



ViPNet EndPoint Protection

Руководство пользователя

Версия продукта: 1.8.0

© АО «ИнфоТеКС», 2026

ФРКЕ.00238-01 34 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.....	4
Для кого предназначен документ	5
Соглашения документа	6
О программном комплексе	7
Обратная связь.....	8
 Глава 1. Как работать с ViPNet EPP	9
Открытие сеанса работы пользователя.....	10
Смена пароля при первом подключении.....	11
Режимы работы модулей защиты	12
Просмотр режимов и статуса защиты	13
Просмотр статуса выполнения политики ZTNA	15
Просмотр журнала событий.....	17
Завершение сеанса работы пользователя	21
Уведомления о срабатывании модулей защиты	22
Обновление ViPNet SafeBoot	23
Для администраторов и аудиторов	24
 Приложение А. Термины и сокращения	25



Введение

Для кого предназначен документ	5
Соглашения документа	6
О программном комплексе	7
Обратная связь	8

Для кого предназначен документ

Документ предназначен для пользователей персональных компьютеров корпоративных сетей с ОС Windows, защиту которых от [угроз безопасности информации](#) обеспечивает программный комплекс ViPNet EndPoint Protection (далее — ViPNet EPP). В документе приведены сведения о режимах работы модулей защиты ViPNet EPP, просмотре данных о срабатывании модулей защиты и просмотре журнала событий



Внимание! При возникновении любых неисправностей в работе ViPNet EPP необходимо сообщить об этом администратору ViPNet EPP.

Соглашения документа

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



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

О программном комплексе

Персональные компьютеры пользователей и корпоративные серверы являются основными объектами информационной инфраструктуры организаций, подверженными угрозам безопасности информации.

ViPNet EPP выявляет нарушения безопасности информации и блокирует **угрозы** с помощью 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 других приложений; предотвращает установку и запуск вредоносного программного обеспечения.
- Обнаружение и предотвращение вторжений — обнаруживает различные сетевые угрозы и блокирует их.
- ZTNA — отслеживает выполнение политики ZTNA, заданной администратором в ViPNet EPP Сервер. 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 политики ZTNA на защищаемом узле. Если на защищаемом узле получены данные об исключениях из политики ZTNA, при невыполнении политики ZTNA ресурсы защищенной сети ViPNet из списка исключений останутся доступными.

ViPNet EPP применяется для защиты отдельных компонентов информационной инфраструктуры организаций — персональных компьютеров пользователей и корпоративных серверов.

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

Как работать с ViPNet EPP

Открытие сеанса работы пользователя	10
Режимы работы модулей защиты	12
Просмотр статуса выполнения политики ZTNA	15
Просмотр журнала событий	17
Завершение сеанса работы пользователя	21
Уведомления о срабатывании модулей защиты	22
Обновление ViPNet SafeBoot	23
Для администраторов и аудиторов	24

Открытие сеанса работы пользователя

ViPNet EPP запускается автоматически при старте ОС Windows. Чтобы открыть сеанс работы ViPNet EPP с учетной записью пользователя:

- 1 Выполните одно из действий:
 - В меню **Пуск** начните вводить **ViPNet EndPoint Protection** и запустите найденную программу.
 - Щелкните значок ViPNet EPP  в области уведомлений панели задач.
- 2 В окне аутентификации введите параметры входа:
 - Введите имя учетной записи и пароль, которые вам сообщил администратор ViPNet EPP.
 - Чтобы при последующем запуске ViPNet EPP не вводить имя учетной записи и пароль, установите флажок **Запомнить меня**.

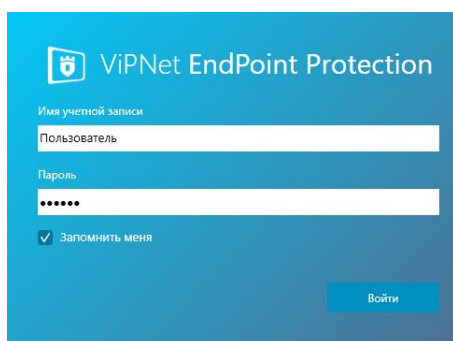


Рисунок 1. Вход в ViPNet EPP с учетной записью пользователя

- 3 Нажмите **Войти**.



Внимание! Если вы три раза подряд введете неверные данные учетной записи, возможность входа в ViPNet EPP будет заблокирована на три минуты и в окне аутентификации будет выведено сообщение  **Блокировка доступа пользователей.**

- 4 Если запрошена смена пароля, смените его (см. [Смена пароля при первом подключении](#)).

При успешной аутентификации откроется [инфопанель ViPNet EPP](#).

Смена пароля при первом подключении

При первом подключении пользователя после создания его учетной записи, а также после обновления ViPNet EPP на версию 1.8 необходимо сменить пароль учетной записи. Для этого в процессе открытия сеанса пользователя в окне **Смена пароля**:

1 Введите новый пароль в соответствии с требованиями:

- 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 **!@#\$%^&*()_+=;:'",.<>/?\|`~[]{}.**

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.

2 Нажмите **Готово**.

Режимы работы модулей защиты

Возможность использования модулей защиты определяется установленной лицензией. В таблице ниже приведено описание режимов работы модулей защиты.

Пользователь ViPNet EPP может просматривать [режимы на инфопанели](#) и в области уведомлений. О режиме работы модуля ZTNA см. в разделе [Просмотр статуса выполнения политики ZTNA](#).

Таблица 1. Режимы работы персонального межсетевого экрана

Режим	Описание режима
Полная блокировка трафика	Блокируются любые входящие и исходящие открытые соединения, кроме локального трафика. Компьютер не взаимодействует с внешними сетями.
Публичная сеть	Режим рекомендуется использовать при подключении к общественной сети. Режим с максимальной степенью защиты, определяемой корпоративными правилами безопасности.
Частная сеть	Режим рекомендуется использовать при подключении к частной сети, например, из дома. Степень защиты определяется корпоративными правилами безопасности. Дополнительно, для учета особенностей фильтрации трафика на компьютере, администратор ViPNet EPP может создавать локальные фильтры .
Корпоративная сеть	Режим рекомендуется использовать при подключении к частной сети с низким уровнем угроз безопасности внутри периметра сети. Степень защиты определяется только локальными фильтрами, которые может создавать администратор ViPNet EPP.
Отключено	Персональный межсетевой экран отключен и не влияет на трафик.

Таблица 2. Режимы работы контроля приложений

Режим	Описание режима
Блокировать	Запуск приложений, не входящих в белый и черный списки, блокируется. Попытки запуска приложений фиксируются в журнале событий.
Разрешать	Запуск приложений, не входящих в белый и черный списки, разрешен.
Отключено	Контроль приложений отключен и не влияет на работу приложений.

Таблица 3. Обнаружение вторжений работает всегда. Режимы работы предотвращения вторжений

Режим	Описание режима
Усиленный	Используется полный набор правил предотвращения вторжений. Использование режима может приводить к снижению производительности компьютера.

Режим	Описание режима
Базовый	Используется оптимальный набор правил предотвращения вторжений, обеспечивающий защиту в большинстве случаев.
Минимальный	Используется минимальный набор правил предотвращения вторжений, защищающих от наиболее критичных атак.
Отключено	Предотвращение вторжений отключено и не влияет на работу компьютера.

Просмотр режимов и статуса защиты

На инфопанели вверху отображается один из статусов защиты ViPNet EPP:

- Надпись  **Устройство защищено** на зеленом фоне — на защищаемом узле модули защиты работают в штатном режиме.
- Надпись  **Пониженный уровень защиты** на желтом фоне — может возникать из-за отсутствия подключения к ViPNet EPP Сервер, отключения некоторых модулей защиты или прогнозируемых проблем с лицензией.
- Надпись  **Защита отключена** на красном фоне — может возникать из-за отключения всех модулей защиты, отсутствия лицензии или проблем с текущей, отсутствия базы правил, ошибки подключения к ViPNet EPP Сервер.

Для желтого и красного статусов отображается информация о возможных причинах проблемы. Если проблему разрешить не получается, обратитесь к администратору ViPNet EPP.

Ниже вы можете посмотреть установленные режимы работы.

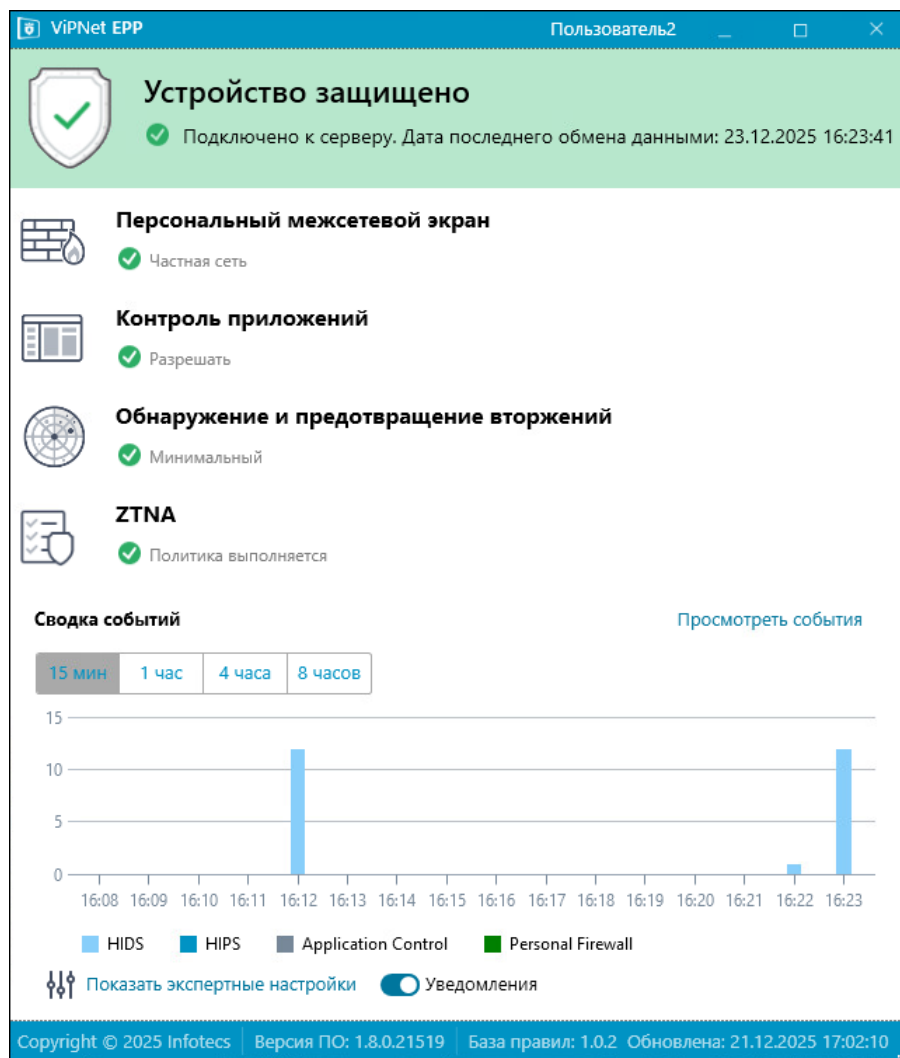


Рисунок 2. Инфопанель ViPNet EPP

Чтобы посмотреть режимы и статус защиты ViPNet EPP в области уведомлений панели задач ОС Windows, в области уведомлений правой кнопкой мыши щелкните значок ViPNet EPP .

Просмотр статуса выполнения политики ZTNA

Функция недоступна для защищаемых узлов с автономным ViPNet EPP Агент.

Политика ZTNA устанавливаются централизованно с ViPNet EPP Сервер. Вы можете просмотреть статус выполнения политики ZTNA одним из способов:

- На инфопанели в разделе **ZTNA**.
- В области уведомлений.

Чтобы просмотреть подробную информацию о выполнении политики ZTNA на инфопанели, щелкните **ZTNA**.

Статусы выполнения политики ZTNA могут быть следующими:

- **Политика выполняется** — проверка успешно пройдена в соответствии со всеми заданными правилами политики ZTNA. Если на защищаемом узле установлена программа ViPNet Client 5, доступ к защищенной сети ViPNet разрешен.
- **Политика не выполняется** — проверка по заданным правилам политики ZTNA не пройдена. Ниже в списке будут перечислены правила, параметрам которого не соответствует защищаемый узел. Если на защищаемом узле установлена программа ViPNet Client 5 и включен персональный межсетевой экран, доступ к ресурсам 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.

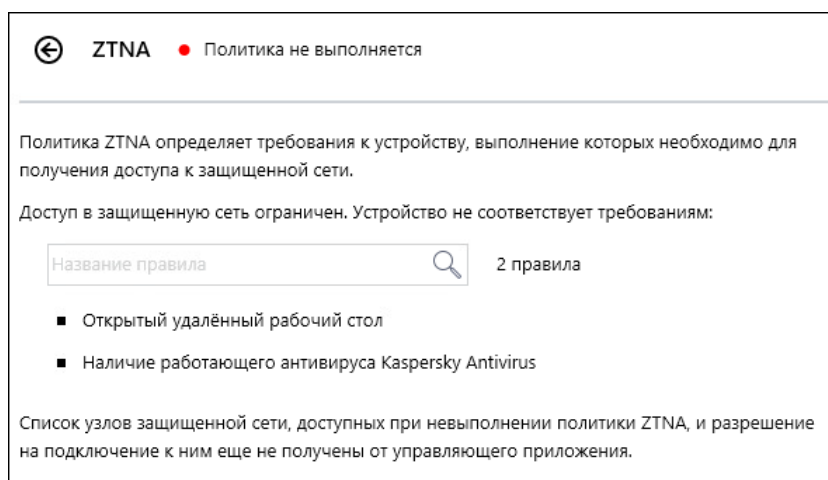


Рисунок 3. Политика ZTNA не выполняется

Чтобы разблокировать доступ к ресурсам защищенной сети ViPNet, выполните требования политики ZTNA, указанные в подробной информации. При возникновении проблем обратитесь к администратору ViPNet EPP.

- **Политика не назначена** — политики ZTNA выключены либо для персонального сетевого экрана выбран режим работы **Отключено** (см. [Режимы работы модулей защиты](#)). Доступ к защищенной сети ViPNet дополнительно не контролируется.

Чтобы просмотреть статус выполнения политики ZTNA в области уведомлений панели задач ОС Windows, в области уведомлений правой кнопкой мыши щелкните значок ViPNet EPP  и выберите **ZTNA**.

Просмотр журнала событий

События информационной безопасности, идентифицированные модулями защиты ViPNet EPP, регистрируются в журнале событий. Чтобы просмотреть журнал событий:

- 1 На инфопанели нажмите **Просмотреть события**.

Дата, время	Идентификатор	Описание	Модуль	Попытки
23.12.2025 18:36:25	400072	Отключение задачи плани...	HIDS	1
23.12.2025 16:02:37	300761	Загрузка библиотеки через "...	HIDS	1
23.12.2025 12:36:42	300761	Загрузка библиотеки через "...	HIDS	1
23.12.2025 06:04:34	3308323	AM CURRENT_EVENTS	HIDS	1
23.12.2025 06:04:34	300699	Загрузка библиотеки через...	HIDS	1
23.12.2025 05:22:04	750000	Контроль установки прилож...	HIDS	2
23.12.2025 05:19:21	3308323	AM CURRENT_EVENTS	HIDS	1
23.12.2025 04:12:42	300761	Загрузка библиотеки через "...	HIDS	1
22.12.2025 23:11:19	300699	Загрузка библиотеки через...	HIDS	1
22.12.2025 23:11:17	3308323	AM CURRENT_EVENTS	HIDS	1
22.12.2025 18:36:21	400072	Отключение задачи планир...	HIDS	1
22.12.2025 15:35:01	300761	Загрузка библиотеки через "...	HIDS	1
22.12.2025 12:36:36	300761	Загрузка библиотеки через "...	HIDS	3
22.12.2025 06:04:40	300699	Загрузка библиотеки через...	HIDS	1
22.12.2025 06:04:39	3308323	AM CURRENT_EVENTS	HIDS	1
22.12.2025 03:53:09	300761	Загрузка библиотеки через "...	HIDS	1
22.12.2025 00:35:01	300699	Загрузка библиотеки через...	HIDS	1
22.12.2025 00:35:00	3308323	AM CURRENT_EVENTS	HIDS	1

Copyright © 2025 Infotecs | Версия ПО: 1.8.0.21519 | База правил: 1.0.2 | Обновлено: 21.12.2025 17:02:10

Рисунок 4. Журнал событий ViPNet EPP

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.
- **Описание** — описание события.
- **Модуль** — модуль, в котором сработало правило:
 -  PFW — персональный межсетевой экран.
 -  AppC — контроль приложений.
 -  HIDS — обнаружение вторжений.
 -  HIPS — предотвращение вторжений.
- **Попытки** — количество повторений события на устройстве в течение заданного периода опроса. Повторные события определяются по одинаковому идентификатору сработавшего правила.



Примечание. 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**.

- 2 Чтобы просмотреть сведения о событии, дважды щелкните строку с событием в журнале — на панели справа на вкладке **Сработавшее правило** будут отображены сведения о правиле. Для ряда критических и опасных событий будут указаны рекомендуемые действия в связи возникновением события.

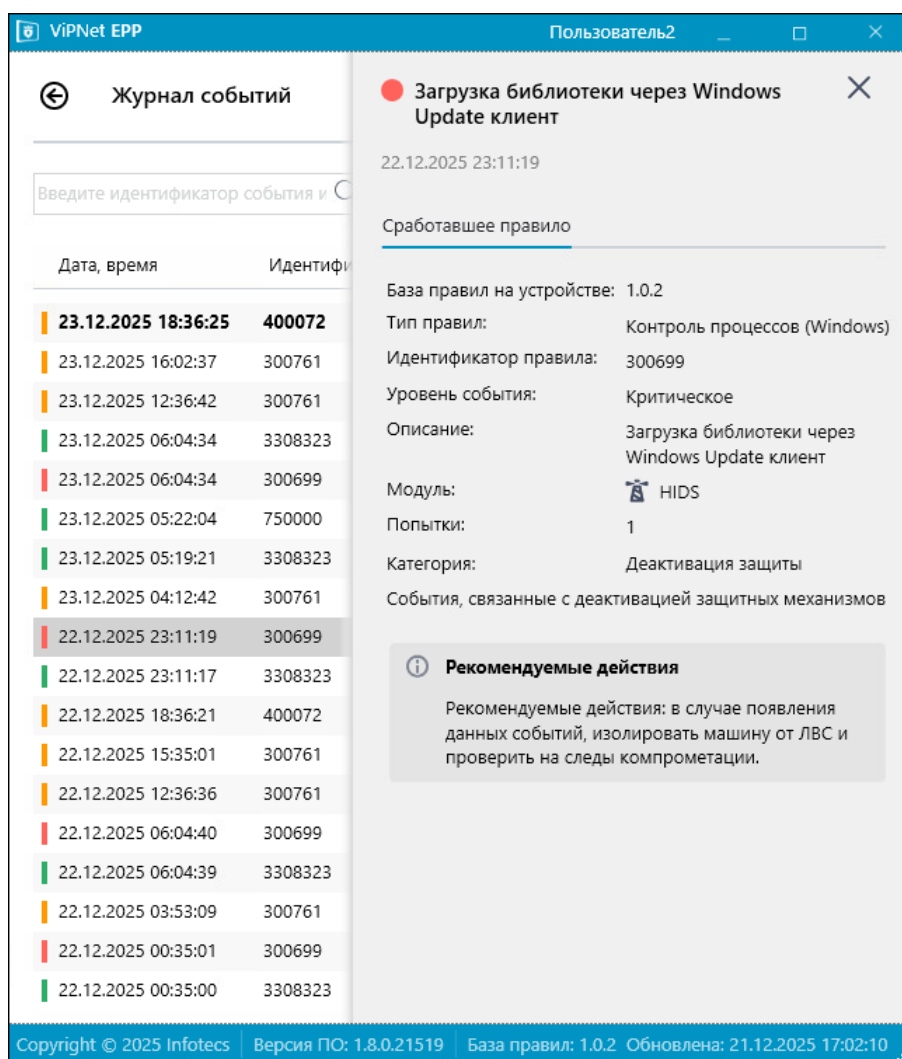


Рисунок 5. Сведения о событии

3 Для поиска событий в журнале используйте фильтр:

3.1 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.

Тип правил:

Все

События модуля:

Все

☐ Только события, не доставленные на сервер

Уровень событий

☒ Информационное

☒ Важное

☒ Опасное

☒ Критическое

Временной период

События с: 22.12.2025 00 : 00

по: 23.12.2025 23 : 59

[Сбросить](#) [Применить](#) [Отменить](#)

Рисунок 6. Параметры фильтрации журнала событий

3.2 Нажмите Применить.

Завершение сеанса работы пользователя



Примечание. После завершения сеанса пользователя модули защиты ViPNet EPP продолжают работу.

Чтобы завершить текущий сеанс работы пользователя, в области уведомлений панели задач ОС Windows правой кнопкой мыши щелкните значок ViPNet EPP  и выберите **Выход**.

Уведомления о срабатывании модулей защиты

Если в настройках центра уведомлений ОС Windows включено получение уведомлений от приложений и других отправителей и на инфопанели ViPNet EPP включены  **Уведомления**, вы будете получать всплывающие уведомления:

- о срабатывании блокирующих правил контроля приложений и веб-фильтров ViPNet EPP;
- о смене статуса выполнения политики ZTNA.

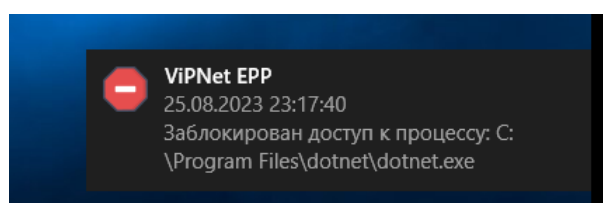


Рисунок 7. Пример уведомления о срабатывании блокирующих правил контроля приложений

Обновление ViPNet SafeBoot

Если на вашем компьютере установлен программный комплекс «Программный модуль доверенной загрузки ViPNet SafeBoot» (далее — ViPNet SafeBoot), вы можете получать из ViPNet EPP Сервер обновления ViPNet SafeBoot. Обновления применяются после перезагрузки.

Если в настройках центра уведомлений ОС Windows включено получение уведомлений от приложений и других отправителей и на инфопанели ViPNet EPP включены  **Уведомления**, при получении обновления ViPNet SafeBoot появится всплывающее уведомление.



Внимание! Перед перезагрузкой убедитесь, что к компьютеру не подключен USB-носитель с установочным пакетом ViPNet SafeBoot.

Чтобы обновление ViPNet SafeBoot применилось, перезагрузите компьютер. Из-за применения обновления ViPNet SafeBoot ваш компьютер будет загружаться более длительное время.

Для администраторов и аудиторов

Чтобы завершить сеанс работы пользователя и войти в программу с учетной записью администратора или аудитора ViPNet EPP:

- 1 На инфопанели нажмите  **Показать экспертные настройки**.
- 2 Подтвердите смену учетной записи, нажав **Да**.

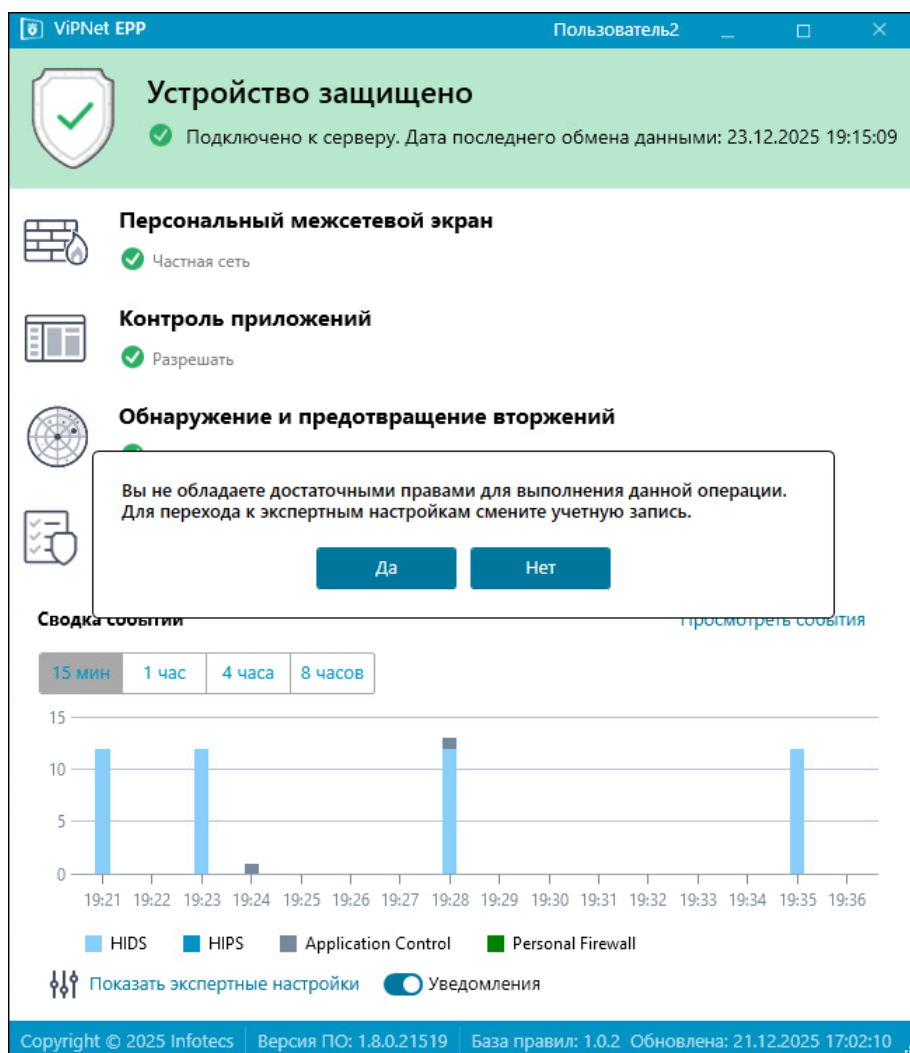


Рисунок 8. Завершение сеанса пользователя ViPNet EPP и смена учетной записи

- 3 Введите учетные данные администратора или аудитора ViPNet EPP.



Термины и сокращения

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.

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.

Безопасность информации

Состояние информации, обрабатываемой в информационной системе, при котором сохраняется её конфиденциальность, целостность и доступность.

Правила доступа

Правила, определяющие доступ приложения из белого списка к файлам, веткам реестра Windows, процессам и параметрам командной строки других приложений. Для файлов и реестра можно разрешить или запретить создание, чтение, изменение, удаление файла или ветки реестра. Для процессов — разрешить или запретить запуск исполняемого файла процесса. Для командной строки — разрешить или запретить использование отдельных аргументов командной строки приложения.

Правила обнаружения вторжений

Основаны на сигнатурном и эвристическом методах анализа трафика. Сигнатурные правила содержат сигнатуры, позволяющие определить сетевую атаку по конкретным, свойственным ей признакам. Эвристические правила отслеживают изменения в различных журналах ОС Windows и приложений, а также обнаруживают аномальный сетевой трафик.

Сетевой фильтр

Правило обработки IP-пакета сетевого трафика на основании IP-адресов источника и получателя, протоколов, расписания (времени применения). По типу действия различают блокирующие и разрешающие сетевые фильтры.

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).

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

Списки приложений, установленных на компьютере пользователя. Запуск приложений из черного списка запрещен. Запуск приложений из белого списка разрешен, а их активность определяется [правилами доступа](#). Первоначально списки формируются при установке ViPNet EPP на компьютер пользователя. Списки могут изменяться администратором ViPNet EPP.

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.