Алексей Грибанов

Антивирус **AVG**

Краткое описание и основы работы.

Об авторских правах:

Автор: Алексей Грибанов

Оглавление

Введение

Чешская Компания Grisoft, разрабатывающая данный антивирус, сделала очень удачный маркетинговый ход для привлечения новых клиентов - выпустила бесплатную версию антивируса, которая практически ничем не отличается от платной. Борьба за соблюдение авторских прав на интеллектуальную собственность, сегодня привела к тому, что тема **бесплатного** программного обеспечения стала особенно актуальной. Как правило, бесплатные приложения создаются энтузиастами и нередко уступают платным аналогам по функциональным возможностям. В случае с антивирусом **AVG Free Edition** это не так.

Компания **Grisoft** выпускает целый ряд программных продуктов под общим брендом **AVG**. Ее продуктовая линейка включает в себя как небольшие утилиты для домашнего компьютера, так и комплексные решения для защиты информации уровня предприятия. Специально для домашних пользователей предназначен **бесплатный** антивирус **AVG Anti-Virus Free Edition**.

1. Возможности

С помощью этого антивируса можно **сканировать** выбранные файлы (даже внутри архивов), отдельные директории, либо жесткие диски целиком, а также **вести мониторинг** системы в режиме реального времени. При сканировании программа применяет **эвристические методы анализа**. Найденные зараженные файлы помещаются на "карантин". Есть **возможность запланировать** регулярное сканирование в определенный период времени.

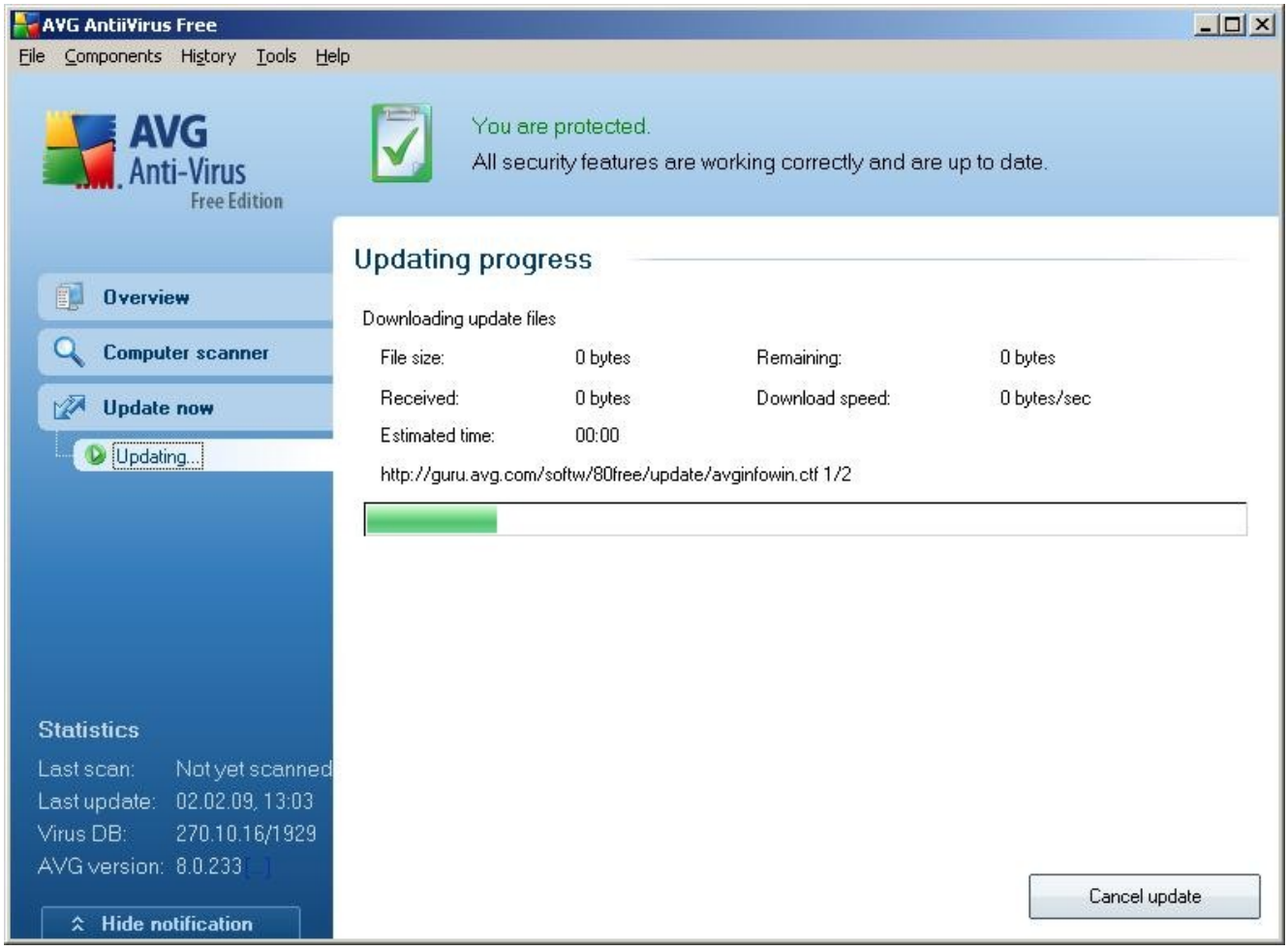
К сожалению, в бесплатной версии **отсутствует возможность проверки на наличие руткитов (RootKit)**, но это поправимо. Скачать утилиту для обнаружения руткитов можно
здесь: http://www.grisoft.cz/filedir/beta/avgarkt/

Примечание: *В системе Windows под **RootKit** принято считать программу, которая внедряется в систему и перехватывает системные API функции, или производит замену системных библиотек. Это позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения даже антивирусным ПО. Кроме того, RootKit способен маскировать присутствие в системе любых процессов, папок и файлов на диске, ключей в реестре. Многие RootKit устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми»).*

Интерфейс AVG Anti-Virus Free Edition переведён на множество языков, однако **русского языка** в их числе **нет**. Это тоже можно было бы считать недостатком, если бы программа требовала сколько-нибудь сложной настройки. Но число настроек минимально, а интерфейс интуитивно понятен.

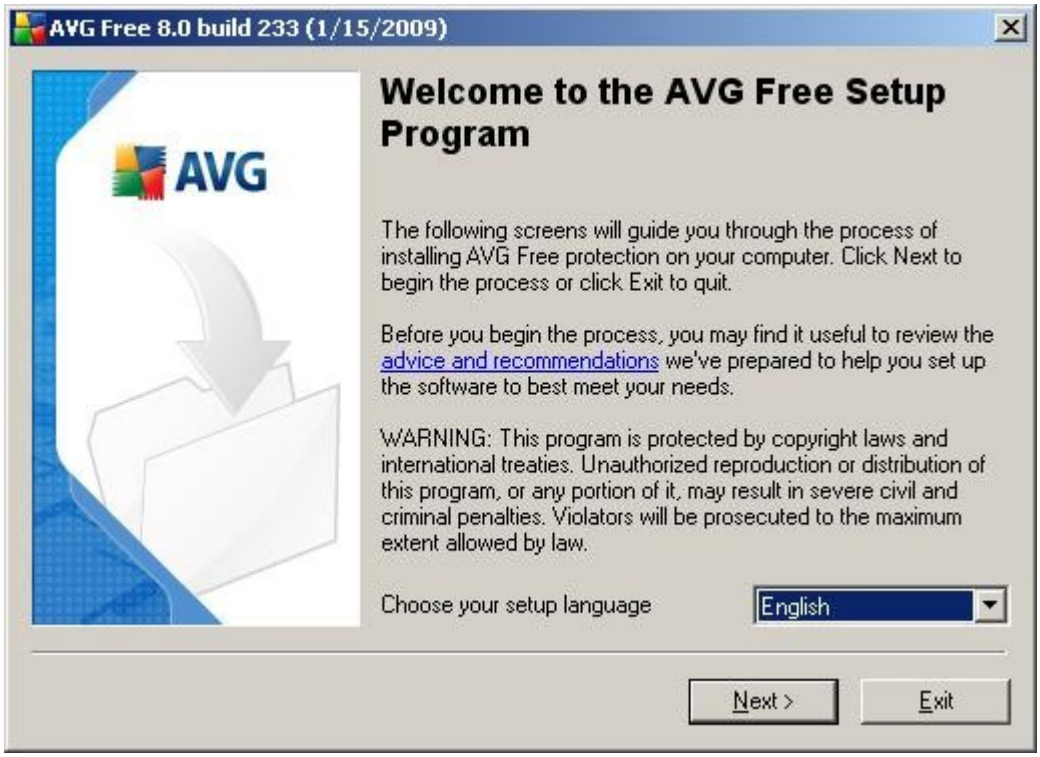
В качестве несомненных достоинств можно упомянуть **небольшой размер регулярных обновлений антивирусных баз**. При этом размер дистрибутива программы довольно внушителен – 57,2 Мб.

2. Сравнение с платными версиями



Усовершенствования платного релиза касаются не основных опций программы по проверке системы на наличие вирусов, а **настройки интерфейса** и некоторых других второстепенных возможностей. Например, для владельцев AVG Antivirus Professional доступны **дополнительные языки** интерфейса (полагаем, что без бразильского, португальского и сербского можно обойтись), автоматическое **обновление** антивирусных **баз с быстрых серверов**, круглосуточная **поддержка по почте**, возможность **планирования заданий** для каждого пользователя отдельно. Думаем, что большинство пользователей, в особенности, домашних ПК вполне может обойтись без этих расширений.

3. Установка

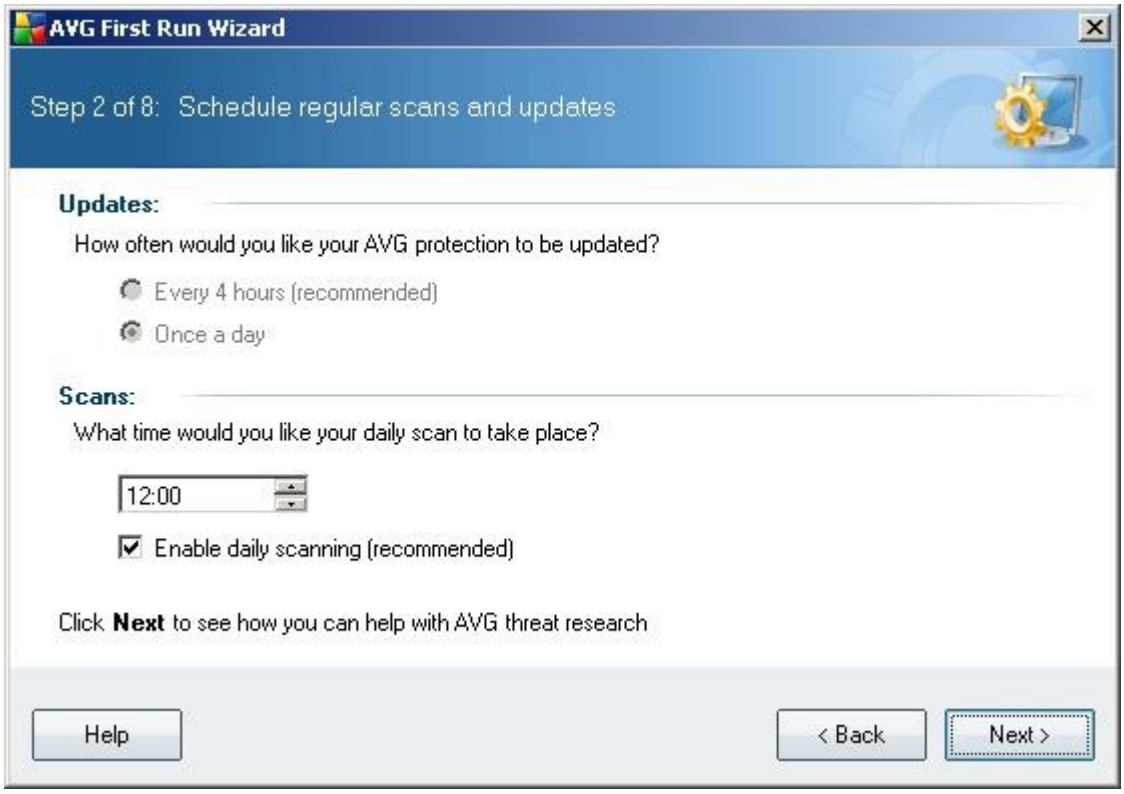


Установка не отличается никакими особенностями и состоит их 8 этапов. На первом из них программа делает уточняющие запросы, при этом заданы все ответы по умолчанию. В процессе установки нужно будет:

- выбрать язык (Английский или испанский);
- подтвердить намерение использовать программу дома в личных целях;
- согласиться с условиями лицензии;
- выбрать стандартную установку (или вручную);
- просмотреть регистрационный номер;
- инсталляцию тулбара,

4. Первый запуск.

После установки, запустится мастер первого запуска AVG, программа предложит задать **график обновлений** (не редактируется – 1 раз в день) и **график проверок.**

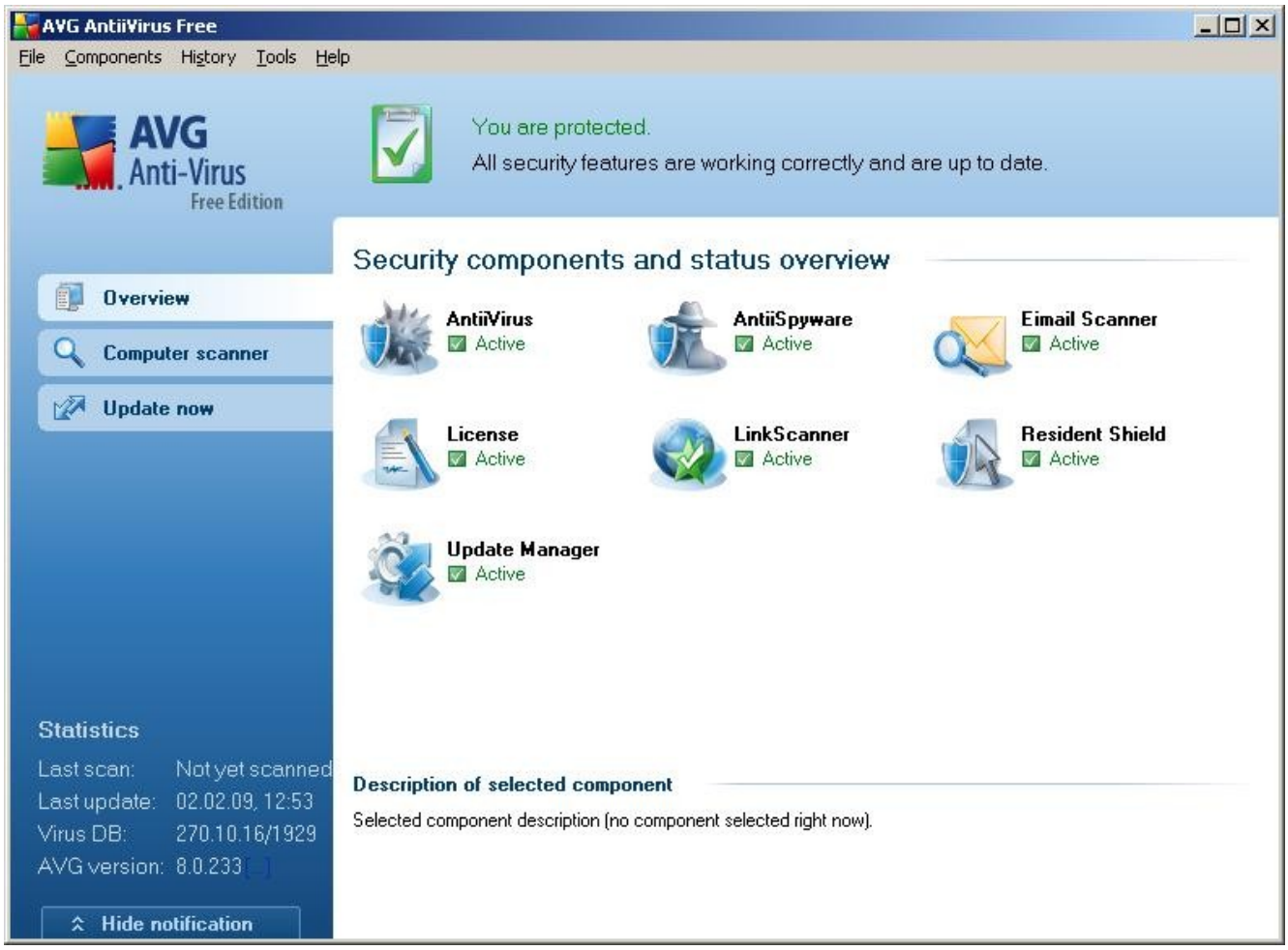


Затем последует еще несколько несущественных запросов: **интеграция** в тулбар поисковика (заодно рекомендация по установке Yahoo в качестве основного поиска) и **регистрация**.

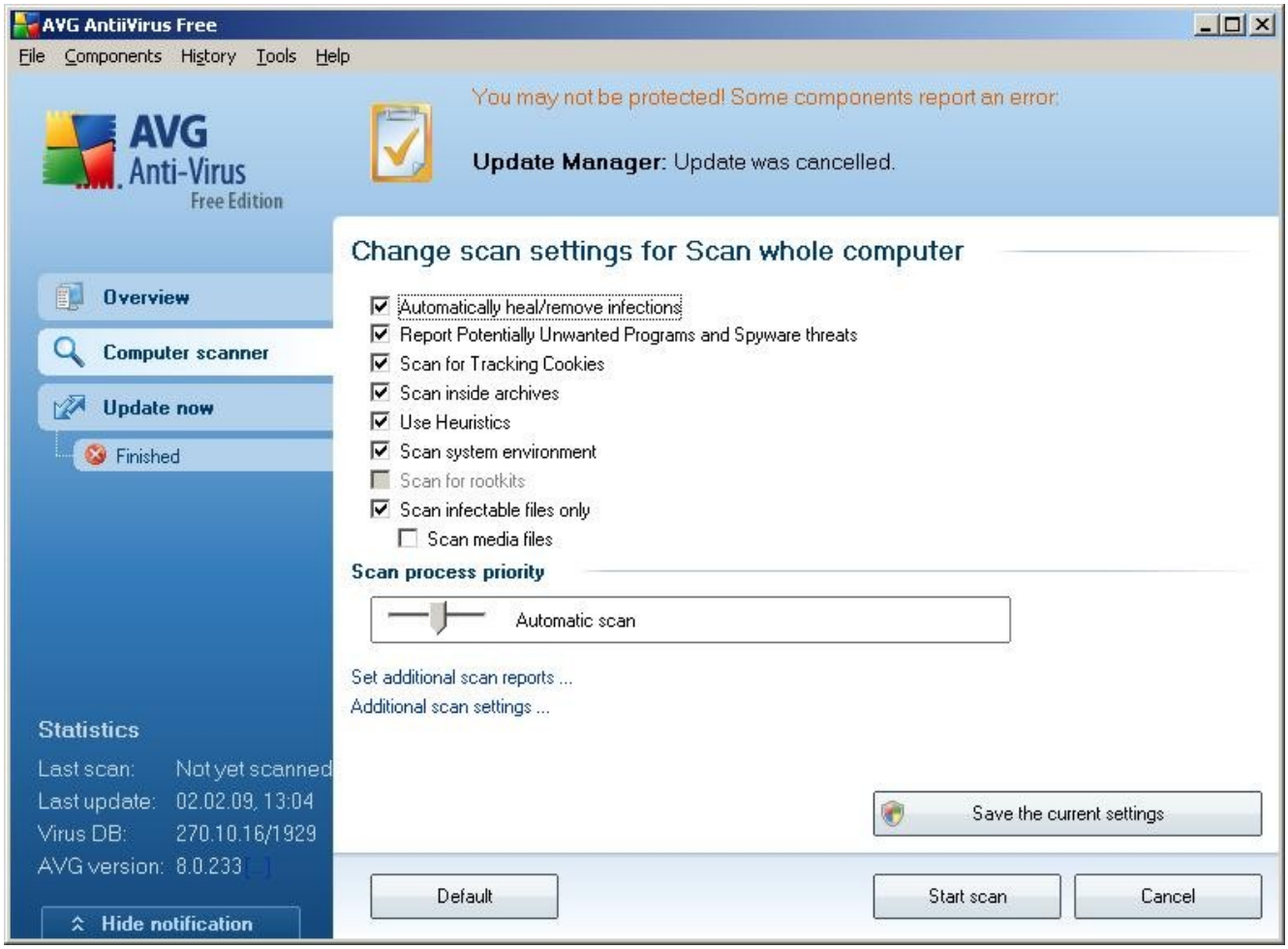
Поскольку AVG Free Edition - это бесплатное приложение, вы можете его и не регистрировать. **Регистрация** позволит вам получить **доступ к форуму**, где вы можете задавать любые вопросы, касающиеся работы с антивирусом. Также после регистрации вы сможете получать **письма** от Grisoft **с информацией об обновлениях** программы.

5. Основные функции

Программа **имеет три основных вкладки** - **Overview** (Общая), **Computer Scaner** (Сканирование) и **Update now** (Обновить). Интерфейс бесплатной версии программы английский и не поддерживает многоязыковую поддержку (кстати, в версии Pro, несмотря на наличие нескольких альтернативных языков интерфейса, **русский язык отсутствует**). Вкладка **Overview** позволяет просмотреть наличие и текущее состояние элементов защиты и их настройки.



Достаточно нажать на любой из элементов и посмотреть все его характеристики, дату обновления, активность и пр.

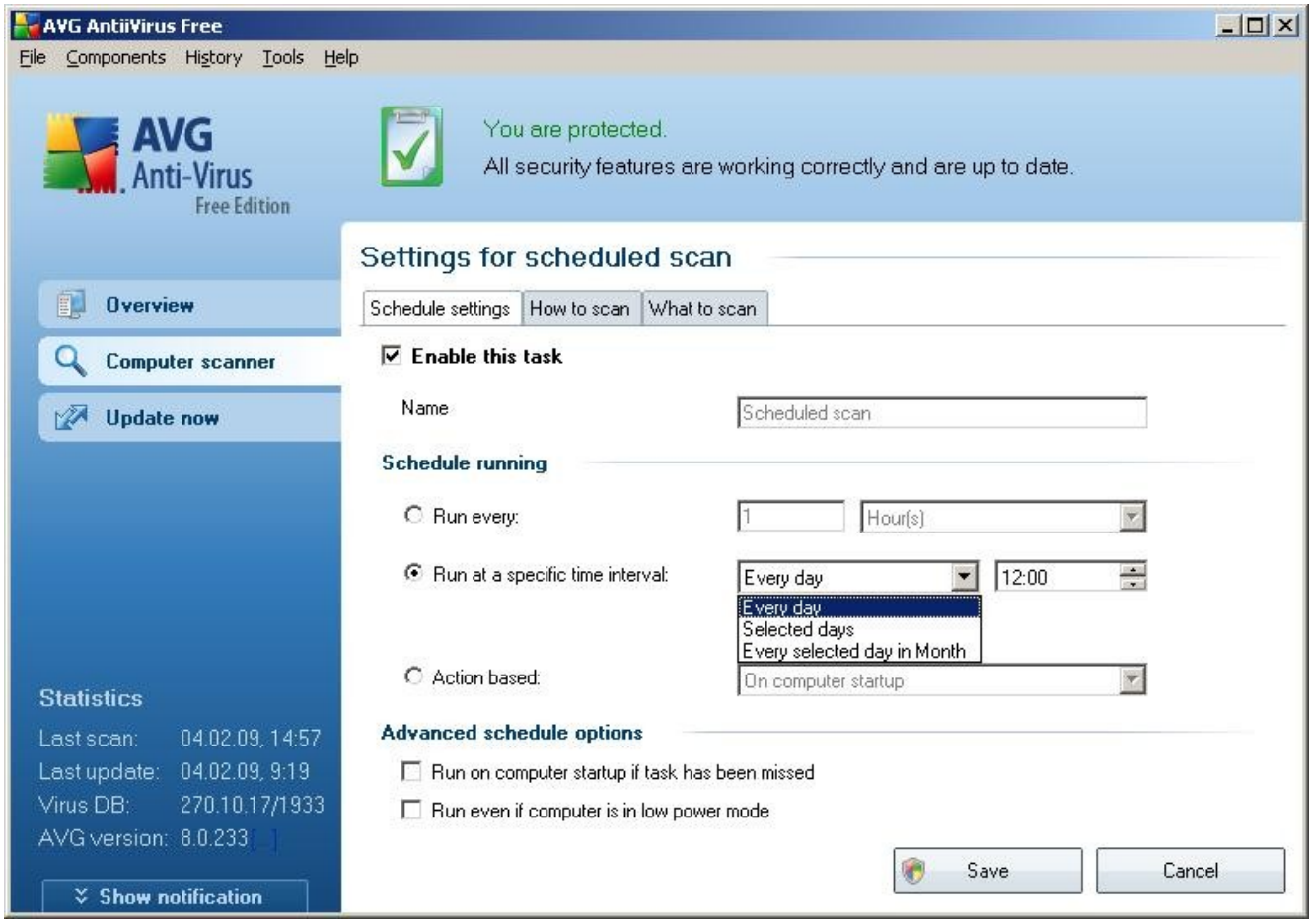


Вторая вкладка **Computer Scaner** позволяет управлять настройками сканирования, формированием отчетов и т.д. Здесь же можно установить приоритет, т.е. какой процент ресурсов антивирус может использовать в своих целях. Если вы планируете выполнять сканирование, например, по ночам, в Ваше отсутствие, можно смело ставить максимальный приоритет – это повысит скорость обработки.

Программа хранит информацию о нескольких последних запусках антивируса (верхнее меню **History**).

Отсюда также можно получить доступ к **результатам** тестирования или настроить **планировщик** заданий (**Scheduler**). Правда, в бесплатной версии отсутствует возможность создания собственных задач по расписанию, однако вы можете редактировать **базовые задания**.

6. Настройка расписания



Вариантов немного, но вполне достаточно. Во-первых, нужно включить работу по расписанию (галочка **Enable this task**), Затем выбрать один из 3-х вариантов:

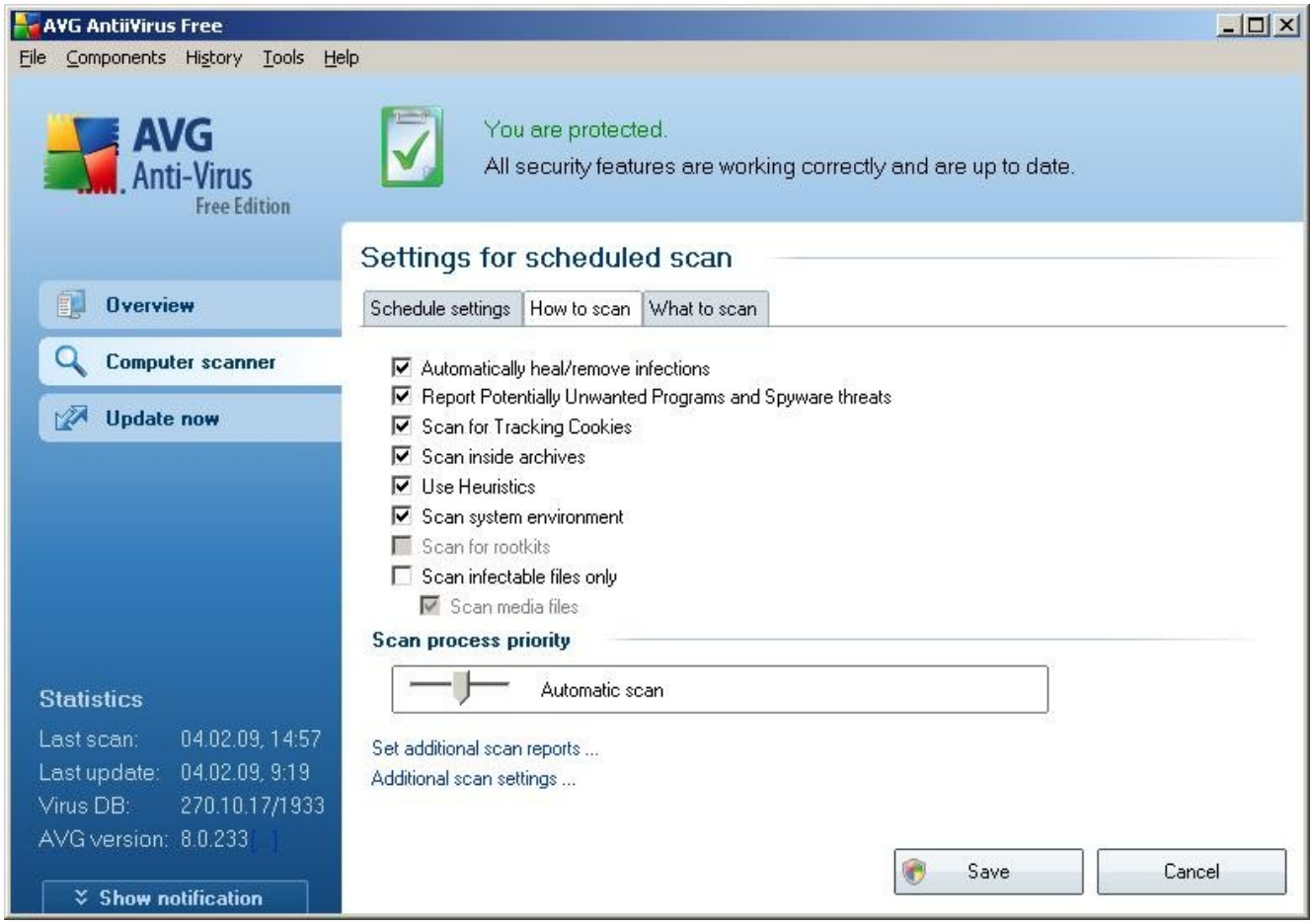
1. Запускать каждые n-часов (по-умолчанию 1);
2. Запускать в определенное время ежедневно, по определенным дням недели или по определенным числам месяца (например 1-го числа каждого месяца);
3. Запускать при каждом включении компьютера

После того, как определились с расписанием, нужно отметить, что должна сделать программа, если выполнить задание не удалось (выходной, отпуск и т.п.)

Есть два варианта: выполнить задание **при первом же включении** компьютера или запускать его в фоновом режиме, когда компьютер не используется (**спящий режим**). Последний вариант предполагает автоматическое включение проверки, ее остановку, если вы снова работаете и продолжение проверки, когда вы снова пошли покурить.

Вы можете настроить программу на выполнение сканирования **ежедневно** в заданное время или установить **временной интервал**, в течение которого будет происходить проверка наличия обновлений (например, с четырех до шести утра, когда вы спите, а интернет доступен).

В этом же окне есть еще две дополнительные вкладки: Как сканировать (**How to scan**) и Что сканировать (**What to scan**). На первой можно уточнить параметры сканирования:



- Автоматическое лечение/удаление зараженных файлов
- Отчет о потенциально-опасных программах и программ-шпионов
- Сканирование «куков» (ссылок Интернета)
- Сканирование внутри архивов
- Использование эвристики
- Проверка системных драйверов
- Проверка только потенциально-опасных файлов (.exe, .com и т.п)
- Проверка медиа-файлов (музыки, видео и т.д.)

Если нажать на «**Additional scan settings...**», появится такое окошко. Здесь можно разрешить выключение компьютера после выполнения проверки. И, если разрешено, то можно еще разрешить форсированное его выключение, в случае обнаружения вирусной атаки. Т.е. не дожидаясь окончания проверки (чтобы без вашего ведома вирус не натворил чего-нибудь)

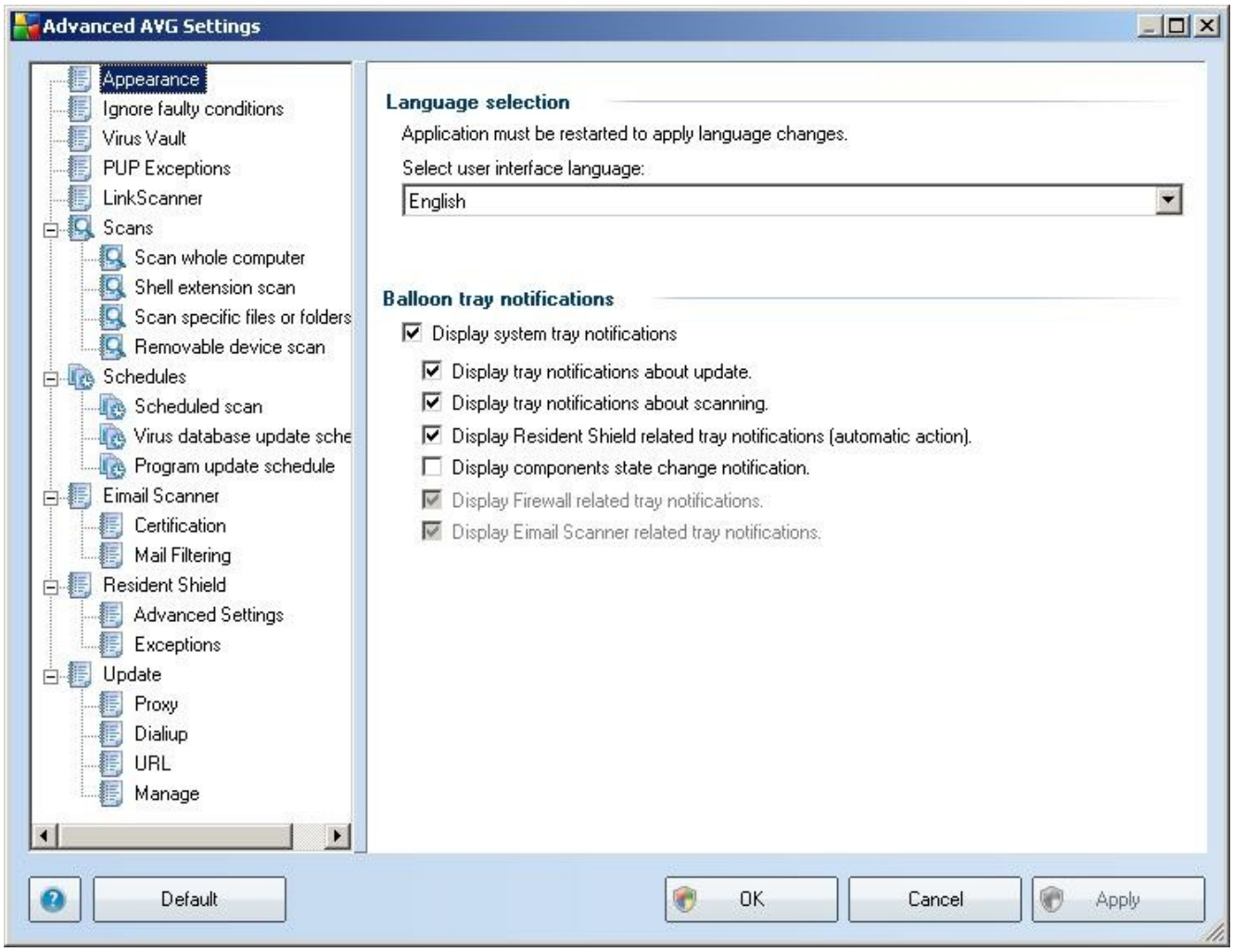
На вкладке «Что сканировать» можно ограничить область сканирования каким-нибудь одним или несколькими дисками, папками или даже файлами. Но зачем?

7. Окно «Вирусный склеп»

Окно Virus Vault. Во многих современных антивирусных пакетах присутствует функция "**карантин**", блокирующая доступ к подозрительным файлам. Аналогичная опция есть и в AVG. К ее созданию авторы отнеслись с долей чешского юмора и назвали ее **Virus Vault** (Вирусный склеп). При появлении признаков вирусной деятельности, разработчики рекомендуют помещать в этот склеп файлы, вызывающие сомнение. (Для этого иногда вполне достаточно просто «разрешить» сделать это самой программе во время проверки).

Если вы загрузили из Интернета какой-нибудь архив, после чего система стала работать нестабильно, добавьте этот файл в список Virus Vault. Если архив содержит вирус, и он не успел распространиться на другие файлы, у вас есть шанс, что после блокирования к нему доступа нормальная работа будет восстановлена. Файлы, помещенные на карантин, могут занимать до **двадцати процентов объема жесткого диска**. Размер дискового пространства для «склепа» также задается в настройках.

8. Окно всех настроек



И, наконец, через меню **Tools-Advansed settings...** можно попасть в меню со всеми настройками AVG. Здесь можно получить доступ ко всем упоминавшимся настройкам и к тем, о которых речи еще не было.

9. Обновление и интеграция

При помощи модуля **Update Manager** (меню **Components**), можно определить настройки обновления AVG Free Edition. Обновление может быть запущено при каждой перезагрузке компьютера или вручную. При этом информация о ходе выполнения операции может отображаться или не отображаться на экране.

AVG Free Edition **интегрируется в систему** и может быть вызван также через **контекстное меню**. Вы можете выбрать объекты для быстрой проверки, после чего запустить их сканирование. Большим достоинством программы является **высокая скорость работы**, сканирование файлов и папок происходит очень быстро. При этом, **на производительность** операционной системы процесс выявления вирусов практически никак **не влияет**.

В целом антивирус AVG Free Edition прекрасно **подходит для домашних пользователей** ПК. Программа нетребовательна к системным ресурсам, проста в настройке и, к тому же, бесплатна. AVG работает достаточно стабильно, **конфликтов с другими приложениями пока замечено не было**.

Желающие попробовать этот антивирусный пакет могут скачать его с официального сайта: http://free.avg.com/download?prd=afe

Заключение

Итак, учитывая полную бесплатность программы и ее весьма работоспособный функционал, AVG Free Edition составляет серьезную конкуренцию даже своим бесплатным «коллегам». Скачать дистрибутив можно на сайте бесплатного ПО: http://www.bestfree.ru/soft/sec/antivirus.php#AVGAntiVirusFree .

P.S. Отличным дополнением для AVG может стать программа-антишпион **Spyware Terminator.** Ее описание и дистрибутив можно найти здесь: http://www.bestfree.ru/soft/sec/antitroyan.php#SpywareTerminator

Также, возможно, Вас заинтересует еще одна антивирусная программа, но уже полностью на русском языке **Avast**: http://www.avast.com (сайт производителя)