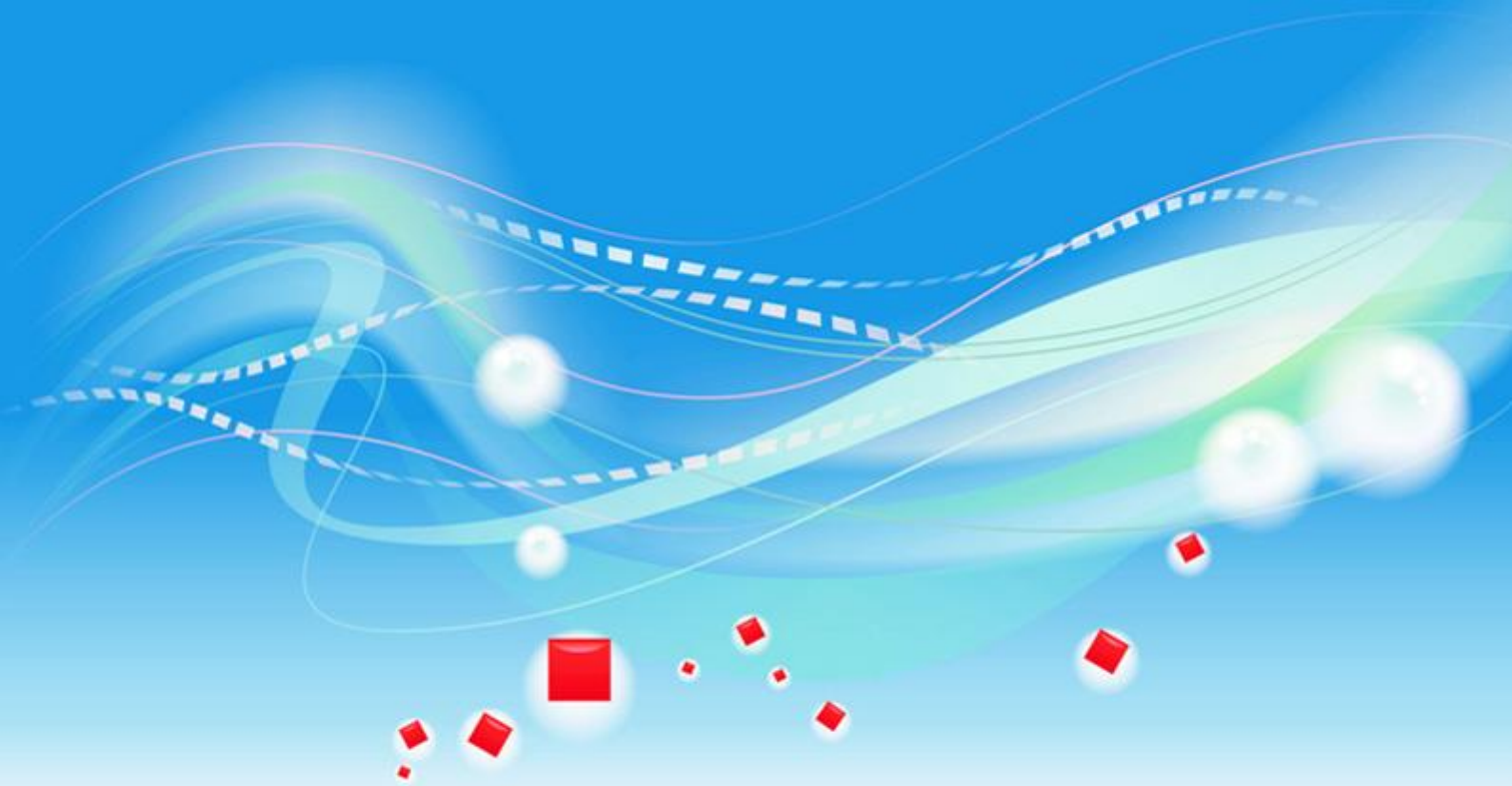


ViPNet Контроль приложений 4.2

Руководство пользователя

ViPNet Virtual Private Network

infotecs

ФРКЕ.00116-03 34 04

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В данном документе описывается назначение и применение программы ViPNet Контроль приложений, принцип и особенности работы, а также содержится информация о настройке и использовании возможностей данной программы.

Для кого предназначен документ

Документ предназначен для пользователей ПО ViPNet, в состав которого входит программа ViPNet Контроль приложений.

Предполагается, что читатель данного руководства имеет общее представление о сетевых технологиях.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю >	Иерархическая последовательность элементов. Например, пункты меню

Команда	или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О программе

Программа ViPNet Контроль приложений позволяет следить за сетевой активностью приложений, установленных на компьютере. Приложения, проявляющие сетевую активность (например, обращение к удаленному веб-узлу, передача файла по протоколу FTP, «прослушивание» сетевых портов или передача пакетов в сеть), регистрируются в программе «Контроль приложений», и в зависимости от выбора пользователя доступ таких приложений в сети блокируется или разрешается. «Контроль приложений» предоставляет защиту от таких угроз, как, например, несанкционированный доступ к пользовательским данным или запуск «шпионских» программ.

Программа «Контроль приложений» является компонентом программного обеспечения ViPNet Client, ViPNet Coordinator, ViPNet Personal Firewall и ViPNet Office Firewall. При этом программа «Контроль приложений» входит в состав ViPNet Client и ViPNet Coordinator, только если это определено регистрационным файлом, а в состав ViPNet Personal Firewall и ViPNet Office Firewall программа «Контроль приложений» входит всегда.

Примечание. При работе с ПО ViPNet VPN программа «Контроль приложений» входит только в состав ViPNet Coordinator.

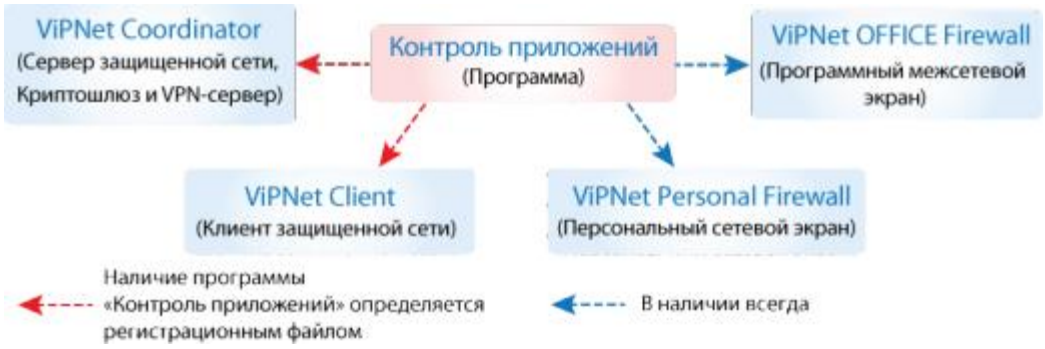


Рисунок 1: ПО ViPNet, в состав которого входит «Контроль приложений»

Системные требования

Программа ViPNet Контроль приложений устанавливается только в комплекте с другим ПО ViPNet, поэтому минимальные требования к компьютерам для успешной работы данной программы определяются требованиями ПО, в состав которого она входит.

Таблица 3. Минимальные системные требования для установки ПО ViPNet

Системные требования	**ПО ViPNet: Coordinator, Office Firewall**	**ПО ViPNet: Client, Personal Firewall**
Операционная система	Microsoft Windows XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Server 2012 (64-разрядная).	
	Примечание. Для операционной системы должен быть установлен самый последний пакет обновлений.	
Прикладное ПО	При использовании Internet Explorer – версия 6.0 или выше;	
	Отсутствие других программных межсетевых экранов (Firewall).	
Процессор	Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.	
Объем оперативной памяти	Не менее 1024 Мбайт.	Не менее 512 Мбайт.
Свободное место на жестком диске	Не менее 300 Мбайт при работе с ViPNet Registration Point.	Не менее 150 Мбайт.
	Не менее 1000 Мбайт при работе с ViPNet Coordinator.	
Сетевые интерфейсы	Любые, с поддержкой IPv4.	Любые, с поддержкой IPv4.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание комплекса ViPNet CUSTOM http://www.infotecs.ru/products/line/custom.php.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/vpn/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Форум ОАО «ИнфоТеКС» http://www.infotecs.ru/forum.
- 8 (495) 737-6196 — «горячая линия» службы технической поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения http://infotecs.ru/products/disclosure.php. Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru.

1

Общие положения

Принцип работы программы

Программа «Контроль приложений» позволяет обнаружить сетевую активность приложений на компьютере, а именно:

- Попытки создания исходящих соединений.
- Попытки открытия портов для входящих соединений.
- Отправку пакетов без предварительного создания соединения.

В случае обнаружения сетевой активности появляется окно с сообщением об активности приложения. В этом окне можно разрешить или запретить приложению доступ в сеть. Программа позволяет задать правила контроля приложений, согласно которым приложениям автоматически разрешается или запрещается выполнение каких-либо операций в сети, а также настроить работу программы в неинтерактивном режиме (см. «Неинтерактивный режим» на стр. 63).

Рисунок 2: Принцип работы программы ViPNet Контроль приложений

Если пользователь определил, разрешить или запретить приложению работать с сетью, данное приложение регистрируется программой «Контроль приложений». Это значит, что выбранное действие запоминается программой «Контроль приложений» и выполняется при каждой следующей сетевой активности данного приложения.

Уровни полномочий при работе с ViPNet Контроль приложений

При работе с ПО ViPNet CUSTOM возможность изменения настроек программы «Контроль приложений» зависит от уровня полномочий пользователя сетевого узла (см. «Полномочия пользователя» на стр. 63). Уровень полномочий задается администратором сети ViPNet в программе ViPNet Administrator. Подробнее о полномочиях при работе с ПО ViPNet смотрите в документе «Классификация полномочий. Приложение к документации ViPNet».

При работе с ПО ViPNet VPN, ViPNet Personal Firewall или ViPNet Office Firewall все возможности программы «Контроль приложений» доступны.

Примечание. При необходимости выполнить недоступные настройки обратитесь к администратору сети ViPNet (см. «Администратор сети ViPNet» на стр. 62). Подробнее о возможности входа под учетной записью администратора см. раздел Вход в программу от имени администратора (на стр. 46).

При работе с ПО ViPNet CUSTOM, а именно на сетевом узле с установленным ПО ViPNet Client или Coordinator:

- Если для сетевого узла (см. «Сетевой узел ViPNet» на стр. 63) задан максимальный уровень полномочий, то все возможности программы «Контроль приложений» будут доступны.
- Если для сетевого узла задан минимальный или средний уровень полномочий, будут действовать следующие ограничения:
  - Запрещено изменять параметры в разделе **Настройка**.
  - Запрещено изменять настройки в разделе **Журнал событий > Настройка журнала** (за исключением параметров группы **Отображение журнала событий**).
  - Запрещено изменять состав списков запрещенных и разрешенных приложений.
  - Запрещено отключать программу ViPNet Контроль приложений (в меню **Сервис** недоступны пункты **Отключить контроль приложений** и **Выход**).

Подробнее об ограничениях при специальном уровне полномочий см. документ «Классификация полномочий. Приложение к документации ViPNet».

Примечание. Если на сетевом узле принято обновление ключевой информации, ограничивающее полномочия пользователя, то ограничения в программе «Контроль приложений» вступят в силу только после перезапуска этой программы.

Интерфейс программы ViPNet Контроль приложений

Внешний вид окна программы ViPNet Контроль приложений представлен на следующем рисунке:

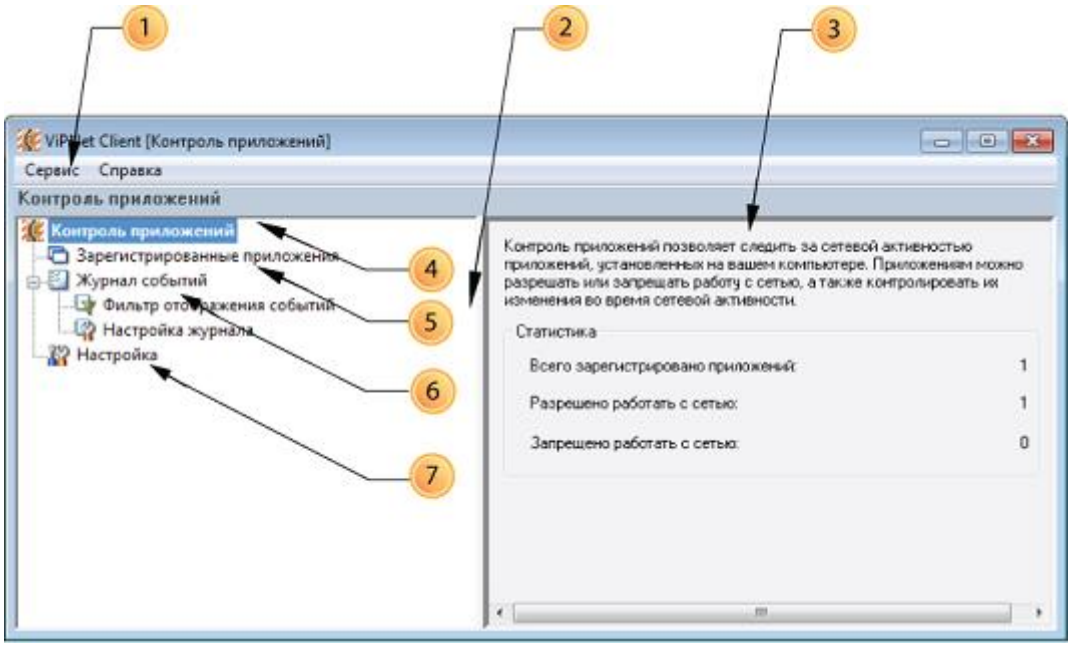


Рисунок 3: Окно программы ViPNet Контроль приложений

Цифрами на рисунке обозначены:

1 Главное меню программы.

2 Панель навигации, на которой отображается список основных возможностей программы.

3 Панель просмотра, на которой отображается содержание разделов, выбранных на панели навигации.

4 Раздел **Контроль приложений**. Содержит информацию о назначении программы и статистические данные о приложениях, которым разрешено или запрещено работать в сети.

5 Раздел **Зарегистрированные приложения**. Позволяет просмотреть информацию о приложениях, зарегистрированных программой «Контроль приложений».

   В разделе **Зарегистрированные приложения** можно также изменить режим доступа (см. «Изменение режима доступа приложения в сеть» на стр. 40) зарегистрированного приложения в сеть или отменить регистрацию приложения (см. «Удаление приложения из списка зарегистрированных приложений» на стр. 41).

6 Раздел **Журнал событий**. Позволяет просмотреть информацию об изменениях режимов доступа приложений в сеть. В соответствующих подразделах можно изменить настройки журнала (см. «Настройка параметров журнала событий» на стр. 58) и установить фильтр отображения событий в журнале (см. «Настройка фильтра отображения событий» на стр. 60).

7 Раздел **Настройка**. Позволяет настроить параметры слежения за сетевой активностью приложений (см. «Настройка параметров слежения за сетевой активностью приложений» на стр. 52) и за изменениями в приложениях (см. «Настройка параметров слежения за изменениями в приложениях» на стр. 54).

Особенности работы с программой «Контроль приложений» в терминальной сессии

Работа с программой «Контроль приложений» на терминальном сервере позволяет каждому пользователю разрешать или запрещать сетевую активность приложений, запущенных в собственной сессии, разрешать или запрещать сетевую активность сетевых служб, а также менять настройки программы для всех пользовательских сессий при достаточном уровне полномочий (см. «Уровни полномочий при работе с ViPNet Контроль приложений» на стр. 13). Работа с программой «Контроль приложений» на терминальном сервере имеет некоторые особенности.

Если на терминальном сервере активно несколько пользовательских сессий и один из пользователей выполняет настройку программы «Контроль приложений» (см. «Настройка программы ViPNet Контроль приложений» на стр. 51), то изменения будут применены во всех пользовательских сессиях и интерфейс программы «Контроль приложений» обновится во всех пользовательских сессиях в соответствии с новыми параметрами.

Если несколько пользователей одновременно выполняют настройку программы «Контроль приложений», то применены будут изменения только того пользователя, который первым сохранит изменения. В сессиях остальных пользователей при попытке применить изменения появится окно с сообщением о том, что параметры работы программы были изменены другим пользователем.

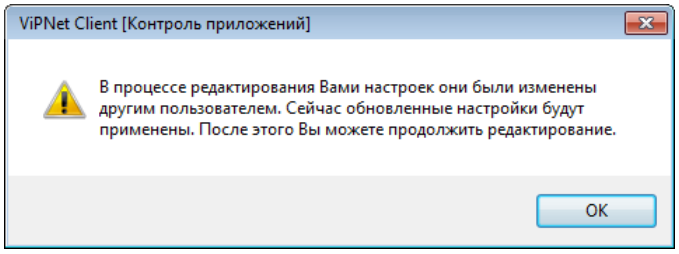


Рисунок 4: Сообщение о том, что настройки программы уже были изменены в другой пользовательской сессии

Если один из пользователей запустил приложение, проявившее сетевую активность, то окно, позволяющее выбрать дальнейшие действия программы «Контроль приложений» по отношению к этому приложению, появится только в сессии этого пользователя.

Если в одной из пользовательских сессий зарегистрировано приложение, то оно отобразится в списке зарегистрированных приложений (см. «Просмотр списка зарегистрированных приложений» на стр. 37) во всех пользовательских сессиях. Об особенностях регистрации сетевых служб см. раздел Настройка доступа сетевой службы в сеть при работе на терминальном сервере (на стр. 35).

О смене пользователя и входе в программу «Контроль приложений» от имени администратора при работе в терминальной сессии см. разделы:

- Смена пользователя при работе в терминальной сессии (на стр. 44);
- Вход в программу от имени администратора при работе в терминальной сессии (на стр. 46).

Рассмотрим пример регистрации приложения при работе на терминальном сервере:

1. На терминальном сервере установлено ПО ViPNet с программой «Контроль приложений» и выполнены следующие условия:
   - Для сетевого узла задан средний уровень полномочий (см. «Уровни полномочий при работе с ViPNet Контроль приложений» на стр. 13).
   - Пользователь А работает в режиме администратора сетевого узла (см. «Пароль администратора сетевого узла ViPNet» на стр. 63).
   - В настройках программы установлен флажок **Автоматически запускать после авторизации в ViPNet при старте Windows**.
   - При настройке правил контроля приложений выбрано правило **Запросить разрешение у пользователя** (см. «Выбор правила „Запросить разрешение у пользователя“» на стр. 32).
2. Пользователь Б заходит на терминальный сервер под своей учетной записью пользователя Windows для работы удаленно.
3. В сессии пользователя Б автоматически запускается программа «Контроль приложений».
4. Пользователь Б запускает программу Internet Explorer и получает сообщение о том, что приложение Internet Explorer проявило сетевую активность. В окне сообщения предлагается выбрать действие, которое программа «Контроль приложений» должна выполнить по отношению к программе Internet Explorer.
5. Пользователь Б разрешает приложению работать в сети.
6. Приложение регистрируется в программе «Контроль приложений» для работы с сетью. Список зарегистрированных приложений (см. «Работа со списком

зарегистрированных приложений» на стр. 37) обновляется в сессиях обоих пользователей.

Если впоследствии Пользователь Б решит, что нужно запретить программе Internet Explorer работать в сети или удалить ее из списка зарегистрированных приложений, то он не сможет этого сделать, так как средний уровень полномочий не позволяет выполнять такие настройки. В этом случае Пользователь Б может обратиться к Пользователю А, который может войти в программу «Контроль приложений» от имени администратора сетевого узла (см. «Вход в программу от имени администратора при работе в терминальной сессии» на стр. 46) и выполнить все необходимые настройки.

Если на терминальном сервере сетевую активность проявляет служба (см. «Настройка доступа сетевой службы в сеть при работе на терминальном сервере» на стр. 35), то механизм работы программы «Контроль приложений» будет другим.

Быстрый старт

Как разрешить приложению работать в сети

Сразу после установки ПО ViPNet программа «Контроль приложений» начинает следить за сетевой активностью приложений. По умолчанию сетевая активность всех приложений разрешена, поэтому при первой же сетевой активности какого-либо приложения появляется окно с сообщением о том, что данному приложению разрешено работать в сети. В этом же окне предлагается выбрать, какие действия следует выполнить программе «Контроль приложений» при следующей сетевой активности данного приложения.

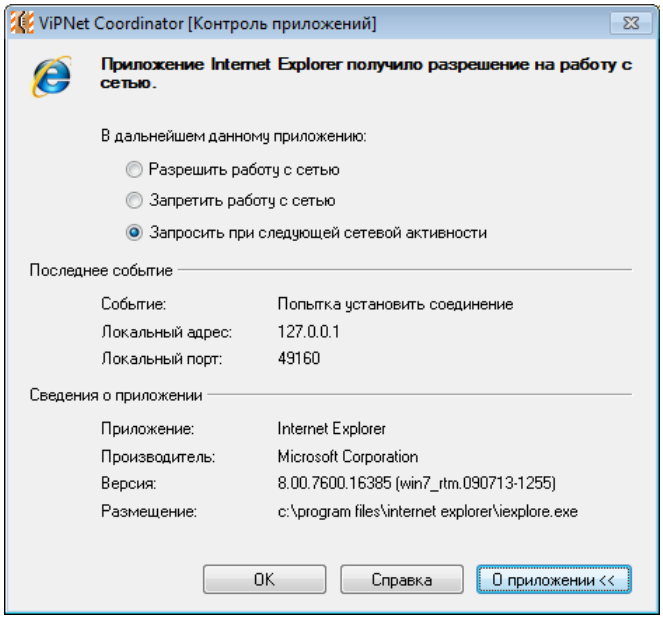


Рисунок 5: Окно запроса приложения на работу с сетью

Чтобы разрешить приложению работать в сети:

1. В окне с сообщением выберите **Разрешить работу с сетью**.
2. Нажмите кнопку **ОК**.

В результате данное приложение будет зарегистрировано, и ему будет разрешено работать в сети.

Чтобы разрешить приложению доступ в сеть при следующей сетевой активности, но вновь получить сообщение, позволяющее определить дальнейшие действия программы «Контроль приложений»:

1. В окне с сообщением выберите **Запросить при следующей сетевой активности**.
2. Нажмите кнопку **ОК**.

В результате при следующей сетевой активности доступ в сеть данному приложению будет разрешен, а окно, позволяющее разрешить или запретить в следующий раз сетевую активность этому приложению, снова будет выведено на экран.

Как запретить приложению работать в сети

В окне, которое по умолчанию появляется при первой сетевой активности приложения, можно запретить приложению работать в сети. Для этого:

1. Выберите **Запретить работу с сетью**.
2. Нажмите кнопку **ОК**.

В результате данное приложение будет зарегистрировано, а доступ в сеть для него будет заблокирован.

Чтобы разрешить заблокированному приложению доступ в сеть, выполните одно из действий:

- Удалите его из списка зарегистрированных приложений (см. «Удаление приложения из списка зарегистрированных приложений» на стр. 41) и заново зарегистрируйте.
- Измените режим доступа приложения в сеть (см. «Изменение режима доступа приложения в сеть» на стр. 40).

Как отменить получение сообщений и запросов

Чтобы не получать сообщения о запрете или разрешении сетевой активности приложений и не выбирать действия программы при каждой сетевой активности незарегистрированного приложения:

1. В главном окне программы «Контроль приложений» на панели навигации выберите раздел **Настройка**.
2. В группе **Правила контроля приложений** в списке **При сетевой активности приложения** выберите:
   - **Разрешить работу с сетью**. Сетевая активность незарегистрированных приложений будет разрешена.
   - **Запретить работу с сетью**. Сетевая активность незарегистрированных приложений будет запрещена.

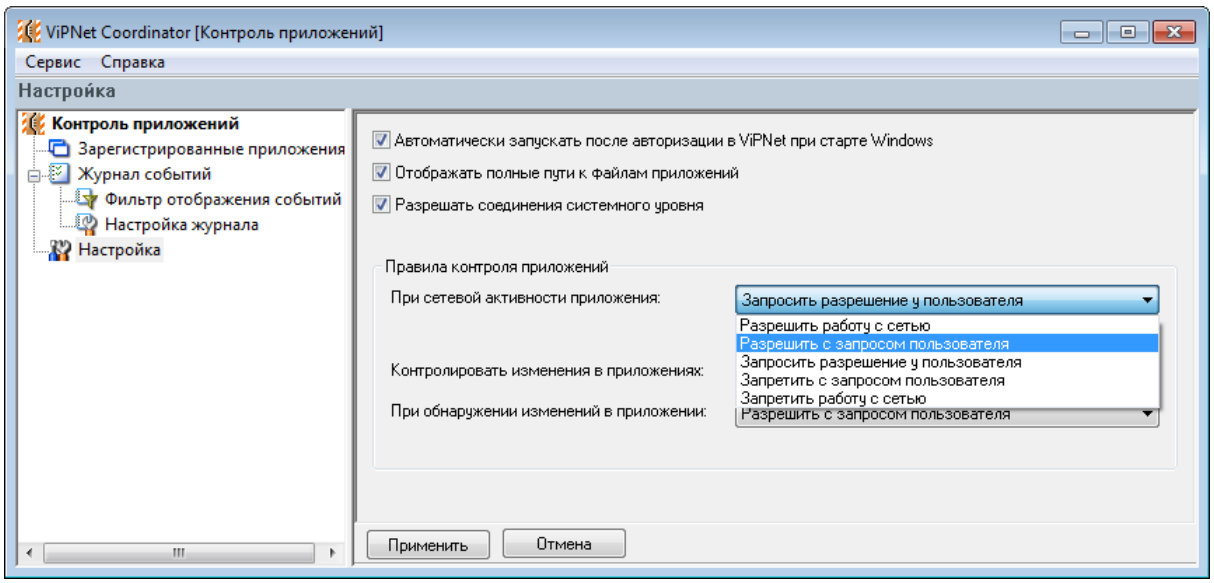


Рисунок 6: Настройка правил контроля при сетевой активности приложения

3. Нажмите кнопку **Применить**.

В результате действие, указанное на этих шагах, будет выполнено автоматически.

Чтобы не получать сообщения программы «Контроль приложений», можно также отключить функцию контроля приложений (см. «Отключение слежения за сетевой активностью приложений» на стр. 43).

Как разрешить или запретить незарегистрированному приложению доступ в сеть, не дожидаясь запроса

Незарегистрированным является приложение, которое ещё не проявляло сетевую активность, или для которого в окне сообщения о разрешении работать в сети выбиралось **Запросить при следующей сетевой активности**, **Разрешить однократно** или **Запретить однократно**. Если возникла необходимость задать параметры для приложений, которые либо не были зарегистрированы, либо еще не проявили сетевую активность, выполните следующие действия:

1. В меню **Сервис** выберите **Зарегистрировать приложение**.
2. В зависимости от цели — разрешить для приложения работу с сетью или запретить — выберите **Для разрешения работы с сетью** или **Для запрета работы с сетью** соответственно.
3. В окне **Добавить файл в список** найдите файл приложения с расширением `.exe` и нажмите кнопку **Открыть**.

В результате в таблице зарегистрированных приложений появится выбранное приложение со статусом **Запрещена** или **Разрешена** в колонке **Работа с сетью**.

Таким образом, выбранное приложение будет зарегистрировано программой «Контроль приложений», иными словами, приложению будет разрешена или запрещена сетевая активность.

3

Контроль сетевой активности приложений

Запуск и завершение работы с программой «Контроль приложений»

При работе с ПО ViPNet CUSTOM программа «Контроль приложений» по умолчанию запускается одновременно с ПО ViPNet, компонентом которого является. В случае необходимости, автоматический запуск программы «Контроль приложений» можно отменить (см. «Как отменить автоматический запуск программы „Контроль приложений“» на стр. 29).

При работе с ПО ViPNet VPN первый запуск программы «Контроль приложений» можно выполнить только вручную, а затем, в случае необходимости, можно настроить автоматический запуск программы.

Чтобы запустить программу «Контроль приложений» вручную, в главном окне программы ViPNet Client или Coordinator Монитор в меню **Приложения** выберите **Контроль приложений**. При работе с программами ViPNet Personal Firewall или ViPNet Office Firewall в главном окне программы в меню **Файл** выберите **Контроль приложений**.

Чтобы выйти из программы «Контроль приложений», выполните одно из следующих действий:

- В правом верхнем углу окна нажмите кнопку **Закрыть**  .
- В меню **Сервис** выберите пункт **Скрыть** или **Выход**.
- Нажмите сочетание клавиш **Alt+F4**.

В результате слежение за сетевой активностью приложений будет прекращено.

Об отключении функции контроля приложений см. Отключение слежения за сетевой активностью приложений (на стр. 43).

Как отменить автоматический запуск программы «Контроль приложений»

Чтобы программа «Контроль приложений» не запускалась автоматически одновременно с ПО ViPNet, компонентом которого является, выполните следующие действия:

1 В главном окне программы на панели навигации выберите раздел **Настройка**.

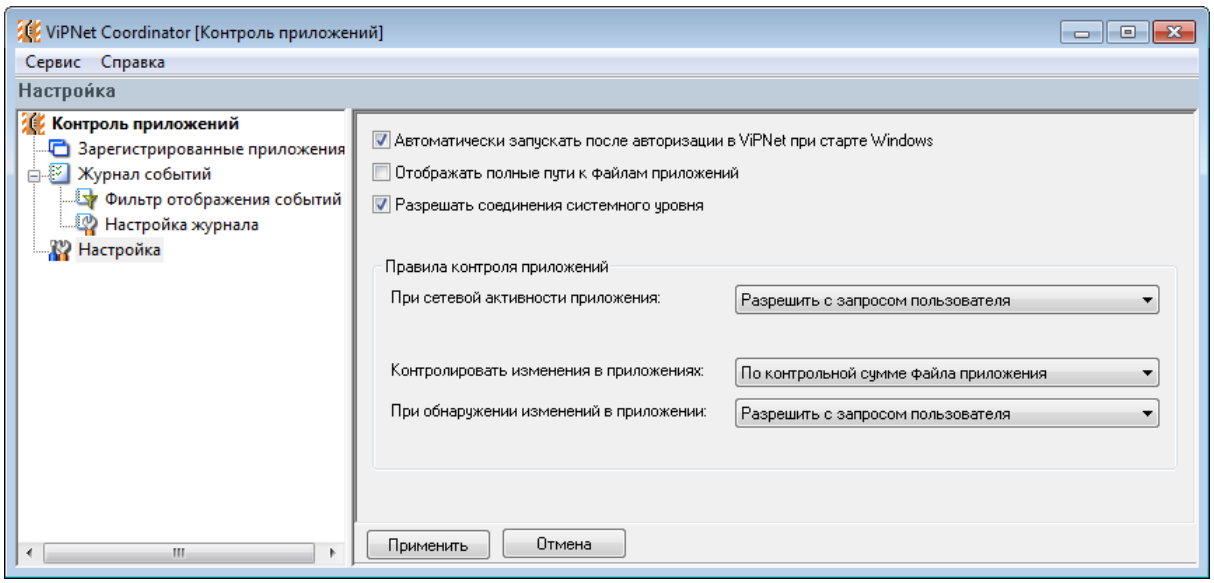


Рисунок 7: Раздел настройки программы «Контроль приложений»

2 Снимите флажок **Автоматически запускать после авторизации в ViPNet при старте Windows**.

3 Нажмите кнопку **Применить**.

В результате программа «Контроль приложений» не будет запускаться при старте ОС Windows. В таком случае, чтобы осуществлялся контроль сетевой активности приложений, программу «Контроль приложений» нужно будет запустить вручную (см. «Запуск и завершение работы с программой „Контроль приложений“» на стр. 28).

Программа «Контроль приложений» запускается только вместе с ПО ViPNet, компонентом которого является, поэтому, если при старте системы вы откажетесь от запуска ПО ViPNet, в состав которого входит программа «Контроль приложений», то

«Контроль приложений» не будет запущен. Если после старта системы вы запустите ПО ViPNet вручную, то программу «Контроль приложений» также нужно будет запустить вручную (см. «Запуск и завершение работы с программой „Контроль приложений“» на стр. 28).

Настройка доступа приложения в сеть

Одно из назначений программы «Контроль приложений» — регистрация приложений, проявляющих сетевую активность на компьютере. Вам будет предложено определить, можно ли приложению работать с сетью, если:

- Приложение не зарегистрировано программой «Контроль приложений».
- Приложение удалено из списка зарегистрированных приложений (см. «Удаление приложения из списка зарегистрированных приложений» на стр. 41).
- Приложение уже было ранее зарегистрировано программой «Контроль приложений», но свойства этого приложения были изменены (см. «Настройка параметров слежения за изменениями в приложениях» на стр. 54), например, обновлена версия приложения.

Когда фиксируется попытка приложения выполнить какую-либо операцию в сети, по умолчанию работа в сети этому приложению разрешается, и появляется окно, позволяющее определить действия программы «Контроль приложений» при следующей сетевой активности приложения.

Вид окна с сообщением о сетевой активности приложения зависит от выбранного правила контроля приложений (см. «Настройка параметров слежения за сетевой активностью приложений» на стр. 52). Программа «Контроль приложений» позволяет выбрать одно из следующих правил:

- Разрешить работу с сетью.
- Разрешить с запросом пользователя.
- Запросить разрешение у пользователя.
- Запретить с запросом пользователя.
- Запретить работу с сетью.

При выборе **Разрешить работу с сетью** и **Запретить работу с сетью** доступ приложения в сеть разрешается или блокируется без появления в дальнейшем окна с сообщением.

Выбор правила «Разрешить с запросом пользователя»

Если используется правило контроля приложений, установленное по умолчанию (выбрано правило **Разрешить с запросом пользователя**), то приложению, проявившему сетевую активность, работа с сетью будет разрешена. При этом в окне с сообщением о сетевой активности приложения нужно выбрать, какие действия должны быть выполнены программой «Контроль приложений» при следующей сетевой активности приложения. В неинтерактивном режиме (см. «Неинтерактивный режим» на стр. 63) работа приложения в сети будет разрешена.

Чтобы разрешить приложению доступ в сеть при выбранном правиле **Разрешить с запросом пользователя**, выполните действия, описанные в разделе Как разрешить приложению работать в сети (на стр. 21).

Чтобы запретить приложению доступ в сеть при выбранном правиле **Разрешить с запросом пользователя**, выполните действия, описанные в разделе Как запретить приложению работать в сети (на стр. 23).

Выбор правила «Запросить разрешение у пользователя»

Если при настройке правил контроля приложений (см. «Настройка параметров слежения за сетевой активностью приложений» на стр. 52) выбрано правило **Запросить разрешение у пользователя**, то при следующей сетевой активности приложения не будет выполнено каких-либо действий до указаний пользователя.

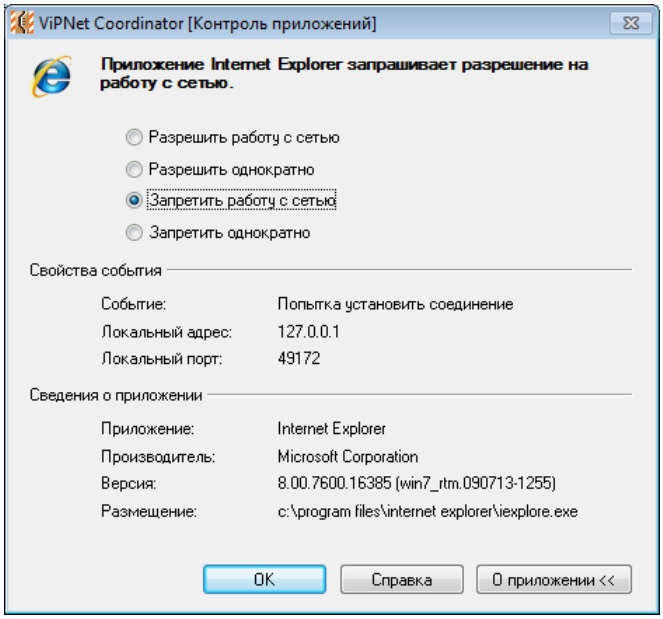


Рисунок 8: Окно с сообщением о сетевой активности приложения при выбранном правиле «Запросить разрешение у пользователя»

Совет. Чтобы скрыть или отобразить в окне запроса группу **Сведения о приложении**, нажмите кнопку **О приложении**.

Чтобы разрешить приложению доступ в сеть при выбранном правиле **Запросить разрешение у пользователя**:

1. В окне с сообщением о сетевой активности приложения выберите:
   - **Разрешить работу с сетью** — приложение будет зарегистрировано в программе «Контроль приложений», и сетевая активность для данного приложения будет разрешена.
   - **Разрешить однократно** — работа с сетью данного приложения разрешена для текущего сеанса, но при следующей его сетевой активности вновь будет выдано это же окно с запросом. Приложение не будет зарегистрировано.
2. Нажмите кнопку **ОК**.

Чтобы запретить приложению доступ в сеть при выбранном правиле **Запросить разрешение у пользователя**:

1. В окне с сообщением о сетевой активности приложения выберите:
   - **Запретить работу с сетью** — приложение будет зарегистрировано в программе «Контроль приложений», и сетевая активность этого приложения будет запрещена, то есть любые его попытки выйти в сеть будут блокироваться.
   - **Запретить однократно** — работа с сетью данного приложения запрещена для текущего сеанса, но при следующей его сетевой активности вновь будет выдано это же окно с запросом. Приложение не будет зарегистрировано.
2. Нажмите кнопку **ОК**.

Если выбрано правило **Запросить разрешение у пользователя** и приложение проявило сетевую активность, но в данный момент у вас нет возможности выбрать то или иное действие в окне с сообщением, то «Контроль приложений» будет обрабатывать запросы приложений на работу с сетью в неинтерактивном режиме (см. «Неинтерактивный режим» на стр. 63). Подробнее о неинтерактивном режиме обработки запросов, см. раздел Обработка запросов приложений на работу с сетью в неинтерактивном режиме (на стр. 56).

Выбор правила «Запретить с запросом пользователя»

Если при настройке правил контроля приложений выбрано правило **Запретить с запросом пользователя**, то приложению, проявившему сетевую активность, работа с сетью будет запрещена. При этом в окне с сообщением о сетевой активности приложения нужно выбрать, какие действия должны быть выполнены программой «Контроль приложений» при следующей сетевой активности приложения. В неинтерактивном режиме работа приложения в сети будет запрещена.

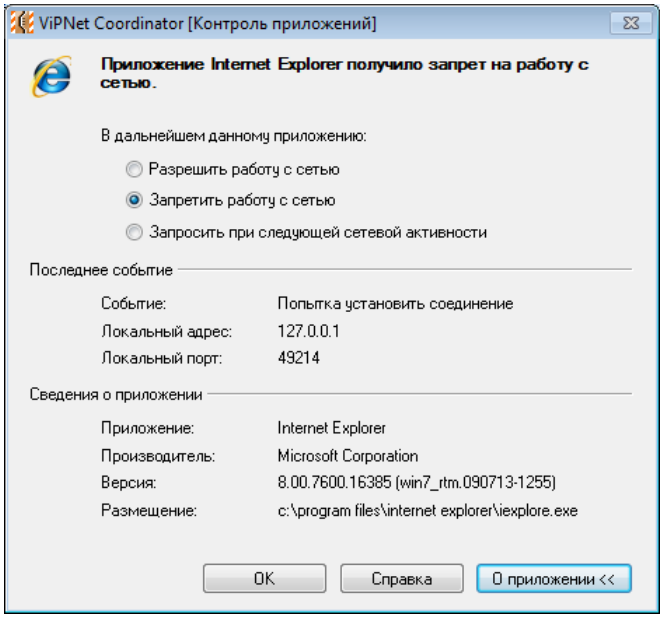


Рисунок 9: Окно с сообщением о сетевой активности приложения при выбранном правиле «Запретить с запросом пользователя»

Чтобы разрешить приложению доступ в сеть при выбранном правиле **Запретить с запросом пользователя**:

1. В окне с сообщением о сетевой активности приложения выберите:
   - **Разрешить работу с сетью**, чтобы зарегистрировать данное приложение для работы сетью и не получать запросы на разрешение при каждой попытке этого приложения выйти в сеть.
   - **Запросить при следующей сетевой активности**, чтобы разрешить данному приложению работать с сетью в этот раз, а при следующей сетевой активности вновь получить сообщение, позволяющее определить дальнейшие действия программы «Контроль приложений».
2. Нажмите кнопку **ОК**.

Чтобы запретить приложению доступ в сеть при выбранном правиле **Запретить с запросом пользователя**:

1. В окне с сообщением о сетевой активности приложения выберите **Запретить работу с сетью**, чтобы зарегистрировать данное приложение для запрета работы сетью и не получать запросы при каждой попытке этого приложения выйти в сеть.
2. Нажмите кнопку **ОК**.

Настройка доступа сетевой службы в сеть при работе на терминальном сервере

Если сетевая служба на терминальном сервере проявит сетевую активность, в сессии пользователя, работающего на данном сервере, откроется окно с сообщением о сетевой активности службы, в котором можно определить дальнейшее действие программы «Контроль приложений» по отношению к этой службе. Такое окно с сообщением может быть отправлено только одному пользователю, поэтому если несколько пользовательских сессий активны на терминальном сервере, то окно появляется в сессии одного из пользователей согласно следующему приоритету:

1. пользователь, обладающий полномочиями администратора сетевого узла ViPNet и работающий на сервере локально;
2. пользователь, обладающий полномочиями администратора сетевого узла ViPNet и работающий на сервере удаленно;
3. пользователь, не обладающий полномочиями администратора сетевого узла ViPNet и работающий на сервере локально;
4. пользователь, не обладающий полномочиями администратора сетевого узла ViPNet и работающий на сервере удаленно.

Например:

1. На терминальном сервере запущены две пользовательские сессии:
   - пользователь А работает локально и не обладает полномочиями администратора;
   - пользователь Б работает удаленно от имени администратора сетевого узла ViPNet.
2. На терминальном сервере сетевая служба BranchCache пытается получить доступ к сети.
3. Окно с сообщением о сетевой активности службы будет отправлено пользователю Б, который выберет одно из предложенных в окне действий.

4 Программа «Контроль приложений» применит выбранное действие по отношению к данной сетевой службе.

5 Если служба будет зарегистрирована для разрешения или запрета работы в сети (см. «Быстрый старт» на стр. 20), то она появится в списке зарегистрированных приложений обоих пользователей.

Работа со списком зарегистрированных приложений

Просмотр списка зарегистрированных приложений

Программа ViPNet Контроль приложений позволяет просмотреть информацию о приложениях, которые были зарегистрированы и которым была разрешена или запрещена работа с сетью. Для этого в главном окне программы «Контроль приложений» на панели навигации выберите раздел **Зарегистрированные приложения**.

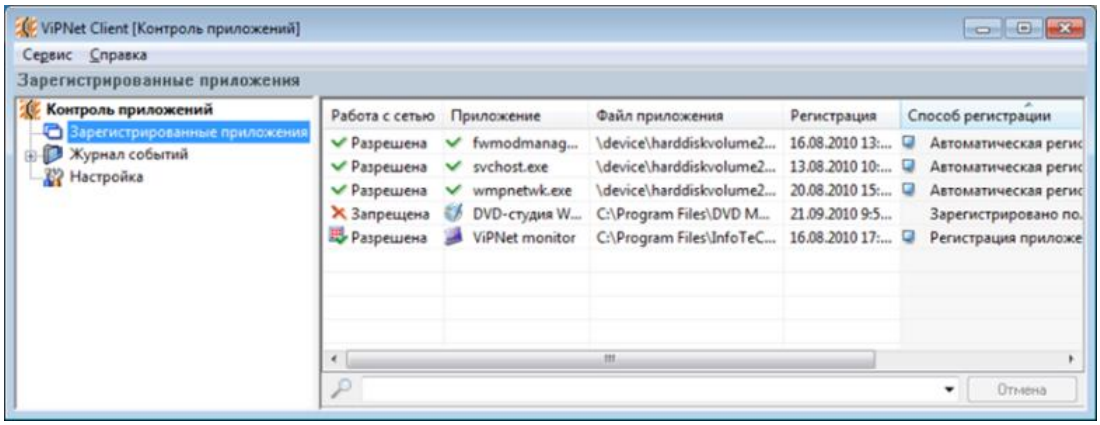


Рисунок 10: Просмотр параметров зарегистрированных приложений

В результате на панели просмотра в виде таблицы будет отображена следующая информация о зарегистрированных приложениях:

1. В столбце **Работа с сетью** отображена информация о том, разрешено или запрещено приложению работать с сетью. Возможны следующие режимы работы с сетью:
   - **Разрешена**, если приложению разрешена работа с сетью.
   - **Запрещена**, если приложению запрещена работа с сетью.
   - **Разрешена**, если приложению ViPNet разрешена работа с сетью.
   - **Запрещена**, если приложению ViPNet запрещена работа с сетью.
2. В столбце **Приложение** приведены названия зарегистрированных приложений.

3 В столбце **Файл приложения** по умолчанию отображается путь к исполняемому файлу. Чтобы в этой колонке отображалось только название исполняемого файла:

- В главном окне программы «Контроль приложений» на левой панели выберите раздел **Настройка**.
- На панели просмотра снимите флажок **Отображать полные пути к файлам приложений**.

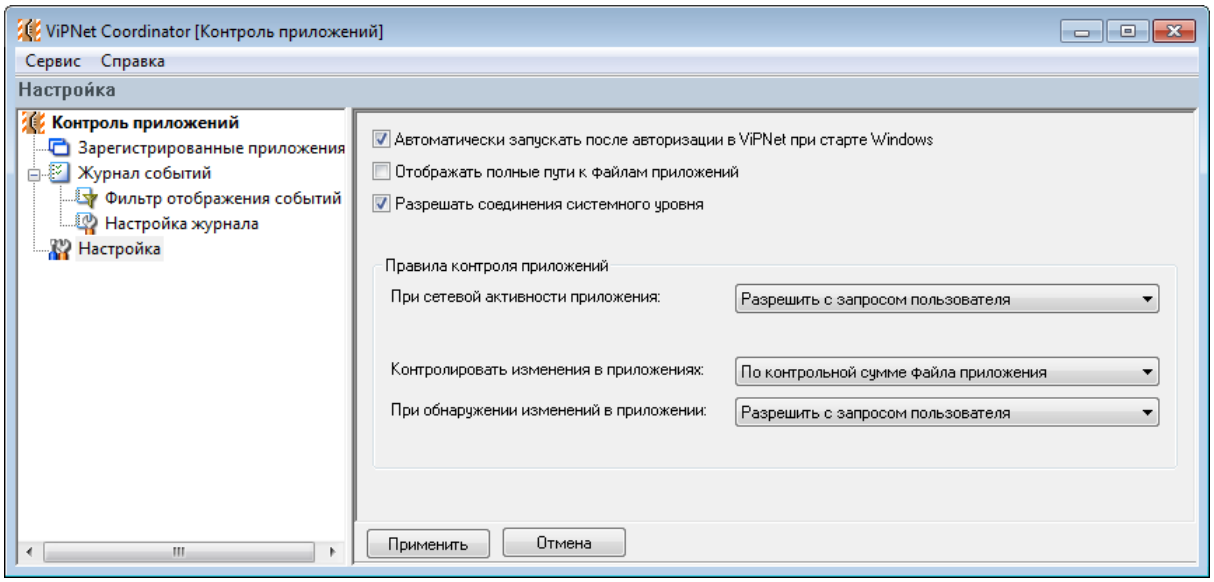


Рисунок 11: Настройка отображения имени и пути исполняемого файла

4 В столбце **Регистрация** отображается информация о дате и времени начала слежения за сетевой активностью приложения программой «Контроль приложений».

5 В столбце **Способ регистрации** отображается один из следующих способов регистрации приложения:

- **Зарегистрировано пользователем**, если при настройке правил контроля приложений выбрано правило **Запросить разрешение у пользователя** (см. «Выбор правила „Запросить разрешение у пользователя“» на стр. 32) или приложение добавлено в список зарегистрированных приложений вручную (см. «Как разрешить или запретить незарегистрированному приложению доступ в сеть, не дожидаясь запроса» на стр. 26).
- **Автоматическая регистрация**, если при настройке правил контроля приложений выбрано любое правило (см. «Настройка доступа приложения в сеть» на стр. 31), кроме **Запросить разрешение у пользователя**.
- **Регистрация приложения ViPNet**, если зарегистрированное приложение входит в комплект поставки ПО ViPNet.

- **Изменение приложения по запросу пользователя**, если приложение изменено и при настройке параметров слежения за изменениями в зарегистрированных приложениях выбрано правило **Запросить разрешение у пользователя** (см. «Выбор правила „Запросить разрешение у пользователя“» на стр. 32).
- **Автоматическая регистрация изменения приложения**, если приложение изменено и при настройке параметров слежения за изменениями в зарегистрированных приложениях выбрано любое правило (см. «Настройка параметров слежения за изменениями в приложениях» на стр. 54), кроме **Запросить разрешение у пользователя**.
- **Обновление приложения ViPNet**, если в зарегистрированном приложении, входящем в комплект поставки ПО ViPNet, обнаружено изменение.

6 В столбце **Изменения приложения** отображается информация о дате и времени последнего изменения приложения (см. «Настройка параметров слежения за изменениями в приложениях» на стр. 54). Если приложение не изменялось, то ячейка будет пустой.

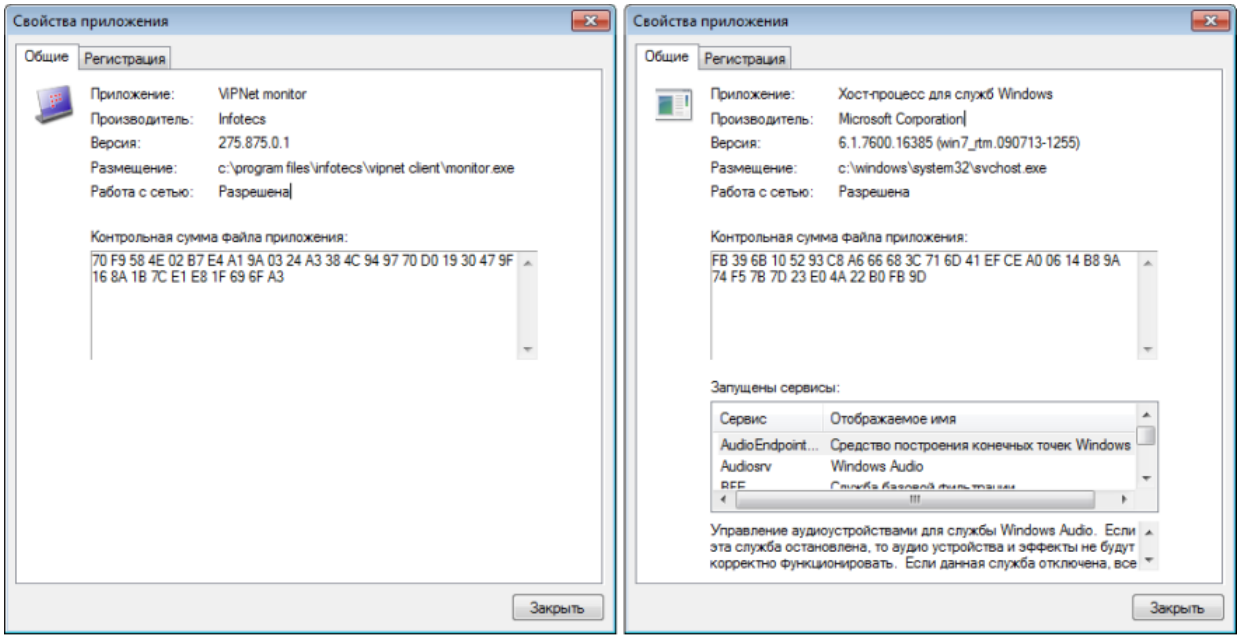
Чтобы изменить объем информации, отображаемой в разделе **Зарегистрированные приложения**, щелкните правой кнопкой мыши на заголовке любого из столбцов и установите или снимите нужные флажки.

Чтобы просмотреть свойства зарегистрированных приложений в отдельном окне:

1 В окне **Зарегистрированные приложения** щелкните правой кнопкой мыши на строке приложения, свойства которого нужно просмотреть.

2 Выберите **Свойства**.

В результате общие свойства приложения и сведения о регистрации можно будет просмотреть в отдельном окне. В окне свойств хост-процесса, помимо общей информации, также содержится список служб, работающих в данном процессе, и общие сведения о них.



Свойства программы ViPNet Monitor

Свойства хост-процесса Svchost.exe

Рисунок 12: Окно свойств приложения

Изменение режима доступа приложения в сеть

Чтобы изменить существующие настройки зарегистрированных приложений (то есть тех приложений, для которых в окне запроса было выбрано **Разрешить работу с сетью** или **Запретить работу с сетью**):

1. В главном окне программы «Контроль приложений» (см. «Интерфейс программы ViPNet Контроль приложений» на стр. 15) на панели навигации выберите **Зарегистрированные приложения**.
2. В таблице щелкните правой кнопкой мыши на строке приложения, для которого нужно изменить настройки.

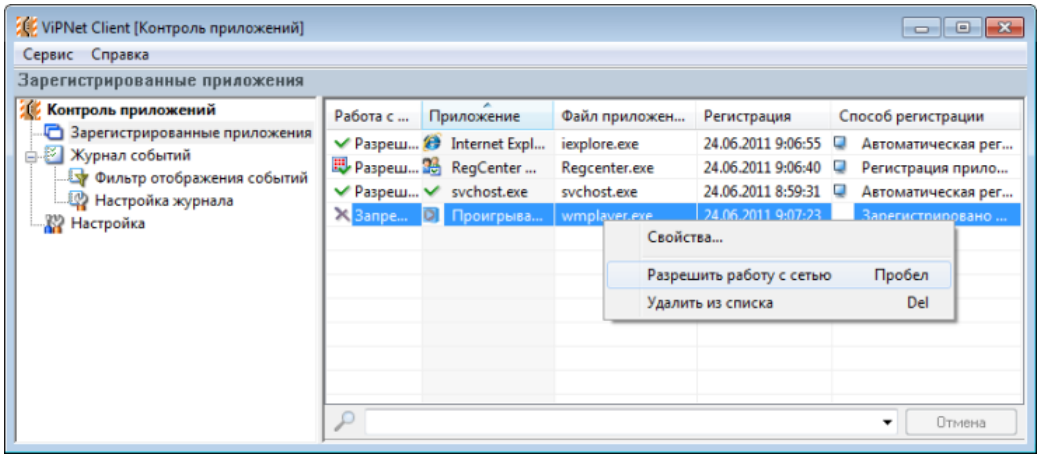


Рисунок 13: Таблица зарегистрированных приложений

3 Выберите нужный режим:

- Если работа с сетью для данного приложения разрешена, то будет предложено запретить работу с сетью.
- Если работа с сетью для данного приложения запрещена, то будет предложено разрешить работу с сетью.
- Чтобы при следующей сетевой активности приложения был выдан запрос на разрешение работы с сетью, выберите **Удалить из списка.** Подробнее см. в разделе Удаление приложения из списка зарегистрированных приложений (на стр. 41).

4 В таблице зарегистрированных приложений в колонке **Работа с сетью** изменится статус приложения (при выборе запрета или разрешения работы с сетью) или приложение не будет отображаться в списке (если приложение было удалено из списка).

Если возникла необходимость задать параметры для приложений, которых нет в списке зарегистрированных приложений, выполните регистрацию приложений вручную (см. «Как разрешить или запретить незарегистрированному приложению доступ в сеть, не дожидаясь запроса» на стр. 26).

Удаление приложения из списка зарегистрированных приложений

При работе с программой «Контроль приложений» может понадобиться, чтобы приложение, которому ранее уже была разрешена или запрещена сетевая активность,

запрашивало разрешение при каждой попытке работать с сетью. Для этого нужно удалить приложение из списка зарегистрированных приложений и установить новые параметры.

Чтобы удалить приложение из списка зарегистрированных приложений:

1. В окне программы «Контроль приложений» на панели навигации выберите **Зарегистрированные приложения**.
2. В таблице зарегистрированных приложений щелкните правой кнопкой мыши на строке приложения, запись о котором нужно удалить.
3. Выберите **Удалить из списка**.

В результате удалённое приложение станет незарегистрированным. Это означает, что при первой же его сетевой активности, будет выдан запрос на установку новых параметров для этого приложения. Вновь зарегистрировать данное приложение можно также вручную (см. «Как разрешить или запретить незарегистрированному приложению доступ в сеть, не дожидаясь запроса» на стр. 26).

Отключение слежения за сетевой активностью приложений

Примечание. По умолчанию контроль сетевой активности приложений включен, поэтому, когда запускается ПО ViPNet, компонентом которого является «Контроль приложений», программа «Контроль приложений» сразу начинает следить за сетевой активностью приложений.

Отключение функции контроля сетевой активности приложений приводит к прекращению слежения за приложениями, пытающимися получить доступ к сети. Отключение контроля сетевой активности приложений, с одной стороны, резко снижает уровень защищенности вашего компьютера и может позволить злоумышленникам получить доступ к персональным данным, хранящимся на вашем компьютере. С другой стороны, это позволяет устранить проблемы, вызванные конфликтом программы «Контроль приложений» с каким-либо программным обеспечением, которому доступ в сеть необходим для корректной работы. «Контроль приложений» совместим с большинством приложений, требующих доступ в сеть, но при возникновении каких-либо неполадок отключение контроля над сетевой активностью может помочь в диагностике проблем отдельных приложений сторонних производителей.

Внимание! Для обеспечения безопасности на компьютере настоятельно рекомендуется, чтобы программа «Контроль приложений» была включена. Поэтому не забудьте вернуть функцию контроля сетевой активности приложений в активное состояние, когда необходимость в отключении исчезнет. Для этого в меню **Сервис** выберите **Включить контроль приложений**.

Чтобы отключить контроль сетевой активности приложений, в главном окне программы «Контроль приложений» в меню **Сервис** выберите **Отключить контроль приложений.** В результате слежение за активностью приложений будет прекращено.

Смена пользователя в программе «Контроль приложений»

Программа «Контроль приложений» в составе ПО ViPNet Client и Coordinator позволяет сменить пользователя. Благодаря этой функции, с программой «Контроль приложений» могут работать разные пользователи ViPNet, при этом каждый из них будет работать со своим списком зарегистрированных приложений и своими настройками.

На одном компьютере несколько пользователей могут работать с ПО ViPNet Client и Coordinator, в состав которого входит «Контроль приложений». Возможность смены пользователя позволяет каждому пользователю заходить в «Контроль приложений» под своей учетной записью, не завершая работу ПО ViPNet. Чтобы сменить пользователя программы «Контроль приложений»:

1. В меню **Сервис** выберите **Сменить пользователя.**
2. Введите пароль и нажмите кнопку **ОК.**

Примечание. Смена пользователя в одном из приложений используемого ПО ViPNet не приведет к смене пользователя во всех остальных компонентах данного ПО. Например, смена пользователя в ПО ViPNet Монитор не приведет к смене пользователя в программе «Контроль приложений» и наоборот.

В результате в программе «Контроль приложений» будут отображены настройки и данные о зарегистрированных приложениях нового пользователя.

Смена пользователя при работе в терминальной сессии

Смена пользователя также возможна при работе в терминальной сессии. Например, если на терминальном сервере работал другой пользователь и в программе «Контроль приложений» отображаются его настройки, смена пользователя позволит войти в программу под своей учетной записью и работать со своими настройками. Для этого:

1. В своей сессии в меню **Сервис** выберите **Сменить пользователя.**
2. Введите пароль и нажмите кнопку **ОК.**

В результате в программе «Контроль приложений» будут использоваться настройки нового пользователя и будет обновлен интерфейс во всех пользовательских сессиях на данном терминальном сервере.

Если на терминальном сервере несколько пользователей пытаются одновременно сменить пользователя в программе «Контроль приложений», то завершить операцию сможет только тот, кто первым выбрал команду **Сменить пользователя**. В сессиях остальных пользователей появится сообщение о том, что смена пользователя программы «Контроль приложений» уже производится другим пользователем и повторить операцию можно будет позже.

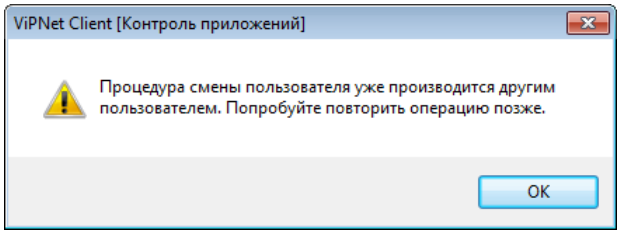


Рисунок 14: Сообщение о том, что смена пользователя уже производится в другой пользовательской сессии

Если на терминальном сервере один из пользователей выполняет настройку программы «Контроль приложений», а второй пользователь в это же время пытается выполнить команду **Сменить пользователя**, то второй пользователь получит сообщение о том, что в другой сессии производится редактирование параметров работы программы «Контроль приложений» и смена пользователя в данный момент невозможна. Операцию смены пользователя можно будет провести позже.

Вход в программу от имени администратора

Администратор сети ViPNet может выполнить вход от своего имени в программу «Контроль приложений» на любом сетевом узле и выполнить настройки, которые могут быть недоступны пользователю из-за недостаточного уровня полномочий.

Чтобы выполнить вход администратора:

1. В меню **ViPNet Контроль приложений** выберите **Войти в режим администратора**.
2. Введите пароль администратора сетевого узла ViPNet (на стр. 63) и нажмите кнопку **ОК**.

В результате все настройки программы «Контроль приложений» будут доступны для редактирования.

Вход в программу от имени администратора при работе в терминальной сессии

При работе на терминальном сервере можно осуществить вход в программу «Контроль приложений» от имени администратора с целью выполнить настройку параметров, недоступных из-за недостаточного уровня полномочий.

Если на терминальном сервере в одной из пользовательских сессий осуществлен вход в программу «Контроль приложений» от имени администратора, то в других пользовательских сессиях уровень полномочий изменен не будет. Однако настройки, выполняемые от имени администратора, будут применяться к программе «Контроль приложений» во всех сессиях.

4

Просмотр статистики и журнала событий

Просмотр статистики

Сведения о зарегистрированных приложениях можно посмотреть в виде:

- статистики, представляющей собой количество зарегистрированных приложений;
- подробной информации о приложениях и их возможности работать в сети.

Для просмотра статистики в главном окне программы на панели навигации выберите **Контроль приложений**.

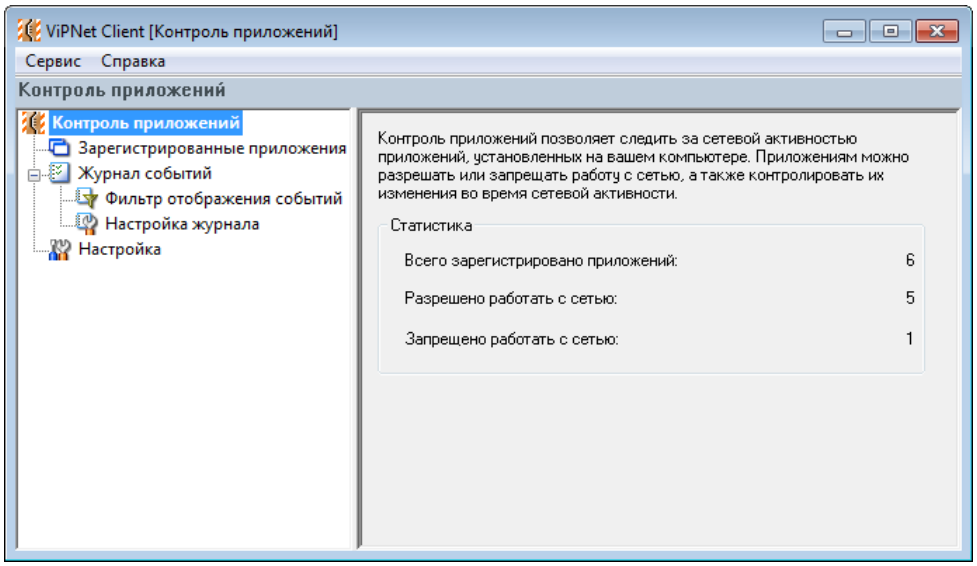


Рисунок 15: Просмотр статистики зарегистрированных приложений

В разделе **Контроль приложений** можно просмотреть следующие данные:

- Сколько всего приложений зарегистрировано программой.
- Для какого количества приложений сетевая активность разрешена.
- Для какого количества приложений сетевая активность запрещена.

Просмотр журнала событий

Записи из журнала событий представлены в виде таблицы, содержащей информацию об изменениях статусов приложений. Таким образом, журнал событий позволяет проследить, какие действия и когда совершались над приложениями. Характер и объем отображаемой и заносимой в журнал информации задается в настройках журнала (см. «Настройка параметров журнала событий» на стр. 58) и в настройках фильтра отображения событий (см. «Настройка фильтра отображения событий» на стр. 60).

Чтобы просмотреть журнал событий:

1. В главном окне программы «Контроль приложений» на панели навигации выберите **Журнал событий**.
2. В окне **Журнал событий** нажмите кнопку **Обновить**.
3. В результате в окне появится список событий.

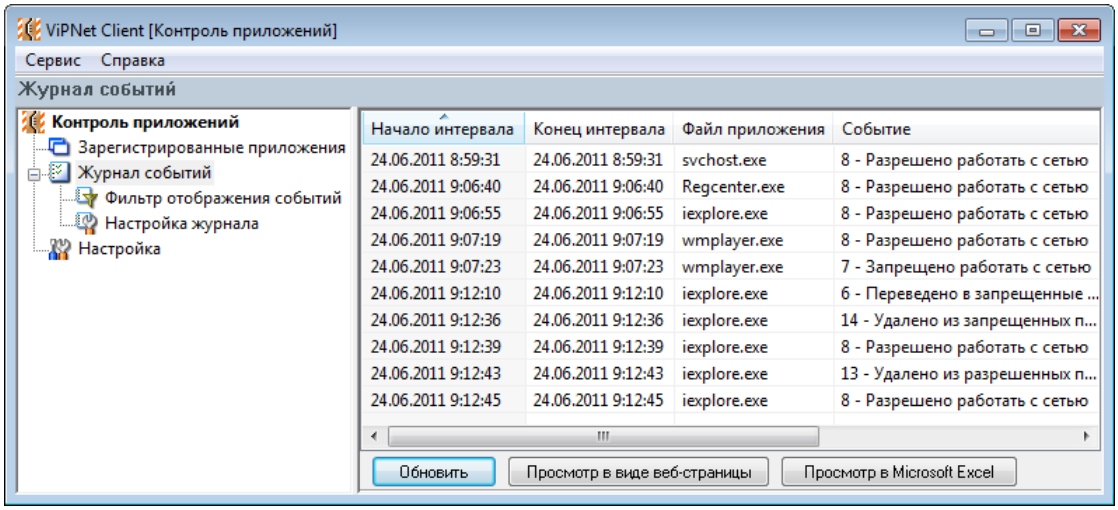


Рисунок 16: Журнал событий

Журнал событий можно просмотреть в других программах:

- Для просмотра журнала событий в HTML-формате, нажмите **Просмотр в виде веб-страницы**.
- Для просмотра журнала событий в виде таблицы Microsoft Excel, нажмите **Просмотр в Microsoft Excel**.

Просмотр журнала событий в других программах позволяет редактировать журнал, сохранять и распечатывать для дальнейшего использования.

В журнале программы «Контроль приложений» регистрируются 14 типов событий. Все возможные типы событий приведены в таблице ниже.

Таблица 4. Типы событий, отображаемых в журнале программы «Контроль приложений»

Код события	Описание события
1	Блокирована передача
2	Разрешена передача
3	Запрещено работать с сетью в связи с изменением приложения
4	Разрешено работать с сетью после изменения приложения
5	Переведено в разрешенные приложения пользователем
6	Переведено в запрещенные приложения пользователем
7	Запрещено работать с сетью
8	Разрешено работать с сетью
9	Блокировано открытие порта для приема данных
10	Разрешено открытие порта для приема данных
11	Блокирована установка соединения
12	Разрешена установка соединения
13	Удалено из разрешенных приложений пользователем
14	Удалено из запрещенных приложений пользователем

Настройка программы ViPNet Контроль приложений

Настройка параметров слежения за сетевой активностью приложений

Настройка параметров слежения за сетевой активностью позволяет назначить действия, которые будут выполнены программой «Контроль приложений» при сетевой активности какого-либо приложения. Чтобы настроить эти параметры:

1 В главном окне программы на панели навигации выберите **Настройка**.

2 В группе **Правила контроля приложений** в списке **При сетевой активности приложения** выберите одно из правил (см. «Настройка доступа приложения в сеть» на стр. 31).

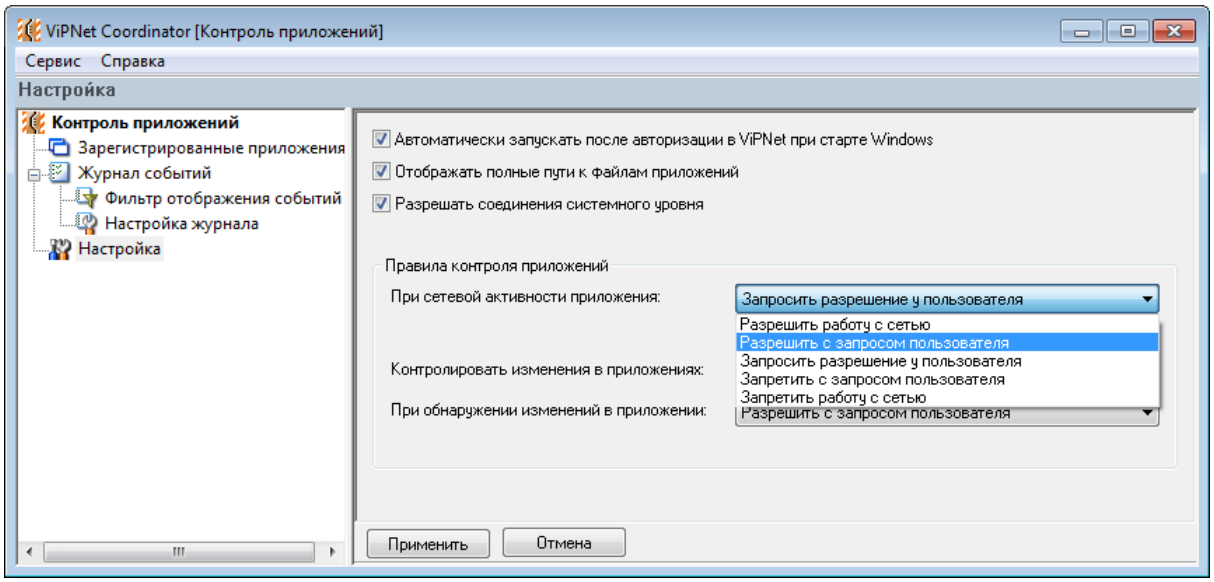


Рисунок 17: Настройка параметров слежения за сетевой активностью приложений

3 По умолчанию соединения системного уровня разрешены. При необходимости, в целях безопасности, чтобы злоумышленник не мог установить соединение от имени системы, нужно снять флажок **Разрешать соединения системного уровня**.

Внимание! Запрет соединений системного уровня может привести к нежелательным последствиям. Использовать эту возможность рекомендуется только продвинутым пользователям ОС Windows.

4 Нажмите кнопку **Применить**.

В результате при сетевой активности приложений будет выполняться указанное действие.

Настройка параметров слежения за изменениями в приложениях

После того как приложение зарегистрировано в программе «Контроль приложений», оно может подвергнуться каким-либо изменениям. Эти изменения, с одной стороны, могут быть результатом нормальной работы приложения, например, обновления программного обеспечения, добавления новых функций. С другой стороны, вредоносное ПО может модифицировать зарегистрированные приложения, и в таком случае нужно запретить приложению доступ в сеть.

Настройка параметров слежения за изменениями в приложениях позволяет определить, должна ли программа «Контроль приложений» контролировать изменения в зарегистрированных приложениях, если да, то какие именно, и какие действия предпринимать, если изменения обнаружены.

Чтобы настроить параметры слежения за изменениями в приложениях:

1. В главном окне программы на панели навигации выберите **Настройка.**
2. В окне **Настройка** в группе **Правила контроля приложений** в списке **Контролировать изменения в приложениях** выберите:
   - **Не контролировать**, если не хотите, чтобы изменения в приложениях влияли на разрешение или запрет работы приложения с сетью.
   - **По контрольной сумме файла приложения**, то есть по некоторому значению, подтверждающему целостность и подлинность файла приложения, если нужно, чтобы изменения контролировались и чтобы в результате изменения контрольной суммы файла приложения требовалась повторная регистрация приложения.
   - **По размеру файла приложения**, чтобы в результате изменения размера исполняемого файла приложения требовалась повторная регистрация приложения.

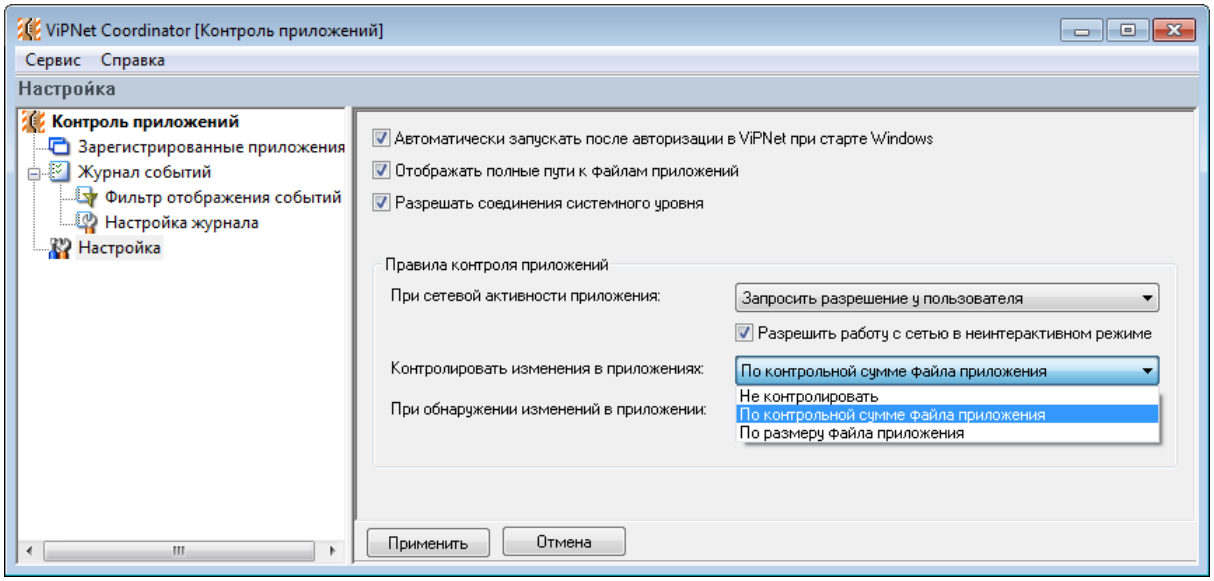


Рисунок 18: Настройка параметров слежения за изменениями в приложениях

3 В группе **Правила контроля приложений** в списке **При обнаружении изменений в приложении** выберите одно из правил. Здесь предлагается тот же список действий, что и в списке **При сетевой активности приложения** (см. «Настройка доступа приложения в сеть» на стр. 31).

4 Нажмите кнопку **Применить**.

В результате при следующей сетевой активности измененного приложения будут выполнены выбранные действия.

Обработка запросов приложений на работу с сетью в неинтерактивном режиме

Обработка запроса приложения на работу с сетью в неинтерактивном режиме позволяет разрешить или запретить приложению работать в сети, если выбрана одна из интерактивных правил контроля приложений (см. «Интерактивное правило контроля приложений» на стр. 62) и в данный момент у пользователя нет возможности выбрать действие программы ViPNet Контроль приложений в окне сообщения о сетевой активности приложения. Обработка запросов в неинтерактивном режиме осуществляется в следующих случаях:

- текущая сессия пользователя заблокирована;
- программа «Контроль приложений» не запущена;
- при загрузке операционной системы, когда вход в ПО ViPNet, компонентом которого является программа «Контроль приложений», еще не осуществлен.

Например, необходимость разрешать сетевую активность приложений в неинтерактивном режиме может возникнуть при загрузке служб операционной системы, когда слежение за сетевой активностью приложений уже началось, но вход в ПО ViPNet, компонентом которого является программа «Контроль приложений», еще не осуществлен. Своевременный выход служб в сеть позволит избежать проблем при загрузке системы.

Если выбрано правило «Разрешить с запросом пользователя» или «Запретить с запросом пользователя», то в неинтерактивном режиме работа приложения в сети будет разрешена или запрещена соответственно (так же как и при обычном режиме работы). В интерактивном режиме откроется окно с сообщением о сетевой активности приложения, в котором пользователь выберет дальнейшие действия программы «Контроль приложений».

Если выбрано правило «Запросить разрешение у пользователя», то по умолчанию в неинтерактивном режиме работа приложения в сети будет разрешена. Чтобы запретить работу приложения в сети при обработке запроса в неинтерактивном режиме, выполните следующие действия:

1 В главном окне программы «Контроль приложений» на панели навигации выберите **Настройка**.

2 На панели просмотра в группе **Правила контроля приложений** снимите флажок или флажки **Разрешить работу с сетью в неинтерактивном режиме**.

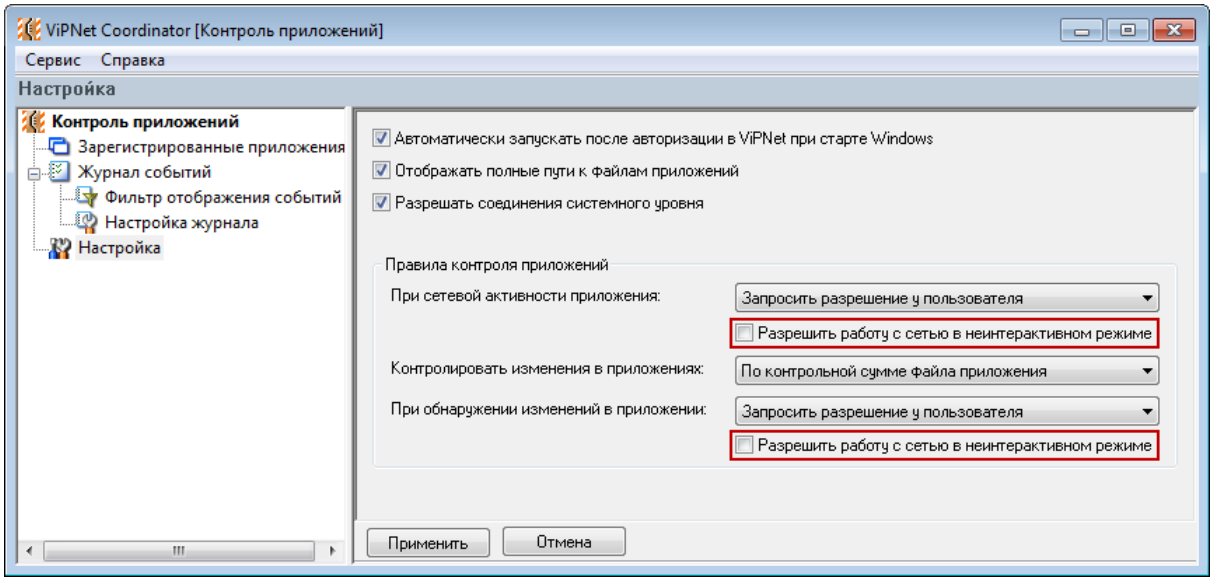


Рисунок 19: Настройка обработки запросов на работу в сети в неинтерактивном режиме

3 Нажмите кнопку **Применить**.

В результате при обработке запросов приложений в неинтерактивном режиме работа приложений в сети будет запрещена.

Настройка параметров журнала событий

Программа «Контроль приложений» позволяет настроить максимальный размер журнала событий (см. «Просмотр журнала событий» на стр. 49), тип регистрируемых событий, параметры обновления журнала. Чтобы настроить параметры журнала событий:

1. В главном окне программы разверните **Журнал событий.**
2. На панели навигации выберите **Настройка журнала.**
3. Чтобы установить максимальный размер журнала, в соответствующем поле укажите нужное значение (в мегабайтах). При достижении максимального размера журнала все записи в хронологическом порядке перемещаются в архив журнала. При значении 0 ограничения на размер журнала отсутствуют.

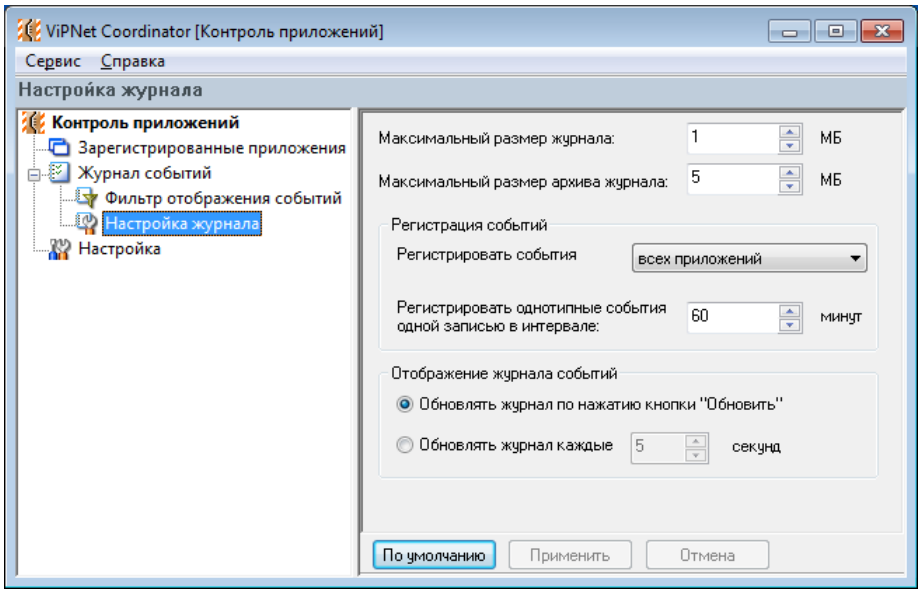


Рисунок 20: Настройка параметров журнала

4. Чтобы установить максимальный размер архива журнала, в соответствующем поле укажите нужное значение (в мегабайтах). При достижении максимального размера архива журнала наиболее старые записи удаляются. При значении 0 ограничения на размер архива журнала отсутствуют.

5 В группе **Регистрация событий** в списке **Регистрировать события** выберите тип приложений (разрешенные, запрещенные, все), изменения статуса которых будут регистрироваться в журнале.

Внимание! Независимо от значения, выбранного в списке **Регистрировать события**, в журнале фиксируются все события, связанные с изменением списка зарегистрированных приложений (события с кодами 3, 4, 5, 6, 7, 8, 13, 14).

6 В поле **Регистрировать однотипные события одной записью в интервале** укажите значение в минутах. По умолчанию установлено 60. В результате все однотипные события, то есть события с одинаковыми параметрами, кроме времени, будут зарегистрированы одной записью.

Примечание. Чтобы регистрировать каждое событие отдельной записью, укажите для интервала значение 0 минут.

7 Чтобы настроить обновление журнала событий, в группе **Отображение журнала** событий:

- Для обновления журнала вручную выберите **Обновлять журнал по нажатию кнопки «Обновить».**
- Для автоматического обновления журнала выберите **Обновлять журнал каждые** и укажите период обновления в секундах.

8 Нажмите кнопку **Применить.**

Таким образом, будет определен размер журнала и архива журнала, тип регистрируемых событий и способ обновления журнала событий.

Настройка фильтра отображения событий

Параметры событий, отображаемых в разделе **Журнал событий**, указываются в настройках фильтра отображения событий. Возможность фильтрации событий позволяет найти конкретные события, например, события, ассоциируемые с определенным приложением или IP адресом.

Чтобы настроить фильтр отображения событий:

1. В главном окне на панели навигации разверните **Журнал событий**.
2. Выберите **Фильтр отображения событий**.
3. Чтобы определить период времени, за который будут отображены события, в группе **Время отображения событий** выберите один из предлагаемых вариантов и укажите интервал времени.

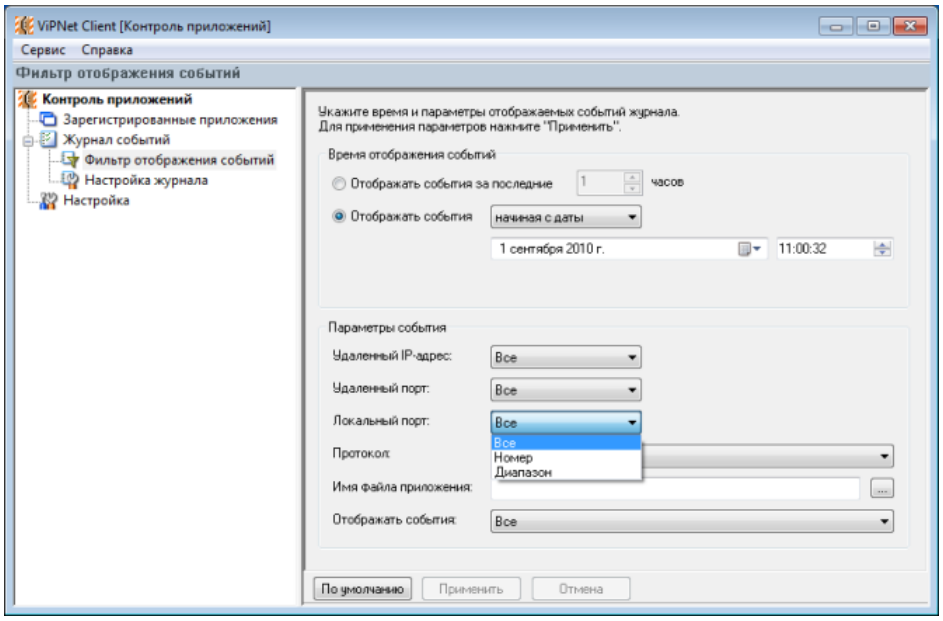


Рисунок 21: Окно настройки фильтра отображения событий

4. Чтобы настроить остальные параметры события, такие как удаленные IP-адрес и порт, локальный порт, протокол, имя файла приложения, тип отображаемого события, в группе **Параметры события** установите нужные значения.

5 Нажмите кнопку **Применить**.

Например, необходимо просмотреть события, ассоциируемые с торрент-клиентом uTorrent за определенный промежуток времени — 1 апреля 2011 года по 15 апреля 2011 года. Для этого:

1 В главном окне на панели навигации разверните **Журнал событий**.

2 Выберите **Фильтр отображения событий**.

3 В группе **Время отображения событий** в списке **Отображать события** выберите **В интервале** и укажите нужные даты.

4 В группе **Параметры события**:

- В списке **Протокол** выберите TCP (Transmission control protocol).
- В поле **Имя файла приложения** укажите `utorrent.exe`.
- Убедитесь, что в списке **Отображать события** выбрано **Все**.

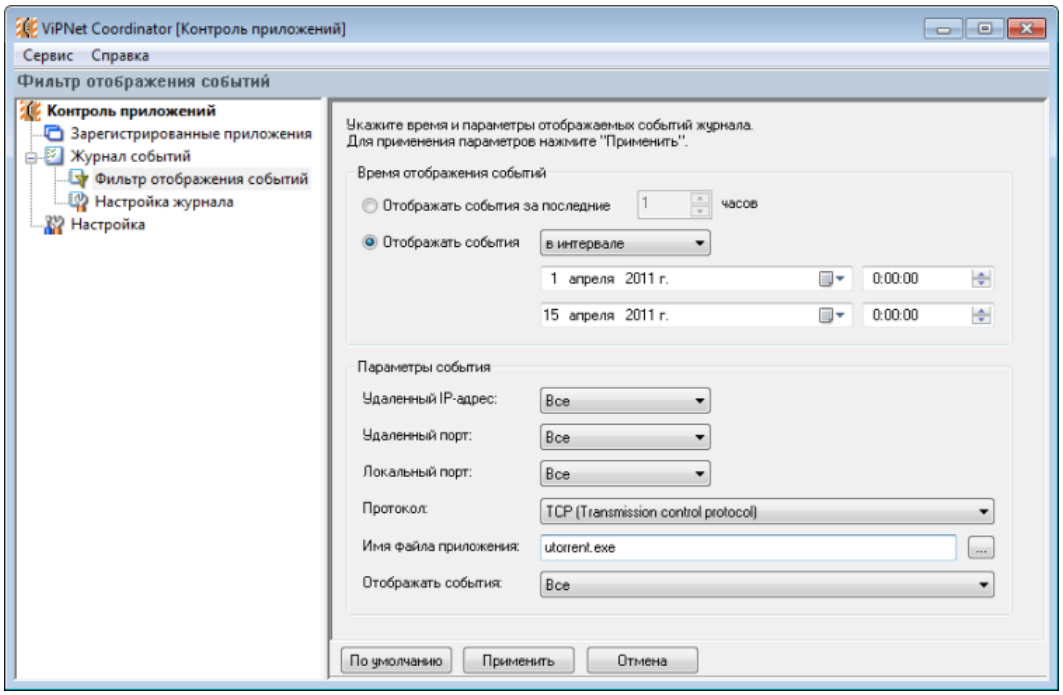


Рисунок 22: Настройка фильтра отображения событий торрент-клиента uTorrent

5 Нажмите кнопку **Применить**.

В результате в разделе **Журнал событий** будут отображаться только события, соответствующие сделанным настройкам.

Глоссарий

А

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

И

Интерактивное правило контроля приложений

Одно из правил контроля приложений, применяемых в программе ViPNet Контроль приложений, при котором пользователь сам определяет дальнейшие действия при обработке запроса приложения на работу с сетью. К интерактивным правилам контроля приложений относятся:

- «Разрешить с запросом пользователя»;
- «Запросить разрешение у пользователя»;
- «Запретить с запросом пользователя».

Л

Лицензия

Разрешение на пользование определенным набором функций ПО ViPNet. Лицензия на сеть ViPNet определяет: максимальное количество координаторов, клиентов на координатор, незащищенных узлов для туннелирования одним координатором (туннелируемых соединений) и некоторые другие параметры.

Н

Неинтерактивный режим

Режим обработки запросов приложений на работу с сетью программой ViPNet Контроль приложений, при котором программа «Контроль приложений» автоматически может определить, какое действие применить при обработке запроса приложения.

П

Пароль администратора сетевого узла ViPNet

Пароль для включения на сетевом узле ViPNet режима администратора, в рамках которого появляются дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан в УКЦ или ViPNet Network Manager администратором сети ViPNet.

См. также: Сетевой узел ViPNet (на стр. 63).

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

См. также: Пароль администратора сетевого узла ViPNet (на стр. 63), Сетевой узел ViPNet (на стр. 63).

С

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью или ViPNet Network Manager.

Указатель