер в режиме администратора ViPNet EPP

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

- **Инфопанель** — просмотр режимов работы модулей защиты ViPNet EPP Агент на узлах, запросов на подключение узлов и доступное количество лицензий, актуальности баз правил, состояние обмена с ViPNet TIAS и Syslog, сводки событий.

- **События** — просмотр событий, обнаруженных ViPNet EPP Агент на защищаемых узлах, в режиме, близком к реальному времени (см. Журнал событий).
- **Устройства** — подключение защищаемых узлов, управление группами защищаемых узлов, просмотр состояния узлов и событий, зарегистрированных на них (см. Управление защищаемыми узлами и группами).
- **Базы правил** — управление базами правил:
  - Загрузка базы правил на ViPNet EPP Сервер (см. Загрузка обновления базы правил вручную).
  - Настройка и создание новой версии базы правил (см. Настройка базы правил).
- **Доверенная загрузка** — управление ViPNet SafeBoot на защищаемых узлах.
- **Критерии обнаружения аномалий** — настройка критериев обнаружения аномалий.
- **Поведенческий анализ** — настройка модели нормальной активности для защищаемых узлов (см. Настройка модели нормальной активности защищаемого узла).
- **AntiMalware** — настройка и запуск сканирования AntiMalware на защищаемых узлах (см. Сканирование AntiMalware).
- **Журналы** — просмотр журнала аудита (см. Журнал аудита), проверка работоспособности ViPNet EPP Сервер (см. Проверка работоспособности).
- **Параметры системы** — настройка параметров ViPNet EPP Агент и ViPNet EPP Сервер (см. Настройка параметров системы), резервное копирование и восстановление баз правил, журналов и настроек ViPNet EPP Сервер (см. Резервное копирование и восстановление конфигурации).
- **Учетные записи** — управление учетными записями ViPNet EPP Сервер: создание, редактирование, удаление (см. Управление учетными записями).
- **Передача данных** — интеграция с внешними системами:
  - Передача уведомлений по электронной почте.
  - Подключение к домену Active Directory.
  - Передача уведомлений в ViPNet TIAS или сторонние системы мониторинга (см. Передача событий в сторонние системы по протоколу UDP, Передача событий информационной безопасности в сторонние системы).
- **О программе** — версия программного обеспечения ViPNet EPP, контактные данные ИнфоТеКС, текст лицензионного соглашения, статус лицензии и действия с ней:
  - Установка и активация лицензии.
  - Обновление лицензии.
- **Выход** — завершение сеанса работы с ViPNet EPP Сервер.

Установка и активация лицензии

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

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **О программе** > **Данные**.

3 Нажмите **Загрузить лицензию** и выберите файл лицензии формата `itcslic`.

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

После загрузки лицензии на вкладке отобразится информация о лицензии.

4 Активируйте лицензию одним из способов:

- Онлайн-активация (необходим доступ в интернет) — нажмите **Активировать лицензию онлайн**.
- С помощью запроса на активацию:

  4.1.1 Нажмите **Выгрузить запрос на активацию** и сохраните файл запроса.

  4.1.2 Отправьте письмо с файлом запроса на электронный адрес reg@infotecs.ru.

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

  4.1.3 Нажмите **Ввести регистрационный код**.

  4.1.4 Чтобы поля заполнились автоматически, скопируйте и вставьте содержимое ответного письма в окне активации лицензии, нажмите **Активировать**.

При успешной активации в строке **Статус** появится сообщение **Лицензия 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 для включения на них модулей защиты, отслеживания событий информационной безопасности и возможности управления настройками модулей защиты.

После установки ViPNet EPP Агент защищаемого узла автоматически отправляет в ViPNet EPP Сервер запрос на подключение. Защищаемый узел, от которого поступил запрос, отображается на сервере в разделе  **Устройства** в служебной группе **Запросы на подключение**. Для подключения к серверу защищаемый узел необходимо перенести в пользовательскую группу на сервере, указав модули ViPNet EPP, которые будут доступны на узлах. Не рекомендуем добавлять более 300 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 базу правил (см. Назначение базы правил группе узлов). Если база правил уже была назначена группе, модули защиты включатся на защищаемом узле автоматически после перемещения в группу и получения базы правил.

В ViPNet EPP предусмотрены служебные и пользовательские группы узлов:

- Служебные группы:
  - **Запросы на подключение** — группа узлов, от которых пришел запрос на подключение. Если есть необработанные запросы на подключение, группа будет отмечена значком .
  - **Все** — группа всех подключенных узлов.

  Служебные группы невозможно удалить, а также назначить им базу правил.
- Пользовательские предустановленные группы:
  - **Главная.**
  - **Дом.**
  - **Мобильные.**
  - **Офис**.

  Пользовательские группы можно удалять и назначать им базу правил. Администратор ViPNet EPP Сервер может создавать новые пользовательские группы узлов (см. Управление группами защищаемых узлов и просмотр сведений о группах).

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 базу правил, сетевые фильтры которой не блокируют трафик между защищаемыми узлами других групп и ViPNet EPP Сервер.

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

Чтобы подключить один или несколько защищаемых узлов вручную:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

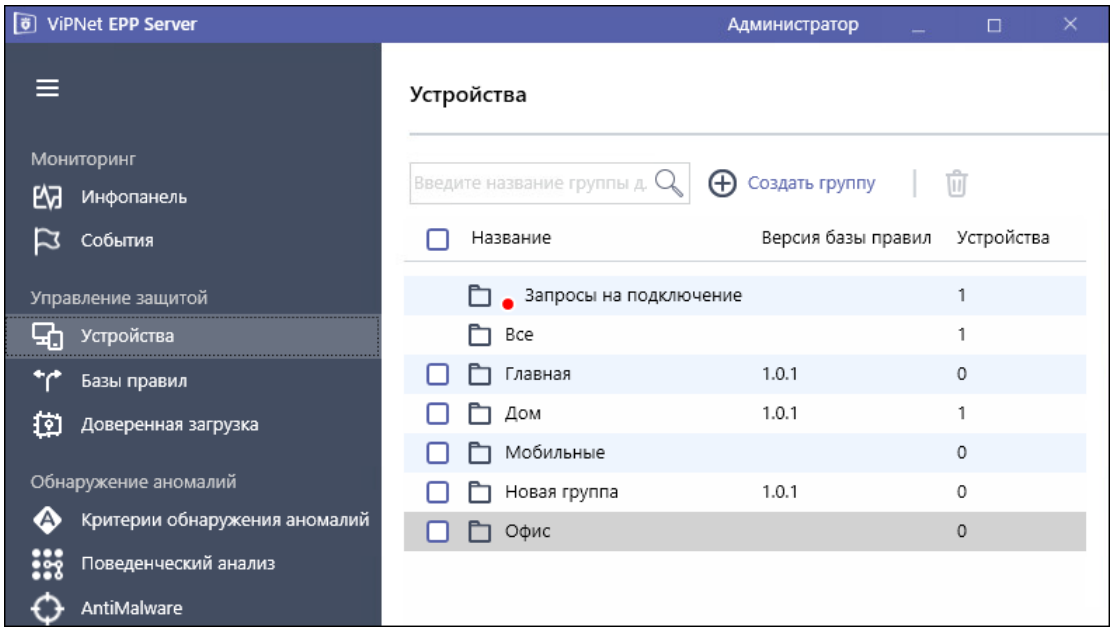


Рисунок 17. Служебные и пользовательские группы защищаемых узлов

2 Выберите **Устройства** > **Запросы на подключение**.

3 Выберите флажками узлы, которые необходимо подключить к ViPNet EPP Сервер.

4 На панели вверху в меню **Переместить** выберите пользовательскую группу для перемещения в нее узлов.

5 Выберите флажками модули ViPNet EPP, которые должны быть доступны на узле.

Список доступных модулей зависит от лицензии ViPNet EPP (см. Лицензирование). Для защищаемых узлов с ViPNet EPP Агент for Linux не выбирайте модуль **Application Control**, поскольку он не реализован в текущей версии программы.

Внимание! После подключения защищаемого узла изменение списка доступных модулей невозможно. Внимательно указывайте доступные модули.

Чтобы изменить список модулей после подключения, потребуется временное отключение узла от ViPNet EPP Сервер (см. Управление защищаемыми узлами группы) и затем повторное подключение.

6 Нажмите **Подключить**.

Если в вашей сети используется служба каталогов Active Directory или развернута виртуальная частная сеть ViPNet, вы можете подключить защищаемые узлы, импортировав их из домена Active Directory (см. Импорт защищаемых узлов из домена Active Directory).

После подключения защищаемых узлов на пользовательские группы узлов необходимо назначать базы правил, если они еще не назначены (см. Назначение базы правил 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 .

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 модулей из лицензии ViPNet EPP. В результате автоматического подключения на защищаемом узле будут доступны все модули защиты из лицензии. 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 **Запросы на подключение**, откуда их можно будет подключить вручную (см. Подключение защищаемых узлов).

Чтобы включить автоматическое подключение новых защищаемых узлов:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Параметры системы** > **Параметры сервера**.

3 Выберите **Автоматически подключать новые агенты** и в списке справа выберите группу, в которую будут перемещаться новые защищаемые узлы.

4 Нажмите **Сохранить**.

Для включения на защищаемом узле доступных модулей защиты назначьте выбранной пользовательской группе базу правил (см. Назначение базы правил группе узлов). Если база правил уже назначена группе, модули защиты включатся на защищаемом узле автоматически после перемещения в группу и получения базы правил.

Импорт защищаемых узлов из домена Active Directory

При импорте защищаемых узлов из домена Active Directory можно сразу же создать пользовательские группы и перенести в них узлы:

Примечание. Импорт защищаемых узлов из Active Directory доступен только для защищаемых узлов, которые были добавлены в домен Active Directory до установки ViPNet EPP Агент.

---

1 Укажите домен Active Directory, в котором находятся защищаемые узлы (см. Подключение к домену Active Directory).

2 Выберите **Устройства** > **Запросы на подключение**.

3 Дважды щелкните строку **Запросы на подключения** и на панели справа нажмите **Импортировать при помощи Active Directory**.

4 Укажите параметры импорта:

- Чтобы узлы были перенесены в пользовательские группы с именами подразделения Active Directory, выберите **Перенести в нее устройства**.
- Чтобы узлы были перенесены в пользовательскую группу с именем **Active Directory**, снимите флажок **Перенести в нее устройства**.

Примечание. Группа **Active Directory** служебная, используется только для импорта защищаемых узлов из домена Active Directory. После импорта необходимо распределить защищаемые узлы в другие группы для назначения базы правил.

- Чтобы имя агента подключенных устройств совпадало с именем устройства, снимите флажок **Импортировать имена пользователей в названия устройств**.
- Чтобы имя агента подключенных устройств совпадало с именем последнего авторизованного на узле пользователя, выберите **Импортировать имена пользователей в названия устройств**.

5 Нажмите **Начать** и дождитесь завершения импорта. Нажмите **OK**.

Управление группами защищаемых узлов и просмотр сведений о группах

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

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Устройства** и просмотрите сведения о группах. Для групп в списке отображаются:

- **Название** — названия групп. Группы могут быть отмечены следующими значками:
  - ● — в группе **Запросы на подключение** есть необработанные запросы.
  - Ⓐ — для группы настроено автоматическое подключение защищаемых узлов.
- **Версия базы правил** — номер версии базы правил, назначенной для группы.
- **Устройства** — количество устройств в группе.

3 Чтобы посмотреть список всех защищаемых узлов, щелкните группу **Все**.

4 Чтобы создать новую группу, нажмите ⊕ **Создать группу**, введите название новой группы и нажмите **Сохранить**.

5 Чтобы найти группу узлов, в поле поиска введите имя группы или его часть и нажмите 🔍.

6 Чтобы удалить одну или несколько групп, выберите флажками нужные группы, нажмите 🗑 и подтвердите удаление.

ℹ **Примечание.** При удалении группы все защищаемые узлы из нее автоматически перемещаются в группу **Запросы на подключение**.

---

7 Чтобы просмотреть политики аудита, примененные к группе узлов, дважды щелкните значок 🗁 нужной группы — на панели справа отобразятся политики аудита, примененные к группе узлов (см. Настройка политик аудита).

Управление защищаемыми узлами группы

Все защищаемые узлы, как подключенные, так и ожидающие подключения, распределены по группам и отображаются в разделе **Устройства**. Вы можете управлять защищаемыми узлами группы и просматривать сведения о них:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Устройства** и выполните:

- Чтобы посмотреть список всех защищаемых узлов, щелкните группу **Все**.
- Чтобы просмотреть список защищаемых узлов в определенной группе, щелкните группу, например группу **Офис**.

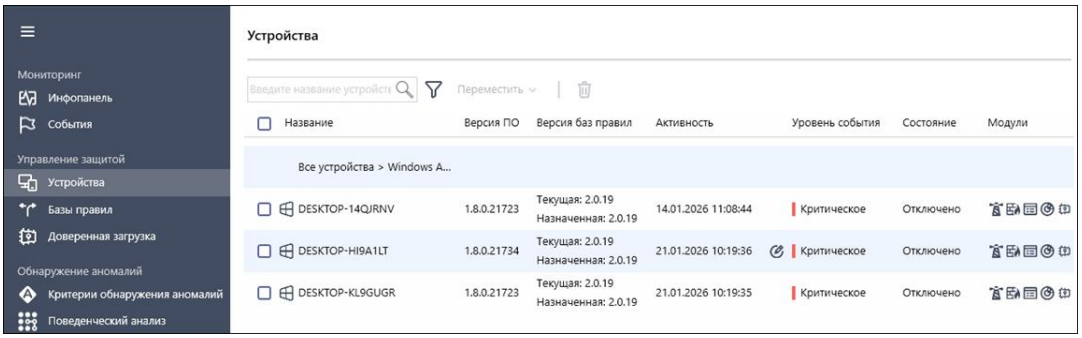


Рисунок 18. Список защищаемых узлов в группе

В зависимости от используемой операционной системы подключенные защищаемые узлы отмечены значками:

- — защищаемые узлы с ОС Windows.
- — защищаемые узлы с ОС GNU/Linux.

Для защищаемого узла в списке отображаются:

- **Название** — имя защищаемого узла.

  Значок — режим работы одного или нескольких модулей защиты был изменен пользователем в ViPNet EPP Агент защищаемого узла и отличается от установленного в назначенной базе правил. Этот значок появляется только для защищаемых узлов с ОС Windows.
- **Версия ПО** — номер версии ViPNet EPP Агент, установленной на защищаемом узле.
- **Версия баз правил** — номер версии базы правил, используемой на узле (текущая), и номер версии назначенной базы правил.
- **Активность** — время последнего обмена данными с сервером.
- **Уровень события** — наиболее опасный уровень события (см. Уровни событий информационной безопасности), зарегистрированный на защищаемом узле за время отслеживания.

Примечание. **Критическое**, **Опасное** и **Важное** события требуют реагирования со стороны администратора ViPNet EPP. После принятия мер эти события необходимо удалить, чтобы не пропустить следующее опасное событие.

- **Состояние** — активность узла. Узел активен, если он регулярно обменивается данными с ViPNet EPP Сервер. Если в течение времени, определяемого параметром **Период неактивности** (см. Настройка параметров системы), обмена данными не происходит, то защищаемый узел считается неактивным (**Отключено**). Это означает, что связь с узлом потеряна, и события на узле могут не отслеживаться.
- **Модули** — подключенные модули защиты ViPNet EPP на узле, указанные при подключении узла к серверу (см. Подключение защищаемых узлов):
  - — Personal Firewall.

- — Application Control.
- — HIDS.
- — HIPS.
- — SafeBootMC.

- Чтобы в списке узлов найти определенный узел, в поле поиска введите часть имени узла или имя целиком и нажмите .
- Чтобы просмотреть подробные сведения об определенном узле, найдите этот узел в списке и дважды щелкните его — на правой панели будут отображены вкладки:
  - **Сведения** — имя узла, группа, к которой относится узел, имя назначенной базы правил, дата и время последней активности узла, подключенные модули, другая информация о защищаемом узле. Вы можете выделить и скопировать имя устройства, адрес устройства и идентификатор устройства.

    Чтобы время на узле было синхронизировано со временем ViPNet EPP Сервер, выберите **Выполнять синхронизацию времени с сервером** и нажмите **ОК**.
  - **События** — список событий информационной безопасности, зарегистрированных на узле, и полученных на ViPNet EPP Сервер. Периодичность опроса данных о событиях на узле определяется параметром **Период опроса** (см. Настройка параметров системы).
    - Чтобы отфильтровать список событий по ключевому слову столбца **Событие**, в поле поиска введите ключевое слово и нажмите .
    - Чтобы удалить события, выберите флажками нужные события, нажмите и подтвердите удаление.
  - **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 системы).
  - **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 и выберите из списков критерии фильтрации, нажмите **Применить**.
- Чтобы переместить защищаемый узел в другую пользовательскую группу, выполните одно из действий:
  - Выберите флажком узел, в меню **Переместить** выберите группу.
  - Дважды щелкните узел, на панели справа в списке **Устройство входит в группу** выберите пользовательскую группу и нажмите **ОК**.
- Чтобы временно отключить узел от ViPNet EPP Сервер (прекратить отслеживание событий узла), выберите флажком узел, нажмите и подтвердите удаление — узел будет

перемещен в группу **Запросы на подключение**. Временно отключенные узлы можно удалить с ViPNet EPP Сервер.

- Чтобы удалить узел с ViPNet EPP Сервер, в группе **Запросы на подключение** выберите его флажком, нажмите  и подтвердите удаление узла.

Управление базами правил

В ViPNet EPP Сервер встроена база правил по умолчанию. Для своевременного выявления новых угроз безопасности информации базу правил необходимо обновить с сервера обновлений сразу после установки ViPNet EPP Сервер и далее обновлять регулярно. Варианты загрузки обновлений базы правил на ViPNet EPP Сервер:

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

Не рекомендуем хранить на сервере более 30 баз правил. Это может привести к большой нагрузке на сервер и замедлению работы компьютера. Регулярно удаляйте ненужные базы правил.

Чтобы просмотреть список баз правил ViPNet EPP Сервер и найти в нем нужную базу:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

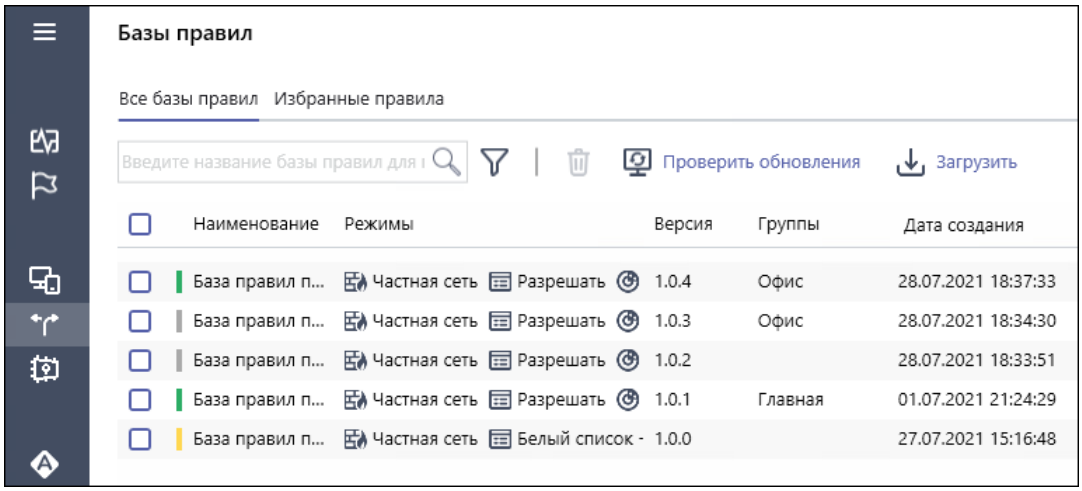


Рисунок 19. Список баз правил ViPNet EPP Сервер на вкладке «Все базы правил»

3 В строке поиска введите часть названия базы правил или название целиком и нажмите .

Чтобы просмотреть сведения об определенной базе правил:

1 В списке баз правил дважды щелкните базу правил. На панели справа на вкладке **Основные** просмотрите сведения о базе правил — дата создания, версия, статус активности, режимы работы модулей защиты.

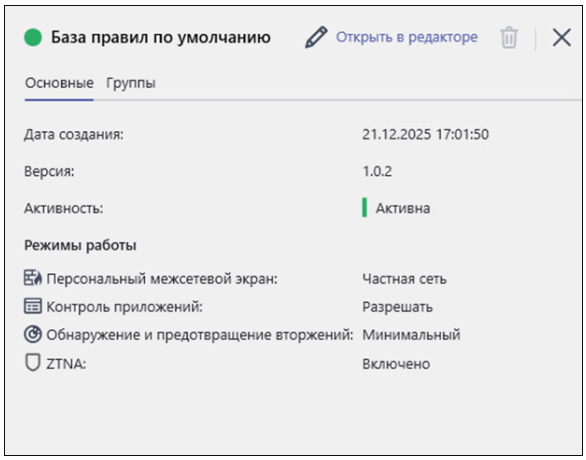


Рисунок 20. Сведения о базе правил на вкладке «Основные»

Статусы базы правил:

- **Активна** — применяется на защищаемых узлах групп.
- **Устарела** — база правил уже не назначена никаким группам узлов, но есть узлы, на которых эта база еще используется, например, защищаемый узел неактивен и на него еще не загружена новая назначенная ему база правил.
- **Не используется** — не применяется ни на одном защищаемом узле.

2 Для просмотра списка групп защищаемых узлов, на которые назначена база правил, выберите вкладку **Группы**.

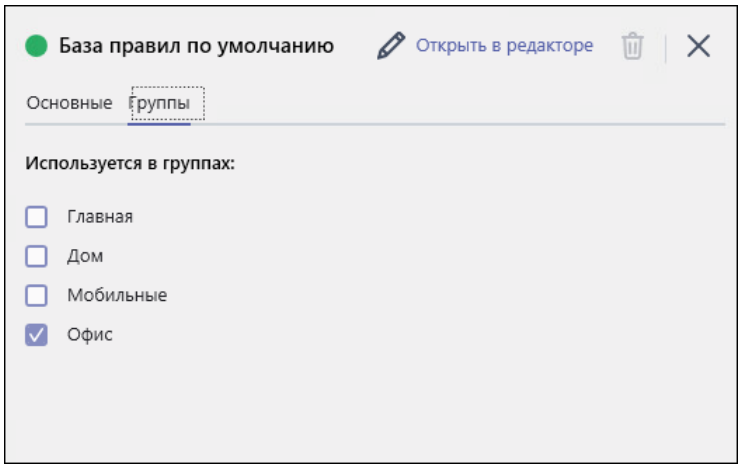


Рисунок 21. Сведения о базе правил на вкладке «Группы»

Чтобы создать новую версию базы правил на основе выбранной и настроить ее:

1 В списке баз правил дважды щелкните нужную базу правил.

2 На панели справа нажмите **Открыть в редакторе**.

3 Внесите требуемые изменения и сохраните их (см. Настройка базы правил).

Примечание. Правила формирования номера версии базы правил:

- старшая цифра номера версии присваивается при загрузке обновления базы правил на ViPNet EPP Сервер и не изменяется при создании новой версии базы правил;
- средняя цифра присваивается разработчиком базы правил и не изменяется при создании новой версии базы правил;
- младшая цифры номера версии последовательно увеличиваются на единицу при каждом сохранении изменений в базе правил.

Например, вы загрузили на ViPNet EPP Сервер обновление базы правил из файла Epp_20210111_12_1.0-1.2_RU.zip, которому будет присвоена версия 2.0.0. Далее, на основе этой базы правил вы можете создавать новые версии этой базы правил, номера которых последовательно будут увеличиваться на единицу — 2.0.1, 2.0.2, 2.0.3 и так далее. Версии удаленных баз правил более не используются при создании новых версий базы правил.

Если вы настроили автоматическую загрузку обновлений, которая выполняется с заданным интервалом времени, но хотите проверить наличие обновления прямо сейчас, нажмите **Проверить обновления**. Если обновление есть — оно будет загружено в ViPNet EPP Сервер и отобразится в списке баз правил. После проверки или загрузки обновления появится сообщение о завершении действия. Нажмите **OK**.

Чтобы отфильтровать список баз правил по статусу использования:

1. Нажмите и выберите критерии фильтрации — актуальные, устаревшие или неиспользуемые базы правил.
2. Нажмите **Применить**.

Неиспользуемые версии базы правил рекомендуется периодически удалять. Вы можете удалить базу правил, которая не назначена ни одной группе. Чтобы удалить базу правил:

1. Выберите ее флажком в списке.
2. Нажмите и подтвердите удаление базы правил.

Загрузка обновлений баз правил на ViPNet EPP Сервер

Автоматическая загрузка обновлений базы правил

ViPNet EPP поддерживает автоматическую загрузку обновлений базы правил с сервера обновлений.

Для настройки автоматической загрузки вам могут потребоваться:

- Имя и пароль 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.
- Если интернет доступен через прокси-сервер, потребуются параметры доступа к прокси-серверу: адрес и порт прокси-сервера, имя и пароль пользователя (при их наличии). Получите эти данные у администратора сети.



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 базу правил, сетевые фильтры которой не блокируют трафик между ViPNet EPP Сервер и сервером обновлений.

Чтобы настроить автоматическую загрузку:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите  **Параметры системы**.

3 На вкладке **Обновление баз правил** включите  **Использовать автоматическую загрузку обновлений баз правил**.

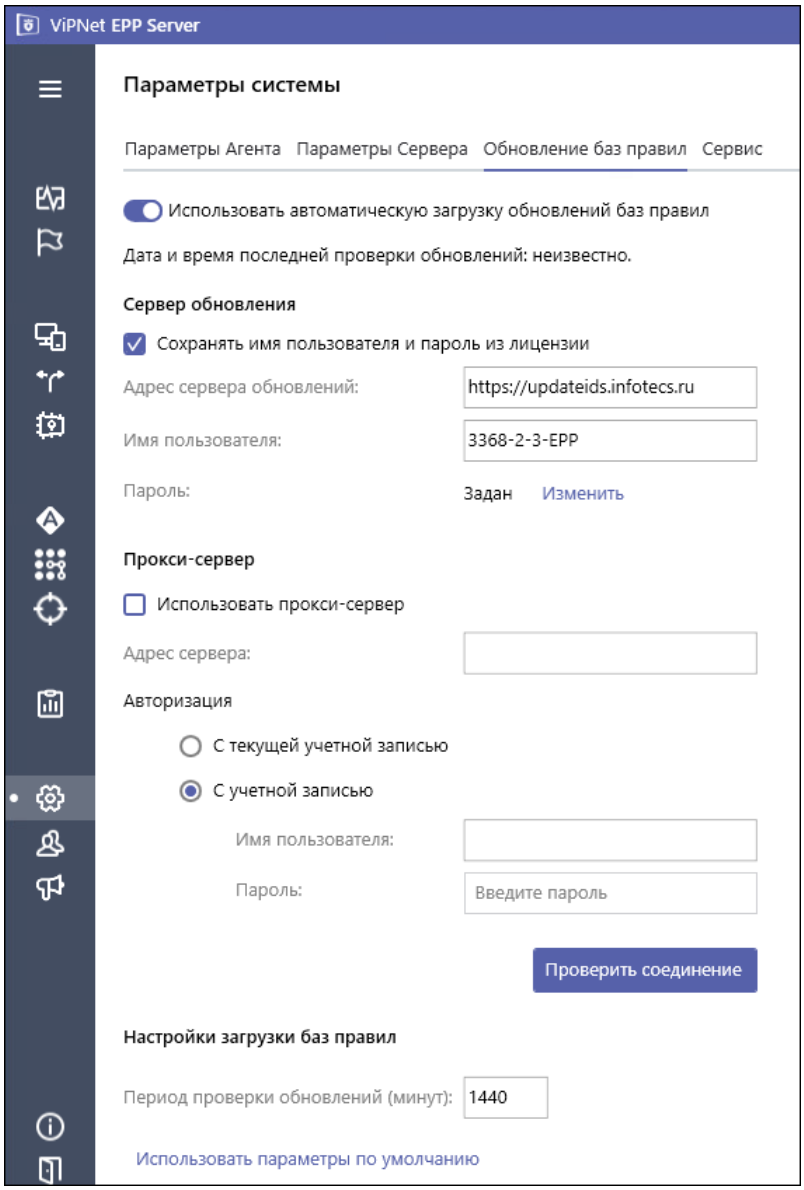


Рисунок 22. Настройка автоматической загрузки обновлений базы правил

4 Если в PDF-файле лицензии указан адрес сервера обновлений, отличный от установленного по умолчанию (`https://updateids.infotecs.ru`), задайте его.

5 Если после установки ViPNet EPP Сервер вы не снимали флажок **Сохранять имя пользователя и пароль из лицензии**, а также была установлена лицензия, имя пользователя и пароль для подключения к серверу обновлений уже указаны в соответствующих полях.

6 Если имя пользователя и пароль автоматически не добавились, выполните одно из действий:

- Вручную введите имя пользователя и пароль, указанные в PDF-файле лицензии.
- Выберите **Сохранять имя пользователя и пароль из лицензии** и повторно установите лицензию (см. Установка и активация лицензии). Активация при этом не потребуется.

7 Если для доступа в интернет в сети вашей организации используется прокси-сервер, выберите **Использовать прокси-сервер**:

7.1 Введите IP-адрес прокси-сервера.

7.2 В зависимости от способа авторизации на прокси-сервере выберите учетную запись и введите учетные данные.

8 Для проверки подключения к серверу обновлений нажмите **Проверить соединение**.

9 При необходимости измените период проверки обновлений базы правил (по умолчанию — 1440 минут).

10 Нажмите **Сохранить**.

Загрузка обновления базы правил вручную

Если с ViPNet EPP Сервер нет доступа к интернету, вы можете скачать обновление с сервера обновлений вручную. При загрузке обновления базы правил на ViPNet EPP Сервер проверяется электронная подпись базы правил. С сервера обновлений необходимо скачать файл с архивом обновления базы правил (формата ZIP) и файл с электронной подписью (формата SIG).



Совет. Для скачивания обновлений базы правил с сервера обновлений рекомендуется использовать выделенный компьютер с доступом к 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 файлы с архивом обновления базы правил с электронной подписью 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:

4.1 Щелкните файл обновления в одноименном столбце. Файл с обновлением будет сохранен на компьютер.

4.2 Щелкните файл электронной подписи в столбце **Электронная подпись**. Файл с электронной подписью будет сохранен на компьютер.

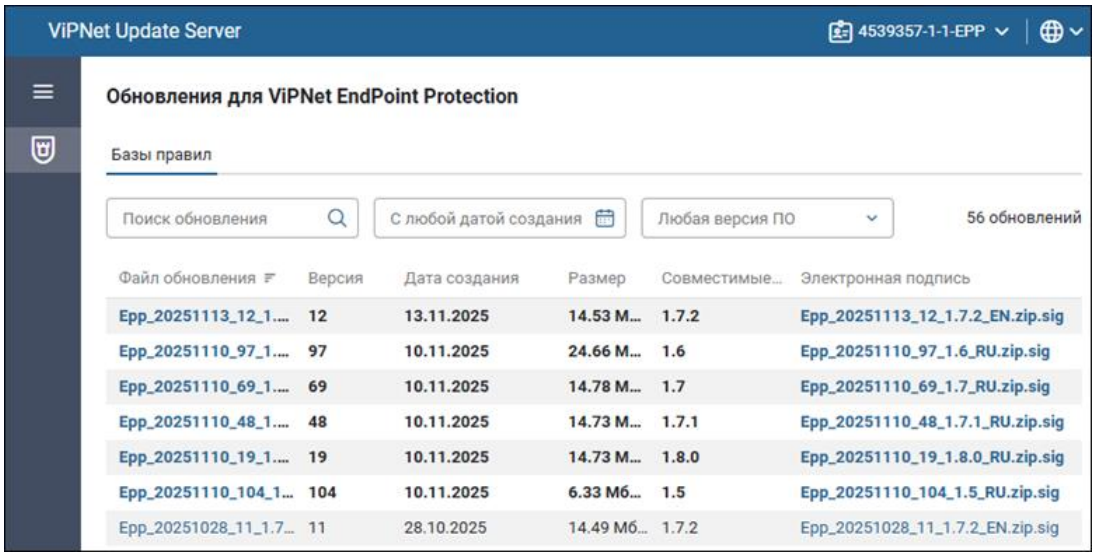


Рисунок 23. Главная страница сервера обновлений ViPNet Update Server

5 Скопируйте файлы с архивом обновления и с электронной подписью на USB-носитель в одну папку.

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

Чтобы загрузить на ViPNet EPP Сервер обновление базы правил:

1 Подключите к компьютеру USB-носитель с файлами с архивом обновления базы правил и с электронной подписью.

2 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

3 Выберите **Базы правил**.

4 Нажмите **Загрузить** и выберите на USB-носителе сразу два файла: с архивом обновления базы правил и с электронной подписью базы правил. База правил должна быть совместима с установленной у вас версией ViPNet EPP.

5 Нажмите **Открыть**.

6 В редакторе базы правил на панели слева нажмите **Назад к EndPoint Protection**.

7 Подтвердите сохранение изменений, нажав **Да**.

После успешной проверки подписи база правил отобразится в списке баз правил.

Просмотр и удаление избранных правил

Часть глобальных настроек базы правил (фильтры политик безопасности, правила доступа контроля приложений, веб-фильтры и политики ZTNA) можно добавить в избранное и использовать в разных версиях базы правил.

Правила, добавленные в избранное, вы можете просматривать и удалять.

Чтобы просмотреть избранные правила, добавленные ранее:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил** > **Избранные правила** — добавленные ранее объекты будут отображены в списках модулей защиты: **Персональный межсетевой экран**, **Контроль приложений**, **Веб-фильтрация**, **ZTNA**.

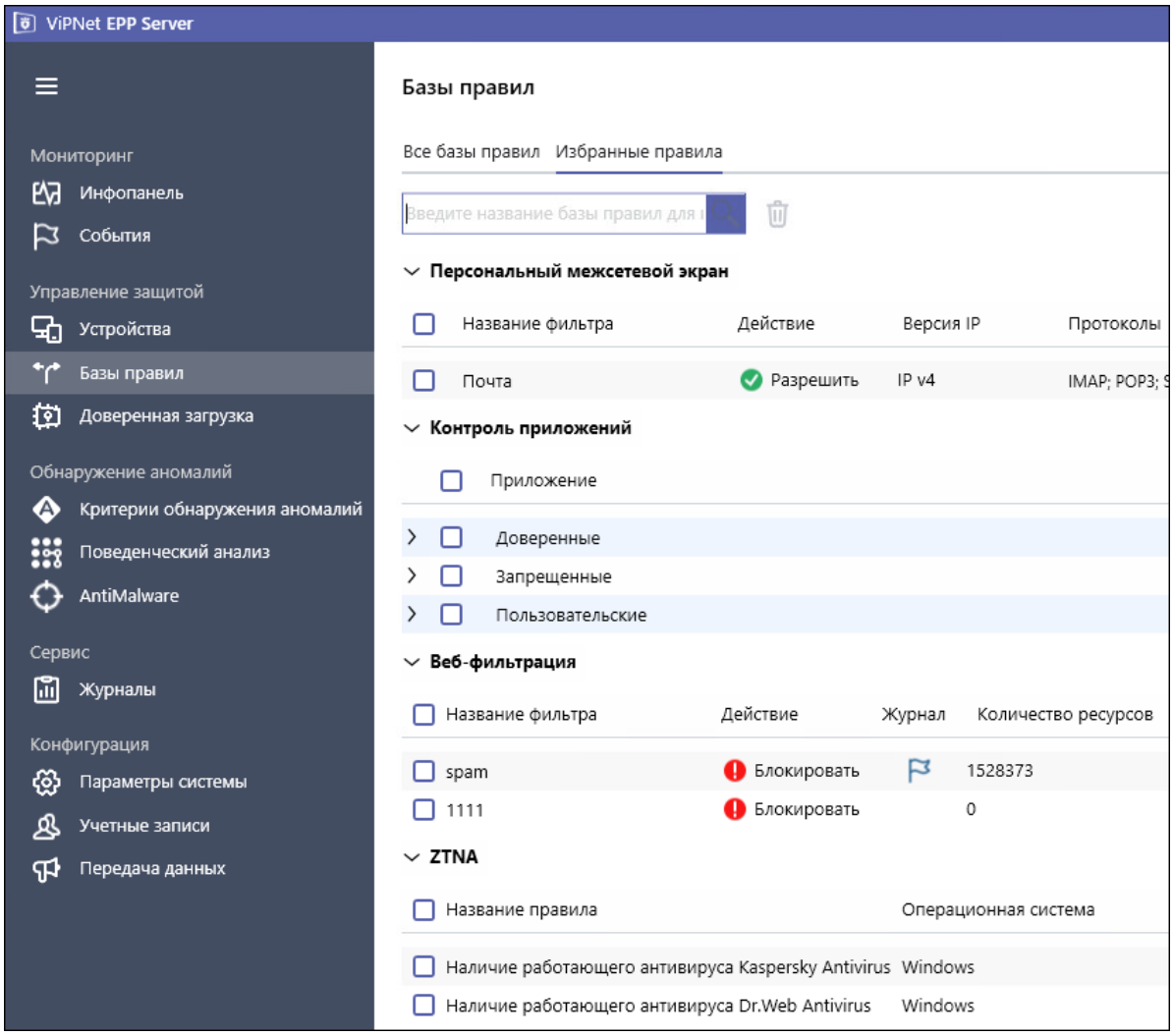


Рисунок 24. Список избранных правил

Чтобы просмотреть параметры определенного правила, в списке избранных правил дважды щелкните правило.

Чтобы удалить определенные правила из избранного:

1. В списке избранных правил выберите правила флажками.
2. Нажмите  и подтвердите удаление правил.

Настройка базы правил

После того как вы подключили защищаемые узлы, распределили их по группам и загрузили последнее обновление базы правил с сервера обновлений, назначьте эту базу правил группам узлов и при необходимости настройте ее в соответствии с требованиями обеспечения безопасности информации вашей организации.

Примечание. Настройкой базы правил 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.

Таблица 5. Порядок действий по настройке базы правил

	Действие	Ссылка
☐	Выберите группы узлов, на которые будет назначена база правил	Назначение базы правил группе узлов
☐	Измените режимы работы модулей защиты ViPNet EPP	Выбор режимов работы модулей защиты
☐	Настройте фильтры политик безопасности, а также глобальных справочников протоколов, расписаний, адресов и сетей	Управление фильтрацией трафика
☐	Настройте политики ZTNA	Управление политиками ZTNA
☐	Настройте глобальные списки контроля приложений и правила доступа приложений	Управление запуском и активностью приложений
☐	Настройте глобальные правила HIDS и HIPS и политики аудита	Управление обнаружением и предотвращением вторжений

После настройки базы правил и сохранения изменений создается ее новая версия, которая автоматически назначается и отправляется на выбранные группы узлов.

Назначение базы правил группе узлов

Чтобы ViPNet EPP Агент обнаруживал и предотвращал угрозы безопасности информации на защищаемых узлах, назначьте базу правил группам, в которые входят эти узлы:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, которую требуется назначить определенным группам, и на панели справа нажмите **Открыть в редакторе**.

4 При необходимости измените название базы правил в поле **Название**.

5 В разделе **Группы** выберите флажками группы защищаемых узлов, на которые будет назначена база правил.

6 Нажмите **Сохранить** или **Назад к EndPoint Protection**.

7 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Да.**

8 Убедитесь, что в списке баз правил созданная новая версия базы правил имеет статус активной (может появиться не сразу). Это свидетельствует о том, что база правил передана и применена как минимум на одном защищаемом узле, обнаружение и предотвращение угроз безопасности информации на этом узле происходит согласно правилам этой базы.

9 Выберите **Устройства** и проверьте, что для выбранных на шаге 5 групп в столбце **Версия базы правил** отображается номер версии созданной базы правил.

Чтобы проверить, что назначенная база правил применяется на всех защищаемых узлах группы:

1 На панели слева выберите **Устройства**.

2 Щелкните проверяемую группу защищаемых узлов.

3 В списке узлов группы дважды щелкните защищаемый узел — на панели справа на вкладке **Сведения** значения строк **Назначенная база правил** и **База правил на устройстве** должны совпадать.

4 Повторите шаг 3 для всех защищаемых узлов проверяемой группы.

Выбор режимов работы модулей защиты

В базе правил, загруженной на ViPNet EPP Сервер, режимы работы модулей защиты ViPNet EPP установлены по умолчанию (см. База правил (политика безопасности)).

Примечание. Мы не рекомендуем отключать предотвращение вторжений в базе правил, предназначенной для использования защищаемыми узлами с ViPNet EPP Linux Агент.

В зависимости от политики информационной безопасности вашей организации измените режимы работы модулей защиты:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните нужную базу правил и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Режимы работы**.

5 В разделах модулей защиты выберите нужные режимы. Выбранный режим будет отмечен .

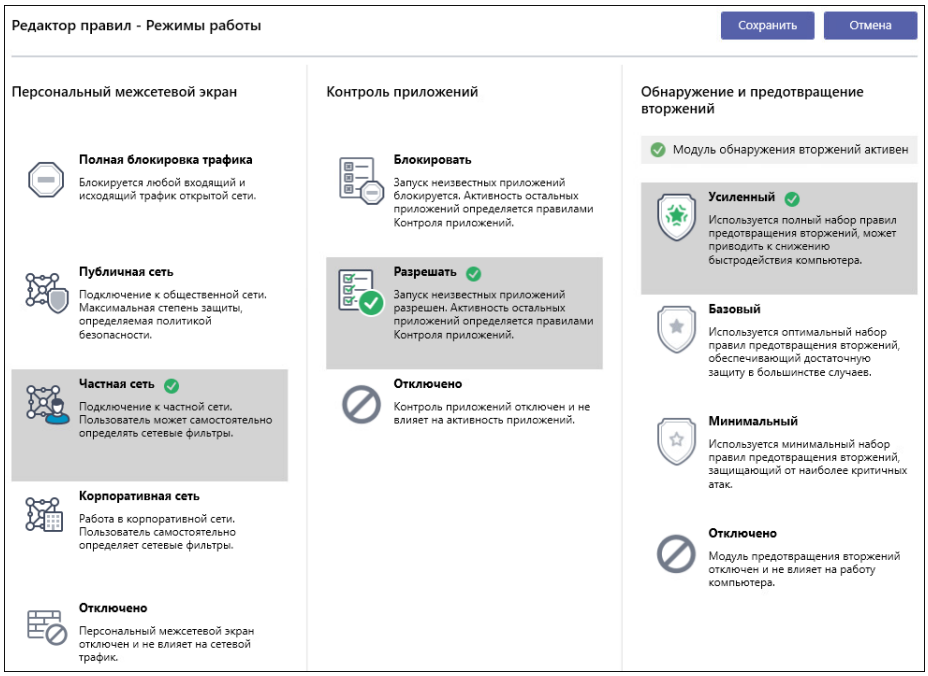


Рисунок 25. Выбор режимов работы для средств защиты

6 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Управление фильтрацией трафика

Настройка фильтров политик безопасности

Фильтры политик безопасности (см. Персональный межсетевой экран) применяются для обработки IP-пакетов сетевого трафика персональным межсетевым экраном ViPNet EPP Агент. Фильтры действуют в режимах публичной и частной сети базы правил, в которой они были созданы или изменены.

Для настройки фильтров политик безопасности доступны:

- Создание фильтра.
- Добавление фильтров в избранное для возможности использования в других базах правил.
- Импорт из избранного ранее добавленных фильтров в базу правил.

- Изменение параметров уже добавленных фильтров.
- Удаление фильтров.
- Настройка справочников.

Общий порядок управления фильтрами политики безопасности

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните нужную базу правил и на панели справа нажмите **Открыть в редакторе**.

4 На панели слева выберите **Персональный межсетевой экран**.

5 На панели слева выберите один из режимов — **Публичная сеть** или **Частная сеть**.

6 Просмотрите текущий список фильтров. Для каждого фильтра в списке отображаются параметры фильтрации IP-пакетов:

- Название фильтра.
- Статус — фильтр включен или выключен .
- Действие — фильтр разрешает или блокирует IP-пакеты с заданными настройками.
- Версия IP — версия IP-протокола: IP v4 или IP v6.
- Протокол — протоколы передачи IP-пакетов.
- Источник и Назначение — отправители и получатели IP-пакетов.
- Расписание — время действия фильтра.

7 Выполните действия в соответствии с описанием ниже.

8 Нажмите **Назад к редактору**.

9 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Создание фильтра политик безопасности

1 В разделе выбранного режима **Публичная сеть** или **Частная сеть** на панели вверху нажмите **Добавить** и в меню выберите **Создать новый фильтр**.

2 Следуйте указаниям мастера создания фильтра:

2.1 Выберите версию IP-протокола: IP v4 или IP v6. После перехода на следующий шаг изменить версию IP-протокола будет невозможно.

2.2 Определите действие фильтра при срабатывании:

- **Разрешить** — пропустить IP-пакет.
- **Блокировать** — блокировать IP-пакет.

2.3 Выберите режимы, в которых фильтр будет применяться. Вы можете создать фильтр как для одного режима, так и сразу для двух — **Публичная сеть** и **Частная сеть**.

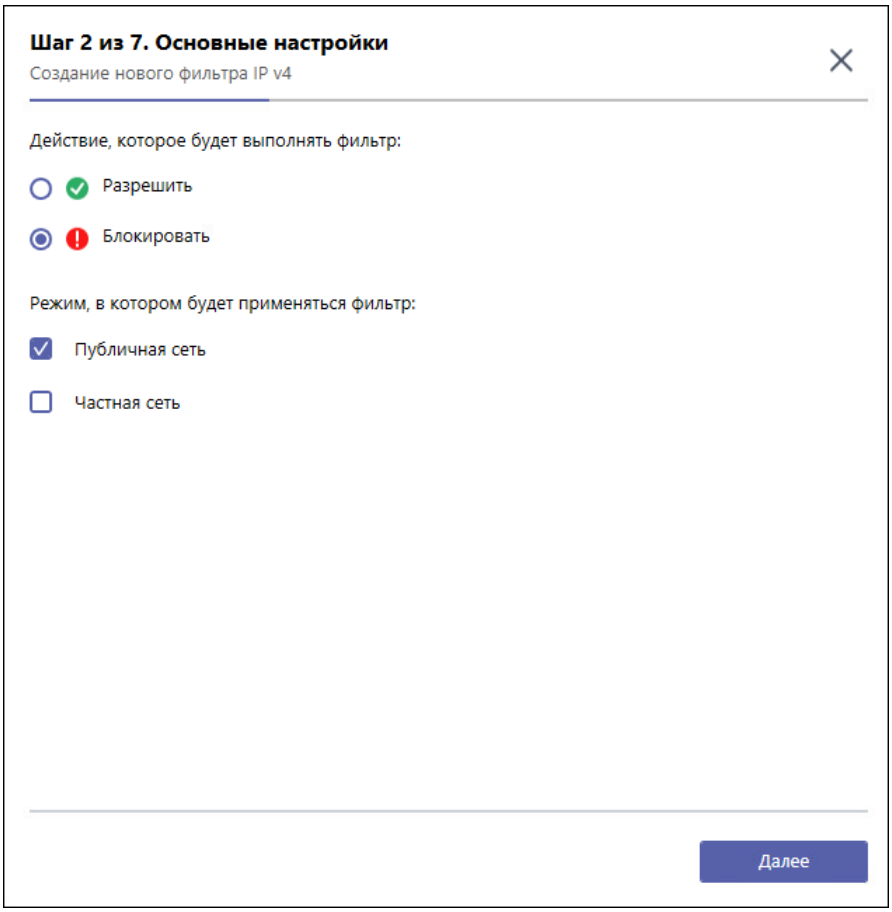


Рисунок 26. Настройка действия и режима применения фильтра

2.4 Укажите протоколы передачи IP-пакетов, включив нужные справочники. Доступны справочники, созданные для версии IP-протокола, выбранной на первом шаге мастера.

По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам.

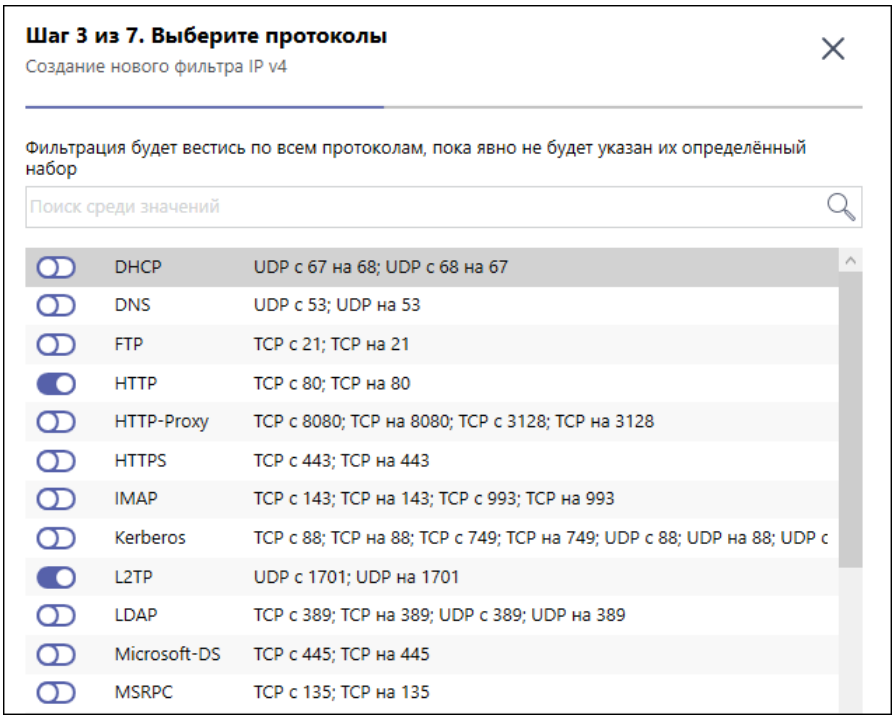


Рисунок 27. Выбор протоколов

2.5 На странице **Укажите адреса источников** задайте отправителей IP-пакетов. По умолчанию фильтр применяется к IP-пакетам с любыми адресами отправителя в формате выбранной на первом шаге версии IP-протокола. Для выбора определенных IP-адресов отправителей, на основании которых будет срабатывать фильтр, выберите нужные справочники адресов или введите IP-адреса. Доступны справочники, созданные для версии IP-протокола, выбранной на первом шаге мастера.

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

Чтобы указать IP-адреса, которых нет в справочнике, введите их в строку поиска в формате выбранной на первом шаге версии IP-протокола и нажмите .

Примечание. При указании диапазона IP-адресов разделяйте начальное и конечное значение диапазона дефисом. Например, 192.168.0.1-192.168.0.100. При указании нескольких IP-адресов или диапазонов IP-адресов разделяйте их запятыми. Например, 192.168.0.1-192.168.0.100,192.168.0.111,192.168.0.120.

Если IP-адреса не будут найдены в справочниках, нажмите **Добавить новый справочник адресов** и с помощью появившегося мастера создайте новый справочник адресов (см. Мастер «Новый справочник адресов»). В результате созданный справочник адресов будет добавлен в фильтр.

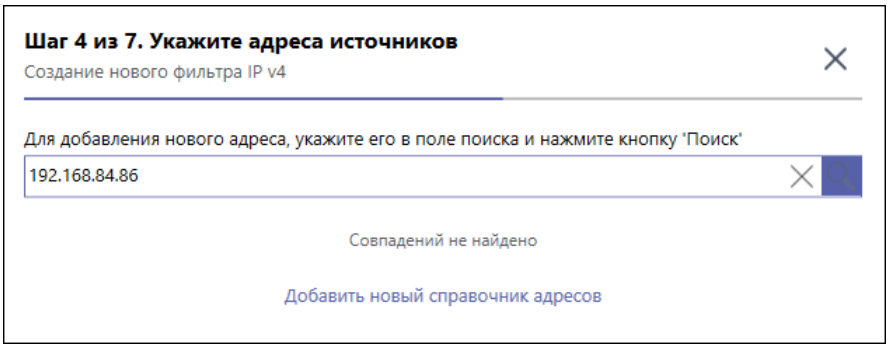


Рисунок 28. Добавление нового IP-адреса в фильтр

2.6 На странице **Укажите адреса назначений** задайте получателей IP-пакетов. По умолчанию фильтр применяется к IP-пакетам с любыми адресами получателя в формате выбранной на первом шаге версии IP-протокола. Для выбора определенных IP-адресов получателей, на основании которых будет срабатывать фильтр, выберите нужные справочники адресов или введите нужные IP-адреса точно таким же образом, что и адреса источников.

Внимание! Если адреса источников и адреса назначений оставлены по умолчанию (любые IP-адреса), персональный межсетевой экран ViPNet EPP Агент на защищаемом узле с ОС Windows будет разрешать или блокировать IP-пакеты со всеми адресами источника и назначения независимо от версии IP-протокола, выбранной на первом шаге мастера.

2.7 На странице **Установите расписание** назначьте справочники расписаний. Если расписания не установлены, фильтр политик безопасности будет действовать постоянно.

2.8 На странице **Подтверждение** введите название фильтра и проверьте заданные параметры.

2.9 Нажмите **Готово**.

В результате для указанных режимов будет создан фильтр политик безопасности.

3 Задайте порядок действия фильтров: переместите созданный фильтр в группе **Фильтры политик безопасности** на нужный уровень с помощью кнопок ↓ или ↑.

4 Нажмите **Применить**.

Изменение порядка применения фильтров

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

1 В разделе выбранного режима **Публичная сеть** или **Частная сеть** в списке фильтров политик безопасности выберите флажками фильтры, порядок применения которых необходимо изменить.

2 На панели вверху нажмите ↑ или ↓ для перемещения выбранных фильтров в списке.

3 Нажмите **Применить**.

Добавление фильтров в избранное

В избранном сохраняются все параметры фильтра политик безопасности, кроме статуса. При сохранении фильтра политик безопасности в избранном проверяется его уникальность — набор параметров: название фильтра, используемые протоколы, адреса источников и назначений, расписания. Идентичные фильтры политик безопасности не сохраняются.

Чтобы сохранить в избранном определенные фильтры политик безопасности текущей версии базы правил, например фильтры работы с корпоративными ресурсами:

1. В разделе выбранного режима **Публичная сеть** или **Частная сеть** в списке фильтров политик безопасности выберите флажками фильтры, которые вы хотите сохранить в избранном.
2. На панели вверху нажмите **Добавить в избранное**.
3. Если обнаружены идентичные фильтры, появится сообщение с их списком. Для продолжения нажмите **ОК**.
4. Дождитесь завершения операции и нажмите **ОК**.

В результате сохраненные фильтры будут отображаться в разделе **Базы правил** на вкладке **Избранные правила** > **Персональный межсетевой экран** (см. Просмотр и удаление избранных правил).

Импорт фильтров из избранного

Чтобы добавить фильтры политик безопасности, ранее сохраненные в избранном, в текущую версию базы правил:

1. В разделе выбранного режима **Публичная сеть** или **Частная сеть** на панели вверху нажмите **Добавить**.
2. Выберите **Импортировать из избранного** и следуйте указаниям мастера импорта фильтра:
   - **2.1** В окне **Импорт избранных фильтров** выберите флажками нужные фильтры.
   - **2.2** Нажмите **Импортировать**.
   - **2.3** При обнаружении фильтров, уже имеющихся в базе правил, появится сообщение о наличии дубликатов. Выберите, нужно импортировать дубликаты фильтров или нет. Чтобы импортировать дубликаты, нажмите **Нет** и откажитесь от исключения дубликатов из импортируемого набора. По завершении импорта фильтры с одинаковыми названиями рекомендуем переименовать.
3. Установите порядок действия фильтров, переместив импортированные фильтры на нужный уровень с помощью кнопок ↓ или ↑.
4. Нажмите **Применить**.

В результате фильтры будут добавлены в базу правил со статусом **Включено**.

Изменение параметров фильтров

1 В разделе выбранного режима **Публичная сеть** или **Частная сеть** в списке фильтров политик безопасности дважды щелкните нужный фильтр или предварительно на панели вверху воспользуйтесь поиском по названию фильтра.

2 На панели справа на вкладке **Основные** вы можете изменить активность фильтрации, название и действие фильтра.

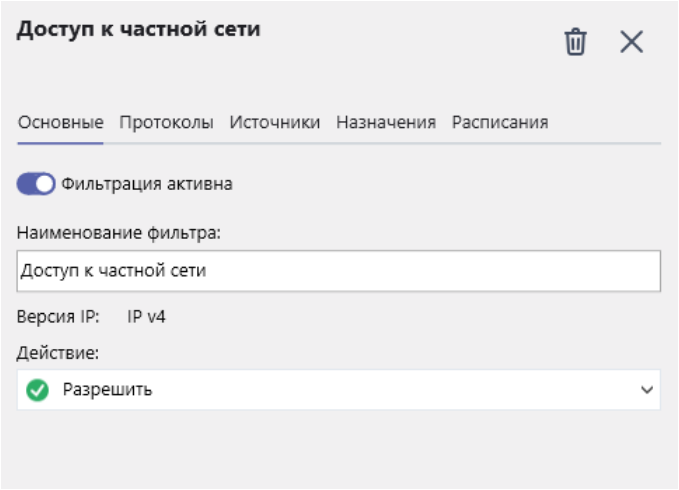


Рисунок 29. Дополнительная панель редактирования фильтра политик безопасности

3 На вкладках **Протоколы**, **Источники**, **Назначения** и **Расписания** внесите необходимые изменения.

4 Нажмите **OK**, чтобы сохранить изменения.

5 Нажмите **Применить**.

Удаление фильтров

1 В разделе выбранного режима **Публичная сеть** или **Частная сеть** в списке фильтров политик безопасности выберите флажками фильтры.

2 На панели вверху нажмите .

3 Подтвердите удаление.

4 Нажмите **Применить**.

Настройка справочников

Справочники позволяют упростить процессы создания и изменения сетевых фильтров.

Чтобы создать справочник:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните нужную базу правил и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Персональный межсетевой экран**.

5 На панели слева выберите тип создаваемого справочника:

- **Протоколы** и на панели вверху нажмите **Добавить протоколы**.
- **Адреса и сети** и на панели вверху нажмите **Добавить адреса**.
- **Расписания** и на панели вверху нажмите **Добавить расписание**.

6 Следуйте указаниям мастера создания справочника выбранного вида:

- Мастер «Новый справочник протоколов».
- Мастер «Новый справочник адресов».
- Мастер «Новый справочник расписаний».

В результате будет создан справочник выбранного вида.

7 Нажмите **Применить**.

8 Чтобы выйти из настроек персонального межсетевого экрана, нажмите **Назад к редактору**.

9 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Чтобы изменить настройки справочника или удалить справочник:

1 На панели слева выберите вид справочника:

- **Протоколы**.
- **Адреса и сети**.
- **Расписания**.

2 В списке справочников дважды щелкните нужный справочник или предварительно на панели вверху воспользуйтесь поиском по названию справочника.

3 На панели справа на вкладке **Основные** вы можете изменить название справочника, а также просмотреть применение справочника в сетевых фильтрах.

4 На вкладках **Состав** и **Исключения** внесите необходимые изменения — удалите или добавьте параметры. Для добавления новых параметров нажмите **Добавить**, внесите изменения и нажмите **Сохранить**.

5 Нажмите **ОК**, чтобы сохранить все изменения.

6 Чтобы удалить справочник, дважды щелкните строку справочника в списке и на панели справа нажмите . Чтобы удалить сразу несколько справочников, выберите их флажками и на панели справа нажмите . Подтвердите удаление. В результате справочники будут удалены, если они не используются в сетевых фильтрах.

7 Нажмите **Применить**.

8 Сохраните изменения и отправьте на защищаемые узлы в соответствии с шагами 9-10 предыдущего сценария.

Мастер «Новый справочник протоколов»

В мастере **Новый справочник протоколов**:

1 Выберите версию IP-протокола: IP v4 или IP v6, для которой будет создан справочник. После перехода на следующий шаг изменить версию IP-протокола будет невозможно.

2 В зависимости от выбранной версии IP-протокола выберите один из предложенных объектов справочника и настройте его:

- Выберите **Протокол TCP**:
  - Введите порты источника, приемника.
  - Укажите команды протокола HTTP, которые должны быть запрещены.
  - Укажите типы файлов, в виде которых должна быть запрещена передача мобильного кода.
  - Нажмите **Сохранить**.

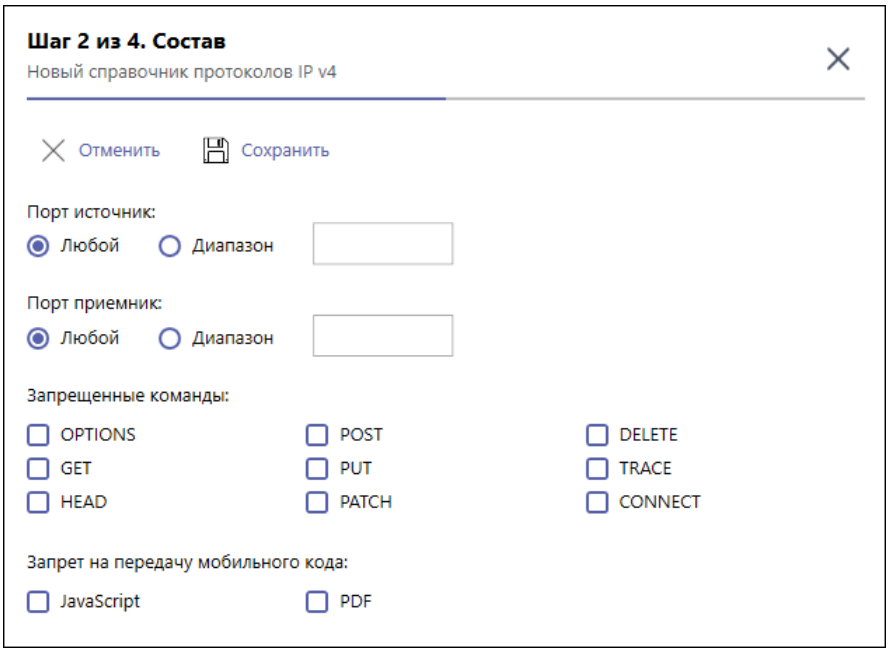


Рисунок 30. Настройка параметров протокола TCP

- Выберите **Протокол UDP** и:

- Введите порты источника, приемника.
- Нажмите **Сохранить**.

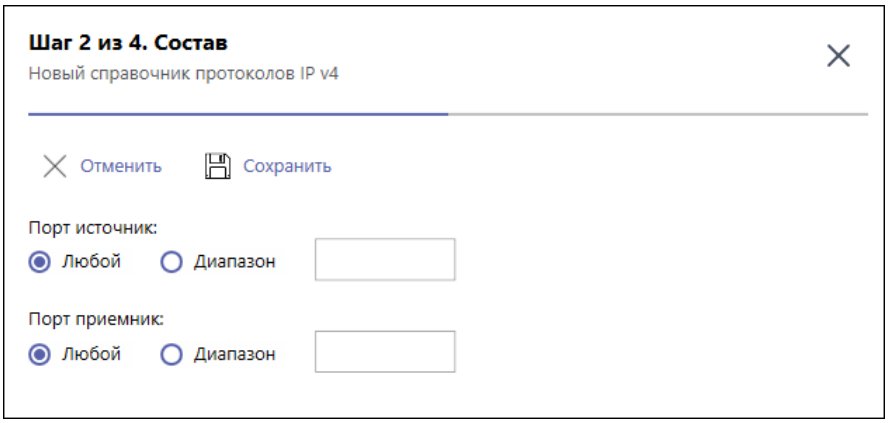


Рисунок 31. Настройка параметров протокола UDP

- Щелкните **Сообщение ICMP** и:
  - Выберите в списке нужный тип ICMP-сообщений и при необходимости их код.
  - Нажмите **Сохранить**.



Рисунок 32. Настройка параметров протокола ICMP

- Щелкните **Сообщение ICMPv6**. Этот справочник доступен только в случае выбора на первом шаге мастера версии IP-протокола IP v6.
  - Выберите в списке нужный тип ICMPv6-сообщений и при необходимости их код.
  - Нажмите **Сохранить**.

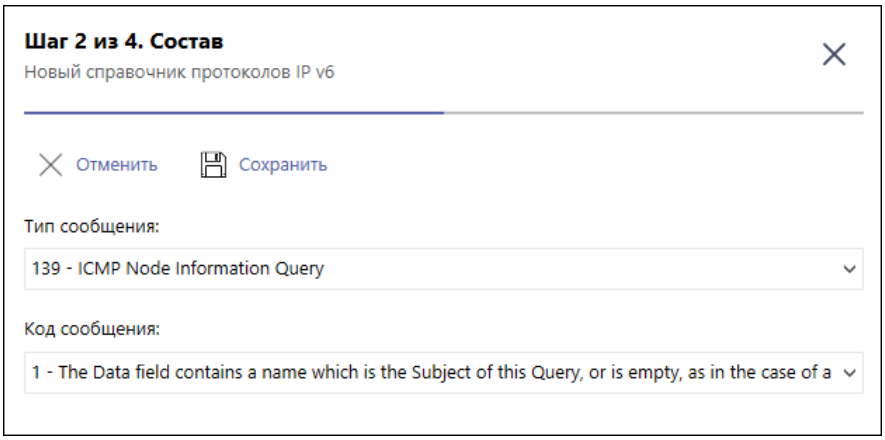


Рисунок 33. Настройка параметров протокола ICMPv6

3 Чтобы выбрать еще один объект справочника и настроить его, нажмите **Добавить** и повторите действия шага 2 текущего сценария.

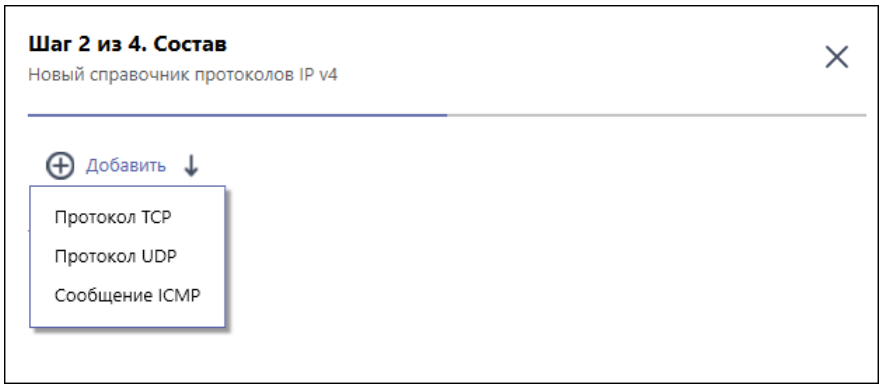


Рисунок 34. Повторный выбор объекта справочника для версии протокола IP v4

4 Задайте объекты исключений справочника, повторив действия шагов 2 и 3 текущего сценария.

5 Укажите название нового справочника протоколов, а также проверьте состав и исключения справочника.

6 Нажмите **Готово**.

Мастер «Новый справочник адресов»

В мастере **Новый справочник адресов**:

1 Выберите версию IP-протокола: IP v4 или IP v6, для которой будет создан справочник. После перехода на следующий шаг изменить версию IP-протокола будет невозможно.

2 В зависимости от выбранной версии IP-протокола выберите один из предложенных объектов справочника и настройте его:

- Выберите **Адрес IP v4** и:
  - Введите IP-адрес, подсеть или диапазон адресов.
  - Нажмите **Сохранить**.

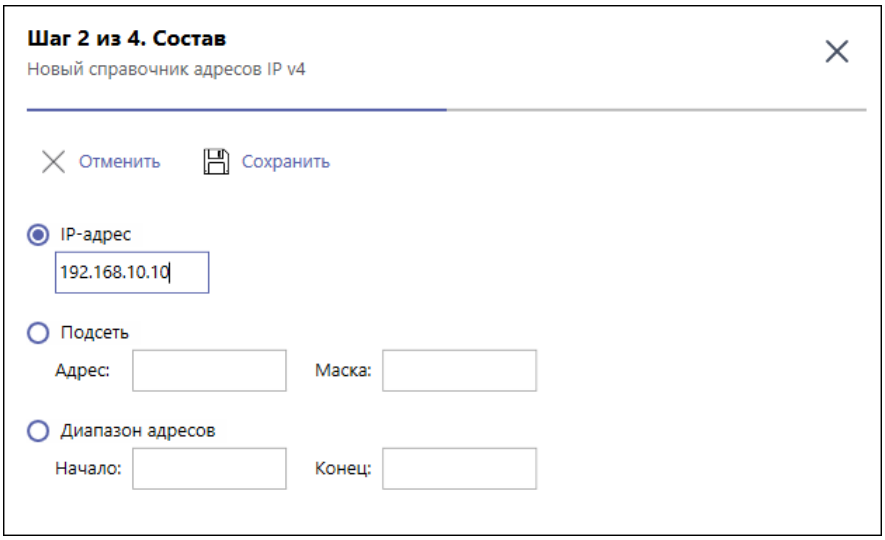


Рисунок 35. Настройка IPv4-адресов

- Выберите **Адрес IP v6** и:
  - Введите адрес в формате IP v6, например `2001:db80:0000:a000:c000:d000:b000:e2f0`.
  - Введите длину префикса подсети.
  - Нажмите **Сохранить**.

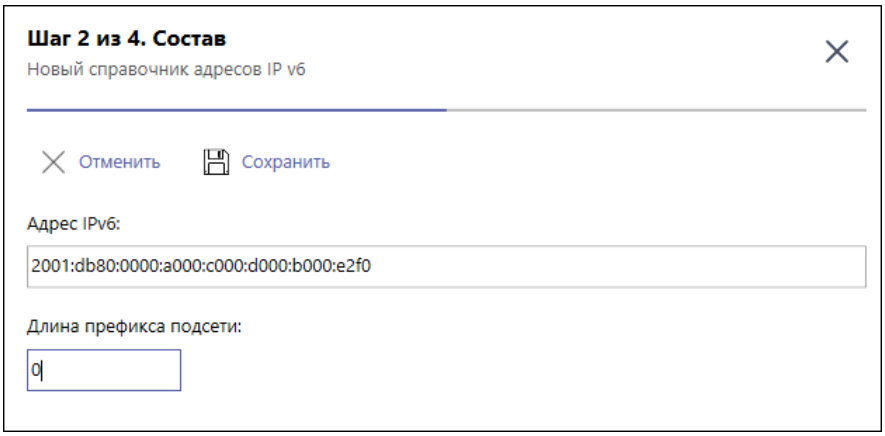


Рисунок 36. Настройка IPv6-адресов

3 Чтобы выбрать еще один объект справочника и настроить его, нажмите **Добавить** и повторите действия шага 2 текущего сценария.

4 Задайте объекты исключений справочника, повторив действия шагов 2 и 3 текущего сценария.

5 Укажите название нового справочника адресов, а также проверьте состав и исключения справочника.

6 Нажмите **Готово**.

Мастер «Новый справочник расписаний»

В мастере **Новый справочник расписаний**:

1 Выберите **Новое расписание** и:

1.1 Выберите тип расписания (выполнять ежедневно или еженедельно) и укажите параметры расписания.

1.2 Нажмите **Сохранить**.

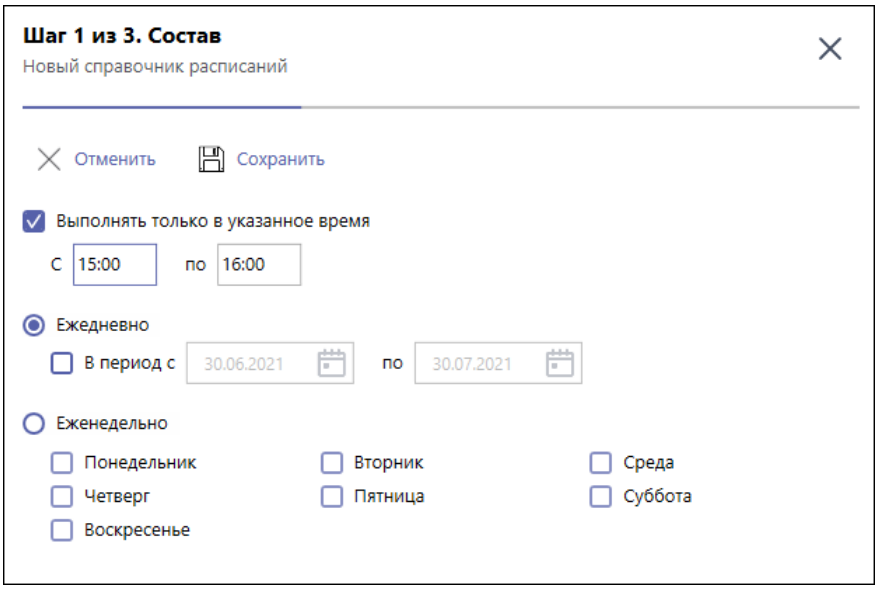


Рисунок 37. Настройка параметров расписания

2 Чтобы выбрать еще один объект справочника и настроить его, нажмите **Добавить** и повторите действия шага 1 текущего сценария.

3 Задайте объекты исключений справочника, повторив действия шагов 1 и 2 текущего сценария.

4 Укажите название нового справочника расписаний, а также проверьте состав и исключения справочника.

5 Нажмите **Готово**.

Настройка источника получения фильтров политик безопасности

На защищаемом узле в ViPNet EPP Агент в качестве фильтров политик безопасности открытой сети могут использоваться сетевые фильтры, полученные из одного из следующих источников (см. Персональный межсетевой экран):

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

Примечание. Возможность передачи фильтров политик безопасности открытой сети в ViPNet EPP Агент из ViPNet Prime Policy Management будет реализована в сертифицированной версии ViPNet Client 5.

По умолчанию в ViPNet EPP Агент используются фильтры, полученные из ViPNet EPP Сервер. Вы можете изменить источник получения фильтров. После смены источника получения фильтров политик безопасности на ViPNet Policy Manager (ViPNet Prime Policy Management) в ViPNet EPP Агент будут игнорироваться фильтры политик безопасности ViPNet EPP Сервер независимо от наличия фильтров ViPNet Policy Manager (ViPNet Prime Policy Management).

Чтобы в ViPNet EPP Агент начали использоваться фильтры политик безопасности, полученные из ViPNet Policy Manager (ViPNet Prime Policy Management):

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите **Базы правил**.
3. В списке баз правил дважды щелкните нужную базу правил и на панели справа нажмите **Открыть в редакторе**.
4. На панели слева выберите **Персональный межсетевой экран**.
5. На панели слева выберите — **Дополнительные опции**.
6. Включите **Использовать фильтры политик безопасности ViPNet Prime Policy Management/ViPNet Policy Manager**.
7. Чтобы выйти из настроек персонального межсетевого экрана, нажмите **Назад к редактору**.
8. Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Чтобы в ViPNet EPP Агент снова начали использоваться фильтры политик безопасности, полученные из ViPNet EPP Сервер, выключите **Использовать фильтры политик безопасности ViPNet Prime Policy Management/ViPNet Policy Manager**.

Управление политиками ZTNA

Политики ZTNA (см. Сетевой доступ с нулевым доверием (ZTNA)) будут применяться на защищаемых узлах, если они включены и настроены правила ZTNA. По умолчанию политики ZTNA выключены.

Политики ZTNA действуют в пределах одной базы правил и задаются набором правил. По умолчанию база правил уже содержит ряд правил для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux. Правила для антивирусов удалить нельзя.

Для управления политиками ZTNA доступны:

- Включение политик ZTNA.
- Добавление и настройка новых правил (см. Добавление и настройка новых правил политики ZTNA).
- Настройка правил для антивирусов.
- Добавление правил в избранное для возможности использования в других базах правил.
- Импорт из избранного ранее добавленных правил в базу правил.
- Изменение параметров уже добавленных правил, включение и выключение правил.
- Удаление ненужных правил.

Общий порядок управления политиками ZTNA

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить политику ZTNA, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **ZTNA**.

5 Выберите вкладку **Windows** (для настройки ZTNA для защищаемых узлов с ОС Windows) или **Linux** (для настройки ZTNA для защищаемых узлов с ОС Linux).

6 Внесите необходимые изменения в соответствии со сценариями ниже или добавьте и настройте новые правила ZTNA (см. Добавление и настройка новых правил политики ZTNA).

Все новые или измененные правила будут выделены **жирным** шрифтом до момента сохранения.

7 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Начало использования политики ZTNA на защищаемом узле

1 Включите **Включить политики ZTNA**.

2 Добавьте и настройте правила (см. Добавление и настройка новых правил политики ZTNA).

3 Настройте правила для антивирусов и другие уже добавленные правила (см. ниже).

Настройка правил для антивирусов политики ZTNA

1 Включите  **Наличие работающего антивируса Kaspersky Antivirus** или **Наличие работающего антивируса Dr.Web Antivirus**. Можно включить только одно правило.

2 Наведите указатель на строку с названием включенного правила и справа от статуса правила нажмите  .

3 На панели слева выберите **Актуальность базы антивируса**, выберите **Включить проверку актуальности баз антивируса** и укажите период времени в днях, через который нужно проверять актуальность баз. По умолчанию установлен период 2 дня.

4 При необходимости настройте другие параметры правила аналогично описанию в сценарии добавления и настройки правил (см. Добавление и настройка новых правил политики ZTNA).

5 Нажмите **Сохранить**.

Добавление правил в избранное

В избранном сохраняются все параметры правил политик ZTNA, кроме статуса. При сохранении правил в избранном проверяется на уникальность набор параметров: название правила, для какой ОС предназначено, а для правил антивирусов дополнительно — параметр **Актуальность базы антивируса**. Идентичные правила не сохраняются. Правила антивирусов с отличающимся значением параметра **Актуальность базы антивируса** будут сохранены и переименованы — к названию правил добавится цифра (1), либо уже имеющаяся цифра увеличится на единицу. Например, правило **Наличие работающего антивируса Dr.Web Antivirus** будет переименовано в **Наличие работающего антивируса Dr.Web Antivirus (1)**. Если требуется сохранить в избранное правило, которое удовлетворяет требованиям идентичности, но другие параметры у него различаются, сначала переименуйте правило в базе правил, либо удалите старое правило из избранного.

Чтобы сохранить в избранном определенные правила текущей версии базы правил:

1 В списке правил выберите флажками правила, которые вы хотите сохранить в избранном.

2 На панели вверху нажмите **Добавить в избранное**.

3 Если обнаружены идентичные правила, появится сообщение с их списком. Для продолжения нажмите **OK**.

4 Дождитесь завершения операции и нажмите **OK**.

В результате сохраненные правила будут отображаться в разделе **Базы правил** на вкладке **Избранные правила** > **ZTNA** (см. Просмотр и удаление избранных правил).

Импорт правил из избранного в базу правил

При импорте правил из избранного:

- Правила из избранного (кроме правил антивирусов) добавляются в список правил со статусом **Включено**. При импорте проверяются дубли по набору параметров: название правила, для какой ОС предназначено. При наличии дублей вы сможете выбрать импортировать их из избранного или отказаться от их импорта.
- Правила антивирусов всегда перезаписываются правилами антивирусов из избранного, результирующее правило будет иметь статус **Выключено**.

Чтобы добавить правила ZTNA, ранее сохраненные в избранном, в текущую версию базы правил:

1 В списке правил на панели вверху нажмите **Импортировать из избранного**.

1.1 В окне **Импорт избранных правил** выберите флажками правила и нажмите **Импортировать**.

1.2 При обнаружении правил, уже имеющихся в базе правил, появится сообщение о наличии дубликатов. Чтобы импортировать дубликаты из избранного, нажмите **Нет** и откажитесь от исключения дубликатов из набора. Импортированные дубликаты правил будут добавлены в список правил и переименованы аналогично сценарию добавления правил в избранное (см. выше).

Для продолжения нажмите **OK**.

1.3 Нажмите **OK**.

2 Нажмите **Сохранить**.

Изменение и удаление параметров ранее добавленных правил политики ZTNA

1 В списке правил включите **Включено** или выключите **Выключено** нужные правила политики ZTNA. Чтобы включить или выключить сразу несколько правил, выберите их флажками и нажмите **Включить** или **Выключить**.

2 Чтобы изменить параметры правила, наведите указатель на строку с названием правила и справа от статуса правила нажмите .

2.1 Чтобы изменить название правила, на панели слева выберите **Сведения** и внесите изменения в название.

2.2 Чтобы изменить настройки параметров правила, на панели слева выберите название типа параметра и:

2.2.1 В колонке статус для выбранного параметра включите **Включено** или исключите **Выключено** проверку параметра. Чтобы включить или исключить сразу несколько параметров, выберите их флажками и на панели вверху нажмите **Включить** или **Исключить**.

2.2.2 Чтобы изменить настройки параметра, наведите указатель на строку с названием параметра и справа от его статуса нажмите . Внесите изменения аналогично описанию в сценарии добавления и настройки правил (см. Добавление и настройка новых правил политики ZTNA).

2.2.3 Чтобы удалить параметр из правила, наведите указатель на строку с названием параметра, справа от его статуса нажмите  и подтвердите удаление. Чтобы удалить сразу несколько параметров, выберите их флажками и на панели вверху нажмите  .

2.2.4 Нажмите **Сохранить**.

Удаление ранее добавленных правил политики ZTNA

В списке правил наведите указатель на строку с названием правила, справа от статуса правила нажмите  и подтвердите удаление. Чтобы удалить сразу несколько правил, выберите их флажками и на панели вверху нажмите  .

Добавление и настройка новых правил политики ZTNA

Чтобы добавить и настроить новые правила политики ZTNA:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите  **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить политику ZTNA, и нажмите  **Открыть в редакторе**.

4 На панели слева выберите  **ZTNA**.

5 Выберите вкладку **Windows** (для настройки ZTNA для защищаемых узлов с ОС Windows) или **Linux** (для настройки ZTNA для защищаемых узлов с ОС GNU/Linux).

6 Чтобы добавить новое правило, нажмите  **Добавить**, введите название правила и нажмите **Сохранить**.

В список правил добавиться правило со статусом  **Включено**. Чтобы правило применялось на узле, настройте параметры правила.

7 Чтобы настроить параметры правила, наведите указатель на строку с названием правила и справа от статуса правила нажмите  .

8 Чтобы настроить проверку правилом ZTNA наличия установленного обновления ОС Windows на защищаемом узле, на панели слева выберите **Обновления ОС** и на панели вверху:

- Для создания нового параметра правила вручную нажмите  **Добавить** и выберите **Создать новое правило**:
  - Выберите выпуск, версию и сборку ОС из списка доступных или укажите свой вариант. По умолчанию выбраны все выпуски ОС Windows и любые значения версий и сборок. Т.е. правило будет проверяться на защищаемых узлах со всеми ОС Windows.

Для указания своего варианта в списке **Операционная система** выберите определенный выпуск ОС,в списках **Версия ОС** и **Сборка ОС** выберите **Другая** и в полях укажите значения в соответствии с требованиями, указанными на странице.

- В разделе **Обновления ОС** нажмите  и введите системные обновления ОС Windows, установку которых нужно отслеживать. Формат ввода: `KB<цифры>` или `<цифры>`. При вводе нескольких обновлений разделяйте их запятой или пробелом. Например, `KB2669970, 4338825`. Нажмите **Сохранить**.

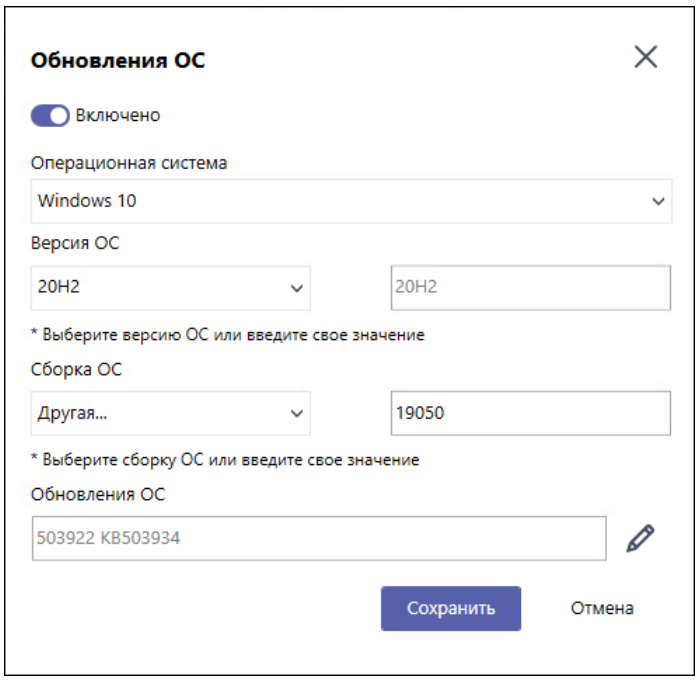


Рисунок 38. Пример настройки обновлений Windows вручную

- Нажмите **Сохранить**.

- Для добавления параметров правила с помощью импорта из файла формата CSV, выгруженного из Windows Server Update Services, нажмите  **Добавить** и выберите **Перезаписать из файла**.

  - Выберите файл формата CSV. Файл должен соответствовать требованиям:
    - Кодировка UTF-8.
    - В качестве разделителей внутри записи используются запятые. Разделитель между записями — перенос строки.
    - Файл содержит заголовок с указаниями наименований атрибутов.
      - Обязательные атрибуты (порядок не важен): ProductFamilyTitles; ProductTitles; Title; KnowledgebaseArticles;
      - Остальные атрибуты не важны.
    - Строковые данные могут быть заключены в "".

  Если файл корректный, на основе импортированных данных из файла будут созданы параметры для проверки обновления ОС правила ZTNA.

Внимание! При успешном импорте все ранее созданные параметры типа **Обновления ОС** в составе правила ZTNA будут заменены новыми данными.

9 Чтобы настроить другие параметры правила, на панели слева выберите тип параметра, который вы хотите добавить для проверки на защищаемом узле правилом ZTNA, на панели вверху нажмите **Добавить**:

9.1 При настройке для защищаемых узлов с ОС Windows:

- При выборе **Программное обеспечение** введите имя ПО и выберите в каком состоянии должно быть это ПО на защищаемом узле: **Установлено** или **Не установлено**. Имя ПО должно совпадать с именем в **Программы и компоненты Windows**.

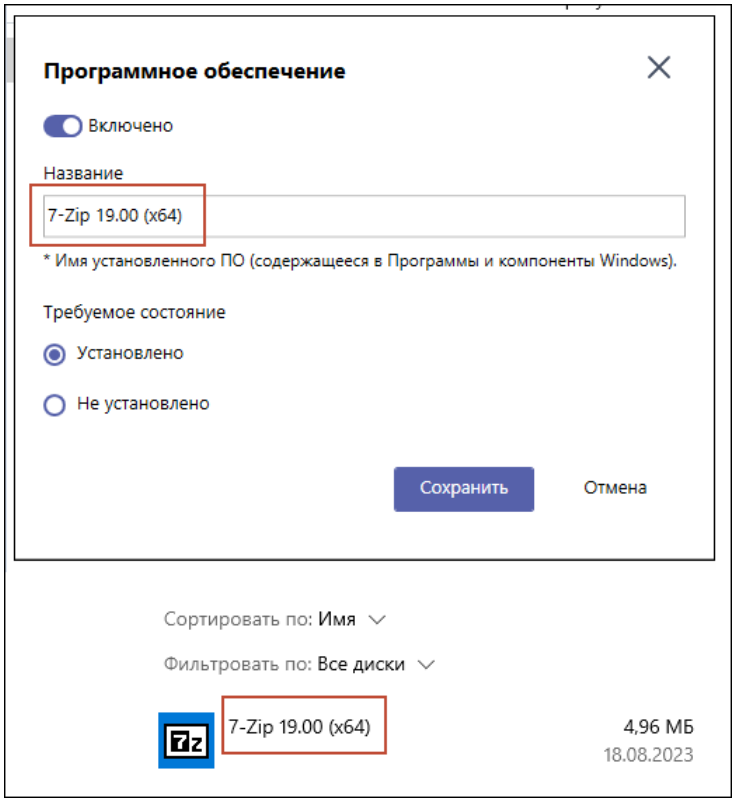


Рисунок 39. Пример задания названия программного обеспечения

- При выборе **Процессы** введите имя процесса и выберите в каком состоянии должен быть этот процесс на защищаемом узле: **Запущен** или **Не запущен**. Имя процесса должно совпадать с именем в **Диспетчер задач** > **Подробности**, но указываться без расширения.

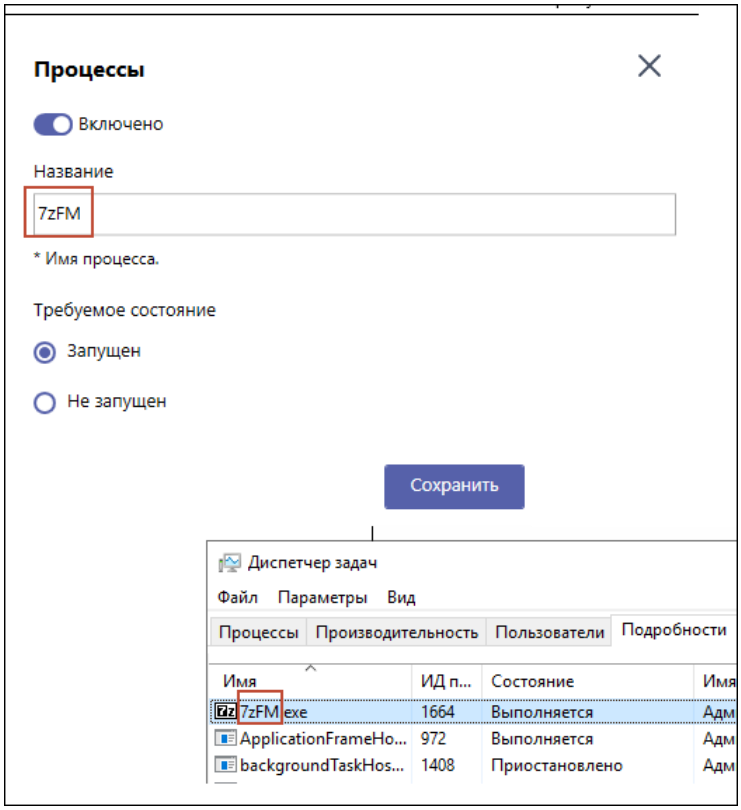


Рисунок 40. Пример задания названия процесса

- При выборе **Службы** введите имя службы и выберите в каком состоянии должна быть эта служба на защищаемом узле: **Выполняется** или **Не выполняется**. Имя службы должно совпадать с именем в **Службы** (`services.msc`).

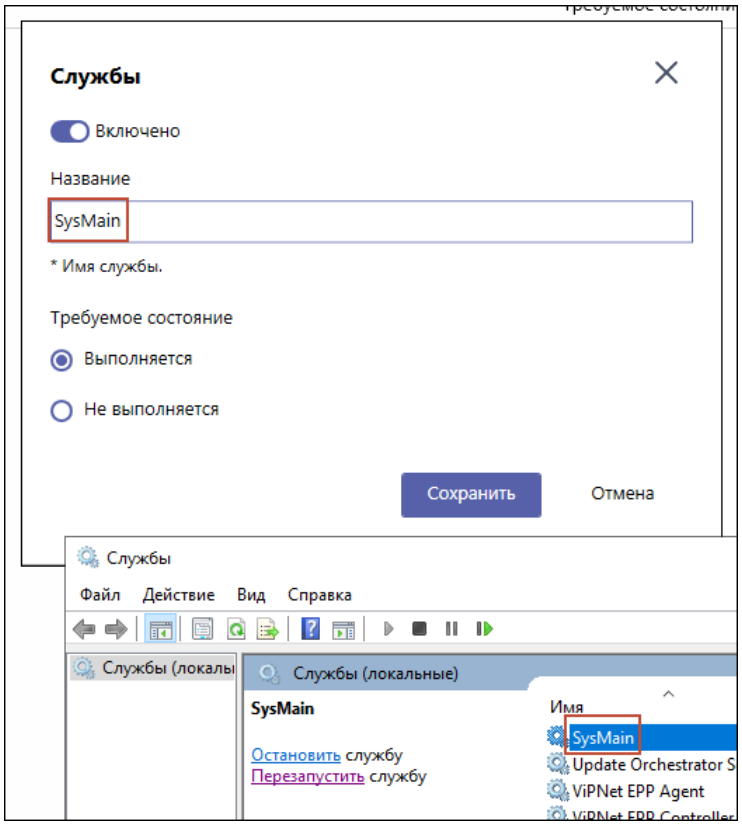


Рисунок 41. Пример задания названия службы

- При выборе **Файлы** введите полный путь к файлу, например, `C:\Program Files\Test\test.exe`. Допускается указание сетевого пути к файлу, например `\\Server\Test\test.exe`. Путь должен содержать не более 1000 символов.

  Выберите состояние файла на защищаемом узле: **Присутствует** или **Отсутствует**.

- При выборе **Реестр** введите путь к ключу или параметру реестра и задайте критерии для сравнения. Путь должен содержать не более 1000 символов. Можно использовать полное и сокращенное название ключей корневого уровня реестра, например, `HKLM\SOFTWARE\test\paramtest`, за исключением `HKEY_CURRENT_USER` (`HKCU`). Вместо `HKEY_CURRENT_USER` (`HKCU`) следует указывать `HKEY_USERS` и идентификатор конкретного пользователя. При задании критериев соблюдайте правила:

  - **Существует** или **Не существует**. Критерии можно задавать для любых типов значений реестра. В этом случае путь должен быть указан до параметра реестра.

- **Равно** или **Не равно**. Критерии можно задавать только для целочисленных и строковых значений параметров реестра. В этом случае путь должен быть указан до параметра реестра. После выбора критерия укажите значение для сравнения в десятичной системе счисления. Для критерия **Равно** для строкового значения параметра можно оставить пустое значение для сравнения.

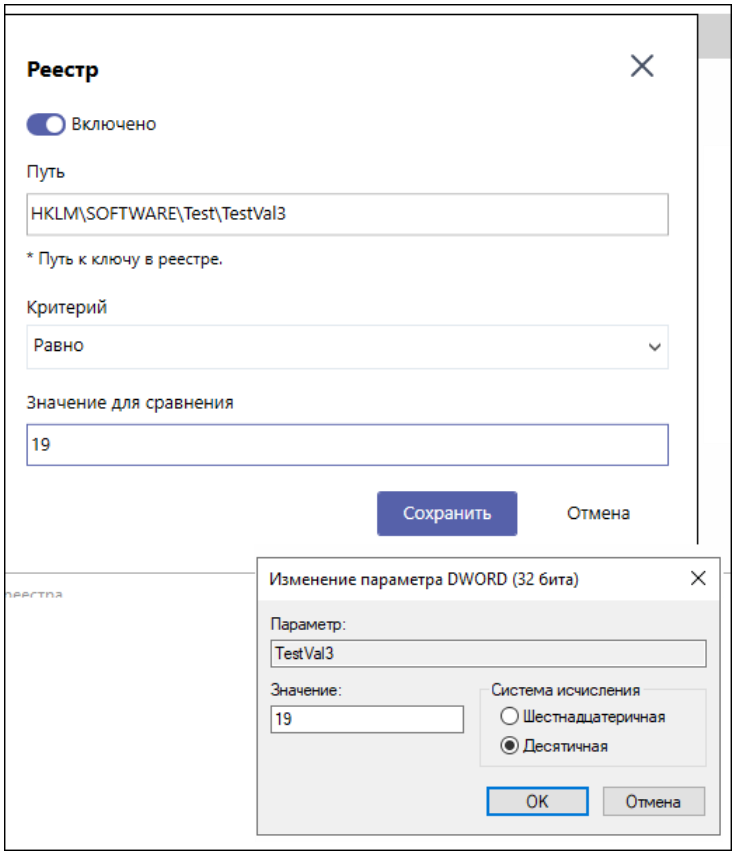


Рисунок 42. Пример задания параметров реестра

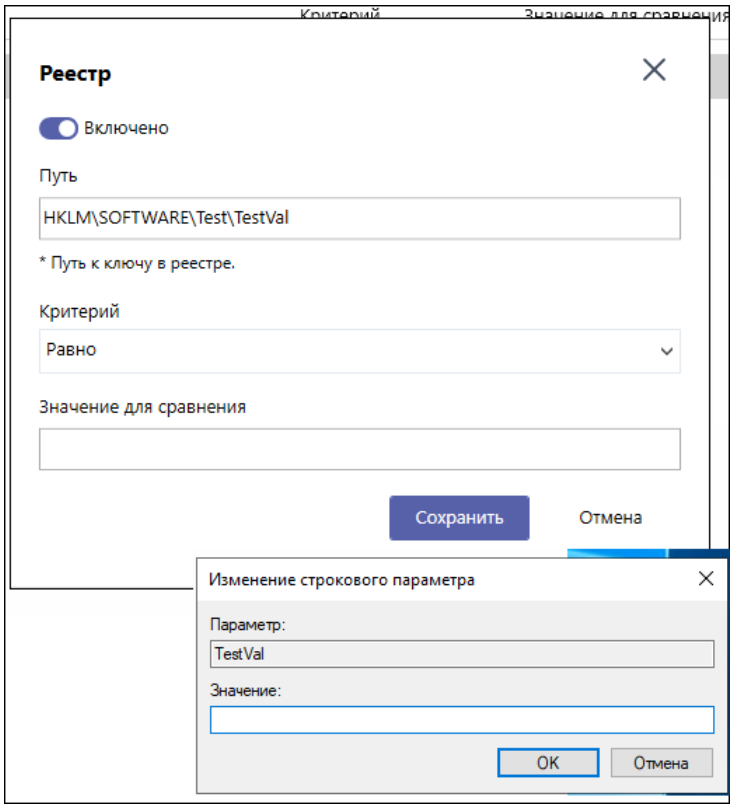


Рисунок 43. Пример задания параметров реестра с нулевым значением

- **Содержит** или **Не содержит**. Критерии можно задавать только для строковых значений параметров реестра. В этом случае путь должен быть указан до параметра реестра. После выбора критерия укажите значение для сравнения.

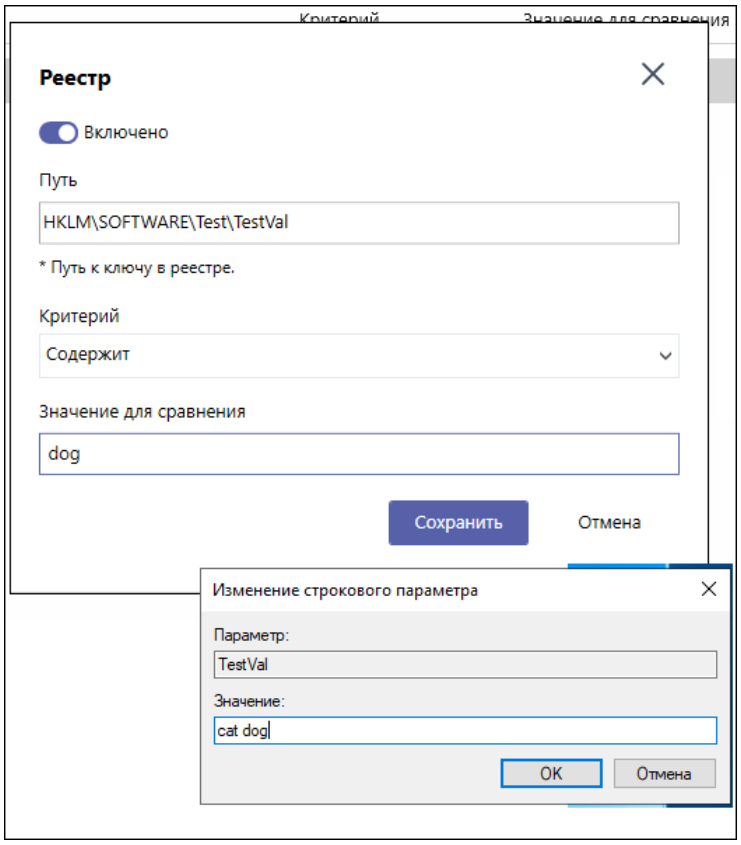


Рисунок 44. Пример задания параметров реестра

- **Меньше**, **Больше**, **Меньше или равно**, **Больше или равно**. Критерии можно задавать для целочисленных значений параметров реестра. В этом случае путь должен быть указан до параметра реестра. После выбора критерия укажите значение для сравнения в десятичной системе счисления.

9.2 При настройке для защищаемых узлов с ОС GNU/Linux:

- При выборе **Службы systemd** введите имя службы systemd и выберите в каком состоянии должна быть эта 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.

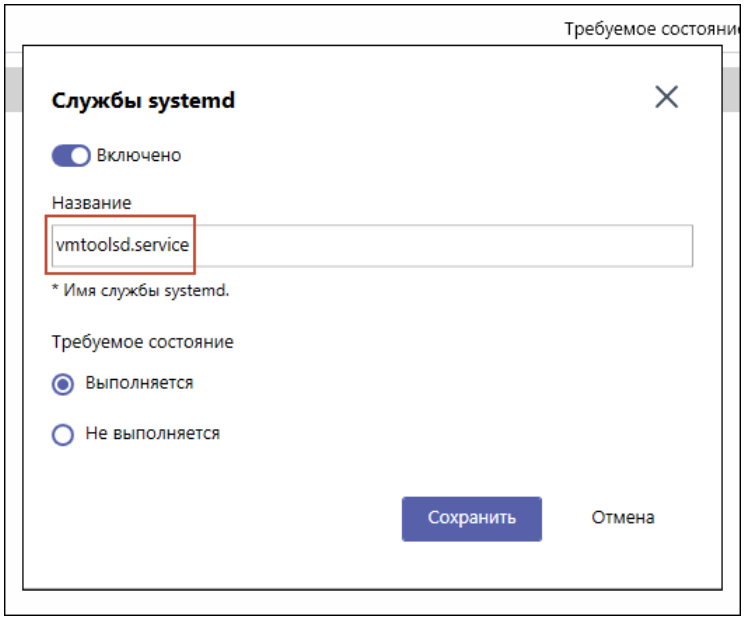


Рисунок 45. Пример задания названия службы systemd

- При выборе **Файлы** введите путь к файлу, например `/home/user/test.txt`. Путь должен содержать не более 1000 символов. Выберите состояние файла на защищаемом узле: **Присутствует** или **Отсутствует**.
- При выборе **Модули ядра** введите имя модуля ядра и выберите состояние модуля 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 **Версия ядра** укажите критерий сравнения (**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.

10 Нажмите **Сохранить**.

11 Добавьте все параметры в соответствии с шагами 8-9.

Все созданные параметры добавятся со статусом **Включено** в раздел для соответствующего типа параметра.

12 Чтобы выйти из настроек правил политики ZTNA, нажмите **Назад к EndPoint Protection**.

13 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Управление запуском и активностью приложений

Управление запуском и активностью приложений (см. Контроль приложений) возможно только для защищаемых узлов с ViPNet EPP Агент, установленных в ОС Windows.

Чтобы настроить правила контроля приложений настройте правила запуска приложений (см. Управление запуском приложений) и правила доступа для этих приложений (см. Управление активностью приложений).

Управление запуском приложений

Правила запуска приложений определяются списками контроля приложений. Вы можете добавлять правила запуска приложения в глобальные списки контроля (белый или черный), пользовательские группы белого списка, а также изменять порядок применения групп правил и правил в группах. Активность приложений из правил запуска пользовательских групп белого списка определяется правилами доступа. Для правил запуска приложений и правил доступа вы можете настроить регистрацию событий в журнале событий. Запуск и активность приложений из черного списка запрещена.

Списки контроля приложений и правила доступа действуют в пределах одной базы правил. Правила запуска приложений, включая правила доступа, можно сохранить в избранном и использовать в других базах правил.

Для настройки глобальных правил контроля приложений доступны:

- Создание правила запуска приложения (добавление в белый или черный списки).
- Создание правил доступа приложения (см. Управление активностью приложений).
- Изменение параметров отслеживания приложения в правиле запуска
- Удаление правила запуска приложения
- Перемещение правил запуска приложений между белым и черным списками
- Добавление правил запуска приложений в избранное для возможности использования в других базах правил.
- Импорт из избранного ранее добавленных правил запуска в базу правил.

Общий порядок управления правилами контроля приложений

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните нужную базу правил и на панели справа нажмите **Открыть в редакторе**.

4 На панели слева выберите **Контроль приложений**.

5 Просмотрите текущий список правил контроля приложений:

- В разделе **Запуск приложений** на вкладках **Белый список** и **Черный список** просмотрите правила запуска приложений.
- В разделе **Правила доступа** просмотрите правила доступа для приложений из правил запуска.

6 Выполните действия в соответствии с описанием ниже.

7 Нажмите **Назад к редактору**.

8 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Создание правила запуска приложения (добавление в белый или черный списки)

Чтобы создать новое правило запуска приложений:

1 На панели слева выберите **Запуск приложений**.

2 На вкладке **Белый список** или **Черный список** нажмите **Добавить** и в меню выберите **Создать новое правило**:

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 подпапках (см. Особенности задания и использования правил доступа).

2.2 Чтобы при запуске приложения не регистрировалось событие в журнале, снимите флажок **Формировать события**.

Примечание. Обратите внимание, что при включении опции формирования 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 формирование событий включенным на срок не более одних суток.

2.3 Выберите одну из групп или создайте новую, в которую будет добавлено правило запуска приложения:

- **Доверенные** — правило будет добавлено в белый список в группу **Доверенные** и приложению будут разрешены любые действия.

- **Запрещенные** — правило будет добавлено в черный список и приложению будут запрещены любые действия.
- **Пользовательские группы**, далее выберите группу из списка. Список **Пользовательские группы** содержит предустановленные группы **Частичное доверие** и **Слабое доверие**, а также группы, ранее созданные администратором ViPNet EPP Сервер. Правило будет добавлено в белый список в выбранную группу.
- **Новая группа**, далее укажите название новой группы, которая будет создана в белом списке. Правило будет добавлено в созданную группу.

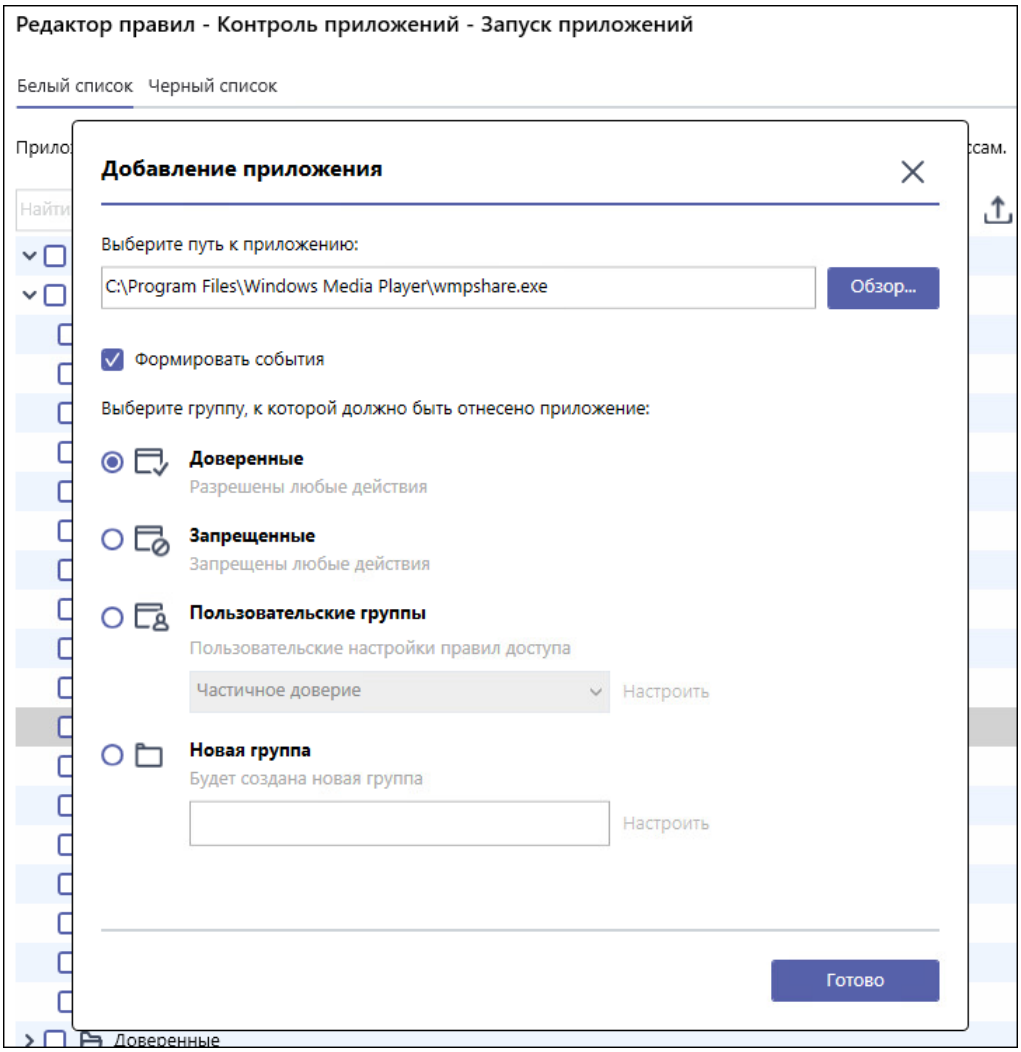


Рисунок 46. Внесение приложения wmpshare.exe в группу «Доверенные» белого списка

2.4 Если правило запуска приложения добавлено в существующую пользовательскую группу или в новую группу, будут применяться правила доступа по умолчанию, установленные для этой группы. Чтобы сразу задать правила доступа (см. Создание правил доступа приложения), требуемые именно для этого приложения, нажмите **Настроить**.

Примечание. Вы можете задать правила доступа позже, после того, как создадите все правила запуска приложений.

2.5 Нажмите **Готово**.

3 Нажмите **Применить**.

Изменение параметров отслеживания приложения в правиле запуска

Чтобы изменить путь к приложению или параметр **Формировать события** в правиле запуска приложения:

1 На панели слева выберите **Запуск приложений**.

2 На вкладке **Белый список** или **Черный список** дважды щелкните правило и на правой панели измените параметры.

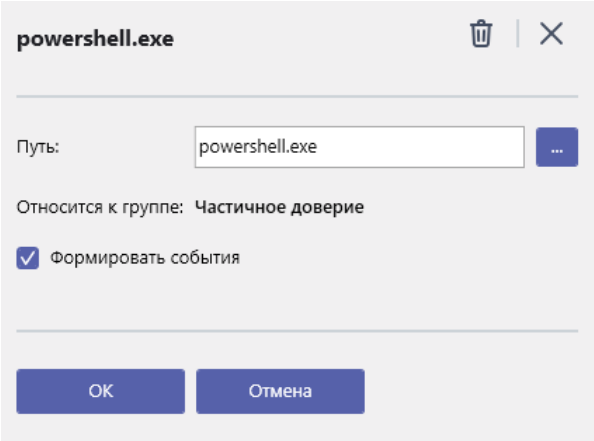


Рисунок 47. Дополнительная панель изменения параметров приложения

3 Нажмите **OK**.

4 Нажмите **Применить**.

Удаление правила запуска приложения

Чтобы удалить правила запуска приложения из белого или черного списка:

1 На панели слева выберите **Запуск приложений**.

2 На вкладке **Белый список** или **Черный список** раскройте группы правил и выберите флажками нужные правила.

3 Нажмите .

4 Нажмите **Применить**.

Перемещение правил запуска приложений между белым и черным списками

Перемещение правил запуска приложения между списками контроля выполняется в два этапа: сначала удалите правило из одного списка, затем добавьте его в другой. Таким же образом можно переместить правило из одной группы белого списка в другую.

Добавление правил запуска приложений в избранное

В избранном сохраняются все параметры правил запуска приложений (включая правила доступа), кроме статуса.

При сохранении правил запуска приложений в избранное выполняются проверка уникальности путей и распределение по группам:

- **Запрещенные** — правила черного списка; сохраняется путь к приложению; идентичные правила запуска не добавляются.
- **Доверенные** — правила группы **Доверенные** белого списка; сохраняется путь к приложению; идентичные правила запуска не добавляются.
- **Пользовательские** — правила пользовательских групп белого списка; сохраняется путь к приложению и правила доступа; идентичные правила запуска можно перезаписать.

Чтобы сохранить в избранном определенные правила запуска приложений текущей версии базы правил:

1. На панели слева выберите **Запуск приложений**.
2. На вкладке **Белый список** или **Черный список** в группах правил выберите флажками правила.
3. На панели вверху нажмите **Добавить в избранное**.
4. Если обнаружены идентичные правила запуска, будет предложено перезаписать их. Выберите флажками правила для перезаписи и нажмите **Перезаписать**.
5. Дождитесь завершения операции и нажмите **OK**.

В результате сохраненные правила запуска приложений будут отображаться в разделе **Базы правил** на вкладке **Избранные правила** > **Контроль приложений** (см. Просмотр и удаление избранных правил).

Импорт правил запуска приложений из избранного в базу правил

Чтобы добавить правила запуска приложений, ранее сохраненные в избранном, в текущую версию базы правил:

1. На панели слева выберите **Запуск приложений** или **Правила доступа**.
2. Выберите вкладку **Белый список** или **Черный список**.
3. На панели вверху нажмите **Добавить** и в меню выберите **Импортировать из избранного**.

4 Следуйте указаниям мастера импорта избранных правил:

4.1 Выберите группу, из которой нужно импортировать правила: **Запрещенные**, **Доверенные** или **Пользовательские**.

4.2 Выберите флажками правила, которые необходимо добавить в базу правил.

4.3 Выберите группу, в которую будут добавлены правила в разделе **Запуск приложений**:

- **Существующая группа** — выберите из списка одну из уже имеющихся групп.

> **Примечание.** При добавлении правил в существующую группу проверяется уникальность путей. Идентичные правила можно перезаписать. При обнаружении правил, уже имеющихся в базе правил, на странице мастера с перечнем дубликатов выберите, нужно ли перезаписать дубликат или нет.

- **Новая группа** — укажите название новой группы, которая будет создана.

4.4 Нажмите **Готово**.

4.5 Дождитесь завершения операции и нажмите **ОК**.

5 Нажмите **Применить**.

В результате правила будут добавлены в базу правил со статусом **Включено**.

Управление активностью приложений

Правила доступа определяют активность приложения из правила запуска пользовательской группы белого списка. В правилах доступа для каждого действия приложения можно настроить формирование события в журнале.

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

Чтобы создать правила доступа для приложения:

1 На панели слева выберите **Контроль приложений** > **Правила доступа**.

2 Раскройте пользовательскую группу и щелкните название нужного правила запуска приложения.

3 Чтобы создать правила доступа приложения к файлу, на правой панели выберите вкладку **Файлы** и нажмите **Добавить правило**.

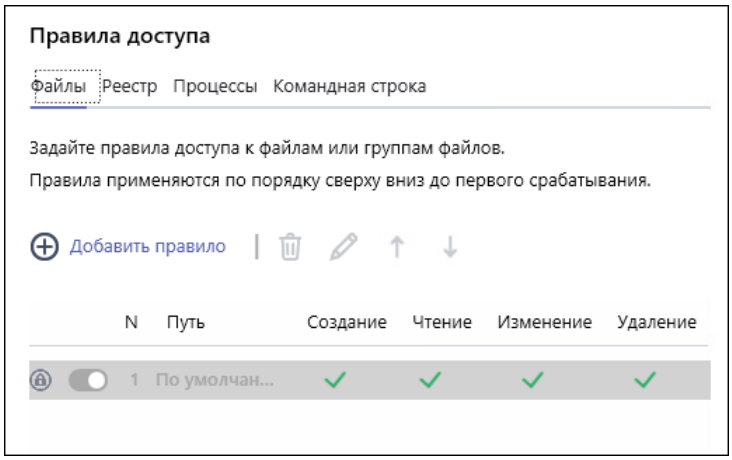


Рисунок 48. Настройка правил доступа приложения

4 В окне **Правило доступа к файлам**:

4.1 В поле **Выберите и отредактируйте путь к файлу** укажите путь к файлу, такой же, как на защищаемом узле.

4.2 Выберите в списках **Создание**, **Чтение**, **Изменение** и **Удаление** нужные разрешения для операций с файлом или группами файлов.

4.3 Чтобы при срабатывании правила в журнал записывались события, для каждого разрешения выберите **Формировать события**.

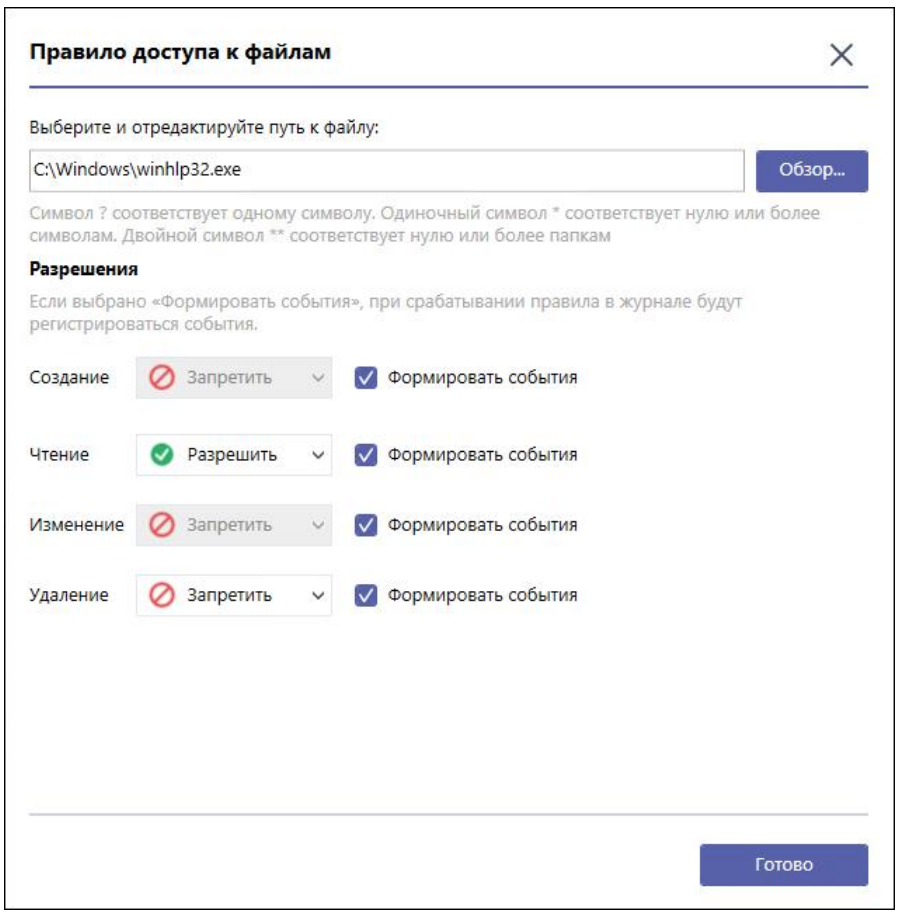


Рисунок 49. Создание правила доступа к файлу

4.4 Нажмите **Готово**.

5 Чтобы создать несколько правил доступа к файлам, повторите шаги 6 и 7.

6 Настройте порядок применения правил доступа к файлам (см. Изменение порядка применения правил доступа для приложений).

7 Чтобы создать правила доступа приложения к ветви реестра, на правой панели выберите вкладку **Реестр** и нажмите **Добавить правило**.

8 В окне **Правило доступа к реестру** укажите путь к ветви реестра, как на защищаемом узле, настройте параметры формирования событий и разрешения по аналогии с шагами 7.2 и 7.3.

Нажмите **Готово**.

9 Чтобы создать несколько правил доступа к ветвям реестра, повторите шаги 10 и 11.

10 Настройте порядок применения правил доступа к ветвям реестра (см. Изменение порядка применения правил доступа для приложений).

11 Чтобы создать правила доступа приложения к процессам, выберите вкладку **Процессы** и нажмите **Добавить правило**.

12 В окне **Правило доступа к процессам**:

12.1 Укажите путь к исполняемому файлу процесса как, на защищаемом узле.

12.2 Чтобы при срабатывании правила в журнал записывались события, выберите **Формировать события**.

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

12.4 Нажмите **Готово**.

13 Чтобы создать несколько правил доступа к процессам, повторите шаги 14 и 15.

14 Настройте порядок применения правил доступа к процессам (см. Изменение порядка применения правил доступа для приложений).

15 Чтобы создать правила доступа для запуска приложения с помощью определенных параметров командной строки, выберите вкладку **Командная строка** и нажмите **Добавить правило**.

16 В окне **Правило контроля командной строки**:

16.1 Укажите параметр командной строки.

16.2 Чтобы при срабатывании правила в журнал записывались события, выберите **Формировать события**.

16.3 Выберите в списке **Доступ** разрешать или запрещать использование параметра для запуска приложения.

16.4 Нажмите **Готово**.

17 Чтобы создать несколько правил доступа к параметрам командной строки, повторите шаги 18 и 19.

18 Настройте порядок применения правил доступа к параметрам командной строки (см. Изменение порядка применения правил доступа для приложений).

19 Нажмите **Применить**.

20 Чтобы выйти из настроек контроля приложений, нажмите **Назад к редактору**.

21 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Чтобы изменить существующее правило доступа для приложения из правила запуска пользовательской группы:

1 Раскройте пользовательскую группу и щелкните название правила запуска.

2 На панели справа выберите нужную вкладку (**Файлы**, **Реестр**, **Процессы**, **Командная строка**) и дважды щелкните правило, которое вы собираетесь изменить или нажмите .

3 В окне настройки правила доступа установите параметры по аналогии с шагами предыдущего сценария.

4 Нажмите **Готово**.

5 Нажмите **Применить**.

6 Сохраните изменения и отправьте на защищаемые узлы в соответствии с шагами 23-24 предыдущего сценария.

Настройка контроля обращений 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 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется добавить приложение в списки, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Контроль приложений** > **Общие настройки**.

5 Выключите **Контролировать обращения к сетевым папкам**.

6 Чтобы выйти из настроек контроля приложений, нажмите **Назад к редактору**.

7 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Чтобы в ViPNet EPP Агент сетевые папки снова контролировались, включите **Контролировать обращения к сетевым папкам**.

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\eplcontrol\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.

Изменение порядка применения правил доступа для приложений

Правила доступа для приложений применяются последовательно сверху вниз. 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 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется изменить порядок применения приложений или групп приложений, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Контроль приложений** > **Правила доступа**.

5 Выберите объекты, порядок применения которых вы хотите изменить:

- Отметьте флажками одну или несколько групп приложений.
- Раскройте одну или несколько групп приложений и отметьте флажками одно или несколько приложений.

6 На панели вверху нажмите ↑ или ↓ для перемещения выбранных объектов в списке.

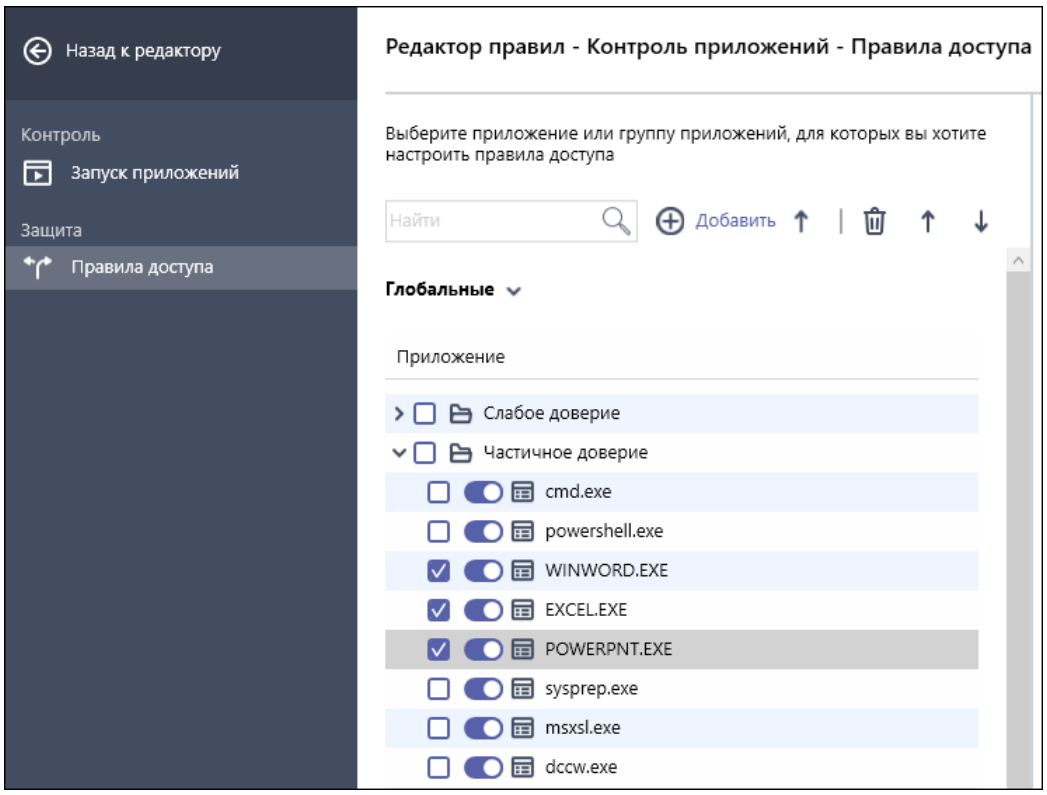


Рисунок 50. Изменение порядка применения выбранных приложений

7 Нажмите **Применить**.

8 Чтобы выйти из настроек контроля приложений, нажмите **Назад к редактору**.

9 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Чтобы изменить порядок применения правил доступа для выбранного приложения:

1 В разделе **Правила доступа** раскройте группу, где находится приложение, и выберите приложение, например `powershell.exe`.

2 На панели справа выберите вкладку, например **Процессы** и выберите флажками одно или несколько правил доступа, порядок применения которых вы хотите изменить.

3 Нажмите ↑ или ↓ для перемещения выбранных правил в списке.

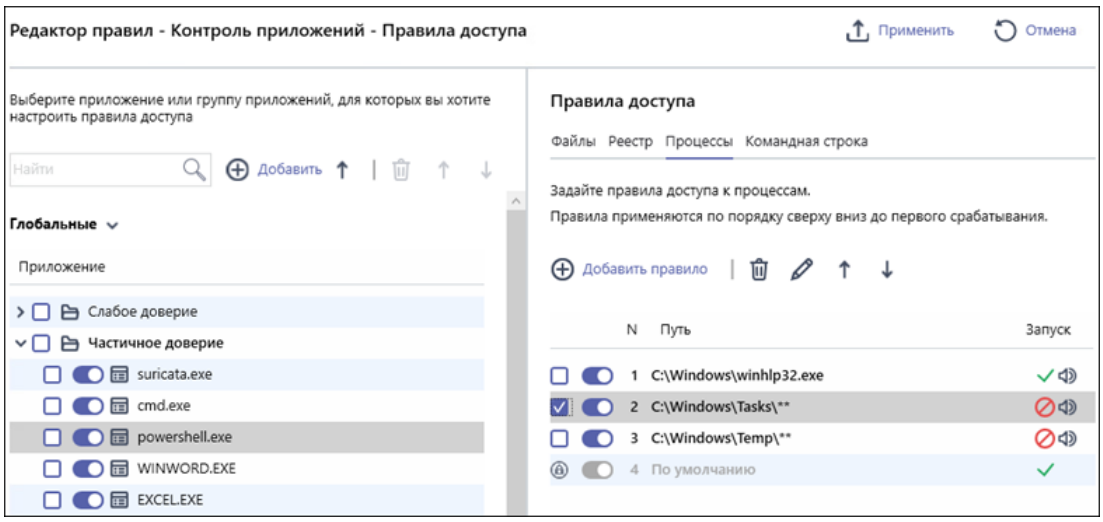


Рисунок 51. Изменение порядка применения правил доступа приложения powershell.exe

4 Нажмите **Применить**.

5 Сохраните изменения и отправьте на защищаемые узлы в соответствии с шагами 8-9 предыдущего сценария.

Настройка правил доступа по умолчанию для группы приложений

Правила доступа по умолчанию применяются для всех приложений группы в случае, если ни одно из правил доступа приложения не сработало. Правила доступа по умолчанию определены в базе правил. Чтобы изменить правила доступа по умолчанию:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется изменить правила доступа пользовательской группы по умолчанию, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Контроль приложений** > **Правила доступа**.

5 Щелкните название группы, например **Частичное доверие**.

Примечание. Правила доступа по умолчанию группы **Доверенные** и **Слабое доверие** изменить невозможно.

6 На панели справа выберите нужную вкладку (**Файлы**, **Реестр**, **Процессы**, **Командная строка**) и нажмите .

7 Настройте правила доступа для выбранного объекта операционной системы аналогично сценарию настройки правил доступа приложения (см. Управление активностью приложений).

8 Нажмите **Применить**.

9 Чтобы выйти из настроек контроля приложений, нажмите **Назад к редактору**.

10 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Управление обнаружением и предотвращением вторжений

Настройка правил HIDS

Правила HIDS актуальной версии базы правил выявляют широкий спектр угроз безопасности информации, но при необходимости вы можете изменить существующие правила HIDS, а также создать новые.

Чтобы настроить правила HIDS:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить правила HIDS, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Обнаружение и предотвращение вторжений** > **HIDS**.

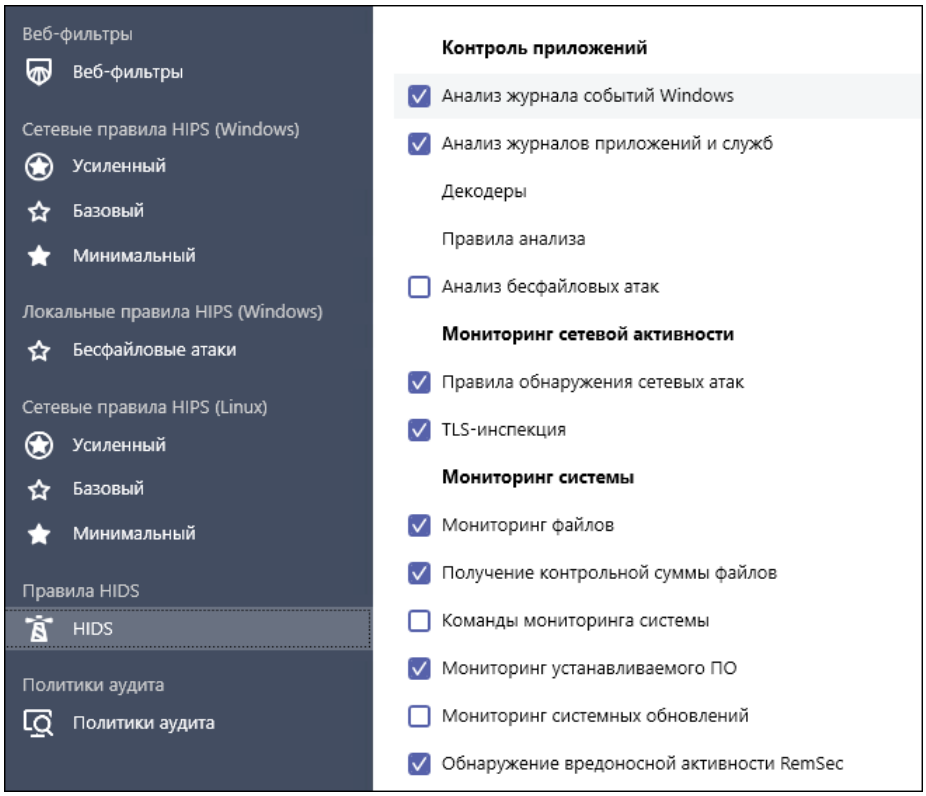


Рисунок 52. Настройка правил HIDS

5 Настройте параметры работы правил обнаружения локальных угроз безопасности информации:

- Отслеживание изменений в журналах событий ОС Windows.
- Отслеживание изменений в журналах приложений и служб.
- Отслеживание событий обнаружения вирусов.
- Отслеживание изменений в реестре ОС Windows.

Чтобы внести изменения в тексты правил обнаружения локальных угроз:

- Настройте декодеры (см. Настройка декодеров).
- Настройте правила анализа (см. Настройка правил анализа).

6 Настройте параметры работы правил обнаружения бесфайловых атак (см. Обнаружение бесфайловых атак).

7 Настройте параметры работы правил отслеживания изменений в файлах (см. Отслеживание изменений в файлах).

8 Настройте параметры работы правил отслеживания создания файлов и вычисления их контрольных сумм (см. Отслеживание создания файлов и вычисление их контрольных сумм).

9 Настройте параметры работы правил отслеживания установки системных обновлений ОС Windows (см. Отслеживание установки системных обновлений ОС Windows).

10 Настройте обнаружение вредоносной активности RemSec.

11 Настройте правила обнаружение сетевых атак (см. Отслеживание сетевой активности).

12 Настройте TLS-инспекцию (см. Настройка TLS-инспекции).

13 Настройте отслеживание состояния защищаемого узла с помощью команд мониторинга.

14 Настройте отслеживание установки программного обеспечения.

Примечание. При вводе недопустимого параметра поле параметра подсвечивается красной рамкой, а рядом с настраиваемым правилом появится ⚠. Если перед сохранением базы правил вы не исправите недопустимые параметры, при сохранении базы правил для этих параметров будут сохранены значения по умолчанию.

---

15 Нажмите **Назад к редактору**.

16 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Примечание. После настройки правил HIDS для защищаемых узлов с ОС Windows для корректной работы правил проверьте, что заданы корректные параметры политик аудита (см. Настройка политик аудита).

В правилах HIDS для указания путей и масок вы можете использовать шаблоны:

- `%directory%` — системная переменная среды ОС Windows, задающая путь к папке. Допускается использовать несколько системных переменных одновременно.

  Пример: если значение системной переменной среды `%SystemRoot% = C:\Windows`, путь `%SystemRoot%\Test` преобразуется в `C:\Windows\Test`.

- `*` — последовательность допустимых символов любой длины.

  Пример: если значение системной переменной среды `%SystemDrive% = C:\`, в правиле HIDS указан путь `%SystemDrive%\Test*`, при этом на диске имеются папки `C:\Test1`, `C:\Test2` и `C:\Test3`, то правило HIDS применяется к этим папкам.

Настройка декодеров

Для первичного анализа ряда изменений, происходящих на защищаемом узле, используются декодеры. Декодеры отображаются в виде xml-файлов, содержащих текст правил в соответствии с синтаксисом OSSEC:

- win decoder.xml — правила для защищаемых узлов с ОС Windows.
- *nix decoder.xml — правила для защищаемых узлов с ОС GNU/Linux.

Чтобы изменить уже имеющиеся правила или добавить новые:

1 В группе правил **Контроль приложений** выберите **Декодеры**.

2 На панели справа напротив нужного файла, например win decoder.xml, нажмите ✎.

3 Внесите новые правила или отредактируйте уже существующие в соответствии с синтаксисом OSSEC.

4 Нажмите **Сохранить**.

Настройка правил анализа

Для детального разбора информации от декодеров используются правила анализа. Текст правил анализа содержится в файлах и написан в соответствии с синтаксисом OSSEC. По умолчанию используются правила анализа из файлов:

- win EventRules — правила для защищаемых узлов с ОС Windows.
- *nix ids_rules — правила для защищаемых узлов с ОС GNU/Linux.

Чтобы изменить уже имеющиеся правила или добавить новые:

1 В группе правил **Контроль приложений** выберите **Правила анализа**.

2 На панели справа выберите файл с правилами, например win EventRules и нажмите  .

3 Внесите новые правила анализа или отредактируйте уже существующие в соответствии с синтаксисом OSSEC.

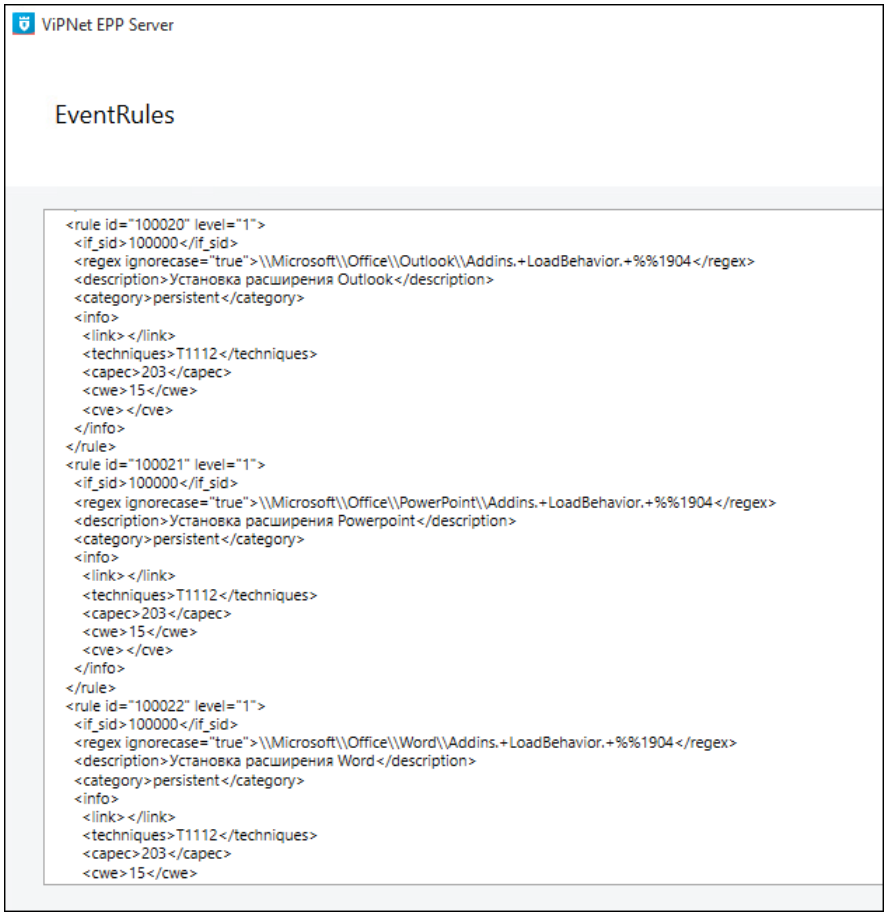


Рисунок 53. Пример синтаксиса OSSEC в правилах анализа

4 Нажмите **Сохранить**.

Чтобы загрузить еще один файл, содержащий правила анализа:

1. Нажмите **Добавить файл**. Вы можете добавить файл с правилами только для защищаемых узлов с ОС Windows.
2. Выберите файл правил анализа.
3. Нажмите **Сохранить**.

Отслеживание изменений в журналах событий ОС Windows

Правила отслеживания изменений в журналах событий ОС Windows (Приложение, Безопасность, Система и другие) содержатся в правилах анализа. По умолчанию отслеживание включено. Отслеживаются изменения во всех журналах, указанных в базе правил.

Чтобы изменить настройки отслеживания изменений в журналах ОС Windows:

1. В группе правил **Контроль приложений** выберите **Анализ журнала событий Windows** — на панели справа будет отображен список отслеживаемых журналов Windows.

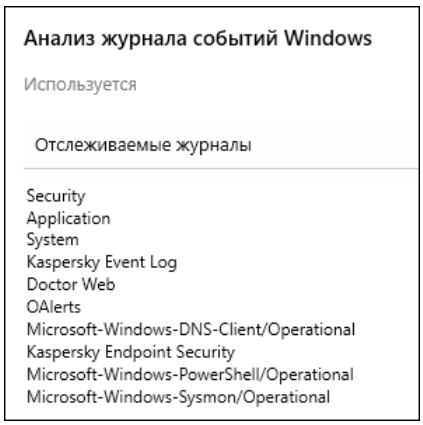


Рисунок 54. Список отслеживаемых журналов ОС Windows

2. Для добавления журнала в список дважды щелкните пустую строку, расположенную ниже последнего журнала в списке и введите имя журнала. Вы можете добавлять любые журналы событий Windows.
3. Для исключения журнала из списка отслеживания щелкните строку с исключаемым журналом и нажмите клавишу **Delete**.

Чтобы отключить отслеживание изменений в журналах событий ОС Windows, снимите флажок **Анализ журнала событий Windows**.

Отслеживание изменений в журналах 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 отслеживание изменений в журналах приложений и служб включено. Отслеживаются изменения в журналах, указанных в базе правил. Доступно изменение частоты проверки журналов и списка отслеживаемых журналов отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

Чтобы настроить параметры отслеживания изменений в журналах приложений и служб:

1 В группе правил **Контроль приложений** выберите **Анализ журналов приложений и служб**.

2 На панели справа выберите вкладку **Windows** или **Linux**:

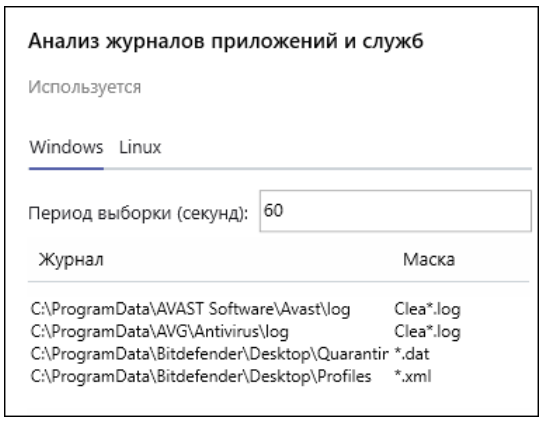


Рисунок 55. Настройка периода выборки и списка отслеживаемых журналов

3 В поле **Период выборки** укажите частоту проверки журналов. При изменении этого параметра стоит учитывать, что чем меньше значение вы укажете, тем больше будет нагрузка на ViPNet EPP Сервер и ViPNet EPP Агент. Может принимать значение из диапазона 60–120 секунд, рекомендуемое — 60 секунд.

4 Для добавления журнала в список дважды щелкните пустую строку, расположенную ниже последнего журнала в списке, и введите путь поиска журнала:

- Для Windows:
  - В поле **Журнал** укажите корневую папку для поиска журналов.
  - В поле **Маска** укажите части имени файла, расширение или имя файла журнала целиком.
- Для Linux в поле **Журнал** укажите путь к файлу с журналом.

5 Для исключения журнала из списка отслеживания щелкните строку с исключаемым журналом и нажмите клавишу **Delete**.

Чтобы отключить отслеживание изменений в журналах приложений и служб, снимите флажок **Анализ журналов приложений и служб**.

Обнаружение бесфайловых атак

ViPNet EPP позволяет обнаруживать бесфайловые атаки на защищаемых узлах с ОС Windows, выполняемых с помощью методов по классификации MITRE ATT&CK®.

По умолчанию обнаружение бесфайловых атак отключено. После включения обнаружения доступно изменение частоты сканирования процессов.

После применения на защищаемом узле базы правил (политики безопасности) с настройками бесфайловых атак, чтобы изменения вступили в действие, необходимо перезагрузить защищаемый узел в следующих случаях:

- Если было включено хотя бы одно правило для бесфайловых атак в разделе **Обнаружение и предотвращение вторжений** > **Бесфайловые атаки** или **HIDS**, 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 включить обнаружение и изменить параметры:

1. В группе правил **Контроль приложений** выберите **Анализ бесфайловых атак** и установите флажок.
2. На панели справа в поле **Период** задайте частоту сканирования ViPNet EPP Агент процессов на защищаемом узле. Рекомендуемое значение — 600 секунд. Доступно задание значений от 60 до 86400 секунд.
3. Чтобы в журнале событий отображалась также информация о сканировании процессов, в результате которого не были обнаружены потенциальные атаки, снимите флажок **Скрывать информационные события**.

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

Отслеживание изменений в файлах

ViPNet EPP позволяет обнаруживать изменения в файлах на защищаемых узлах с ОС Windows и ОС GNU/Linux. По умолчанию отслеживание включено. Доступна настройка параметров отслеживания отдельно для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux.

Чтобы изменить настройки отслеживания:

1. Чтобы отслеживание изменений в файлах работало на защищаемых узлах с ОС GNU/Linux, в группе **Мониторинг системы** убедитесь, что установлен флажок **Анализ журналов приложений и служб**.
2. Выберите **Мониторинг файлов**.
3. На панели справа выберите вкладку **Windows** или **Linux** и задайте:
   - 3.1 В поле **Путь** укажите папку для поиска изменяемых файлов.
   - 3.2 В поле **Маска** укажите маску, по которой будет происходить поиск изменяемых файлов. Вы можете задать несколько папок или файлов для отслеживания.



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

3.3 Параметры отслеживания:

- — исключать отслеживание файлов по маске.
- — отслеживать создание файла.
- — отслеживать изменение файла.
- — отслеживать удаление файла.
- — отслеживать все вложенные папки в случае их наличия.

> **Примечание.** При заданных настройках отслеживания вложенных папок 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.

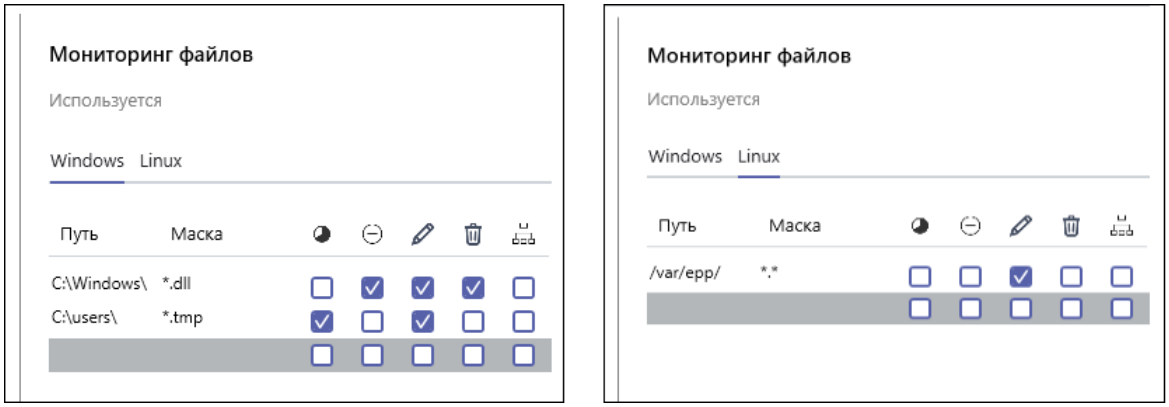


Рисунок 56. Дополнительная панель «Мониторинг файлов»

Чтобы отключить отслеживание изменений файлов, снимите флажок **Мониторинг файлов**.

Отслеживание создания файлов и вычисление их контрольных сумм

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. По умолчанию отслеживание отключено. Чтобы включить отслеживание создания новых файлов и вычисление их контрольных сумм:

1 Чтобы вычисление контрольных сумм для новых файлов выполнялось на защищаемых узлах с ОС GNU/Linux, в группе **Мониторинг системы** установите флажок **Анализ журналов приложений и служб**.

2 Выберите **Получение контрольной суммы файлов** и установите флажок.

3 На панели справа выберите вкладку **Windows** или **Linux** и нажмите **Добавить**:

3.1 Если выбрана вкладка **Windows**:

3.1.1 В поле **Маска** задайте маску пути, по которой будет происходить поиск создаваемых файлов.

3.1.2 В поле **Исключающая маска** задайте маску пути, по которой будет происходить исключение файлов из отслеживания.

Для задания масок вы можете использовать шаблоны правил HIPS (см. Настройка правил HIDS). После задания шаблонов каждые 60 секунд будет выполняться сверка на наличие новых папок, удовлетворяющих настроенным шаблонам.

3.1.3 В списке **Алгоритм** выберите алгоритм вычисления контрольной суммы: MD5, SHA256, SpamSum.

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

3.2 Если выбрана вкладка **Linux**:

3.2.1 В поле **Путь** задайте папку для отслеживания создаваемых файлов.

3.2.2 В поле **Маска** задайте маску, по которой будет происходить поиск создаваемых файлов.

Например, путь может быть задан в следующем формате: `постоянная часть/часть_имени_папки_*/`, а маска файла — `*.расширение`. Символ `*` указывается на месте изменяемой части названия папки или файла. Может использоваться несколько символов `*`.

Для задания пути и маски вы можете использовать шаблоны правил HIDS (см. Настройка правил HIDS). После задания шаблонов каждые 60 секунд будет выполняться сверка на наличие новых папок, удовлетворяющих настроенным шаблонам.

3.2.3 В списке **Алгоритм** выберите алгоритм вычисления контрольной суммы.

3.2.4 Чтобы исключить отслеживание файлов по маске, выберите **Исключить по маске**.

3.2.5 Чтобы отслеживать все вложенные папки, выберите **Рекурсивно**.

Примечание. Вложенные папки, созданные с помощью команды `mkdir -p`, отслеживаться не будут, если папки более высокого уровня не были созданы до запуска команды.

В результате при создании новых файлов по указанным путям и с заданными параметрами в журнале событий будет регистрироваться событие получения контрольной суммы.

Отслеживание событий обнаружения вирусов

ViPNet EPP позволяет отслеживать работу антивирусного программного обеспечения, установленного на защищаемых узлах (см. Отслеживание работы антивирусов).

События обнаружения вирусов отслеживаются по правилам анализа. По умолчанию отслеживание событий включено, события обнаружения вирусов регистрируются в журнале событий.

Чтобы отключить отслеживание событий обнаружения вирусов, отредактируйте правила анализа, связанные с обработкой таких событий (см. Настройка правил анализа).

Отслеживание установки системных обновлений ОС Windows

ViPNet EPP позволяет отслеживать наличие установленных системных обновлений ОС Windows на защищаемых узлах. По умолчанию отслеживание отключено. Чтобы включить отслеживание и настроить параметры:

1. В группе **Мониторинг системы** выберите **Мониторинг системных обновлений** и установите флажок.
2. На панели справа задайте параметры мониторинга:
   - 2.1 В списке **Уровень событий** выберите уровень, который будет присваиваться событиям, регистрируемым в результате установки системных обновлений ОС Windows.
   - 2.2 В поле **Период выборки (секунд)** задайте частоту проверки факта наличия установленного системного обновления ОС Windows.
   - 2.3 В поле **Системные обновления** укажите (в любом регистре) системные обновления ОС Windows, установку которых нужно отслеживать. При вводе нескольких обновлений разделяйте их запятой. Например, KB2669970, KB4338825.

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.

Обнаружение вредоносной активности RemSec

ViPNet EPP позволяет обнаруживать вредоносную активность RemSec на защищаемых узлах с ОС Windows. Правила отслеживания активности RemSec содержатся в базе правил. По умолчанию отслеживание включено.

Чтобы отключить обнаружение активности RemSec, в группе **Мониторинг системы** снимите флажок **Обнаружение вредоносной активности RemSec**.

Отслеживание изменений в реестре ОС Windows

Изменения в разделе реестра `HKEY_CURRENT_USER` отслеживаются ViPNet EPP по умолчанию. Для отслеживания изменений в других разделах реестра добавьте правило анализа для отслеживания изменений в нужном разделе реестра (см. Настройка правил анализа).

Отслеживание сетевой активности

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 (см. Блокирование сетевой активности).

По умолчанию отслеживание сетевой активности включено.

Текст правил обнаружения сетевых атак написан в соответствии с синтаксисом Suricata и содержится в файлах:

- win net.rules — правила для защищаемых узлов с ОС Windows.
- *nix net.rules — правила для защищаемых узлов с ОС GNU/Linux.



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 изменить уже имеющиеся правила или добавлять новые:

1. В группе **Мониторинг сетевой активности** выберите **Правила обнаружения сетевых атак**.
2. На панели справа выберите файл с правилами, например win net.rules, и нажмите  .
3. Внесите новые правила или измените уже существующие в соответствии с синтаксисом Suricata.
4. Нажмите **Сохранить**.

Чтобы отключить отслеживание сетевой активности на защищаемых узлах, снимите флажок **Правила обнаружения сетевых атак**.

Отслеживание состояния защищаемого узла с помощью команд мониторинга

ViPNet EPP для отслеживания состояния защищаемых узлов с ОС Windows позволяет использовать команды мониторинга. По умолчанию использование команд мониторинга отключено.

Таблица 6. Команды мониторинга состояния защищаемого узла

Назначение команды	Команда
Получение общей сетевой информации по TCP-соединениям	`netstat -nabop tcp`
Получение сетевой информации по TCP-соединениям по слушающим портам	`netstat -nabop tcp | findstr LISTENING`
Получение общей сетевой информации по UDP-соединениям	`netstat -nabop udp`
Разрешение доменного имени	`nslookup <имя домена> <IP DNS-сервера>`, где `<IP DNS-сервера>` — необязательный параметр, без него используется IP-адрес сервера по умолчанию
Разрешение IP-адреса	`nslookup -q=ptr <IP> <IP DNS-сервера>`, где `<IP`

Назначение команды	Команда
	DNS-сервера> — необязательный параметр, без него используется IP-адрес сервера по умолчанию
Получение списка почтовых серверов домена	nslookup -q=mx <имя домена> <IP DNS-сервера>, где <IP DNS-сервера> — необязательный параметр, без него используется IP-адрес сервера по умолчанию
Получение списка авторитетных DNS-серверов домена	nslookup -q=ns <имя домена> <IP DNS-сервера>, где <IP DNS-сервера> — необязательный параметр, без него используется IP-адрес сервера по умолчанию
Получение списка контроллеров домена Active Directory	nslookup -type=srv _ldap._tcp.<имя домена> | findstr "internet address"
Список подключенных общих сетевых ресурсов	net use
Получение данных по общим ресурсам	wmic share
Список дисковых устройств	wmic diskdrive get Model,Description,Status
Список сетевых интерфейсов	wmic nic get Name,NetEnabled
Список установленного программного обеспечения	wmic product get Name,Version,Vendor
Список автозагрузки	wmic startup get Name,Location,User
Список драйверов	driverquery
Текущие пользовательские сессии	query session
Проверка сетевого соединения	ping <IP-адрес узла>
Таблица маршрутизации IP v4	route print -4
Таблица маршрутизации IP v6	route print -6
Трассировка маршрута	tracert -d <IP-адрес>

Чтобы использовать команды мониторинга:

1. В группе **Мониторинг системы** выберите флажком **Команды мониторинга системы**.
2. На панели справа задайте параметры:
   - **2.1** В списке **Уровень событий** выберите уровень, который будет присваиваться событиям, регистрируемым в результате выполнения команд.
   - **2.2** В поле **Период выборки** задайте частоту выполнения команды. Минимальное допустимое и рекомендуемое значение — 60 секунд.
   - **2.3** Щелкните поле **Команда** и задайте команду из списка доступных команд, с помощью которой будет отслеживаться состояние защищаемых узлов.



Внимание! Если вы зададите недопустимую команду или команду в неправильном формате, окно ввода команды будет подсвечено красной рамкой и выделено красным фоном. появится подсказка со списком доступных команд.

2.4 Укажите параметры команды:

- Чтобы предыдущий результат выполнения команды сравнивался с текущим и отображалась разница, установите флажок **Дельта**.
- Чтобы с помощью параметра **Дельта** сравнивались результаты, содержащие только определенные данные, задайте маску для выполняемых команд. Для этого в поле **Маска** укажите сведения, по которым будут отфильтрованы результаты. Например, чтобы сравнивались результаты выполнения команды `ping 127.0.0.1`, имеющие интервал ожидания 32 мс, в поле **Маска** задайте величину этого интервала — `32`.

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

Отслеживание установки программного обеспечения

ViPNet EPP позволяет отслеживать установку программного обеспечения на защищаемых узлах с ОС Windows. По умолчанию отслеживание включено с периодом слежения 600 секунд.

Чтобы изменить период слежения:

1 В группе **Мониторинг системы** выберите **Мониторинг устанавливаемого ПО**.

2 На панели справа в поле **Период слежения** укажите период проверки установленного программного обеспечения.

Чтобы отключить отслеживание установки нового программного обеспечения, снимите флажок **Мониторинг устанавливаемого ПО**.

Настройка TLS-инспекции

ViPNet EPP с помощью функции TLS-инспекции позволяет расшифровывать HTTPS-трафик на защищаемых узлах с ОС Windows для возможности проверки его правилами HIPS, сетевыми правилами HIDS и веб-фильтрами.

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

Чтобы включить TLS-инспекцию, в группе правил **Мониторинг сетевой активности** выберите **TLS-инспекция**.

Настройка правил HIPS

Чтобы правила HIPS работали, модуль защиты **Обнаружение и предотвращение вторжений** должен быть включен — установлен один из режимов работы (см. Выбор режимов работы модулей защиты).

С помощью правил HIPS можно настроить:

- Блокирование сетевой активности.
- Блокирование бесфайловых атак типа Keylogging, обнаруженных правилами HIDS для бесфайловых атак (см. Обнаружение бесфайловых атак).
- Блокирование бесфайловых атак с целью получения адресов функций в модулях ядра ОС Windows.
- Блокирование бесфайловых атак типа Hollowing и Doppelganging.

После применения на защищаемом узле базы правил (политики безопасности) с настройками бесфайловых атак, чтобы изменения вступили в действие, необходимо перезагрузить защищаемый узел в следующих случаях:

- Если было включено хотя бы одно правило для бесфайловых атак в разделе **Обнаружение и предотвращение вторжений** > **Бесфайловые атаки** или **HIDS**, 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.

Блокирование сетевой активности

База правил содержит предустановленные правила HIPS для защищаемых узлов с ОС Windows и для защищаемых узлов с ОС GNU/Linux, а также для каждого из режимов работы обнаружения и предотвращения вторжений: усиленного, базового и минимального.

Для учета особенностей контроля сетевой активности на защищаемых узлах доступно:

- Добавление новых правил HIPS.
- Изменение имеющихся правил HIPS.
- Удаление ненужных правил HIPS.

Правила HIPS для защищаемых узлов содержатся в файле и написаны в соответствии с синтаксисом Suricata. Изменения можно внести путем редактирования файла. При написании правил учитывайте, что в ViPNet EPP Агент применяются правила HIPS только с действиями правил:

- `drop` ( **Блокировать**) — IP-пакет блокируется сетевым фильтром HIPS персонального 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 добавить, отредактировать или удалить правило HIPS:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить правила HIPS, и нажмите **Открыть в редакторе**.

4 Выберите **Обнаружение и предотвращение вторжений**.

5 Чтобы настроить правила HIPS, выберите один из режимов работы **Усиленный**, **Базовый** или **Минимальный**:

- Для защищаемых узлов с ОС Windows — в группе **Сетевые правила HIPS (Windows)**.
- Для защищаемых узлов с ОС GNU/Linux — в группе **Сетевые правила HIPS (Linux)**.

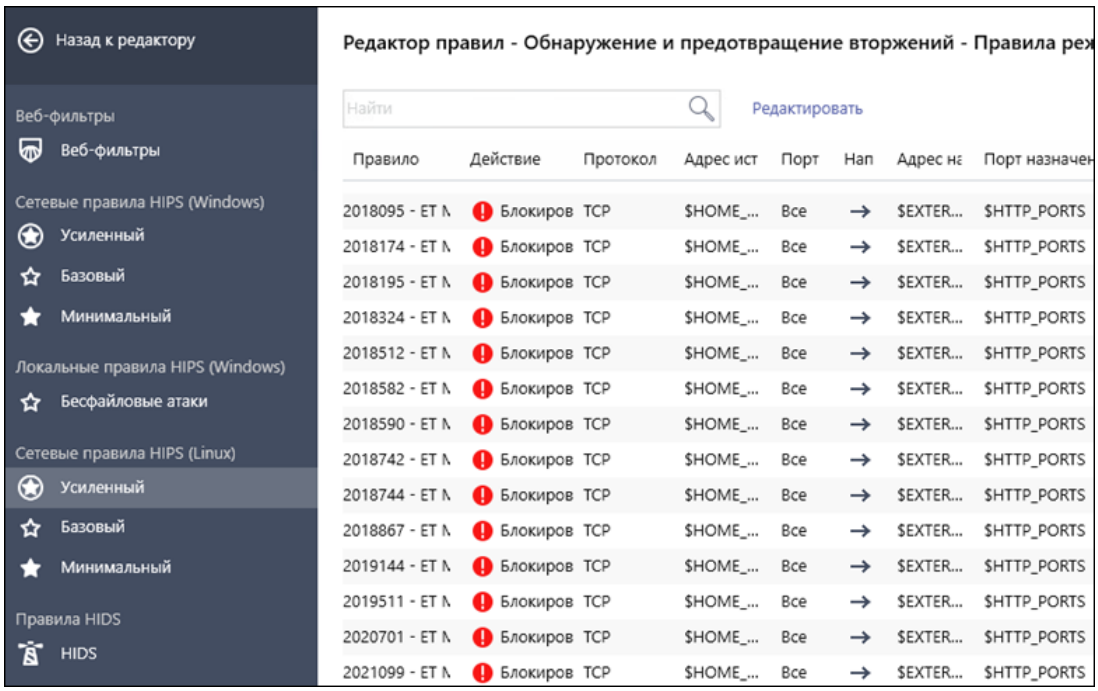


Рисунок 57. Список правил HIPS

6 На панели вверху нажмите **Редактировать**.

7 Внесите необходимые изменения в соответствии с синтаксисом правил Suricata и нажмите **Сохранить**.

8 Нажмите **Применить**.

9 Нажмите **Назад к редактору**.

10 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Блокирование бесфайловых атак типа Keylogging

Для управления блокированием бесфайловых атак, выполняемых с помощью вызова функции ОС Windows `SetWindowsHookEx` (см. Обнаружение и предотвращение бесфайловых атак), доступны:

- Добавление новых правил.
- Изменение имеющихся правил.
- Изменение порядка применения правил.
- Временное отключение или удаление правил.

Общий порядок управления правилами HIPS для бесфайловых атак

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить правила HIPS, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Обнаружение и предотвращение вторжений** > **Бесфайловые атаки**.

5 Добавьте, измените правило HIPS, измените порядок применения правил, временно отключите или удалите ненужные правила в соответствии с описанием ниже.

6 Нажмите **Применить**.

7 Нажмите **Назад к редактору**.

8 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Добавление нового правила

1 На панели вверху нажмите **Добавить** и задайте параметры правила:

2 Укажите название правила.

3 Выберите тип отслеживаемых hook:

- **Клавиатура** — контроль сообщений от клавиатуры.

- **Мышь** — контроль сообщений от мыши.
- **Окна** — контроль событий от окон.
- **Прочее** — контроль прочих системных сообщений.

4 Определите действие правила HIPS:

-  **Блокировать** — при срабатывании правила атака будет заблокирована и в журнале событий зарегистрируется событие блокирования атаки.
-  **Разрешить** — при срабатывании правила в журнале событий зарегистрируется событие обнаружения атаки.

5 Укажите маску отслеживаемого процесса. 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 `*`.

6 Укажите маску отслеживаемого вредоносного модуля, 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.

7 Чтобы зарегистрированные события фиксировались в журнале событий (см. Журнал событий), выберите **Формировать события**.

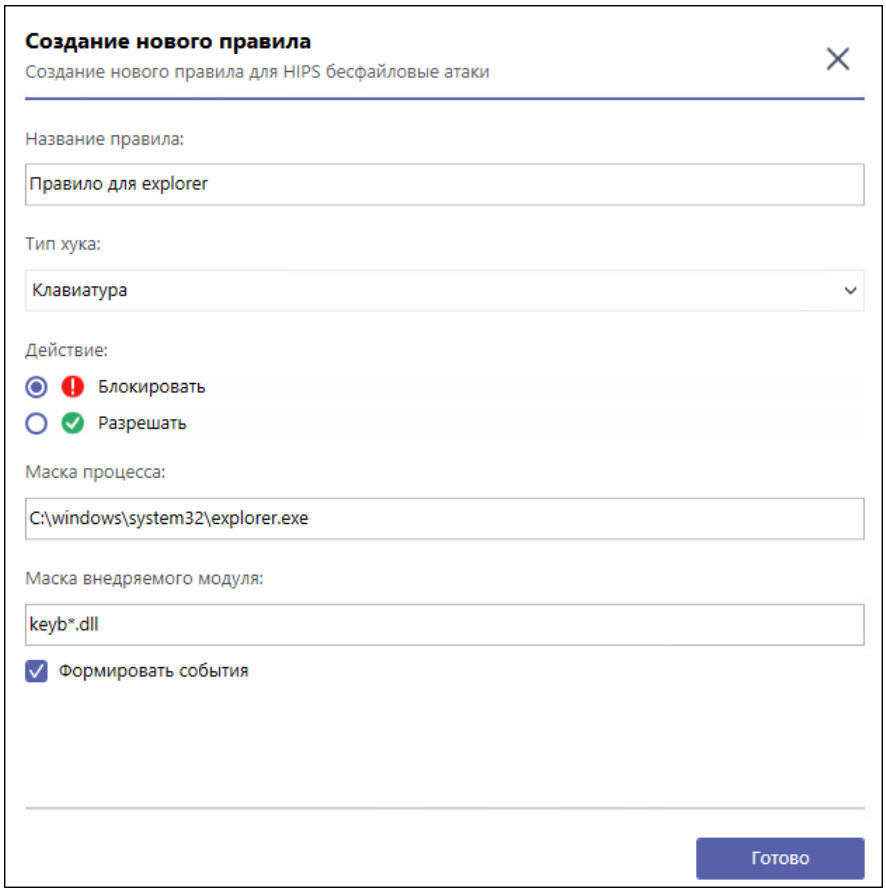


Рисунок 58. Создание правила HIPS для бесфайловых атак

8 Нажмите **Готово**.

Изменение правила

1 В списке правил дважды щелкните строку правила.

2 На панели справа внесите изменения в параметры правила.

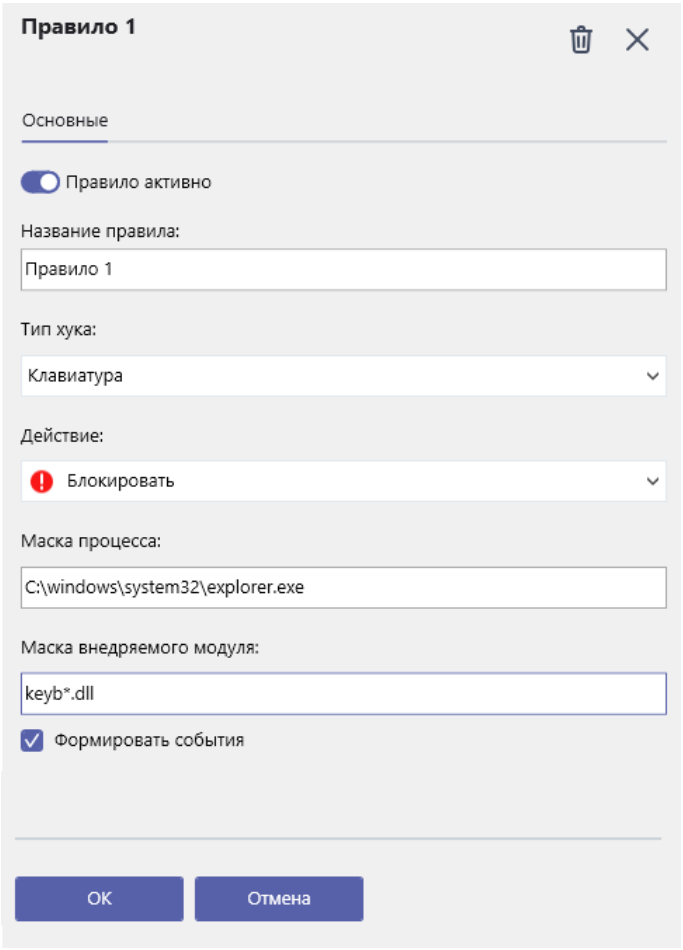


Рисунок 59. Изменение параметров правила

3 Нажмите **OK**.

Изменение порядка применения правил

Правила HIPS для бесфайловых атак применяются в списке последовательно, сверху вниз, до первого срабатывания. Чтобы изменить порядок применения правил HIPS:

1 В списке правил выберите флажками правила, порядок применения которых необходимо изменить.

2 На панели вверху нажмите ↑ или ↓ для перемещения выбранных правил HIPS в списке.

Временное отключение и удаление правила

Чтобы временно отключить правило HIPS для бесфайловых атак, в списке правил HIPS выключите **Правило активно** перед названием правила.

Чтобы удалить правила HIPS для бесфайловых атак:

1 В списке правил HIPS выберите флажками правила, которые необходимо удалить.

2 На панели вверху нажмите **Удалить**.

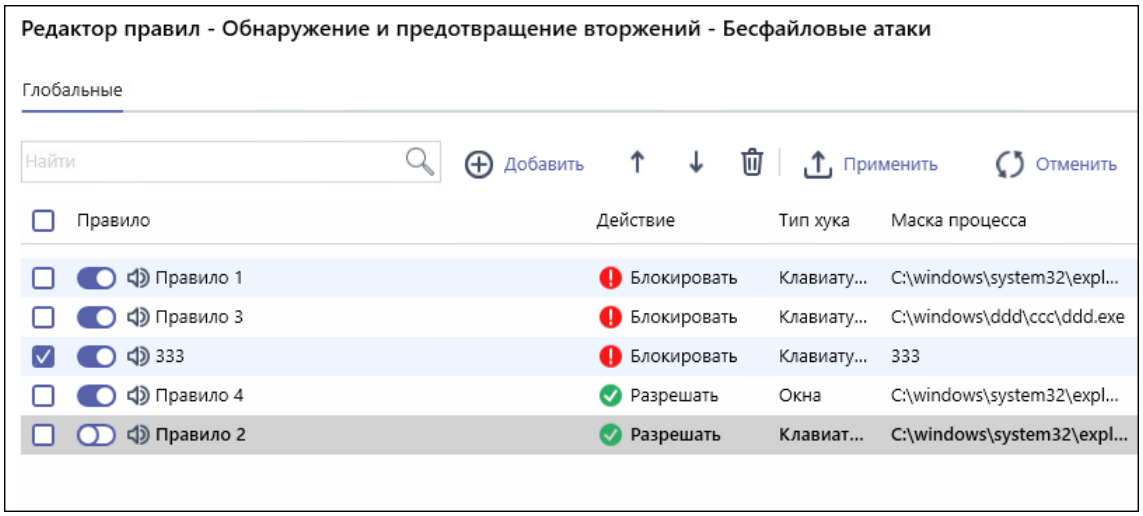


Рисунок 60. Список созданных правил HIPS для бесфайловых атак

Блокирование бесфайловых атак с целью получения адресов функций в модулях ядра ОС Windows

ViPNet EPP позволяет обнаруживать и предотвращать бесфайловые атаки на защищаемых узлах с ОС Windows, связанные с получением адресов функций в модулях ядра ОС Windows (см. Обнаружение и предотвращение бесфайловых атак). По умолчанию обнаружение и блокирование таких бесфайловых атак отключено.

Чтобы включить правила обнаружения и блокирования бесфайловых атак, связанных с получением адресов функций в модулях ядра Windows:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить правила HIDS, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Обнаружение и предотвращение вторжений** > **Бесфайловые атаки**.

5 В разделе **Предотвращение бесфайловых атак** выберите **Предотвращение получения адресов функций в модулях ядра Windows**.

6 Нажмите **Применить**.

7 Нажмите **Назад к редактору**.

8 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

При обнаружении и блокировании бесфайловой атаки на защищаемом узле, связанной с получением адресов функций в модулях ядра Windows, в журнале событий ViPNet EPP Сервер и Агент будет регистрироваться событие **Блокирование Kernel module load**.

Блокирование бесфайловых атак типа Hollowing и Doppelganging

ViPNet EPP позволяет обнаруживать и предотвращать бесфайловые атаки на защищаемых узлах с ОС Windows, относящиеся к методам Process Hollowing и Process Doppelganging (см. Обнаружение и предотвращение бесфайловых атак). По умолчанию обнаружение и блокирование таких бесфайловых атак отключено.

Чтобы включить правила предотвращения бесфайловых атак:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить правила HIDS, и нажмите **Открыть в редакторе**.

4 На панели слева выберите **Обнаружение и предотвращение вторжений** > **Бесфайловые атаки**.

5 В разделе **Предотвращение бесфайловых атак** выберите **Предотвращение атак типа Hollowing и Doppelganging**.

6 Нажмите **Применить**.

7 Нажмите **Назад к редактору**.

8 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

При обнаружении и блокировании бесфайловых атак типа Hollowing или Doppelganging на защищаемом узле в журнале событий ViPNet EPP Сервер и Агент будут регистрироваться события **Блокирование Hollowing** или **Блокирование Doppelganging** соответственно.

Настройка веб-фильтров

База правил содержит предустановленные веб-фильтры (см. Блокировка доступа к вредоносным веб-ресурсам) для защищаемых узлов с ОС Windows. Для учета особенностей контроля доступа к веб-ресурсам на защищаемых узлах доступно:

- Создание веб-фильтров.

- Добавление веб-фильтров в избранное для возможности использования в других базах правил.
- Импорт из избранного ранее добавленных веб-фильтров.
- Изменение веб-фильтров.
- Изменение порядка применения веб-фильтров.
- Удаление ненужных веб-фильтров.

Адреса контролируемых веб-ресурсов в веб-фильтре могут быть заданы в виде:

- IP-адреса, только в формате IP v4, например `98.144.73.193`. Использовать маски нельзя.
- Доменного имени, 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, например `http://wasjar.dynu.net`. При задании URL-адресов:
  - В качестве хоста можно использовать доменное имя или IP-адрес в формате IP v4, 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 `\` .

Вы можете задавать адреса контролируемых веб-ресурсов вручную или добавить списком из файла. Перед добавлением адресов из файла подготовьте текстовые файлы формата `csv` с адресами веб-ресурсов, соблюдая требования:

- Для адресов каждого вида подготовьте отдельный файл.
- Адреса должны быть добавлены в соответствии с требованиями к формату для каждого вида, указанными выше.
- Каждый адрес в файле задавайте с новой строки.



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.

Общий порядок управления веб-фильтрами

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить правила HIPS, и нажмите **Открыть в редакторе**.

4 Выберите **Обнаружение и предотвращение вторжений** > **Веб-фильтры**.

5 Просмотрите текущий список веб-фильтров. Для каждого фильтра в списке отображаются:

- Название фильтра.
- Статус — включен или выключен.
- Действие — разрешает или блокирует доступ к настроенным веб-адресам.
- Журнал — регистрируются ли в журнале событий обращения к веб-ресурсам из фильтра.
- Количество ресурсов — количество контролируемых фильтром веб-адресов.

6 Добавьте, измените веб-фильтр, измените порядок применения фильтров, временно отключите или удалите ненужные фильтры в соответствии с описанием ниже.

7 Нажмите **Назад к редактору**.

8 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Создание веб-фильтра

Чтобы добавить веб-фильтр, на панели вверху нажмите **Добавить** > **Создать новый фильтр** и задайте параметры фильтра:

1 На странице **Основные настройки**:

1.1 Выберите действие фильтра при срабатывании: **Разрешить** доступ к веб-ресурсу или **Блокировать** доступ к веб-ресурсу.

1.2 Чтобы добавить адреса веб-ресурсов вручную:

1.2.1 В разделе **Веб-ресурсы** напротив формата адреса, в котором вы хотите указать адрес (**IP-адрес**, **Доменные имена** или **URL**), нажмите и выберите **Изменить**.

1.2.2 Добавьте адреса веб-ресурсов в соответствии с требованиями к формату, указанными в начале раздела.

Для ввода каждого следующего адреса веб-ресурса нажимайте клавишу **Enter**.

Если появилось сообщение о нескольких одинаковых строках, нажмите **Удалить дубликаты**.

1.2.3 Чтобы удалить добавленный веб-ресурс, выберите его в списке и нажмите клавишу **Delete**.

1.2.4 Нажмите **Сохранить**.

1.3 Чтобы добавить адреса веб-ресурсов из подготовленных файлов формата `csv`, в разделе **Веб-ресурсы** напротив формата адреса, в котором вы хотите добавить адреса (**IP-адрес**, **Доменные имена** или **URL**), нажмите ⋮ и:

1.3.1 Для добавления из файла только новых адресов, выберите **Добавить из файла** и укажите файл.

1.3.2 Для перезаписи всех имеющихся в фильтре адресов адресами из файла, выберите **Перезаписать из файла** и укажите файл. Перезапись из файла имеет смысл выбирать только при изменении веб-фильтров.

1.4 Внесите данные во все необходимые файлы в соответствии с шагами 1.2-1.3.

1.5 Нажмите **Далее**.

2 На странице **Подтверждение**:

2.1 Введите название фильтра и проверьте выбранное действие фильтра. Название фильтра должно содержать не более 30 символов и состоять из следующих символов: a-z, A-Z, 0-9, _ (нижнее подчеркивание).

2.2 Чтобы обращения к настроенным в фильтре адресам регистрировались в журнале событий, выберите **Записывать обращения к веб-ресурсу в журнал**.

2.3 Нажмите **Готово**.

2.4 Нажмите **Применить**.

Добавление веб-фильтров в избранное

В избранном сохраняются все параметры веб-фильтра, кроме статуса. При сохранении веб-фильтра в избранном проверяется на уникальность название фильтра. Идентичные фильтры не сохраняются.

Чтобы сохранить в избранном определенные веб-фильтры текущей версии базы правил:

1 В списке веб-фильтров выберите флажками фильтры, которые вы хотите сохранить в избранном.

2 На панели вверху нажмите **Добавить в избранное**.

3 Дождитесь завершения операции и нажмите **OK**.

В результате сохраненные веб-фильтры будут отображаться в разделе **Базы правил** на вкладке **Избранные правила** > **Веб-фильтрация** (см. Просмотр и удаление избранных правил).

Импорт веб-фильтров из избранного в базу правил

Чтобы добавить веб-фильтры, ранее сохраненные в избранном, в текущую версию базы правил:

1 На панели вверху нажмите **Добавить** > **Импортировать из избранного** и следуйте указаниям мастера импорта фильтра:

1.1 В окне **Импорт избранных фильтров** выберите флажками фильтры.

1.2 Нажмите **Импортировать**.

1.3 Если обнаружены веб-фильтры, уже имеющихся в базе правил, появится сообщение о наличии дубликатов. Выберите, нужно ли импортировать дубликаты фильтров или нет.

- Чтобы не импортировать дубликаты, нажмите **Да** для исключения дубликатов из импортируемого набора.
- Чтобы импортировать дубликаты, нажмите **Нет** и откажитесь от исключения дубликатов из импортируемого набора. По завершении импорта дубликаты фильтров будут добавлены в список. Нажмите **OK**. Переименуйте фильтры с одинаковыми названиями (см. сценарий «Изменение параметров веб-фильтров»).

1.4 Если дубликатов не обнаружено, нажмите **OK**.

2 Установите порядок действия фильтров, переместив импортированные фильтры на нужный уровень с помощью кнопок ↓ или ↑.

3 Нажмите **Применить**.

В результате фильтры будут добавлены в базу правил со статусом включен.

Изменение параметров веб-фильтров

1 В списке веб-фильтров дважды щелкните строку фильтра.

2 На панели справа внесите изменения в параметры фильтра. Вы можете изменить:

- название и действие фильтра;
- необходимость записи обращений к веб-ресурсу в журнал;
- контролируемый список веб-ресурсов. Внесите изменения в контролируемый список веб-ресурсов аналогично описанию в сценарии создания веб-фильтра (см шаги 1.2-1.3).

3 Нажмите **OK**.

4 Чтобы временно отключить веб-фильтр, в списке фильтров выключите **Фильтрация активна** после названия фильтра.

5 Нажмите **Применить**.

Изменение порядка применения веб-фильтров

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

1 В списке веб-фильтров выберите флажками фильтры, порядок применения которых необходимо изменить.

2 На панели вверху нажмите ↑ или ↓ для перемещения выбранных фильтров в списке.

3 Нажмите **Применить**.

Удаление ненужных веб-фильтров.

1 В списке веб-фильтров выберите флажками фильтры, которые необходимо удалить.

2 На панели вверху нажмите **Удалить** и подтвердите удаление.

3 Нажмите **Применить**.

Настройка политик аудита

База правил содержит политики аудита для защищаемых узлов с ОС Windows. Политики аудита определяют, какие типы событий ОС Windows должна записывать в журнал безопасности Windows на защищаемом узле.

Чтобы настроить политики аудита:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Базы правил**.

3 В списке баз правил дважды щелкните базу правил, для которой требуется настроить правила HIPS, и нажмите **Открыть в редакторе**.

4 Выберите **Обнаружение и предотвращение вторжений** > **Политики аудита**.

5 Настройте политики, выбирая вкладки категорий:

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. Слишком большое количество отслеживаемых объектов может приводить к значительному потреблению ресурсов компьютера.

- **Аутентификация** — политика аудита аутентификации пользователей (см. Политика аудита аутентификации пользователей в ОС Windows).
- **Реестр** — политика аудита изменений в реестре.

- **Файловая система** — политика аудита изменений в файловой системе.
- **Управление учетными записями** — политика аудита управления учетными записями.
- **Прочие** — политика аудита для отслеживания других типов событий (см. Другие политики аудита).

6 Нажмите **Назад к редактору**.

7 Чтобы сохранить изменения и разослать новую версию базы правил на группы защищаемых узлов, нажмите **Сохранить** или **Назад к EndPoint Protection,** затем для подтверждения нажмите **Да.**

Политика аудита аутентификации пользователей в ОС Windows

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

1 На вкладке **Аутентификация** выберите операции аутентификации пользователей, которые должны отслеживаться.

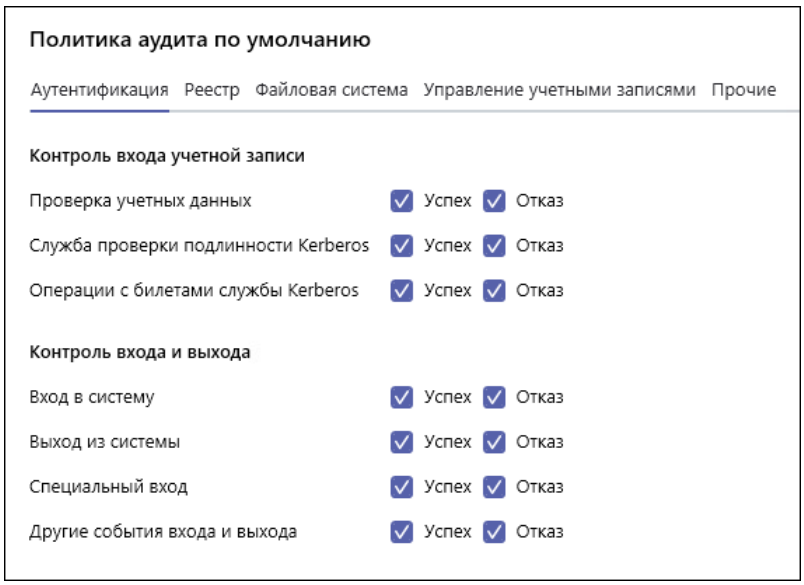


Рисунок 61. Настройка политик аудита для событий аутентификации пользователей

2 Нажмите **Сохранить**.

Политика аудита изменений в реестре

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

1 На вкладке **Реестр** в разделе **Аудируемые пути** щелкните раздел реестра, для которого вы будете настраивать политику аудита:

1.1 Выберите операции с разделом реестра, которые должны отслеживаться.

1.2 Выберите область применения политики.

1.3 Задайте подразделы реестра из раздела, указанного на шаге 1, для которых политика применяться не будет. Для этого в разделе **Исключения** нажмите ⊕ **Добавить** и введите путь к подразделу. Нажмите **Сохранить**.

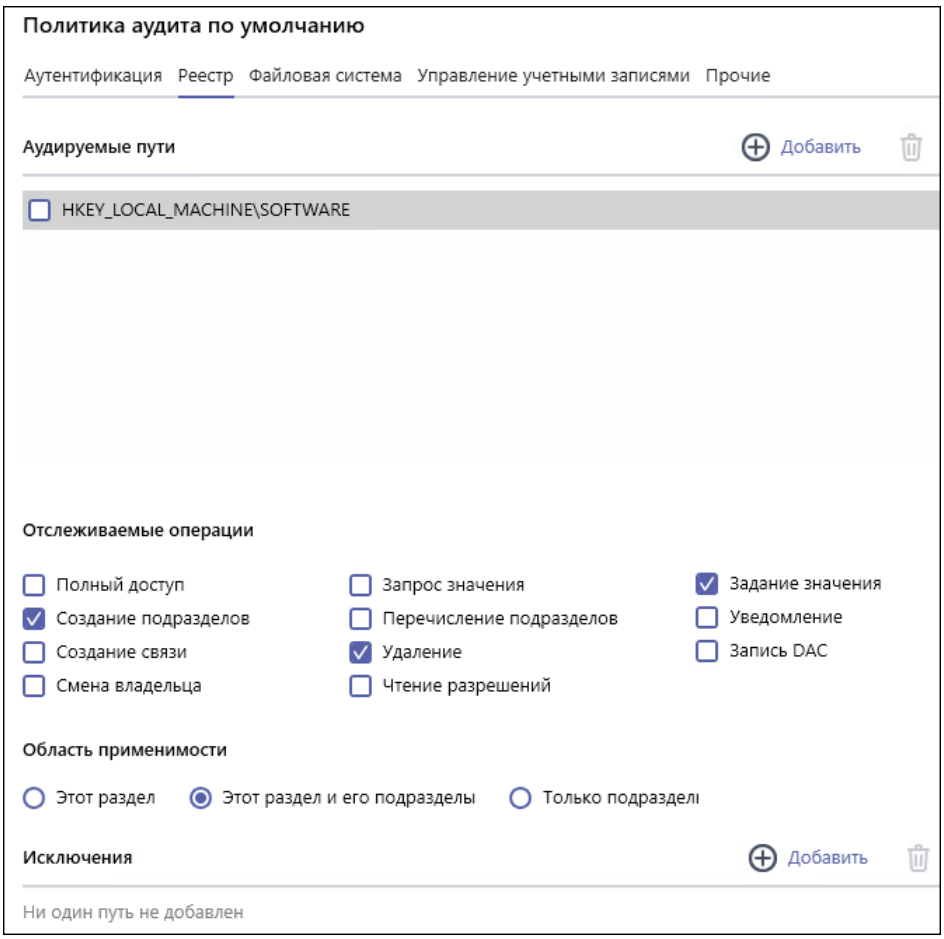


Рисунок 62. Настройка политик аудита для отслеживания изменений в реестре

2 Добавьте другие разделы реестра, которые вы хотите отслеживать. Для этого в разделе **Аудируемые пути** нажмите ⊕ **Добавить** и введите путь к разделу. Нажмите **Сохранить**.

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`

---

3 Повторите шаг 1 для каждого раздела реестра в разделе **Аудируемые пути**.

4 Нажмите **Сохранить**.

Политика аудита изменений в файловой системе

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

1 На вкладке **Файловая система** в разделе **Аудируемые пути** щелкните путь к папке, для которого вы будете настраивать политику аудита, и:

1.1 Выберите операции с файлами, которые должны отслеживаться.

1.2 Выберите область применения политики.

1.3 Задайте подпапки папки, указанной на шаге 1, для которых политика применяться не будет. Для этого в разделе **Исключения** нажмите ⊕ **Добавить** и введите путь к подпапке. Нажмите **Сохранить**.

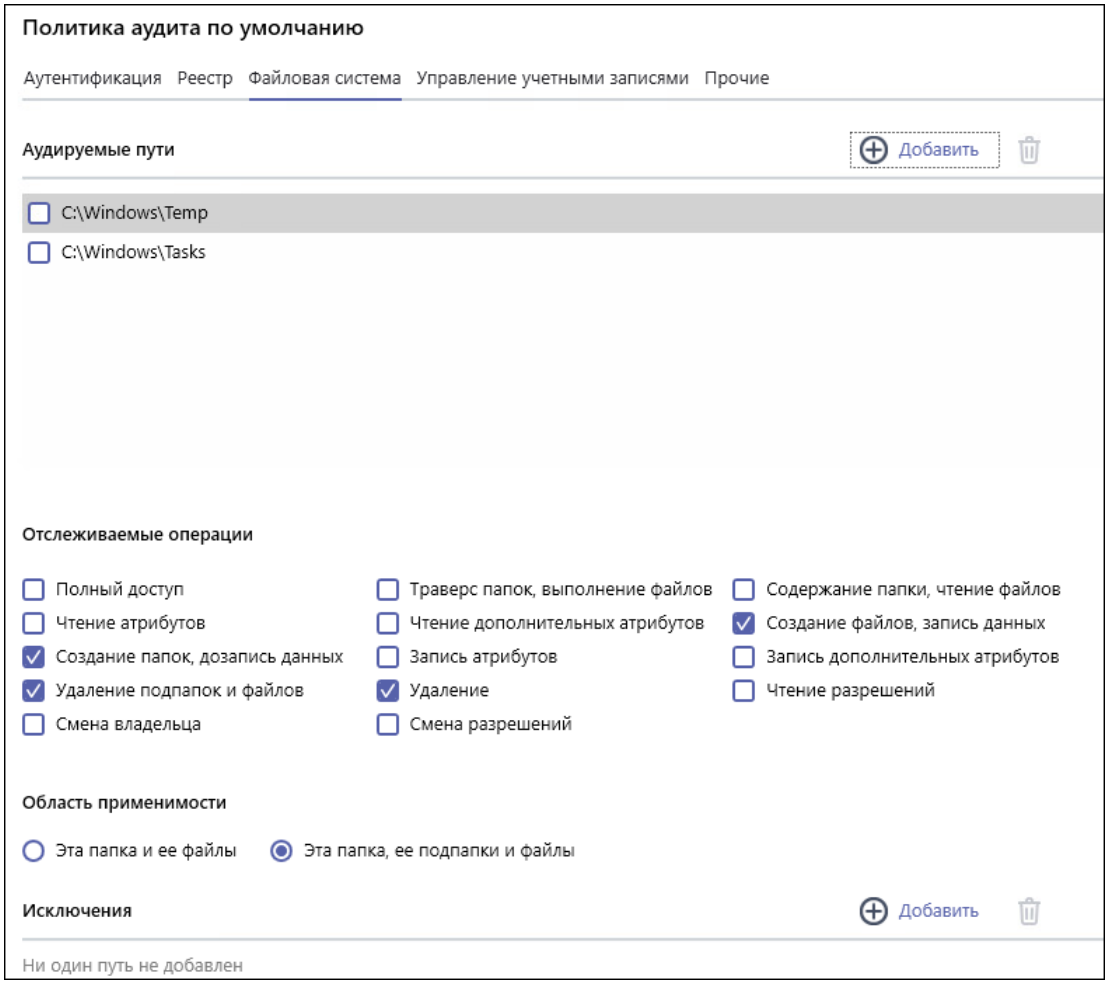


Рисунок 63. Настройка политик аудита для отслеживания изменений в файловой системе

2 Добавьте другие пути к папкам, которые вы хотите отслеживать. Для этого в разделе **Аудируемые пути** нажмите ⊕ **Добавить** и введите путь к папке. Нажмите **Сохранить**.

3 Повторите шаг 1 для каждого пути к папке в разделе **Аудируемые пути**.

4 Нажмите **Сохранить**.

Если у вас включено отслеживание записей в журналах приложений и служб (см. Отслеживание изменений в журналах приложений и служб) и настроена политика аудита для соответствующих папок, изменения в файлах этих папок будут отслеживаться.

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 На вкладке **Управление учетными записями** выберите операции с учетными записями, которые должны отслеживаться.

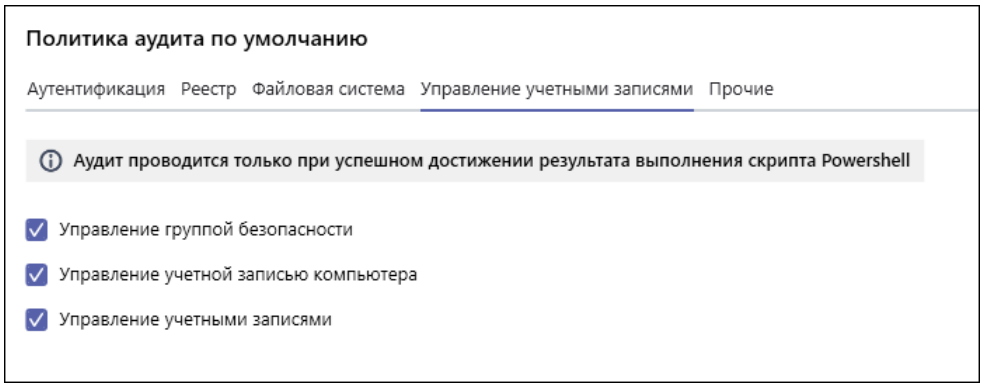


Рисунок 64. Настройка политик аудита управления учетными записями

2 Нажмите **Сохранить**.

Другие политики аудита

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

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

1 На вкладке **Прочие** выберите операции, которые должны отслеживаться.

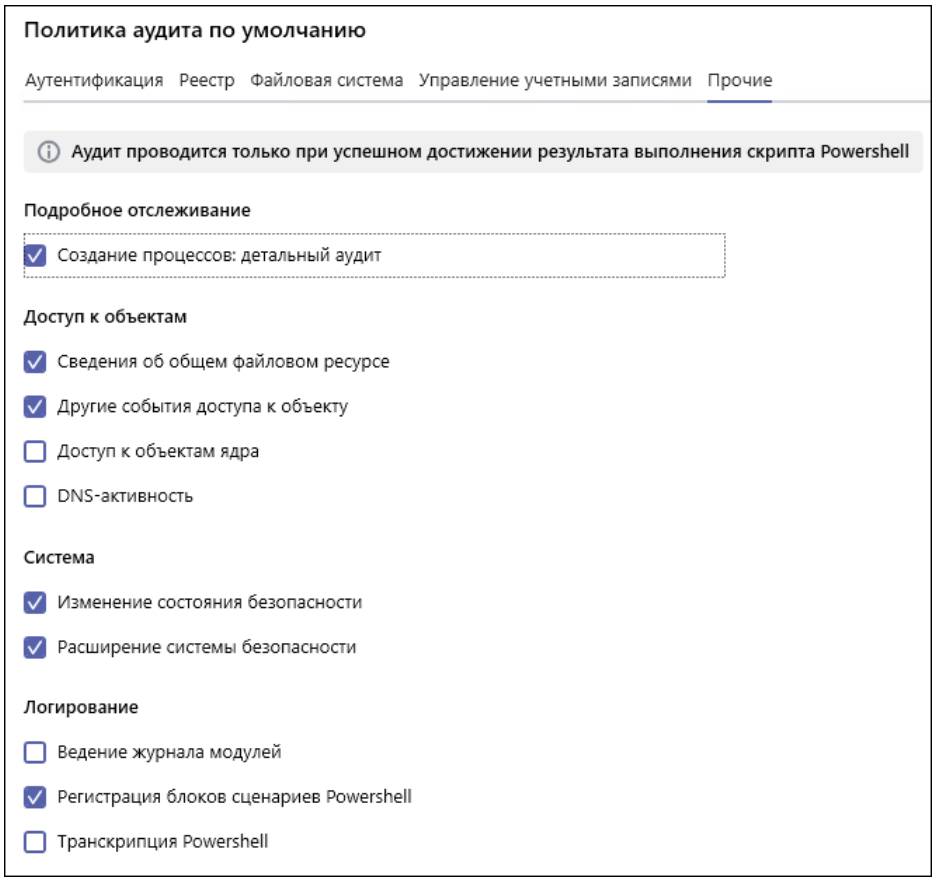


Рисунок 65. Настройка дополнительных политик аудита

2 Нажмите **Сохранить**.

Управление ViPNet SafeBoot на защищаемых узлах

Порядок управления

Чтобы в ViPNet EPP Сервер управлять ViPNet SafeBoot, установленными на защищаемых узлах (см. Управление доверенной загрузкой), получите в ИнфоТеКС:

1. Лицензию ViPNet EPP с разрешением на использование модуля SafeBootMC и максимальным количеством доступных для управления узлов (если текущая лицензия уже не содержит это разрешение).
2. Лицензии ViPNet SafeBoot для установки и активации на защищаемых узлах с ViPNet SafeBoot.



Внимание! Защищаемые узлы должны быть активны и доступны по сети в момент выполнения действий:

- Управление лицензиями.
- Просмотр учетных записей пользователей, корневых сертификатов, CRL, уже существующих на защищаемых узлах.
- Управление учетными записями.
- Выгрузка журналов аудита.

Для выполнения остальных действий защищаемый узел в момент выполнения действия может быть не доступен по сети, изменения будут применены в ViPNet SafeBoot после подключения узла к сети и повторной перезагрузки компьютера.

Порядок подготовки к управлению ViPNet SafeBoot на защищаемых узлах:

	Действие	Ссылка
☐	Убедитесь, что в лицензии ViPNet EPP доступно использование модуля SafeBootMC. Если недоступно, обновите лицензию	Обновление лицензии
☐	Подключите защищаемые узлы к ViPNet EPP Сервер, разрешив работу модуля SafeBootMC	Подключение защищаемых узлов
☐	Проверьте, установлен ли на защищаемых узлах ViPNet SafeBoot	Просмотр информации о версии и состоянии ViPNet SafeBoot на защищаемых узлах
☐	Установите ViPNet SafeBoot поддерживаемой версии на те защищаемые узлы, где он еще не установлен	В соответствии с документацией к ViPNet SafeBoot Совместимость ViPNet EPP со сторонним программным обеспечением
☐	В настройках ViPNet SafeBoot разрешите удаленное управление	В соответствии с документацией к ViPNet SafeBoot
☐	Загрузите лицензии ViPNet SafeBoot на ViPNet EPP Сервер	Загрузка лицензий ViPNet SafeBoot на ViPNet EPP Сервер
☐	Отправьте и активируйте лицензии ViPNet SafeBoot на защищаемых узлах, на которых еще нет лицензий	Распределение, отправка и активация лицензии ViPNet SafeBoot на защищаемых узлах

После подключения защищаемых узлов с ViPNet SafeBoot поддерживаемой версии (см. Совместимость ViPNet EPP со сторонним программным обеспечением) и распределения лицензий будут доступны следующие возможности управления:

- Просмотр, создание, редактирование и удаление учетных записей пользователей ViPNet SafeBoot.
- Отправка обновления ViPNet SafeBoot. Эта возможность доступна и до распределения лицензии на защищаемый узел с ViPNet SafeBoot.
- Просмотр, отправка и выгрузка корневых сертификатов и CRL.
- Выгрузка журнала аудита с защищаемых узлов — доступна как для узлов с распределенной лицензией, так и для узлов без лицензии.

Просмотр информации о версии и состоянии ViPNet SafeBoot на защищаемых узлах

После подключения к ViPNet EPP Сервер защищаемые узлы с разрешенным модулем SafeBootMC (далее — защищаемые узлы с SafeBoot) отображаются в разделе **Доверенная загрузка** в группах, в которые узлы были распределены при подключении. Для каждого узла доступна информация о его состоянии, установленной версии ViPNet SafeBoot, установленной лицензии и состоянии процесса обновления ПО.

Чтобы просмотреть информацию о защищаемых узлах с SafeBoot:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите группу, в который расположены защищаемые узлы с SafeBoot.

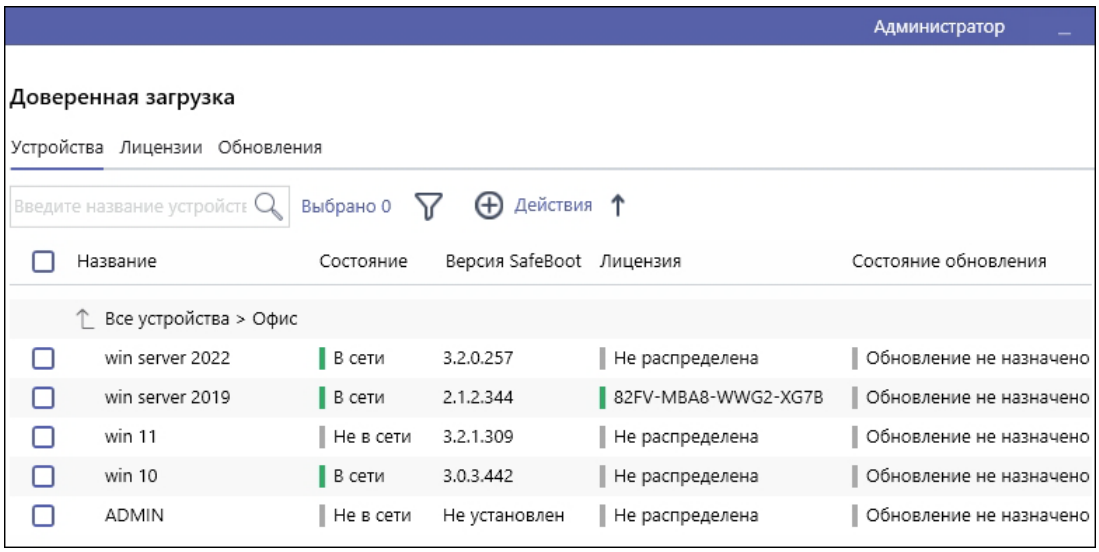


Рисунок 66. Просмотр информации о защищаемых узлах с SafeBoot

Для защищаемого узла в списке отображаются:

- **Название** — имя защищаемого узла.
- **Состояние** — активность узла:
  - **В сети** — узел активен, он регулярно обменивается данными с ViPNet EPP Сервер.
  - **Не в сети** — узел неактивен. В течение времени, определяемого параметром **Период неактивности** (см. Настройка параметров системы), не было обмена данными с ViPNet EPP Сервер. Это означает, что связь с узлом потеряна и ряд действий по управлению ViPNet SafeBoot будет недоступно (см. Порядок управления).
- **Версия SafeBoot** — установлен ли на узле ViPNet SafeBoot:
  - **Не установлен** — на узле ViPNet SafeBoot не установлен.
  - Если ViPNet SafeBoot установлен на узле, отображается номер версии.

- **Лицензия** — информация о лицензии ViPNet SafeBoot, установленной на узле:
  - **Не распределена** — на узле еще нет лицензии.
  - **Не активирована** — на узле лицензия установлена, но еще не активирована.
  - **Активирована** — на узле лицензия установлена и активирована.
  - **Недействительна** — на узле лицензия установлена, но при активации лицензия была отклонена сервером активации, как недействительная.
- **Состояние обновления** — информация о состоянии обновления ViPNet SafeBoot, отправленного на узел:
  - **Обновление не назначено** — обновление еще не назначено.
  - **Ожидает обновления** — обновление назначено, но на узле процесс обновления еще не запущен. В этом состоянии доступна отмена обновления.
  - **Идет процесс обновления** — обновление на узле в процессе установки. В этом состоянии нельзя отправить узлу новое обновление ViPNet SafeBoot. После завершения процесса обновления статус сменится на **Обновление не назначено**.

4 Чтобы в списке узлов найти определенные узлы:

- В поле поиска введите часть имени узла или имя целиком и нажмите .
- Нажмите и выберите критерии фильтрации: состояние устройства, установленная версия SafeBoot, состояние лицензии. Нажмите **Применить**.

Управление лицензиями

Загрузка лицензий ViPNet SafeBoot на ViPNet EPP Сервер

Лицензии на использования ViPNet SafeBoot должны быть получены в ИнфоТеКС. Лицензия ViPNet SafeBoot для одного узла представляет из себя серийный номер вида `XXXX-XXXX-XXXX-XXXX`, например `9YDS-YHDE-WBG1-XF7B`. Каждая лицензия предназначена для определенной версии ViPNet SafeBoot. Перед отправкой лицензий на защищаемые узлы, загрузите их на ViPNet EPP Сервер. Вы можете загружать лицензии, как вводя серийные номера вручную, так и указав файл со списком серийных номеров. Текстовый файл (*.txt) со списком серийных номеров необходимо подготовить самостоятельно, указав каждый серийный номер с новой строки.

Чтобы загрузить лицензии ViPNet SafeBoot в ViPNet EPP Сервер:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Лицензии**.

3 Чтобы загрузить лицензии из подготовленного файла, нажмите **Из файла** и выберите файл.

4 Чтобы загрузить лицензии вручную, нажмите **Ввести номер** и введите один или несколько серийных номеров по одному в каждой строке. Нажмите **Добавить**.

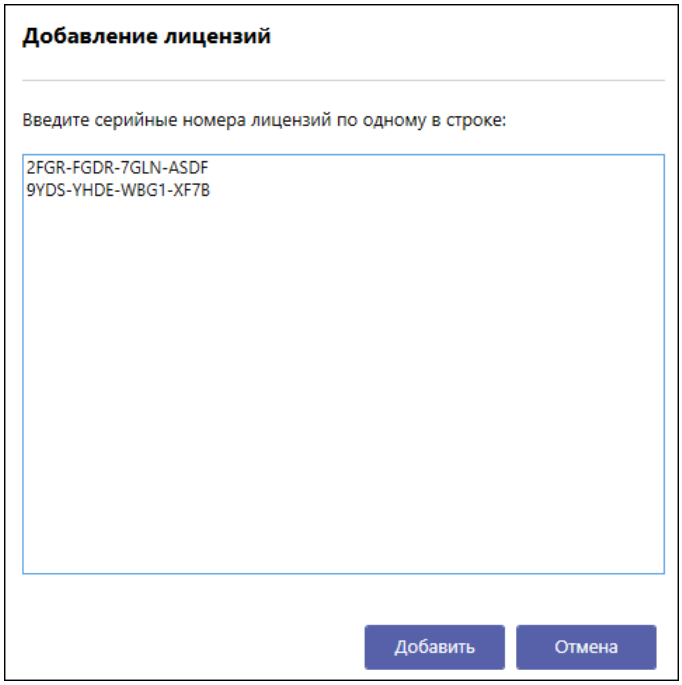


Рисунок 67. Добавление серийных номеров вручную

Информация о добавленных лицензиях появится на вкладке **Лицензии** (см. Просмотр информации о свободных лицензиях ViPNet SafeBoot).

Просмотр информации о свободных лицензиях ViPNet SafeBoot

Вы можете отслеживать информацию о количестве лицензий ViPNet SafeBoot для разных версий, загруженных в ViPNet EPP Сервер, распределенных и отправленных на защищаемые узлы, а также свободных. Для свободных лицензий доступен просмотр списка серийных номеров.

Чтобы посмотреть информацию о количестве лицензий ViPNet SafeBoot:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Лицензии**.



Рисунок 68. Просмотр информации о количестве лицензий ViPNet SafeBoot

Для каждой версии ViPNet SafeBoot в списке отображаются:

- **Свободно** — количество неиспользованных лицензий, т.е. лицензии еще не были распределены и отправлены на узлы.
- **Распределено** — количество уже распределенных и отправленных на узлы лицензий.
- **Всего** — общее количество загруженных лицензий.

Чтобы посмотреть информацию о свободных лицензиях для определенной версии ViPNet SafeBoot, щелкните значение в столбце **Свободно**. Отобразится список свободных серийных номеров.

Распределение, отправка и активация лицензии ViPNet SafeBoot на защищаемых узлах

Распределение, отправка и активация лицензии доступны для защищаемых узлов с ViPNet SafeBoot, если лицензия еще не установлена либо установлена, но не активирована, а также если не закончился деморежим ViPNet SafeBoot. Защищаемые узлы должны находиться в состоянии **В сети**. Также для успешной отправки лицензии убедитесь, что на ViPNet EPP Сервер есть свободные лицензии для нужной версии ViPNet SafeBoot (см. Просмотр информации о свободных лицензиях ViPNet SafeBoot).

Отправлять лицензии можно сразу на группы защищаемых узлов или отдельным узлам в выбранной группе.

Чтобы распределить и отправить или активировать лицензию на защищаемых узлах:

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите **Доверенная загрузка** > **Устройства**.
3. Выберите флажками одну или несколько групп с защищаемыми устройствами или защищаемые устройства в выбранной группе и нажмите **Действия** > **Активировать лицензию**.

В результате на узлах, которые находятся в сети:

- Если на узле еще нет лицензии, будет распределена и отправлена лицензия для версии ViPNet SafeBoot, установленной на узле, и автоматически активирована.

- Если на узле лицензия установлена, но не активирована, лицензия на узле автоматически активируется.

В случае недостаточного количества загруженных лицензий или проблем с активацией появится соответствующее предупреждение.

Выгрузка журнала аудита ViPNet SafeBoot с защищаемых узлов

Для успешной выгрузки журнала аудита защищаемые узлы с ViPNet SafeBoot должны находиться в состоянии **В сети**. При выгрузке журнал аудита сохраняется в текстовый файл. Для каждого защищаемого узла формируется отдельный файл в формате: `<дата и время выгрузки журнала>_<имя узла>_<идентификатор агента>.log`

Выгружать журнал аудита можно как с отдельных защищаемых узлов, так и сразу с групп защищаемых узлов или нескольких узлов в выбранной группе.

Чтобы выгрузить журнал аудита с защищаемых узлов:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите флажками одну или несколько групп с защищаемыми узлами или защищаемые узлы в выбранной группе и нажмите **Действия** > **Выгрузить журнал аудита**.

4 Укажите папку сохранения файла с журналом и нажмите **OK**.

5 В появившемся окне нажмите **OK**.

Примечание. При неуспешной попытке выгрузки журнала аудита с нескольких устройств в журнале аудита будет зарегистрировано только одно событие для первого устройства из списка выбранных.

Управление учетными записями пользователей ViPNet SafeBoot

Вы можете управлять учетными записями пользователей ViPNet SafeBoot на защищаемых узлах.

Доступны следующие действия:

- Просмотр информации об учетных записях пользователей.
- Добавление новой учетной записи пользователя.

- Изменение параметров учетной записи пользователя, в том числе блокирование учетной записи на защищаемом узле.
- Удаление учетной записи.

Управлять учетными записями ViPNet SafeBoot можно как на отдельных защищаемых узлах, так и сразу на группах защищаемых узлов или нескольких узлах в выбранной группе. Просмотр информации об учетных записях доступен только для выбранного защищаемого узла.

Для возможности управления учетными записями защищаемый узел должен находиться в состоянии **В сети**. Все изменения учетных записей будут применены в ViPNet SafeBoot на защищаемых узлах после перезагрузки компьютеров узлов и только в том случае, если в ViPNet SafeBoot такие операции применимы.

В ViPNet EPP Сервер сразу после внесения изменений в учетные записи ViPNet SafeBoot измененные данные отобразятся в списке учетных записей для соответствующих узлов (см. Просмотр учетных записей на защищаемых узлах). Это подтверждает факт отправки данных на защищаемые узлы с ViPNet SafeBoot, но не факт применения в ViPNet SafeBoot. Подтверждением успешного применения изменений учетных записей на защищаемых узлах в ViPNet SafeBoot будет служить отображение информации об изменениях учетных записей (см. Просмотр учетных записей на защищаемых узлах) после перезагрузки компьютера защищаемого узла.

Просмотр учетных записей на защищаемых узлах

Для просмотра учетных записей пользователей ViPNet SafeBoot защищаемый узел должен находиться в состоянии **В сети**.

Чтобы просмотреть информацию об учетных записях пользователей ViPNet SafeBoot на защищаемом узле:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите группу, дважды щелкните защищаемый узел с SafeBoot.

4 На панели справа на вкладке **Пользователи** просмотрите имена учетных записей, роли, время действия пароля, заблокирована учетная запись или нет. Для просмотра подробной информации, выберите учетную запись и нажмите . В открывшемся окне вы сможете посмотреть информацию и внести изменения (см. Изменение параметров и блокировка учетной записи).

Изменение параметров и блокировка учетной записи

Вы можете изменять следующие параметры учетных записей:

- Пароль и срок действия пароля. Доступно только для учетных записей со способом аутентификации **По паролю**. Срок действия пароля можно изменить только одновременно со сменой пароля.
- Блокировка учетной записи.

Вы можете просмотреть, включен ли для учетной записи пользователя ViPNet SafeBoot режим Single Sign-On. Настройка режима Single Sign-On в ViPNet EPP недоступна.

Чтобы изменить параметры учетной записи пользователя ViPNet SafeBoot или заблокировать учетную запись на выбранных защищаемых узлах:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите один из способов изменения:

   - Чтобы изменить учетную запись на одном защищаемом узле, дважды щелкните защищаемый узел, на панели справа на вкладке **Пользователи** выберите учетную запись и справа от названия нажмите . Защищаемый узел должен находиться в состоянии **В сети**.
   - Чтобы изменить одну одинаковую учетную запись сразу на нескольких защищаемых узлах, выберите флажками одну или несколько групп с защищаемыми узлами или один или несколько защищаемых узлов в группе и нажмите **Действия** > **Изменить учетную запись**. В окне группового редактирования в поле **Имя** введите имя учетной записи, которую нужно изменить.

Примечание. В ViPNet SafeBoot имя учетной записи и роль изменять нельзя, поэтому в ViPNet EPP они тоже недоступны для изменения.

---

4 Чтобы заблокировать учетную запись пользователя ViPNet SafeBoot на защищаемом узле, выберите **Заблокировать пользователя**.

5 Чтобы посмотреть настройку режима Single Sign-On для учетной записи, проверьте наличие флажка в **Single Sign-On**. Режим включен, если в **Single Sign-On** установлен флажок.

6 Чтобы изменить пароль и параметры пароля, снимите флажок **Не изменять настройки аутентификации пользователя** и внесите изменения:

Примечание. Если в **Способ аутентификации** указано значение, отличное от **По паролю**, снять флажок **Не изменять настройки аутентификации пользователя** и изменить параметры учетной записи невозможно.

6.1 Введите новый пароль в поле **Пароль** и **Повторите пароль**. Минимальная и максимальная длина пароля должна удовлетворять требованиям, отображаемым в соответствующих полях. Остальные параметры пароля аналогичны указанным в разделе создания учетной записи в зависимости от выбора **Использовать простой пароль**.

Количество попыток ввода пароля изменить нельзя. Отображается значение по умолчанию (16) или значение, заданное в ViPNet SafeBoot.

6.2 Чтобы изменить срок действия пароля, укажите значение от 1 до 1095 дней или выберите **Бессрочный пароль**.

7 Нажмите **Готово**.

Данные об изменениях учетной записи будут отправлены на защищаемые узлы для применения изменений в ViPNet SafeBoot.

Добавление новых учетных записей

Чтобы добавить новую учетную запись пользователя ViPNet SafeBoot с аутентификацией по паролю на выбранных защищаемых узлах:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите флажками одну или несколько групп с защищаемыми узлами или несколько защищаемых узлов в группе и нажмите **Действия** > **Создать учетную запись**.

Если защищаемый узел с SafeBoot находится в состоянии **В сети**, для создания учетной записи на нем вы можете воспользоваться способом: дважды щелкните защищаемый узел и на панели справа на вкладке **Пользователи** нажмите **Добавить**.

4 В окне **Создание учетной записи** укажите:

- **Имя** — имя учетной записи в соответствии с требованиями:

  Имя учетной записи пользователя может содержать:

  - от 4 до 32 символов;
  - прописные буквы латинского алфавита от A до Z;
  - строчные буквы латинского алфавита от a до z;
  - десятичные цифры от 0 до 9;
  - другие символы, кроме \ и №.

- **Роль** — полномочия учетной записи: администратор, аудитор, пользователь. О полномочиях пользователей ViPNet SafeBoot см. в документации к продукту ViPNet SafeBoot.

- Если нужно сразу заблокировать учетную запись пользователя ViPNet SafeBoot на защищаемом узле, выберите **Заблокировать пользователя**.

- **Single Sign-On** — флажок снят. Учетная запись будет создана с выключенным режимом Single Sign-On. Настройка этого режима недоступна в ViPNet EPP.

- **Пароль** и **Повторите пароль** — пароль пользователя в соответствии с требованиями:

- По умолчанию выбрано **Использовать простой пароль**. Введите пароль в соответствии с требованиями:
    - Минимальная длина пароля — 8 символов.
    - Максимальная длина — 31 символ.
    - Допустимо использовать 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 `!@#$%^&*()-_+=;:'",.<>/?\|`~[]{}.`
- В целях безопасности использовать простые пароли не рекомендуется. Чтобы задать надежный пароль, снимите флажок **Использовать простой пароль** и введите пароль в соответствии с требованиями:
    - Длина пароля — аналогично простому паролю.
    - В пароле должны одновременно присутствовать символы четырех категорий, перечисленных выше для простого пароля.

- **Количество попыток ввода пароля** — количество неудачных попыток аутентификации пользователя подряд, после которых учетная запись будет заблокирована. Установлено значение `16`. Параметр изменить нельзя.
- **Действие пароля в днях** — срок действия пароля учетной записи. По умолчанию 30 дней. Вы можете задать значения от 1 до 1095 дней включительно.
- Чтобы пароль не имел срока действия, выберите **Бессрочный пароль**.

5 Нажмите **Готово**.

Данные об учетной записи будут отправлены на защищаемые узлы для добавления учетной записи пользователя в ViPNet SafeBoot.

Удаление учетных записей

Чтобы удалить учетную запись пользователя ViPNet SafeBoot на выбранных защищаемых узлах:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите один из способов удаления:

- Чтобы удалить учетную запись на одном защищаемом узле, дважды щелкните защищаемый узел, на панели справа на вкладке **Пользователи** выберите флажком учетную запись и нажмите **Удалить**. Защищаемый узел должен находиться в состоянии **В сети**.
- Чтобы удалить одну одинаковую учетную запись сразу на нескольких защищаемых узлах, выберите флажками одну или несколько групп с защищаемыми узлами или несколько защищаемых узлов в группе и нажмите **Действия** > **Удалить учетную запись**. В окне группового удаления в поле **Имя** введите имя учетной записи, которую нужно удалить.

Примечание. Учетную запись Administrator, созданную в ViPNet SafeBoot по умолчанию, удалить нельзя.

4 Подтвердите удаление.

Данные об удалении учетной записи будут отправлены на защищаемые узлы для удаления этой учетной записи в ViPNet SafeBoot.

Обновление ViPNet SafeBoot на защищаемых узлах

В ViPNet EPP Сервер вы можете обновлять ViPNet SafeBoot на защищаемых узлах. Обновление доступно для защищаемых узлов как с распределенной лицензией, так и без лицензии, а также если не закончился деморежим ViPNet SafeBoot. Отправлять обновление можно как на отдельные защищаемые узлы, так и сразу на группы защищаемых узлов или нескольким узлам в выбранной группе. Обновление будет установлено на защищаемых узлах только после их перезагрузки.

Пока на защищаемом узле не запустился процесс обновления ViPNet SafeBoot, вы можете отменить обновление.

Внимание! Если на защищаемый узел отправлено обновление ViPNet SafeBoot, требующее установки новой лицензии (при изменении первой цифры номера версии, например, обновление ViPNet SafeBoot версии 2.1.2 на 3.0.3), перед перезагрузкой компьютера обновляемого защищаемого узла убедитесь, что к компьютеру не подключен USB-носитель с установочным пакетом ViPNet SafeBoot.

Получите архивы обновления ViPNet SafeBoot в ИнфоТеКС и загрузите их в ViPNet EPP Сервер (см. Загрузка и удаление обновлений на ViPNet EPP Сервер).

Если помимо архива обновления ViPNet SafeBoot есть архив расширения для установки, перед загрузкой в ViPNet EPP Сервер упакуйте их в один архив:

1 Создайте копию архива обновления ViPNet SafeBoot и задайте другое имя, например, связанное с применением расширения.

2 Откройте созданную копию архива и добавьте в него содержимое архива расширения.

3 Сохраните архив и загрузите его в ViPNet EPP Сервер (см. Загрузка и удаление обновлений на ViPNet EPP Сервер).

Внимание! Обновление с помощью архива обновления ViPNet SafeBoot, включающего в себя расширение снятия защиты платформы, не будет выполнено. В поддерживаемых версиях ViPNet SafeBoot это не реализовано. Обновить можно локально путем полного удаления и последующей установкой ViPNet SafeBoot.

Перед отправкой обновления на защищаемых узлах в ViPNet SafeBoot экспортируйте настройки и журнал на любой USB-носитель (см. «ViPNet SafeBoot. Руководство администратора», разделы «Импорт настроек», «Экспорт записей журнала событий»). Во время обновления все настройки ViPNet SafeBoot будут удалены.

Чтобы отправить обновление ViPNet SafeBoot на защищаемые узлы:

1 Убедитесь, что сервер активации лицензий доступен по сети, выполнив команду: `ping regboxproduct.infotecs.ru`

2 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

3 Выберите **Доверенная загрузка** > **Устройства**.

4 Выберите флажками одну или несколько групп с защищаемыми узлами или один или несколько защищаемых узлов в группе и нажмите **Действия** > **Установить обновление**.

5 Выберите обновление в списке и проверьте список защищаемых узлов, которые были выбраны для отправки обновления, и посмотрите информацию о планируемом обновлении.

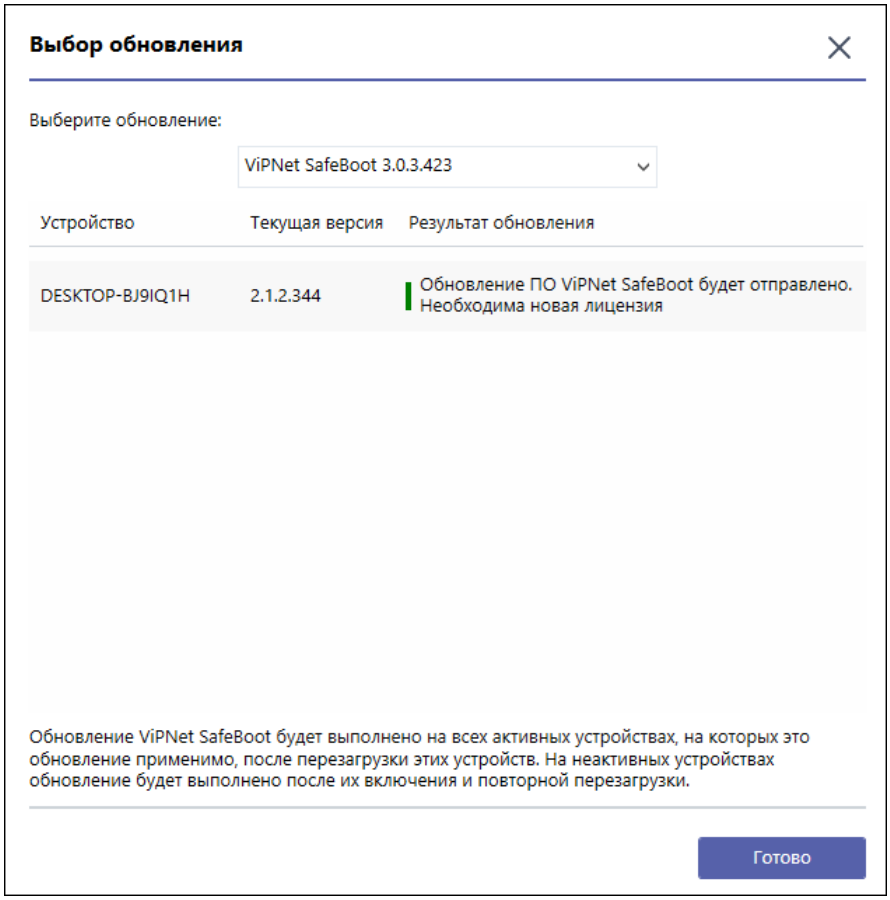


Рисунок 69. Выбор и просмотр параметров обновления

Для каждого защищаемого узла в списке отображаются:

- **Устройство** — имя защищаемого узла.
- **Текущая версия** — версия ViPNet SafeBoot, установленная на защищаемом узле в настоящий момент.

- **Результат обновления** — дополнительная информация о планируемом обновлении:
  - `Обновление ПО ViPNet SafeBoot не выбрано` — вы не выбрали обновление для отправки.
  - `Обновление ПО ViPNet SafeBoot отправлено не будет` — на защищаемый узел выбранное обновление отправлено не будет, например, если на узле не установлен ViPNet SafeBoot или установлена версия, выше отправляемой.
  - `Агент в процессе обновления ПО ViPNet SafeBoot` — на защищаемый узел выбранное обновление отправлено не будет, поскольку предыдущее обновление на узле еще в процессе установки (состояние обновления для узла — **Идет процесс обновления**).
  - `Обновление ПО ViPNet SafeBoot будет отправлено. Необходима новая лицензия` — для обновления ViPNet SafeBoot на защищаемом узле потребуется новая лицензия. В этом случае при отправке обновления лицензия будет автоматически выделена из числа свободных и активирована на защищаемом узле в процессе обновления ViPNet SafeBoot. Убедитесь, что у вас хватает лицензий для этого обновления (см. Просмотр информации о свободных лицензиях ViPNet SafeBoot), иначе обновление отправлено не будет.
  - `Обновление ПО ViPNet SafeBoot будет отправлено` — на защищаемый узел будет отправлено обновление, новая лицензия не потребуется.
  - `Обновление ПО ViPNet SafeBoot будет отправлено после включения устройства` — защищаемый узел находится не в сети, обновление будет отправлено после подключения узла к сети.

6 Нажмите **Готово** и подтвердите отправку обновления.

Чтобы отменить обновление ViPNet SafeBoot, которое отправлено, но еще не запущено на узлах (состояние обновления для узла — **Ожидает обновления**):

1 На странице **Доверенная загрузка** на вкладке **Устройства** выберите флажками защищаемые узлы, на которых нужно отменить обновление, и нажмите **Действия** > **Отменить обновление**.

2 Подтвердите отмену обновления.

При получении обновления на защищаемом узле появится уведомление. Чтобы обновление было установлено на защищаемом узле, перезагрузите компьютер защищаемого узла. Если при отправке обновления защищаемый узел не был доступен по сети (имел состояние **Не в сети**), обновление ViPNet SafeBoot будет установлено после его подключения к сети и повторной перезагрузки компьютера.

Внимание! При перезагрузке компьютера с ViPNet SafeBoot нельзя отключать питание компьютера. Для применения обновления требуется дополнительное время, поэтому перезагрузка будет выполняться дольше обычного.

Примечание. В процессе обновления ViPNet SafeBoot на защищаемом узле файлы обновления будут временно помещены в корень диска C. После завершения обновления файлы удалятся.

Если обновление ViPNet SafeBoot успешно установилось на защищаемом узле, информация о номере версии отобразится для этого узла в списке устройств в столбце **Версия SafeBoot** (см. Просмотр информации о версии и состоянии ViPNet SafeBoot на защищаемых узлах).

Загрузка и удаление обновлений на ViPNet EPP Сервер

Чтобы загрузить обновление ПО ViPNet SafeBoot на ViPNet EPP Сервер:

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите **Доверенная загрузка** > **Обновления**.
3. Нажмите **Загрузить** и выберите файл в формате ZIP.

Информация о добавленных обновлениях появится на вкладке **Обновления**.

Если обновление более не требуется, вы можете удалить его. Перед удалением убедитесь, что обновление применилось на всех защищаемых узлах, на которые оно было отправлено. После удаления обновления с ViPNet EPP Сервер, оно не будет применено на защищаемых узлах, на которые это обновление было отправлено, но еще не применялось.

Чтобы удалить обновления:

1. На вкладке **Обновления** выберите флажками обновления и на панели вверху нажмите .
2. Подтвердите удаление.

Управление корневыми сертификатами и CRL

Корневые сертификаты и CRL требуются в ViPNet SafeBoot для аутентификации пользователей с помощью внешнего устройства. В ViPNet EPP Сервер вы можете управлять корневыми сертификатами и CRL на защищаемых узлах с ViPNet SafeBoot.

Доступны следующие действия:

- Просмотр информации о сертификатах, установленных на защищаемых узлах; выгрузка их в файл; загрузка на ViPNet EPP Сервер и удаление сертификатов.
- Установка сертификатов и CRL на защищаемые узлы.

Управлять сертификатами и CRL можно как на отдельных защищаемых узлах, так и сразу на группах защищаемых узлов или нескольких узлах в выбранной группе. Просмотр информации о

сертификатах и действия с сертификатами, установленными на защищаемых узлах, доступны только для одного выбранного защищаемого узла.

Просмотр информации о сертификатах на защищаемых узлах, выгрузка и удаление сертификатов

Чтобы просмотреть информацию о корневых сертификатах и CRL, установленных на защищаемом узле с ViPNet SafeBoot:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите группу, дважды щелкните защищаемый узел с SafeBoot. Защищаемый узел должен находиться в состоянии **В сети**.

4 На панели справа на вкладке **Сертификаты** просмотрите информацию об установленных корневых сертификатах и CRL. Если на защищаемом узле есть установленные сертификаты, они будут отображаться в столбцах:

- **Сертификат** — корневые сертификаты.
- **Список отзыва сертификатов** — CRL для корневого сертификата.

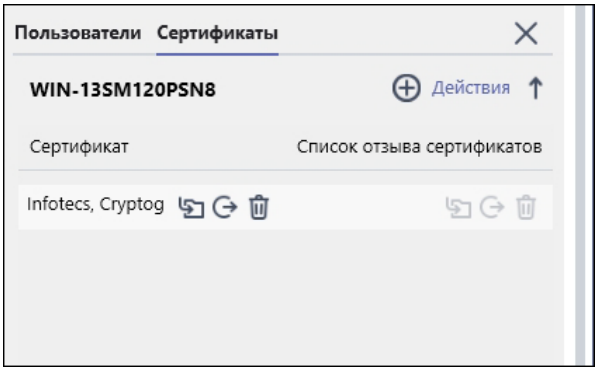


Рисунок 70. Просмотр корневых сертификатов и CRL

5 Чтобы выгрузить установленный корневой сертификат или CRL в файл, нажмите справа от названия сертификата или CRL и укажите место сохранения файла.

6 Чтобы загрузить установленный корневой сертификат или CRL с защищаемого узла на ViPNet EPP Сервер, нажмите справа от названия сертификата или CRL.

7 Чтобы удалить корневой сертификат или CRL с защищаемого узла, нажмите справа от названия сертификата или CRL и подтвердите удаление.

Установка корневых сертификатов и CRL

Вы можете установить на каждый защищаемый узел с ViPNet SafeBoot не более четырех корневых сертификатов. Сертификаты и CRL будут установлены на защищаемых узлах только после перезагрузки.

На защищаемых узлах сначала должен быть установлен корневой сертификат, а затем — CRL. Без установленного корневого сертификата CRL не установится.

Чтобы установить корневой сертификат или CRL на защищаемые узлы с ViPNet SafeBoot:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Доверенная загрузка** > **Устройства**.

3 Выберите флажками одну или несколько групп с защищаемыми узлами или один или несколько защищаемых узлов в группе и нажмите **Действия** > **Установить корневой сертификат** или **Установить список отзыва сертификатов**.

Для отправки корневого сертификата или CRL на один защищаемый узел с SafeBoot вы можете воспользоваться способом: дважды щелкните защищаемый узел и на панели справа на вкладке **Сертификаты** нажмите **Действия** > **Установить корневой сертификат** или **Установка списка отзыва сертификатов**. Чтобы использовать этот способ, выбранный защищаемый узел должен находиться в состоянии **В сети**.

4 В окне установки сертификата или списка отзыва сертификатов:

4.1 Выберите флажком в списке сертификаты или CRL для установки на выбранных защищаемых узлах. В списке будут отображаться только те сертификаты, которые были ранее загружены в ViPNet EPP Сервер.

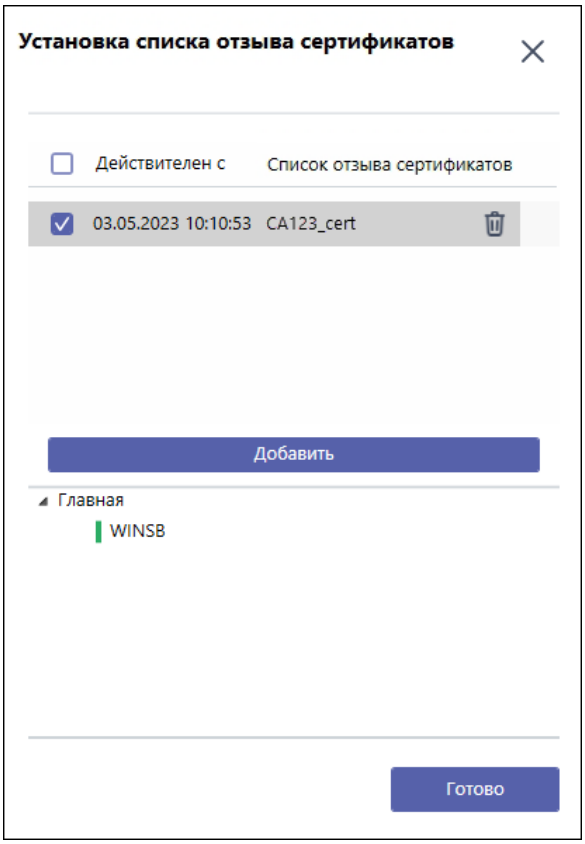


Рисунок 71. Выбор и отправка CRL на защищаемый узел

4.2 Если нужного сертификата или CRL нет, нажмите **Добавить** и укажите файл с сертификатом или CRL. После добавления выберите его флажком.

4.3 Убедитесь, что выбраны необходимые защищаемые узлы и нажмите **Готово**. Появится сообщение об отправке данных на защищаемые узлы.

Если при отправке сертификатов защищаемый узел не был доступен по сети (имел состояние **Не в сети**), сертификаты или CRL будут установлены после его подключения к сети и повторной перезагрузки компьютера.

В ViPNet EPP Сервер сразу после отправки сертификатов или CRL на защищаемые узлы информация о них отобразится на вкладке **Сертификаты** (см. Просмотр информации о сертификатах на защищаемых узлах, выгрузка и удаление сертификатов). Это подтверждает факт отправки данных на защищаемые узлы, но не факт применения в ViPNet SafeBoot. Подтверждением успешной установки сертификатов или CRL на защищаемых узлах в ViPNet SafeBoot будет служить отображение информации о сертификатах или CRL на вкладке **Сертификаты (см.** Просмотр информации о сертификатах на защищаемых узлах, выгрузка и удаление сертификатов**)** после перезагрузки компьютера защищаемого узла.

Настройка критериев обнаружения аномалий

Критерии 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. 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 Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Критерии обнаружения аномалий**.

3 Для добавления нового критерия обнаружения аномалий на панели вверху нажмите **Создать**.

4 В окне **Создание критерия обнаружения аномалий** укажите:

4.1 Выберите тип правил HIDS, например контроль файлов, срабатывание правил анализа или правил обнаружения сетевых атак.

4.2 В полях **Время начала** и **Время окончания** укажите границы временного интервала, в котором активность считается нетипичной.

4.3 Укажите через запятую идентификаторы правил выбранного типа. Идентификаторы правил можно посмотреть в журнале событий в столбце **Идентификатор**.

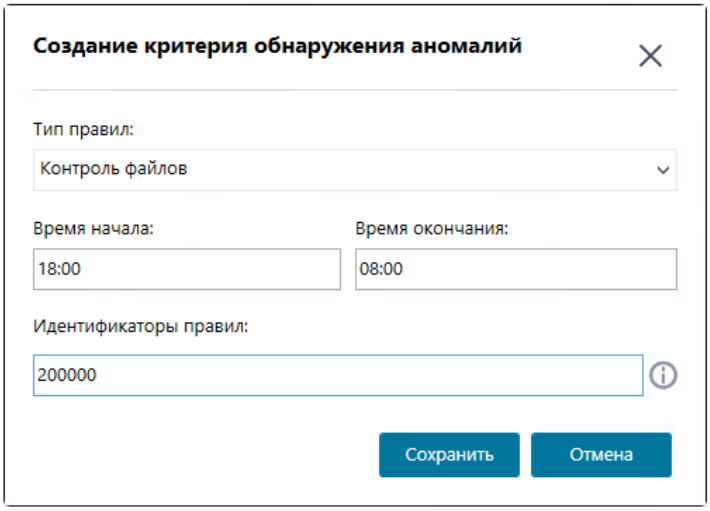


Рисунок 72. Создание критерия обнаружения аномалий

5 Нажмите **Сохранить**.

Настройка модели нормальной активности защищаемого узла

Модуль поведенческого анализа Behavior Analytics накапливает события информационной безопасности защищаемых узлов для проведения первичного обучения в течение 30 дней, начиная с момента получения от узлов первых событий. Для каждого защищаемого узла с завершенным периодом накопления событий администратор ViPNet EPP может запустить первичное обучение модуля поведенческого анализа. Запустить обучение можно для отдельных узлов в группе и для групп узлов.

Чтобы запустить первичное обучение модуля поведенческого анализа на защищаемых узлах группы, где оно доступно:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Поведенческий анализ**.

3 Включите модуль поведенческого анализа.

4 Щелкните группу, на защищаемых узлах которой вы предполагаете запустить первичное обучение модуля поведенческого анализа, например **Офис**. Вы можете запустить обучение на узлах со статусом **Требуется обучение**.

Совет. Обучение модуля поведенческого анализа, запущенное одновременно на большом количестве защищаемых узлов, может стать причиной высокой загрузки процессора компьютера ViPNet EPP Сервер. Рекомендуется запускать обучение последовательно на небольших группах узлов.

---

5 Чтобы запустить первичное обучение на одном защищаемом узле:

5.1 Дважды щелкните узел в списке.

5.2 На панели справа нажмите **Запустить обучение**.

5.3 Подтвердите запуск обучения.

6 Чтобы запустить первичное обучение на нескольких защищаемых узлах:

6.1 Выберите флажками нужные узлы.

6.2 На панели вверху нажмите **Запустить обучение**.

6.3 Подтвердите запуск обучения.

После запуска первичного обучения статус обучения выбранных защищаемых узлов изменится на **Идет обучение**, а по завершении обучения — на **Обучен**.

Запуск повторного обучения модуля поведенческого анализа выполняется по аналогии с запуском первичного обучения.

Чтобы запустить обучения модуля поведенческого анализа (первичного и повторного) на уровне групп защищаемых узлов:

1 Выберите  **Поведенческий анализ**.

2 В списке групп защищаемых узлов выберите флажками нужные.

3 На панели вверху нажмите  **Запустить обучение**.

4 Подтвердите запуск обучения.

Обучение модуля поведенческого анализа будет запущено только на защищаемых узлах групп со статусом обучения **Требуется обучение**.

По завершении обучения и построения моделей нормальной активности защищаемых узлов, выполняется обнаружение аномалий.

В некоторых случаях, например при высокой загрузке процессора компьютера ViPNet EPP Сервер или для накопления большего количества событий информационной безопасности, процесс обучения модуля поведенческого анализа требуется остановить. Это можно выполнить только для всех защищаемых узлов, на которых идет обучение, одновременно. Чтобы остановить обучение модуля поведенческого анализа:

1 На панели вверху в окне списка групп защищаемых узлов или списка узлов группы нажмите **Остановить обучение**.

2 Подтвердите остановку процесса обучения.

Статус обучения защищаемых узлов будет возвращен в состояние, которое было до начала первичного или повторного обучения.

Для поиска защищаемых узлов с определенным статусом обучения модуля поведенческого анализа в группе используйте фильтр:

1 Щелкните нужную группу защищаемых узлов.

2 На панели вверху нажмите  и выберите параметры фильтрации:

- **Недостаточно данных для обучения**.
- **Требуется обучение**.
- **Идет обучение**.
- **Ошибка обучения**.
- **Обучен**.

3 Нажмите **Применить**.

При выключении модуля поведенческого анализа процесс обнаружения аномалий останавливается, все построенные модели нормальной активности защищаемых узлов сохраняются. При повторном включении модуля модели сразу используются для обнаружения аномалий.

Сканирование AntiMalware

Администратор ViPNet EPP Сервер может запускать поиск признаков вредоносного ПО в исполняемых файлах ОС с помощью сканирования AntiMalware (см. Обнаружение признаков вредоносности в исполняемых файлах с помощью сканирования AntiMalware и блокировка опасных файлов) на защищаемых узлах (недоступно для защищаемых узлов с ViPNet EPP Linux Агент).

Сканирование доступно только для защищаемых узлов, на которых при подключении к ViPNet EPP Сервер была разрешена работа модуля Application Control. Защищаемые узлы должны быть в активном состоянии и контроль приложений не должен быть отключен.

Типы сканирования AntiMalware:

- Полное — проверка всех исполняемых файлов *.exe и *.dll на жестких дисках компьютера защищаемого узла. Может выполняться длительное время.
- Быстрое — проверка исполняемых файлов в системных папках (включая подпапки):
  - `\Windows\Temp\`;
  - `\Windows\Tasks\`;
  - `\Windows\System32\Tasks\`;
  - `*\AppData\Roaming\`;
  - `*\AppData\Local\`;
  - `\Program Files (x86)` — проверяются файлы только в корне папки;
  - `\ProgramData` — проверяются файлы только в корне папки.
- Выборочное — проверка исполняемых файлов, указанных администратором. Можно указать определенные файлы или папки.

Перед запуском сканирования вы можете настроить уровни опасности и автоматическую блокировку обнаруженных в результате сканирования исполняемых файлов критического уровня опасности (см. Просмотр и настройка параметров сканирования).

Для регулярной проверки защищаемых узлов предусмотрена настройка автоматического запуска сканирования по расписанию (см. Настройка расписания автоматического запуска сканирования).

По завершении сканирования формируется отчет, по результатам которого администратор может заблокировать исполняемые файлы, которые он считает потенциально опасными (см. Просмотр и обработка результатов сканирования).

Запуск сканирования вручную

Запуск сканирования AntiMalware вручную доступен для групп защищаемых узлов и для отдельных узлов. Сканирование будет выполнено в соответствии с параметрами, заданными для группы защищаемого узла (см. Просмотр и настройка параметров сканирования).

Чтобы запустить сканирование AntiMalware на защищаемом узле:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **AntiMalware**.

3 Щелкните группу, где расположен защищаемый узел.

4 Дважды щелкните нужный узел и на панели справа:

4.1 Посмотрите параметры сканирования, нажав .

4.2 Нажмите **Запустить сканирование**.

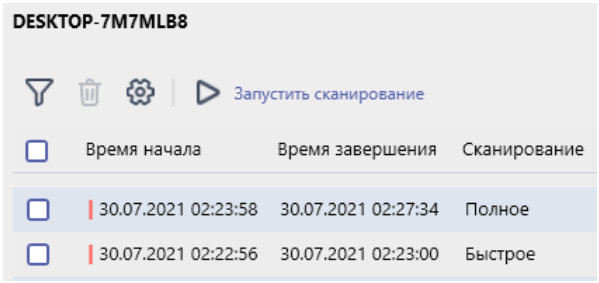


Рисунок 73. Запуск сканирования

5 Выберите тип сканирования: **Полное**, **Быстрое** или **Выборочное**. При выборе **Выборочное** укажите полные пути к файлам или папкам на защищаемом узле, которые необходимо сканировать:

5.1 Нажмите **Добавить пути к файлам/папкам** и введите один или несколько путей по одному в каждой строке. При указании путей маски объектов файловой системы указывать нельзя.

5.2 Нажмите .

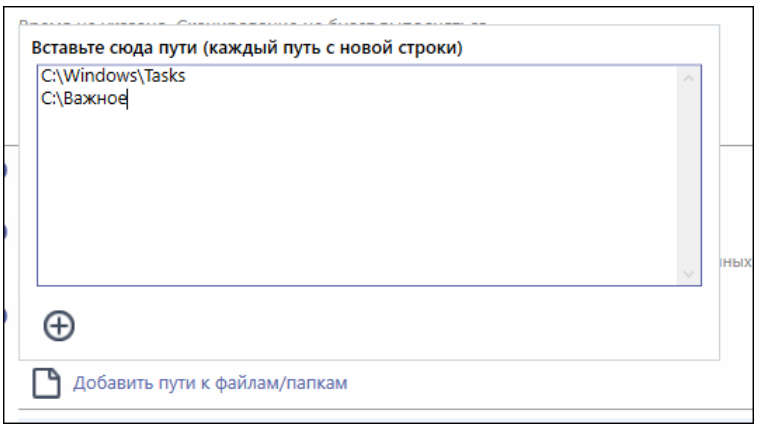


Рисунок 74. Добавление полных путей для сканирования

6 Нажмите **Запустить сканирование**. Полное сканирование может занять продолжительное время. Для отображения актуального прогресса сканирования нажимайте клавишу F5.

В результате сканирования будет создан отчет (см. Просмотр и обработка результатов сканирования).

В некоторых случаях, например для изменения варианта сканирования, процесс сканирования требуется остановить. Чтобы остановить сканирование, на панели справа нажмите одноименную кнопку.

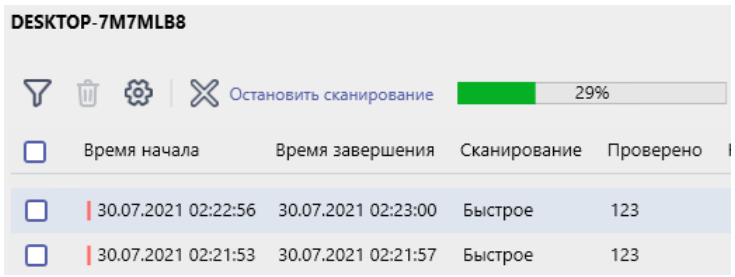


Рисунок 75. Идет процесс сканирования

Чтобы запустить сканирование AntiMalware на нескольких защищаемых узлах:

1 На странице **AntiMalware** выберите флажками группы защищаемых узлов или защищаемые узлы и на панели сверху нажмите **Запустить сканирование**.

2 Выберите тип сканирования в соответствии с предыдущим сценарием и нажмите **Запустить сканирование**.

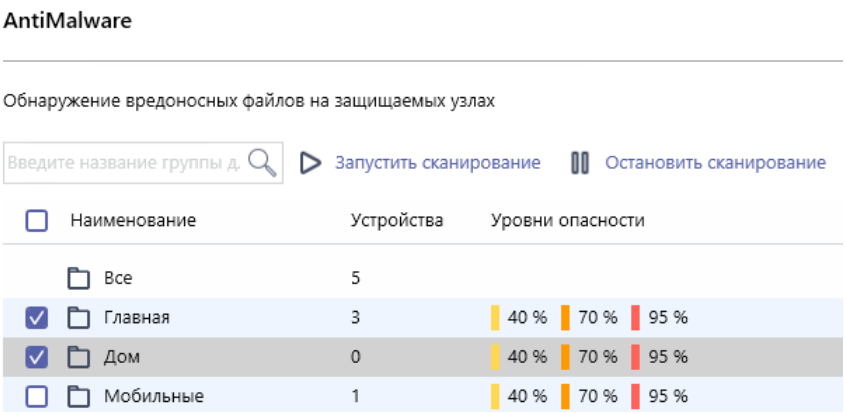


Рисунок 76. Запуск сканирования для нескольких групп защищаемых узлов

Просмотр и обработка результатов сканирования

Результаты сканирования AntiMalware доступны в ViPNet EPP Сервер в виде отчетов только для защищаемых узлов в активном состоянии. Администратору доступен просмотр кратких и

подробных отчетов по каждому защищаемому узлу. Сохраняются только сто последних отчетов для каждого защищаемого узла. Чтобы заблокировать потенциально опасные исполняемые файлы, обнаруженные на защищаемых узлах, доступно добавление их в пользовательский черный список контроля приложений на защищаемом узле. В черный список могут быть добавлены только файлы *.exe.

Чтобы просмотреть отчеты с результатами сканирования AntiMalware на активном защищаемом узле:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **AntiMalware**.

3 Щелкните группу, где расположен защищаемый узел.

Для всех узлов в группе отображается краткая информация о сканировании:

- Название узла и состояние его активности.
- **Сканирование** — выполняется ли в настоящий момент сканирование на узле.
- **Отчеты** — количество подробных отчетов в результате проведенных сканирований.
- **Последний отчет (UTC)** — дата и время завершения последнего сканирования (в стандарте UTC) и наивысший из уровней опасности, который был присвоен файлам при сканировании.

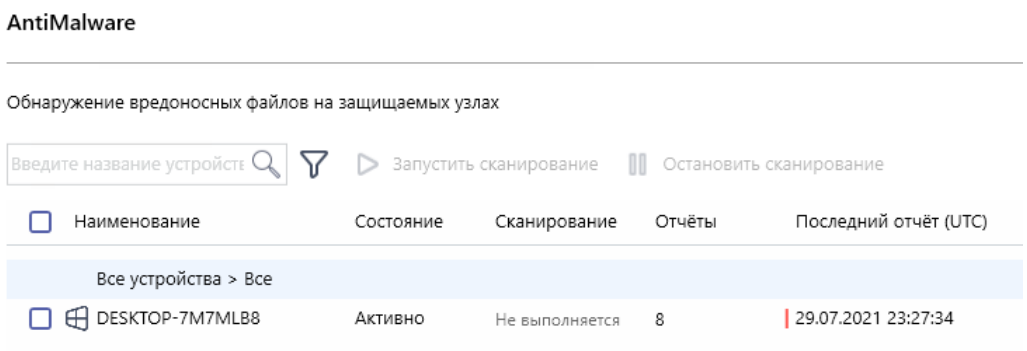


Рисунок 77. Краткая информация о сканировании

4 Чтобы посмотреть список всех отчетов о сканировании для защищаемого узла и краткую информацию о них, дважды щелкните защищаемый узел. На панели справа для каждого отчета отображаются:

- Дата и время начала и завершения сканирования и наивысший из уровней опасности, который был присвоен файлам при данном сканировании.
- Тип сканирования.
- Количество проверенных файлов.
- Количество файлов, которые не удалось проверить.
- Количество найденных потенциально опасных файлов.
- Результат проверки: завершено, отменено или ошибка.

5 Для просмотра определенных отчетов нажмите и выберите критерии фильтрации: тип сканирования, результат проверки, уровень опасности или время завершения сканирования. Нажмите **Применить**.

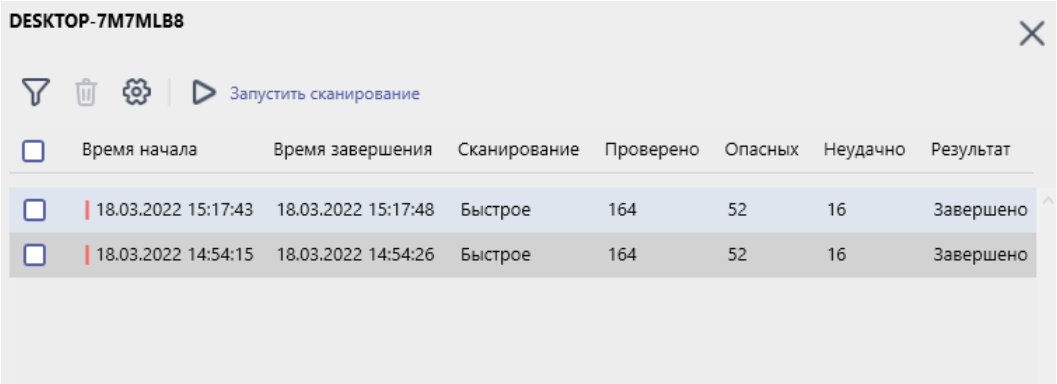


Рисунок 78. Просмотр списка всех отчетов о сканировании AntiMalware

6 Для просмотра подробной информации об отчете дважды щелкните отчет. На панели справа отобразятся:

- Краткие сведения о сканировании со страницы со списком отчетов. Для отмененных отчетов будут доступны результаты проверки до момента отмены пользователем.
- Список проверенных файлов и уровень их опасности:
  - **Критический** — высочайший уровень опасности (по умолчанию значения от 0,95 до 1). Проверенный объект с большой долей вероятности является вредоносным ПО.
  - **Высокий** — высокий уровень (по умолчанию значения 0,7-0,94).
  - **Средний** — средний уровень (0,4-0,69).
  - **Низкий** — низкий уровень (0-0,39). Проверенный объект с большой долей вероятности не является вредоносным ПО.
  - **Неопределенный** — файл не удалось проверить.

  Пороговые значения для уровней опасностей могли быть изменены (см. Просмотр и настройка параметров сканирования).

7 Для удобства просмотра вы можете отфильтровать список файлов на панели справа:

- В поле поиска введите часть имени файла или пути к файлу и нажмите .
- Нажмите и выберите критерии фильтрации: уровень опасности, тип файла (*.exe и *.dll) и внесен ли файл в черный список блокировки. Нажмите **Применить**.

8 Чтобы скопировать путь к файлу в буфер обмена, отметьте файл флажком и нажмите .

9 Для просмотра списка файлов, которые не удалось проверить, и причин возникших ошибок, в строке **Неудачно** нажмите **Показать**. Информацию о непроверенных файлах можно скопировать в буфер обмена, нажав **Копировать список**.

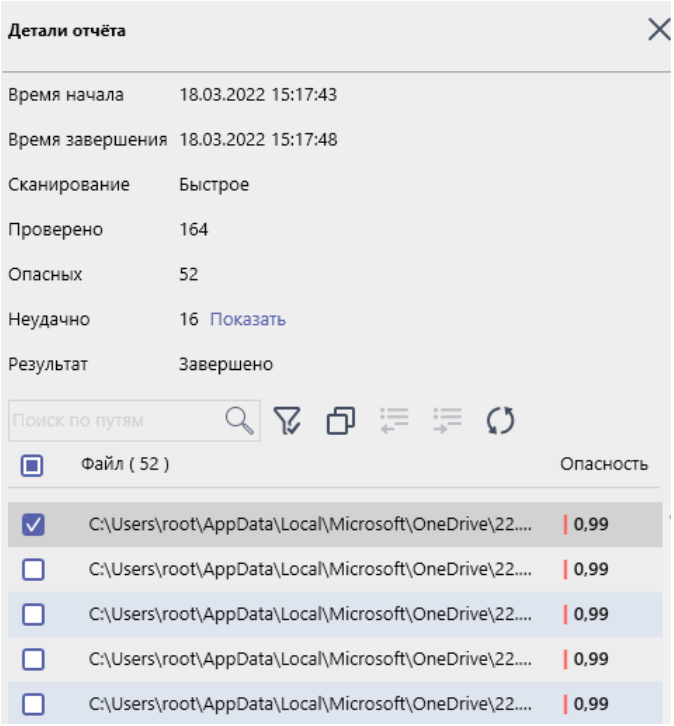


Рисунок 79. Подробная информация об отчете

Чтобы поместить потенциально опасные файлы *.exe в пользовательский черный список контроля приложений на защищаемом узле:

1. На панели справа отметьте файлы флажками и нажмите .
2. Подтвердите добавление в черный список.

В результате строки с файлами будут выделены **жирным шрифтом** и отмечены значком ★, а файлы добавятся на защищаемом узле в пользовательский черный список контроля приложений и для них в ViPNet EPP Агент создадутся блокирующие правила (см. Просмотр списков контроля приложений).

Если для защищаемого узла настроена автоматическая блокировка файлов критического уровня опасности, эти действия будут выполнены автоматически для всех файлов критического уровня.

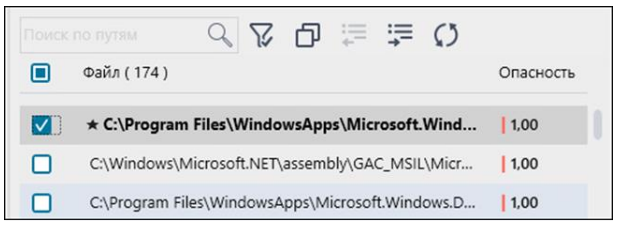


Рисунок 80. Приложение добавлено в пользовательский черный список

Примечание. Если добавленный файл временно исключить из черного списка контроля приложений (см. Управление пользовательскими списками приложений), в отчете AntiMalware строка с этим файлом так и останется выделенной **жирным шрифтом** и отмеченной значком ★.

Чтобы удалить файлы из черного списка, выберите их флажками и нажмите . Подтвердите удаление. Вышеперечисленные отметки черного списка будут сняты.

Чтобы удалить отчеты, например устаревшие, отметьте их флажками и на панели вверху нажмите . Подтвердите удаление.

Просмотр и настройка параметров сканирования

Настройка параметров сканирования AntiMalware доступна для групп защищаемых узлов и будет действовать на все защищаемые узлы в группе. Администратор может просматривать заданные параметры для групп узлов и изменять их.

Чтобы посмотреть заданные параметры сканирования для всех групп:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **AntiMalware**.

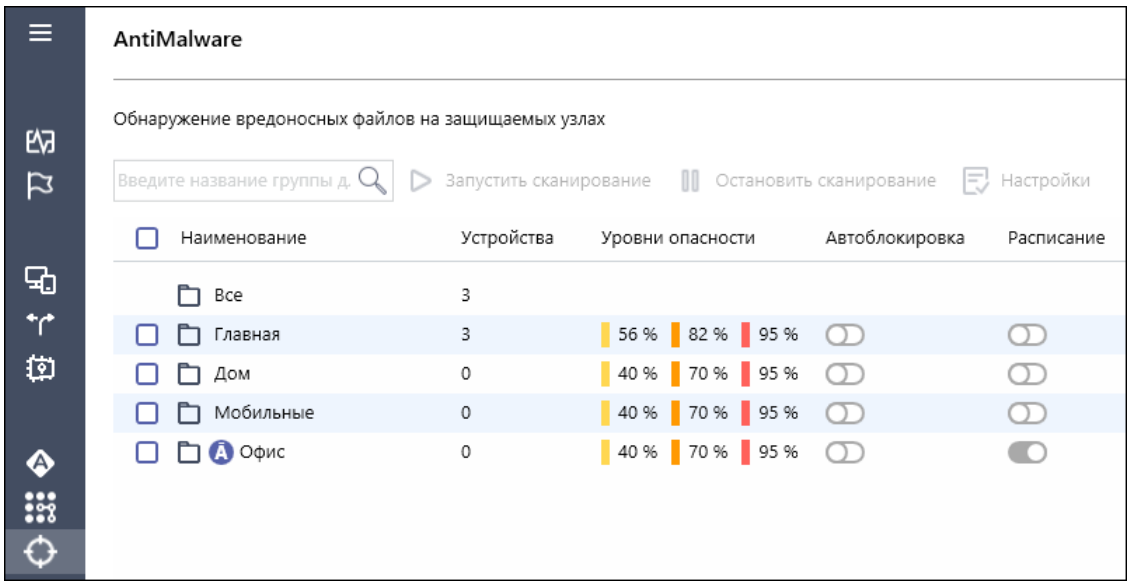


Рисунок 81. Просмотр параметров сканирования, заданных для групп защищаемых узлов

Для групп в списке отображаются:

- **Название** — имя группы.

- **Устройства** — количество защищаемых узлов в группе, для которых применяются нижеприведенные параметры. В текущей версии ViPNet EPP отображается общее количество защищаемых узлов в группе (включая защищаемые узлы с ОС GNU/Linux, на которых сканирование AntiMalware не может быть выполнено).
- **Уровни опасности** — пороговые значения для трех наиболее высоких уровней опасности, в соответствии с которыми при сканировании будет присваиваться тот или иной уровень опасности потенциально вредоносным файлам. По умолчанию установлены пороговые значения для уровней опасности:
  - **Критический** — наивысший уровень опасности (95%). Т.е. в результате сканирования критический уровень опасности будет присвоен файлам, которые с вероятностью 0,95 и более являются вредоносным ПО.
  - **Высокий** — высокий уровень (70%).
  - **Средний** — средний уровень (40%).
- **Автоблокировка** — включена или выключена автоматическая блокировка файлов критического уровня опасности.
- **Расписание** — настроено или не настроено расписание автоматического сканирования (см. Настройка расписания автоматического запуска сканирования).

Чтобы изменить параметры сканирования для одной или нескольких групп защищаемых узлов:

1. На странице **AntiMalware** выберите группы флажками и на панели вверху нажмите **Настройки**.
2. Щелкните **Управление уровнями опасности** и задайте пороговые значения уровней опасности. Чтобы скрыть настройку, еще раз щелкните **Управление уровнями опасности**.

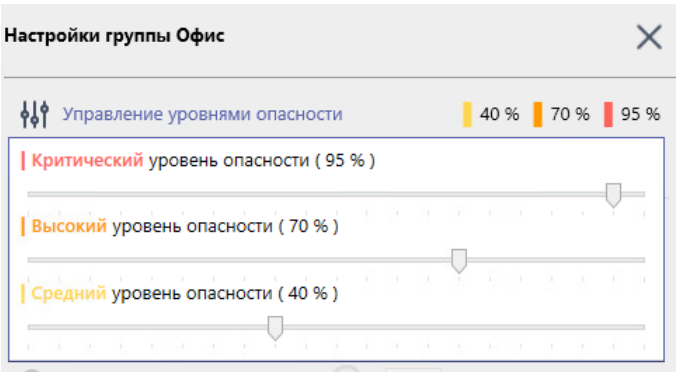


Рисунок 82. Управление пороговыми значениями уровней опасности

3. Если требуется, чтобы в результате сканирования найденные файлы *.exe критической опасности автоматически помещались в пользовательский черный список контроля приложений, выберите **Автоматическая блокировка файлов критической опасности**.
4. Нажмите **Сохранить и отправить**. Настройки будут отправлены на защищаемые узлы группы. В появившемся окне нажмите **ОК**.

Настройка расписания автоматического запуска сканирования

Настройка расписания автоматического запуска сканирования доступна для групп защищаемых узлов и будет действовать на все защищаемые узлы в группе. По умолчанию автоматический запуск сканирования AntiMalware отключен.

Чтобы на защищаемых узлах группы включить автоматический запуск сканирования AntiMalware и настроить расписание запуска:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **AntiMalware**.

3 Выберите одну или несколько групп защищаемых узлов флажками и на панели вверху нажмите **Настройки**.

3.1 Включите **Автоматическое сканирование**.

3.2 Выберите формат времени применения расписания:

- **UTC** — расписание будет применяться на защищаемых узлах в единое время (в стандарте UTC), заданное данными настройками.
- **Локально** — расписание будет применяться на защищаемых узлах в заданное данными настройками время, но в зависимости от настроек часовых поясов на узлах.

3.3 Выберите один из типов расписания:

- **Выполнять периодически** — укажите время запуска и период запуска сканирования (в минутах).

- **Выполнять в указанное время** — выберите флажками дни недели, в которые необходимо запускать сканирование и добавьте одно или несколько значений времени начала сканирования, введя время и нажав ⊕. Если время не задать, сканирование запускаться не будет.

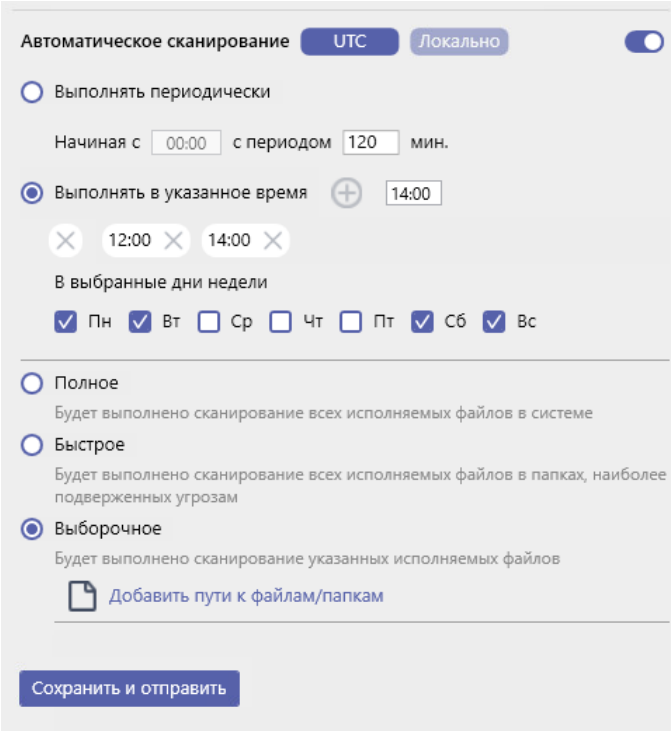


Рисунок 83. Настройка расписания автоматического запуска сканирования

- Выберите тип сканирования — **Полное**, **Быстрое** или **Выборочное**. При выборе **Выборочное** укажите полные пути к файлам или папкам на защищаемых узлах, которые необходимо сканировать. Для этого нажмите **Добавить пути к файлам/папкам** и введите один или несколько путей по одному в каждой строке. При указании путей маски объектов файловой системы указывать нельзя. Нажмите ⊕.

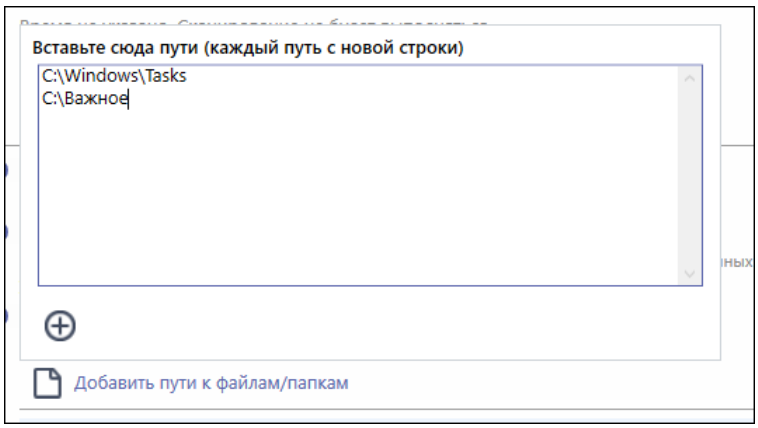


Рисунок 84. Добавление полных путей для сканирования

3.4 Нажмите **Сохранить и отправить**.

3.5 В появившемся окне нажмите **ОК**.

В результате настройки будут отправлены на выбранные защищаемые узлы.

Работа с журналами

В ViPNet EPP Сервер ведутся журналы:

- Журнал событий информационной безопасности защищаемых узлов (см. Журнал событий).
- Журнал аудита действий пользователей (см. Журнал аудита).

При переполнении журналов в соответствии с параметрами хранения выполняется автоматическая ротация событий и журналов (см. Настройка параметров системы).

Журнал событий

ViPNet EPP консолидирует события информационной безопасности защищаемых узлов в журнале событий ViPNet EPP Сервер в режиме, близком к реальному времени. Вы можете просматривать журнал событий и удалять события.

Чтобы просмотреть журнал событий и выполнить возможные действия:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **События**.

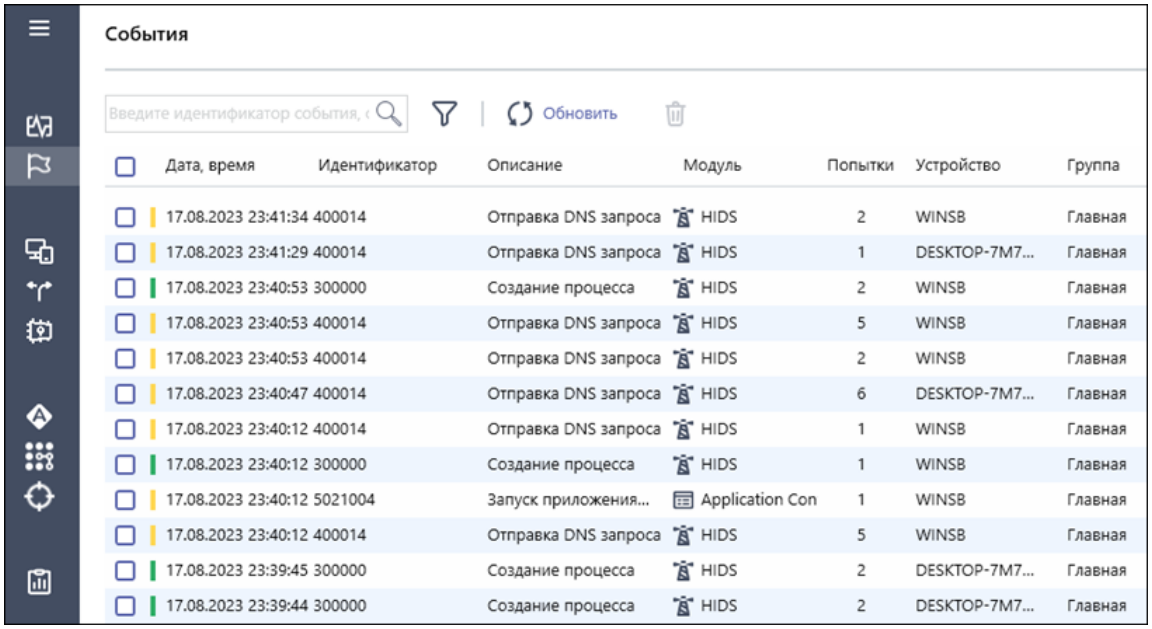


Рисунок 85. Журнал событий ViPNet EPP Сервер

Каждая запись о событии в журнале содержит:

- Цветовой индикатор уровня события:
  - — критическое.

- — опасное.
- — важное.
- — информационное.

- **Дата, время** — дата и время идентификации события.
- **Идентификатор** — идентификатор сработавшего правила (см. Типы и идентификаторы правил). Если событие свидетельствует об аномалии, обнаруженной с помощью заданных критериев, то поле идентификатора помечается значком .
- **Описание** — текстовое описание события.
- **Модуль** — модуль, в котором сработало правило:
  - **PFW** — персональный межсетевой экран (Personal Firewall).
  - **AppC** — контроль приложений (Application Control).
  - **HIDS** — обнаружение вторжений.
  - **HIPS** — предотвращение вторжений.
  - **BA** — поведенческий анализ (Behavior Analytics). Событие, свидетельствует об аномальной активности защищаемого узла; обнаружено с помощью поведенческого анализа.
- **Попытки** — количество повторений события на защищаемом узле в течение заданного периода опроса. Повторные события определяются по одинаковому идентификатору сработавшего правила.
- **Устройство** — сетевое имя защищаемого узла, на котором зарегистрировано событие.
- **Группа** — группа устройств, к которой относится защищаемый узел.

3 Чтобы просмотреть сведения о событии, дважды щелкните строку с нужным событием в журнале — на панели справа на вкладке **Сработавшее правило** будут отображены сведения о сработавшем правиле и количестве зафиксированных повторений события в течение заданного периода опроса:

- Для событий **PFW**, **AppC**, **HIDS** и **HIPS**.

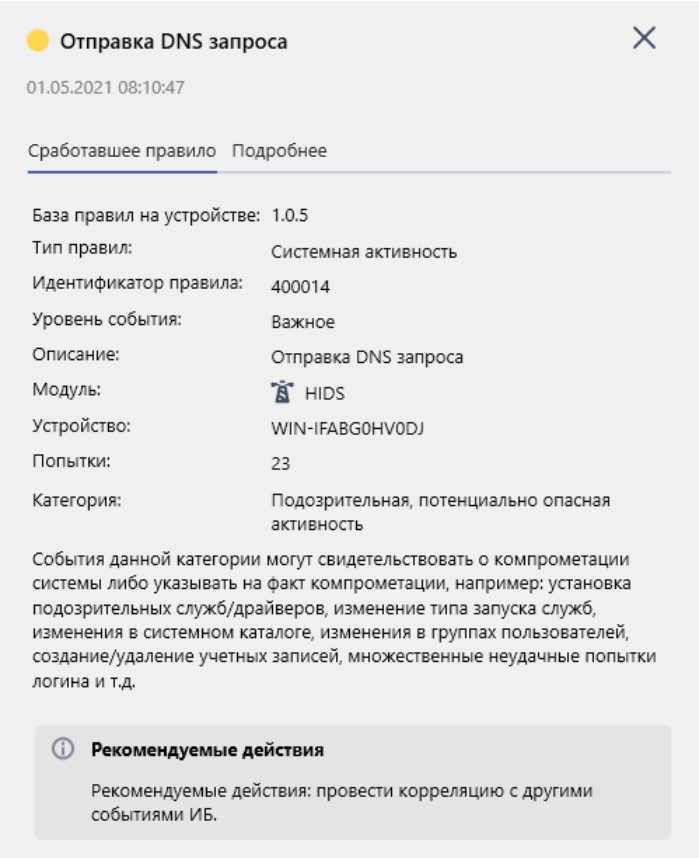


Рисунок 86. Просмотр сведений о событиях модулей PFW, AppC, HIDS и HIPS

- Для событий **BA**.

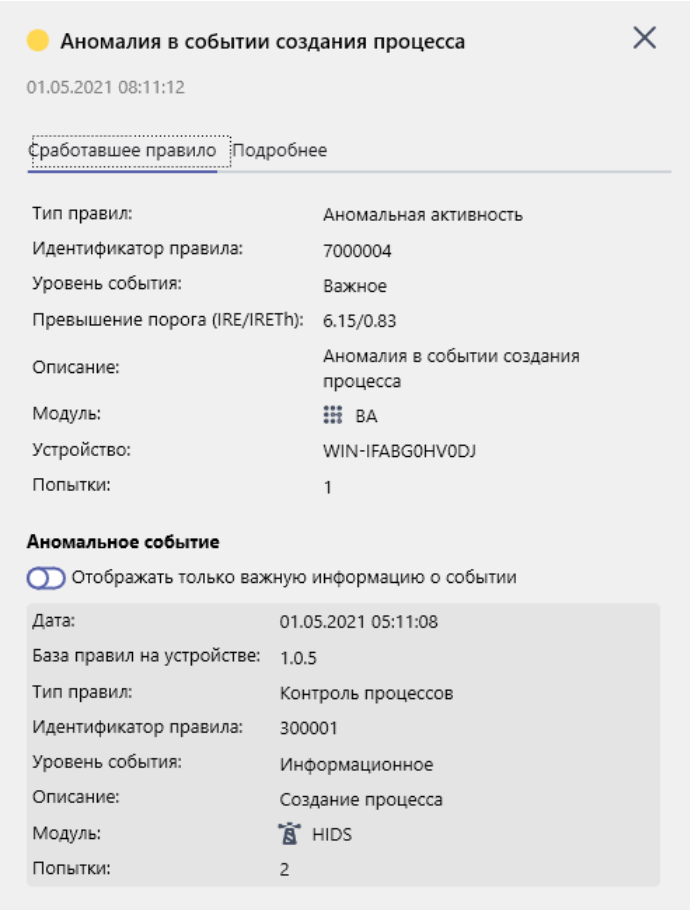


Рисунок 87. Просмотр сведений о событиях модуля BA

4 Для просмотра подробных сведений о событии выберите вкладку **Подробнее**. По умолчанию отображаются только важные сведения о событии в удобном для чтения виде. Для просмотра полных сведений выключите **Отображать только важную информацию о событии**.

Если было зарегистрировано несколько повторений события с одинаковым идентификатором, на вкладке **Подробнее** будут отображены только события с уникальными полными сведениями о событии. Например, событие с идентификатором правила `300001` произошло 5 раз, на вкладке **Сработавшее правило** отображается 5 попыток. У двух событий в полных сведениях содержится `ABC`, а у трех событий — `XYZ`. В этом случае на вкладке **Подробнее** будет отображена информация о двух событиях с идентификатором `300001`.

- Для событий **PFW**, **AppC**, **HIDS** и **HIPS**.

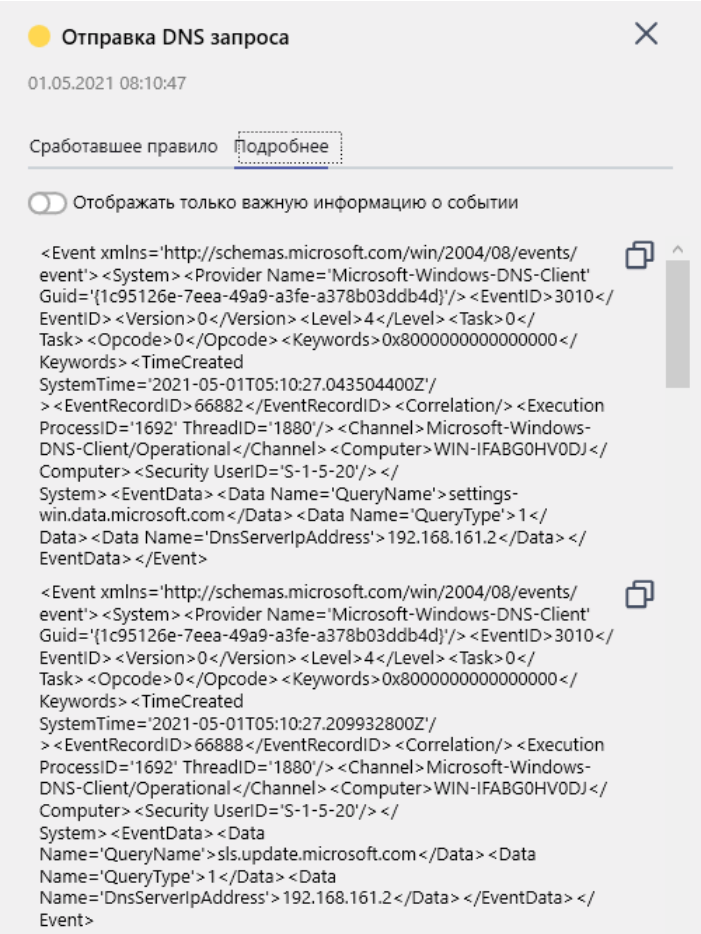


Рисунок 88. Просмотр подробных сведений о событиях модулей PFW, AppC, HIDS и HIPS

- Для событий **BA**.

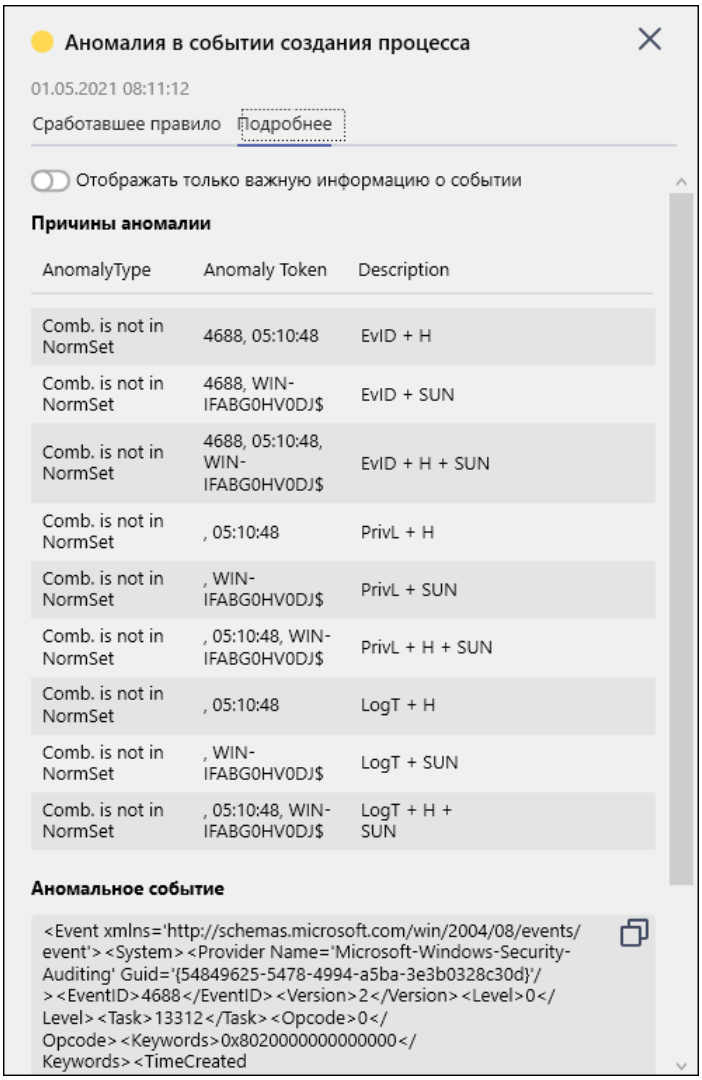


Рисунок 89. Просмотр подробных сведений о событиях модуля BA

Примечание. При просмотре подробных сведений о событии модуля Behavior Analytics вы можете провести анализ причин аномалии и определить, является ли аномалия ложной. Подробнее (см. Выявление ложных аномалий).

Чтобы скопировать полные сведения в буфер обмена, нажмите .

5 Для поиска событий в журнале используйте фильтр:

5.1 Нажмите и задайте параметры фильтрации:

- Выберите тип правил, с помощью которых были обнаружены события.
- Выберите группу защищаемых узлов, для которой нужно отобразить обнаруженные события.
- Выберите защищаемые узлы, для которых нужно отобразить обнаруженные события.
- Выберите модули, для которых нужно отобразить обнаруженные события.

- Если вы хотите отобразить только аномальные события, выберите **Только аномальные события** (см. Настройка критериев обнаружения аномалий).
- Выберите уровни событий, которые нужно отобразить.
- Укажите промежуток времени, в течение которого происходили искомые события.

5.2 Нажмите **Применить**.

6 Чтобы удалить события, выберите флажками события, на панели вверху нажмите  и подтвердите удаление.

Выявление ложных аномалий

События обнаружения аномалий модуля поведенческого анализа Behavior Analytics регистрируются в журнале событий ViPNet EPP Сервер. Поскольку модели нормальной активности обладают некоторой погрешностью обнаружения, часть аномалий могут оказаться ложными.

Чтобы выявлять ложные аномалии, администратор ViPNet EPP должен просматривать в журнале события модуля поведенческого анализа и анализировать причину аномалии — событие информационной безопасности, свидетельствующее об отклонении активности защищаемого узла от нормальной:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите  **События**.

3 В журнале событий дважды щелкните строку с событием  **BA** (обнаруженной аномалией).

4 На панели справа на вкладке **Подробнее** выполните анализ причин аномалии.

Причины аномалии представлены в одноименном разделе вкладки, в порядке уменьшения вероятности. Строка описания причины состоит из следующих полей:

- **AnomalyType** — тип аномалии.
- **Anomaly Token** — токен (объект связанного события информационной безопасности раздела вкладки **Аномальное событие**). Несколько токенов перечисляются через разделитель.
- **Description** — описание токена или их комбинации.

Тип аномалии может принимать следующие значения:

- **Unknown object** — неизвестный структурированный объект, например путь, которого не было в выборке событий информационной безопасности при обучении.
- **Anomaly number of objects** — аномальное количество структурированных объектов одного типа, например, много путей одного типа.
- **Exceeding the maximum** — превышение максимума.
- **Comb. is not in NormSet** — аномальная комбинация токенов, которой не было в выборке событий информационной безопасности при обучении. Используемые

комбинации: EvID + H, EvID + SUN, EvID + H + SUN, PrivL + H, PrivL + SUN, PrivL + H + SUN, LogT + H, LogT + SUN, LogT + H + SUN, где:

- **EvID** — EventID.
- **H** — Hour.
- **SUN** — SubjectUserName.
- **PrivL** — PrivilegeList.
- **LogT** — LogonType.

5 Если аномалия ложная:

5.1 В журнале событий ViPNet EPP Сервер удалите событие информационной безопасности, связанное с аномалией.

5.2 Запустите повторное обучение модуля поведенческого анализа на защищаемом узле (см. Настройка модели нормальной активности защищаемого узла).

Журнал аудита

В журнале аудита ViPNet EPP Сервер регистрируются события, вызванные действиями пользователей, а также системные события ViPNet EPP Сервер и результаты самотестирования ViPNet EPP Агент на защищаемых узлах.

Чтобы просмотреть журнал аудита:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора или аудитора ViPNet EPP.

2 Выберите **Журналы**.

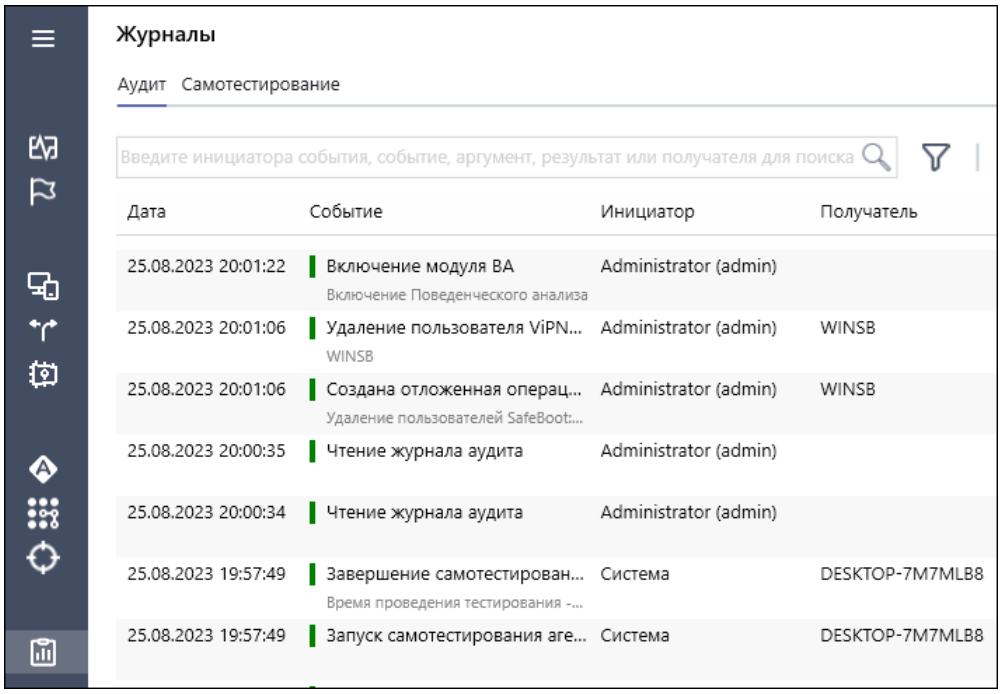


Рисунок 90. Журнал аудита ViPNet EPP Сервер

Каждая запись в журнале содержит:

- **Дата** — 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 будет больше заданного периода времени для действия из события.

- **Событие** — цветовой индикатор (— действие, вызвавшее событие успешно или — не успешно) и описание события.
- **Инициатор:**
  - Система (например, системные события «Запуск службы» ViPNet EPP Сервер и «Самотестирование агента»).
  - Администраторы, аудиторы и пользователи ViPNet EPP Сервер (например, аутентификация администратора ViPNet EPP на ViPNet EPP Сервер).
- **Получатель:**
  - Устройства, зарегистрированные в группе **Все** на ViPNet EPP Сервер (например, ViPNet EPP Сервер или подключенное устройство).
  - Администраторы, аудиторы и пользователи ViPNet EPP Сервер. Для некоторых событий поле может быть пустым.

3 Для поиска событий журнала аудита, удовлетворяющих определенным параметрам, используйте фильтр:

3.1 Нажмите и выберите критерии фильтрации: период регистрации события, инициатор и получатель события, тип события, результат действия.

3.2 Нажмите **Применить**.

Запрос журнала регистрации трафика с ViPNet EPP Агент

Администратор ViPNet EPP Сервер может запрашивать данные журнала регистрации трафика на защищаемых узлах за заданный период времени. Запрос данных доступен только для защищаемых узлов, на которых при подключении к ViPNet EPP Сервер была разрешена работа модуля Персональный межсетевой экран. Защищаемые узлы должны быть в активном состоянии.

Запрос формируется для выбранного защищаемого узла на основе заданных параметров:

- название сработавших сетевых фильтров персонального межсетевого экрана;
- действие сработавших сетевых фильтров (блокирует или разрешает IP-пакеты);
- период времени, за который нужны данные журнала трафика.

  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 на 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. Отчеты можно удалить и вручную.

Чтобы запросить данные журнала трафика с защищаемого узла:

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите  **Устройства**.
3. Найдите защищаемый узел в списке и дважды щелкните его.
4. На панели справа выберите вкладку **Трафик**.
5. Нажмите  , укажите параметры запрашиваемых событий журнала трафика и период времени, за который вы хотите получить отчет. Нажмите **Применить**.

6 Нажмите  и дождитесь создания отчета.

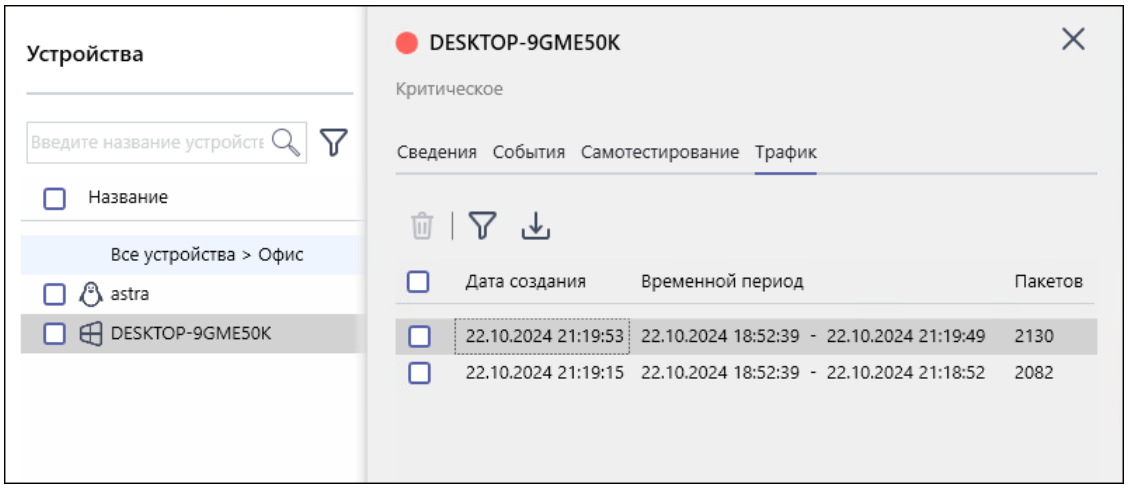


Рисунок 91. Запрос данных журнала трафика с защищаемого узла

Чтобы просмотреть отчеты о трафике с выбранного защищаемого узла:

1 На панели справа на вкладке **Трафик** для каждого отчета отображаются:

- Дата создания отчета.
- Временной период, за который был запрошен отчет о трафике.
- Количество зарегистрированных IP-пакетов.

2 Для просмотра подробной информации в отчете дважды щелкните отчет и просмотрите данные о событиях в окне **Трафик**.

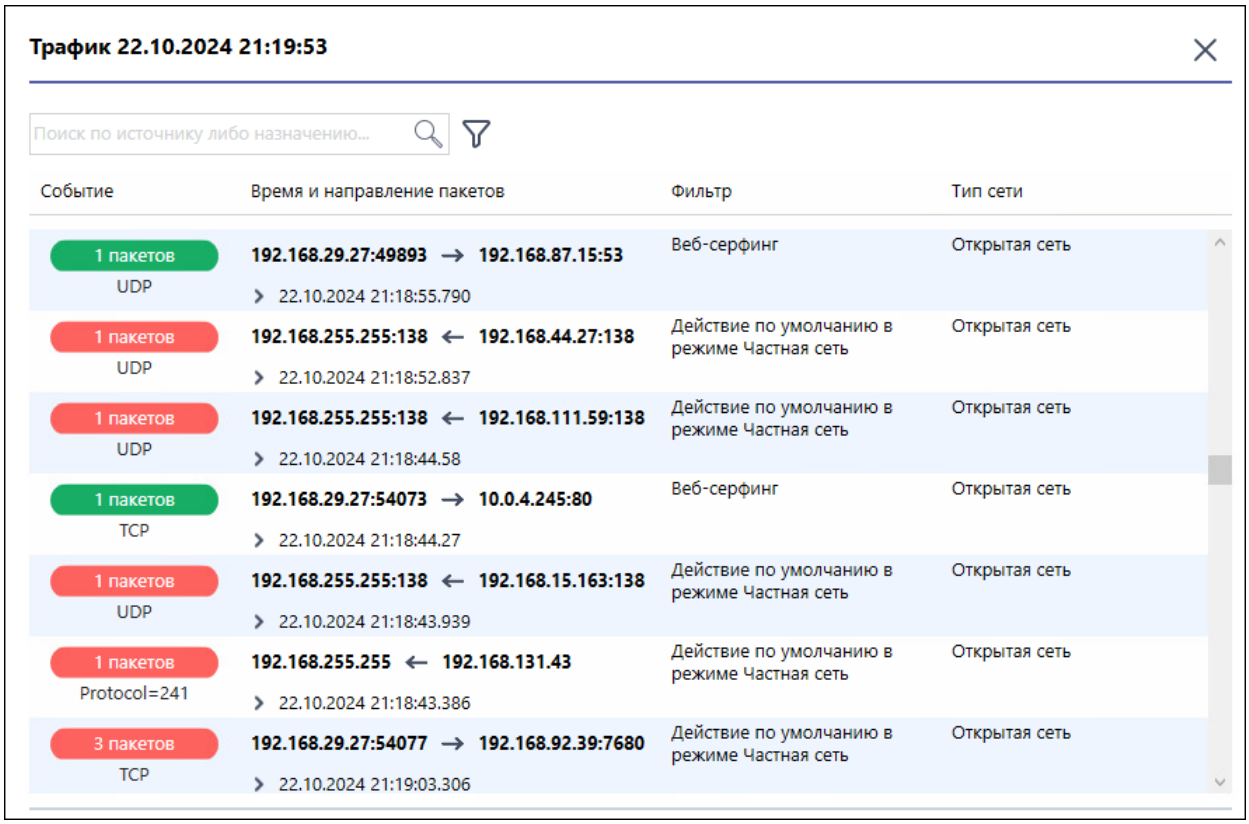


Рисунок 92. Просмотр подробной информации в отчете о трафике

Каждая запись о событии содержит:

- **Событие** — протокол передачи и количество зарегистрированных однотипных IP-пакетов за указанный период времени. Зеленым цветом отмечены разрешенные IP-пакеты, а красным цветом — заблокированные.
- **Время и направление пакетов** — направление (← — входящие IP-пакеты, → — исходящие IP-пакеты), IP-адреса и порты источника и назначения, а также дату и время регистрации последнего IP-пакета данного типа. Слева всегда отображается адрес защищаемого узла, с которого запрошен журнал трафика.
- **Фильтр** — сетевой или системный фильтр, по срабатыванию которого было зарегистрировано событие:
  - Сетевой фильтр из списка фильтров для режимов работы.
  - Сетевой фильтр, по которому заблокировано активное соединение приложения:
    - Название фильтра (на агенте for Windows).
    - Блокировка сетевых соединений приложения (на агенте for Linux).
  - 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.

- **Тип сети** — 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.

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 и/или воспользуйтесь фильтром поиска  по названию, действию сетевого фильтра, периоду времени.

4 Чтобы просмотреть дату и время регистрации каждого IP-пакета события, выберите событие и щелкните поле даты и времени регистрации последнего IP-пакета события.

Чтобы удалить отчеты о трафике с выбранного защищаемого узла, например устаревшие, на панели справа на вкладке **Трафик** выберите отчеты флажками и на панели вверху нажмите  . Подтвердите удаление.

Администрирование ViPNet EPP Сервер

Управление учетными записями

При установке ViPNet EPP Сервер автоматически создается учетная запись администратора ViPNet EPP (см. Ролевая модель). Она позволяет подключаться к ViPNet EPP Сервер с помощью ViPNet EPP Серверная консоль и выполнять все возможные настройки, включая создание новых учетных записей и изменение существующих.

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 `!@#$%^&*()-_+=;:'",.<>/?\|`~[]{}.`

Просмотр списка учетных записей

Чтобы просмотреть список учетных записей ViPNet EPP Сервер:

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите **Учетные записи**.
3. Для поиска учетных записей по критерию роли (администратор, аудитор и пользователь):
   - 3.1 Нажмите .
   - 3.2 Выберите роли учетных записей.
   - 3.3 Нажмите **Применить**.
4. Чтобы найти учетную запись в списке, в поле поиска введите часть имени учетной записи или имя целиком и нажмите .

Создание учетной 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 создать новую учетную запись:

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите **Учетные записи** и на панели вверху нажмите **Создать учетную запись**.
3. В окне **Новая учетная запись** укажите:
   - Имя пользователя, например фамилия и имя.
   - Имя учетной записи.
   - Роль учетной записи: администратор, аудитор, пользователь (см. Ролевая модель).
   - Пароль пользователя в соответствии с требованиями (см. Требования к имени и паролю учетной записи).

Примечание. Вы можете выбрать **Использовать простой пароль** и в поле **Пароль** указать любой пароль, но в целях безопасности использовать простые пароли не рекомендуется.

4 Нажмите **Готово**.

Изменение учетной записи

Чтобы изменить параметры существующей учетной записи (имя пользователя, имя учетной записи, пароль и роль):

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Учетные записи**.

3 Дважды щелкните нужную учетную запись в списке.

4 На панели справа:

- Укажите новые имя пользователя и имя пользователя.
- Выберите другую роль.
- Для смены пароля в поле **Пароль** нажмите **Изменить** и укажите новый пароль.

Примечание. Вы можете выбрать **Использовать простой пароль** и в поле **Пароль** указать любой пароль, но из соображений безопасности использовать простые пароли не рекомендуется.

5 Нажмите **OK**.

Удаление учетной записи

Чтобы удалить одну или несколько учетных записей:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Учетные записи**.

3 В списке выберите флажками учетные записи, подлежащие удалению. Удаление своей учетной записи, под которой вы авторизованы на ViPNet EPP Сервер, недоступно.

4 Нажмите **Удалить**.

5 Нажмите **Да** для подтверждения удаления выбранных учетных записей.

Настройка параметров системы

Параметры системы относятся к работе ViPNet EPP в целом и определяют:

- Период обмена данными между ViPNet EPP Сервер и ViPNet EPP Агент.
- Сроки хранения и максимальное количество записей аудита в ViPNet EPP Сервер и ViPNet EPP Агент.

  Параметры для ViPNet EPP Сервер влияют на записи в журнале событий от агентов, журнале аудита сервера.

  Параметры для ViPNet EPP Агент влияют на записи в журнале событий, журнале аудита, журнале трафика, журнале контроля приложений.
- Срок хранения в ViPNet EPP Сервер запрошенных с защищаемых узлов данных журнала трафика.
- Периоды самотестирования ViPNet EPP Сервер и ViPNet EPP Агент.
- Возможность отслеживать работу антивирусов на защищаемых узлах (см. Отслеживание работы антивирусов).

При переполнении журналов в ViPNet EPP Агент и в ViPNet EPP Сервер 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.

В ViPNet EPP Сервер при уменьшении объема свободного места на диске ниже 10 Гбайт удаляются наиболее старые записи журнала событий до момента, пока объем свободного места не достигнет 10 Гбайт. При этом записи за текущий день не удаляются.

Информация о переполнении журнала и удалении событий фиксируется в журнале аудита.

Чтобы изменить параметры системы:

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите  **Параметры системы**.
3. На вкладке **Параметры агента** задайте:
   - **Период опроса (секунд)** — промежуток времени, через который происходит опрос защищаемых узлов о зарегистрированных событиях информационной безопасности и результатах самотестирования. Рекомендуемое значение — 20 секунд.
   - **Период самотестирования агента (секунд)** — промежуток времени, через который происходит автоматическая проверка работоспособности ViPNet EPP Агент (см. Проверка работоспособности). Рекомендуемое значение — 600 секунд.
   - **Период неактивности (секунд)** — промежуток времени, в течение которого защищаемый узел не проявляет активности. Рекомендуемое значение — 300 секунд. Если защищаемый узел не проявил активность в течение заданного промежутка, в свойствах этого узла будет отображаться состояние **Отключено**. Это означает, что связь с узлом потеряна и узел не защищен.

- **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 (дней)** — записи, зарегистрированные ранее указанного срока, удаляются из журналов в ViPNet EPP Агент. Рекомендуемое значение — 30 дней.
- **Максимальное число записей** — максимальное число записей, которое может храниться в каждом из журналов в ViPNet EPP Агент. Может принимать значение из диапазона 1–100000, рекомендуемое — 50000.
- **Число записей, удаляемых при достижении максимума** — количество записей, которое удаляется из каждого журнала в ViPNet EPP Агент в случае достижения максимального количества хранимых записей. Может принимать значение из диапазона 1–50000, рекомендуемое — 1000.
- Для возврата измененных параметров агента к значениям по умолчанию нажмите **Использовать параметры по умолчанию**.

4 На вкладке **Параметры сервера** задайте:

- **Период самотестирования сервера (секунд)** — промежуток времени, через который проверяется работоспособность ViPNet EPP Сервер (см. Проверка работоспособности). Рекомендуемое значение — 600 секунд.
- **Срок хранения снимков трафика (дней)** — записи журнала трафика, запрошенного с защищаемого узла, созданные ранее указанного срока, удаляются из журналов сервера. Может принимать значение из диапазона 1–180, рекомендуемое значение — 30 дней.
- **Автоматически подключать новые агенты** (см. Настройка автоматического подключения защищаемых узлов).
- **Срок хранения (дней)** — события, зарегистрированные ранее указанного срока, удаляются из журнала аудита сервера. Рекомендуемое значение — 400 дней.
- **Максимальное число записей** — максимальное число записей, которое может храниться в журнале аудита и журнале событий от агентов. Может принимать значение из диапазона 1–100000, рекомендуемое — 50000.
- **Число записей, удаляемых при достижении максимума** — количество записей, которое удаляется из журнала аудита и журнала событий агентов в случае достижения максимального количества хранимых записей в журнале. Может принимать значение из диапазона 1–50000, рекомендуемое — 10000.

- Для возврата измененных параметров сервера к значениям по умолчанию нажмите **Использовать параметры по умолчанию**.

5 Нажмите **Сохранить**.

Проверка работоспособности

Для контроля работоспособности в ViPNet EPP Сервер выполняется:

- Контроль целостности важных файлов ПО ViPNet EPP. Выполняется при старте программы и периодически в процессе работы программы. При возникновении ошибок целостности важных файлов ПО ViPNet EPP Сервер становится неработоспособным. Данные о нарушении целостности будут записаны в служебные диагностические журналы. Для восстановления работоспособности см. раздел Восстановление или удаление ViPNet EPP Сервер и ViPNet EPP Серверная консоль.
- Контроль целостности журналов аудита и журнала событий. Выполняется при старте ПО ViPNet EPP и по расписанию (см. Настройка параметров системы) в рамках самотестирования (по умолчанию — каждые 600 секунд).

Администратор ViPNet EPP может запустить самотестирование вручную и получить сведения о состоянии ViPNet EPP Сервер:

- Подключение к базе данных PostgreSQL: выполнено успешно или ошибка.
- Целостность журнала аудита и журнала событий: нарушена или нет.
- Актуальность версии базы правил: есть активные версии базы правил или нет.
- Факт блокировки пользователей после трех неудачных попыток авторизации: есть заблокированные пользователи или нет.
- Состояние службы ViPNet EPP Сервер: выполняется или остановлена.

Результаты проверки работоспособности регистрируются в журнале аудита ViPNet EPP Сервер (см. Журнал аудита).

Чтобы запустить проверку работоспособности ViPNet EPP Сервер вручную:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите  **Журналы**.

3 На вкладке **Самотестирование** нажмите **Запустить самотестирование**.

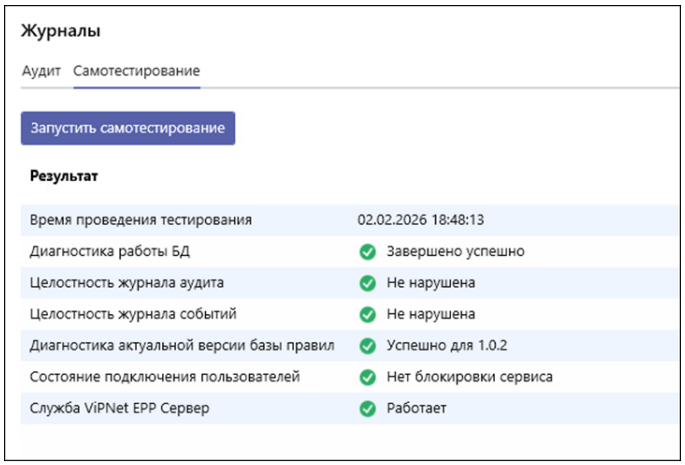


Рисунок 93. Проверка работоспособности ViPNet EPP Сервер

Дождитесь завершения проверки работоспособности ViPNet EPP Сервер.

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 папках:

- `C:\ProgramData\InfoTeCS\ViPNet EndPoint Protection Server`
- `C:\ProgramData\InfoTeCS\ViPNet EndPoint Protection Server Console`

Обновление лицензии

В некоторых случаях необходимо обновить существующую лицензию, например для продления срока действия лицензии или увеличения количества защищаемых узлов. Для получения новой лицензии обратитесь в ИнфоТеКС (см. Обратная связь).

После получения лицензии обновите ее:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **О программе**.

3 На вкладке **Данные** нажмите **Обновить лицензию** и выберите файл новой лицензии формата `itcslic`.

4 Подтвердите обновление лицензии.

После обновления в окне 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).

Резервное копирование и восстановление конфигурации

Резервное копирование позволяет сохранять конфигурацию ViPNet EPP Сервер для быстрого восстановления в случаях сбоев или переустановки программного обеспечения. В резервной копии сохраняются:

- Используемые базы правил.
- Настройки ViPNet EPP Сервер.
- Журнал аудита ViPNet EPP Сервер.

Резервное копирование и восстановление из резервной копии возможно только в ViPNet EPP Серверная консоль, установленной на одном компьютере с ViPNet EPP Сервер.

Внимание! Восстановить конфигурацию из резервной копии возможно только на ViPNet EPP Сервер той же версии, что была при создании резервной копии.

Чтобы создать резервную копию текущей конфигурации ViPNet EPP Сервер:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Параметры системы**.

3 На вкладке **Сервис** нажмите **Создать копию**.

4 Укажите папку сохранения и имя файла резервной копии формата `bak`, нажмите **Сохранить**.

Внимание! При указании сетевой папки компьютер с ViPNet EPP Сервер и компьютер, где находится сетевая папка, должны входить в домен.

Чтобы восстановить конфигурацию ViPNet EPP Сервер из ранее сохраненной резервной копии:

1 Запустите ViPNet EPP Серверная консоль от имени администратора ОС Windows на компьютере, где установлен ViPNet EPP Сервер.

2 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

3 Выберите  **Параметры системы**.

4 На вкладке **Сервис** нажмите **Восстановить**.

5 Выберите файл резервной копии конфигурации формата `bak` и нажмите **Открыть**.

6 Для подтверждения восстановления из резервной копии нажмите **Да**.

7 Дождитесь восстановления конфигурации из резервной копии и нажмите **ОК**. ViPNet EPP Серверная консоль будет перезапущена.

8 Подключитесь к ViPNet EPP Сервер с любыми полномочиями. В результате начнет действовать восстановленная конфигурация.

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.

Чтобы настроить уведомления о событиях по электронной почте:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Передача данных**.

3 На вкладке **Электронная почта** включите **Использовать рассылку по электронной почте**.

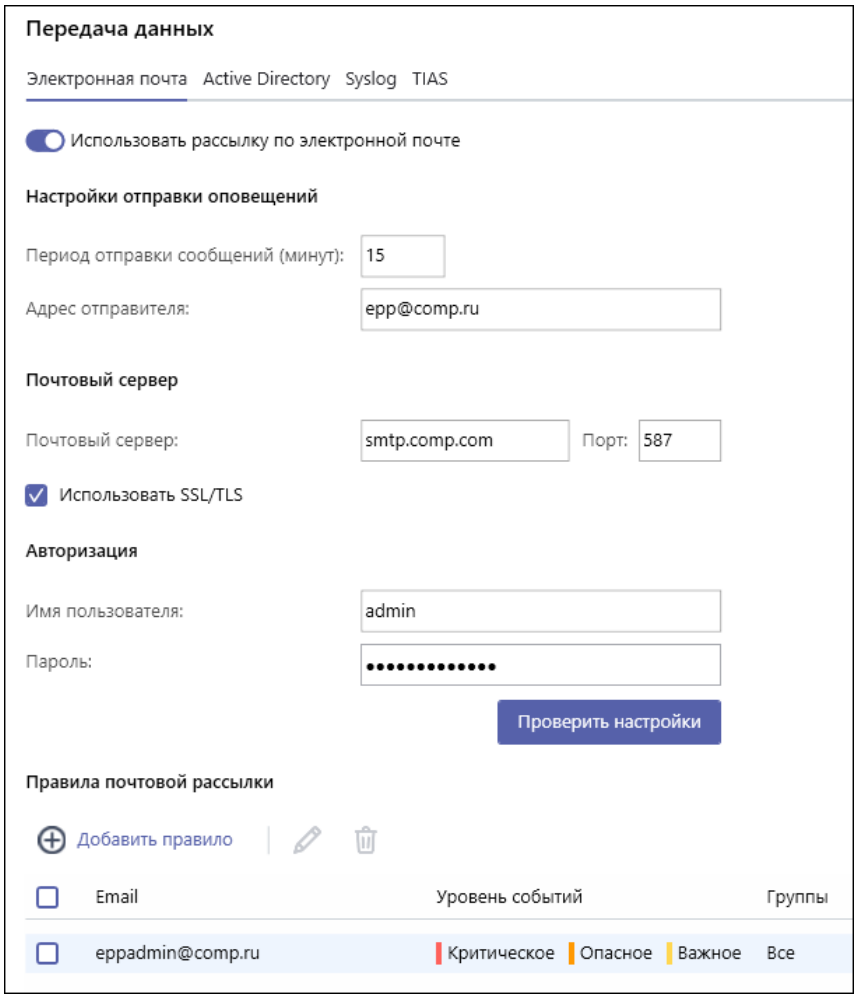


Рисунок 94. Настройка передачи уведомлений по электронной почте

4 В поле **Период отправки сообщений (минут)** укажите период рассылки уведомлений по электронной почте (рекомендуется — 15 минут).

5 В поле **Адрес отправителя** укажите электронный адрес, от имени которого будет осуществляться рассылка уведомлений.

6 В поле **Почтовый сервер** укажите адрес SMTP-сервера.

7 В поле **Порт** укажите порт SMTP-сервера (по умолчанию — 587).

8 Для защищенной передачи уведомлений по криптографическим протоколам SSL/TLS выберите **Использовать SSL/TLS**.

9 В полях **Имя пользователя** и **Пароль** укажите параметры доступа к электронному почтовому ящику, от имени которого будет осуществляться рассылка уведомлений.

10 Чтобы проверить правильность введенных данных, нажмите **Проверить настройки**.

11 Чтобы добавить правила почтовой рассылки, нажмите **Добавить правило**.

11.1 Введите адрес электронной почты получателя уведомления.

11.2 Выберите флажками уровни событий, при регистрации которых необходимо оповещать получателя.

11.3 Выберите группы, при регистрации событий на защищаемых узлах которых необходимо оповещать получателя.

11.4 Нажмите **Сохранить**.

12 Чтобы сохранить настройки уведомлений о событиях по электронной почте, нажмите **Сохранить**.

Подключение к домену Active Directory

Если защищаемые узлы расположены в корпоративной сети со службой каталогов Active Directory, вы можете импортировать их в ViPNet EPP Сервер из каталога. Перед импортом защищаемых узлов (см. Импорт защищаемых узлов из домена Active Directory) необходимо указать домен Active Directory:

1 Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.

2 Выберите **Передача данных**.

3 На вкладке **Active Directory** в поле **Домен** укажите имя домена, в котором находятся защищаемые узлы.

4 Нажмите **Сохранить**.

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 ViPNet EPP 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 ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите **Передача данных**.
3. На вкладке **Syslog** включите **Передача событий в Syslog**.
4. Выберите минимальный уровень событий — на сервер Syslog будут передаваться события этого и более высоких уровней:
   - **Критическое** — события критического уровня.
   - **Опасное** — события критического и опасного уровней (установлен по умолчанию).
   - **Важное** — события критического, опасного и важного уровней.
   - **Информационное** — о событиях всех уровней.
5. Выберите флажками типы правил — на сервер Syslog будут передаваться события о срабатывании правил выбранных типов (см. Типы и идентификаторы правил).
6. Укажите IP-адрес и UDP-порт сервера Syslog.
7. Чтобы проверить правильность настройки и доступность сервера Syslog, нажмите **Отправить тестовое сообщение**.
8. В появившемся окне нажмите **OK**.
9. Скопируйте идентификатор ViPNet EPP Сервер. Сообщите администратору сторонней системы IP-адрес и идентификатор ViPNet EPP Сервер.
10. Нажмите **Сохранить**.

Передача событий в ViPNet TIAS

Чтобы настроить передачу событий в ViPNet TIAS по протоколу TCP:

1. Подключитесь к ViPNet EPP Сервер с полномочиями администратора ViPNet EPP.
2. Выберите **Передача данных**.
3. На вкладке **TIAS** включите **Передача событий в ViPNet TIAS**.
4. Выберите минимальный уровень событий — в ViPNet TIAS будут передаваться события этого и более высоких уровней:
   - **Критическое** — события критического уровня.
   - **Опасное** — события критического и опасного уровней (установлен по умолчанию).
   - **Важное** — события критического, опасного и важного уровней.
   - **Информационное** — о событиях всех уровней.

5 Выберите флажками типы правил — в ViPNet TIAS будут передаваться события о срабатывании правил выбранных типов.

6 Укажите IP-адрес сервера ViPNet TIAS.



Внимание! По умолчанию сервер ViPNet TIAS использует TCP-порт 34222. Не изменяйте его без указания администратора ViPNet TIAS.

7 Чтобы проверить правильность настройки и доступность сервера ViPNet TIAS, нажмите **Отправить тестовое сообщение**.

8 Скопируйте идентификатор ViPNet EPP Сервер. Сообщите администратору ViPNet TIAS IP-адрес и идентификатор ViPNet EPP Сервер.

9 Нажмите **Сохранить**.

4

Локальное управление ViPNet EPP Агент

Подключение к ViPNet EPP Агент 240

Интерфейс ViPNet EPP Агент 241

Установка и активация лицензии 243

Управление базой правил 244

Управление фильтрацией трафика 248

Просмотр статуса выполнения политики ZTNA 259

Управление запуском и активностью приложений 260

Управление обнаружением и предотвращением вторжений 275

Настройка критериев обнаружения аномалий 284

Работа с журналами 285

Администрирование ViPNet EPP Агент 292

Подключение к ViPNet EPP Агент

ViPNet EPP Агент запускается автоматически при загрузке ОС Windows. Чтобы подключиться к ViPNet EPP Агент:

1 В меню **Пуск** начните вводить **ViPNet EndPoint Protection** и запустите найденную программу.

2 В окне аутентификации введите параметры входа в ViPNet EPP Агент:

- Введите имя и пароль вашей учетной записи.

  При первом подключении к ViPNet EPP Агент после установки войдите с учетной записью администратора агента, заданной при установке ViPNet EPP Агент вручную (см. Установка ViPNet EPP Агент вручную) или с помощью групповых политик (см. Установка ViPNet EPP Агент с помощью групповых политик Active Directory).

- Чтобы при последующем запуске ViPNet EPP Агент не вводить имя пользователя и пароль учетной записи, выберите **Запомнить меня**.

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** 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 **Использовать простой пароль** и указать любой пароль, отличающийся от предыдущего, но в целях безопасности использовать простые пароли не рекомендуется.

5 Нажмите **Готово**.

6 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, загрузки базы правил.

Интерфейс ViPNet EPP Агент

Интерфейс ViPNet EPP Агент зависит от способа работы (автономно или под управлением сервера) и полномочий пользователя.

На рисунке ниже в качестве примера представлено главное окно автономного ViPNet EPP Агент пользователя с максимальными полномочиями администратора агента.

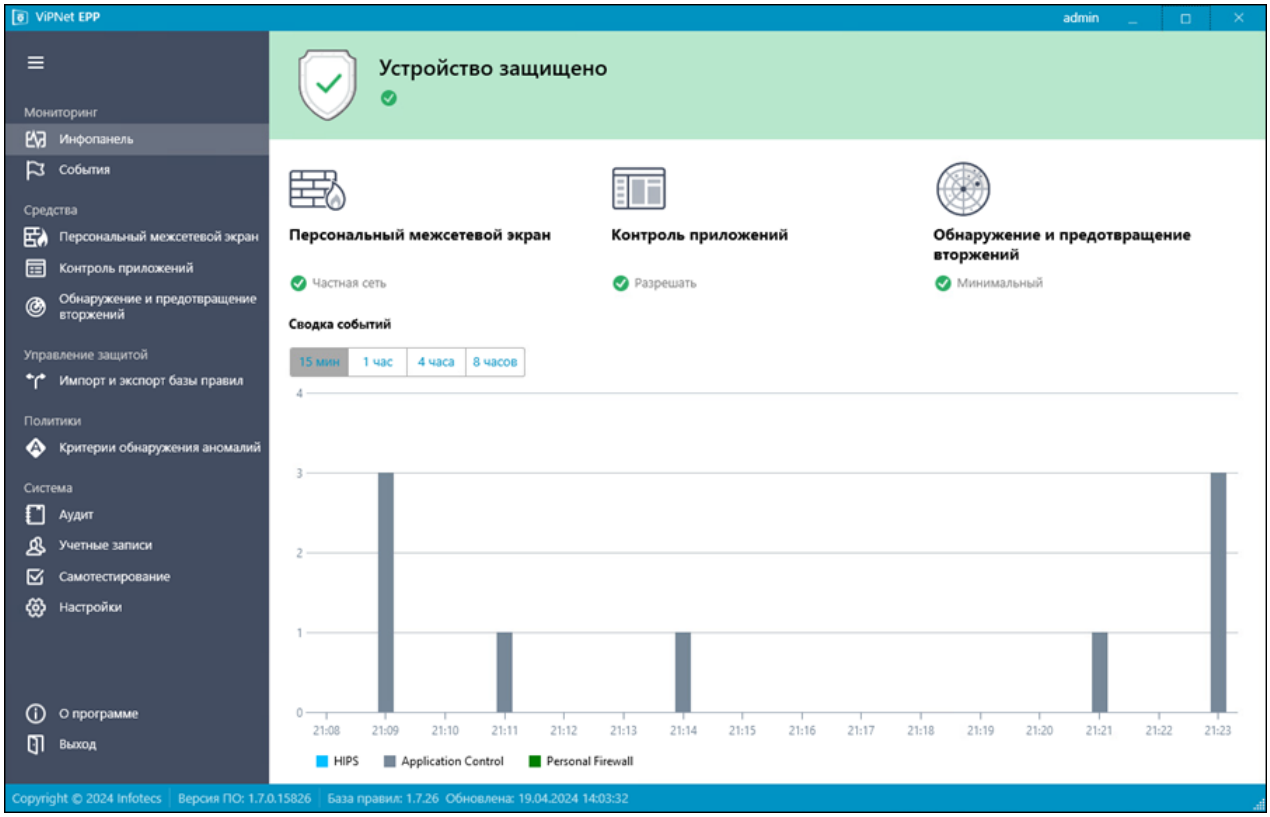


Рисунок 95. Главное окно автономного ViPNet EPP Агент

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

- **Инфопанель** — статус защиты устройства, просмотр режимов работы модулей защиты ViPNet EPP Агент, сводка событий.
- **События** — просмотр зарегистрированных событий на защищаемом узле (см. Журнал событий).
- **Персональный межсетевой экран** — управление фильтрацией трафика на защищаемом узле (см. Управление фильтрацией трафика).
- **Контроль приложений** — управление запуском и активностью приложений на защищаемом узле (см. Управление запуском и активностью приложений).

- **Обнаружение и предотвращение вторжений** — управление обнаружением и предотвращением вторжений на защищаемом узле (см. Управление обнаружением и предотвращением вторжений).
- **ZTNA** — доступно только в ViPNet EPP Агент под управлением сервера. Просмотр статуса выполнения политики ZTNA.
- **Импорт и экспорт базы правил** — доступно только в автономном ViPNet EPP Агент. Загрузка и выгрузка базы правил (см. Управление базой правил).
- **Критерии обнаружения аномалий** — доступно только в автономном ViPNet EPP Агент. Настройка критериев обнаружения аномалий.
- **Аудит** — просмотр журнала аудита ViPNet EPP Агент (см. Журнал аудита).
- **Учетные записи** — управление учетными записями ViPNet EPP Агент (см. Управление учетными записями).
- **Самотестирование** — проверка работоспособности ViPNet EPP Агент (см. Проверка работоспособности).
- **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 лицензии). Для автономного ViPNet EPP Агента — установка и активация лицензии.
- **Выход** — 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** > **Данные**.

3 Нажмите **Загрузить лицензию** и выберите файл лицензии формата `itcslic`.

После загрузки лицензии на вкладке отобразится информация о лицензии. Статус лицензии: **Не активирована**. Тип лицензии: **Автономная**.

4 Активируйте лицензию одним из способов аналогично действиям в ViPNet EPP Сервер (см. Установка и активация лицензии).

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 на 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 базу правил 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 Windows (см. Распространение настроек средств защиты на другие агенты). Загрузка базы правил, экспортированной с автономного ViPNet EPP Агент for Linux, 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 к 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.

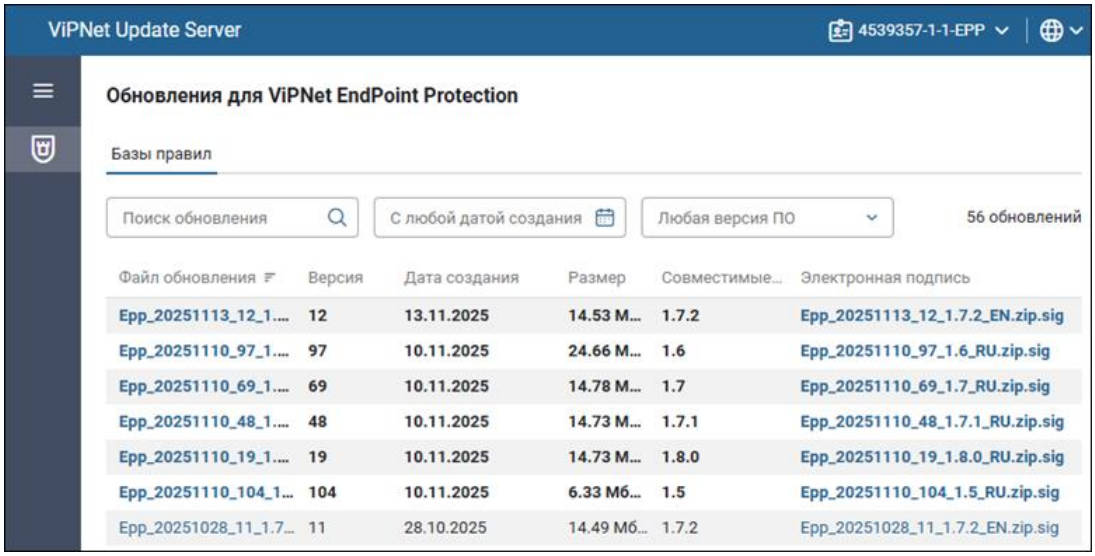


Рисунок 96. Главная страница сервера обновлений ViPNet Update Server

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 Нажмите **Импорт базы 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 Нажмите **Открыть**.

6 Если база правил была загружена впервые, дождитесь завершения импорта базы правил. Нажмите **OK**.

7 Если ранее в ViPNet EPP Агент уже была загружена база правил:

7.1 В окне **Настройки импорта** укажите, какие параметры установленной базы правил нужно заменить параметрами импортируемой базы правил, а какие параметры оставить без изменения:

- Для режимов работы модулей, правил **HIDS**, правил **HIPS** и веб-фильтров, модели и настроек **AntiMalware**, настроек агента и политик аудита выберите: заменить или оставить без изменений (не заменять).

- Для правил **Контроля приложений** выберите: заменить, добавить новые правила после существующих (добавить в конец) или оставить без изменения (не заменять). Правила, созданные в ViPNet EPP Агент по умолчанию, не будут изменены при любом выборе.
- Для сетевых фильтров и справочников **Персонального межсетевого экрана** выберите:
  - Заменить, не заменять, добавить новые сетевые фильтры после существующих или добавить новые сетевые фильтры до существующих, в зависимости от приоритета.
  - Импортировать ли новые справочники, не используемые в импортируемых сетевых фильтрах. Справочники, используемые в импортируемых сетевых фильтрах, импортируются всегда.
- Для критериев обнаружения аномалий выберите: заменить, добавить новые критерии после существующих (добавить в конец) или оставить без изменения (не заменять).

7.2 Нажмите **Готово**.

7.3 Дождитесь завершения импорта базы правил. Нажмите **OK**.

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.

  Источник получения базы правил (**Комплект поставки** или **Сервер обновлений**). Если база правил была отредактирована пользователем, дополнительно будет указано — **отредактированная**.
- Имя файла обновления.

Распространение настроек средств защиты на другие агенты

Если модули защиты и параметры работы нескольких автономных 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 запуском и активностью приложений.
   - 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 (см. Экспорт базы правил).

4 Загрузите экспортированную базу правил на другие агенты (см. Загрузка и обновление базы правил).

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_AgentWin_Policy_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 **Экспорт базы правил**, укажите папку сохранения и имя файла архива базы правил в формате ZIP. Нажмите **Сохранить**.

Дождитесь завершения экспорта базы правил. Нажмите **OK**.

Управление фильтрацией трафика

Выбор режима работы

По умолчанию режим работы персонального межсетевого экрана устанавливается из базы правил. При автономной работе ViPNet EPP Агент режим **Публичная сеть** не используется и не отображается.

Для учета особенностей фильтрации IP-пакетов на защищаемом узле режим работы можно изменить:

1. Подключитесь к ViPNet EPP Агент с любыми полномочиями.
2. Выберите **Персональный межсетевой экран** > **Режимы работы**.
3. В разделе **Режим работы** выберите режим. При отключении персонального межсетевого экрана в ViPNet EPP Агент под управлением сервера проверка выполнения настроенной политики ZTNA (см. Просмотр статуса выполнения политики ZTNA) будет продолжена, при этом на защищаемом узле с ViPNet Client 5 не будет блокироваться доступ к защищенной сети ViPNet при невыполнении политики ZTNA.

Выбранный режим будет отмечен .

Основные действия по управлению фильтрацией

Для удобства работы пользователей основные действия по управлению фильтрацией трафика защищаемого узла собраны в одном разделе:

1. Подключитесь к ViPNet EPP Агент с любыми полномочиями.
2. Выберите **Персональный межсетевой экран** > **Режимы работы**.
3. В разделе **Задачи:**

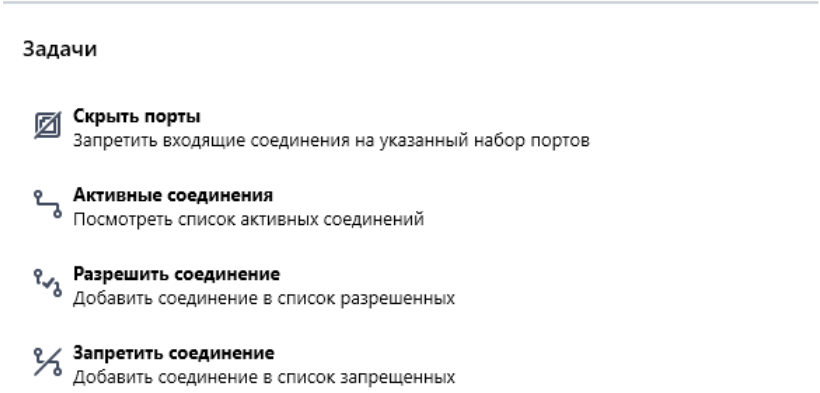


Рисунок 97. Основные действия по управлению фильтрацией трафика

- Чтобы запретить входящие соединения по определенным портам, создайте блокирующий пользовательский фильтр (см. Запрет входящих соединений).
- Чтобы просмотреть список активных соединений, Журнал активных соединений.
- Чтобы разрешить или запретить соединение, создайте разрешающий или блокирующий пользовательский фильтр (см. Настройка пользовательских сетевых фильтров).

Настройка пользовательских сетевых фильтров

Сетевые фильтры персонального межсетевого экрана ViPNet EPP Агент (см. Персональный межсетевой экран) применяются на защищаемом узле для контроля и фильтрации IP-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 5, доступно создание пользовательских сетевых фильтров защищенной сети ViPNet.

Чтобы настроить пользовательский сетевой фильтр:

1 Подключитесь к ViPNet EPP Агент с учетной записью администратора агента.

2 Выберите **Персональный межсетевой экран**.

3 Выберите один из режимов сети (**Частная сеть** или **Корпоративная сеть**) и нажмите **Создать фильтр**.

4 Чтобы создать фильтр для открытого трафика, не относящегося к защищенной сети ViPNet, выберите **Фильтр открытой сети**. Выполните последовательность действий по созданию пользовательского сетевого фильтра, аналогичную созданию фильтра политик безопасности на ViPNet EPP Сервер (см. Настройка фильтров политик безопасности).

5 Чтобы создать сетевой фильтр для защищенной сети ViPNet, выберите **Фильтр защищенной сети ViPNet**. Этот пункт доступен для выбора только если на защищаемом узле установлена программа ViPNet Client 5. Далее следуйте указаниям мастера создания фильтра:

5.1 Определите действие фильтра при срабатывании и выберите режимы, в которых фильтр будет применяться (**Частная сеть** или **Корпоративная сеть**).

- **Разрешить** — пропустить IP-пакет.
- **Блокировать** — блокировать IP-пакет.

5.2 Укажите протоколы передачи IP-пакетов, включив нужные справочники протоколов. По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам.

5.3 На странице **Укажите адреса источников** задайте отправителей IP-пакетов, на основании которых будет срабатывать фильтр. Для этого включите нужные справочники адресов. Доступны справочники, созданные на вкладке **Справочники ViPNet**.

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

5.4 На странице **Укажите адреса назначений** задайте получателей IP-пакетов, на основании которых будет срабатывать фильтр. Для этого включите нужные справочники адресов. Доступны справочники, созданные на вкладке **Справочники ViPNet**.

5.5 На странице **Установите расписание** назначьте справочники расписаний. Если расписания не установлены, фильтр политик безопасности будет действовать постоянно.

5.6 На странице **Подтверждение** введите название фильтра и проверьте заданные параметры.

5.7 Нажмите **Готово**.

В результате выполнения шагов 4 и 5 для указанных режимов в разделе **Пользовательские фильтры** будет создан пользовательский сетевой фильтр для открытой сети или для защищенной сети ViPNet соответственно. Сетевые фильтры защищенной сети ViPNet будут отмечены значком . Новые созданные сетевые фильтры будут выделены жирным шрифтом.

6 Задайте порядок применения пользовательских фильтров в каждом из режимов (**Частная сеть** и/или **Корпоративная сеть**) с помощью ↑ и ↓.

7 Чтобы изменения вступили в силу, в каждом из режимов (**Частная сеть** и/или **Корпоративная сеть**) нажмите **Применить**.

Чтобы изменить параметры пользовательского фильтра:

1 Выберите один из режимов сети (**Частная сеть** или **Корпоративная сеть**).

2 В списке пользовательских фильтров дважды щелкните строку фильтра или предварительно на панели вверху воспользуйтесь поиском по названию фильтра.

3 На панели справа на вкладке **Основные** вы можете изменить название, действие и активность фильтра.

4 На панели справа на вкладках **Протоколы**, **Источники**, **Назначения** и **Расписания** внесите необходимые изменения.

5 Нажмите **OK**.

6 Нажмите **Применить**.

Настройка пользовательских справочников

При создании и изменении пользовательских фильтров применяются пользовательские справочники протоколов, адресов и сетей, расписаний. Эти справочники устанавливаются и обновляются на защищаемом узле вместе с ViPNet EPP Агент. Чтобы настроить пользовательские справочники:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Персональный межсетевой экран**.

3 Выберите тип справочника:

- **Протоколы** и на вкладке **Пользовательские** нажмите **Добавить протоколы**.
- **Адреса и сети** и на вкладке **Пользовательские** нажмите **Добавить адреса**.
- **Расписания** и на вкладке **Пользовательские** нажмите **Добавить расписание**.

Примечание. На вкладке **Глобальные** вы можете просмотреть глобальные справочники персонального межсетевого экрана ViPNet EPP Агент.

---

4 Выполните последовательность действий, такую же, как при настройке глобальных справочников на ViPNet EPP Сервер (см. Настройка справочников).

Чтобы изменить пользовательский справочник:

1 Дважды щелкните строку справочника в списке или предварительно на панели вверху воспользуйтесь поиском по названию справочника.

2 На панели справа на вкладке **Основные** вы можете изменить название справочника, а также просмотреть применение справочника в сетевых фильтрах.

3 На вкладках **Состав** и **Исключения** внесите необходимые изменения и нажмите **Сохранить**.

4 Нажмите **OK**.

5 Нажмите **Применить**.

Чтобы удалить пользовательский справочник, на вкладке **Пользовательские** дважды щелкните строку справочника в списке и на панели справа нажмите . Чтобы удалить сразу несколько справочников, выберите их флажками и на панели справа нажмите . В результате справочники будут удалены, если они не используются в сетевых фильтрах. Нажмите **Применить**.

Настройка справочников ViPNet

Если на защищаемом узле установлена программа ViPNet Client 5, доступно создание пользовательских справочников адресов сети ViPNet, которые можно использовать при создании пользовательских сетевых фильтров защищенной сети ViPNet (см. Настройка пользовательских сетевых фильтров).

Чтобы добавить справочник адресов ViPNet:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Персональный межсетевой экран** > **Адреса и сети**.

3 На вкладке **Справочники ViPNet** на панели вверху нажмите **Добавить адреса**.

Примечание. Если ViPNet Client 5 не установлен, рядом с кнопкой добавления справочника будет отображаться сообщение **Нет данных об адресах сети ViPNet** и кнопка создания справочника будет недоступна.

---

4 Выберите флажками один или несколько сетевых узлов ViPNet. В списке сетевых узлов отображаются только узлы, с которыми есть связь в программе ViPNet Client 5.

5 Укажите название нового справочника адресов ViPNet и проверьте состав справочника.

6 Нажмите **Готово**.

7 Нажмите **Применить**.

Чтобы изменить настройки справочника адресов ViPNet:

1 На вкладке **Справочники ViPNet** в списке справочников дважды щелкните нужный справочник или предварительно на панели вверху воспользуйтесь поиском по названию справочника.

2 На панели справа на вкладке **Основные** вы можете изменить название справочника, а также просмотреть применение справочника в сетевых фильтрах.

3 На вкладке **Состав** внесите необходимые изменения и нажмите **Сохранить**.

4 Нажмите **OK**, чтобы сохранить все изменения.

5 Нажмите **Применить**.

Чтобы удалить справочник адресов ViPNet, на вкладке **Справочники ViPNet** дважды щелкните строку справочника в списке и на панели справа нажмите . Чтобы удалить сразу несколько справочников, выберите их флажками и на панели справа нажмите . В результате справочники будут удалены, если они не используются в сетевых фильтрах. Нажмите **Применить**.

Запрет входящих соединений

Если требуется ограничить доступ к защищаемому узлу через определенные порты, создайте блокирующий пользовательский фильтр по портам:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Персональный межсетевой экран** > **Режимы работы**.

3 В разделе **Задачи** нажмите **Скрыть порты**.

4 На шаге 1 выберите версию IP-протокола.

5 На шаге 2:

5.1 Укажите один или несколько портов, на которые вы хотите запретить входящие соединения.

Примечание. При указании диапазона портов разделяйте начальное и конечное значение диапазона дефисом. Например, 20-27. При указании нескольких портов или диапазонов портов разделяйте их запятыми. Например, 40-45,80,81,593.

5.2 Выберите режимы, в которых будет действовать фильтр.

6 На шаге 3 включите нужные справочники расписаний. Если расписания не установлены, фильтр будет действовать постоянно.

7 На шаге 4 введите название фильтра и проверьте заданные параметры. Чтобы изменить параметры, используйте кнопку **Назад**. Режим и расписание можно изменить, щелкнув значение параметра.

8 Нажмите **Готово**.

В результате для указанных режимов будет создан фильтр, который отобразится на страницах сетевых фильтров для выбранных режимов (**Частная сеть** или **Корпоративная сеть**) в группе **Пользовательские фильтры**.

9 Задайте порядок применения пользовательского фильтра в каждом из режимов с помощью или .

10 Чтобы изменения вступили в силу, на странице каждого режима, для которого создан фильтр, нажмите **Применить**.

Работа с журналами персонального межсетевого экрана

Журнал активных соединений

Персональный 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 персонального межсетевого экрана ViPNet EPP Агент. При обнаружении подозрительной сетевой активности приложений вы можете заблокировать их.

Примечание. Приложение можно заблокировать, если персональный 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 **Персональный межсетевой экран** > **Активные соединения**.

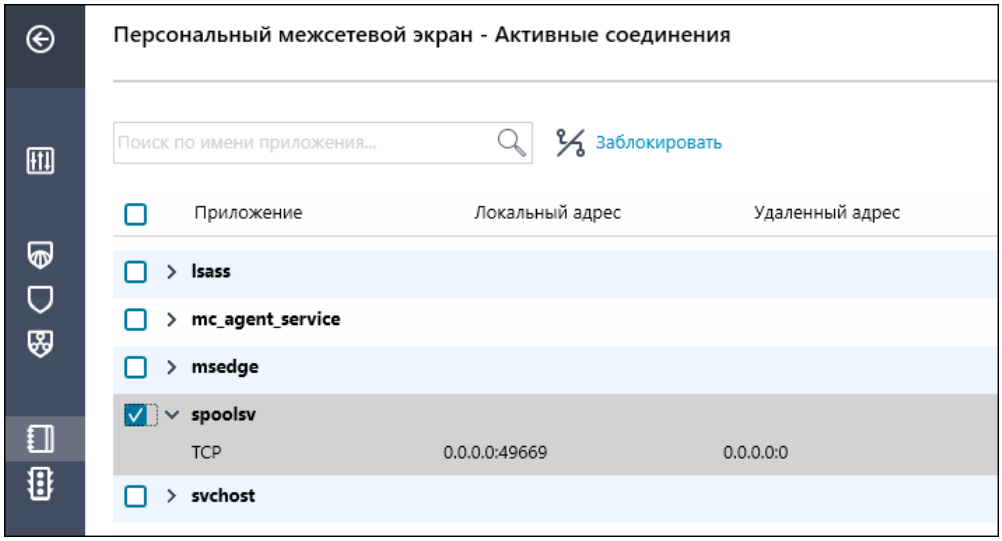


Рисунок 98. Журнал активных соединений персонального межсетевого экрана ViPNet EPP Агент

3 Для просмотра параметров соединения (протокола, локального и удаленного адресов) щелкните .

4 Чтобы разорвать соединение и заблокировать приложение:

4.1 Выберите флажком нужное приложение.

4.2 На панели вверху нажмите **Заблокировать**.

4.3 Для подтверждения нажмите **Да**.

4.4 При блокировании приложения создается пользовательский сетевой фильтр с действием **Блокировать**. Фильтр отобразится в разделе сетевых фильтров частной или корпоративной сети, в зависимости от режима работы персонального межсетевого экрана ViPNet EPP Агент и будет выделен жирным шрифтом (см. Настройка пользовательских сетевых фильтров). Порядок расположения этого фильтра не имеет значения, фильтр будет действовать независимо от других сетевых фильтров. Чтобы фильтр начал действовать, на странице сетевых фильтров режима нажмите **Применить.**

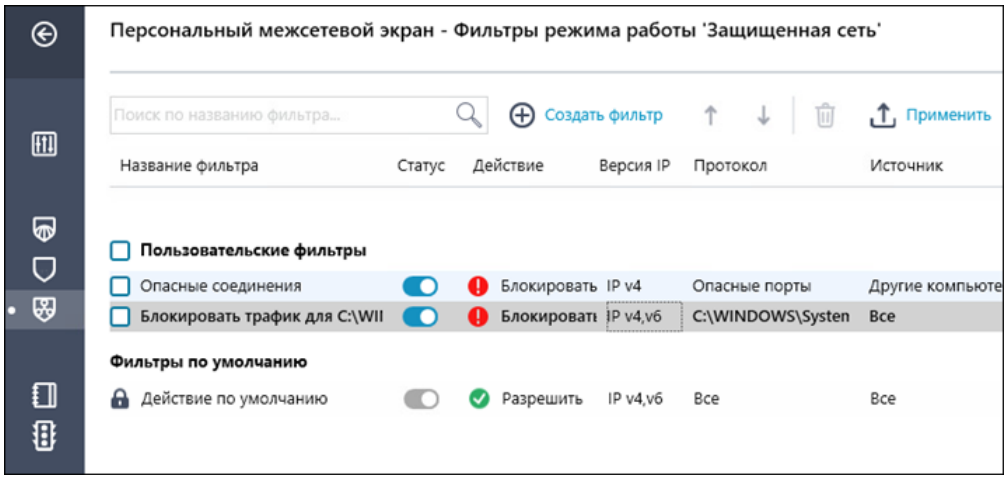


Рисунок 99. Создание пользовательского блокирующего фильтра для приложения из журнала активных соединений

Чтобы разблокировать приложение — разрешить сетевую активность, необходимо удалить пользовательский фильтр, блокирующий приложение, или изменить статус активности фильтра — в столбце **Статус** выключите .

Журнал трафика

В персональном 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 персонального межсетевого экрана ViPNet EPP Агент:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.

2 Выберите **Персональный межсетевой экран** > **Трафик**.

Примечание. По умолчанию отображается информация обо всех зарегистрированных IP-пакетах за последние сутки.

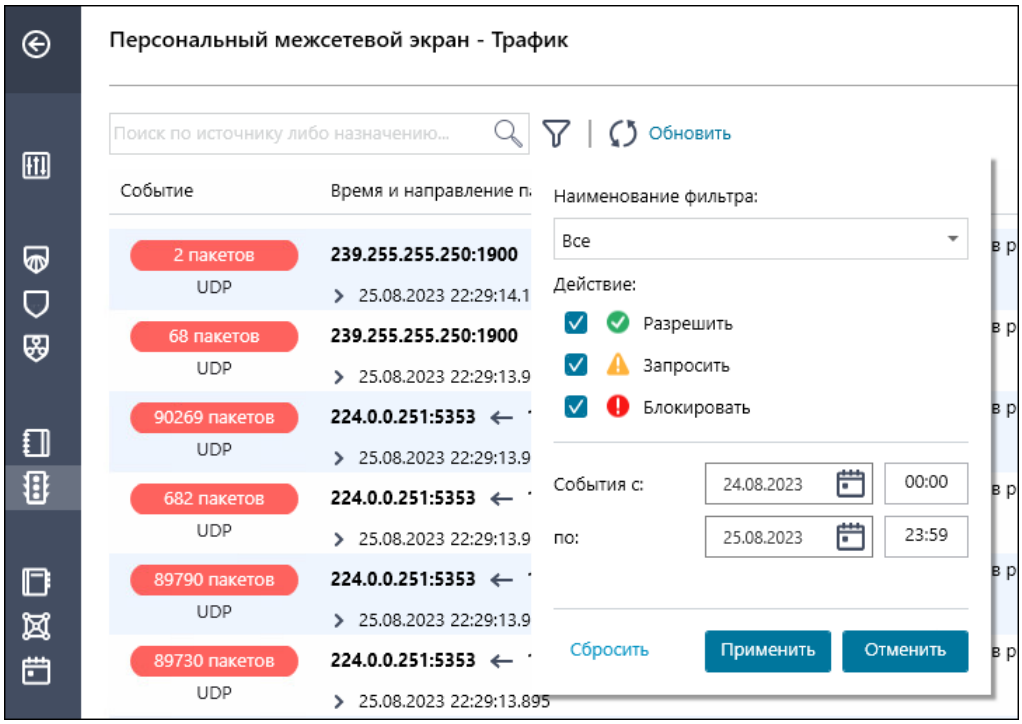


Рисунок 100. Журнал регистрации трафика персонального межсетевого экрана ViPNet EPP Агент

Каждая запись о событии в журнале содержит:

- **Событие** — протокол передачи и количество зарегистрированных однотипных IP-пакетов за указанный период времени. Зеленым цветом отмечены разрешенные IP-пакеты, а красным цветом — заблокированные.
- **Время и направление пакетов** — направление (← — входящие IP-пакеты, → — исходящие IP-пакеты), IP-адреса и порты источника и назначения, а также дату и время

регистрации последнего IP-пакета данного типа. Слева всегда отображается адрес вашего защищаемого узла, на котором открыт просмотр журнала трафика.

- **Фильтр** — сетевой фильтр из разделов **Частная сеть** и **Корпоративная сеть** или системный фильтр, по срабатыванию которого было зарегистрировано событие (подробнее см. в разделе для сервера Запрос журнала регистрации трафика с ViPNet EPP Агент).
- **Тип сети** — 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.

Вы можете отсортировать записи журнала по любому из указанных параметров.

3 Чтобы найти определенные события, в поле поиска введите часть адреса источника или назначения IP-пакета и/или воспользуйтесь фильтром поиска по названию, действию сетевого фильтра, периоду времени.

4 Чтобы просмотреть дату и время регистрации каждого IP-пакета события, выберите нужное событие и щелкните поле даты и времени регистрации последнего IP-пакета события.

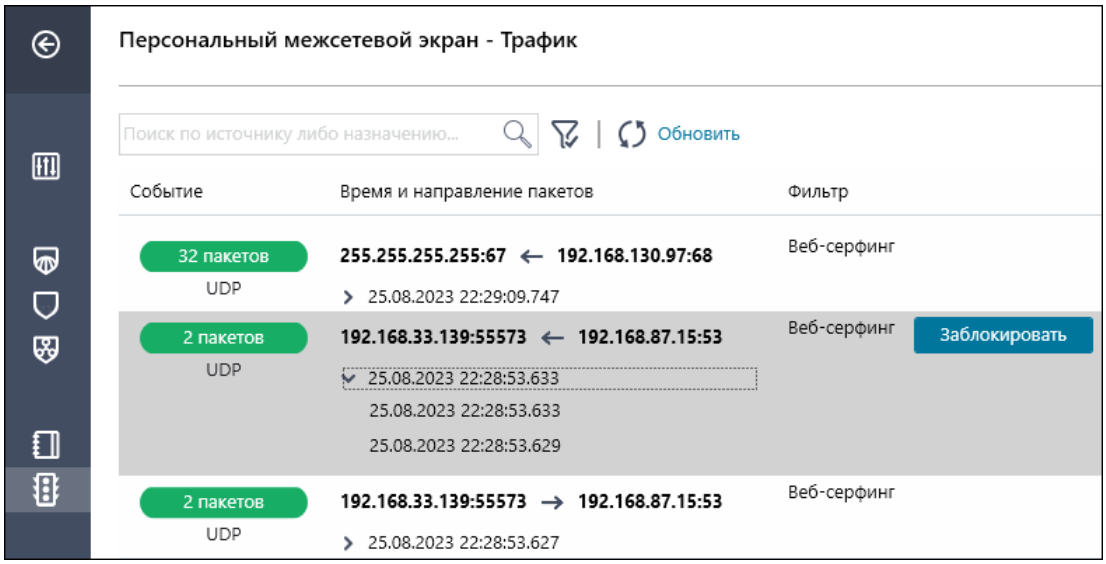


Рисунок 101. Просмотр даты и времени регистрации каждого IP-пакета события

Чтобы на основе зарегистрированного события, не относящегося к защищенному трафику сети ViPNet, создать блокирующий или разрешающий пользовательский фильтр:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Персональный межсетевой экран** > **Трафик**.

3 Выполните одно из действий:

- Чтобы заблокировать ранее разрешенный пользовательскими фильтрами открытый трафик, наведите указатель на строку с нужным событием (с параметрами разрешенного

трафика, который вы хотите заблокировать) и нажмите появившуюся кнопку **Заблокировать**.

- Чтобы разрешить ранее заблокированный пользовательскими фильтрами открытый трафик, наведите указатель на строку с нужным событием (с параметрами заблокированного трафика, который вы хотите разрешить) и нажмите появившуюся кнопку **Разблокировать**.

4 В окне создания блокирующего или разрешающего фильтра:

4.1 Укажите название фильтра.

4.2 Выберите режимы, в которых будет применяться фильтр.

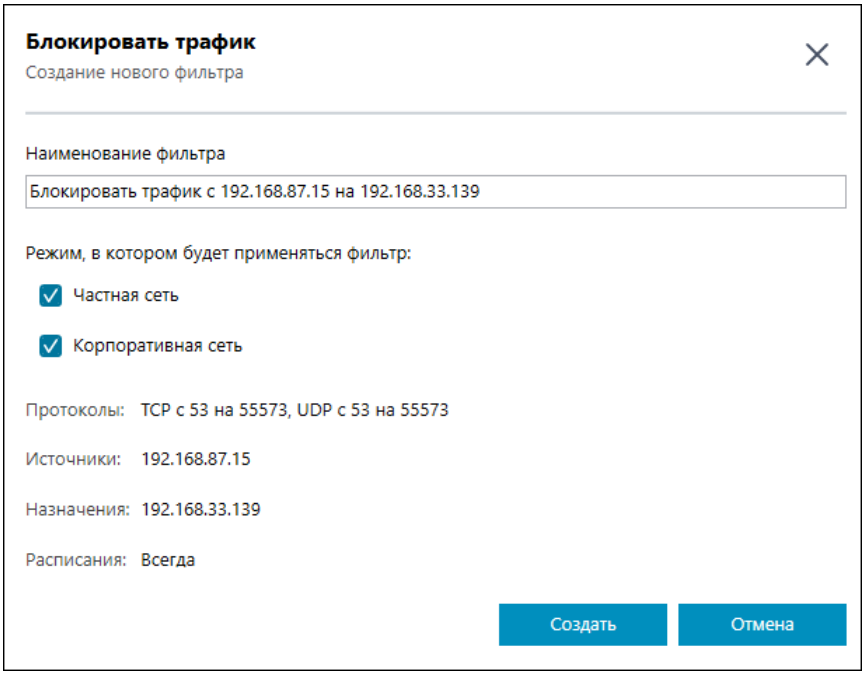


Рисунок 102. Создание пользовательского блокирующего фильтра

4.3 Нажмите **Создать**.

Фильтр отобразится на странице частной или корпоративной сетей, в зависимости от режима, в котором будут применяться фильтры.

4.4 На странице частной или корпоративной сетей нажмите **Применить**.

Примечание. Если для события журнала трафика ранее создавался пользовательский фильтр с противоположным действием, такой фильтр необходимо либо удалить, либо выключить, либо изменить порядок применения.

Просмотр статуса выполнения политики ZTNA

Функция недоступна для защищаемых узлов с автономным ViPNet EPP Агент.

Политики ZTNA (см. Сетевой доступ с нулевым доверием (ZTNA)) для группы защищаемых узлов устанавливаются централизованно при назначении на группу базы правил.

Чтобы просмотреть статус выполнения политики ZTNA:

1 Подключитесь к ViPNet EPP Агент с любыми полномочиями.

2 Выберите **ZTNA**.

3 Просмотрите статус выполнения политики ZTNA:

- **Политика выполняется** — защищаемый узел прошел проверку в соответствии со всеми Управление политиками ZTNA. Если на защищаемом узле установлена программа ViPNet Client 5, доступ к защищенной сети ViPNet разрешен.
- **Политика не выполняется** — защищаемый узел не прошел проверку по заданным правилам политики ZTNA. Ниже в списке будут перечислены правила, параметрам которых не соответствует защищаемый узел. Если на защищаемом узле установлена программа ViPNet Client 5 и включен персональный межсетевой экран, доступ к ресурсам защищенной сети защищенной сети ViPNet 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**.
- **Политика не назначена** — политики ZTNA выключены в базе правил.

  Если отключен персональный межсетевой экран, на защищаемом узле с ViPNet Client 5 не будет блокироваться доступ к защищенной сети ViPNet при невыполнении политики ZTNA.

Управление запуском и активностью приложений

Выбор режима работы контроля приложений

По умолчанию режим работы контроля приложений устанавливается из базы правил. Режим работы определяет возможность запуска приложений, не входящих в списки контроля приложений (см. Просмотр списков контроля приложений). Для учета особенностей контроля активности приложений на защищаемом узле режим работы можно изменить:

1 Подключитесь к ViPNet EPP Агент с любыми полномочиями.

2 Выберите **Контроль приложений** > **Режимы работы**.

3 В разделе **Режим работы** выберите нужный режим (Блокировать, Разрешать или Отключено).

Выбранный режим будет отмечен .

Чтобы разрешить или запретить запуск определенных приложений, в разделе **Задачи**:

- Чтобы внести приложение в одну из групп приложений белого списка, нажмите **Разрешить приложение** и выполните шаги сценария добавления приложения в белый список, как на ViPNet EPP Сервер (см. Управление запуском приложений).
- Чтобы внести приложение в группу **Запрещенные** черного списка, нажмите **Запретить приложение** и выполните шаги сценария добавления приложения в черный список, как на ViPNet EPP Сервер (см. Управление запуском приложений).

Просмотр списков контроля приложений

К спискам контроля приложений, используемым на защищаемом узле, относятся:

- Глобальные белый и черный списки (только для ViPNet EPP Агент под управлением ViPNet EPP Сервер).
- Пользовательские белый и черный списки.
- Прочие списки активности приложений, не попавших ни в белый, ни в черный список.

Чтобы просмотреть списки контроля приложений на защищаемом узле:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.

2 Выберите **Контроль приложений** > **Запуск приложений**.

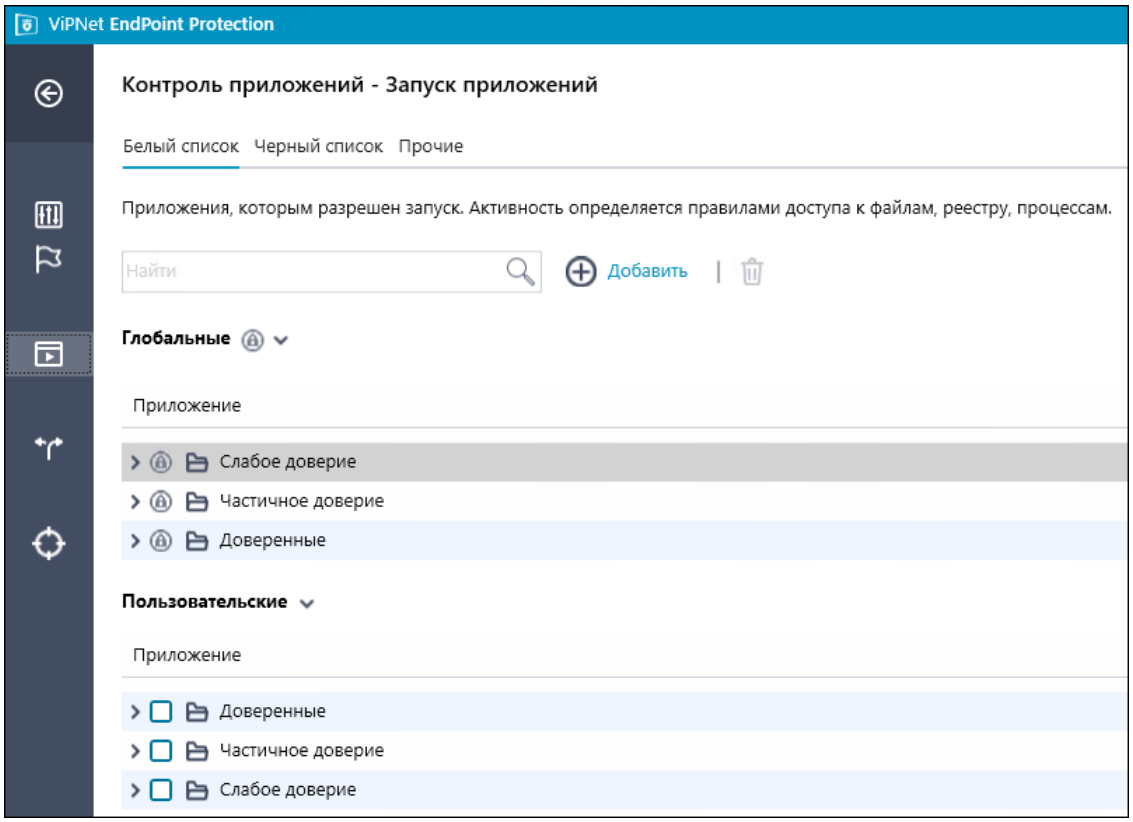


Рисунок 103. Просмотр списков приложений ViPNet EPP Агент

3 Выберите вкладку списка:

- **Белый список.**
  - Для просмотра приложений глобального белого списка раскройте последовательно список **Глобальные** и далее нужную группу приложений, например **Доверенные**.
  - Для просмотра приложений пользовательского белого списка раскройте последовательно список **Пользовательские** и далее нужную группу приложений, например **Доверенные**.
- **Черный список**.
  - Для просмотра приложений глобального черного списка раскройте список **Глобальные**.
  - Для просмотра приложений пользовательского черного списка раскройте список **Пользовательские**.
- **Прочие** — в этом списке отображаются запускаемые на защищаемом узле приложения, не входящие в черный и белый списки. Активность приложений определяется режимом работы контроля приложений. Если режим работы **Блокировать**, запуск приложения будет запрещен, если режим работы **Разрешать**, запуск приложения будет разрешен.

4 Для поиска приложения в выбранном списке, в поле поиска введите часть имени приложения или имя целиком и нажмите .

Управление пользовательскими списками приложений

Чтобы разрешить запуск приложения, добавьте правило запуска в пользовательский белый список:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **Запуск приложений**.

3 На вкладке **Белый список** нажмите **Добавить** и выполните шаги сценария создания правила запуска и добавления в белый список, как в ViPNet EPP Сервер (см. Управление запуском приложений).

Примечание. При внесении приложения в группу пользовательского белого списка вы можете сразу задать правила доступа (см. Создание правил доступа приложения).

Чтобы запретить запуск приложения, добавьте правило запуска в пользовательский черный список:

1 На вкладке **Черный список** нажмите **Добавить**.

2 Выполните шаги сценария создания правила запуска и добавления в черный список, как на ViPNet EPP Сервер (см. Управление запуском приложений).

Чтобы изменить параметры правила запуска приложений из пользовательского белого или черного списков:

1 Выберите вкладку **Белый список** или **Черный список**.

2 Дважды щелкните строку с названием приложения в списке и на панели справа:

2.1 В поле **Путь** измените путь к приложению.

2.2 Включите или выключите формирование событий. По умолчанию формирование событий включено.

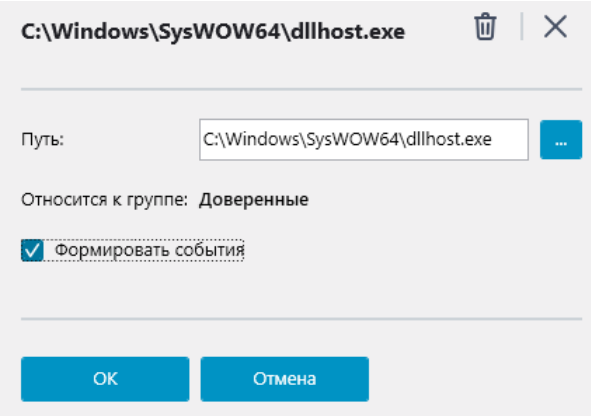


Рисунок 104. Дополнительная панель параметров приложения

2.3 Нажмите **OK**.

3 Нажмите **Применить**.

Чтобы временно исключить правила запуска приложения из пользовательского белого или черного списков:

1 Выберите вкладку **Белый список** или **Черный список**.

2 Выключите правила приложений, которые необходимо исключить из выбранного списка.

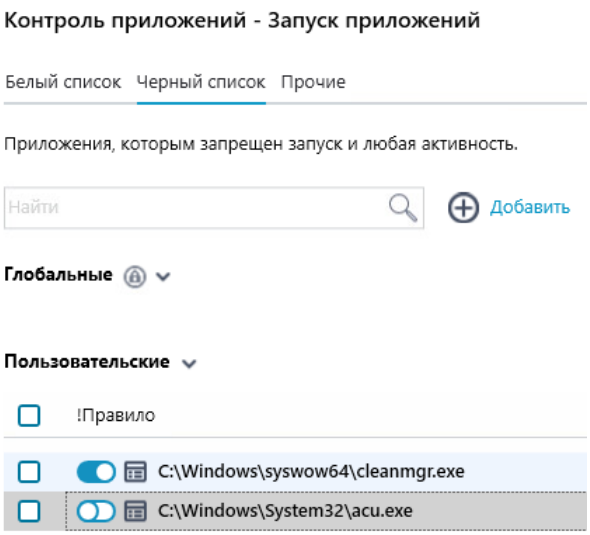


Рисунок 105. Временное исключение приложения из пользовательского черного списка

3 Нажмите **Применить**.

Чтобы удалить правила запуска приложений из пользовательских белого или черного списков:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **Запуск приложений**.

3 Выберите вкладку **Белый список** или **Черный список**.

4 Выберите флажками правила для удаления и нажмите .

5 Нажмите **Применить**.

Перемещение правила запуска приложения между пользовательскими белым и черным списками выполняется в два этапа:

1 Удалите правило из одного пользовательского списка, например из черного.

2 Создайте аналогичное правило в другом списке, например в белом.

Таким же образом можно переместить правила из одной группы пользовательского белого списка в другую, например из группы **Частичное доверие** в группу **Слабое доверие**.

Создание правил доступа приложения

При создании правил доступа приложения необходимо учитывать особенности задания и использования этих правил (см. Особенности задания и использования правил доступа).

Чтобы создать правила доступа приложения из пользовательского белого списка:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **Правила доступа**.

3 Раскройте группу и щелкните строку с названием приложения.

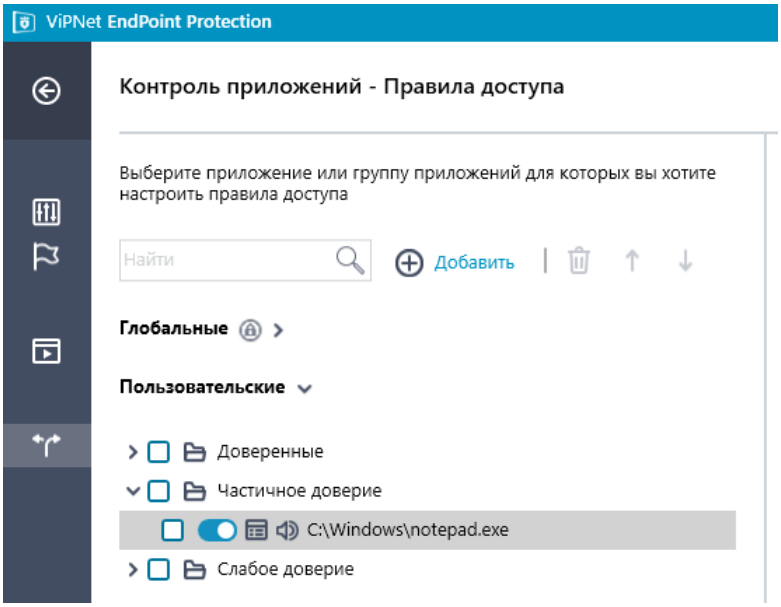


Рисунок 106. Настройка правил доступа приложения пользовательского белого списка

4 На панели справа выберите нужную вкладку (**Файлы**, **Реестр**, **Процессы**, **Командная строка**).

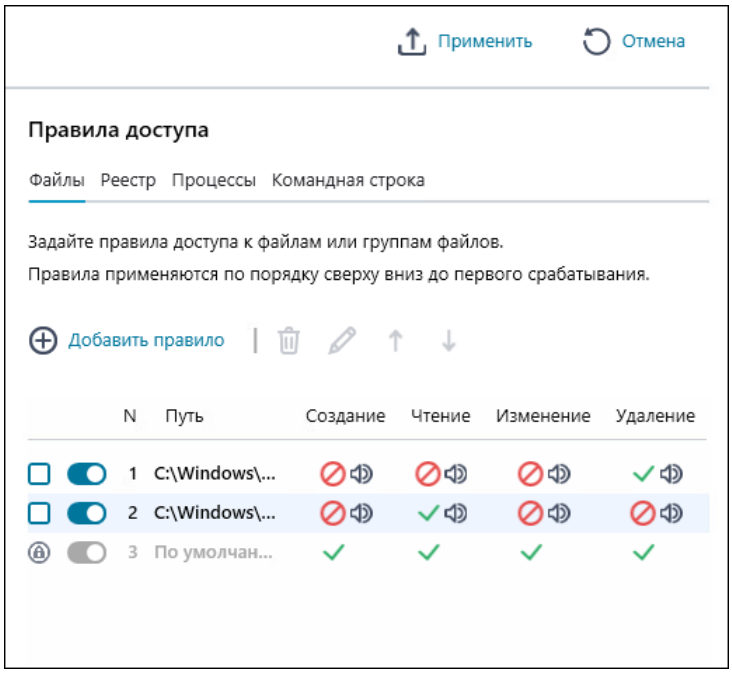


Рисунок 107. Панель справа «Правила доступа»

5 Нажмите ⊕ **Добавить правило** и выполните шаги сценария добавления правил доступа приложения, как на ViPNet EPP Сервер (см. Управление активностью приложений).

6 Чтобы изменить правило доступа приложения, на панели справа дважды щелкните строку с названием правила или нажмите ✎.

6.1 Внесите необходимые изменения в параметры правила.

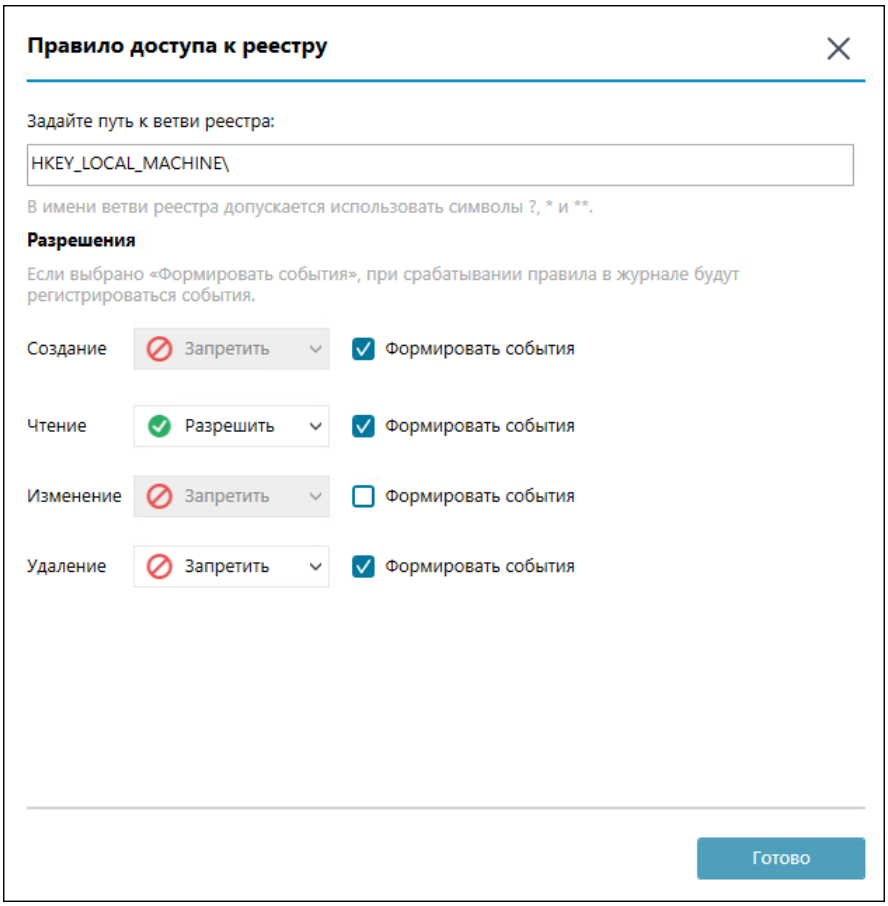


Рисунок 108. Изменение параметров правила доступа приложения

6.2 Нажмите **Готово**.

7 Нажмите **Применить**.

Изменение порядка применения правил доступа для приложений

Чтобы изменить порядок применения правил запуска приложений или групп приложений в пользовательском белом списке:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **Правила доступа**.

3 Раскройте список **Пользовательские** и выберите флажками правила или группы, порядок применения которых вы хотите изменить.

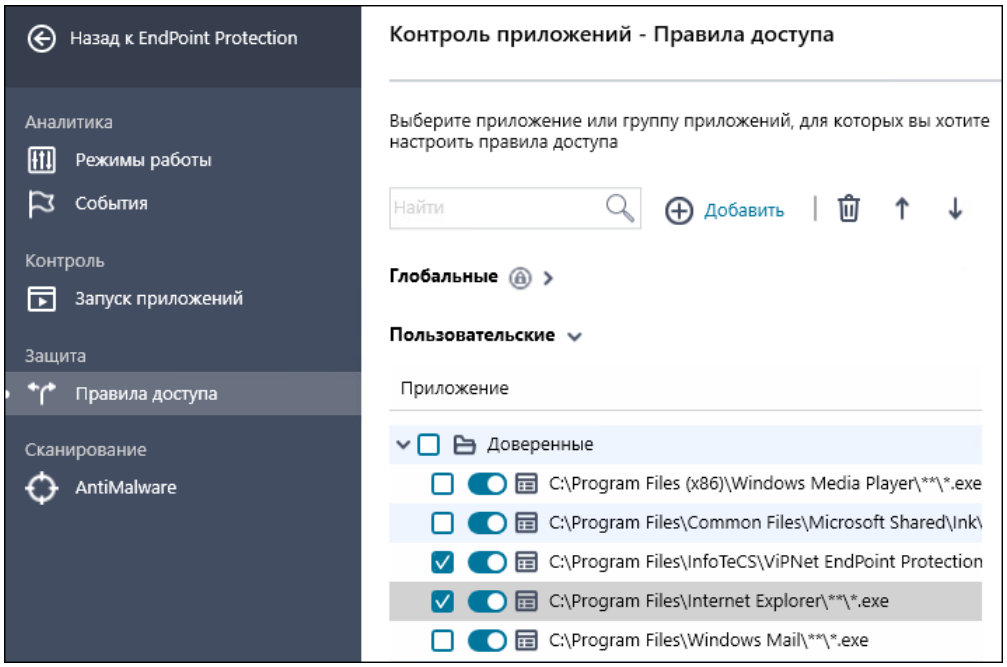


Рисунок 109. Изменение порядка применения приложений и групп приложений пользовательского белого списка

4 Нажмите ↑ или ↓ для перемещения отмеченных объектов в списке. Вы можете перемещать или группы, или приложения в пределах одной группы.

5 Нажмите **Применить**.

Правила доступа приложения применяются сверху вниз до первого срабатывания. Если ни одно из правил доступа не сработало, применяются правила доступа по умолчанию для группы этого приложения. Чтобы изменить порядок применения правил доступа приложения:

1 Раскройте список **Пользовательские**, далее группу приложения и выберите приложение.

2 На панели справа перейдите на нужную вкладку (**Файлы**, **Реестр**, **Процессы**, **Командная строка**) и выберите флажками правила, порядок применения которых вы хотите изменить.

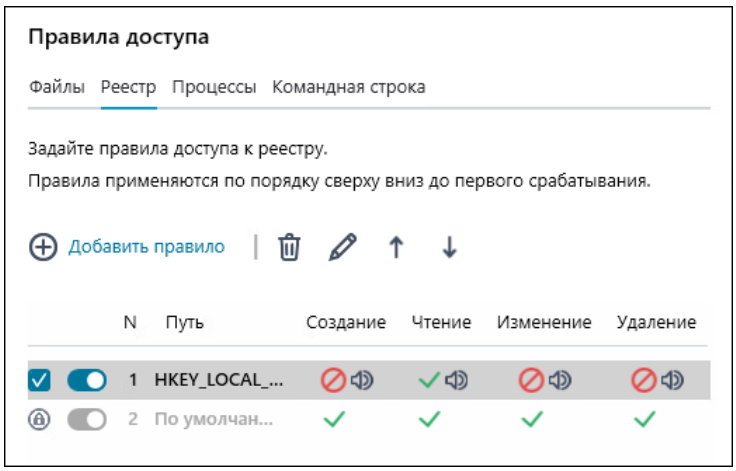


Рисунок 110. Панель справа «Правила доступа»

3 Нажмите ↑ или ↓ для перемещения выбранных правил в списке.

4 При необходимости повторите шаги 2 и 3 для правил доступа в других вкладках.

5 Нажмите **Применить**.

Настройка контроля обращений к сетевым папкам

Настройка контроля обращений к сетевым папкам доступна только в автономном ViPNet EPP Агент.

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 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **Общие настройки**.

3 Выключите **Контролировать обращения к сетевым папкам**.

Чтобы в ViPNet EPP Агент сетевые папки снова контролировались, включите **Контролировать обращения к сетевым папкам**.

Настройка правил доступа по умолчанию для группы приложений

Чтобы изменить правила доступа по умолчанию для группы приложений пользовательского белого списка:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **Правила доступа**.

3 Раскройте список **Пользовательские** и щелкните строку с названием группы приложений, правила доступа по умолчанию которой вы хотите изменить.

Примечание. Изменить правила доступа по умолчанию группы **Доверенные** невозможно.

---

4 На панели справа перейдите на нужную вкладку (**Файлы**, **Реестр**, **Процессы**, **Командная строка**).

5 Нажмите и установите параметры правила по аналогии с шагами сценария добавления правил доступа, как на ViPNet EPP Сервер (см. Управление активностью приложений) для выбранного объекта.

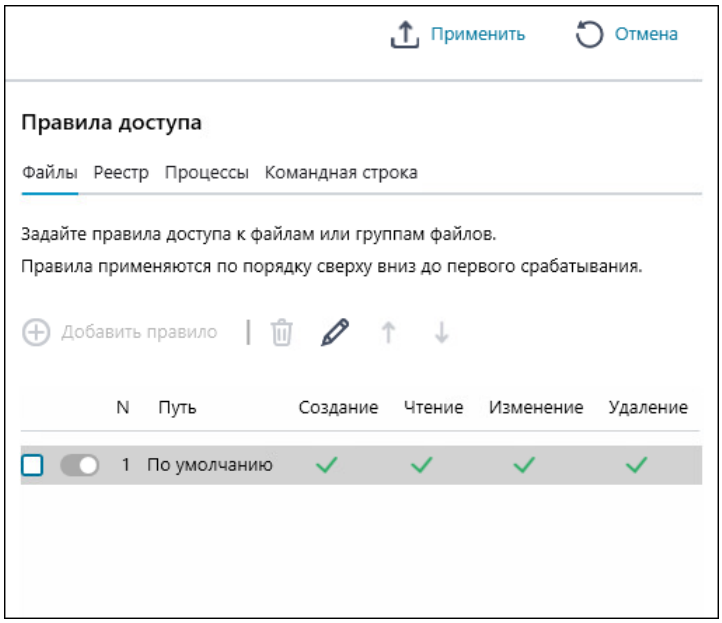


Рисунок 111. Панель справа «Правила доступа» группы приложений по умолчанию

6 Нажмите **Применить**.

Сканирование AntiMalware

Возможность настройки параметров сканирования AntiMalware зависит от способа работы ViPNet EPP Агент:

- При работе под управлением ViPNet EPP Сервер (см. Подключение защищаемых узлов) параметры сканирования AntiMalware настраиваются на сервере (см. Сканирование AntiMalware) и передаются в составе базы правил на ViPNet EPP Агент. В ViPNet EPP Агент изменение параметров сканирования недоступно.
- При автономной работе ViPNet EPP Агент доступна настройка параметров сканирования AntiMalware.

Сканирование будет выполнено в соответствии с параметрами, заданными для защищаемого узла. Сканирование будет недоступно, если контроль приложений отключен (см. Выбор режима работы контроля приложений).

Чтобы настроить параметры сканирования:

1 Подключитесь к автономному ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **AntiMalware**.

3 На панели вверху нажмите **Настройки** и настройте параметры сканирования (см. Просмотр и настройка параметров сканирования) и расписание автоматического сканирования (см. Настройка расписания автоматического запуска сканирования) аналогично настройкам в ViPNet EPP Сервер.

Чтобы запустить сканирование AntiMalware:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **AntiMalware**.

3 На панели вверху нажмите **Запустить сканирование**.

4 Выберите тип сканирования: **Полное**, **Быстрое** или **Выборочное**.

5 При выборе типа сканирования **Выборочное** укажите файлы или папки для сканирования с помощью кнопок добавки файлов или папок.

6 Нажмите **Запустить сканирование**. Полное сканирование может занять продолжительное время.

В результате сканирования будет создан отчет (см. Просмотр и обработка результатов сканирования AntiMalware).

В некоторых случаях, например при высокой загрузке процессора компьютера ViPNet EPP Агент или для изменения варианта сканирования, процесс сканирования требуется остановить. Чтобы остановить сканирование, на панели сверху нажмите одноименную кнопку.

Просмотр и обработка результатов сканирования AntiMalware

Результаты сканирования сохраняются в ViPNet EPP Агент в виде отчетов. Сохраняются отчеты:

- запущенные в ViPNet EPP Агент;
- запущенные в ViPNet EPP Сервер для ViPNet EPP Агент (только для ViPNet EPP Агент под управлением ViPNet EPP Сервер);
- запущенные автоматически по расписанию.

Администратору доступен просмотр списков отчетов и подробной информации об отчете. Доступны только сто последних отчетов. Чтобы заблокировать потенциально опасные исполняемые файлы, доступно добавление их в пользовательский черный список контроля приложений. Добавить в черный список можно только файлы *.exe.

Чтобы просмотреть отчеты с результатами сканирования AntiMalware:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.

2 Выберите **Контроль приложений** > **AntiMalware**.

Появится список всех отчетов. Просмотр отчетов происходит таким же образом, как и на ViPNet EPP Сервер (см. Просмотр и обработка результатов сканирования).

Чтобы поместить потенциально опасные файлы `*.exe` в пользовательский черный список контроля приложений:

1 Убедитесь, что вы подключились к ViPNet EPP Агент с полномочиями администратора агента.

2 На панели справа с подробной информацией об отчете выберите файлы флажками и нажмите .

3 Подтвердите добавление в черный список.

В результате строки с файлами будут выделены **жирным шрифтом** и отмечены значком ★, а файлы добавятся в пользовательский черный список контроля приложений и для них создадутся блокирующие правила (см. Просмотр списков контроля приложений).

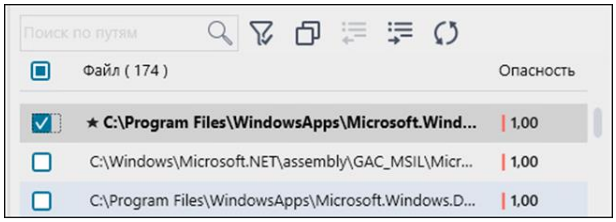


Рисунок 112. Приложение добавлено в пользовательский черный список

Примечание. Если добавленный файл временно исключить из черного списка контроля приложений (см. Управление пользовательскими списками приложений), в отчете AntiMalware строка с этим файлом так и останется выделенной **жирным шрифтом** и отмеченной значком ★.

Чтобы обновить информацию о файлах в черном списке, нажмите .

Чтобы удалить файлы из черного списка выберите их флажками и нажмите . Подтвердите удаление. Вышеперечисленные отметки черного списка будут сняты.

Чтобы удалить отчеты, например устаревшие, выберите их флажками и на панели вверху нажмите . Подтвердите удаление.

Журнал событий контроля приложений

События информационной безопасности, идентифицированные модулем контроля приложений ViPNet EPP Агент, регистрируются в журнале событий контроля приложений ViPNet EPP Агент. К ним относятся события категорий:

- Запуск приложений.
- Защита файлов.
- Защита реестра.
- Защита процессов.
- Контроль параметров командной строки.

Примечание. События категорий защиты файлов, реестра, процессов, а также контроля командной строки, регистрируются в журнале событий контроля приложений ViPNet EPP Агент в том случае, если в соответствующих правилах доступа установлен флажок **Формировать события**.

Чтобы просмотреть журнал событий контроля приложений ViPNet EPP Агент:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.

2 Выберите **Контроль приложений** > **События**.

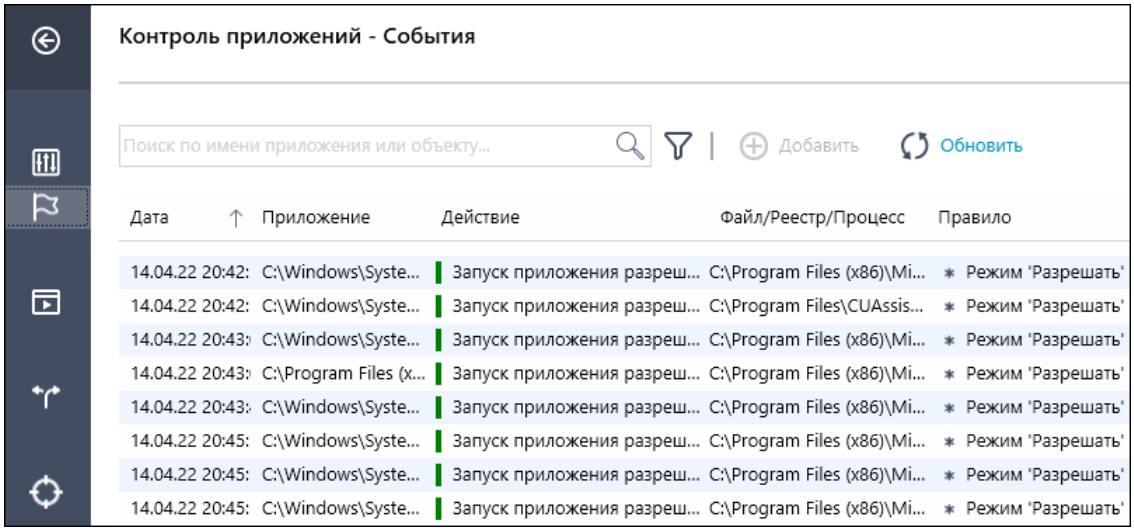


Рисунок 113. Журнал событий контроля приложений ViPNet EPP Агент

Каждая запись о событии в журнале содержит:

- **Дата** — дата и время события.
- **Приложение** — приложение, вызвавшее событие.

- **Действие** — статус действия (— разрешить или — запретить) и вид действия с приложением.
- **Файл/Реестр/Процесс** — объект ОС Windows, с которым связано сработавшее правило доступа.
- **Правило** — сработавшее правило доступа, белый или черный списки, или режим работы контроля приложений:
  - — режим работы контроля приложений ViPNet EPP Агент.
  - — запуск приложения из белого или черного списков.
  - — правило доступа к файлам.
  - — правило доступа к реестру.
  - — правило доступа к процессам.
  - — правило доступа к командной строке.

  Для событий самозащиты (см. Настройка самозащиты) этом столбце ничего не отображается.

3 Чтобы в списке событий найти определенное событие, в поле поиска введите часть любого параметра события (кроме даты) или параметр целиком и нажмите .

4 Чтобы отфильтровать события по параметрам, используйте фильтр:

4.1 Нажмите и задайте параметры фильтрации:

- Раскройте список **Категория** и выберите флажками нужные категории событий.
- Выберите в списке **Действие** статус: **Любое**, **Разрешить**, **Запретить**.
- Раскройте список **Вид действия** и выберите флажками нужные виды действия с приложениями.

- Выберите в календаре временной интервал отображаемых событий.

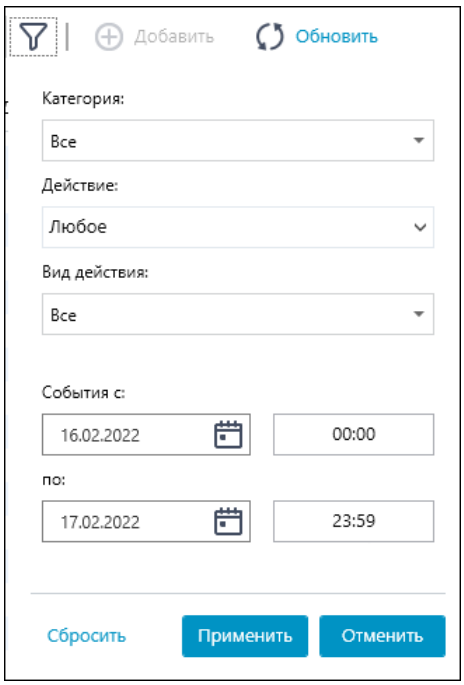


Рисунок 114. Параметры фильтрации журнала событий контроля приложений ViPNet EPP Агент

4.2 Нажмите **Применить**.

На странице **Контроль приложений — События** будут отображены события с заданными параметрами фильтрации журнала.

Чтобы из журнала событий контроля приложений ViPNet EPP Агент добавить приложение в пользовательские черный или белый списки:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Контроль приложений** > **События**.

3 Выберите нужное событие и нажмите **Добавить**.

4 Внесите приложение в группу пользовательского белого или черного списка (см. Управление пользовательскими списками приложений).

Приложение будет внесено в соответствующий пользовательский черный или белый список на странице **Контроль приложений — Запуск приложений**.

Для удобства работы администратора агента активность приложений, не входящих в белый и черный списки, регистрируется в списке **Прочие** контроля приложений ViPNet EPP Агент. Вы можете просмотреть этот список и при необходимости добавить приложение в пользовательские черный или белый списки (см. Управление пользовательскими списками приложений).

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
```

Выбор режима работы

По умолчанию режим работы обнаружения и предотвращения вторжений ViPNet EPP Агент (см. Обнаружение и предотвращение вторжений) устанавливается из базы правил. Для учета особенностей предотвращения вторжений на защищаемом узле режим работы можно изменить:

1 Подключитесь к ViPNet EPP Агент с любыми полномочиями.

2 Выберите **Обнаружение и предотвращение вторжений** > **Режимы работы**.

3 В разделе **Режим работы** выберите нужный режим.

Выбранный режим будет отмечен .

При выборе режима **Отключено** правила фильтрации модуля HIPS (сетевые правила HIPS, веб-фильтры, правила бесфайловых атак) применяться не будут.

Просмотр и настройка правил 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 (см. Настройка правил HIDS). В ViPNet EPP Агент вы можете только просматривать статус применения групп правил HIDS.
- При автономной работе ViPNet EPP Агент доступна локальная настройка правил HIDS.

Чтобы просмотреть или настроить правила HIDS:

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 и предотвращение вторжений** > **HIDS**.

3 В зависимости от способа работы ViPNet EPP Агент:

   3.1 Посмотрите статусы применения групп правил HIDS. Группы правил HIDS, отмеченные флажками, применяются ViPNet EPP Агент для обнаружения вторжений на защищаемом узле.

   3.2 Настройте правила HIDS аналогично настройкам в ViPNet EPP Сервер (см. Настройка правил HIDS).

Просмотр и настройка сетевых правил HIPS

Сетевые правила HIPS применяются ViPNet EPP Агент для предотвращения вторжений. 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 базы правил на ViPNet EPP Агент (см. Настройка правил HIDS). В ViPNet EPP Агент вы можете только просматривать список правил HIPS.

- При автономной работе ViPNet EPP Агент доступна настройка правил HIPS.

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 **Обнаружение и предотвращение вторжений** и в разделе **Сетевые правила HIPS** выберите режим работы:

   - **Усиленный**.
   - **Базовый**.
   - **Минимальный**.

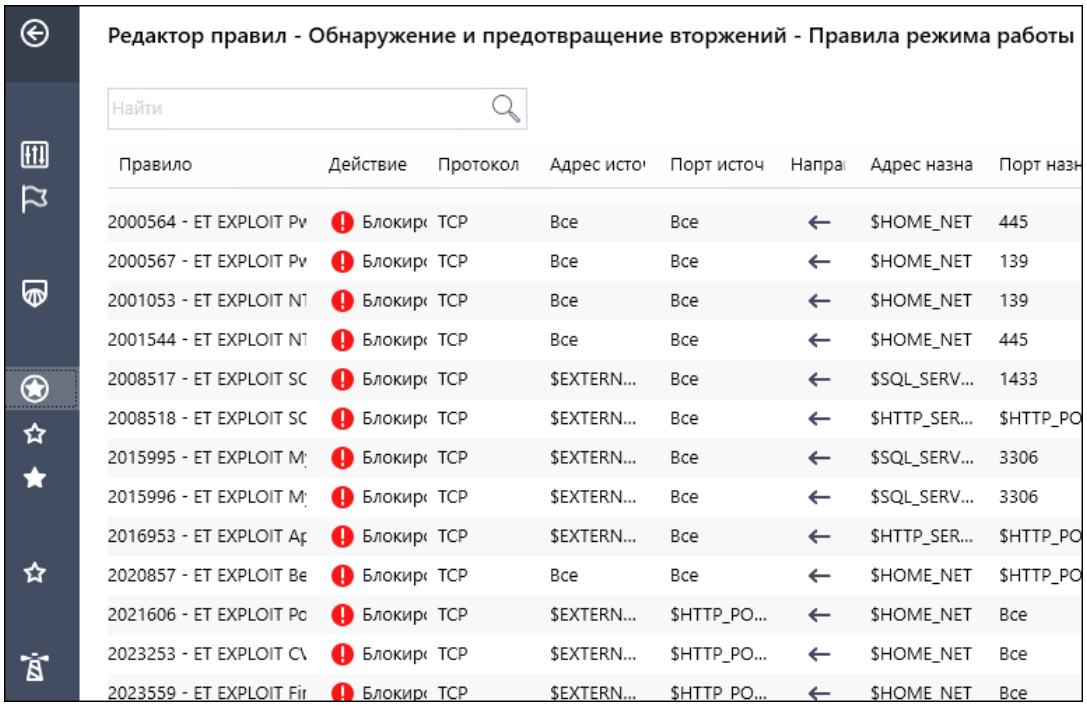


Рисунок 115. Набор сетевых правил HIPS выбранного режима работы

3 В зависимости от способа работы ViPNet EPP Агент:

3.1 Посмотрите информацию о правилах HIPS. В списке для каждого правила отображаются параметры: название, действие (**Блокировать** или **Уведомлять**) протокол, адреса и порты источника и назначения, направление.

3.2 При автономной работе ViPNet EPP Агент, настройте правила HIPS аналогично настройкам в ViPNet EPP Сервер (см. Блокирование сетевой активности). Нажмите **Применить**.

Просмотр и настройка веб-фильтров

Веб-фильтры применяются в ViPNet EPP Агент для контроля доступа к веб-ресурсам (см. Блокировка доступа к вредоносным веб-ресурсам). Возможность настройки веб-фильтров зависит от способа работы ViPNet EPP Агент:

- При работе под управлением ViPNet EPP Сервер (см. Подключение защищаемых узлов) веб-фильтры настраиваются на сервере и передаются в составе базы правил на ViPNet EPP Агент. В ViPNet EPP Агент вы можете только просматривать веб-фильтры.
- При автономной работе ViPNet EPP Агент доступна локальная настройка веб-фильтров.

Чтобы просмотреть или настроить веб-фильтры:

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 и предотвращение вторжений** > **Веб-фильтры**.
3 В зависимости от способа работы ViPNet EPP Агент просмотрите или настройте веб-фильтры аналогично настройке фильтров в ViPNet EPP Сервер. Нажмите **Применить**.

Управление пользовательскими правилами HIPS для бесфайловых атак

Возможности настройки правил HIPS для бесфайловых атак зависит от способа работы ViPNet EPP Агент:

- При работе под управлением ViPNet EPP Сервер (см. Подключение защищаемых узлов) правила HIPS для бесфайловых атак настраиваются на сервере и передаются в составе базы правил на ViPNet EPP Агент (см. Настройка правил HIPS). В ViPNet EPP Агент вы можете только просматривать список полученных правил. Для учета особенностей предотвращения бесфайловых атак типа Keylogging в ViPNet EPP Агент вы можете добавить новые пользовательские правила HIPS для бесфайловых атак, изменить пользовательские правила, изменить порядок их применения, временно отключить или удалить ненужные пользовательские правила. Изменение действия правил бесфайловых атак типа Hollowing и Doppelganging, а также правил предотвращения получения адресов функций в модулях ядра Windows, недоступны.
- При автономной работе ViPNet EPP Агент доступны настройки всех правил HIPS для бесфайловых атак.

После применения на защищаемом узле базы правил (политики безопасности) с настройками бесфайловых атак, чтобы изменения вступили в действие, необходимо перезагрузить защищаемый узел в следующих случаях:

- Если было включено хотя бы одно правило для бесфайловых атак в разделе **Обнаружение и предотвращение вторжений** > **Бесфайловые атаки** или **HIDS**, 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 пользовательские правила HIPS для бесфайловых атак:

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 и предотвращение вторжений** > **Бесфайловые атаки**.
3. На вкладке **Пользовательские** добавьте, измените правило HIPS для бесфайловых атак типа Keylogging, измените порядок применения правил, временно отключите или удалите ненужные правила аналогично настройкам правил в ViPNet EPP Сервер (см. Блокирование бесфайловых атак типа Keylogging).
4. Чтобы настроить правила бесфайловых атак типа Hollowing и Doppelganging (см. Блокирование бесфайловых атак типа Hollowing и Doppelganging), правила предотвращения получения адресов функций в модулях ядра Windows (см. Блокирование бесфайловых атак с целью получения адресов функций в модулях ядра ОС Windows) выполните действия аналогично настройкам этих правил в ViPNet EPP Сервер.
5. Нажмите **Применить**.

Политика аудита

Политики аудита входят в состав базы правил и применяются ViPNet EPP Агент для определения типов событий ОС Windows, которые будут записываться в журнал безопасности Windows на защищаемом узле.

Политики аудита доступны для настройки только в автономном ViPNet EPP Агент. В ViPNet EPP Агент, работающем под управлением ViPNet EPP Сервер, доступен только просмотр настроек.

Чтобы настроить или просмотреть политики аудита:

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 и предотвращение вторжений** > **Политика аудита**.

3 В зависимости от способа работы ViPNet EPP Агент настройте или просмотрите политики аналогично настройкам в ViPNet EPP Сервер (см. Настройка политик аудита), выбирая вкладки категорий:

- **Аутентификация** — политики отслеживания событий аутентификации пользователей в ОС Windows (см. Политика аудита аутентификации пользователей в ОС Windows).
- **Реестр** — политики отслеживания изменений в реестре (см. Политика аудита изменений в реестре).
- **Файловая система** — политики отслеживания изменений в файловой системе (см. Политика аудита изменений в файловой системе).
- **Управление учетными записями** — политики аудита управления учетными записями (см. Политика аудита управления учетными записями).
- **Прочие** — дополнительные политики аудита (см. Другие политики аудита).

Журнал событий обнаружения и предотвращения вторжений

События информационной безопасности, идентифицированные модулем обнаружения и предотвращения вторжений ViPNet EPP Агент, регистрируются в журнале событий обнаружения и предотвращения вторжений ViPNet EPP Агент.

Чтобы просмотреть журнал событий обнаружения и предотвращения вторжений ViPNet EPP Агент и выполнить возможные действия:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора или аудитора агента.

2 Выберите **Обнаружение и предотвращение вторжений** > **События**.

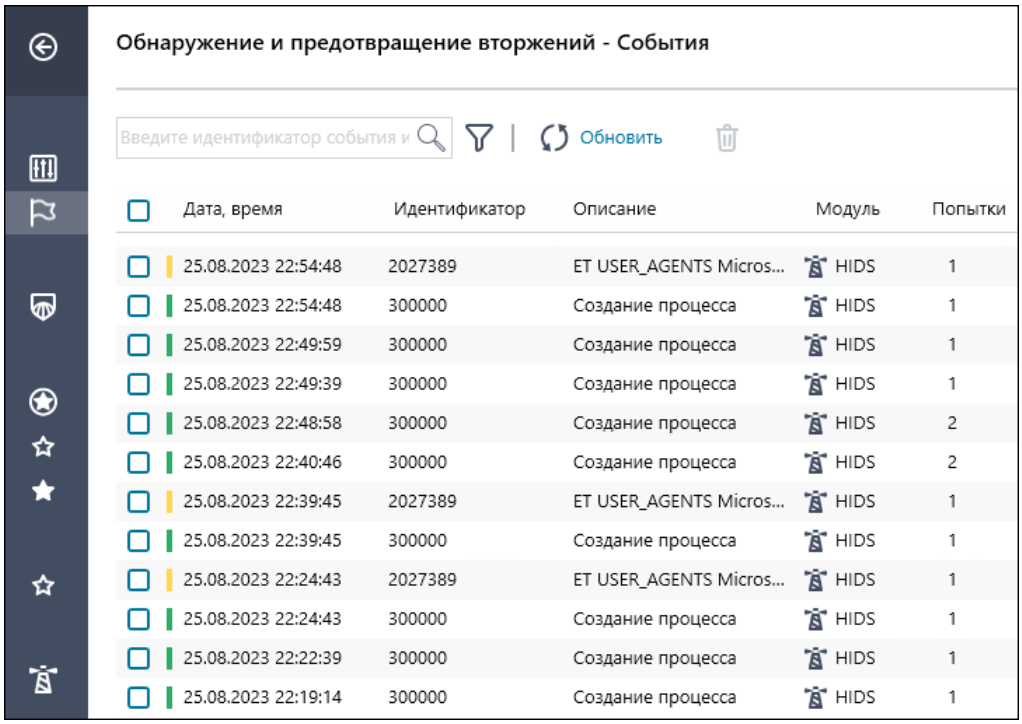


Рисунок 116. Журнал событий обнаружения и предотвращения вторжений ViPNet EPP Агент

Каждая запись о событии в журнале содержит:

- Цветовой индикатор уровня события:
  - — критическое.
  - — опасное.
  - — важное.
  - — информационное.
- **Дата и время** — дата и время обнаружения.
- **Идентификатор** — идентификатор правила, при срабатывании которого зарегистрировано событие (см. Типы и идентификаторы правил).
- **Описание** — описание события.
- **Модуль** — модуль, в котором сработало правило:
  - HIDS — обнаружение вторжений.
  - HIPS — предотвращение вторжений.
- **Попытки** — количество повторений события на устройстве в течение заданного периода опроса.

Примечание. При работе ViPNet EPP Агент под управлением ViPNet EPP Сервер события информационной безопасности защищаемого узла пересылаются на ViPNet EPP Сервер. До тех пор, пока событие не доставлено на ViPNet EPP Сервер, строка с описанием события в журнале будет выделена **жирным шрифтом**.

3 Чтобы просмотреть сведения о событии, выберите строку с нужным событием в журнале — на панели справа на вкладке **Сработавшее правило** будут отображены сведения о правиле.

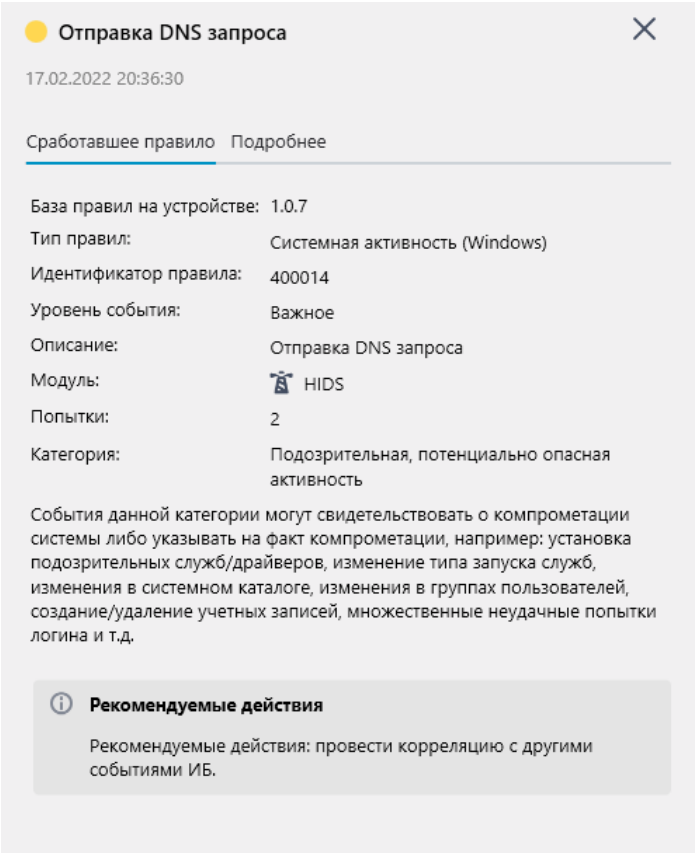


Рисунок 117. Вкладка «Сработавшее правило» дополнительной панели

4 Для просмотра подробных сведений о событии выберите вкладку **Подробнее**. По умолчанию отображаются только важные сведения о событии в удобном для чтения виде.

- Для просмотра полных сведений выключите **Отображать только важную информацию о событии**.
- Чтобы скопировать их в буфер обмена, нажмите .

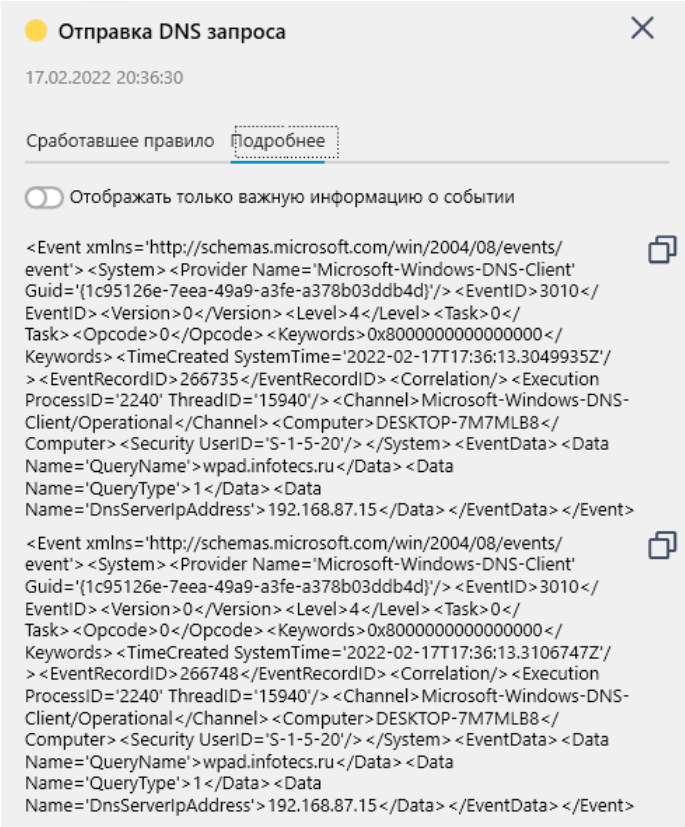


Рисунок 118. Подробные сведения о событии

5 Для поиска событий в журнале используйте фильтр:

5.1 Нажмите  и задайте параметры фильтрации:

- Выберите тип правил, с помощью которых были идентифицированы события.
- Выберите модули, события которых нужно отобразить.
- Выберите **Только не доставленные на сервер**, чтобы отобразить такие события (доступно только при работе ViPNet EPP Агент под управлением ViPNet EPP Сервер).
- Выберите уровни, события которых нужно отобразить.
- Укажите промежуток времени, в течение которого происходили искомые события.

5.2 Нажмите **Применить**.

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).

Чтобы настроить критерии обнаружения аномалий:

1. Подключитесь к ViPNet EPP Агент с полномочиями администратора агента или аудитора агента (только для просмотра).
2. Выберите  **Критерии обнаружения аномалий**.
3. Для добавления нового критерия обнаружения аномалий на панели вверху нажмите  **Создать** и выполните действия аналогично настройкам в ViPNet EPP Сервер (см. Настройка критериев обнаружения аномалий).

Работа с журналами

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.
  - Журнал событий контроля приложений.
  - Журнал событий обнаружения и предотвращения вторжений.

При переполнении журналов (журнала событий, журнал контроля приложений, 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**.

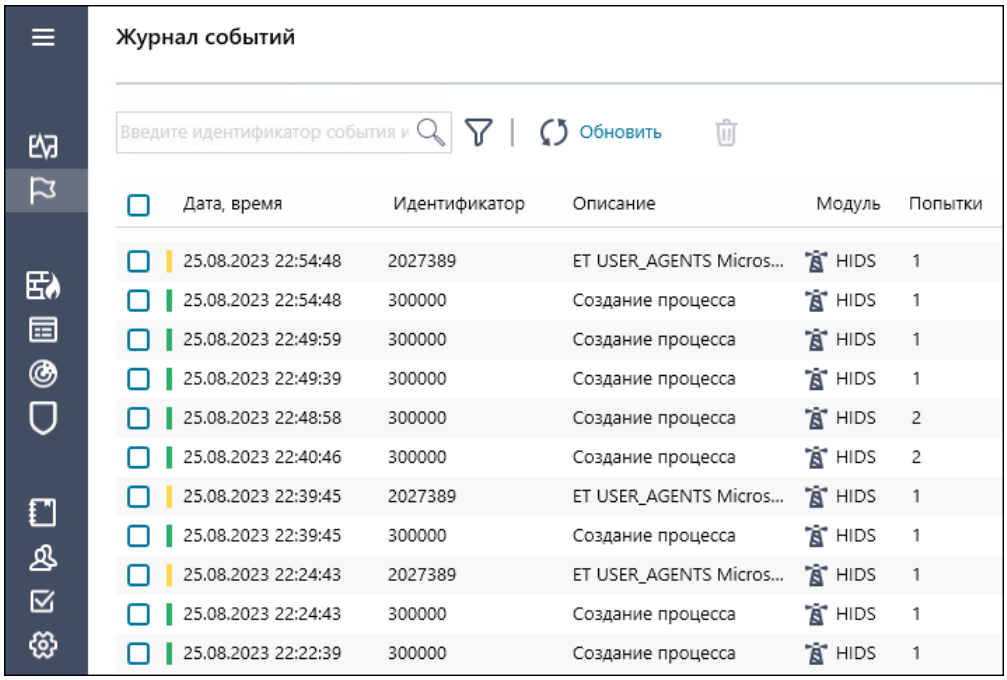


Рисунок 119. Журнал событий ViPNet EPP Агент

Примечание. По умолчанию отображается информация обо всех зарегистрированных событиях за последние сутки.

Каждая запись о событии в журнале содержит:

- Цветовой индикатор уровня события:
  - — критическое.
  - — опасное.
  - — важное.
  - — информационное.
- **Дата и время** — дата и время обнаружения.
- **Модуль** — модуль, в котором сработало правило:
  - PFW — персональный межсетевой экран.
  - AppC — контроль приложений.
  - HIDS — обнаружение вторжений.
  - HIPS — предотвращение вторжений.
- **Идентификатор** — идентификатор правила, при срабатывании которого зарегистрировано событие (см. Типы и идентификаторы правил).
- **Описание** — описание события.

- **Попытки** — количество повторений события на устройстве в течение заданного периода опроса. Повторные события определяются по одинаковому идентификатору сработавшего правила.

Примечание. При работе ViPNet EPP Агент под управлением ViPNet EPP Сервер события информационной безопасности защищаемого узла пересылаются на ViPNet EPP Сервер. До тех пор, пока событие не доставлено на ViPNet EPP Сервер, строка с описанием события в журнале будет выделена **жирным шрифтом**.

---

3 Чтобы просмотреть сведения о событии, дважды щелкните строку с событием в журнале — на панели справа на вкладке **Сработавшее правило** будут отображены сведения о сработавшем правиле и количестве зафиксированных повторений события в течение заданного периода опроса (**Попытки**). Для ряда критических и опасных событий будут указаны рекомендуемые действия в связи возникновением события.

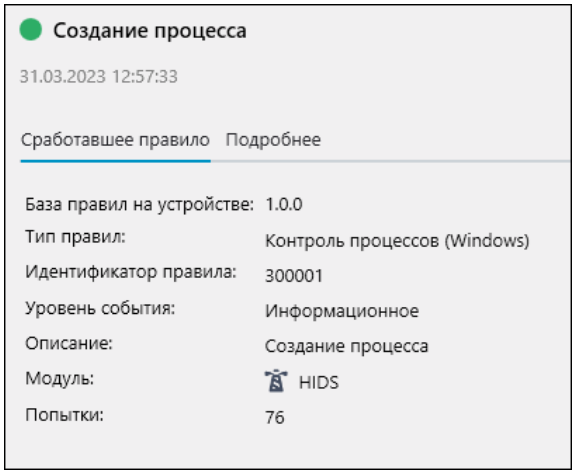


Рисунок 120. Просмотр сведений о событии

4 Для просмотра подробных сведений о событии перейдите на вкладку **Подробнее**. По умолчанию отображаются только важные сведения о событии в удобном для чтения виде. Для просмотра полных сведений выключите **Отображать только важную информацию о событии**.

Если было зарегистрировано несколько повторений события с одинаковым идентификатором, на вкладке **Подробнее** будут отображены только события с уникальными полными сведениями о событии. Например, событие с идентификатором правила `300001` произошло 5 раз, на вкладке **Сработавшее правило** отображается 5 попыток. У двух событий в полных сведениях содержится `ABC`, а у трех событий — `XYZ`. В этом случае на вкладке **Подробнее** будет отображена информация о двух событиях с идентификатором `300001`.

Чтобы скопировать сведения в буфер обмена, нажмите .

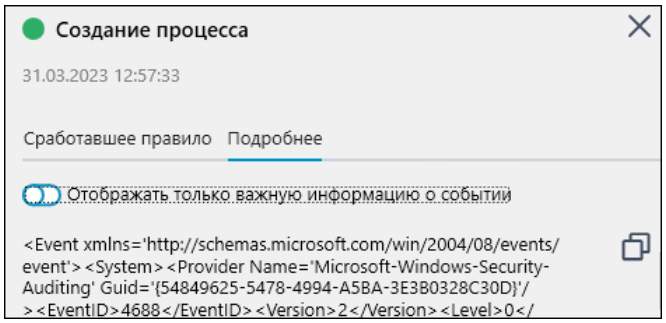


Рисунок 121. Подробные сведения о событии

5 Для поиска событий в журнале используйте фильтр:

5.1 Нажмите и задайте параметры фильтрации:

- Выберите тип правил, с помощью которых были идентифицированы события.
- Выберите события модуля, которые нужно посмотреть.
- Чтобы отобразить события, зарегистрированные заданными критериями аномалий, выберите **Только аномальные события** (доступно только для автономного ViPNet EPP Агент).
- Выберите **Только события, не доставленные на сервер**, чтобы отобразить такие события (доступно только при работе ViPNet EPP Агент под управлением ViPNet EPP Сервер).
- Выберите флажками уровни, события которых нужно отобразить.
- Укажите промежуток времени, в течение которого происходили искомые события.

5.2 Нажмите **Применить**.

6 Чтобы удалить события, выберите флажками события, на панели вверху нажмите и подтвердите удаление.

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 **Аудит**.

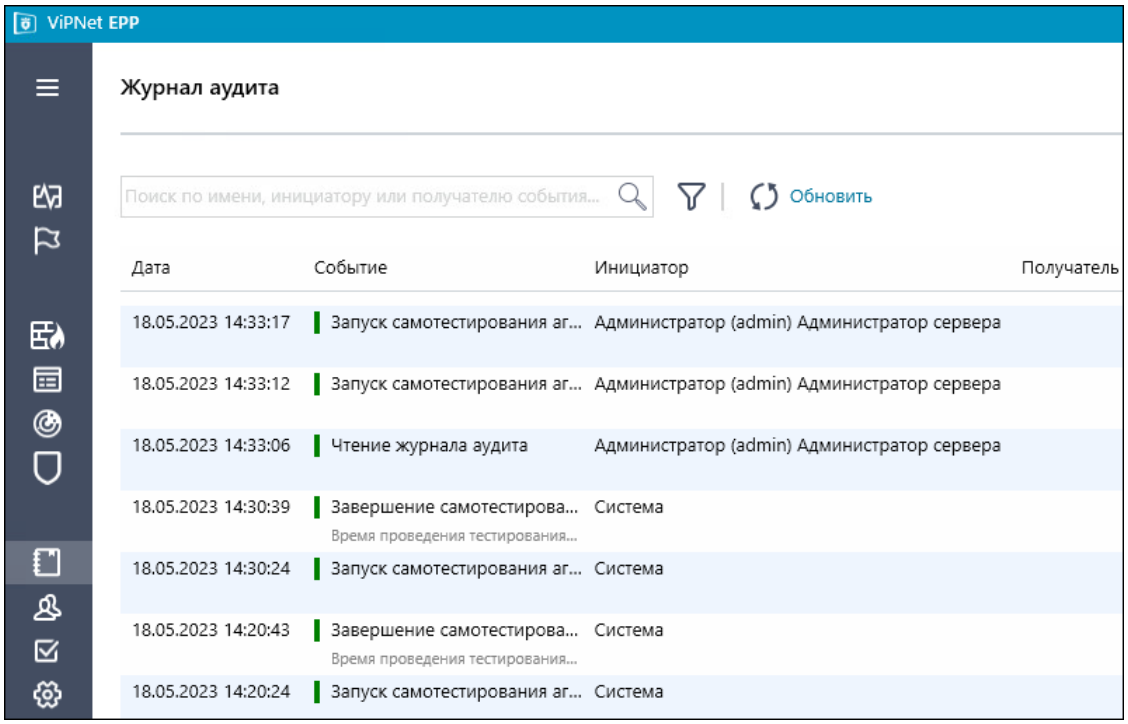


Рисунок 122. Журнал аудита ViPNet EPP Агент

Каждая запись о событии в журнале содержит:

- **Дата** — дата и время, когда событие произошло.
- **Событие** — цветовой индикатор (— действие, вызвавшее событие успешно или — не успешно) и описание события.
- **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 Net Sensor.
  - Администраторы, аудиторы и пользователи ViPNet EPP Агент. Для некоторых событий поле может быть пустым.

3 Для поиска событий в журнале используйте фильтр:

3.1 Нажмите  и задайте параметры фильтрации

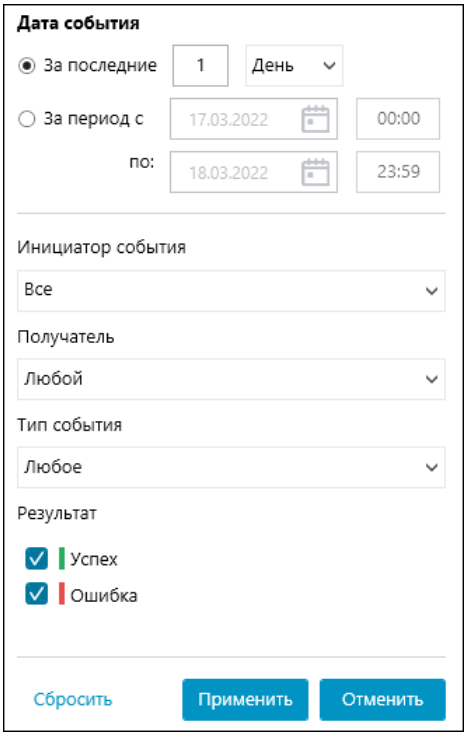


Рисунок 123. Параметры фильтрации журнала аудита ViPNet EPP Агент

3.2 Нажмите **Применить**.

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.
- Функционирование EPP агента.
- Операции с учетными записями.
- Управление правилами обнаружения аномалий.
- Операции с журналами.
- Операции с базой правил.
- Управление правилами модулей.
- Установка режимов работы модулей.
- Блокировка трафика.
- Лицензия.
- Регистрируются всегда — события самотестирования, очистки журналов, восстановления работоспособности после нарушения целостности журналов, восстановления базы данных и таблиц после повреждений, создания резервной копии поврежденной базы данных.

Вы можете отключить регистрацию событий одного, нескольких или сразу всех типов, кроме типа **Регистрируются всегда**.

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 **Регистрируемый тип событий журнала аудита**:
   - **3.1** Чтобы просмотреть список событий, раскройте список с названием типа событий.
   - **3.2** Снимите флажки типов событий, которые не должны регистрироваться в журнале.
   - **3.3** 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. Нажмите **Сохранить**.

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. Для поиска учетных записей на основе их ролей (администратор, аудитор и пользователь) используйте фильтр:
   - **3.1** Нажмите .
   - **3.2** Выберите роль учетных записей.
   - **3.3** Нажмите **Применить**.
4. Для поиска учетных записей по имени в поле поиска введите часть имени или имя целиком и нажмите .
5. Создание, изменение и удаление учетных записей ViPNet EPP Агент выполняется аналогично операциям с учетными записями в ViPNet EPP Сервер (см. Управление учетными записями).

Просмотр и настройка параметров работы

После установки параметры работы ViPNet EPP Агент заданы по умолчанию. Возможность настройки параметров работы зависит от способа работы ViPNet EPP Агент:

- При работе под управлением ViPNet EPP Сервер (см. Подключение защищаемых узлов) в ViPNet EPP Агент передаются глобальные параметры работы и хранения журналов, заданные на сервере (см. Настройка параметров системы). 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), настроить уведомления. 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 аудита, журнала трафика, журнала контроля приложений) 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.

Информация о переполнении журнала и удалении событий фиксируется в журнале 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. Чтобы на защищаемом узле в центре уведомлений ОС Windows появлялись уведомления о срабатывании блокирующих правил контроля приложений и веб-фильтров ViPNet EPP, убедитесь что включены  **Уведомления**.
5. При работе под управлением ViPNet EPP Сервер, настройте адрес и порт ViPNet EPP Сервер (см. Изменение адреса ViPNet EPP Сервер) и посмотрите настройки остальных параметров.
6. При работе в автономном режиме, посмотрите и настройте остальные параметры аналогично настройкам в ViPNet EPP Сервер на вкладке **Параметры агента** (см. Настройка параметров системы).

Перевод автономного ViPNet EPP Агент под управление ViPNet EPP Сервер

Если ViPNet EPP Агент 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 базы правил в ViPNet EPP Агент будут заменены данными с ViPNet EPP Сервер:

- Лицензия (см. Лицензирование).
- Параметры агента (см. Настройка параметров системы).
- Фильтры политик безопасности, глобальные справочники.
- Все правила HIDS.
- Все глобальные правила контроля приложений.
- Критерии обнаружения аномалий.
- Режимы работы.
- Политики аудита.
- Все правила HIPS, за исключением пользовательских правил для бесфайловых атак типа Keylogging.

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 Выберите **Работа под управлением сервера** и укажите адрес сервера и порт (по умолчанию — 25010).

4 Нажмите **Сохранить**.

5 Подтвердите необходимость переключения.

В результате переход ViPNet EPP Агент под управление ViPNet EPP Сервер будет выполнен после обработки запроса на подключение на сервере и получения от сервера базы правил.

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 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. Укажите новые значения адреса сервера и номера порта.
4. Нажмите **Сохранить**.
5. Перезагрузите компьютер защищаемого узла.

Если в вашей корпоративной сети используется служба каталогов Active Directory, вы можете изменить адрес ViPNet EPP Сервер в настройках ViPNet EPP Агент защищаемых узлов с помощью групповых политик (см. Установка ViPNet EPP Агент с помощью групповых политик Active Directory).

Настройка самозащиты

В ViPNet EPP Агент реализован механизм самозащиты, который позволяет защитить от случайного или намеренного удаления и изменения важные файлы, процессы и службы ViPNet EPP Агент, а также значения в системном реестре, отвечающие за функционирование ПО. По умолчанию самозащита включена. Попытки изменения защищаемых объектов фиксируются в журнале событий контроля приложений ViPNet EPP Агент (см. Журнал событий контроля приложений).

Если администратору потребуется, например, перезапустить службу ViPNet EPP Агент, необходимо временно отключить самозащиту. Информация об отключении или включении механизма самозащиты регистрируется в журнале аудита ViPNet EPP Агент (см. Журнал аудита).

Чтобы отключить самозащиту:

1. Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.
2. Выберите  **Настройки**.
3. Снимите флажок **Включить самозащиту**.
4. Нажмите **Сохранить**.

Проверка работоспособности

Для контроля работоспособности в ViPNet EPP Агент выполняется:

- Контроль целостности важных 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 нарушении целостности будут записаны в служебные диагностические журналы. 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 системы) 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.
- Номер версии ViPNet EPP.
- Работоспособность сетевого сенсора ViPNet EPP (Net Sensor) — работает или остановлен.
- Работоспособность службы контроля ViPNet EPP (Controller) — работает или остановлена.
- Состояние подключения к базе данных ViPNet EPP Агент — завершено успешно или завершено с ошибкой.
- Дата и время обновления базы правил.
- Версия базы правил.
- Последнее время восстановления работоспособности ViPNet EPP Агент службой контроля ViPNet EPP.
- Самозащита — включена или отключена.
- Целостность журнала аудита, целостность журнала контроля приложений, 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 папке установки ViPNet EPP Агент (по умолчанию `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection`) в файлах:
    - `audit_journal_backup_дата и время создания.json` — журнал аудита;
    - `application_control_journal_backup_дата и время создания.json` — журнал контроля приложений;
    - `traffic_journal_backup_дата и время создания.json` — журнал трафика;
    - `event_journal_backup_дата и время создания.json` — журнал событий.
  - Из текущего журнала, целостность которого нарушена, будут удалены все события и зарегистрируется первое событие о восстановлении работоспособности после нарушения целостности соответствующего журнала.
- Состояние подключения к ViPNet EPP Сервер (только в ViPNet EPP Агент под управлением сервера):
  - Сервер не задан — настройки подключения к ViPNet EPP Сервер не заданы.
  - Ожидает подключения — находится в группе **Запросы на подключение** ViPNet EPP Сервер.
  - Подключен — перемещен из группы **Запросы на подключение** в одну из пользовательских групп ViPNet EPP Сервер.

- Удален — не посылает запросы на подключение к ViPNet EPP Сервер.
- Ошибка — проверка состояния подключения завершилась ошибкой.

- Актуальность базы правил — актуальная, устарела или отсутствует (только для ViPNet EPP Агент под управлением сервера).
- Режимы работы модулей защиты ViPNet EPP Агент (Контроль приложений, Персональный межсетевой экран и Предотвращение вторжений) — отключен, установлен из базы правил или локальный (изменен администратором агента). Отображаются только для ViPNet EPP Агент под управлением сервера.

Результаты самотестирования, выполненного автоматически или вручную, регистрируются в журнале аудита ViPNet EPP Агент (см. Журнал аудита) и передаются на ViPNet EPP Сервер (только для ViPNet EPP Агент под управлением сервера).

Если в результате самотестирования были выявлены потенциальные проблемы, раздел **Самотестирование** будет отмечен желтым .

Чтобы запустить самотестирование ViPNet EPP Агент:

1 Подключитесь к ViPNet EPP Агент с полномочиями администратора агента.

2 Выберите **Самотестирование**.

3 Нажмите **Запустить самотестирование** и дождитесь результатов.

Диагностические журналы

Диагностические журналы ViPNet EPP сохраняются в папках:

- `C:\ProgramData\InfoTeCS\ViPNet EndPoint Protection`
- `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection\Suricata\log`

Просмотр сведений о лицензии

Чтобы просмотреть сведения о 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** > **Данные** и посмотрите сведения о лицензии ViPNet EPP Агент на защищаемом узле:

- Контактная информация ИнфоТеКС.
- Статус лицензии: не загружена, установлена, активирована, истек срок действия.

- Срок действия — дата окончания действия лицензии или бессрочная лицензия.
- Срок действия подписки на обновление базы правил.
- Идентификатор лицензии.
- Тип лицензии: автономная или серверная.
- Доступные модули и срок действия лицензии на них.

3 Для ознакомления с лицензионным соглашением на использование ViPNet EPP выберите вкладку **Лицензионное соглашение**.

Управление из области уведомлений панели задач ОС Windows

Чтобы управлять ViPNet EPP Агент из области уведомлений панели задач ОС Windows:

1 Правой кнопкой мыши щелкните ViPNet EPP Агент .

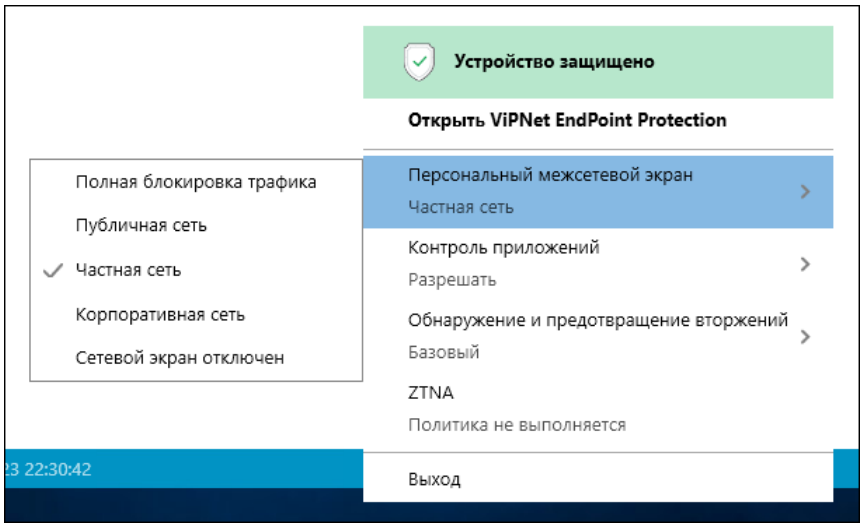


Рисунок 124. Управление ViPNet EPP Агент из области уведомлений панели задач ОС Windows

В верхней части окна управления ViPNet EPP Агент отображается статус защиты:

- **Устройство защищено**.
- **Пониженный уровень защиты**.
- **Защита отключена**.

2 Чтобы открыть главное окно ViPNet EPP Агент в режиме текущего пользователя, выберите **Открыть ViPNet EndPoint Protection**.

3 Чтобы изменить режим работы персонального межсетевого экрана, выберите **Персональный межсетевой экран** и выберите нужный режим.

4 Чтобы изменить режим работы контроля приложений, выберите **Контроль приложений** и выберите нужный режим.

5 Чтобы изменить режим работы обнаружения и предотвращения вторжений, выберите **Обнаружение и предотвращение вторжений** и выберите нужный режим.

6 Чтобы просмотреть подробнее о статусе выполнения политики ZTNA, выберите **ZTNA**. В автономном ViPNet EPP Агент этот пункт не отображается.

7 Чтобы завершить текущий сеанс работы с ViPNet EPP Агент, выберите **Выход**.

Уведомления о срабатывании модулей защиты и обновлении ViPNet SafeBoot

На защищаемом узле могут появляться всплывающие уведомления центра уведомлений ОС Windows:

- о срабатывании блокирующих правил контроля приложений и веб-фильтров ViPNet EPP;
- 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).

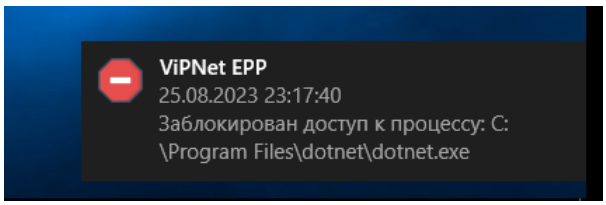


Рисунок 125. Пример уведомления о срабатывании блокирующих правил контроля приложений

Чтобы на защищаемом узле получать уведомления, убедитесь, что:

1 В настройках центра уведомлений ОС Windows включено получение уведомлений от приложений и других отправителей.

2 В настройках ViPNet EPP Агент включены **Уведомления** (см. Просмотр и настройка параметров работы).

A

Полномочия пользователей

Полный список полномочий пользователей ViPNet EPP Сервер приведен в таблице ниже.

Таблица 7. Полномочия пользователей ViPNet EPP Сервер в соответствии с назначенной ролью

Полномочия пользователя	**Администратор**	**Аудитор**	**Пользователь**
Просмотр информации о состоянии ViPNet EPP на инфопанели	+	+	-
Просмотр информации о лицензии ViPNet EPP	+	+	+
Установка и активация лицензии ViPNet EPP	+	-	-
Управление защищаемыми узлами и группами	+	-	-
Управление учетными записями ViPNet EPP Сервер	+	-	-
Настройка конфигурации ViPNet EPP Сервер	+	-	-
Настройка конфигурации ViPNet EPP Агент	+	-	-
Резервное копирование и восстановление конфигурации	+	-	-
Настройка критериев обнаружения аномалий	+	-	-
Настройка модели нормальной активности защищаемых узлов модуля BA	+	-	-
Просмотр журнала событий	+	+	+
Запрос журнала регистрации трафика с ViPNet EPP Агент	+	-	-
Удаление событий	+	-	-
Просмотр журнала аудита ViPNet EPP Сервер	+	+	-

Настройка параметров журнала аудита ViPNet EPP Сервер	+	-	-
Настройка параметров журнала аудита ViPNet EPP Агент	+	-	-
Загрузка обновлений базы правил	+	-	-
Настройка автоматической загрузки обновлений базы правил	+	-	-
Просмотр основных сведений базы правил: дата создания, версия, активность, режимы работы модулей защиты, группы узлов	+	+	+
Просмотр и управление избранными правилами (сетевыми фильтрами, правилами контроля приложений, веб-фильтров и правилами ZTNA)	+	-	-
Просмотр детальных сведений базы правил: дата создания, версия, активность, группы узлов, детальные настройки модулей защиты — сетевых фильтров, справочников, списков контроля приложений, правил доступа, правил HIDS и HIPS	+	-	-
Настройка базы правил: выбор групп узлов и режимов работы модулей защиты; настройка модулей защиты	+	-	-
Управление ViPNet SafeBoot на защищаемых узлах	+	-	-
Управление сканированием AntiMalware	+	-	-
Проверка работоспособности ViPNet EPP Сервер	+	-	-

Полный список полномочий пользователей ViPNet EPP Агент приведен в таблице ниже.

Таблица 8. Полномочия пользователей ViPNet EPP Агент в соответствии с назначенной ролью

Полномочия пользователя	**Администратор**	**Аудитор**	**Пользователь**
Просмотр информации о состоянии ViPNet EPP Агент на инфопанели	+	+	+
Управление учетными записями ViPNet EPP Агент	+	-	-
Просмотр и редактирование настроек ViPNet EPP Агент	+	-	-
Изменение адреса ViPNet EPP Сервер (IP-адреса и TCP-порта)	+	-	-
Просмотр основных сведений журнала событий ViPNet EPP Агент	+	+	+
Просмотр детальных сведений журнала событий ViPNet EPP Агент	+	+	-
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	+	-	-
Настройка оповещений по событиям безопасности	+	-	+
Проверка работоспособности ViPNet EPP Агент (запуск самотестирования)	+	-	-
Управление самозащитой ViPNet EPP Агент	+	-	-
Просмотр информации о программе ViPNet EPP Агент и о результатах самотестирования	+	+	-
Установка и активация лицензии ViPNet EPP Агент (доступно только в автономном ViPNet EPP Агент)	+	-	-
Импорт и экспорт базы правил (доступно только в автономном ViPNet EPP Агент)	+	-	-
Просмотр уведомлений ViPNet EPP центра уведомлений ОС Windows	+	+	+
Персональный межсетевой экран PFW			
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	+	+	-
Блокирование и разблокирование трафика на основе событий журнала трафика PFW	+	-	-
Блокирование и разблокирование сетевой активности приложения на основе событий журнала активных соединений PFW	+	-	-
Просмотр глобальных справочников протоколов PFW (недоступно в автономном ViPNet EPP Агент)	+	-	-
Настройка пользовательских справочников протоколов PFW	+	-	-
Настройка пользовательских справочников адресов и сетей PFW	+	-	-
Просмотр глобальных справочников расписаний PFW (недоступно в автономном ViPNet EPP Агент)	+	-	-
Просмотр пользовательских справочников PFW	+	+	-
Настройка пользовательских справочников расписаний PFW	+	-	-
Настройка справочников ViPNet	+	-	-
Контроль приложений AppC			
Изменение режима работы AppC	+	+	-
Просмотр журнала событий AppC	+	+	-
Добавление приложения в пользовательские списки контроля приложений на основе события AppC	+	-	-

Просмотр глобальных и пользовательских списков контроля приложений (просмотр глобальных списков недоступен в автономном ViPNet EPP Агент)	+	+	-
Управление пользовательскими списками контроля приложений	+	-	-
Просмотр правил доступа глобального и пользовательского списков контроля приложений (просмотр глобальных правил недоступен в автономном ViPNet EPP Агент)	+	+	-
Управление правилами доступа пользовательского списка контроля приложений	+	-	-
Сканирование AntiMalware и добавление приложений в черный список	+	-	-
Просмотр отчетов AntiMalware	+	-	-
Обнаружение и предотвращение вторжений HIPS/HIDS			
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 веб-фильтров	+	+	-
Управление веб-фильтрами (доступно только в автономном ViPNet EPP Агент)	+	-	-
Просмотр правил HIDS	+	+	-
Управление правилами HIDS (доступно только в автономном ViPNet EPP Агент)	+	-	-
Просмотр правил HIPS для бесфайловых атак	+	+	-
Управление пользовательскими правилами HIPS для бесфайловых атак	+	-	-
Просмотр политик аудита	+	+	-
Управление политиками аудита (доступно только в автономном ViPNet EPP Агент)	+	-	-

B

Типы и идентификаторы правил

Таблица 9. 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) Локальные атаки (в Linux)		Правила HIDS для мониторинга событий реестра
200000–209999 210001–299999	Контроль файлов (Windows)	Правила анализа	Правила обнаружения локальных атак (в Windows) Локальные атаки (в Linux)	Обнаружение атак (HIDS)	Правила HIDS для мониторинга изменений файловой системы
210000	Контроль файлов (Windows)	Мониторинг файлов	Мониторинг файлов (в Windows) Операции с файлами (в Linux)		Правила HIDS для мониторинга файлов

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
860000–869999	Изменение файловой системы (Linux)	860000–860015, 860020–869999 – правила анализа 860016 – получение контрольной суммы файлов 860017–860019 – мониторинг файлов	860000–860015, 860020–869999 – правила обнаружения локальных атак (в Windows) Локальные атаки (в Linux) 860016 – получение контрольной суммы файлов (в Windows) Расчет контрольных сумм файлов (в Linux) 860017–860019 – мониторинг файлов (в Windows) 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) 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) Локальные атаки (в Linux)		Правила HIDS для обнаружения бесфайловых атак
400000–499999	Системная активность (Windows)	Правила анализа Анализ журнала событий Windows	Правила обнаружения локальных атак (в Windows) Локальные атаки (в Linux)		Правила HIDS для контроля системной активности

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
870000–879999	Системная активность (Linux)	Правила анализа	Правила обнаружения локальных атак (в Windows) Локальные атаки (в Linux)		Правила HIDS для контроля системной активности
500000–599999	Логины пользователей (Windows)	Правила анализа Анализ журнала событий Windows	Правила обнаружения локальных атак (в Windows) 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) Локальные атаки (в Linux)		Правила HIDS для контроля аутентификации пользователей
600000–699999	Изменения учетных записей (Windows)	Правила анализа Анализ журнала событий Windows	Правила обнаружения локальных атак (в Windows) 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) Локальные атаки (в Linux)		
700000–749999	Выполняемые команды (Windows)	Команды мониторинга системы	Выполняемые команды (в Windows) Команды мониторинга системы Windows (в Linux)		Правила HIDS для контроля за выполнением команд
839999–859999	Выполняемые команды (Linux)	Команды мониторинга	Выполняемые команды		

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
		системы			
750000–779999	Контроль установки приложений (Windows)	Мониторинг устанавливаемого ПО	Обнаружение установки ПО (в Windows) 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) 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) 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) 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) 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) Сетевые атаки (в Linux)		Сетевые правила HIDS защищаемого узла

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
2000000–4000000	Правила предотвращения сетевых атак (Windows/Linux)	Правила обнаружения сетевых атак	Правила обнаружения сетевых атак (в Windows) Сетевые атаки (в Linux)	HIPS	Правила HIPS защищаемого узла
4000001–4099999	—	—	— (в Windows) Межсетевой экран (в Linux)	Межсетевой экран (PFW)	Фильтры политик безопасности, задаваемые в базе правил (политике безопасности) в ViPNet EPP Сервер
4100000–4199999	—	—	— (в Windows) Межсетевой экран (в Linux)		Пользовательские фильтры, задаваемые в ViPNet EPP Агент защищаемого узла
4950000–4999999	—	—	—(в Windows) Межсетевой экран (в Linux)		Сетевые фильтры блокирования контента
5000000–5199999	Контроль активности приложений (Windows)	—	Контроль приложений	Контроль приложений (AppC)	Черный и белый списки
5200000–5399999	Контроль доступа приложений к файлам (Windows)	—	Контроль приложений		Правила доступа к файлам
5400000–5599999	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)	—	—		Веб-фильтрация

C

Типы аномалий, обнаруживаемые с помощью поведенческого анализа

Таблица 10. Типы аномалий, обнаруживаемые с помощью поведенческого анализа

Тип аномалии	Идентификатор события модуля BA
Аномальный вход в систему	7000000
Аномальное изменение значения раздела реестра (изменение настроек прокси-сервера)	7000001
Аномальное изменение значения раздела реестра (изменение адреса сервера обновлений ОС Windows)	7000002
Аномальный вход в систему с привилегиями	7000003
Аномалия в событии создания процесса	7000004
Аномалия в событии создания задачи	7000005
Аномалия в событии удаления задачи	7000006
Аномалия в событии включения задачи	7000007
Аномалия в событии отключения задачи	7000008

Тип аномалии	Идентификатор события модуля BA
Аномалия в событии обновления задачи	7000009
Аномалия в событии записи в файл `etc/hosts`	7000010
Аномальный запуск `powershell.exe`	7000100
Аномальный запуск `rundll32.exe`	7000101
Аномальный запуск `regsvr32.exe`	7000102
Аномальный запуск `wscript.exe`	7000103
Аномальный запуск `cscript.exe`	7000104
Аномальный запуск `mshta.exe`	7000105
Аномальный запуск `cmd.exe`	7000106
Аномальный запуск `msbuild.exe`	7000107
Аномальный запуск `installutil.exe`	7000108
Аномальный запуск `msiexec.exe`	7000109
Аномальный запуск `control.exe`	7000110
Аномальный запуск `certutil.exe`	7000111
Аномальный запуск `wmic.exe`	7000112
Аномальный запуск `regsvcs.exe`	7000113
Аномальный запуск `mavinject.exe`	7000114
Аномальный запуск `odbcconf.exe`	7000115
Аномальный запуск `schtasks.exe`	7000116
Неизвестное аномальное событие	7099999

D

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 11. Описание полей заголовка CEF-сообщения

Поле	Описание
Version	Текущая версия формата CEF — `0`
Device Vendor	Наименование производителя ViPNet EPP — `infotecs`
Device Product	Наименование продукта — `EPP`
Device Version	Версия ViPNet EPP в формате: X.Y.Z. Например, `1.1.3.3036`
Device Event Class	Уникальный идентификатор класса события в одном из следующих форматов:

ID или Signature ID	• Формат для сетевых событий (Device Event Class ID): `[Номер типа правила]:[Идентификатор правила]:[Версия правила]`, где: `[Номер типа правила]` — номер, который идентифицирует метод обнаружения угрозы. Для сигнатурных правил параметр имеет постоянное значение — `1`. `[Идентификатор правила]` — уникальный номер, присваиваемый каждому правилу для идентификации события. `[Версия правила]` — номер версии правила. Значения [`Идентификатор правила`] и [`Версия правила`] прописаны для каждого правила в базе правил. Например, Device Event Class ID может содержать значение — `1:2100366:4` • Формат других событий (Signature ID): `[Идентификатор правила]` Например, Signature ID может содержать значение — `190001` 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».
Name	Описание события. Например, — `Изменение журнала приложений`
Severity	Уровень события: • `0` — информационное событие (в TIAS — низкий). • `4` — важное событие (в TIAS — средний). • `6` — опасное событие (в TIAS — высокий). • `10` — критическое событие (в TIAS — критичный).

- `[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 12. Общие ключи поля расширения

Ключ	Описание ключа	Пример значения ключа или поддерживаемые ключи
Обязательные ключи		
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 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
Необязательные ключи		

cnt	Количество срабатываний правила, в результате которых зарегистрировано событие	Например, `17`
anomaly	Аномальное событие; обнаружено с помощью критерия	`1`
agentMac	Mac-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 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 13. Описание значений ключа `deviceFacility`

Значения ключа deviceFacility	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 14. 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 15. Зависимость обязательных ключей и распределение поддерживаемых дополнительных ключей

Диапазон идентификаторов правил	Тип правил	Значения ключа deviceFacility	Поддерживаемые значения ключа threatSourceCat	Поддерживаемые дополнительные ключи
100000-199999	Контроль реестра	eventlog	RegeditControl	RegistryKey; RegistryNewValue; RegistryOldValue; RegistryOperationType; RegistryPath; sntdom; sproc; suid suser
200000-299999	Контроль файлов	eventlog	FileControl	filePath; FileOperationType; message sntdom; sproc; suid; suser
300000-379999	Контроль процессов	eventlog	ProcessControl	CommandLine; ParentProcessName; message sntdom; sproc; suid; suser
380000-399999	Обнаружение бесфайловых атак		ProcessControl	sproc; suser

400000-499999	Системная активность	eventlog	SystemActivity	filePath; AuthenticationPackageName; DeviceName; DnsServerIpAddress; DomainQueryName; DomainQueryType; KasperskyEventType; KasperskyResult; KasperskyResultName; KasperskyResultType; KasperThreatSever; NewSD; NotificationPackageName; ObjectName; OldSD; SecurityPackageName; ServiceAccount; ServiceAlias; ServiceFileName; ServiceStartType; ServiceStartTypeNewValue; ServiceStartTypeOldValue; ServiceType; SoftName; TaskCommand; TaskName; WindowCaption; WindowMsg; reasonDescription; sntdom; sourceServiceName; sproc; src; suid; suser virusName
500000-599999	Логины пользователей	eventlog	LoginControl	dntdom; duid; duser;

				AuthType; LogOnType; SessionName; tgtOpt; reasonDescription; shost; sntdom; spt; src; suid; suser
600000-699999	Изменения учетных записей	eventlog	UserChangesControl	dntdom; duid; duser; SidUserGroup; UserGroup; sntdom; suid suser
700000-749999	Команды мониторинга	command_control	CommandControll	executedCommands
750000-779999	Контроль установки приложений	newsoft	InstallAppControl	SoftName; SoftPublisher; SoftVersion
780000-789999	Мониторинг системных обновлений	update_kb	InstallKbControl	Updates
790000-799999	Получение контрольной суммы файлов	integritycontrol	SystemActivity	filePath; FileHash; FileHashType
800000-839998	Журнал приложений	applog	AppControl	message
839999-859999	Команды мониторинга ОС *nix	command_control	CommandControll	executedCommands
860000-869999	Контроль 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; filePath
2000000-4000000	Правила обнаружения сетевых атак	snort, suricata	NetAgentRules	dpt; dst; transportProto; spt; src
4950000–4999999	Сетевая активность	suricata	NetAgentRules	dpt; dst; transportProto; spt; src; cnt
5000000-5199999	Контроль активности приложений		AppControl	cnt; data
5200000-5399999	Контроль доступа приложений к файлам		FileControl	cnt; data
5400000-5599999	Контроль доступа приложений к реестру		RegeditControl	cnt; data

Перечень и описание поддерживаемых дополнительных ключей приведены в таблице ниже.

Таблица 16. Список дополнительных ключей расширения

Ключ	Описание ключа	Пример значения ключа
cnt	Количество	10

data	Данные в текстовом формате JSON	[{ "app_path": "", //Приложение/путь к приложению "reg_path": "", //Путь к ветке реестра },]
reasonDescription	Описание вредоносной активности	Обнаружен PoC CVE-2020-0986
dntdom	Домен целевой учетной записи	DESKTOP-EQSPQ7H 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-clientext_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 обнаруженного вируса	Минимальная
LogOnType	Тип входа	user
NotificationPackageName	Наименование пакета уведомлений	"WDIGEST"
ObjectName	Имя объекта	Папка
ParentProcessName	Имя родительского 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 безопасности	"Kerberos"
ServiceAccount	Учетная запись службы	LocalSystem
ServiceAlias	Псевдоним службы	TrustedInstaller
ServiceFileName	Полный путь к образу службы	"C:\Program Files\Zabbix Agent\zabbix_agentd.exe"
ServiceStartType	Тип запуска службы	auto start
ServiceStartTypeNewValue	Тип запуска службы (новое значение)	Автоматически
ServiceStartTypeOldValue	Тип запуска службы (старое значение)	Вручную
ServiceType	Тип службы	user mode service
SessionName	Имя сессии	user
SidUserGroup	Идентификатор целевой 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 D:\test\test-Win64-Shipping.exe
message	Сообщение	postgres - "C:/Program Files (x86)/PostgreSQL/bin/postgres.exe" "--forkbackend" "4084"
executedCommands	Выполняемые команды	Обмен пакетами с 127.0.0.1 по с 32 байтами данных: Превышен интервал ожидания для запроса. ... Пакетов: отправлено = 4, получено = 0, потеряно = 4 (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 17. Примеры CEF-сообщений по категории события

Категория события (threatSourceCat)	Пример CEF-сообщения
AppControl	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
CommandControl	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<1мс TTL\=128 Ответ от 127.0.0.1: число байт\=32 время<1мс TTL\=128 Ответ от 127.0.0.1: число байт\=32 время<1мс TTL\=128 Ответ от 127.0.0.1: число байт\=32 время<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>

FileControl	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
InstallAppControl	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'.|
InstallKbControl	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
LoginControl	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=-
NetAgentRules	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

ProcessControl	Mar 16 12:46:23.135 EPP-Server 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
RegeditControl	Mar 16 12:46:23.135 EPP-Server CEF:0|infotecs|EPP|1.0.0.0|100016|Изменение типа запуска службы (реестр)|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\\FDResPub\\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
SystemActivity	Mar 16 12:46:23.135 EPP-Server 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
UserChangesControl	Mar 16 12:46:23.135 EPP-Server 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

E

Возможные неполадки

В ViPNet EPP Сервер не приходит запрос на подключение от ViPNet EPP Агент

Эта ситуация может возникнуть при повторном подключении ViPNet EPP Агент к ViPNet EPP Сервер, например после переустановки ViPNet EPP Сервер или если защищаемый узел был удален из группы **Запросы на подключение** ViPNet EPP Сервер. Для повторного подключения ViPNet EPP Агент к ViPNet EPP Сервер:

1. Удалите ViPNet EPP Агент. Обязательно перезагрузите компьютер.
2. Откройте файловый менеджер и удалите папку `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection`.
3. Переустановите ViPNet EPP Агент (см. Установка ViPNet EPP Агент вручную). Обязательно перезагрузите компьютер.

Защищаемый узел вновь пришлет в ViPNet EPP Сервер запрос на подключение и запрос появится в группе **Запросы на подключение**. Подключите ViPNet EPP Агент к серверу.

Ошибка подключения "Не удалось подключиться к сервису"

Ошибка может появляться в ViPNet EPP Агент, например при использовании на компьютере ПО КриптоПро CSP устаревшей версии (4 и ниже).

Для решения проблемы:

1. Удалите устаревшее ПО КриптоПро CSP средствами ОС Windows или обновите до версии 5.
2. Выполните все действия из раздела В ViPNet EPP Сервер не приходит запрос на подключение от ViPNet EPP Агент.

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.

Ошибка типа «синий экран» ОС Windows на компьютере защищаемого узла

Чтобы на компьютере защищаемого узла избежать появления ошибки типа «синий экран» ОС Windows, установите драйверы сетевого адаптера, рекомендуемые производителем.

Высокая загрузка процессора на компьютере защищаемого узла

Если проблема именно в постоянной загрузке процессора, а не эпизодической, например при получении новой версии базы правил, можно понизить число основных рабочих потоков:

1. В папке установки ViPNet EPP Агент (по умолчанию `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection`) в файле `EppService.dll.config` уменьшите значение параметра `AnalysisThreads` на 2 (по умолчанию используется 4).

   Количество потерянных событий при этом возрастет, но снизится нагрузка на процессор. Минимальное допустимое значение `1` не рекомендуется устанавливать без видимых на то причин.
2. Перезапустите ViPNet EPP Агент.

На компьютере защищаемого узла с ОС Windows 10 сбрасываются приложения по умолчанию

При изменении аудита ветвей реестра `HKEY_USERS` и `HKEY_CURRENT_USER` ОС Windows 10 сбрасывает параметры приложений по умолчанию, например веб-браузера, электронной почты, видеопроигрывателя.

Для выборочного решения проблемы в политике аудита для группы защищаемых узлов на вкладке **Реестр** удалите из путей аудита ветки реестра `HKEY_USERS` и `HKEY_CURRENT_USER` (см. Политика аудита изменений в реестре).

Чтобы решить проблему для всех групп защищаемых узлов, аналогичным образом измените политику аудита по умолчанию.

Не работает блокировка драйвера

Драйвер можно блокировать с помощью глобальных (см. Управление активностью приложений) или пользовательских (см. Создание правил доступа приложения) правил доступа к файлам встроенного модуля контроля приложений ViPNet EPP. Если драйвер запущен, то правила доступа к файлам будут блокировать драйвер после перезагрузки компьютера защищаемого узла.

Не работает блокировка dll-библиотеки с помощью правила доступа к процессам

Правила доступа к процессам контроля приложений не блокируют работу dll-библиотеки.

Чтобы заблокировать dll-библиотеку, используйте глобальные (см. Управление активностью приложений) или пользовательские (см. Создание правил доступа приложения) правила доступа к файлам встроенного модуля контроля приложений ViPNet EPP.

Проблемы при работе с MS Office 2010 x86

Если на защищаемом узле с ОС Windows x64 используется MS Office 2010 x86, то после установки ViPNet EPP возможно возникновение проблем в работе приложений офисного пакета.

Рекомендуется использовать версию MS Office 2010 x64 и добавить приложения офисного пакета в глобальный (см. Управление запуском приложений) и пользовательский (см. Управление пользовательскими списками приложений) белые списки контроля приложений.

Ошибка запуска Powershell после настройки политики аудита

При включении политики аудита **Транскрипция Powershell** (см. Другие политики аудита) на защищаемых узлах с ОС Windows Server, где применяется эта политика, запуск программы Powershell завершается с ошибкой.

Аналогичная проблема наблюдается и при включении такой политики аудита средствами самой ОС.

Для решения ошибки с запуском Powershell отключите аудит **Транскрипция Powershell**.

Ошибка подключения при использовании приложений, создающих сетевые соединения по протоколу SSL/TLS

При включенной TLS-инспекции на защищаемом узле могут возникать проблемы в работе некоторых приложений, создающих сетевые соединения с использованием протокола SSL/TLS.

Для решения проблемы отключите TLS-инспекцию в базе правил, используемой на защищаемом узле.

Ошибка подключения к базе данных при восстановлении ViPNet EPP Сервер

Если при восстановлении ViPNet EPP Сервер возникла ошибка о невозможности подключения к базе данных и необходимости проверки данных подключения, скорее всего не найдены параметры подключения к базе данных PostgreSQL: имя учетной записи, пароль и порт подключения.

Чтобы выполнить восстановление ViPNet EPP Сервер, вы можете вручную указать эти данные. Для этого запустите командную строку ОС Windows (`cmd.exe`) и выполните команду:

```
ViPNetEppServerSetup_x64_RU_x.x.x.xxxx.msi LOGIN=<имя учетной записи> PASSWORD=<пароль>
PORT=<номер порта подключения>
```

Если вы указали корректные данные подключения в базе данных PostgreSQL, восстановление будет завершено без ошибок.

Ошибка «Служба EPP недоступна»

Ошибка «Служба EPP недоступна» появляется в случае большого количества запросов к ViPNet EPP Агент. Ошибка не блокирует работу ViPNet EPP, но означает, что ViPNet EPP Агент не успевает обрабатывать запросы и из них формируется очередь.

Ошибка может появляться на ViPNet EPP Агент и на ViPNet EPP Сервер. Например, на ViPNet EPP Сервер ошибка может появиться при активном просмотре администратором результатов сканирования AntiMalware на ViPNet EPP Агент.

При появлении ошибки рекомендуем вам снизить количество обращений к ViPNet EPP Агент, чтобы дать ему возможность закончить обработку текущих запросов.

Не удается подключиться к удаленному Серверу

Эта ситуация может возникнуть при авторизации в ViPNet EPP Сервер, если вы поменяли адрес Сервера в ViPNet EPP Серверная консоль перед входом. Повторное подключение к другому Серверу из этой же консоли может быть недоступно.

Для решения проблемы, измените конфигурационные данные для ViPNet EPP Серверная консоль. На компьютере, где установлена консоль:

1. Закройте Серверную консоль.
2. С помощью текстового редактора откройте конфигурационный файл `Epp.ServerConsole.dll.config` от имени локального администратора.

   Путь до файла по умолчанию:

   `C:\Program Files\InfoTeCS\ViPNet EndPoint Protection Server Console`
3. В строке вида

   ```
   <setting name="ServerAddress" serializeAs="String">
      <value>localhost</value>
   ```

   измените значение в поле `<value></value>` — вставьте доменное имя или IP-адрес нового Сервера.
4. Сохраните конфигурационный файл.
5. Запустите Серверную консоль и подключитесь к тому Серверу, данные которого вы указали в конфигурационном файле (см. Подключение к ViPNet EPP Сервер).

F

История версий

В приложении описаны основные изменения в предыдущих версиях ViPNet EPP.

Что нового в версии 1.7.1

Краткий обзор изменений и новых возможностей ViPNet EPP версии 1.7.1 по сравнению с версией 1.7.0:

- **Изменения в списке поддерживаемых ОС GNU/Linux для ViPNet EPP Агент**

  Реализована поддержка работы ViPNet EPP Linux Агент в ОС новых версий:

  - Astra Linux Special Edition 1.8.
  - РЕД ОС 8.0 «Муром» Рабочая станция, стандартная редакция.

  Прекращена поддержка работы ViPNet EPP Linux Агент в ОС Альт 8 СП и Debian Linux 11 (bullseye).

  Список всех версий поддерживаемых ОС GNU/Linux с версиями ядер см. в документе «ViPNet EPP Linux. Руководство администратора» в разделе «Требования к установке ViPNet EPP Агент».

- **Изменения в списке поддерживаемых ОС Windows для ViPNet EPP Сервер и ViPNet EPP Агент**

  Прекращена поддержка работы ViPNet EPP в ОС Windows 8.1 и Windows Server 2016 Standard и Datacenter.

  Список всех поддерживаемых ОС Windows см. в разделах Требования к установке ViPNet EPP Сервер и Требования к установке ViPNet EPP Агент.

- **Переход на использование СУБД PostgreSQL версии 14 для ViPNet EPP Сервер в ОС Windows**

Для работы ViPNet EPP Windows Сервер теперь требуется установить СУБД PostgreSQL версии 14. Установочный файл входит в комплект поставки ViPNet EPP. Перед обновлением ViPNet EPP Windows Сервер обновите СУБД PostgreSQL на версию 14.

Подробнее см. в разделах Комплект поставки, Обновление СУБД PostgreSQL версии 12 до версии 14 на компьютере с ViPNet EPP Сервер.

- **Обновление ViPNet EPP**

  Обновление ViPNet EPP до версии 1.7.1 возможно только с версии 1.7.0. Обновление с более старых версий должно выполняться по определенной схеме.

  Подробнее см. в разделе Порядок обновления ViPNet EPP версии 1.5.2 и выше до версии 1.7.1 (см. Порядок обновления ViPNet EPP версии 1.5.2 и выше до версии 1.8.0) и в документе «ViPNet EPP Linux. Руководство администратора» в аналогичном разделе.

- **Изменения в установке ViPNet EPP Сервер (в ОС Windows)**

  При установке и обновлении ViPNet EPP Windows Сервер будет создана отдельная учетная запись `endpoint_protection` для управления базой данных ViPNet EPP в PostgreSQL.

  Подробнее см. в разделах Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль и Обновление ViPNet EPP Сервер и ViPNet EPP Серверная консоль.

- **Запуск графической консоли управления ViPNet EPP Агент (в ОС GNU/Linux)**

  Теперь подключиться к ViPNet EPP Linux Агент и запустить графическую консоль управления можно из меню **Пуск**.

  Подробнее см. в документе «ViPNet EPP Linux. Руководство администратора» в разделе «Подключение к ViPNet EPP Агент».

- **Изменения схемы фильтрации IP-трафика персонального межсетевого экрана ViPNet EPP Агент**

  Теперь при работе ViPNet EPP Агент на компьютере с установленной программой ViPNet Client 5 персональный межсетевой экран ViPNet EPP Агент выполняет фильтрацию IP-трафика открытой сети (не относящегося к сети ViPNet), а для трафика защищенной сети ViPNet применяются политики ZTNA и локальные фильтры защищенной сети ViPNet. В журнале трафика регистрируются события по каждому этапу фильтрации трафика.

  Подробнее см. в разделе Схема фильтрации трафика при интеграции с ViPNet Client 5.

- **Централизованное получение фильтров политик безопасности в ViPNet EPP Агент из ViPNet Policy Manager**

  Реализована возможность на защищаемом узле с установленной программой ViPNet Client 5 в качестве фильтров политик безопасности открытой сети использовать сетевые фильтры, полученные из ViPNet Policy Manager. Источник получения фильтров политик безопасности настраивается в ViPNet EPP Windows Сервер.

  Подробнее см в разделе Персональный межсетевой экран.

- **Использование исключений из политики ZTNA в ViPNet EPP Агент**

  Теперь на защищаемом узле с установленной программой ViPNet Client 5 из ViPNet Policy Manager могут быть получены исключения из политик ZTNA со списком узлов сети ViPNet,

которые будут доступны на защищаемом узле даже при невыполнении политики ZTNA. В ViPNet EPP Агент доступен просмотр статуса выполнения политик ZTNA и списка исключений.

Подробнее см. в разделе Сетевой доступ с нулевым доверием (см. Сетевой доступ с нулевым доверием (ZTNA)).

- **Добавление веб-фильтров в базу правил из файлов**

  Теперь в ViPNet EPP Windows Сервер или в автономном ViPNet EPP Windows Агент при настройке веб-фильтров в базе правил вы можете добавлять адреса контролируемых веб-ресурсов списком из файла формата `.csv`.

  Подробнее см. в разделе Настройка веб-фильтров.

- **Добавление в ViPNet EPP Сервер веб-фильтров и правил политик ZTNA в избранное (в ОС Windows)**

  Теперь при настройке базы правил в ViPNet EPP Windows Сервер вы можете добавлять в избранное веб-фильтры и политики ZTNA, а затем использовать их в разных версиях баз правил. В избранном доступен просмотр и удаление добавленных правил.

  Подробнее см. в разделах Настройка веб-фильтров, Управление политиками ZTNA и Просмотр и удаление избранных правил.

- **Настройка контроля обращений к сетевым папкам для защищаемых узлов**

  Теперь в случае появления на защищаемом узле проблемы замедления работы с файлами, расположенными на сетевых дисках, вы можете в ViPNet EPP Windows Сервер в базе правил, назначенной на проблемный защищаемый узел, отключить контроль обращений к сетевым папкам. В результате на защищаемом узле файлы и папки, расположенные на сетевых дисках, перестанут контролироваться правилами доступа к файлам контроля приложений ViPNet EPP.

  Подробнее см. в разделе Настройка контроля обращений к сетевым папкам.

- **Уведомления в ViPNet EPP Агент о смене статуса выполнения политики ZTNA и о получении обновления ViPNet SafeBoot**

  Реализована возможность уведомлять пользователя защищаемого узла о смене статуса выполнения политики ZTNA и о более долгой загрузке компьютера при установке обновления ViPNet SafeBoot.

  Подробнее см. в разделе Уведомления о срабатывании средств защиты и обновлении ViPNet SafeBoot (см. Уведомления о срабатывании модулей защиты и обновлении ViPNet SafeBoot).

- **Изменения при создании сетевого фильтра из журнала трафика ViPNet EPP Агент**

  Создание фильтров на основе событий журнала трафика доступно только для зарегистрированного трафика открытой сети (не принадлежащего защищенной сети ViPNet).

  Подробнее см. в разделе Журнал трафика.

- **Отображение только аномальных событий в журнале критичных событий ViPNet EPP Сервер (в ОС GNU/Linux)**

  В ViPNet EPP Linux Сервер реализована возможность в журнале критичных событий просматривать только аномальные события ViPNet EPP Агент, зарегистрированные по заданным критериям обнаружения аномалий.

Подробнее см. в документе «ViPNet EPP Linux. Руководство администратора» в разделе «Критичные события агентов».

- **Исправление ошибок**

  Устранены ошибки, выявленные в процессе эксплуатации предыдущей версии.

Что нового в версии 1.7.0

Краткий обзор изменений и новых возможностей ViPNet EPP версии 1.7.1 по сравнению с версией 1.6.0:

- **Автономная модель работы ViPNet EPP Агент**

  Реализована модель работы ViPNet EPP Агент без подключения к ViPNet EPP Сервер. Способ работы ViPNet EPP Агент определяется лицензией. Управление и настройка каждого автономного ViPNet EPP Агент выполняется индивидуально в локальной консоли управления агента. Для включения модулей средств защиты лицензия и база правил должны быть загружены непосредственно на каждый автономный ViPNet EPP Агент.

  Подробнее см. в разделах Модели использования и принципы работы (см. Модели управления и принципы работы), База правил (см. База правил (политика безопасности)), Лицензирование.

- **Графическая консоль управления ViPNet EPP Агент для ОС GNU/Linux**

  Для локального управления ViPNet EPP Linux Агент реализован графический интерфейс пользователя, который теперь является основным средством локального управления агентом.

  Подробнее см. в документе «ViPNet EPP Linux. Руководство администратора» в разделе «Управление с помощью графической консоли управления».

- **Изменения в списке поддерживаемых ОС GNU/Linux для ViPNet EPP Агент**

  Реализована поддержка работы ViPNet EPP Linux Агент в ОС новых версий:

  - Astra Linux Special Edition 1.7.5;
  - РЕД ОС 7.3.4 «Муром» Рабочая станция, стандартная редакция;
  - Debian Linux 12 (bookworm).

  Список всех поддерживаемых ОС GNU/Linux и версий поддерживаемых ядер см. в документе «ViPNet EPP Linux. Руководство администратора» в разделе «Требования к установке ViPNet EPP Агент».

- **Изменения в списке поддерживаемых ОС Windows для ViPNet EPP Сервер и ViPNet EPP Агент**

  Реализована поддержка работы ViPNet EPP в ОС новых версий: Windows 10 Pro версия 22H2, Windows 11 Pro версия 23H2 и Windows Server 2022 Standard и Datacenter версия 21H2.

Список всех поддерживаемых ОС Windows см. в разделах Требования к установке ViPNet EPP Сервер и Требования к установке ViPNet EPP Агент.

- **Обновление ViPNet EPP**

  Обновление ViPNet EPP до версии 1.7.0 возможно только с версии 1.6.0. Обновление с более старых версий должно выполняться по определенной схеме.

  Подробнее см. в разделе Порядок обновления ViPNet EPP версии 1.6.0 до версии 1.7.0 (см. Порядок обновления ViPNet EPP версии 1.5.2 и выше до версии 1.8.0) и в документе «ViPNet EPP Linux. Руководство администратора» в аналогичном разделе.

- **Изменения в установке ViPNet EPP Агент для ОС Windows**

  Теперь при установке ViPNet EPP Windows Агент нужно выбрать способ работы ViPNet EPP Агент: работа под управлением сервера или автономно.

  Ознакомиться и принять лицензионное соглашение теперь можно при первом запуске после установки ViPNet EPP Агент.

  Подробнее см. в разделах Установка ViPNet EPP Агент вручную.

- **Настройка типов регистрируемых событий в журнале аудита ViPNet EPP Агент**

  Теперь в ViPNet EPP Агент вы можете выбрать типы событий, которые будут регистрироваться в журнале аудита.

  Подробнее см. в разделе Настройка типов регистрируемых событий в журнале аудита.

- **Изменения в интерфейсе ViPNet EPP для ОС Windows**

  Настройки политики аудита для защищаемых узлов с ViPNet EPP Windows Агент перенесены в интерфейсе ViPNet EPP Windows Сервер в раздел **Базы правил** и при редактировании базы правил доступны для настройки в разделе **Обнаружение и предотвращение вторжений** > **Политики аудита.** В интерфейсе ViPNet EPP Windows Агент политики аудита доступны в разделе **Обнаружение и предотвращение вторжений** > **Политики аудита.**

  Подробнее см. в разделе Настройка политик аудита.

- **Изменение в ролевой модели**

  Теперь роли управления ViPNet EPP Windows Сервер (Администратор и Аудитор ViPNet EPP) имеют доступ к ViPNet EPP Linux Агент.

  Подробнее см. в разделе Ролевая модель.

- **Расширение возможностей управления доверенной загрузкой на защищаемых узлах с ViPNet EPP Агент для ОС GNU/Linux**

  Теперь для защищаемых узлов с ViPNet EPP Linux Агент в ViPNet EPP Windows Сервер доступны следующие действия по управлению ViPNet SafeBoot:

  - Управление учетными записями пользователей.
  - Управление корневыми сертификатами и списками отозванных сертификатов (CRL).
  - Обновление ПО ViPNet SafeBoot.

  Подробнее см. в разделе Управление доверенной загрузкой.

- **Исправление ошибок**

  Устранены ошибки, выявленные в процессе эксплуатации предыдущей версии.

Что нового в версии 1.6.0

Краткий обзор изменений и новых возможностей ViPNet EPP версии 1.6.0 по сравнению с версией 1.5.2:

- **Реализован ViPNet EPP Сервер для ОС GNU/Linux (ViPNet EPP Linux Сервер)**

  Текущая версия ViPNet EPP Linux Сервер работает в ОС Astra Linux Special Edition 1.7.4. Реализовано управление следующими средствами защиты на защищаемых узлах:

  - Персональный межсетевой экран.
  - Обнаружение вторжений.
  - Предотвращение сетевых вторжений.
  - Обнаружение аномалий с помощью критериев.
  - Отслеживание работы антивирусов.

  К ViPNet EPP Linux Сервер для управления могут быть подключены только ViPNet EPP Linux Агент.

  Подробнее см. в документе «ViPNet EPP Linux. Руководство администратора» в разделе «Основные функции».

- **Изменения в списке поддерживаемых ОС GNU/Linux для ViPNet EPP Агент (ViPNet EPP Linux Агент)**

  Реализована поддержка работы ViPNet EPP Linux Агент в ОС:

  - Astra Linux Special Edition 1.7.4, ядро Linux 5.15.0-70-generic #astra2+ci6;
  - Альт СП Рабочая станция релиз 10, ядро Linux 6.1.29-un-def-alt1;
  - Альт Рабочая станция 10.1, ядро Linux 5.10.164-std-def-alt1;
  - РЕД ОС 7.3.2 «Муром» Рабочая станция, стандартная редакция, ядро Linux 5.15.87-1.el7.3.x86_64;
  - РЕД ОС 7.3.3 «Муром» Рабочая станция, стандартная редакция, ядро Linux 5.15.125-1.el7.3.x86_64.

  Список всех поддерживаемых ОС GNU/Linux см. в документе «ViPNet EPP Linux. Руководство администратора» в разделе Требования к установке ViPNet EPP Агент.

- **Изменения в списке поддерживаемых ОС Windows для ViPNet EPP Сервер и ViPNet EPP Агент**

  Прекращена поддержка работы ViPNet EPP в ОС Windows 8.1 (только для ViPNet EPP Сервер и ViPNet EPP Серверная консоль) и Windows Server 2012.

Список всех поддерживаемых ОС Windows см. в разделах Требования к установке ViPNet EPP Сервер и Требования к установке ViPNet EPP Агент.

- **Изменения в установке ViPNet EPP Сервер и ViPNet EPP Агент для ОС Windows**

  Теперь перед первой установкой ViPNet EPP Сервер необходимо вручную установить СУБД PostgreSQL 12.13 и Microsoft Visual C++ 2015-2022 Redistributable Package (x64), если они не установлены. Эти компоненты входят в комплект поставки. Список всех необходимых компонентов см. в разделе Требования к установке ViPNet EPP Сервер.

  Также переработан мастер установки для более удобной установки ViPNet EPP Сервер и ViPNet EPP Агент.

  Подробнее см. в разделах Установка ViPNet EPP Сервер и ViPNet EPP Серверная консоль и Установка ViPNet EPP Агент вручную.

- **Автоматическое подключение защищаемых узлов к ViPNet EPP Сервер**

  Чтобы не подключать защищаемые узлы к ViPNet EPP Сервер вручную, теперь вы можете настроить автоматическое подключение защищаемых узлов. Настройка недоступна на ViPNet EPP Linux Сервер.

  Подробнее см. в разделе Настройка автоматического подключения защищаемых узлов.

- **Сетевой доступ с нулевым доверием (ZTNA)**

  Реализована технология сетевого доступа с нулевым доверием, позволяющая на защищаемых узлах с установленной программой ViPNet Client 5 дополнительно контролировать доступ к ресурсам защищенной сети ViPNet и разрешать его только при условии соответствия политикам безопасности, заданным для защищаемых узлов. Политики ZTNA настраиваются на ViPNet EPP Сервер и отправляются на ViPNet EPP Агент в составе базы правил. На защищаемом узле можно просмотреть статус выполнения политики ZTNA. Настройка политики ZTNA недоступна в ViPNet EPP Linux Сервер.

  Подробнее см. в разделе Сетевой доступ с нулевым доверием (см. Сетевой доступ с нулевым доверием (ZTNA)).

- **Блокировка доступа к вредоносным веб-ресурсам**

  Реализована возможность на защищаемых узлах с ОС Windows блокировать доступ к веб-ресурсам с вредоносным, фишинговым и спам содержимым. Для этого в ViPNet EPP Агент применяются веб-фильтры. Веб-фильтры настраиваются на ViPNet EPP Сервер и отправляются на ViPNet EPP Агент в составе базы правил. Функция недоступна для защищаемых узлов с ViPNet EPP Linux Агент.

  Подробнее см. в разделе Блокировка доступа к вредоносным веб-ресурсам.

- **Блокирование бесфайловых атак типа Hollowing и Doppelganging**

  Локальными правилами HIPS реализована возможность обнаруживать и предотвращать бесфайловые атаки на защищаемых узлах с ОС Windows, относящиеся к методам Process Hollowing и Process Doppelganging (см. Обнаружение и предотвращение бесфайловых атак). Отслеживание бесфайловых атак настраивается на ViPNet EPP Сервер и отправляется на ViPNet EPP Агент в составе базы правил. Функция недоступна для защищаемых узлов с ViPNet EPP Linux Агент.

Подробнее см. в разделе Обнаружение и предотвращение бесфайловых атак.

- **Настройка TLS-инспекции**

  Правилами HIDS реализована функция TLS-инспекции, при включении которой на защищаемых узлах с ОС Windows будет расшифровываться HTTPS-трафик для возможности проверки его правилами HIPS и веб-фильтрами. По умолчанию TLS-инспекция включена. Функция недоступна для защищаемых узлов с ViPNet EPP Linux Агент.

  Подробнее см. в разделе Настройка TLS-инспекции.

- **Расширение возможностей управления доверенной загрузкой на защищаемых узлах**

  В ViPNet EPP Сервер добавлены следующие действия по управлению ViPNet SafeBoot на защищаемых узлах:

  - Управление учетными записями пользователей.
  - Управление корневыми сертификатами и списками отозванных сертификатов (CRL).
  - Обновление ПО ViPNet SafeBoot.

  Действия недоступны для защищаемых узлов с ViPNet EPP Linux Агент.

  Подробнее см. в разделе Управление доверенной загрузкой.

- **Изменение настроек политик аудита по умолчанию**

  На ViPNet EPP Сервер обновлены настройки политик аудита по умолчанию для защищаемых узлов с ОС Windows.

  Подробнее см. в разделе Настройка политик аудита.

- **Создание в ViPNet EPP Агент пользовательских сетевых фильтров для защищенного трафика сети ViPNet и настройка справочников ViPNet**

  Теперь, если на защищаемом узле установлена программа ViPNet Client 5, администратору в ViPNet EPP Агент доступно создание пользовательских сетевых фильтров для трафика защищенной сети ViPNet (см. Настройка пользовательских сетевых фильтров), а также настройка пользовательских справочников адресов сети ViPNet, которые можно использовать при создании этих сетевых фильтров.

  Подробнее см. в разделе Персональный межсетевой экран.

- **Запрос журнала регистрации трафика с ViPNet EPP Агент**

  Теперь администратор ViPNet EPP Сервер может запрашивать с защищаемых узлов данные журнала регистрации трафика модулем Персональный межсетевой экран за заданный период времени и по определенным критериям. Также в настройки параметров системы добавлена настройка периода хранения отчетов журнала трафика (**Период удаления снимков трафика**) на ViPNet EPP Сервер.

  Подробнее см. в разделе Запрос журнала регистрации трафика с ViPNet EPP Агент.

- **Изменения в интерфейсе ViPNet EPP для ОС Windows**

  Оптимизированы некоторые названия и расположение настроек:

- Переименован режим персонального межсетевого экрана **Защищенная сеть** на **Корпоративная сеть**.
- Настройки правил предотвращения бесфайловых атак объединены в едином месте и при редактировании базы правил доступны для настройки в разделе **Обнаружение и предотвращение вторжений** > **Бесфайловые атаки.** Подробнее см. в разделе Настройка правил HIPS.

- **Изменение комплекта документации для пользователей**

  В комплект документации для пользователей добавлен новый документ «ViPNet EPP Linux. Руководство администратора», в котором содержится руководство по использованию ViPNet EPP Linux Сервер и ViPNet EPP Linux Агент. Раздел «Установка ViPNet EPP Агент Linux» и глава «Настройка ViPNet EPP Агент Linux» удалены из документа «ViPNet EPP. Руководство администратора».

- **Исправление ошибок**

  Устранены ошибки, выявленные в процессе эксплуатации предыдущей версии.

Что нового в версии 1.5.2

Краткий обзор изменений и новых возможностей ViPNet EPP версии 1.5.2 по сравнению с версией 1.5.1:

- **Изменения в списке поддерживаемых ОС для ViPNet EPP Linux Агент**

  Прекращена поддержка работы ViPNet EPP Агент в ОС CentOS 7.5.

  Реализована поддержка работы ViPNet EPP Агент в ОС: Astra Linux Special Edition 1.7.2 «Воронеж» и «Орел»; РЕД ОС 7.3.1 «Муром» Рабочая станция, стандартная редакция.

  Подробнее см. в разделе Требования к установке ViPNet EPP Агент.

- **Изменения в списке необходимых пакетов Microsoft Visual C++Redistributable Package для ViPNet EPP Агент Windows**

  Для установки ViPNet EPP Агент Windows теперь также требуются пакеты Microsoft Visual C++ 2015-2022 Redistributable Package (x86 и x64). Пакеты входят в комплект поставки ViPNet EPP.

  Подробнее см. в разделе Требования к установке ViPNet EPP Агент.

- **Исправление ошибок**

  Устранены ошибки, выявленные в процессе эксплуатации предыдущей версии.



Термины и сокращения

Application Control

Модуль, реализующий функции контроля приложений; объект лицензирования ViPNet EPP.

Behavior Analytics

Модуль, реализующий функцию обнаружения аномалий определенных типов (вход с систему, изменение реестра, запуск системных утилит и другие) методом поведенческого анализа.

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.

Hook

Механизм перехвата особой функцией событий (например, оконные сообщения, ввод с мыши или клавиатуры) до того, как они дойдут до программного компонента. Далее эта функция может реагировать на события, изменяя или дополняя поведение программных компонентов.

Personal Firewall

Модуль, реализующий функции персонального межсетевого экрана; объект лицензирования ViPNet EPP.

SafeBootMC

Модуль, реализующий функции управления ViPNet SafeBoot, установленными на защищаемых узлах; 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 EndPoint Protection

Программный комплекс, предназначенный 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 SafeBoot

Предназначен для идентификации и аутентификации пользователей, разграничения доступа на основе ролей, а также организации доверенной загрузки операционной системы.

Обеспечивает повышение уровня безопасности работы путем:

- Авторизации на уровне BIOS до загрузки основных компонентов операционной системы.
- Контроля целостности на уровне BIOS, защищаемых компонентов операционной системы и аппаратного обеспечения.
- Блокировки загрузки нештатной копии операционной системы.

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 TIAS

Система ViPNet TIAS (Threat Intelligence Analytics System) анализирует события информационной безопасности, поступающие от различных источников: ViPNet IDS NS, ViPNet IDS HS, ViPNet xFirewall, ViPNet EPP; автоматически выявляет инциденты информационной безопасности на основании потока этих событий и оперативно информирует заинтересованных лиц о произошедших инцидентах.

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 активностей 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.

Бесфайловая атака

Компьютерная атака с использованием различных методов внедрения в системные и пользовательские процессы ОС Windows, а также замены кода процесса с целью маскировки под легитимный процесс.

Глобальные правила HIPS

Правила формируются на ViPNet EPP Сервер и действуют в пределах одной базы правил; правила невозможно изменить на защищаемом узле.

Глобальные правила контроля приложений

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.

Защищенный трафик сети ViPNet

Поток IP-пакетов, зашифрованных с помощью программного обеспечения ViPNet Client 5.

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.

Категории угроз

Угрозы безопасности информации, сгруппированные по признаку назначения.

Например, категория угроз «Попытка DoS-атаки» включает несколько видов атак: HTTP GET, HTTP POST, TCP/SYN, UDP-flood и другие. Список категорий угроз определен в базе правил и обновляется вместе с ней.

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.

Контроль приложений

Модуль защиты ViPNet EPP Агент. Управляет запуском и активностью приложений, доступом приложений к файлам, реестру ОС Windows, процессам и параметрам командной строки; предотвращает установку и запуск вредоносного программного обеспечения; реализовано модулем AppC.

Критерий обнаружения аномалий

Временной интервал и список правил HIDS одного типа, для которых локальная или сетевая активность на защищаемом узле нетипична.

Машинное обучение

Класс методов искусственного интеллекта (математических, статистических и вычислительных) для разработки алгоритмов, способных решить задачу не прямым способом, а на основе поиска закономерностей в разнообразных входных данных.

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.

Поведенческий анализ

Метод обнаружения аномалий ViPNet EPP Сервер. Основан на построении модели нормальной активности защищаемого узла с помощью машинного обучения; реализован в модуле BA.

Политика безопасности

Совокупность настроек модулей, системных и пользовательских правил, регулирующая безопасность защищаемых узлов.

Пользовательские правила контроля приложений

Правила контроля приложений, создаваемые и действующие локально на защищаемом узле. Обновление базы правил на защищаемом узле не изменяет пользовательские правила контроля приложений.

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 доступа

Правила доступа приложений определяют взаимодействие приложения с объектами Windows: файлами, процессами, реестром и командным интерпретатором ОС.

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.

Списки контроля приложений

Правила запуска приложений, заданные в черном и белом списках. Запуск и активность приложений из черного списка запрещена. Запуск приложений из белого списка разрешен, а их активность определяется правилами доступа.

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.