



**VIRSHIELD  
SECURITY SOFTWARE.**

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

## ОГЛАВЛЕНИЕ

<b>РИСУНКИ</b> .....	3
<b>ГЛАВА 1</b> .....	4
<b>УСТАНОВКА И НАСТРОЙКА VIRSHIELD</b> .....	4
<b>Установка и настройка приложения</b> .....	4
<b>Обновление приложения</b> .....	4
<b>Удаление приложения</b> .....	4
<b>ГЛАВА 2</b> .....	5
<b>ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ VIRSHIELD</b> .....	5
<b>Главное меню</b> .....	6
<b>Internet Security</b> .....	6
<b>Program Settings</b> .....	6
<b>Browsing Reports</b> .....	6
<b>Help And Support</b> .....	7
<b>ГЛАВА 3</b> .....	8
<b>INTERNET SECURITY</b> .....	8
<b>FireWall</b> .....	8
<b>Program Control</b> .....	10
<b>Expert Rules</b> .....	11
<b>ГЛАВА 4</b> .....	13
<b>PROGRAM SETTINGS</b> .....	13
<b>General options</b> .....	13
<b>White list</b> .....	13
<b>ГЛАВА 5</b> .....	14
<b>BROWSING REPORTS</b> .....	14
<b>Detected infections</b> .....	14
<b>Visited Websites</b> .....	15
<b>Bloced Websites</b> .....	15
<b>ГЛАВА 6</b> .....	16
<b>HELP AND SUPPORT</b> .....	16
<b>ПРИЛОЖЕНИЕ</b> .....	17

## РИСУНКИ

- Рисунок 2.1 Принцип работы FireWall
- Рисунок 2.2 Главное Диалоговое окно VirShield
- Рисунок 3.1 Диалоговое окно FireWall
- Рисунок 3.2 Диалоговое окно для управления степенью доступа приложения
- Рисунок 3.3 Диалоговое окно Program Control
- Рисунок 3.4 Диалоговое окно организации элементарного фильтра
- Рисунок 5.1 Диалоговое окно отображения статистических данных

# ГЛАВА 1

## УСТАНОВКА И НАСТРОЙКА VIRSHIELD

В этой главе содержится информация о том как установить, настроить, обновить и удалить VirShield, а так же какие системные требования необходимы для данного приложения.

### Установка и настройка приложения

Для того что бы установить интернет-защиту VirShield необходимо иметь установочный файл нужной Вам версии. Его можно скачать с сайта <http://www.access-filter.com/index.php?com=download>. После этого, нажав двойным щелчком левой кнопки мышки на иконке установочного файла, вы запустите установку приложения. С помощью VirShield Setup Wizard установка пройдёт на интуитивно понятном уровне и не создаст пользователю лишних неудобств. Необходимо просто следовать инструкциям и нажимать соответствующие кнопки. Ниже показан процесс установки после того как Вы уже скачали установочный файл:

1. Двойной щелчок мышкой на установочном файле (Запустится VirShield Setup Wizard);
2. Нажимаем кнопку „Next“ (появится окошко с запросом о согласии с лицензией продукта);
3. устанавливаем галочку на "I Agree" и нажимаем кнопку „Next“;
4. В появившемся окне у Вас появляется возможность выбрать путь установки приложения, а так же право пользования VirShield. Для выбора пути можно воспользоваться кнопкой "Browse.." либо прописать его вручную. "Disk Cost..." покажет вам доступное место на имеющихся у вас носителях. Для управления правом пользования приложением имеется 2 флажка: при выборе флажка "Just me" приложением сможет пользоваться только пользователь с учётной записью в которой происходит данная установка; при выборе флажка "Every One" приложением смогут пользоваться все пользователи данного компьютера. После того как были проведены необходимые настройки нужно нажать кнопку "Next";
5. Нажимаем кнопку "Next" для окончания установки;
6. "VirShield" произведёт необходимые настройки и копирование файлов, после чего предложит вам перезагрузить компьютер для полного завершения установки приложения. Сохраните все необходимые вам файлы и согласитесь с перезагрузкой.

### Обновление приложения

При появлении новой версии VirShield, приложение сообщит Вам об этом и укажет путь от куда можно будет скачать новую версию. После того как новая версия будет скачана, необходимо повторить стандартную процедуру установки приложения, которая описана выше. При этом настройки будут сохранены, а версия приложения будет обновлена.

### Удаление приложения

Для удаления приложения сделайте следующие шаги:

1. Зайдите в: Start->Settings->Control Panel->Add or remove Programs
2. В появившемся окне найдите приложение VirShield;
3. нажмите на него 1 раз мышкой
4. нажмите на кнопку "Remove"

После этого начнётся удаление приложения.

## ГЛАВА 2

### ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ VIRSHIELD

Эта глава содержит описание основных инструментов и концепций VirShield.

VirShield - это программное обеспечение предназначенное для безопасного интернет-серфинга и защиты трафика пользователя. При посещении пользователем того или иного сайта в сети Интернет возможен риск заражения компьютера вредоносным программным обеспечением таким как MalWare, SpyWare или BadWare что может привести к заражению вашего персонального компьютера. VirShield работает таким образом что при посещении "плохого" сайта он информирует пользователя о предостерегающей опасности, переводя его на страничку своего сервера, где пользователь получит всю доступную и необходимую информацию о "плохом" сайте. После ознакомления с информацией о бэд-страничке пользователь должен решить стоит ли ему разрешить посещение "плохого" сайта и подвергнуться возможному заражению или всё таки отклонить запрос и остаться не инфицированным. Если пользователь разрешит посещение, то посещаемый сайт попадёт в так называемый "белый" список White List. Сайты, находящиеся в этом списке не проверяются приложением и пропускаются им безоговорочно. Если пользователь всё-таки запретил запрос, то блокируется вся информация идущая с "плохого" сайта. Заблокированные объекты можно при этом посмотреть в разделе "Browsing Reports"->Blocked Websites. Благодаря огромной базе данных "плохих" сайтов, которая обновляется несколько раз в сутки, VirShield обеспечивает достаточно высокую защиту вашего Интернет-путешествия.

Кроме проверки посещаемого сайта, пользователь имеет возможность так же настроить персональную защиту компьютера с помощью FireWall. Наличие такой защиты позволяет пропускать или блокировать информацию, поступающую из сети на различных уровнях. Работа FireWall основана на добавлении или удалении правил. Благодаря специальной системе и алгоритму, правило можно настроить на столько гибко, что набор правил может покрыть практически весь необходимый спектр защиты для пользовательского компьютера. Есть возможность контролировать информацию как исходящую так и входящую, возможность указывать спектр IP-адресов, с которых нужно разрешить/запретить передачу данных, Контроль передачи данных по определённым протоколам; Контроль пакетов входящих / исходящих на определенные порты и т.д. Работа данного брэндмаура основана на работе NDIS драйвера.

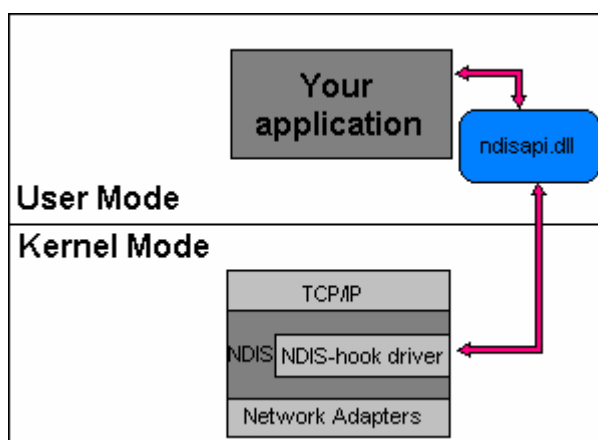


Рис. 2-1 Принцип работы FireWall

Графический интерфейс приложения представляет из себя следующее: VirShield состоит из одного диалогового окна с главным меню и внутреннего диалогового окна с установками для определённой вкладки главного меню.

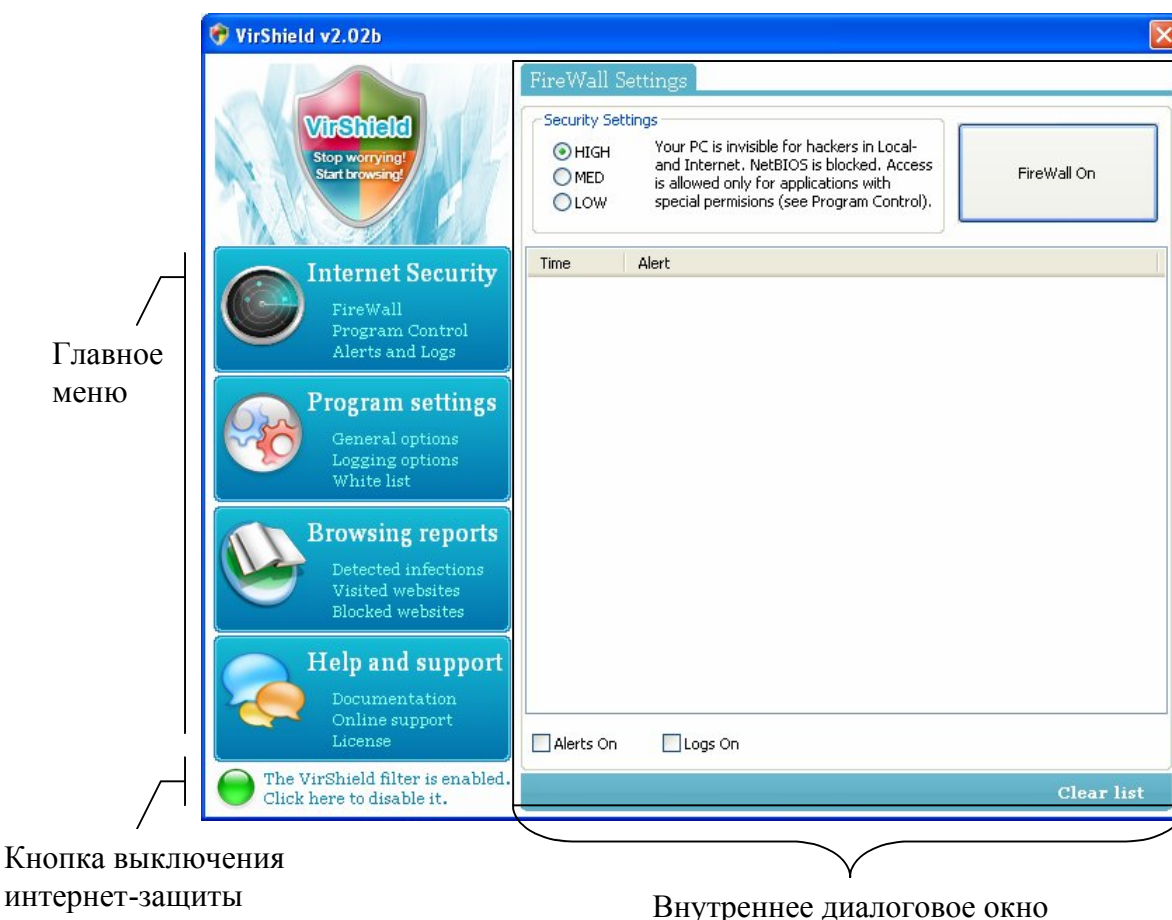


Рис. 2-2 Главное Диалоговое окно VirShield.

### Главное меню

содержит несколько разделов, внутри которых имеются собственные подразделы.

### Internet Security

предназначен для настройки и диагностики пакетов и программ которые имеют / получают доступ к сети (локальной и Интернет). Тут есть возможность настроить личную защиту компьютера и указать нужным приложениям степень доступа к сети. Ведётся также учёт событий связанных с выходом того или иного приложения или пакета в сеть.

### Program Settings

позволяет пользователю настроить VirShield под себя.

### Browsing Reports

содержит информацию о посещаемых и заблокированных приложением сайтах.

## **Help And Support**

содержит описание лицензии, документацию и контакты службы поддержки, по которым пользователь может связаться с инженерами и задать свои вопросы относительно данного приложения.

В зависимости от выбранного подраздела во *внутреннем диалоговом окне* появляются соответствующие настройки и информации. Более детально это будет описано ниже.

**Кнопка включения/выключения интернет-защиты** предназначена для временного или постоянного отключения проверки посещаемых сайтов. Настройки, которые относятся к данной кнопке можно найти в подразделе "General Settings".

## ГЛАВА 3

### INTERNET SECURITY

В данном разделе будут описаны работа и методы настройки интернет-защиты. Раздел Internet Security состоит из трёх подразделов которые между собой тесно связаны:

1. FireWall;
2. Program Control
3. Expert Rules

#### FireWall

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. [Wikipedia].



Рис. 3-1 Диалоговое окно FireWall

После запуска приложения у пользователя есть возможность выбрать одну из трёх степеней защиты для своего компьютера. Эти установки действуют только на брандмауэр. При выборе флажка HIGH, компьютер пользователя полностью защищён от внешнего вторжения и от отправки несанкционированных пакетов информации в сеть (как локальную так и Интернет). Выбрав данный флажок блокируются все порты, включая NetBIOS. Открытыми остаются только те порты, которые необходимы для выхода в Интернет (DNS, DHCP и HTTP), а так же те которые используются приложениями со специальным статусом. Этот статус пользователь выбирает в подразделе Program Control. Активация степени защиты HIGH также активизирует так называемый режим невидимки (stealth mode), что позволяет оставаться компьютеру невидимым во всей сети.

При выборе флажка MED (средняя степень защиты) компьютер пользователя остаётся невидимым только для сети Интернет. Обмен данными между компьютерами локальной сети разрешён. Порты остаются закрытыми кроме тех которые нужны для выхода в Интернет и тех которые принадлежат приложениям с определённым статусом (статус приложения указывается в Program Control).

При самой низкой степени защиты (LOW) компьютер пользователя виден абсолютно во всей сети, порты все открыты. Учитываются только порты приложений с определённым статусом.

После того как пользователь выбрал нужную ему степень защиты, можно включить FireWall, нажав на кнопку в верхнем правом углу. Этой же кнопкой есть возможность также остановить работу FireWall.

При первом запуске брандмауэра, происходит анализ всех приложений имеющих в данное время доступ к сети. Для каждого такого приложения высвечивается диалогов окно с информацией о программе. В этом диалоговом окне пользователь имеет возможность ознакомиться с некоторыми свойствами приложения и указать степень доступа данного приложения для выхода в сеть.

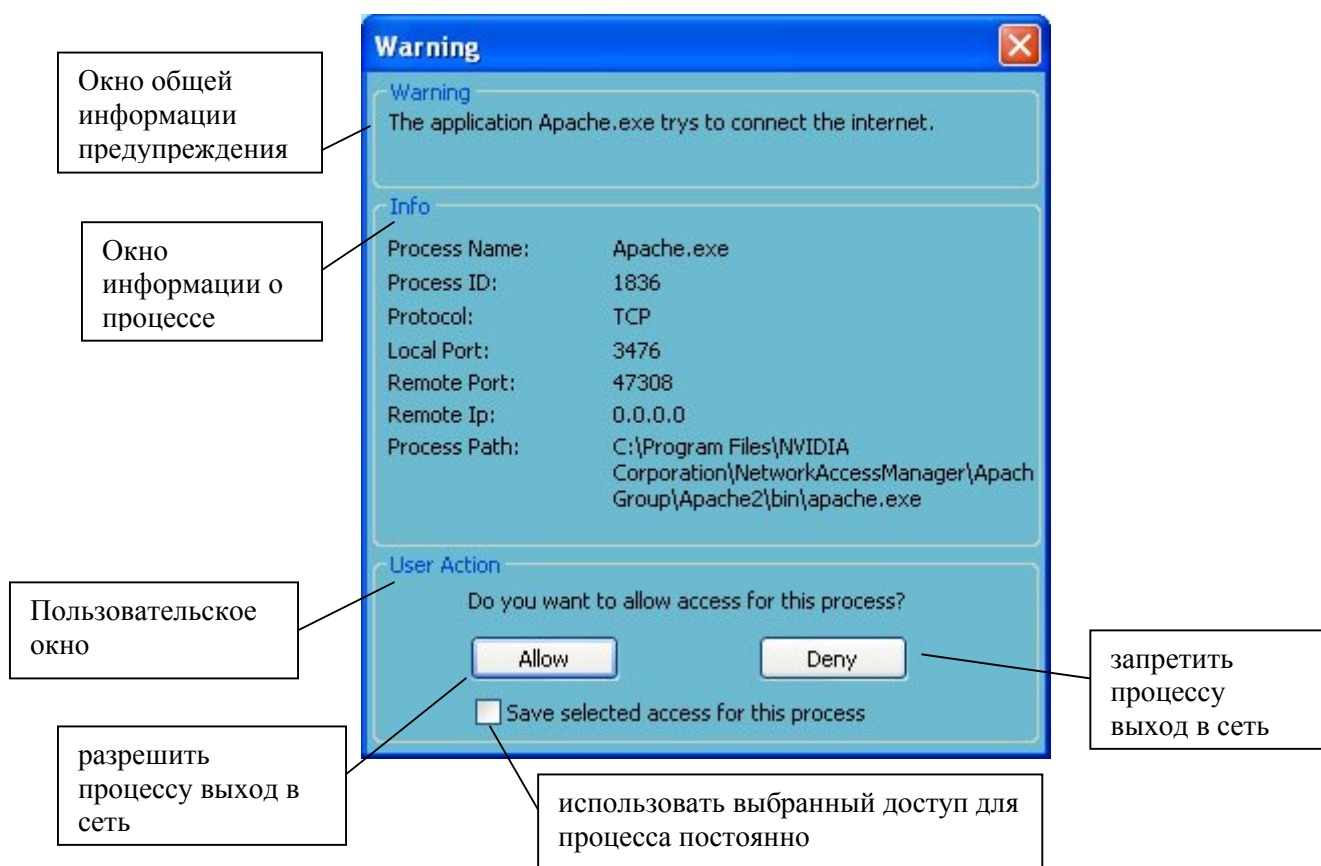


Рис. 3-2 Диалоговое окно для управления степенью доступа приложения

Во время дальнейшей работы брандмауэра, ведётся анализ и проверка исходящих и входящих пакетов. В случае выхода в Интернет нового приложения (которое еще не получило никакого статуса доступа) VirShield заблокирует его до тех пор пока пользователь не определит должно ли приложение выходить в Интернет или нет. После того как доступ в сеть приложения был определён, необходимо нажать соответствующую кнопку:

1. Allow - если приложение получает доступ к сети;
2. Deny - если приложение не должно выходить в сеть;

Встречается такая ситуация что приложение использует несколько портов (Opera.exe, IEexplorer.exe, avp.exe(Касперский) и т.д.). При этом VirShield будет информировать пользователя о каждом порте. Для того что бы уменьшить затраты времени, есть возможность указать выбранную степень доступа для всего приложения и всех портов которые оно использует. Для этого необходимо поставит галочку внизу "диалогового окна управления степенью доступа" (см. рис. 3-2).

Во время работы FireWall, пользователю предоставляется также информация о встречающихся предупреждениях (Alert). В Диалоговом окне брандмауэра имеется окно-список отображающее их. Что бы включить отображение предупреждений и событий необходимо поставить галочки внизу диалогового окна FireWall с названием "Alert On". В окне-списке по определённому событию начнут появляться возникшие во время работы предупреждения и события со временем их появления. Есть также возможность протоколирования процесса защиты. Для этого необходимо поставить галочку в окошке "Logs On", после чего все предупреждения, события и действия будут записаны в файл который по умолчанию хранится в C:\Documents and Settings\All Users\Application Data\BPGroup\VirShield\Log.txt.

### **Program Control**

Диалоговое окно подраздела Program Control показано на рис. 3-3. В этом окне отображаются процессы, которые получили определённые степени доступа в сеть. Имеется две степени доступа: доступ разрешён и доступ запрещён. Для каждого типа доступа имеются соответствующие окна. В этих окнах в виде списков находятся процессы со своим именем и идентификационным номером в системе. При выделении какого-нибудь процесса в нижнем окне "Program Description" появляется информация касающаяся данного процесса:

- его имя,
- идентификационный номер,
- степень доступа о порты которые заняты этим процессом и т.д.

Для случая если степень доступа процесса необходимо изменить у пользователя есть две кнопки находящиеся между списком разрешенных и запрещённых процессов. Нажав на соответствующую стрелочку пользователь переносит процесс из одного списка в другой, тем самым меняя его доступ в сеть.

Возможна такая ситуация когда необходимо предопределит степень доступа определённого приложения. То есть определить доступ приложения до того как оно начнёт выходит в сеть. Для этого есть кнопки "Add Program" и "Remove Program" расположенные в нижнем левом углу окна "Program Control". С помощью этих кнопок пользователь имеет возможность добавит или удалить определённый процесс в соответствующий список.

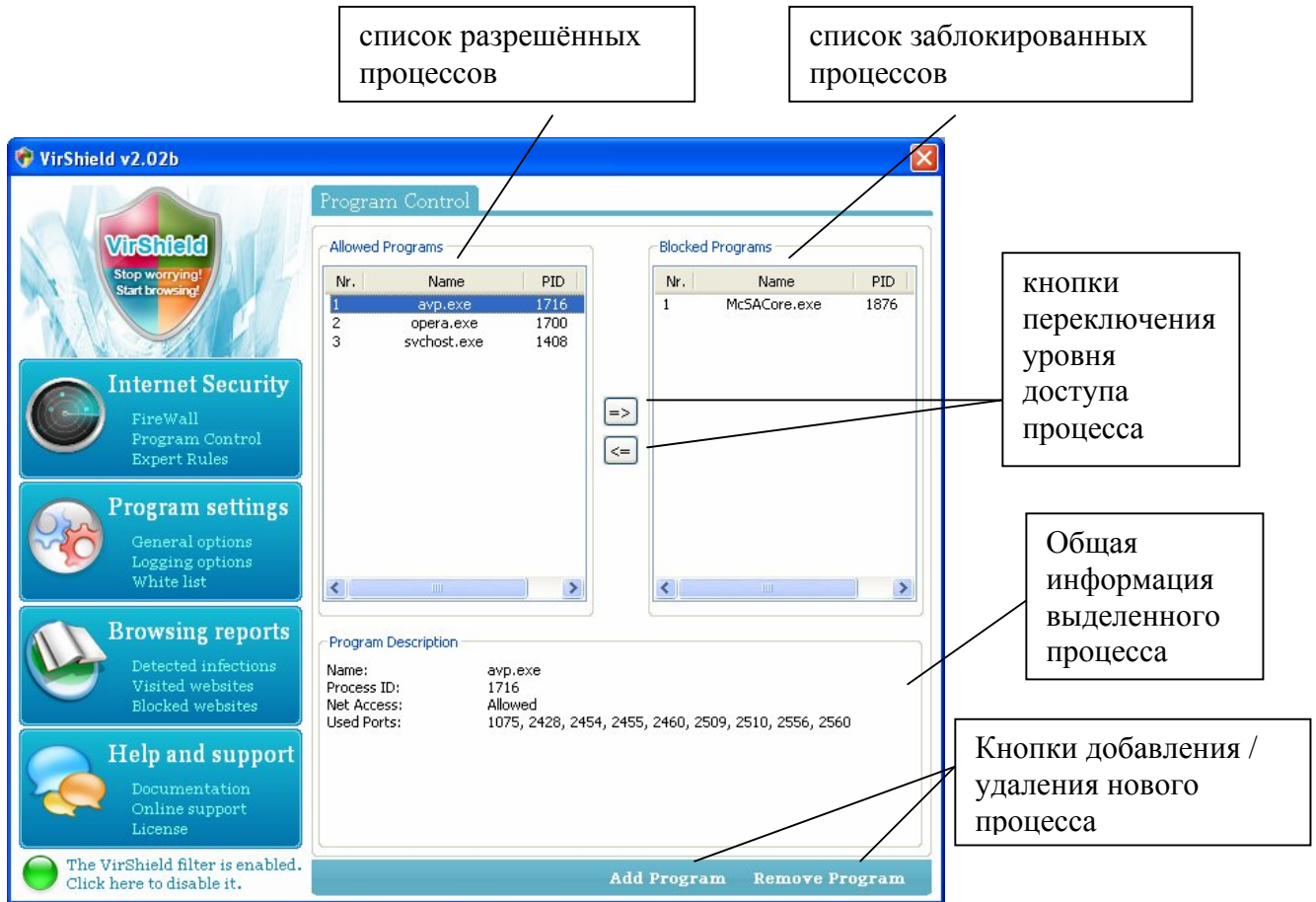


Рис. 3-3 Диалоговое окно Program Control

### Expert Rules

VirShield FireWall - обладает так же функцией добавления / удаления так называемых правил. В данном контексте под словом "правило" понимается элементарный фильтр в котором одновременно можно указать фильтрацию на нескольких уровнях сетевой модели. Пользователь имеет возможность в одном правиле указать свойства доступа (разрешить / запретить) для входящих / исходящих пакетов, указав при этом спектр IP-адресов и/или сетевой протокол и/или спектр портов для которых будет происходить фильтрация. За счёт такого набора элементарных правил пользователь может обеспечить полную безопасность своего персонального компьютера.

Ниже показан пример использования диалогового окна для создания элементарного фильтра. Описание этого правила звучит следующим образом: *Разрешить входящие пакеты по протоколу ICMP, которые идут с IP-адресов с 58.58.45.86 по 158.48.56.1 и приходят на локальные порты с 58 по 8120.*

Диалоговое окно создания фильтра состоит из трёх подокон: "Main Settings" (окно основных настроек), "Filter Description" - окно с описанием правила и "Advanced Setting" - дополнительные настройки.

В окне основных настроек выбираются следующие параметры для фильтра:

- действие фильтра;
- направление фильтруемых пакетов;
- IP-адреса (вх / вых в зависимости от выбранного направления пакетов). Тут есть возможность выбрать как просто один определённый адрес, так и задать границы фильтруемых адресов, либо указать подсеть которую надо фильтровать;
- протокол который необходимо фильтровать

- номера портов. Есть возможность выбрать как локальный порт так и порт с которого поступает информация, а так же границы портов.

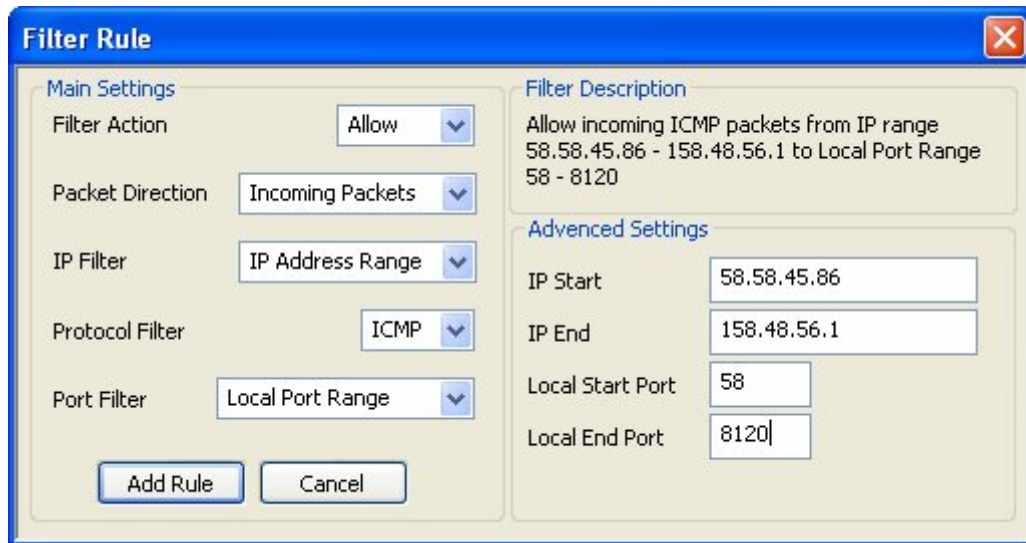


Рис. 3-4 Диалоговое окно организации элементарного фильтра

После того как пользователь создал правило и добавил его, оно попадает в общий список правил FireWall (добавляется к уже установленным степеням защиты). Если включена низкая степень защиты то действуют только те правила которые пользователь создал в подразделе "Expert Rules". Список пользовательских правил отображается так же в этом подразделе в диалоговом окне.

## ГЛАВА 4

### PROGRAM SETTINGS

Programm Settings - раздел в котором пользователь имеет возможность настроить VirShield так как ему удобно. Он состоит из трёх подразделов: " General options" - главные настройки, "Loggin options" - настройки протоколирования и "White List" - белый список.

#### General options

В данном подразделе пользователь может настроить следующие параметры:

- Start with Windows. При выборе данного параметра VirShield будет запускаться каждый раз с запуском ситемы.
- Show system tray icon. Отображение иконки приложения в трэе системы (иконка в правом нижнем углу рабочего стола).
- Start minimized. При выборе данного параметра во время начала работы VirShield главное диалоговое окно отображается как свёрнутое. Если при этом еще стоит галочка отображения иконки в трэе, то оно отобразится как иконка в трэе, в противном случае как стандартное свёрнутое окно, его можно будет найти в панели задач.
- Autorestart protection. Автоматическое включение VirShield через определённое время после его выключения вручную. Это время перезапуска можно тоже установить (задаётся в минутах).

#### White list

Во время интернет-серфинга VirShield информирует пользователя если тот попадает на вредоносный сайт. При этом в браузере открывается web-страничка VirShield с информацией о вредоносности сайта, где также предоставляется возможность выбора дальнейшего посещения зараженной странички. В случае если пользователь одобрит посещение странички и пожелает что бы VirShield больше её не блокировал - он нажимает на "Всегда пускать". После этого хост странички попадет в белый список. В процессе работы VirShield, при посещении пользователем какого-нибудь сайта проверяет его наличие в белом списке. В случае если данный сайт присутствует в этом списке, то дальнейший анализ странички пропускается и пользователь получает доступ к запрашиваемому адресу. Если же сайта в белом списке нет, то он проверяется на вредоносность и выводится результат.

У пользователя есть также возможность вручную ввести имя "белой" странички, которую VirShield не будет анализировать. Так же можно загрузит / сохранить целый список по указанному месту. Для этого в диалоговом окне подраздела "White List" имеются соответствующие кнопки.

## ГЛАВА 5

### BROWSING REPORTS

В процессе работы VirShield идёт проверка посещаемых страничек. Информация о посещаемых сайтах и результат их анализа отображается в разделе Browsing reports. Этот раздел состоит из трёх подразделов:

- "Detected Infections"
- "Visited websites"
- "Blocked websites"

#### Detected infections

Диалоговое окно, которое отображает название сайта, содержащего вирусы. В данном окне ведётся так же учёт количества проверенных и заблокированных интернет-страниц. Параллельно с этим отображается также количество известных вредоносных и инфицированных страничек.

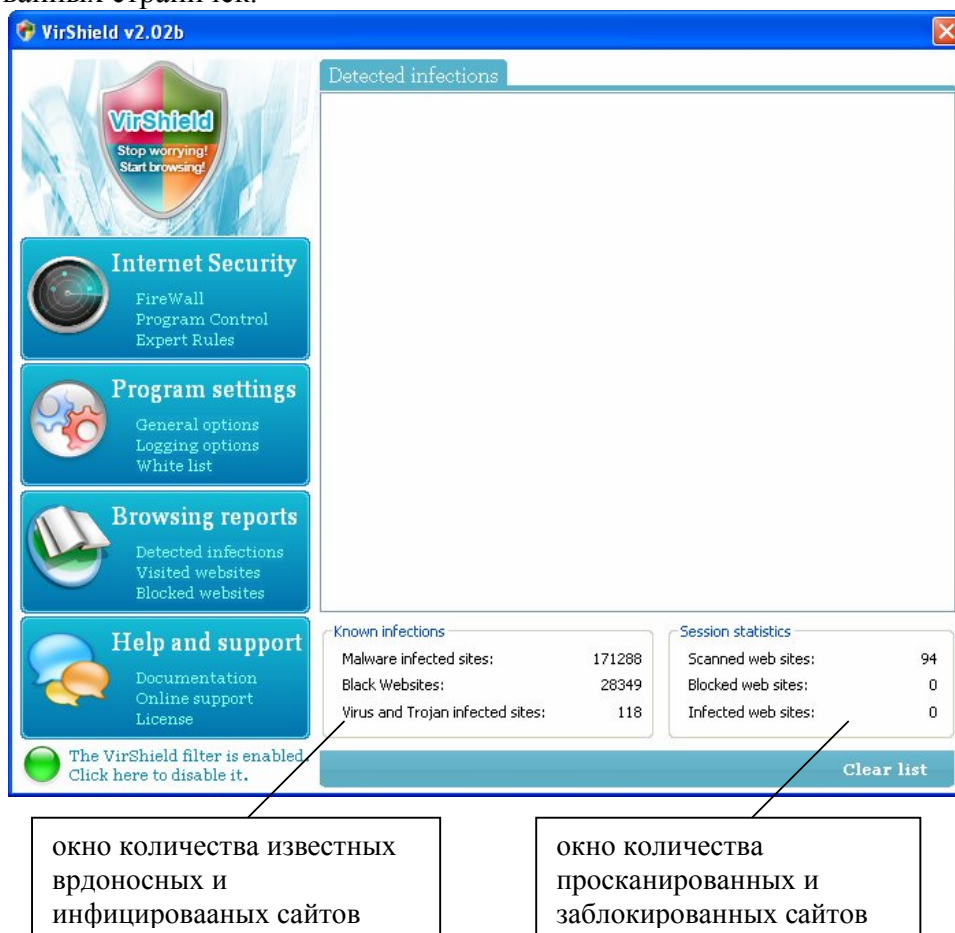


Рис. 5-1 Диалоговое окно отображения статистических данных

**Visited Websites**

в этом диалоговом окне отображается список посещённых сайтов и объектов. Есть возможность очистить данный список при помощи кнопки "Clear List" которая находится в правом нижнем углу окна.

**Blocked Websites**

Если VirShield заблокирует какой-нибудь сайт, на который пользователь собирается зайти, то имя этой странички попадает в список заблокированных сайтов. Этот список можно так же очистить, нажав кнопку "Clear List" в правом нижнем углу окна.

## ГЛАВА 6

### HELP AND SUPPORT

В данном разделе имеется три подраздела:

- документация,
- поддержка
- описание лицензии.

#### **Documentation**

В данном подразделе находятся ссылки на описания соответствующих тем. Нажав на интересующую ссылку пользователь попадает на сайт [www.access-filter.com](http://www.access-filter.com), где и будет описана тема.

В случае выявления каких-нибудь ошибок или неясных ситуаций в приложении, пользователь в любое время может послать запрос в службу поддержки и инженеры постараются как можно быстрее решить возникшую проблему.

В подразделе *License*, пользователь имеет возможность еще раз ознакомиться с правами распространяющимися сданным программным обеспечением.

**ПРИЛОЖЕНИЕ**