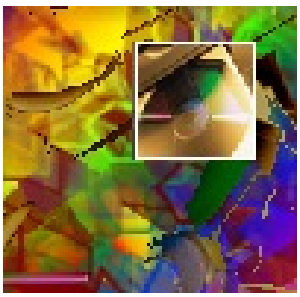
Полное руководство пользователя

Lavasoft Ad-Aware SE Professional



Автор: Максим Вихарев
Дата создания: 29.11.2004

Приобретение продуктов Lavasoft в России:
Продукты Lavasoft Ad-Aware можно приобрести в интернет-магазине www.avsoft.ru
По вопросам приобретения корпоративных версий продуктов обращайтесь по адресу sales@avsoft.ru
Подробная информация о продуктах - www.adaware.ru

Содержание

Что такое Ad-Aware SE?

Ad-Aware SE – последняя версия завоевавшей многочисленные награды программы класса антишпионского программного обеспечения (antispyware). Эта программа – весьма простое, но в тоже время и весьма серьезное решение для сохранения вашей приватности. В версии SE используется новая технология Code Sequence Identification (CSI) (Идентификация Последовательности Кода), которая позволяет защищать вас от новых и неизвестных еще вариантов вредоносных программ, реклам, шпионов и так далее.

Разработанный для Windows 98, Windows 98SE, Windows ME, Windows NT 4, Windows 2000 и Windows XP Home/Professional Lavasoft Ad-Aware SE Professional предлагает самую эффективную защиту приватности, которая когда-либо предлагалась Lavasoft. Новое издание программы всесторонне проверит память, системный реестр, жесткие, сменные и оптические диски на предмет дата-минеров, агрессивного рекламирования, паразитов, скамвара, кейлоггеров, троянов, диалеров, мальвара, налетчиков браузера и трэкинг компонентов.

Смотри далее список изменений в новой версии Ad-Aware SE Professional или системные требования.

Список изменений в Ad-Aware SE

- Новые параметры командной строки, которые помогают автоматизировать выполнение операций Ad-Aware.
- Поддержка UNC (протокола INTERNET), то есть поддержка настроек, определений и журналов Интернет.
- Новый способ выведения экранов результатов и детальной статистики.
- Улучшенный способ ведения журналов и сообщений.
- Защита против несанкционированного удаления программы со стороны сторонних программ плюс зашифрованные файлы определений.
- Ссылки для большей информации об обнаруженных объектах (на сайте Lavasoft).
- Новая опция безопасности, позволяющая защищать чувствительные системные файлы (типа host).

Улучшен механизм сканирования:

- Расширенная защита против DLL-инъекций, SE может выгрузить модули процесса на лету;
- Расширенный режим сканирования памяти;
- Сканирование абсолютно всех модулей процесса;
- Использование новой технологии CSI (Идентификация Последовательности Кода) для идентификации новых неизвестных вариантов вредоносного контента.

Расширенный просмотр системного реестра:

- Сканирование разделов реестра многопользовательских учетных записей;
- Дополнительные сильные проверки для обнаружения динамически созданных ссылок;
- Увеличение скорости сканирования.

Расширенное сканирование дисков:

- Сканирование и просмотр переменных потоков данных на NTFS томах;
- Теперь Ad-Aware поддерживает просмотр cab-файлов (включая заполненные архивы);
- Увеличение скорости сканирования;
- Улучшенный просмотр host-файлов;
- Теперь Ad-Aware и Ad-Watch используют меньшие по объему файлы определений.

Усовершенствований интерфейс пользователя:

- Улучшенная графическая оболочка (UI);
- Поддержка шкурок (skins);
- Дополнения и расширения к программе теперь более дружественны к пользователю (выводятся в отдельных окнах);
- Новое выведение результатов сканирования, включая итоги и детальное представление;
- Ad-Aware теперь связан с внешней сетевой базой данных TAC.

Расширенные варианты доводки программы:

- Выгрузка модулей процессов во время сканирования;
- Получение командной строки сканированных процессов;
- Игнорирование заполненных cab-файлов;
- Просмотр системного реестра для всех пользователей вместо только текущего;
- Постоянное кэширование архивов;
- Попытка всегда выгрузить модуль перед удалением;
- Отключение ручного карантирования при выбранном автокарантине;
- Агрессивное блокирование выскакивающих окон (pop-up);
- Загрузка Ad-Watch минимизированным;
- Скрытие иконки Ad-Watch в трее;

- Запись защищенных системных файлов после ремонта;
- Выбор лимита диска на фиксированные диски;
- Использовать линования в списках элемента;
- Сжатие раздела с деталями журнала.

Process-Watch:

- Улучшенный Process-Watch, увеличение производительности и скорости сканирования (Новый движок сканирования);
- Улучшенный графический интерфейс Process-Watch;
- Опция создания думпа памяти процесса (Hexdump) на диск.

Усовершенствование журнала логов:

- Поддержка удаления отдельных логфайлов;
- Возможность добавление референсов в журнал итогов/индекса;
- Файлы логов содержат более подробную информацию.

Ad-Watch:

- Усовершенствован интерфейс пользователя;
- Ad-Watch теперь поддерживает блокирование кукисов;
- Менеджер сайта для редактирования черного списка pop-up-пов;
- Использование Ad-Watch технологии CSI для обнаружения новых и неизвестных вредителей;
- Новый экран конфигурации Ad-Watch;
- Новый редактор правил для предопределенных исключений блокирования;
- Поддержка скрытия значка в трее.

Системные требования

Процессор: P166
Оперативная память: ОС + 24 МБ
Жесткий диск: 25 МБ свободного места (минимальная конфигурация)
Операционные системы:
Windows 98
Windows 98se
Windows Me
Windows NT4 Workstation
Windows NT4 Server
Windows 2000 Pro
Windows 2000 Server
Windows 2003 Server
Windows XP Home
Windows XP Pro
Windows XP (Home/Professional)
Windows XP 64-Bit Edition
Windows Terminal Services
Иное: Internet Explorer version 5.5 или выше.

Начало работы

Приобретение продуктов в России:
Продукты Lavasoft Ad-Aware можно приобрести в интернет-магазине www.avsoft.ru
По вопросам приобретения корпоративных версий продуктов обращайтесь по адресу sales@avsoft.ru
Подробная информация о продуктах - www.adaware.ru

Как загрузить программу (только для лицензионных пользователей)

Внимание! Вначале просмотрите цветовую идентификацию в данном мануале.

При покупке Ad-Aware SE Professional вам придет электронная почта со ссылкой загрузки. Щелкните по ссылке для запуска загрузки, откроется затемненное всплывающее окно «**File Download**». Удостоверьтесь что имя файла – «aawsepro.exe». Нажмите кнопку «**Save**» и выберите папку «**My Documents**». Щелкните «**Save**» и загрузка начнется.

Установка Ad-Aware SE

При установке Ad-Aware на Windows NT, 2000 или XP, удостоверьтесь, что вы имеете привилегии администратора. Ad-Aware должен быть установлен в учетной записи, имеющей адекватные разрешения исполнения. Если вы не уверены, что у вас достаточно прав, или у вас их нет, то свяжитесь со своим системным администратором или обратитесь к справочной системе вашей операционной системы.

1. **Начало установки**

   После окончания загрузки идите в папку «**My Documents**» (или в папку, куда вы сохранили файл aawsepro.exe) и запустите файл «aawsepro.exe» для начала установки.

2. **Экран приветствия (Welcome Screen)**

   Нажмите «**Next**» для перехода к экрану лицензионного соглашения (Agreement Screen)
   Пожалуйста, прочтите лицензионное соглашение до дальнейшей установки программы. Если вы принимаете соглашение, то поставьте галочку рядом с «**I accept the license agreement**» для перехода к продолжению установки. Нажмите «**Next**» для продолжения установки.

3. **Удаление предыдущих версий Ad-Aware**

   Ad-Aware SE не может правильно функционировать, если старые версии не удалены до установки новой версии или обновления. Для гарантирования правильной инсталляции выберите «**Yes, uninstall previous version of Ad-Aware. (Recommended)**» и щелкните «**Next**» для продолжения.

   - **Выпрыгивающее окно для удаления дополнений и расширений Ad-Aware**
     Если у вас установлены старые версии расширений и дополнений Ad-Aware (plug-in), то вам выпрыгнет серое всплывающее окно с подтверждением удаления старых plug-in. Щелкните «**Yes**», чтобы удалить старые дополнения к программе и продолжить деинсталлирующийся процесс.
   - **Выбор метода деинсталляции**
     Выберите «**Automatic**», и щелкните «**Next**».
   - **Выполнение деинсталляции**
     Щелкните «**Finish**» для завершения удаления старых версий Ad-Aware.
   - **Если все в порядке, то появиться сообщение «Uninstall Successful!»**
     Щелкните «**Next**» для продолжения установки Ad-Aware SE Professional.

4. **Выбор директории инсталляции**

   Щелкните «**Next**» для принятия директории инсталляции по умолчанию (рекомендую, так как так у вас будет в дальнейшем меньше проблем с установкой дополнительных расширений программы и языковых модулей) или выберите «**Browse**» для выбора альтернативного места установки Ad-Aware SE Professional.

5. **Установка ярлыков программы в общее для всех пользователей меню All Users**

   Если у вас на компьютере несколько пользователей и вы хотите, чтобы программу могли запускать все из них, то выберите опцию «**Anyone who uses this computer**» и щелкните «**Next**».

6. **Начало инсталляции**

   Щелкните «**Next**» для начала установки Ad-Aware SE Professional на ваш компьютер. После копирования файлов вы должны получить подтверждение, что инсталляция была успешна.

7. **Успешная инсталляция**

   Щелкните «**Finish**» для завершения процесса установки. На выбор вам предлагается сразу обновить файлы определений программы «**Update the definition file**» (рекомендую – всегда приятно иметь последнюю версию определений) и выполнить полную проверку системы «**Run a full system scan**» (тоже не помешает), а также открыть справочную систему программы «**Open the help file now**» (если интересно).

8. **Русификация программы.**

Для русификации программы я рекомендую использовать специальный языковой пакет Lavasoft Ad-Aware SE Language Pack v.1.1 или более поздний. Просто запустите программу установки и следуйте указаниям инсталлятора. После установки пакета в окне программы запустить меню «**Settings**» (значок механизма на инструментальной панели вверху окна программы) и перейти к подменю «**Interface**» (кнопка слева), и далее выбрать в окне «**Language**» русский язык.

Можно также использовать ручную русификацию программы. Для этого поместите файл Russian.awl, идущий в комплекте с данным руководством в директорию
C:\Program Files\Lavasoft\Ad-Aware SE Professional\Lang
И затем выполните шаги, описанные выше.

Выполнение первого сканирования

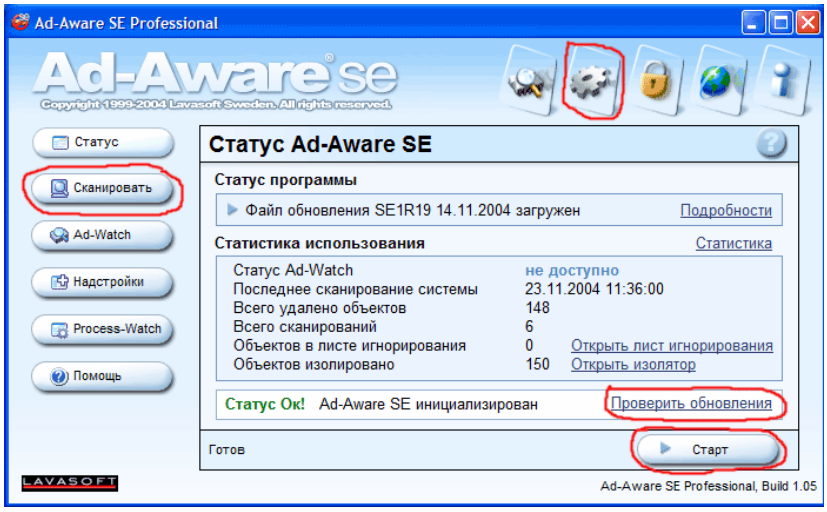


Рисунок 1. Главное окно программы.

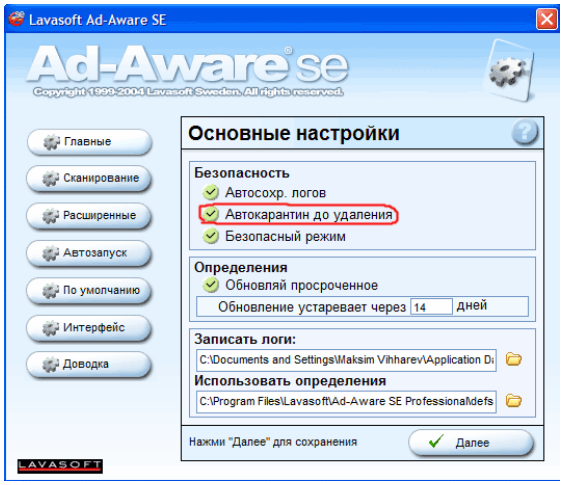


Рисунок 2. Установка автокарантина.

Перед первым сканированием компьютера с Ad-Aware SE необходимо выполнить опцию «**Проверить обновления**» (WebUpdate), чтобы удостовериться, что у вас установлен последний файл определений (см. рис. 1). Также рекомендую включить автокарантирование файлов до их удаления (см. рис. 2). Для этого нажмите кнопку «**Установки Ad-Aware**» (Settings) (символ механизма в верхнем правильном углу главного окна программы) на инструментальной панели запуска. Откроется окно «**Основные настройки**» (General Settings) главных настроек программы. Проверьте, что «**Автокарантин до удаления**» (Automatically quarantine objects prior to removal) включен и затем щелкните «**Далее**» (Proceed) для сохранения изменений.

После того, как проделано вышесказанное, вы готовы к первому сканированию. Щелкните кнопку «**Сканировать**» (Scan now) в главном меню на левой стороне главного окна состояния или нажмите кнопку «**Старт**» (Start) в нижнем правом углу. Откроется окно «**Подготовить сканирование системы**» (Preparing System Scan) (см. рис. 3). Выберите «**Полное сканирование системы**» (Perform Full System scan) и щелкните «**Далее**» (Next) для запуска первого сканирования.

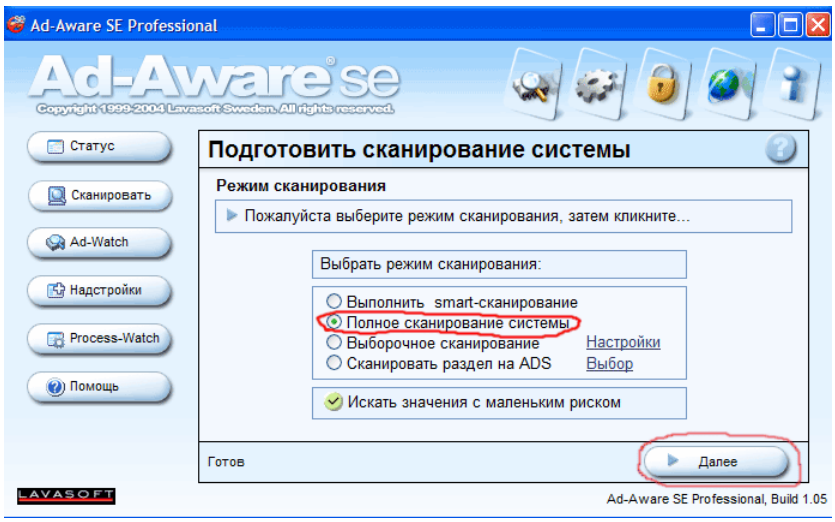


Рисунок 3. Подготовка к сканированию системы.

После завершения сканирования откроется детальный листинг обнаруженных элементов. Внимательно рассмотрите все их перед удалением. Ad-Aware специально разработан для обнаружения и удаления подозрительных вредоносных объектов в вашей системе.

Рисунок 4. Детальная статистика сканирования с выбором объектов через контекстное меню.

Внимание! Производители программы не предлагают, чтобы все обнаруженные объекты были удалены (хотя у меня не разу не было, чтобы программа ошиблась!). Последнее право решения оставлено за пользователем, но для облегчения понимания какой объект действительно вреден была разработана специальная справочная система TAC (диаграммы оценки угрозы) – более подробная информация далее.

Выберите все пункты, которые хотите удалить (если хотите удалить все, то по правому щелчку мыши появится контекстное меню, где есть выбор всех файлов!), а затем щелкните кнопку «**Далее**» (Next) и в появившемся окне «**OK**» для подтверждения удаления (см. рис. 4).

Контекстное меню можно использовать и для осуществления других операций как с отдельными файлами, так и с их группами. Если, например, вы хотите, чтобы некоторые объекты игнорировались даже при дальнейших проверках, то выберите их и через контекстное меню выберите "Игнорировать выбранное" (Add selection to ignore list). Ad-Aware не будет отображать эти элементы в результатах проверок в будущем.

Как только произведена какая-либо отличная от удаления операция с объектами, вы будете возвращены к экрану результатов просмотра, где можно либо выбрать другую операцию, либо выбрать элементы для удаления.

Будьте всегда защищены - установка автоматизации

Для правильной защиты вашего компьютера важно, чтобы файлы дефиниций программы всегда были обновлены. Можно автоматизировать обновление программных файлов дефиниций, сканирования, карантин обнаруженных вредоносных объектов и просмотр с очисткой компьютера при старте операционной системы. Далее приводятся пути автоматизации.

Для настройки автоматизации вам необходимо запустить меню «**Настройки**» (Settings) (значок механизма на инструментальной панели) и выбрать там подменю «**Автозапуск**» (Startup) (кнопка с левой стороны меню) (см. рис. 5).

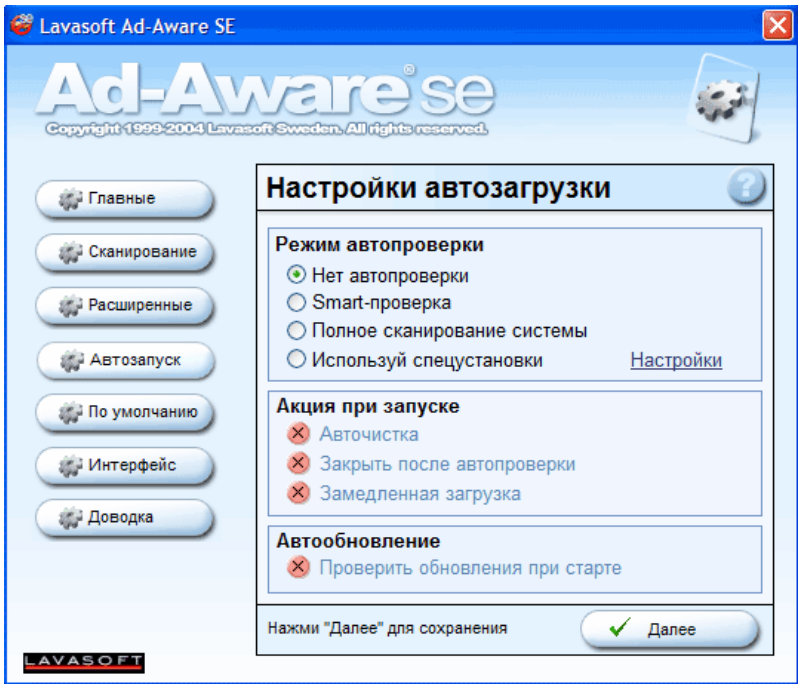


Рисунок 5. Секция автозагрузки в настройках.

Автообновление (Automatic WebUpdate)[1]

В разделе «**Автообновление**» (Auto-Updating) поставьте галочку рядом с «**Проверить обновление при старте**» (Automatically check for updated definitions on startup).

Режим автопроверки (Automatic Scans)

В разделе «**Режим автопроверки**» выбрать режим сканирования:

- **Нет автопроверки** – отключено, то есть при старте компьютера автопроверка проводиться не будет;
- **Smart-проверка** – при старте компьютера будет производиться интеллектуальная проверка;
- **Полное сканирование системы** – при старте компьютера будет производиться полное сканирование системы;
- **Используй спец-установки** – настраиваемая проверка.

Автоматическая очистка (Automatic Cleaning)

В разделе «**Акция при запуске**» (Startup Action) выбрать «**Авточистка**» (Clean automatically).

Автокарантин до удаления (Automatically quarantine objects prior to removal)

Для включения этого режима нажмите кнопку «**Установки Ad-Aware**» (Settings) (символ механизма в верхнем правильном углу главного окна программы) на инструментальной панели запуска. Откроется окно «**Основные настройки**» (General Settings) главных настроек

[1] Необходимо соединение с Интернет

программы. Проверьте, что «**Автокарантин до удаления**» (Automatically quarantine objects prior to removal) включен (см. рис. 2) и затем щелкните «**Далее**» (Proceed) для сохранения изменений.

Интерфейс Ad-Aware SE Professional

В этом разделе подробно приводятся пояснения интерфейса программы. Все описания меню и окон приведены для русской версии Ad-Aware SE. Смотри как русифицировать программу здесь (8 позиция).

Цветовая идентификация

Для облегчения понимания данного мануала я использовал цветовую идентификацию:

- Все окна обозначены **синим цветом**;
- Все разделы меню, которые можно выбрать, обозначены **красным цветом**;
- Все кнопки и ссылки вызова разделов меню обозначены **оранжевым цветом**;
- Тексты в окнах обозначены **малахитовым цветом**.

Инструментальная панель

Ad-Watch
Запускает монитор реального времени Ad-Watch.

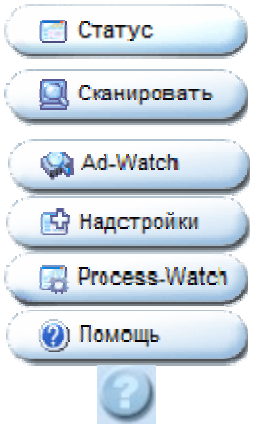
Настройки (Settings)
Открывает главное окно настроек программы.

Карантин (Quarantine)
Открывает менеджер карантина, где можно производить операции с карантированными файлами.

Web обновление (WebUpdate)
Открывает окно "Web обновление", через которое можно обновить свой ref файл (файл определений).

Информация (Information)
Открывает информационное окно Ad-Aware SE, содержащее номер версии и прочую информацию о Ad-Aware SE.

Кнопки основного меню



Показывает статус Ad-Aware.

Открывает окно инициализации проверки системы, в котором можно выбрать режим сканирования.

Запускает монитор реального времени Ad-Watch.

Открывает окно с установленными надстройками и расширениями.

Открывает проводник процессов Process-Watch.

Открывает файл помощи.

Кнопка вызова быстрой помощи, показывает некоторые подсказки.

Окно статуса программы

Статус программы

Показывает текущую версию файла определений, загруженному в Ad-Aware SE. При нажатии на «**Подробности**» выводится детальная информация о файле определений.

Статистика использования

При нажатии на «**Статистика**» выводится детальная статистика программы.

- **Статус Ad-Watch** – показывает загружен ли Ad-Watch.
- **Последнее сканирование системы** – показывает дату и время последнего сканирования системы.
- **Всего удалено объектов** – показывает общее число удаленных объектов.
- **Всего сканирований** – показывает общее число сканирований.
- **Объектов в листе игнорирования** – показывает общее число объектов в листе игнорирования. При нажатии на «**Открыть лист игнорирования**» открывается лист игнорирования.
- **Объектов изолировано** – показывает общее число изолированных объектов. При нажатии на «**Открыть изолятор**» открывается менеджер карантина.

Статус

Статус ОК! – все в порядке, программа готова к работе.

Предупреждение! Файл обновления не найден или поврежден! – необходимо выполнить обновление файла определений. Менеджер «**Web обновления**» запускается через «**Проверить обновления**».

Рисунок 6. Окно статуса программы.

При нажатии на кнопку «**Старт**» программа переходит к окну сканирования системы.

Окно подготовки сканирования системы

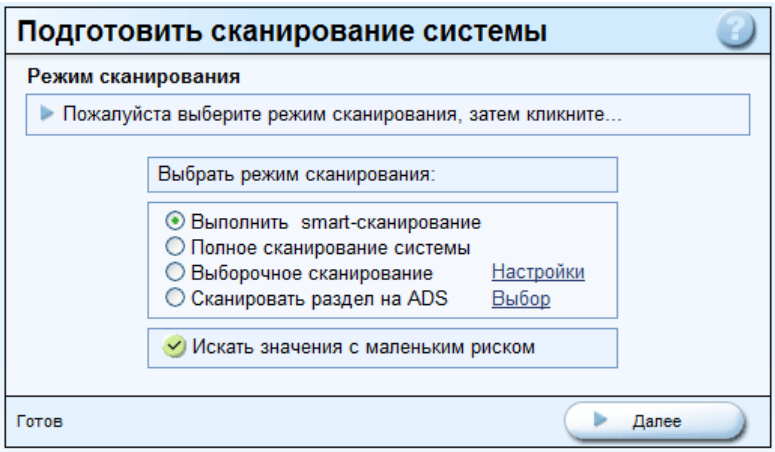


Рисунок 7. Окно подготовки к сканированию системы.

Внимание! Перед сканированием системы рекомендуется обновить файл определений программы. Сделать это можно в окне статуса программы.

Выбор режима сканирования

Выполнить smart-сканирование

Такой метод сканирования является самой быстрой системной проверкой. Рекомендуется использовать каждый день в отличие от полной проверки, которую желательно производить не реже одного раза в месяц. Если вы еще не разу не сканировали свою систему или подозреваете, что ваш компьютер инфицирован, то рекомендуется использовать полную проверку (см. ниже).

В большинстве случаев smart-сканирование обнаружит весь вредоносный контент в вашей системе, так как Ad-Aware SE способен к определению надобности последующей проверки. Так при smart-сканировании не просматриваются архивы, то при первой проверке необходимо выбрать полное сканирование системы.

При выполнении smart-сканирования выполняется:

- Полная проверка памяти;
- Просмотр системного реестра;
- Глубокий просмотр системного реестра;
- Просмотр кукисов;
- Проверка Избранного (Фаворитов);
- Проверка host-файлов;
- Условная проверка.

Примечание! Smart-сканирование не производится в архивах.

Полное сканирование системы

Это – глубокий режим проверки, при котором просматривается весь компьютер на предмет инфекций. При самой первой проверки системы при помощи Ad-Aware рекомендуется использовать только полное сканирование. В дальнейшем рекомендуется использовать полное сканирование системы не реже одного раза в месяц. Такая проверка более медленная, чем smart-сканирование, но зато имеет большую способность к обнаружению инфекций так как производится поиск на всех дисках, включая архивы.

Полное сканирование системы имеет те же настройки, что и smart-сканирование, но при этом проверка производится на всех жестких дисках и в архивах.

Выборочное сканирование

Можно настроить Ad-Aware SE для сканирования определенных дисков и папок. Эта опция позволяет выбрать определенные диски и папки, которые будут сканироваться.

При нажатии на «**Настройки**» появится окно настроек сканирования, в котором можно не только задать диски и папки для проверки, но и изменить некоторые другие параметры проверки.

Сканировать раздел на ADS

При таком сканировании производится проверка переменных потоков данных, которая проходит в два этапа. На первом этапе производится просмотр системы и вся информация кэшируется. Любой файл, рассмотренный в течение этого этапа подсчитан как отдельно просмотренный объект.

В течение второго этапа ищутся и исследуются потоки данных. Каждый поток также подсчитывается как отдельно просмотренный объект. Такой подход позволяет удостовериться, что переменные потоки данных не затрагивают критические объекты, и что последние не привязаны к потокам данных.

Данный режим подразумевает, что пользователь должен выбрать одну или более папок или дисков для сканирования.

Нажмите «**Выбор**» для выбора папок или дисков.

Искать значения с малым риском

Элементами с малым риском являются списки MRU (Most recently used item), то есть списки последних используемых элементов, например, программ, документов, поисков и так далее. При желании такие списки можно обнулить.

Выполнение сканирования системы

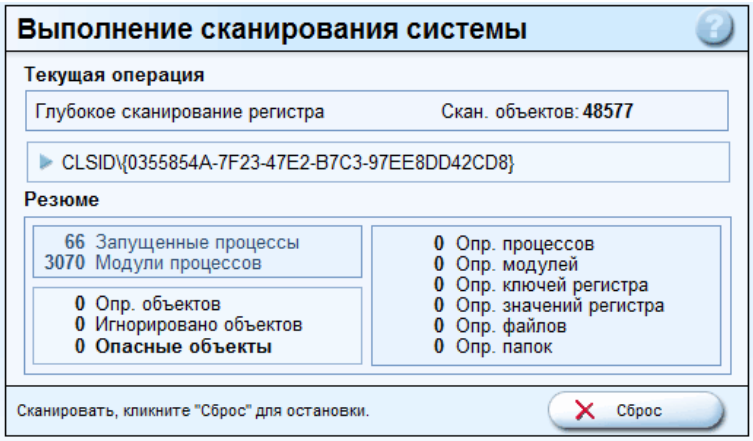


Рисунок 8. Окно выполнения сканирования системы.

- **Текущая операция** – показывает текущую операцию.
- **Скан. объектов** – показывает текущее число сканированных объектов.
- **Резюме** – меняющаяся в реальном времени текущая статистика.
- **Запущенные процессы** – показывается число запущенных в данный момент процессов.
- **Модули процессов** – показывается число запущенных в данный момент модулей процессов.
- **Опр. объектов** – показывает число всех обнаруженных инфицированных объектов на данный момент.
- **Игнорировано объектов** – показывает число игнорированных объектов во время сканирования.
- **Опасные объекты** – показывает количество новых обнаруженных на данный момент объектов в системе.
- **Опр. процессов** – показывается число инфицированных процессов.
- **Опр. модулей** – показывается число инфицированных модулей.
- **Опр. ключей регистра** – показывается число инфицированных ключей регистра.
- **Опр. значений регистра** – показывает количество инфицированных значений регистра.
- **Опр. файлов** – показывается количество зараженных или вредоносных файлов.
- **Опр. папок** – показывается количество инфицированных папок.

Кнопка «**Сброс**» останавливает проверку.

Сканирование выполнено

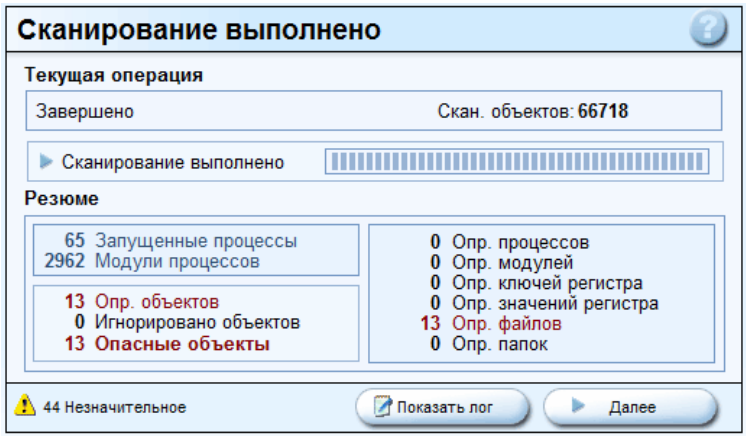


Рисунок 9. Окно, сигнализирующее о выполнении сканирования.

- **Текущая операция** – завершено (показывает, что сканирование выполнено).
- **Резюме** – общая статистика сканирования.
- **Запущенные процессы** – показывает количество просканированных процессов.
- **Модули процессов** – показывает количество просканированных модулей процесса.
- **Опр. объектов** – общее количество вредоносных объектов.
- **Игнорировано объектов** – количество игнорированных во время сканирования объектов.
- **Опасные объекты** – общее количество определенных опасных объектов.
- **Опр. процессов** – показывается число инфицированных процессов.
- **Опр. модулей** – показывается число инфицированных модулей.
- **Опр. ключей регистра** – показывается число инфицированных ключей регистра.
- **Опр. значений регистра** – показывает количество инфицированных значений регистра.
- **Опр. файлов** – показывается количество зараженных или вредоносных файлов.
- **Опр. папок** – показывается количество инфицированных папок.
- **Незначительное** – количество объектов с малым риском (MRU-листы).

Кнопка «**Показать лог**» выводит на экран лог-файл, содержащий подробную информацию о прошедшем сканировании.
Кнопка «**Далее**» открывает экран результатов сканирования.

Результаты сканирования

Резюме проверки

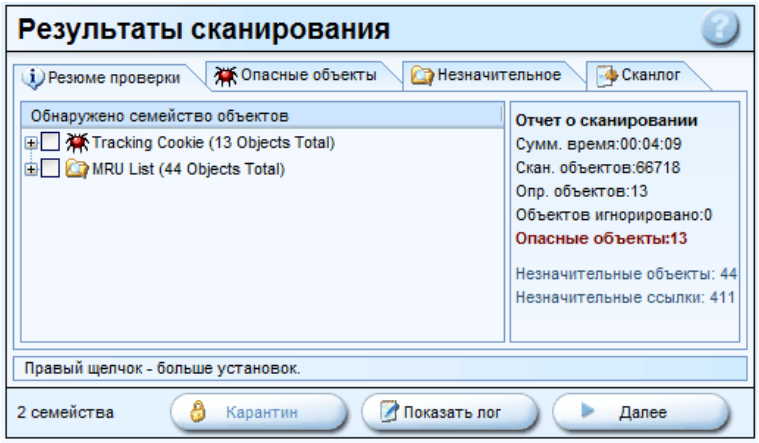


Рисунок 10. Окно результатов сканирования.

Обнаружено семейство объектов

В данном окне представлены семейства вредоносных объектов, обнаруженных при сканировании. При нажатии на «+» у какого-либо семейства вам будет выведен критерий опасности (TAC) для данных элементов.

Помимо опасных объектов в данном окне представлен также листинг малозначительных объектов (MRU-лист).

Отчет о сканировании

Слева в окне результатов сканирования представлен отчет о сканировании, в котором приведено:

- Затраченное на сканирование время;
- Общее количество сканированных объектов;
- Общее количество инфицированных объектов;
- Количество игнорированных объектов;
- Общее количество опасных объектов;
- Количество незначительных объектов;
- Количество незначительных ссылок.

Отчет о сканировании также приведен в конце лог-файла.

Кнопки

«**Карантин**»: Помещает выбранные объекты в файл карантина. Это опция может быть полезной, когда вы не хотите изолировать все объекты, обнаруженные в течение проверки (это и так делает опция автокарантина), а хотите добавить в карантин только некоторые, например, по принципу семейства или категории. **Внимание!** При использовании этой опции вам необходимо будет задать имя файла!

«**Показать лог**»: Отображает журнал, созданный в течение проверки

«**Далее**»: Переводит вас далее к окну подтверждения удаления.

Контекстное меню

Правый щелчок мыши в окне открывает контекстное меню:

- **Показать TAC для «Объект»** - показывает информацию TAC[2] для выбранного объекта (необходимо соединение с Интернет);
- **Выбрать все объекты** – выбор всех объектов;
- **Сбросить все объекты** – сброс выбора для всех объектов;

[2] TAC – диаграмма оценки угрозы.

- **Поменять выбор** – инвертирует выбор;
- **Развернуть все** – разворачивает весь список;
- **Свернуть все** – сворачивает весь список;
- **Изолировать выбранное** – добавляет выбранные объекты в изолятор;
- **Игнорировать выбранное** – добавляет выбранные объекты в лист игнорирования;
- **Опасные объекты** – переключает окно на окно с опасными объектами;
- **Лог сканирования** – открывает журнал сканирования;
- **Незначительные объекты** – открывает окно незначительных по опасности объектов (MRU-листы)
- **Помощь** – открывает файл справки.

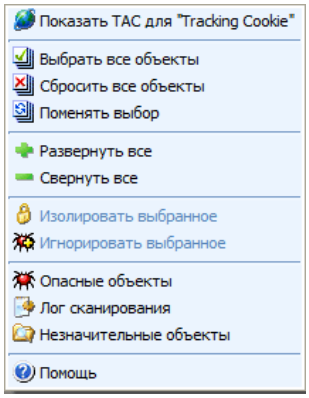


Рисунок 11. Контекстное меню.

Опасные объекты

Представленные здесь объекты являются опасными и их нужно рассматривать как требующие удаления.

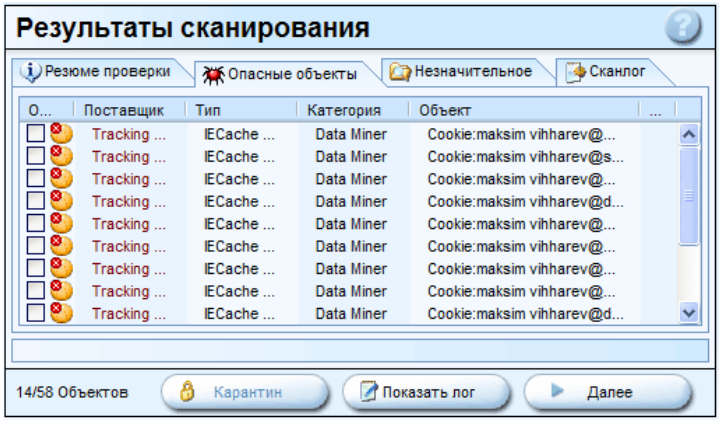


Рисунок 12. Окно опасных объектов.

- **Объект** – блок для выбора объекта. Также рядом с блоком указан символ типа объекта.
- **Поставщик** – имя создателя или просто название объекта.
- **Тип** – указывается объекта (файл, папка, значение реестра и так далее).
- **Категория** – указывается категория объекта.
- **Объект** – месторасположение объекта.
- **Комментарий** – краткий комментарий к объекту.

Кнопки

«**Карантин**»: Помещает выбранные объекты в файл карантина. Это опция может быть полезной, когда вы не хотите изолировать все объекты, обнаруженные в течение проверки и в последствии удаленные (это и так делает опция автокарантина), а хотите добавить в карантин только некоторые, например, по принципу семейства или категории. **Внимание!** При использовании этой опции вам необходимо будет задать имя файла!
«**Показать лог**»: Отображает журнал, созданный в течение проверки
«**Далее**»: Переводит вас далее к окну подтверждения удаления.

Контекстное меню

Правый щелчок мыши в окне открывает контекстное меню.

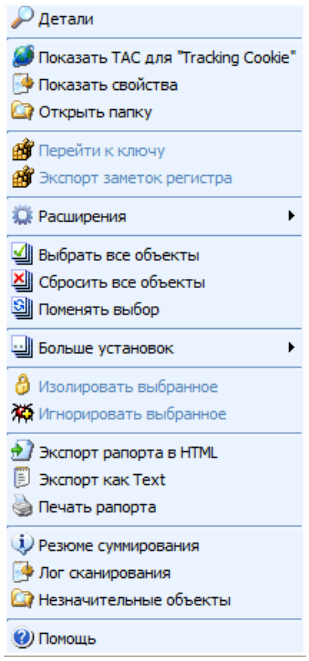


Рисунок 13. Контекстное меню.

- **Детали** – открывает детальную информацию о объекте (в этом окне также можно получить ссылку TAC для этого объекта).
- **Показать TAC для «Объект»** - показывает информацию TAC[3] для выбранного объекта (необходимо соединение с Интернет).
- **Показать свойства** – показывает Свойства выбранного элемента в Проводнике Windows.
- **Открыть папку** – открывает папку с выделенным элементом в Проводнике Windows.
- **Перейти к ключу** – открывает для ветку с ключом в системном реестре для выбранного объекта (требует установленного и связанного с программой RegHance – установки RegHance доступны в установках Ad-Aware по-умолчанию).
- **Экспорт заметок регистра** – производит экспорт ветки регистра для выбранного файла в reg-файл в указанное вами место.
- **Расширения** – запускает расширения программы (зависит от установленных расширений и дополнений Ad-Aware, смотри далее расширения).
- **Выбрать все объекты** – выбор всех объектов;
- **Сбросить все объекты** – сброс выбора для всех объектов;
- **Поменять выбор** – инвертирует выбор;
- **Больше установок** – расширенный выбор объектов:
  - **Выбрать все объекты «данного типа»** - выбор всех объектов данного типа;

[3] TAC – диаграмма оценки угрозы.

- **Сбросить все объекты «данного типа»** - сброс выделения всех объектов данного типа;
- **Выбрать все объекты «поставщика»** - выбор всех объектов данного поставщика;
- **Сбросить все объекты «поставщика»** - сброс выбора всех объектов данного поставщика;
- **Выделить все выбранные объекты** – выбор всех подсвеченных объектов;
- **Сбросить все выбранные объекты** – сброс выбора всех подсвеченных объектов.

- **Изолировать выбранное** – добавляет выбранные объекты в изолятор.
- **Игнорировать выбранное** – добавляет выбранные объекты в лист игнорирования.
- **Экспорт рапорта в HTML** – экспортирует рапорт в указанный вами HTML-файл.
- **Экспорт как Text** – экспорт рапорта в указанный вам текстовой файл.
- **Печать рапорта** – печать рапорта на принтере.
- **Резюме суммирования** – перемещает вас к окну резюме проверки.
- **Лог сканирования** – открывает журнал сканирования.
- **Незначительные объекты** – открывает окно с листингом незначительных по опасности объектов (MRU-листы).
- **Помощь** – открывает файл справки.

Незначительные объекты

Представленные здесь объекты являются малозначными с точки зрения угрозы, но все-же они несут некоторую конфиденциальную информацию о последних используемых программах, открытых файлах, документов и так далее. При желании эти элементы можно совершенно безопасно удалить.

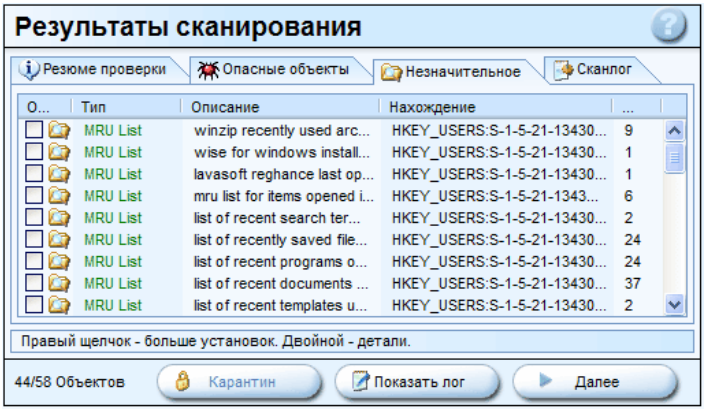


Рисунок 14. Незначительные объекты.

- **Объект** – блок для выбора объекта. Также рядом с блоком указан символ типа объекта (обычно это MRU-лист).
- **Описание** – описание объекта, указывается также программа, содержащая данный MRU-список.
- **Нахождение** – указывается место объекта в реестре Windows.
- **№ значения** – указывается число объектов для данного списка MRU.

Кнопки

«**Карантин**»: Помещает выбранные объекты в файл карантина. Это опция может быть полезной, когда вы не хотите изолировать все объекты, обнаруженные в течение проверки и затем удаленные (это и так делает опция автокарантина), а хотите добавить в карантин только некоторые, например, по принципу семейства или категории. **Внимание!** При использовании этой опции вам необходимо будет задать имя файла!

«**Показать лог**»: Отображает журнал, созданный в течение проверки
«**Далее**»: Переводит вас далее к окну подтверждения удаления.

Контекстное меню

Правый щелчок мыши в окне открывает контекстное меню.

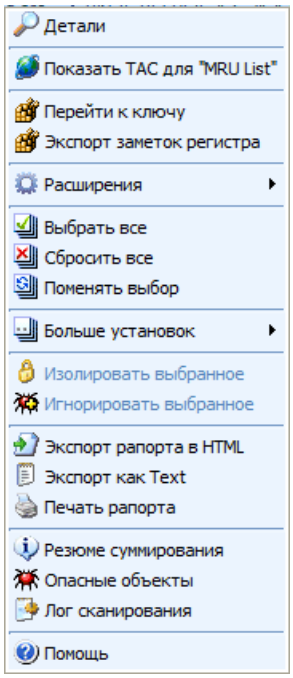


Рисунок 15. Контекстное меню для незначительных по опасности объектов.

- **Детали** – открывает детальную информацию о объекте (в этом окне также можно получить ссылку TAC для этого объекта).
- **Показать TAC для «Объект»** - показывает информацию TAC[4] для выбранного объекта (необходимо соединение с Интернет).
- **Перейти к ключу** – открывает для ветку с ключом в системном реестре для выбранного объекта (требует установленного и связанного с программой RegHance – установки RegHance доступны в установках Ad-Aware по-умолчанию).
- **Экспорт заметок регистра** – производит экспорт ветки регистра для выбранного файла в reg-файл в указанное вами место.
- **Расширения** – запускает расширения программы (зависит от установленных расширений и дополнений Ad-Aware, смотри далее расширения).
- **Выбрать все объекты** – выбор всех объектов;
- **Сбросить все объекты** – сброс выбора для всех объектов;
- **Поменять выбор** – инвертирует выбор;
- **Больше установок** – расширенный выбор объектов:
  - **Выбрать все выбранные объекты** – выбор все подсвеченных объектов;
  - **Сбросить все выбранные объекты** – сброс выбора все подсвеченных объектов.
- **Изолировать выбранное** – добавляет выбранные объекты в изолятор.
- **Игнорировать выбранное** – добавляет выбранные объекты в лист игнорирования.
- **Экспорт рапорта в HTML** – экспортирует рапорт в указанный вами HTML-файл.
- **Экспорт как Text** – экспорт рапорта в указанный вам текстовой файл.
- **Печать рапорта** – печать рапорта на принтере.
- **Резюме суммирования** – перемещает вас к окну резюме проверки.

[4] TAC – диаграмма оценки угрозы.

- **Лог сканирования** – открывает журнал сканирования.
- **Помощь** – открывает файл справки.

Сканлог

Показывает журнал, созданный при сканировании системы. Журнал содержит информацию о параметрах настройки, обнаруженных объектах и процессах. Настройки вывода журнала можно сконфигурировать в меню настроек (об этом далее).

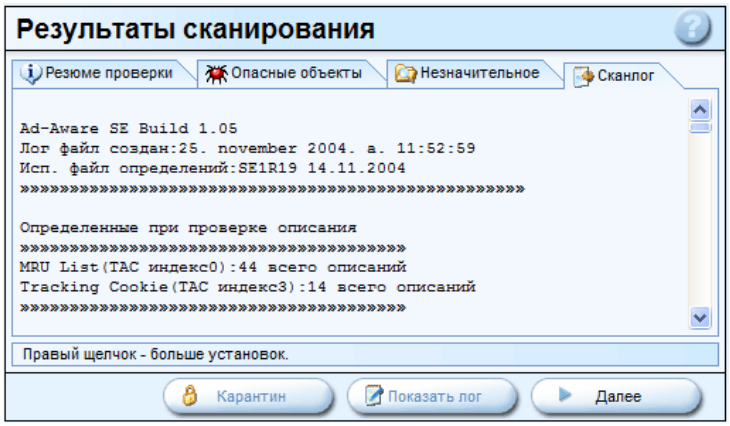


Рисунок 16. Журнал проверки системы.

Кнопки

«**Далее**»: Переводит вас далее к окну подтверждения удаления.

Контекстное меню

Правый щелчок мыши в окне открывает контекстное меню.

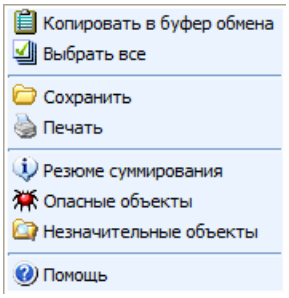


Рисунок 17. Контекстное меню в окне сканлога.

- **Копировать в буфер обмена** – копирует выделенное в буфер обмена.
- **Выбрать все** – выбор всего текста.
- **Сохранить** – сохраняет журнал в заданный вами файл.
- **Печать** – печатает журнал на принтере.
- **Резюме суммирования** – перемещает вас к окну резюме проверки.
- **Опасные объекты** – переключает окно на окно с опасными объектами;
- **Незначительные объекты** – открывает окно с листингом незначительных по опасности объектов (MRU-листы).
- **Помощь** – открывает файл справки.

Лист игнорирования

В данном окне приведены все объекты, которые игнорируются при сканировании и зачистке системы.

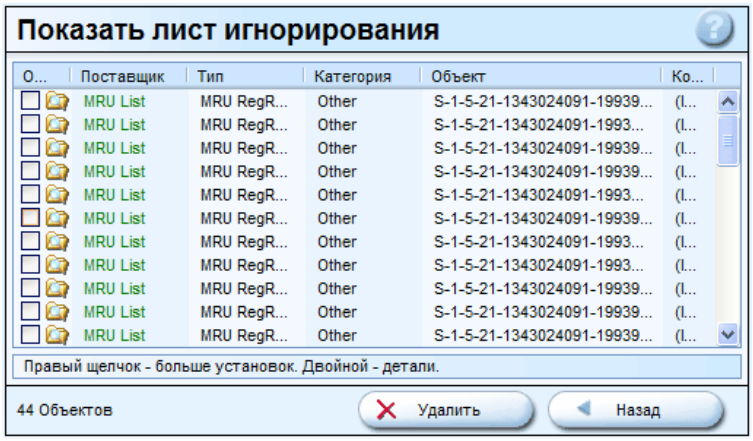


Рисунок 18. Лист игнорирования.

- **Объект** – блок для выбора объекта. Также рядом с блоком указан символ типа объекта.
- **Поставщик** – имя создателя или просто название объекта.
- **Тип** – указывается объекта (файл, папка, значение реестра и так далее).
- **Категория** – указывается категория объекта.
- **Объект** – месторасположение объекта.
- **Комментарий** – краткий комментарий к объекту.

Кнопки

«**Удалить**» - удаляет выбранные элементы из списка игнорирования.

«**Назад**» - возвращает вас к окну статуса программы.

Контекстное меню

Правый щелчок мыши в окне открывает контекстное меню.

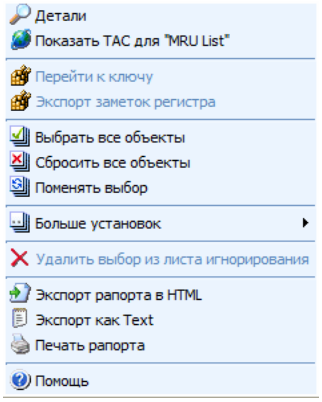


Рисунок 19. Контекстное меню листа игнорирования.

- **Детали** – открывает детальную информацию о объекте (в этом окне также можно получить ссылку TAC для этого объекта).
- **Показать TAC для «Объект»** - показывает информацию TAC[5] для выбранного объекта (необходимо соединение с Интернет).

[5] TAC – диаграмма оценки угрозы.

- **Перейти к ключу** – открывает для ветку с ключом в системном реестре для выбранного объекта (требует установленного и связанного с программой RegHance – установки RegHance доступны в установках Ad-Aware по-умолчанию).
- **Экспорт заметок регистра** – производит экспорт ветки регистра для выбранного файла в reg-файл в указанное вами место.
- **Выбрать все объекты** – выбор всех объектов;
- **Сбросить все объекты** – сброс выбора для всех объектов;
- **Поменять выбор** – инвертирует выбор;
- **Больше установок** – расширенный выбор объектов:
    - **Выбрать все объекты «данного типа»** - выбор всех объектов данного типа;
    - Сбросить все объекты «данного типа» - сброс выделения всех объектов данного типа;
    - **Выбрать все объекты «поставщика»** - выбор всех объектов данного поставщика;
    - **Сбросить все объекты «поставщика»** - сброс выбора всех объектов данного поставщика;
    - **Выделить все выбранные объекты** – выбор все подсвеченных объектов;
    - **Сбросить все выбранные объекты** – сброс выбора все подсвеченных объектов.
- **Удалить из листа игнорирования** – удаляет выбранные объекты из листа игнорирования.
- **Экспорт рапорта в HTML** – экспортирует рапорт в указанный вами HTML-файл.
- **Экспорт как Text** – экспорт рапорта в указанный вам текстовой файл.
- **Печать рапорта** – печать рапорта на принтере.
- **Помощь** – открывает файл справки.

Изолированные объекты

В этом окне показывается листинг всех файлов карантина, которые содержат удаленные из системы объекты.

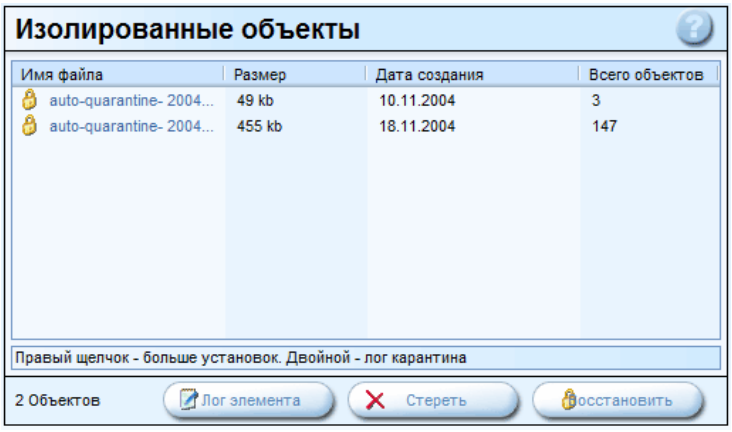


Рисунок 20. Окно карантина.

- **Имя файла** – имя файла карантина.
- **Размер** – размер файла карантина.
- **Дата создания** – дата создания карантинного файла.
- **Всего объектов** – количество объектов внутри файла карантина.

Кнопки

«**Лог элемента**» - показывает информацию о выбранном файле карантина.
«**Стереть**» - удаляет выбранный файл карантина.
«**Восстановить**» - восстанавливает в систему карантированные файлы из выбранного файла карантина.

Контекстное меню

Правый щелчок мыши в окне открывает контекстное меню.

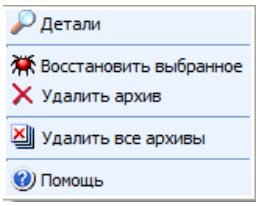


Рисунок 21. Контекстное меню карантина.

- **Детали** – показывает информацию о выбранном файле карантина.
- **Восстановить выбранное** – восстанавливает в систему карантированные файлы из выбранного файла карантина.
- **Удалить архив** – удаляет выбранный файл карантина.
- **Удалить все архивы** – удаляет все файлы карантинов.
- **Помощь** – открывает файл помощи.

Обновление Web

В данном разделе приводится информация о обновлении файлов определений Ad-Aware SE через Интернет.

Обновление Web – главное окно

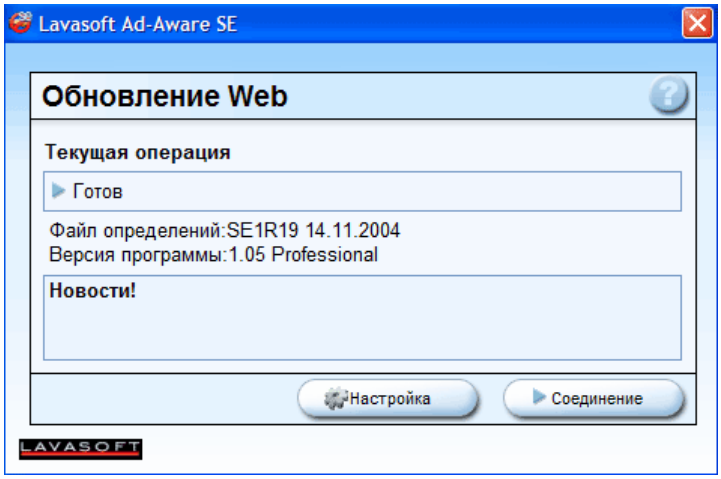


Рисунок 22. Главное окно Web-обновления.

- **Текущая операция** – показывает текущую операцию. Как только вы открываете мастер обновления Web эта позиция должна показывать «Готов» (означает, что программа нормально инициализирована).
- **Файл определений** – показывает установленную версию файла определений.
- **Версия программы** – показывает установленную версию программы.
- **Новости** – показывает новости с сайта Lavasoft (вы должны быть подключены к серверу Lavasoft для просмотра новостей). Когда информация доступна, то в окне отображается маленькое резюме новости и ссылка на полный текст.

Кнопки

«**Настройка**» - открывает окно настроек обновления Web.

«**Соединение**» - соединяет вас с сервером Lavasoft для получения обновления или новости.

Настройка обновления Web

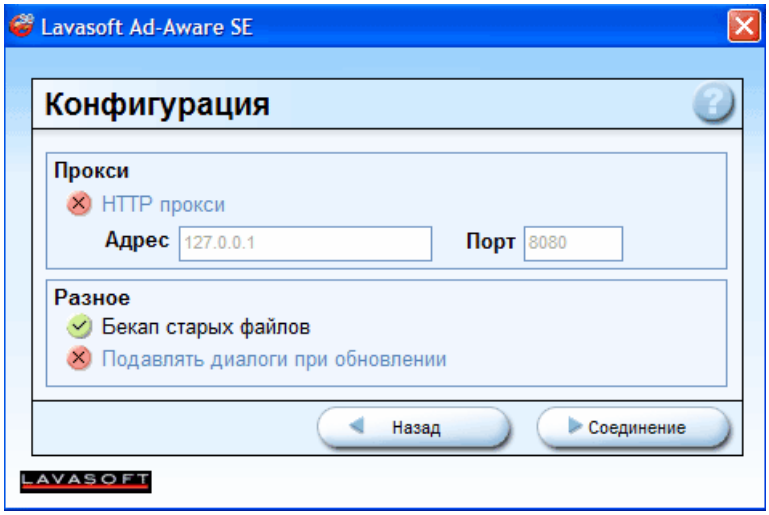


Рисунок 23. Окно настройки обновления Web.

- **Прокси** – включает/выключает использование прокси-сервера.
- **Адрес** – укажите IP адрес используемого Прокси-сервера.
- **Порт** – укажите порт используемого Прокси-сервера.
- **Бекап старых файлов** – делает резервную копию предыдущего файла обновлений перед установкой нового.
- **Подавлять диалоги при обновлении** – при включенной опции не появляются различные диалоги подтверждения операций обновления (типа начать ли загрузку и так далее).

Кнопки
«**Назад**» - возвращает вас обратно к главному окну обновления Web.
«**Соединение**» - соединяет вас с сервером Lavasoft для получения обновления или новости.

Завершение обновления Web

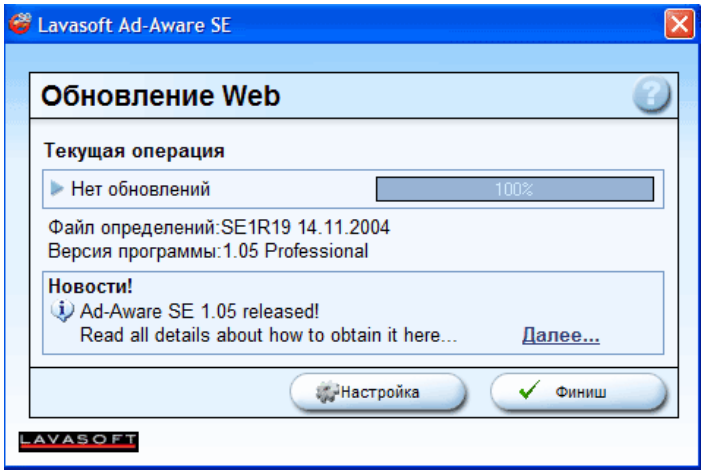


Рисунок 24. Окно завершения обновления Web. В данном случае рапортует об отсутствии обновлений.

Кнопки
«**Настройка**» - открывает окно настроек обновления Web.
«**Финиш**» - возвращает вас обратно к окну статуса программы.

Расширения и дополнения

Инструменты – автономные программы, которые можно использовать без выполнения проверок.
Расширения – обеспечивают дополнительную информацию о найденных объектах и предлагают различные варианты их исследования.
Статистика – показывает информацию о предыдущих проверках системы.

Инструменты

Показывает все установленные в системе инструменты.

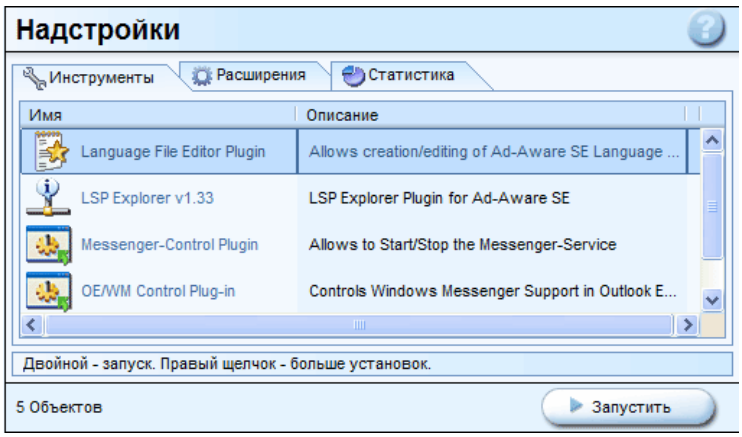


Рисунок 25. Окно надстроек с установленными инструментами.

- **Имя** – название инструмента.
- **Описание** – короткое описание инструмента на английском языке (так и не нашел в программе, каким образом можно перевести это описание – *примечание автора*).
- **Создатель** – автор и создатель инструмента.

Кнопки
«**Запустить**» - запускает выбранный инструмент.
Контекстное меню
Правый щелчок мыши в окне открывает контекстное меню.

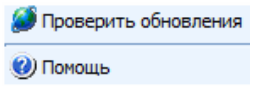


Рисунок 26. Контекстное меню окна инструментов.

- **Проверить обновления** – открывает страницу Lavasoft, где можно найти больше инструментов или их обновлений (необходимо соединение с Интернет).
- **Помощь** – открывает файл справки.

Расширения

Показывает все установленные в системе расширения.

- **Имя** – название расширения.
- **Описание** – короткое описание расширения на английском языке (так и не нашел в программе, каким образом можно перевести это описание на русский– *примечание автора*).
- **Создатель** – автор и создатель расширения.

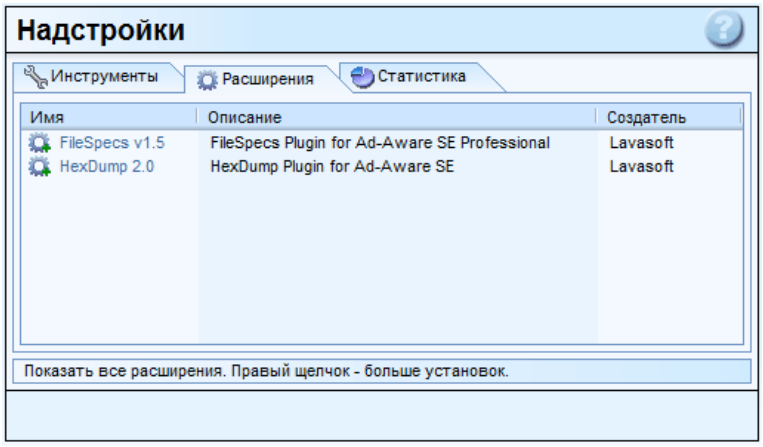


Рисунок 27. Окно настроек с установленными расширениями.

Контекстное меню
Правый щелчок мыши в окне открывает контекстное меню.

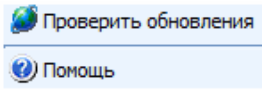


Рисунок 28. Контекстное меню расширений.

- **Проверить обновления** – открывает страницу Lavasoft, где можно найти больше расширений или их обновлений (необходимо соединение с Интернет).
- **Помощь** – открывает файл справки.

Статистика

Показывает статистику предыдущих сканирований.

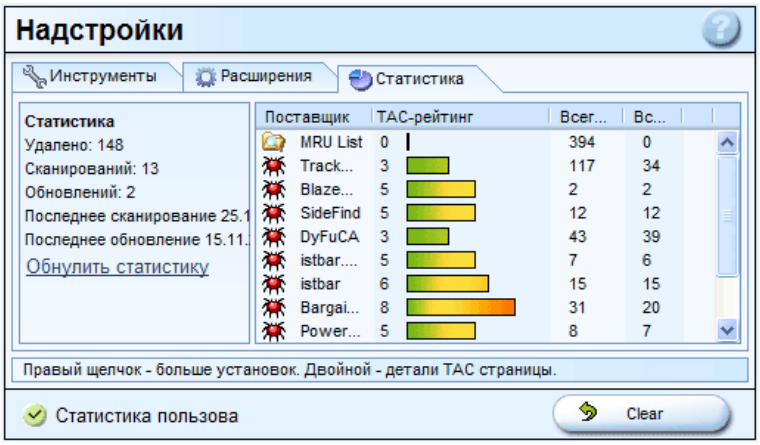


Рисунок 29. Окно статистики предыдущих сканирований.

Слева в окне представлена общая статистика, где есть информация о количестве всех удаленных файлов, числе сканирований, обновлений и так далее. В самом низу этой секции есть опция «Обнулить статистику».
Справа представлена более подробная информация по обнаруженным объектам:

- **Поставщик** – имя объекта или его создатель;
- **TAC-рейтинг** – рейтинг опасности объекта;
- **Всего найдено** – количество всех обнаруженных объектов данного типа;
- **Всего удалено** – количество всех удаленных объектов данного типа;
- **Последний обнаруженный** – дата последнего обнаружения объекта.

Кнопки

«**Clear**» - обнуляет всю статистике в окне.
Опция «**Статистика пользования**» - при включенной данной опции программа ведет статистику использования программой, при отключенной – не ведет.

Контекстное меню

Правый щелчок мыши в окне открывает контекстное меню.

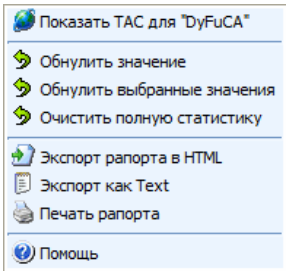


Рисунок 30. Контекстное меню для статистики.

- **Показать TAC для «Объект»** - показывает информацию TAC[6] для выбранного объекта (необходимо соединение с Интернет).
- **Обнулить значение** – обнуляет статистику для выбранного значения.
- **Обнулить выбранные значения** – обнуляет статистику для всех выбранных значений.
- **Очистить полную статистику** – обнуляет всю статистику.
- **Экспорт рапорта в HTML** – экспортирует рапорт в указанный вами HTML-файл.
- **Экспорт как Text** – экспорт рапорта в указанный вам текстовой файл.
- **Печать рапорта** – печать рапорта на принтере.
- **Помощь** – открывает файл справки.

[6] TAC – диаграмма оценки угрозы.

Установки

Установки служат для настройки Ad-Aware под ваши нужды. Вы можете, например, изменить язык интерфейса, сам интерфейс (при помощи шкурок), автоматизировать выполнение большинства действий программы: при старте компьютера программа может обновить свой файл определений, просканировать и вылечить систему.

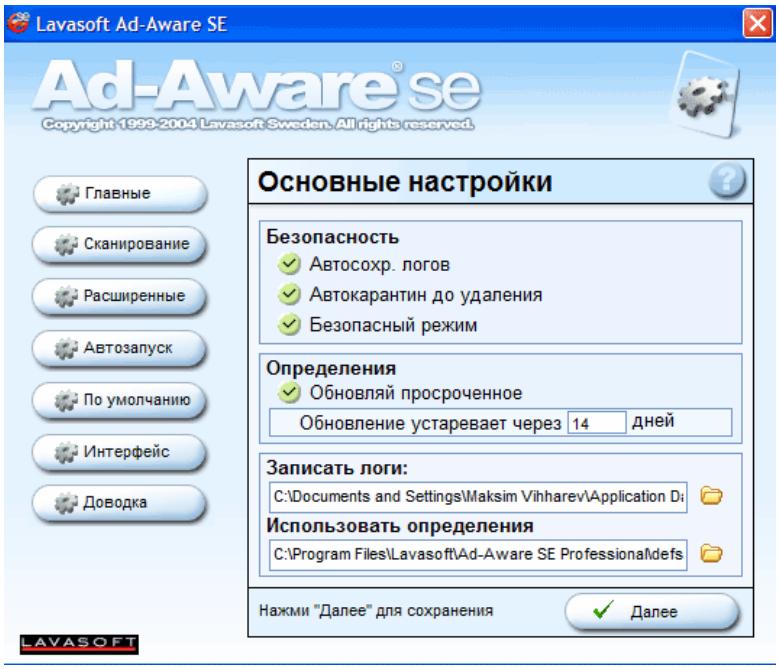


Рисунок 31. Окно основных настроек программы.

Для детального рассмотрения настроек выберите интересующую вас подкатегорию:

- Главные (основные настройки);
- Настройки сканирования;
- Расширенные настройки;
- Настройки автозапуска;
- Настройки по-умолчанию;
- Настройки интерфейса;
- Настройки доводки программы.

Главные настройки

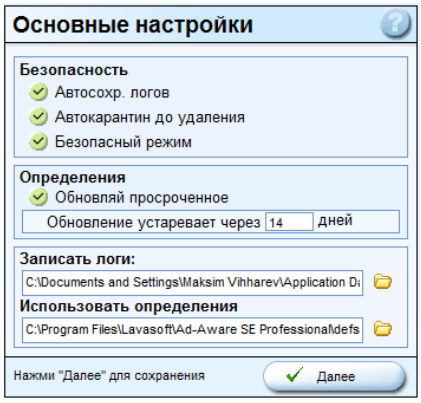


Рисунок 32. Основные (главные) настройки.

Безопасность

- **Автосохранение логов** – автоматическое сохранение журнала после каждого сканирования системы.
- **Автокарантин до удаления** – при удалении инфицированных объектов автоматом создается содержащий их файл карантина.
- **Безопасный режим** – при нахождении опасных объектов всегда будет выводиться окно с запросом о операции с объектами: карантин или удаление.

Определения

- **Обновляй просроченное**[7] – при устаревании файла определений будет происходить автоматическое обновление:
    - **Обновление устаревает через «количество» дней** – установка срока устаревания обновления.

Запись логов

Укажите месторасположение файлов журнала.

Использовать определения

Укажите месторасположение файлов определений.

Для сохранения произведенных изменений необходимо нажать кнопку «Далее», при этом вы будете возвращены к экрану статуса программы.

Внимание! Кнопка «Далее» сохраняет абсолютно все изменения в программных настройках, то есть ли вы хотите поменять и другие настройки, то не надо нажимать каждый раз «Далее» - достаточно нажать один раз после настройки всех опций.

Настройки сканирования

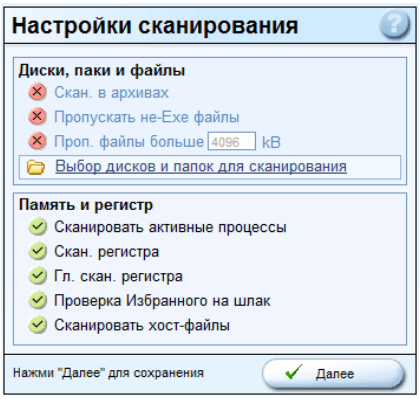


Рисунок 33. Окно настроек сканирования.

Диски папки и файлы

- **Сканировать в архивах** – при сканировании производится и проверка внутри архивов.
- **Пропускать не-Exe файлы** – форсация Ad-Aware для сканирования только исполнительных файлов. Такой метод сканирования очень долгий. **Внимание!** Эта функция должна использоваться только опытными пользователями для определения связанного контента, заставляющего восстанавливаться удаленный исполнительный файл!
- **Пропускать файлы больше «объем» КБ** – использование этой опции уменьшает время сканирования, так как проверка не будет производиться в файлах, больших указанного вами размера (например, в музыкальных и видеофайлах).

[7] Внимание системным администраторам! Если вы не хотите, чтобы конечные пользователи вмешивались в политику обновлений программы (используется прокси-сервер с обновлениями), то оставьте эту опцию выключенной.

- **Выбор дисков и папок для сканирования** – здесь вы можете указать диски и папки, которые будет сканировать программа. Этот выбор сканируемого используется также при запуске проверки через командную строку.

Память и регистр

- **Сканировать активные процессы** – при сканировании будет производиться проверка всех запущенных и активных процессах в памяти.
- **Сканирование регистра** – при сканировании будет производиться проверка известной области в реестре, куда обычно вставляют свои записи шпионы и реклама.
- **Глубокое сканирование регистра** – при сканировании будет производиться проверка всего реестра Windows. Данная опция увеличивает время сканирования (я все-же рекомендую включать эту опцию).
- **Проверка избранного на шлак** – проверка избранного (Фаворитов) на ссылки, ассоциированные с вредоносными объектами (многие шпионы и рекламы записывают в Избранное ссылки на свои страницы).
- **Сканировать хост-файлы**[8] – будет производиться проверка host-файлов. Редактирование таких файлов обычно используется налетчиками Интернет-браузера.

Кнопка «Далее» сохраняет сделанные вами изменения и возвращает вас к окну статуса программы.

Расширенные настройки

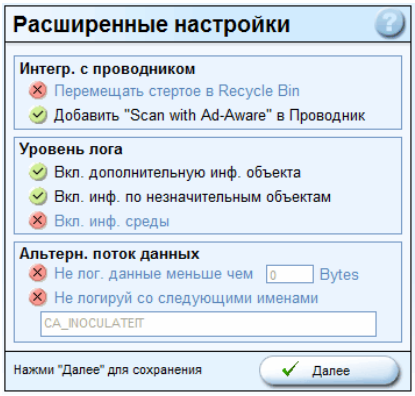


Рисунок 34. Окно расширенных настроек.

Интеграция с проводником

- **Перемещать стертое в Recycle Bin** – при использовании этой опции стертые объекты будут перемещены вместо полного удаления в мусорную корзину вашей операционной системы. Так как при сканировании мусорная корзина тоже проверяется, эти объекты будут повторно найдены (конечно, если вы не опустошили корзину). Используйте данную опцию как дополнительную гарантию создания резервного копирования – после того, как вы удостоверитесь, что созданный файл карантина содержит все удаленные файлы, можете опустошить корзину.
- **Добавить «Scan with Ad-Aware» в проводник** – добавляет опцию сканирования любой папки на компьютере по правому щелчку мыши (по левому – для левшей!) на этой папке в проводнике.

Уровень лога

- **Включить дополнительную информацию объекта** – в журнал сканирования будет включена дополнительная информация о найденных объектах.

[8] При использовании данной опции и обнаружении потенциальной опасности перед блокированием записи из хост-файла необходимо убедиться, что вы совершенно уверены в этой операции, так как неверная интерпретация может повлечь за собой некоторые неудобства.

- **Включить информацию по незначительным объектам** – в журнал сканирования будет включена дополнительная информация о найденных незначительных объектах (MRU-листы).
- **Включить информацию среды** – в журнал будет включена системная информация.

Альтернативные потоки данных

(Только для систем с файловой системой NTFS)

- **Не логируй данные меньше чем «объем» Bytes** – потоки данных с размером меньше указанного не будут включены в журнал.
- **Не логируй со следующими именами «имена»** - переменные потоки данных (ADS) с указанными именами не будут включены в журнал. Для внесения в список нескольких имен, используйте запятую без пробелов.

Кнопка «**Далее**» сохраняет сделанные вами изменения и возвращает вас к окну статуса программы.

Настройки автозапуска

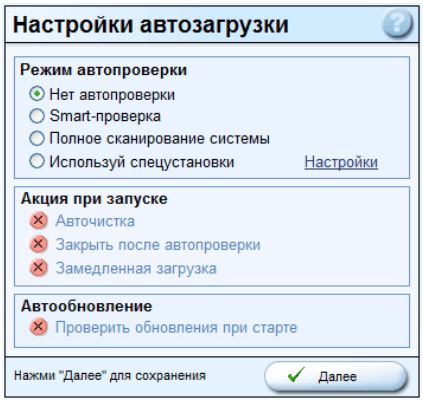


Рисунок 35. Окно настройки автозагрузки.

Режим автопроверки

- **Нет автопроверки** – отключено, то есть при старте компьютера автопроверка проводиться не будет;
- **Smart-проверка** – при старте компьютера будет производиться интеллектуальная проверка;
- **Полное сканирование системы** – при старте компьютера будет производиться полное сканирование системы;
- **Используй спец-установки** – настраиваемая проверка.

Акция при запуске

- **Авточистка** – автоматическая зачистка обнаруженных во время сканирования объектов.
- **Закрыть после автопроверки** – закрытие программы после выполнения автопроверки.
- **Замедленная загрузка** – эта опция полезна при использовании опции автообновления файла определений, так как при загрузке компьютеру может понадобиться некоторое время для связи с Интернетом и установки обновлений. Используйте эту опцию для замедления начала сканирования на 15 секунд.

Автообновление

- **Проверить обновления при старте** – проверка наличия обновления при старте. Если обновление доступно, то будет произведена автоматическая загрузка обновления и его установка.

Кнопка «**Далее**» сохраняет сделанные вами изменения и возвращает вас к окну статуса программы.

Настройки по-умолчанию

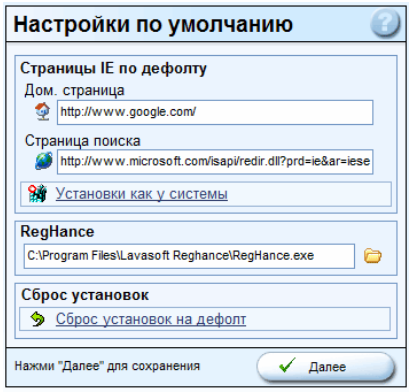


Рисунок 36. Окно настроек по-умолчанию.

Страницы IE по дефолту

- **Домашняя страница** – домашняя страница, которую будет использовать Ad-Aware после восстановления от налетчиков-браузера.
- **Страница поиска** – страница поиска, которую будет использовать Ad-Aware после восстановления от налетчиков-браузера.
- **Установки как у системы** – Ad-Aware выставит такие же установки, как и у вашей системы (прочтет из регистра).

RegHance

Кажите месторасположение **RegHance**[9]. У меня на рисунке показаны установки по дефолту.

Сброс установок

Эта опция сбросит все сделанные вами изменения установок и выставит установки по дефолту (как будто только что установили программу).

Кнопка «**Далее**» сохраняет сделанные вами изменения и возвращает вас к окну статуса программы.

Настройки интерфейса

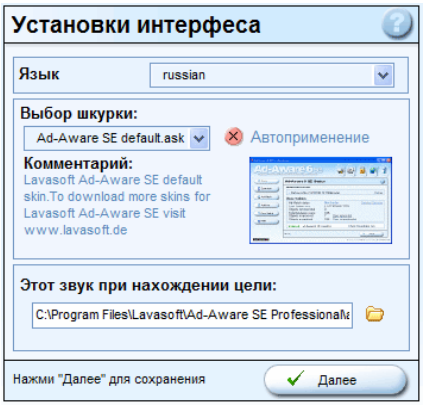


Рисунок 37. Окно настроек интерфейса программы.

Язык

Выбор языка программы. В моем случае стоит русский. Смотри далее более подробно как установить языковые пакеты.

Выбор шкурки

[9] RegHance – расширенный редактор реестра Windows. Это отдельная программа, которую нужно отдельно покупать. Для получения дополнительной информации обратитесь на сайт Lavasoft.

Выбор шкурки программы позволяет изменить внешний вид программы. При изменении шкурки программа автоматом перезапустится после нажатия кнопки «**Далее**».

Этот звук при нахождении цели

Выберите звуковой файл, который будет проигрываться при нахождении при сканировании инфицированных объектов.

Кнопка «**Далее**» сохраняет сделанные вами изменения и возвращает вас к окну статуса программы.

Настройки доводки программы

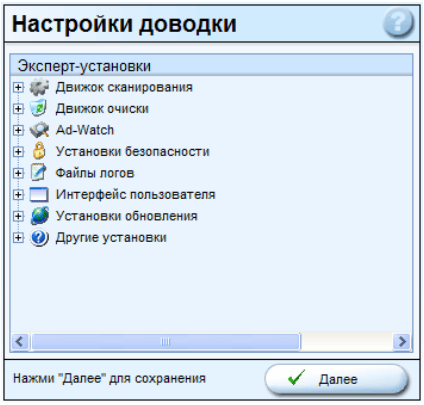


Рисунок 38. Окно доводки программы.

В окне доводки программы представлен ниспадающий список опций. Для их развертывания достаточно нажать «+» рядом со строкой интересующего подменю.

Движок сканирования

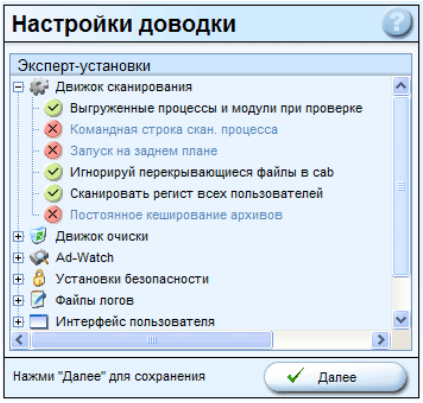


Рисунок 39. Настройка движка сканирования.

- **Выгруженные модули и процессы при проверке** – при включенной опции Ad-Aware выгружает найденные инфицированные модули и процессы во время сканирования. Если опция отключена, то инфицированные модули и процессы остаются загруженными до окончания сканирования. Отключение этой опции не означает, что такой процесс или модуль останутся зараженными, все-же при их выгруженном состоянии дезинфекцию произвести легче.
- **Командная строка сканируемого процесса** – программа способна определить параметры командной строки, запускающей инфицированный процесс. При включенной опции в журнал сканирования эта командная строка будет добавлена, при выключенной – в журнал будет добавлено только месторасположение процесса.

- **Запуск на заднем плане** – опция форсирует Ad-Aware на запуск в фоновом режиме (меньшее использование процессорной мощности). Таким образом можно одновременно выполнять на компьютере несколько программ одновременно (без замедления компьютера).
- **Игнорируй перекрывающиеся файлы в cab** – программа будет игнорировать перекрывающиеся (заполненные) файлы кабинета. Перекрывающийся файл кабинета – файл кабинета, собранный из нескольких кабинетов.
- **Сканировать регистр всех пользователей** – при сканировании будут проверятся секции реестра Windows для всех пользователей на данной машине, а не только для текущего.
- **Постоянное кэширование архивов** – Ad-Aware при самом первом просмотре архивов создаст контрольные суммы каждого архива и при последующих сканированиях будут проверятся только архивы с измененной контрольной суммой (измененные архивы). После обновления файла определений база данных контрольных сумм архивов будет обнулена и архивы опять будут проверяться – таким образом достигается дополнительная безопасность пользователя, так как новый файл определений может содержать информацию о ранее неизвестном вредителе.

Движок очистки

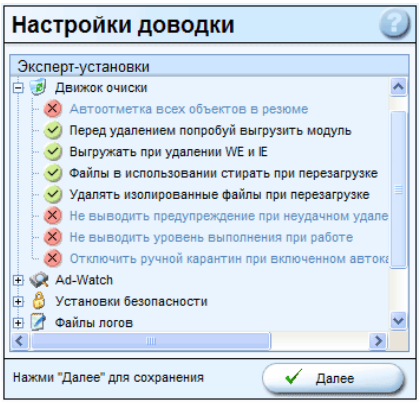


Рисунок 40. Настройка движка очистки.

- **Автоотметка всех объектов в резюме** – в отчете все обнаруженные объекты будут выделены.
- **Перед удалением попробуй выгрузить модуль** – Ad-Aware попробует выгрузить инфицированный модуль перед его удалением.
- **Выгружать при удалении WE и IE** – при удалении вредоносного контента Ad-Aware будет выгружать Windows Explorer и Internet Explorer – это помогает избежать перезагрузки системы для удаления некоторых элементов.
- **Файлы в использовании стирать при перезагрузке** – если программа не смогла стереть некоторые вредные файлы (они чем-то используются), то при перезагрузке Windows Ad-Aware их удалит (для этого при старте системы будет запущено сканирование для их повторного определения).
- **Не выводить предупреждение при неудачном удалении** – если все-же Ad-Aware не смог удалить какой-либо файл, то при включенной этой опции окно предупреждения появляться не будет.
- **Не выводить уровень выполнения при работе** – при включенной опции не будет показываться уровень выполнения удаления или карантирования.
- **Отключить ручной карантин при включенном автокарантине** – отключает возможность создания вручную файла карантина.

Ad-Watch

Настройки монитора реального времени Ad-Watch

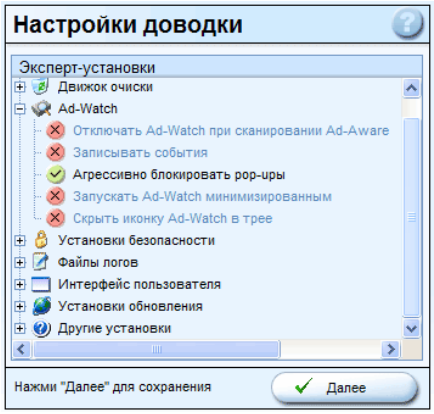


Рисунок 41. Окно настроек монитора реального времени Ad-Watch.

- **Отключать Ad-Watch при сканировании Ad-Aware** – Ad-Watch отключается на время, пока Ad-Aware сканирует систему.
- **Записывать события** – действия Ad-Watch будут добавлены в журнал Ad-Aware.
- **Агрессивно блокировать pop-апы** – Ad-Watch будет блокировать всплывающие окна агрессивно.
- **Запускать Ad-Watch минимизированным** – Ad-Watch будет запускаться минимизированным в системный трей.
- **Скрыть иконку Ad-Watch в трее** – иконка Ad-Watch в трее показываться не будет.

Установки безопасности

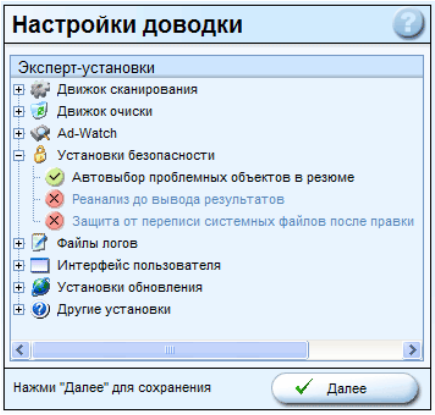


Рисунок 42. Установки безопасности.

- **Автовыбор проблемных объектов в резюме** – Ad-Aware автоматически выделит в резюме полужирным шрифтом проблематичные объекты.
- **Реанализ до вывода результатов** – после завершения сканирования Ad-Aware перед выводом результатов сканирования еще раз их проанализирует.
- **Защита от переписи системных файлов после правки** – Ad-Aware выставит атрибуты важных системных файлов (например, host-файлов) после их вылечивания на «только чтение» (read-only).

Файлы логов

- **Информация о игнорированных объектах** – в журнал будет включена информация о объектах, находящихся в листе игнорирования.
- **Основные установки программы** – в журнал будет включена информация о основных установках программы.
- **Расширенные установки** – в журнал будет включена информация о расширенных установках программы.
- **Параметры командной строки** – в журнал будет включена информация о параметрах командной строки, использовавшихся для запуска Ad-Aware.
- **Имя компьютера и пользователя** – в журнал будет включена информация о компьютере и имени пользователя.
- **Резюме определений** – в журнал будут включено резюме найденных объектов с их TAC рейтингом.
- **Лог для удаленных операций** – в журнал будет включена информация об удаленных объектах, а не только об обнаруженных.
- **Лист модулей** – в журнал будет включен листинг всех модулей для каждого процесса.
- **Альтернативный поток данных** – в журнал будет включена информация об обнаруженных альтернативных (переменных) потоков данных.

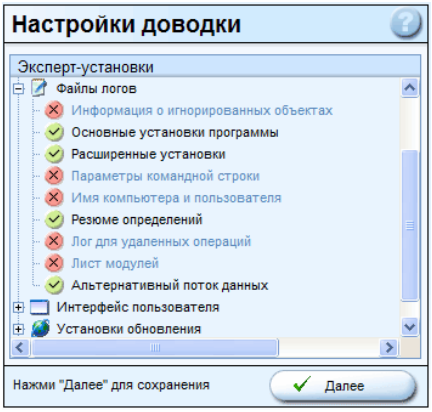


Рисунок 43. Настройка журнала.

Интерфейс пользователя

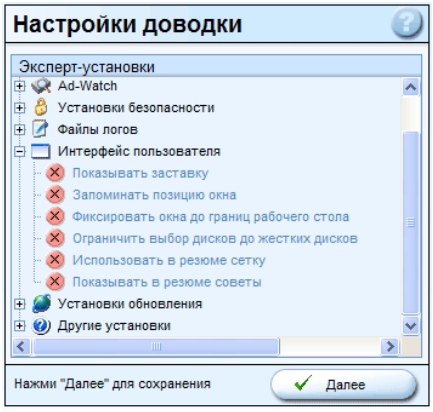


Рисунок 44. Настройка интерфейса пользователя.

- **Показывать заставку** – при запуске программы будет показываться заставка.
- **Запоминать позицию окна** – Ad-Aware и Ad-Watch будут открываться в том же самом окне, в котором были закрыты.

- **Фиксировать окна до границ рабочего стола** – Ad-Aware/Ad-Watch нельзя будет переместить за границы рабочего стола.
- **Ограничить выбор дисков до жестких дисков** – ограничение выбора цели для сканирования до жестких дисков. В таком случае вы не сможете сканировать съемные носители информации (дискеты, CD-диски и так далее).
- **Использовать в резюме сетку** – резюме будет линованным.
- **Показывать в резюме советы** – при наведении указателя мыши в окнах игнорирования, карантина и результатов будет выводиться подробная информация.

Установки обновления

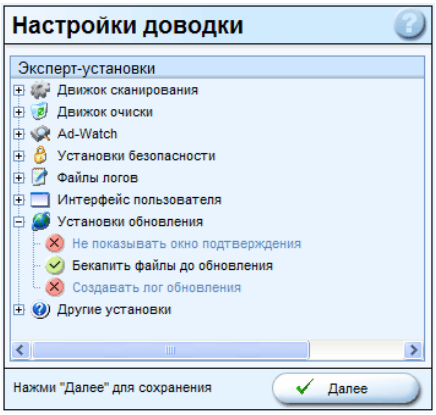


Рисунок 45. Установки обновлений.

- **Не показывать окно подтверждения** – запрет показа подтверждения обновления Web.
- **Бекапить файлы до обновления** – перед обновлением будет сделана резервная копия старого файла определений.
- **Создавать лог обновления** – добавление в журнал отчета об обновлении.

Другие установки

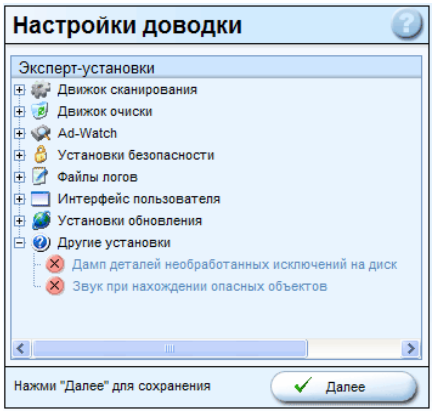


Рисунок 46. Другие установки.

- **Дамп деталей необработанных исключений на диск** – при непредвиденной остановке вся информация о проделанной работе будет сохранена в папке Ad-Aware.
- **Звук при нахождении объекта** – при нахождении инфекций будет проигрываться звуковой файл.

Использование Ad-Aware

Обновление файла определений

Файл определений Ad-Aware – это файл, по аналогии с базами данных антивирусных программ, содержащий описания вредоносных объектов. Он построен на новой технологии Code Sequence Identification (идентификация последовательности кода) и является приемником референсных файлов в версии 6.
Для того, чтобы быть всегда защищенным рекомендуется регулярное обновление файлов определений. Для этого есть пять возможностей.

Обновление через Web

Для старта обновления через Web, нажмите кнопку «**Обновления через Web**» на инструментальной панели или используй кнопку «**Проверить обновления**» в окне статуса программы. Нажмите «**Соединение**» для связи программы с сервером Lavasoft и проверки доступных обновлений. Если обновление доступно, то нажмите «**Ок**» для загрузки и установки.

Автоматическое обновление Web

Вы можете настроить программу на автоматическое обновление файлов определений. Для этого необходимо в окне меню «**Автозагрузки**», в разделе **Автообновление** поставить «**Проверить обновления при старте**» и для сохранения изменений нажать «**Далее**».
Примечание! Для автообновления Web необходимо, чтобы компьютер имел подключение к Интернет. В зависимости от того, какое вы имеете подключение, вам может быть надо выставить «**замедленную загрузку**» в окне меню «**Автозагрузки**» для замедления автообновления на 15 секунд (чтобы компьютер успел связаться с вашим провайдером).

Обновление файла определений вручную

В некоторых случаях невозможно произвести обновление через Web. В таких случаях можно воспользоваться мануальным обновлением. Для этого:

1. Закройте Ad-Aware;
2. Загрузите последний файл определения с сайта Lavasoft в какую либо временную директорию;
3. Распакуйте содержимое архива zip в C:\Program Files\Lavasoft\Ad-Aware SE Professional или эквивалент этому (зависит от директории, в которую установлен Ad-Aware);
4. Запустите программу.

Если обновление произошло успешно, то вы увидите новую версию файла определений в окне «**Статуса программы**».

Обновление файла определений через командную строку

Вы можете использовать параметр **+update** для обновления через командную строку. Если обновление доступно, то оно будет автоматически загружено и установлено.
Пример:
"C:\Program Files\Lavasoft\Ad-Aware SE Professional\Ad-Aware.exe" /smart +update
При использовании такой комбинации программа проверит наличие обновлений (если есть, то загрузит и установит их), а затем запустит сканирование в режиме smart.

Сетевое обновление

Lavasoft Ad-Aware SE Professional поддерживает UNC-протокол (Протокол Интернет). Это означает, что вы можете хранить файл определений на удаленном диске (например, сервере)

и сконфигурировать программу на его использование. При этом после обновления программы на сетевом ресурсе все клиенты будут использовать обновленную версию файла определений.

Использование командной строки

Ad-Aware может использоваться без графического интерфейса пользователя (GUI). Также встроена поддержка UNC.
Пример:
Ad-Aware.exe /smart +silent +update +nice-2
Ad-Aware запуститься без GUI в фоновом режиме, затем проверит обновления и после этого запустит smart-сканирование с высоким приоритетом выполнения.

Доступные параметры командной строки

/smart
Запуск smart-сканирования.
/full
Запуск полного сканирования системы.
/custom
Запуск выборочного сканирования (определяется пользователем заранее в настройках, смотри выше настройки сканирования).
/ads
Запуск проверки на переменные (альтернативные) потоки данных на NTFS-разделах.
При использовании просто параметра **/ads** будет произведена проверка с настройками, определенными ранее.
При использовании **/ads** с параметром пути самым первым параметром, например:
"C:\Program Files\Lavasoft\Ad-Aware SE Professional\Ad-Aware.exe" "C:\test" /ads
будет произведена проверка директории C:\test с настройками, определенными ранее.

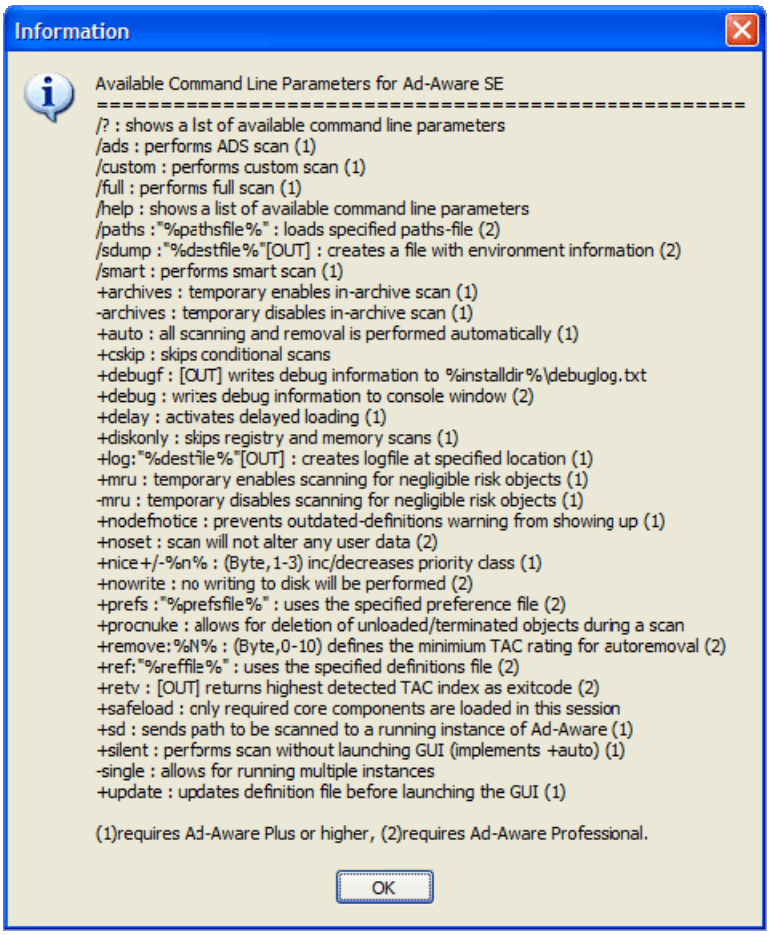


Рисунок 47. Окно помощи с доступными параметрами командной строки.

/?
Вызывает окно справки с доступными параметрами командной строки.
/Help
Вызывает окно справки с доступными параметрами командной строки.
/paths:"%pathsfile%"
Определяет текстовый файл, содержащий директории, подлежащие сканированию. Файл **%pathfile%** может содержать также удаленные диретории.
sdump:"%destinationfile%"
Создает файл в указанной директории, который будет содержать статусную информацию. Эта команда требует задания имени файла назначения. Файл статусной информации будет содержать информацию о версии, сборке, загруженном файле определений, доступных дополнениях, статистику сканирования и так далее.
+archives
Отмена любых настроек архивного сканирования для обязательного сканирования архивов.
-archives
Отмена любых настроек архивного сканирования для обязательного игнорирования архивов.
+auto
Сканирование и удаление инфекций в полноавтоматном режиме с обязательным автокарантированием и ведением журнала согласно настройкам пользователя.
+cskip
Пропуск условного сканирования.
+delay
Активирование заторможенной загрузки.
+diskonly
Выполнение проверки только дисков. Проверка памяти и реестра не производится.
+log:"%destination%"
Создание файла журнала в указанной директории. Необходимо задать полный путь.
+mru
Сканирование на значения с малым риском опасности с временной отменой последних пользовательских опций сканирования.
-mru
Отмена сканирования на значения с малым риском опасности с временной отменой последних пользовательских опций сканирования.
+nice+/-n
(-) увеличивает приоритет запуска (выше среднего, высокий, реального времени). Пример: **nice-1** или **+nice-2**, или **+nice-3**.
(+) уменьшает приоритет запуска (ниже среднего, низкий). Пример: **+nice+1** или **+nice+2**.
+nodefnotice
Подавление сообщений об устаревании файла определений.
+noset
Проверка не будет изменять никаких пользовательских данных.
+nowrite
Отключение любой записи на диск. При использовании этой команды не будут сохранены лист игнорирования, кэш и опции.
+prefs:"%file%"
Задание файла с опциями программы. Необходимо указывать полный путь к имени файла.
+procnuke
Выполнение агрессивного сканирования памяти. Ad-Aware буде пробовать выгружать процесс/модуль и немедленно удалять его. Такая операция часто необходима при удалении взаимных процессов. Такая проверка также выгружает проводник и инфицированные модули независимо от установок программы в секции доводки.
+ref:"%file%"

Задание пользовательского файла определений. Необходимо затать полный путь к имени файла.

+remove:n

Где **n** – число от **0** до **10**. Если использовать эту комбинацию с параметром **/auto**, то автоматически будут удалены инфицированные объекты с TAC-рейтингом равным или большим **n**.

+retv:[out]

Возвращает самый высокий TAC-рейтинг обнаруженных объектов после завершения кода.

+safeload

Загрузка минимальной конфигурации, необходимой для работы Ad-Aware SE. Опускается загрузка Кеша, листа игнорирования, расширений и дополнений программы. Если у вас возникают проблемы с запуском Ad-Aware, то используйте эту команду.

+sd

Посылает команду на выполнение образца Ad-Aware.

+silent

Запуск Ad-Aware без графического интерфейса и сканирование без какого-либо удаления.

+update

Проверка доступности обновления файла определений и загрузка его (при наличий) при старте программы.

Изменение языка на русский

Вы можете изменить язык интерфейса программы на подходящий вам. Для этого вам необходимо загрузить и установить последнюю версию Lavasoft Ad-Aware SE Language Pack (рекомендую использовать этот наш пакет, так как он включает в себя не только языки, доступные на официальном сайте программы (они без изменений включены в наш пакет), но и некоторые другие (в том числе и русский!).
Внимание! До установки языкового пакета рекомендую закрыть программу.
Ход смены языка:

1. Установите Lavasoft Ad-Aware SE Language Pack;
2. Запустите Ad-Aware;
3. Откройте меню «**Settings**» (значок механизма на инструментальной панели);
4. Щелкните слева копку «**Interface**»;
5. В ряду «**Language file**» выберите **Russian**.
6. Нажмите «**Proceed**»;
7. Закройте и перезапустите программу.

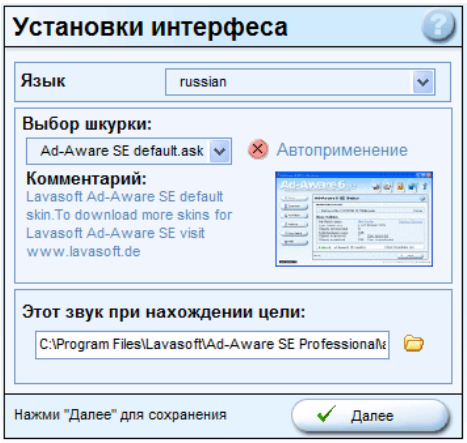


Рисунок 48. Установки интерфейса (языка).

Можно также использовать ручную русификацию программы. Для этого поместите файл Russian.awl, идущий в комплекте с данным руководством в директорию
C:\Program Files\Lavasoft\Ad-Aware SE Professional\Lang
И затем выполните шаги, описанные выше.

Изменение шкурки программы

В программе предусмотрена также смена шкурок. Шкурки возможно бесплатно загрузить с сайта Lavasoft.

Ход смены шкурки:

1. Запустите Ad-Aware;
2. Откройте меню «**Установки Ad-Aware**» (значок механизма на инструментальной панели);
3. Щелкните слева копку «**Интерфейс**»;
4. В ряду «**Выбор шкурки**» выберите «**Необходимую шкурку**».
5. Нажмите «**Proceed**»;
6. Программа автоматически перезапустится и загрузится уже с новой шкуркой.

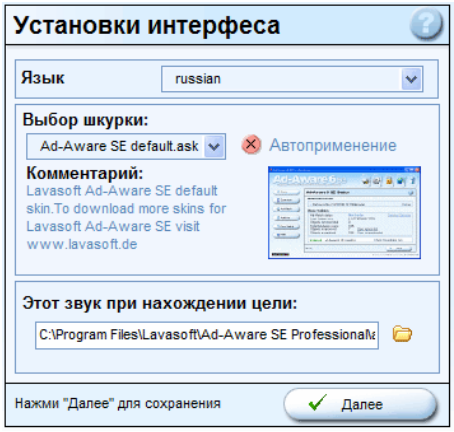


Рисунок 49. Установки интерфейса (шкурки).

Что такое карантин

Карантин используется для изолирования и архивирования, обнаруженных во время сканирования, объектов, с возможностью их последующего восстановления.
Все объекты, перемещенные в карантин, сжаты и зашифрованы, поэтому их можно восстановить, только используя специальный встроенный в программу менеджер карантина. Объекты, сохраненные в карантине, не ставят под угрозу ваш компьютер.

Ручной карантин

Внимание! Можно перемещать в карантин любой объект из листов результатов проверок Ad-Aware, будь то файл, папка, ключ или значение реестра. Объекты могут быть перемещены в карантин только из окна результатов сканирования:

- Резюме проверки
- Опасные объекты
- Незначительные объекты

Добавление объектов в карантин:

1. Запустите сканирование Ad-Aware;
2. В окне результатов сканирования в соответствующих подразделах отметьте необходимые объекты;
3. Нажмите кнопку «**Карантин**» или в ниспадающем контекстном меню по правой кнопке мыши выберите «**Изолировать выбранное**»;
4. Задайте имя файла и нажмите «**ОК**»
5. В появившемся окне, показывающем количество изолируемых объектов, нажмите «**ОК**».

Выбранные файлы теперь добавлены в карантин (изолятор).

Автокарантин объектов до удаления.

Для включения автокарантина объектов до удаления необходимо запустить меню «**Установки**» и затем в «**Главных настройках**» выставить «**Автокарантин до удаления**».

Восстановление объектов из карантина

Для восстановления объектов из карантина:

1. Запустите менеджер карантина, нажав кнопку «**Карантин**» на инструментальной панели или кнопку «**Открыть изолятор**» в окне статуса.
2. Выберите объекты, которые необходимо восстановить.
3. Щелкните в контекстном меню «**Восстановить**» или нажмите кнопку «**Восстановить**».

Что такое лист игнорирования

Иногда требуется сохранить некоторые объекты на компьютере, которые Ad-Aware все время определяет как подлежащие удалению. Для этого существует лист игнорирования. В лист игнорирования можно добавить как целый продукт, так и отдельный файл.

Добавление объектов в лист игнорирования

Внимание! Можно перемещать в лист игнорирования любой объект из листов результатов проверок Ad-Aware, будь то файл, папка, ключ или значение реестра. Объекты могут быть перемещены в лист игнорирования только из окна результатов сканирования:

- Резюме проверки
- Опасные объекты
- Незначительные объекты

Добавление объектов в лист игнорирования:

1. Запустите сканирование Ad-Aware;
2. В окне результатов сканирования в соответствующих подразделах отметьте необходимые объекты;
3. В ниспадающем контекстном меню по правой кнопке мыши выберите «**Игнорировать выбранное**»;
4. В появившемся окне, показывающем количество игнорируемых объектов, нажмите «**ОК**».

Выбранные файлы теперь добавлены в лист игнорирования.

Удаление объектов из листа игнорирования

1. Откройте менеджер листа игнорирования, нажав кнопку «Открыть лист игнорирования» в окне статуса программы.
2. Выберите объекты, подлежащие удалению.
3. В ниспадающем контекстном меню по правой кнопке мыши выберите «**Удалить выбор из листа игнорирования**» или нажмите кнопку «**Удалить**».

Настройка Ad-Aware

Для правильной защиты вашего компьютера важно, чтобы файлы дефиниций программы всегда были обновлены. Можно автоматизировать обновление программных файлов определений, сканирования, карантин обнаруженных вредоносных объектов и просмотр с очисткой компьютера при старте операционной системы. Далее приводятся пути автоматизации.

Для настройки автоматизации вам необходимо запустить меню "**Настройки**" (значок механизма на инструментальной панели) и выбрать там подменю "**Автозапуск**" (кнопка с левой стороны меню) (см. рис. 50).

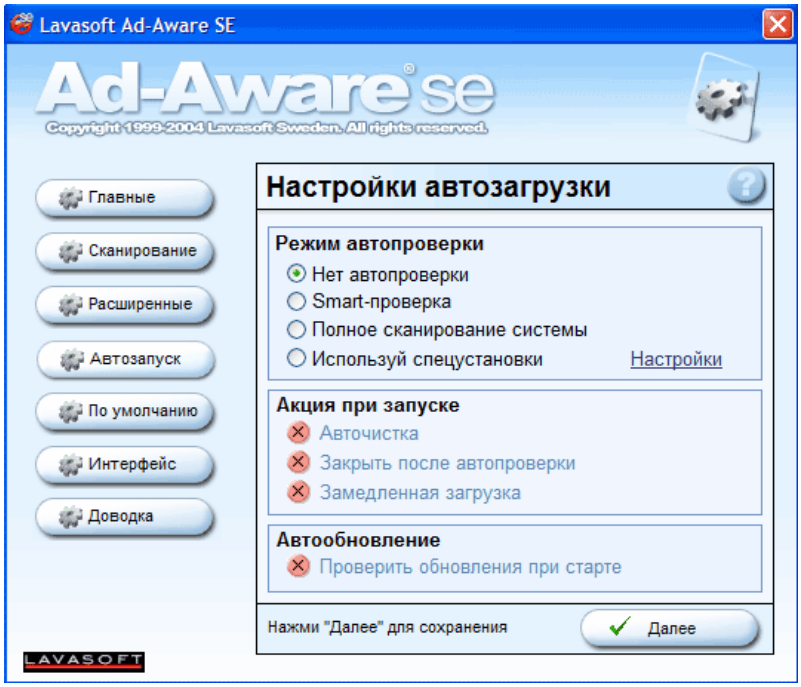


Рисунок 50. Настройка автоматизации.

Автообновление

В разделе "**Автообновление**" поставьте галочку рядом с "**Проверить обновление при старте**"

Режим автопроверки

В разделе "**Режим автопроверки**" выбрать режим сканирования:

- **Нет автопроверки** – отключено, то есть при старте компьютера автопроверка проводиться не будет;
- **Smart-проверка** – при старте компьютера будет производиться интеллектуальная проверка;
- **Полное сканирование системы** – при старте компьютера будет производиться полное сканирование системы;
- **Используй спец-установки** – настраиваемая проверка.

Автоматическая очистка

В разделе "**Акция при запуске**" выбрать "**Авточистка**".

Автокарантин до удаления

Для включения этого режима нажмите кнопку "**Установки Ad-Aware**" (символ механизма в верхнем правильном углу главного окна программы) на инструментальной панели запуска. Откроется окно "**Основные настройки**" главных настроек программы. Проверьте, что "**Автокарантин до удаления**" включен (см. рис. 2) и затем щелкните "**Далее**" для сохранения изменений.

Подготовка к выполнению первого сканирования

Перед первым сканированием компьютера с Ad-Aware SE необходимо выполнить опцию «**Проверить обновления**», чтобы удостовериться, что у вас установлен последний файл определений (см. рис. 1). Также рекомендую включить автокарантирование файлов до их удаления (см. рис. 2). Для этого нажмите кнопку «**Установки Ad-Aware**» (символ механизма в верхнем правильном углу главного окна программы) на инструментальной панели запуска. Откроется окно «**Основные настройки**» главных настроек программы. Проверьте, что «**Автокарантин до удаления**» включен и затем щелкните «**Далее**» для сохранения изменений.

После того, как проделано вышесказанное, вы готовы к первому сканированию. Щелкните кнопку «**Сканировать**» в главном меню на левой стороне главного окна состояния или нажмите кнопку «**Старт**» в нижнем правом углу. Откроется окно «**Подготовить сканирование системы**» (см. рис. 3). Выберите «**Полное сканирование системы**» и щелкните «**Далее**» для запуска первого сканирования.

После завершения сканирования откроется детальный листинг обнаруженных элементов. Внимательно рассмотрите все их перед удалением. Ad-Aware специально разработан для обнаружения и удаления подозрительных вредоносных объектов в вашей системе.

Внимание! Производители программы не предлагают, чтобы все обнаруженные объекты были удалены (хотя у меня не разу не было, чтобы программа ошиблась!). Последнее право решения оставлено за пользователем, но для облегчения понимания какой объект действительно вреден была разработана специальная справочная система TAC.

Выберите все пункты, которые хотите удалить (если хотите удалить все, то по правому щелчку мыши появится контекстное меню, где есть выбор всех файлов!), а затем щелкните кнопку «**Далее**» и в появившемся окне «**OK**» для подтверждения удаления (см. рис. 4).

Если вы хотите сохранить некоторые обнаруженные элементы и не хотите, что Ad-Aware находила их в последствии, то выберите их и через контекстное меню по правой кнопке мыши выберите «**Игнорировать выбранное**».

Как только вы добавите выбранные элементы в лист игнорирования, программа автоматически переведет вас опять к листу результатов сканирования, где вы сможете продолжить необходимые вам действия.

Нажмите далее в окне «**Сканирование выполнено**» для вызова окна «**Результаты сканирования**». Отметьте в этом окне объекты, подлежащие удалению, и нажмите «**Далее**». Затем нажмите «**OK**» для подтверждения удаления.

Автоматические сканирования

Существует три основных вида автоматизации сканирования.

Простое сканирование при старте компьютера

Этот метод можно выставить в «Установках автостарта» в меню установок программы.

Настройки автозапуска

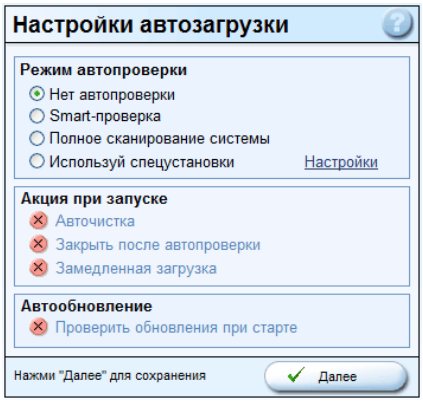


Рисунок 51. Окно настройки автозагрузки

Режим автопроверки

- **Нет автопроверки** – отключено, то есть при старте компьютера автопроверка проводиться не будет;
- **Smart-проверка** – при старте компьютера будет производиться интеллектуальная проверка;
- **Полное сканирование системы** – при старте компьютера будет производиться полное сканирование системы;
- **Используй спец-установки** – настраиваемая проверка.

Для настройки автозапуска сканирования вам необходимо запустить меню «**Настройки**» (значок механизма на инструментальной панели) и выбрать там подменю «**Автозапуск**» (кнопка с левой стороны меню). Выберите необходимый вам режим сканирования.
В разделе «**Акция при запуске**» можно выбрать:

- «**Авточистка**» - после сканирование будет произведена автоочистка инфицированных объектов;
- «**Закрыть после автопроверки**» - после сканирования программа будет автоматически закрыта;
- «**Замедленная загрузка**» - данная опция используется для замедления старта программы в случае, если вы хотите проверять при старте наличие новых обновлений файла определений (для этого в разделе «**Автообновление**» надо выставить «**Проверить обновление при старте**».

Планировщик задач Windows

Автоматизировать сканирование можно используя мощную утилиту Windows – Планировщик задач. Таким образом можно автоматизировать сканирование не только при старте компьютера, но и ежедневно, еженедельно или ежемесячно.
Откройте планировщик задач и выберите значок «Add Scheduled Task». Следуйте указаниям мастера и когда требуется введите требуемый параметр командной строки.
Пример:
"%programfiles%\Lavasoft\Ad-Aware SE Professional\Ad-Aware.exe" /smart +silent +update +nice-2

Ad-Aware запустится без графического интерфейса на заднем плане, перед сканированием проверит обновления (если есть, то загрузит и установит), и затем выполнит smart-проверку в неактивном приоритете.

Расширенная автоматизация

Можно также настроить расширенную автоматизацию программы, используя batch-файлы и сценарии (скрипты).
Пример:
Batch file
@ECHO OFF
"%programfiles%\Lavasoft\Ad-Aware SE Professional\Ad-Aware.exe" /full +update +auto
Такой batch-файл запустит Ad-Aware, выполнит проверку наличия обновлений, затем полное сканирование системы и автоматически удалит все найденные инфицированные объекты.
Пример:
Script
Set WshShell = WScript.CreateObject("WScript.Shell")
Set env = Wshshell.Environment("Process")
Ad-Awarecmd = chr(34) & env("PROGRAMFILES") & "\Lavasoft\Ad-Aware SE Plus\Ad-Aware" & chr(34)
rc = WshShell.Run(Ad-Awarecmd & " /full +update +auto", 0, True)

Предупреждение о вирусе во время сканирования Ad-Aware

При выполнение проверки Ad-Aware фоновый монитор антивирусной программы может выдать предупреждение, что во временном каталоге (%temp%) для текущего пользователя найден вирус.
Это не обязательно означает, что ваш компьютер заражен активным вирусом.
Большинство резидентных антивирусных сканеров не просматривают сжатые файлы на предмет вирусов, а просто проверяют вашу память на предмет подписей активных вирусных инфекций. В течении сканирования Ad-Aware декомпрессирует файлы для их просмотра не активируя содержание, но при этом может сработать резидент антивирусного монитора.
Для избегания этого вы можете удалить вирусоносные файлы, используя менеджер вашей антивирусной программы.
Внимание! Если ваша антивирусная программа не шифрует содержание своего карантина, то поставьте в лист игнорирования Ad-Aware карантинный файл вашего антивируса. В противном случае, возможно, что Ad-Aware будет находить и пытаться вылечить этот файл.

Что такое расширения программы Ad-Aware

Дополнения предназначены для расширения функциональных возможностей Ad-Aware. Они не строго необходимы для работы программы, а только добавляют новые возможности. Они могут помочь для обезвреживания некоторых специальных вредоносителей для Windows, а также предложить дополнительную информацию о подозрительном содержании.
Есть три типа дополнений:

- Инструментальные средства;
- Расширения;
- Статистика.

Инструменты – автономные программы, которые можно использовать без выполнения проверок.
Расширения – обеспечивают дополнительную информацию о найденных объектах и предлагают различные варианты их исследования.
Статистика – показывает информацию о предыдущих проверках системы.
Инструментальные средства и расширения запускаются из окна «**Надстройки**». Инструменты запускаются прямо из этого окна. Расширения возможно запустить только после выполнения сканирования в окнах результатов. Process-Watch можно запустить в любое время.

Загрузка, установка и запуск дополнений

Вы можете бесплатно загрузить дополнения программы с сайта Lavasoft.
Инсталляция дополнений проста. Просто загрузите необходимое вам дополнение и закрыв программу установите его. После этого в окне «**Надстройки**» вы можете запускать установленные дополнения.

Загрузка

1. Идите на сайт Lavasoft.
2. выберите необходимое расширение и щелкните на его ссылке.
3. Внимательно прочтите информацию о расширении, так как там может приводиться критичная информация об его использовании.
4. Внизу страницы с информацией вы найдете ссылку на загрузку дополнения.
5. Нажмите на нее и в появившемся окне задайте имя файла.
6. Выберите местом сохранения папку «**My Documents**» (или что-то подобное) и нажмите «**Save**».
7. Дождитесь полной загрузки.

Установка

1. Из папки «**My Documents**» (или что-то подобного) запустите загруженный файл.
2. Следуйте указаниям мастера инсталляции.

Запуск

Для запуска дополнения в окне «**Настройки**» выберите необходимое вам и нажмите «**Запустить**». Двойной щелчок на элементе также запускает его.

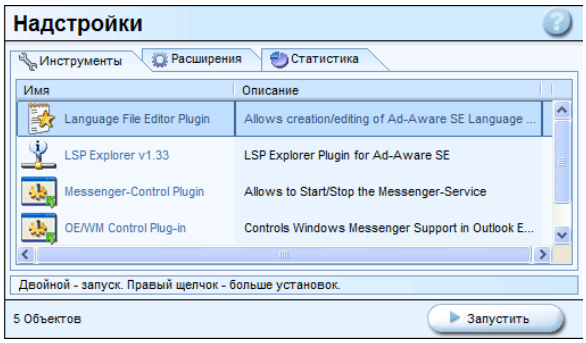


Рисунок 52. Окно надстроек.

Расширения

Расширения запускаются из окон результатов сканирования через контекстное меню.

Удаление дополнений

Все дополнения удаляются автоматически вместе с удалением самого Ad-Aware. Если вы не хотите удалять Ad-Aware, а хотите удалить только какое-либо дополнение, то поступайте так:

1. Закройте Ad-Aware.
2. Нажмите кнопку «**Start**» в Windows.
3. Откройте «**Control Panel**».
4. Далее откройте менеджер «**Add/Remove Program**s».
5. Выберите там подлежащий удалению элемент.
6. Нажмите кнопку «**Change/remove**».
7. Щелкните «**Next**» в появившемся окне.
8. Нажмите «**Finish**» для завершения удаления.

Дополнение деинсталлировано.

Что такое Ad-Watch

Ad-Watch – монитор реального времени. Доступен в версиях Ad-Aware:

- Plus
- Professional

Этот монитор добавляет еще один уровень защиты в вашу систему, так как он работает в режиме реального времени на заднем плане (по аналогии с антивирусным монитором), отсекая паразитов и мальвар от взаимодействия с вашей системой.

Если Ad-Aware чистит вашу систему от уже проникших в нее паразитов, то Ad-Watch ловит и кастрирует этих паразитов еще до входа в систему.

Если Ad-Watch находит вредоносный контент, то он отсекает его и запускает для дополнительной проверки сканер Ad-Aware. Монитор Ad-Watch можно настроить согласно вашим желанием в меню доводки программы.

При помощи Ad-Watch можно блокировать несанкционированные попытки запуска разделов вашего системного реестра, блокировать возможных и фактических налетчиков браузера, блокировать подозрительные процессы, блокировать ассоциации исполняемых файлов, блокировать злонамеренные кукисы, закрывать выпрыгивающие окна. Ad-Watch использует новую технологию CSI, что позволяет блокировать новые элементы.

Если в вашу систему при закрытом Ad-Watch проникнет паразитирующий процесс, то при запуске монитора этот процесс будет «убит».

Если вам необходимо использовать какой-либо процесс, то можно использовать систему фильтрации Ad-Watch. Для этого достаточно нажать «**Принять**»

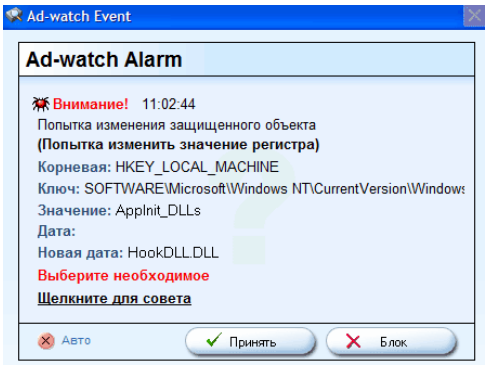


Рисунок 53. Окно нотификации Ad-Watch.

После этого процесс будет добавлен к допускающему фильтру Ad-Watch. Фильтр можно вызвать, нажав кнопку «**Фильтр**» на экране инструментов Ad-Watch.

Кроме того, Ad-Watch содержит также редактор правил, позволяющий вам отредактировать поведение изменения реестра, например, при инсталляции новых программ и смене пользователей.

Примечание! Ad-Watch использует совместно с Ad-Aware файл определений.

Лог событий Ad-Watch

Окно, представленное ниже, показывает все события Ad-Watch.

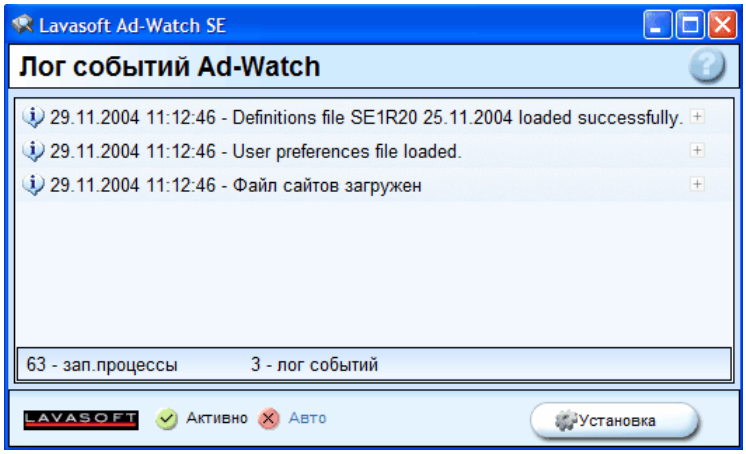


Рисунок 54. Лог событий.

- **Запущенные процессы** – показывает количество запущенных процессов.

Подсказка! При наведении мыши на эту строку вам будут выведены все запущенные в данный момент процессы.

Лог событий – показывает количество событий, отрепортированных за эту сессию Ad-Watch.

Опции:

- **Активно** – включение/выключение монитора без его закрытия;
- **Авто** – все вредные активности блокируются автоматически.

Кнопки

- «**?**» – открывает быструю помощь
- «**Установка**» - открывает окно настройки Ad-Watch.

По правому щелчку мыши вызывается контекстное меню.

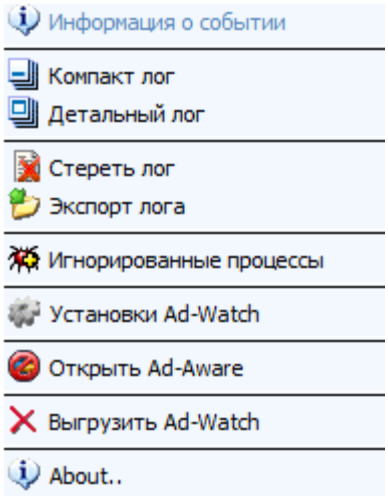


Рисунок 55. Контекстное меню Ad-Watch.

- **Информация о событии** – выводит информацию с сайта Lavasoft о выделенном событии.
- **Компактный лог** – сворачивает информацию в окне в линии.
- **Детальный лог** – разворачивает информацию в окне.
- **Стереть лог** – стирает текущий лог (**Внимание!** Это не стирает журнал событий Ad-Watch).

- **Экспорт лога** – экспортирует лог в выбранный вами текстовый файл.
- **Игнорированные процессы** – команда открывает окно «Фильтр» из настроек программы.
- **Установки Ad-Watch** – открывает окно «**Установки**»
- **Открыть Ad-Aware** – запускает Ad-Aware.
- **Выгрузить Ad-Watch** – выгружает и закрывает Ad-Watch.
- **About** – открывает окно с копирайтом Ad-Aware.

Инструменты и предпочтения

Для облегчения пользования Ad-Watch все настройки были собраны в специальном меню настроек.

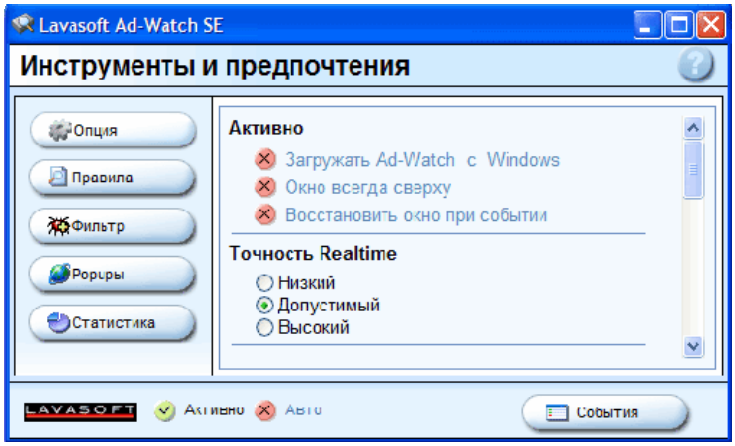


Рисунок 56. Инструменты и предпочтения.

Кнопки

- «**?**» - вызывает быструю подсказку.
- «**События**» - открывает окно «**События**».
- «**Опция**» – открывает окно «**Опции**».
- «**Правила**» - открывает окно «**Правила**».
- «**Фильтр**» - открывает окно «**Фильтр**»
- «**Ропупы**» - открывает окно «**Ропупы**»
- «**Статистика**» - открывает окно «**Статистика**».

Опции:

- **Активно** – включение/выключение монитора без его закрытия;
- **Авто** – все вредные активности блокируются автоматически.

Опции

Активно

- **Загружать Ad-Watch с Windows** – старт Ad-Watch вместе с Windows.
- **Окно всегда сверху** – форсирование программы, чтобы при восстановлении окно Ad-Watch было поверх всех остальных окон.
- **Восстановить окно при событии** – при использовании этой опции окно Ad-Watch открывается только при новом событии.

Точность RealTime

- **Низкий** – монитор Ad-Watch работает с малым системным приоритетом.
- **Допустимый** – монитор Ad-Watch работает с нормальным системным приоритетом.
- **Высокий** – монитор Ad-Watch работает с высоким системным приоритетом.

Условия блока

- **Замок секции startup** – выставляет замок на изменение секции автозапуска в реестре.
- **Замок на ассоциации файлов** – выставляет замок на запуск ассоциации исполнительного файла.
- **Блок возможных атак** – блокирует приклеивание и последующий запуск файлов налетчиков-браузера.
- **Блок подозрительных процессов** – блокирует подозрительные процессы.
- **Блок tracking cookie** – блокировка следящих кукисов.
- **Включить Pop-up блокер** – включение блокиратора выпрыгивающих окон.

Лог и установка

- **Лог активности регистра** – запись в журнал событий активности реестра Windows.
- **Лог Tracking Cookie** – запись в журнал событий лога следящих кукисов.
- **Лог активной памяти** – запись в журнал событий лога активной памяти.
- **Лог Pop-upов** – запись в журнал событий лога блокировки выпрыгивающих окон.
- **Лог внутренних событий** – запись в журнал событий лога внутренних действий программы.

История событий – создание журнала лога блокировки согласно вышеприведенным настройкам.

- **Необходимо указать имя и месторасположения файла журнала.**
- **Показать текущую историю** – показ текущего лога событий.
- **Очистить историю** – очистка содержимого журнала событий.

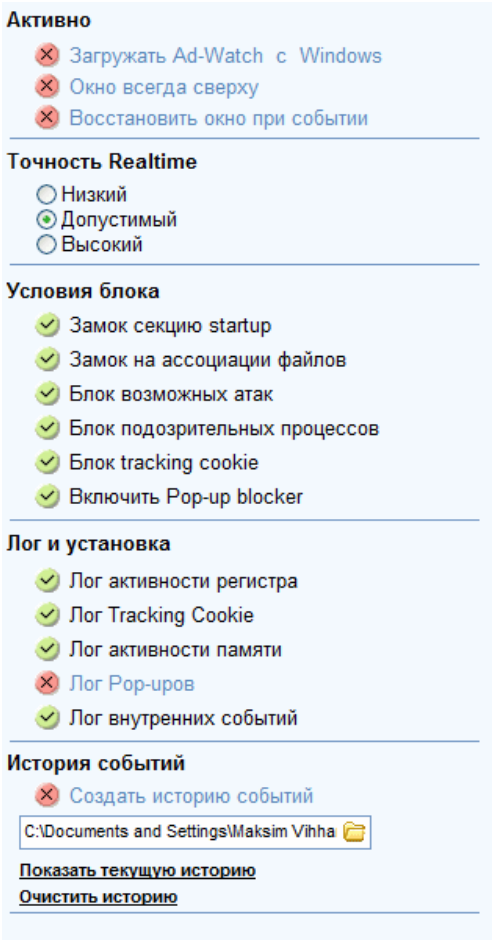


Рисунок 57. Окно опций монитора.

Правила

Определяя правила пользователь может разрешить или запретить изменения реестра.

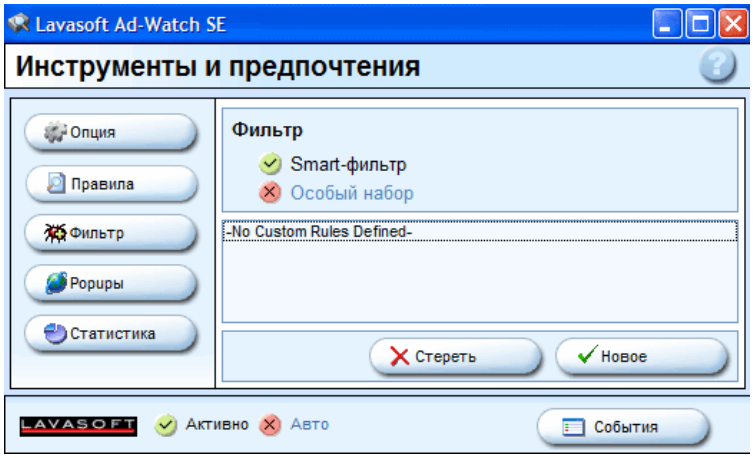


Рисунок 58. Окно правил.

Фильтр

- **Smart-фильтр** – Ad-Watch позволяет/запрещает стандартные события IE, такие как изменения шрифта, его размера, месторасположение панелей инструментов и так далее.
- **Особый набор** – Ad-Watch использует правила, определенные пользователем. Можно использовать совместно со smart-фильтром.

Кнопки

- **Стереть** – стирает выбранное правило
- **Новое** – создание нового правила.

По правому щелчку мыши вызывается контекстное меню.

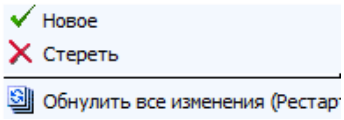


Рисунок 59. Контекстное меню правил.

- **Новое** – создание нового правила.
- **Стереть** – удаление выбранного правила.
- **Обнулить все изменения (рестарт)** – обнуляет все изменения в листе правил. Необходимо подтверждение.

Добавление нового правила

- **Имя правила** – необходимо задать имя правила.

Условия

- **Игнорировать событие при совпадении ключа** – введите ключ реестра.
- **Или совпадении значения** – введите значение реестра.
- **Точное** – точное совпадение.
- **Частичное** – частичное совпадение.

Кнопки

- «Сброс» - выход из менеджера нового правила без сохранения (сброс).
- «Добавить» - добавление нового правила.

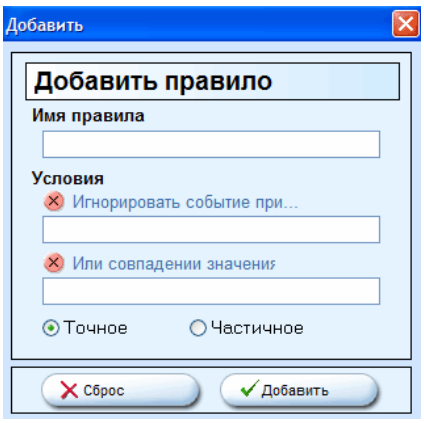


Рисунок 60. Окно добавления нового правила.

Фильтр

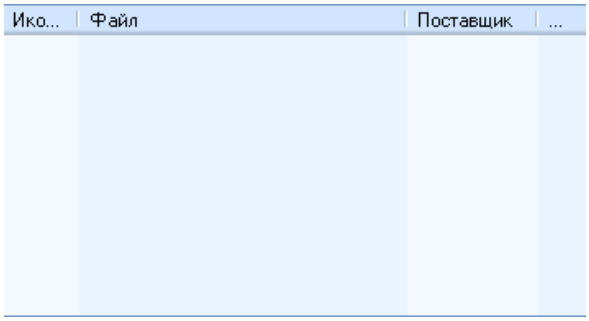


Рисунок 61. Окно фильтра. В данный момент ни одного фильтра не определено.

В данном окне перечислены процессы, которым разрешено запускаться.
Процесс представлен в виде:

- **Иконка** – иконка процесса.
- **Файл** – имя процесса.
- **Поставщик** – создатель или категория процесса.
- **Комментарий** – комментарий к процессу.

Если вы хотите разрешить какой-либо программе загружать свой процесс в память, то отключите в главном окне Ad-Watch опцию «**Авто**». После этого при запросе о разрешении нужного процесса нажмите кнопку «**Принять**» (см. рис. 53).
Если вы хотите запретить этот процесс, то соответственно нажмите «**Блок**».
Внимание! Операции с реестром не могут быть добавлены в этот фильтр.
По правому щелчку мыши вызывается контекстное меню.

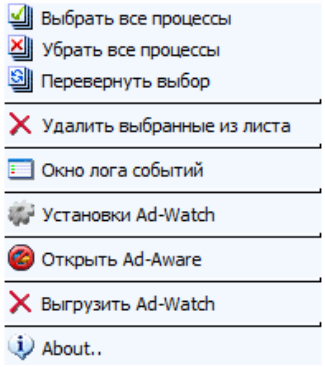


Рисунок 62. Контекстное меню.

- Выбрать все процессы – выбор всех перечисленных в окне процессов.

- **Убрать все процессы** – сброс выбора всех процессов.
- **Перевернуть выбор** – инвертирование выбора.
- **Удалить выбранные из листа** – удаляет выбранные процессы из листа фильтра.
- **Окно лога событий** – вызывает журнал событий.
- **Установки Ad-Watch** – вызывает окно установок Ad-Watch.
- **Открыть Ad-Aware** – запуск Ad-Aware.
- **Выгрузить Ad-Watch** – выгрузка и закрытие Ad-Watch.
- **About** – вызов окна копирайта для Ad-Aware.

Ропупы

Это список сайтов с которых будут блокироваться выскакивающие окна. Весь этот список хранится в файле sites.txt в директории с установленным Ad-Aware SE.

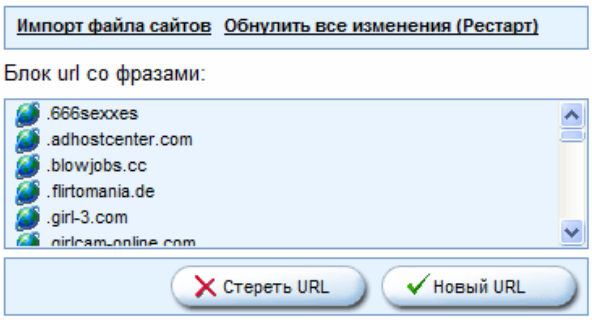


Рисунок 63. Окно блокировки всплывающих окон.

Блокиратор всплывающих окон позволяет легко добавлять или удалят в черный список сайты. Вы также можете создавать собственные черные списки в Блокноте (Notepad). В таком случае каждая строка может содержать или часть, или полную ссылку на сайт. Нельзя приводить в одной строке два разных сайта! Ни в коем случае нельзя после последней строки ставить Enter!

Подсказка! Редактирование файла sites.txt можно использовать в качестве родительского контроля (Parental Control) – просто добавьте ссылку на такой сайт в текстовый документ!

Кнопки

- **Импорт файла сайтов** – импорт в блокиратор созданных пользователем черных списков.
- **Обнулить все изменения** – обнуляет все изменения за текущую сессию. Необходимо подтверждение.
- **Стереть URL** – стирание выделенной ссылки из черного списка.
- **Новый URL** – добавление в черный список новой ссылки.

По правому щелчку мыши вызывается контекстное меню.

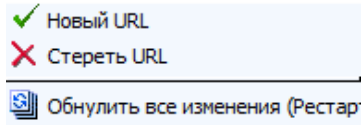


Рисунок 64. Контекстное меню.

- **Новый URL** – добавление в черный список новой ссылки.
- **Стереть URL** – стирание выделенной ссылки из черного списка.
- **Обнулить все изменения** – обнуляет все изменения за текущую сессию. Необходимо подтверждение.

Статистика

Показывает статистику блокировки и фильтрации Ad-Watch.

Рисунок 65. Статистика Ad-Watch.

Кнопки

- «**Как txt-файл**» – экспорт статистики в указанный вам текстовый файл.
- «**Обнулить статистику**» – обнуление всей статистики.

Резюме

- **Всего событий** – общее количество событий Ad-Watch.
- **Блокировано** – количество блокированного контента.
- **Допущено** – количество допущенного контента.

Детали

- **Блокировано процессов** – количество блокированных процессов.
- **Блокировано атак** – количество блокированных атак.
- **Блокирование событий регистра** – количество блокированных операций с реестром.
- **Блокировано Tracking Cookie** – количество блокированных следящих кукисов.
- **Блокировано Порупов** – количество блокированных выпрыгивающих окон.
- **Внутренние события** – количество внутренних событий программы.

Что такое Process-Watch

Профессиональное издание Ad-Aware поставляется вместе с Process-Watch – мощным инструментом для просмотра и управления процессов. Process-Watch позволяет просматривать и проверять процессы и их модули, при использовании дополнений программы также их детально анализировать. Расширение программы требует предварительного выбора обследуемого процесса, а затем запускается через контекстное меню по правой кнопке мыши.

Process-Watch показывает моментальный снимок всех процессов (вершина) и их модулей (основание) во время своего запуска. Этот снимок может быть в любое время обновлен простым нажатием на кнопку «**Обновить**».

Process-Watch отображает два информационных списка. Верхний список – это процессы, а нижний – модули выбранного в верхнем окне процесса.

Process-Watch позволяет «убить» любой процесс или закончить какой-либо модуль. **Внимание!** Некоторые процессы и модули жизненважны для нормальной работы вашего Windows.

При помощи Process-Watch вы можете проверить любой из процессов на «вредность» и в случае надобности закрыть его.

По умолчанию, Process-Watch показывает только привязанные к окнам на экране компьютера процессы, вы можете при необходимости вывести все процессы, убрав опцию «**Ограничить видимые окна**».

Интерфейс Process-Watch

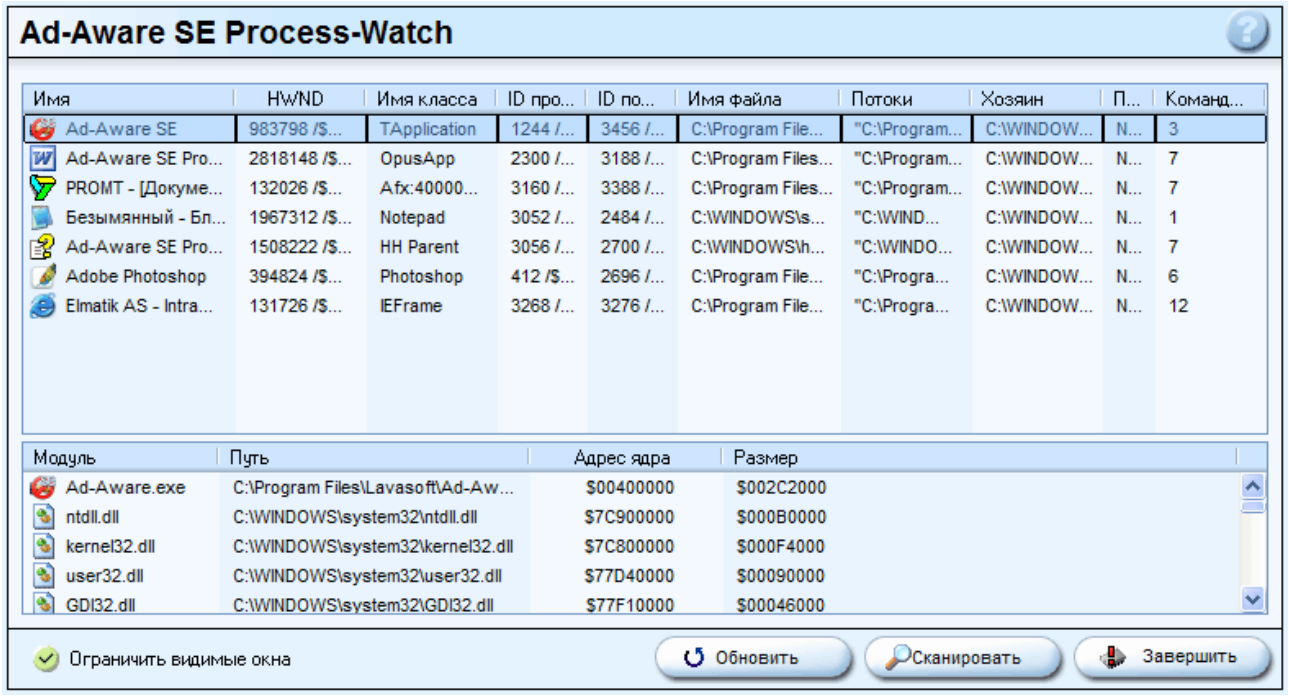


Рисунок 66. Интерфейс Process-Watch.

Кнопки

- «**?**» - показывает подсказку.
- «**Обновить**» - обновляет снимок процессов и модулей.
- «**Сканировать**» - сканирование исполнительных файлов на все процессы. Во время этого сканирования фильтры отменены. Если сканирование найдет вредоносный процесс/модуль, то он будет выделен красным цветом.
- «**Завершить**» - завершение выбранного процесса.

Подсказки!

Двойное нажатие мышкой на процессе открывает окно со свойствами в проводнике Windows.

Двойное нажатие мышкой на модуле откроет в новом окне дамп памяти модуля.

Клавиатурные комбинации

- «↑» или «↓» - перемещение по листу процессов вверх или вниз.
- «**F5**» - обновление снимка процессов.
- «**CTRL+N**» - переключение к следующему инфицированному процессу. Работает только при наличии инфицированных процессов.
- «**CTRL+P**» - переключение к предыдущему инфицированному процессу. Работает только при наличии инфицированных процессов.
- «**CTRL+T**» - прекращение выбранного процесса.

Пояснения в окне

- **Имя** – имя процесса. При выключенной опции привязки к окнам заголовка процесса может и не быть.
- **HWND** – дескриптор, назначенный процессу со стороны Windows.
- **Имя класса** – классификация процесса.
- **ID процесса** – уникальная метка процесса.
- **ID потока** – уникальная метка потока.
- **Имя файла** – имя файла, порождающего процесс, и путь к нему.

- **Потоки** – командная строка вызывающая процесс. Включает путь и имя файла, вызывающего процесс плюс параметры командной строки.
- **Хозяин** – родительский процесс выбранного процесса.
- **Приоритет** – приоритет процесса.
- **Командная строка** – количество потоков, вызванных процессом.

По правому щелчку мыши в окне процессов вызывается контекстное меню.

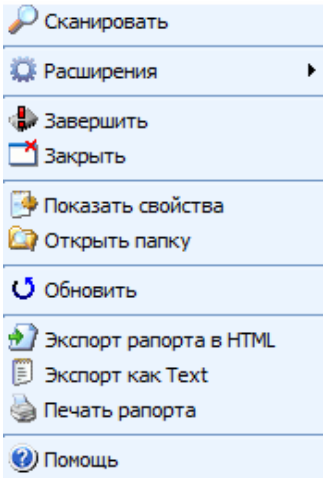


Рисунок 67. Контекстное меню окна процессов.

- **Сканировать** – сканирование исполнительных файлов на все процессы. Во время этого сканирования фильтры отменены. Если сканирование найдет вредоносный процесс, то он будет выделен красным цветом.
- **Расширения** – вызывает доступные расширения программы для дальнейшего анализирования процесса.
- **Завершить** – завершение процесса или модуля.
- **Закрыть** – закрывает окно выбранного процесса без закрытия самого процесса. Можно использовать, например, для закрытия окна проводника.
- **Показать свойства** – показывает свойства файла, вызвавшего процесс, в проводнике.
- **Открыть папку** – открывает папку с файлом, вызвавшим процесс.
- **Обновить** – обновляет снимок процессов.
- **Экспорт рапорта в HTML** – экспортирует рапорт в указанный вами HTML-файл.
- **Экспорт как Text** - экспортирует рапорт в указанный вами текстовый файл.
- **Печать рапорта** – печать рапорта на принтере.
- **Помощь** – открывает файл справки.

По правому щелчку мыши в окне модулей вызывается контекстное меню.

- **Сканмодули** – сканирование всех модулей, вызванных этим процессом. Во время этого сканирования фильтры отменены. Если сканирование найдет вредоносный модуль, то он будет выделен красным цветом.
- **Расширения** – вызывает доступные расширения программы для дальнейшего анализирования модуля.
- **Показать свойства** – показывает свойства модуля в проводнике.
- **Открыть папку** – открывает папку с файлом, вызвавшим модуль процесса.
- **Обновить** – обновляет снимок модулей.
- **Выгрузить модуль** – выгружает выбранный модуль.
- **Дамп памяти процесса** – открывает окно с дампом памяти модуля процесса.
- **Дамп памяти процесса на диск** – создает на диске в указанный файл дамп памяти.
- **Экспорт рапорта в HTML** – экспортирует рапорт в указанный вами HTML-файл.
- **Экспорт как Text** - экспортирует рапорт в указанный вами текстовый файл.

- **Печать рапорта** – печать рапорта на принтере.
- **Помощь** – открывает файл справки.

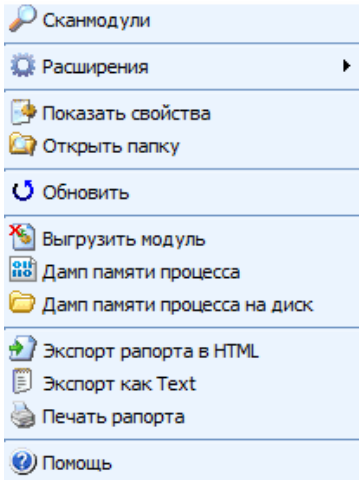


Рисунок 68. Контекстное меню окна модулей.

Покупка дополнительного программного обеспечения Lavasoft.

Приобретение продуктов в России.

Продукты Lavasoft Ad-Aware можно приобрести в интернет-магазине www.avsoft.ru
По вопросам приобретения корпоративных версий продуктов обращайтесь по адресу sales@avsoft.ru
Подробная информация о продуктах - www.adaware.ru

Заказы для домашнего использования.

Пожалуйста посетите: http://www.lavasoft.de/purchase/home/
Или связь по электронной почте: sales@lavasoft.de

Заказы для корпоративных пользователей.

Пожалуйста посетите: http://www.lavasoft.de/purchase/business/
Или связь по электронной почте: corporatesales@lavasoft.de

Выше перечисленные каналы только для закупок, не для обеспечения пользовательской поддержки.

Пользовательская поддержка

Пользовательская поддержка осуществляется здесь.

Или вы всегда можете найти отклик на одном из лучших русскоязычных форумов http://www.imho.ws

Поддержка

Поддержка осуществляется здесь: www.lavasoftsupport.com

База данных программы доступна здесь: http://www.lavasofthelp.com/

TAC рейтинг доступен здесь: http://www.lavasoftnews.com/ms/tac_main.htm

Автору данного мануала можете написать сюда: vihharev@gmail.com (пожалуйста имейте ввиду, что я не осуществляю поддержки программным продуктам Lavasoft, пишите только информацию о этом мануале).

Threat Assessment Chart – TAC

Все найденные Ad-Aware SE объекты классифицируются по Диаграмме оценки угрозы (TAC). Система дает оценки от 1 (наименее опасно) до 10 (наиболее опасно и/или проблематично).