Павшим в борьбе с вирусами ПК,
посвящается

И снова здравствуйте! Вот ведь как получается, когда у меня на руках были все козыри, жизнь начала неожиданно играть в шахматы... Вот эта неожиданность и привела к тому, что цикл статей превратился в перестроечный долгострой :) Но теперь, вроде как, всё устаканилось и долгострой сдвинулся с места. Туда ему и дорога :)

И так, начнём. Я долго думал, что рассмотреть в этот раз. Решение пришло неожиданно — **Avira Antivir.** Последнее время этот антивирус стал очень популярным среди пользователей, оно то и понятно почему. Avira есть в платном и бесплатном варианте. К чести Avira, следует заметить, что несмотря на базовый функционал, бесплатный вариант работает весьма и весьма неплохо. Конечно, холивары на тему «какой антивирус круче» очень интересное занятие, но не предмет обсуждения в этот раз :)

Сайт, на котором живёт Avira, отзывается на http://free-av.com/ :) Смело идём на этот сайт и смотрим раздел Products. Что же нам предлагают? А предлагают нам следующее:

- **Avira AntiVir Personal - FREE Antivirus**
- **Avira AntiVir Premium**
- **Avira Premium Security Suite**

Нас интересуют первые два продукта, ибо третий это уже не антивирус в чистом виде, а мега-комбайн, который убирает пшеницу, кукурузу, копает картошку и кондиционирует воздух :) Давайте посмотрим, чем отличаются все три продукта друг от друга (информация взята с официального сайта Avira):

Функции	Personal	Premium	Security Suite
Защита от вирусов, червей, троянов	*	*	*
Защита от диалеров (дозвонщиков)	*	*	*
Обнаружение и удаление руткитов	*	*	*
Защита от фишинга	*	*	*
Защита от spyware		*	*
Защита электронной почты (POP3, SMTP)		*	*
Быстрое обновление через Premium Server		*	*
Защита от раздражающего adware		*	*
Вэб-антивирус (проверка трафика)		*	*
Создание «спасательного» диска		*	*
Брандмауэр			*
Антиспам и проактивный антифишинг			*
Игровой режим (специальный режим работы брандмауэра)			*
Возможность создания резервной копии данных			*

Для начала возьмём **Avira AntiVir Personal - FREE Antivirus.** Сразу стоит сделать оговорку, лицензионным соглашением предусматривается, что данная версия антивируса будет использоваться на домашних ПК. Использование этого продукта в коммерческих целях -запрещено!

Системные требования

- Процессор, минимум, Pentium 133 MHz
- Операционная система:
  - Microsoft Windows Vista (32 or 64 Bit) or
  - Microsoft Windows XP Home or Professional, (SP2 рекомендуется)
  - Microsoft Windows 2000, (SP 4 рекомендуется)

Avira AntiVir Personal также поддерживает Microsoft Windows XP x64 Edition и 64 Bit Microsoft Windows Vista.

- Не меньше 192 MB RAM при работе в Windows 2000/XP

- Не меньше 512 MB RAM при работе в Windows Vista
- 30 MB свободного места на HDD (больше, если использовать карантин)
- 100 MB свободного места на HDD для временных файлов
- Для установки Avira AntiVir Personal под Windows NT, 2000 и XP требуются права администратора.

Цена: бесплатно.

Интерфейс: англоязычный.

Документация (формат pdf, на англ. Языке)

Загрузить **Avira AntiVir Personal** можно здесь (21,28Mb).

После того как мы скачали пакет, можно приступать у его установке (зачем то же мы его качали?). Вначале покажется окно с кратким пояснением, что сейчас произойдёт. После того, как мы его внимательно прочтём, обязательно жмём кнопку **Accept** (ну, можно и **Decline,** если Вам что-то не понравилось), после чего пакет начнет распаковываться. После распаковки, появится ещё одно окно. Окно полностью бессмысленное и поздравляет нас с началом установки антивируса (хорошо, что салют не устраивают в честь такого события). Жмём кнопку **Далее** как можно быстрее ибо поздравления это скучно. И, о Боже!!, мы опять не приступаем к установке антивируса. Появляется ещё одно окно с кратким пояснением (на английском) для чего предназначена данная версия антивируса и клятва о том, что Avira ляжет костями, но защитит наш ПК от заразы, умрёт, но не пропустит :) Ради интереса можно почитать, но лучше не заморачиваться и жать кнопку **Далее**. И наконец-то появляется окно с лицензионным соглашением. Лицензионное соглашение это всегда интересно, ибо именно из этого соглашения можно узнать, какие страшные кары ждут нас за нарушение авторских прав и других пунктов этого соглашения, а также, что компания-производитель не несёт абсолютно никакой ответственности за последствия работы своего продукта. То есть, если вдруг антивирус сотрёт все файлы на жёстком диске, спалит видеокарту и убьёт Кенни, то претензии предъявить можно будет только в небесную канцелярию. Ну, что ж поделать, оно так всегда. Поставим галочку возле «I accept тра-ля-ля...» и нажмём кнопку **Далее**. (рис.1)

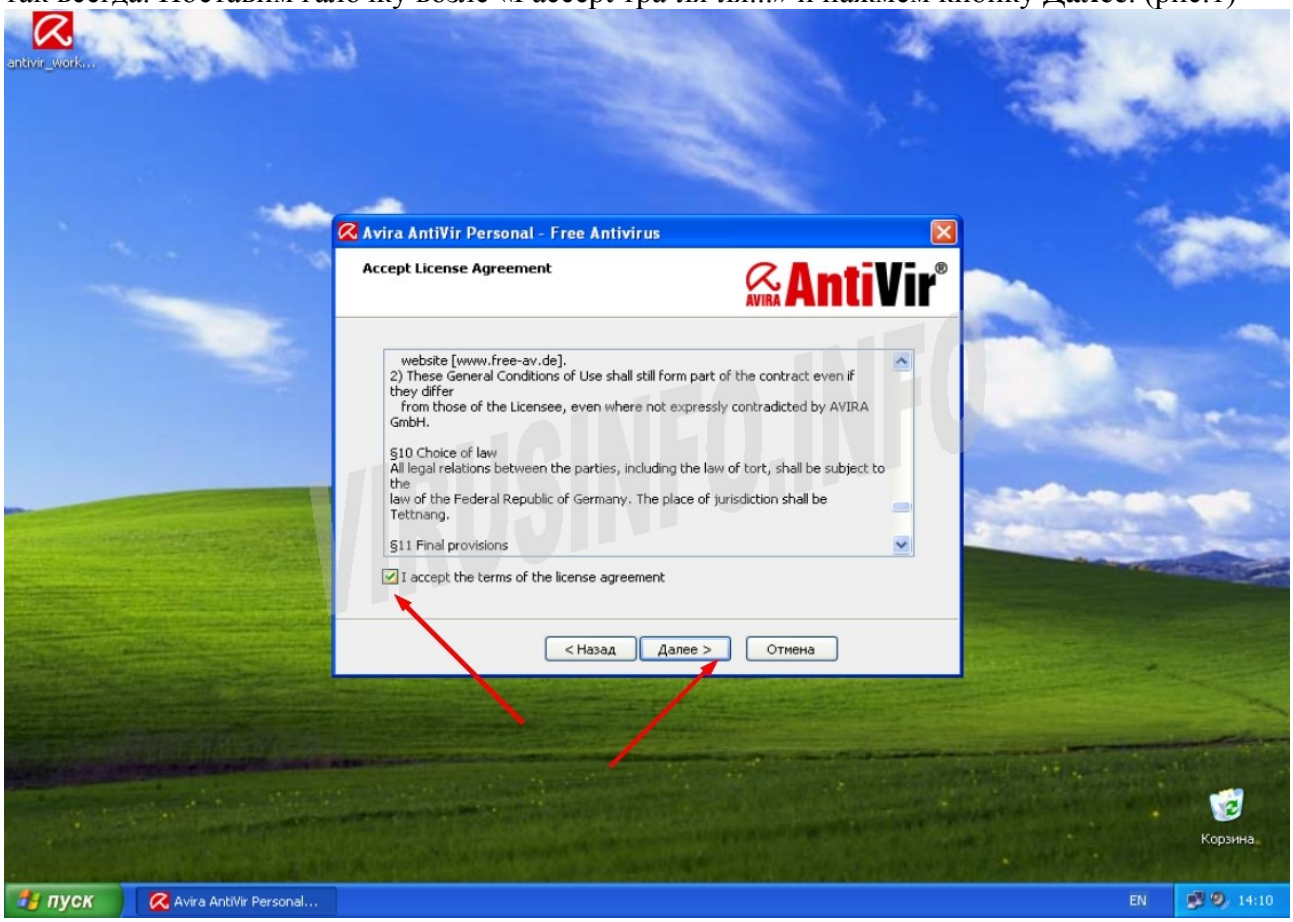

Рис.1

После этого появляется ещё одно окно (рис.2), в котором уточняется, действительно ли мы будем использовать этот продукт только дома, не планируем ли мы его использовать в коммерческих целях, не планируем ли мы отобрать честные трудовые копейки у разработчиков, не диссиденты ли мы, не вкушали мы кукурузу? :) Отвечаем честно, крест на пузе ставим, а заодно с крестом ставим галочку возле «I accept тра-ля-ля...» и нажмём кнопку **Далее**. (рис.2)

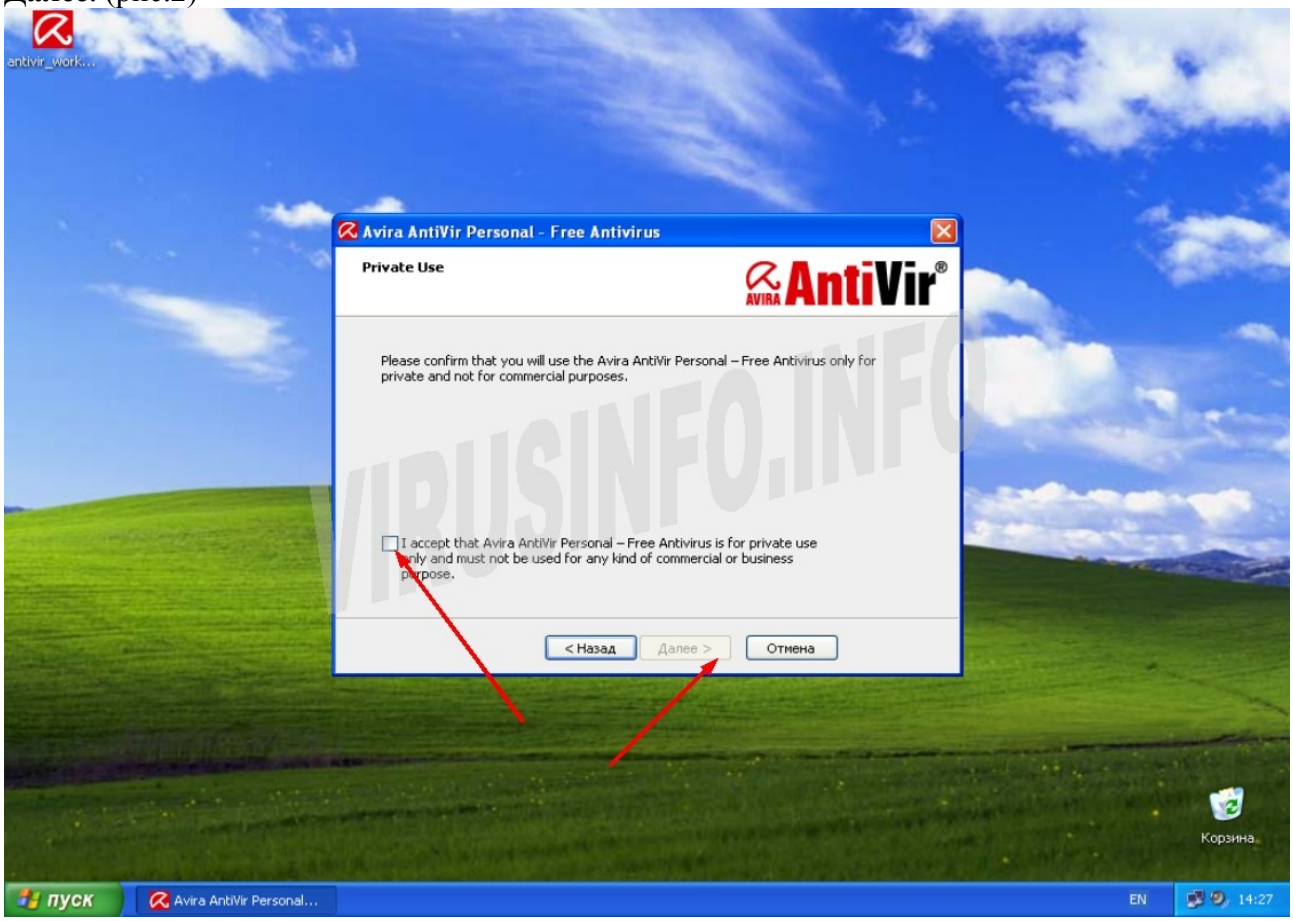

Рис.2

В следующем окне нам нужно нажать лишь кнопку **Далее.** Поясню в чём тут скрытый смысл. В этом окне сообщается о том, что для использования антивируса нам нужен серийный номер, хоть продукт и бесплатный. Также в этом окне есть тыцочка с установленной галочкой, возле которой написано «Сгенерировать серийный номер и передать его во время обновления». Получается, что Avira сама сгенерирует серийный номер и передаст его во время обновления на сервер. Так что нам беспокоиться не надо, всё будет сделано автоматически.

Обратим внимание на следующее окно (рис.3)

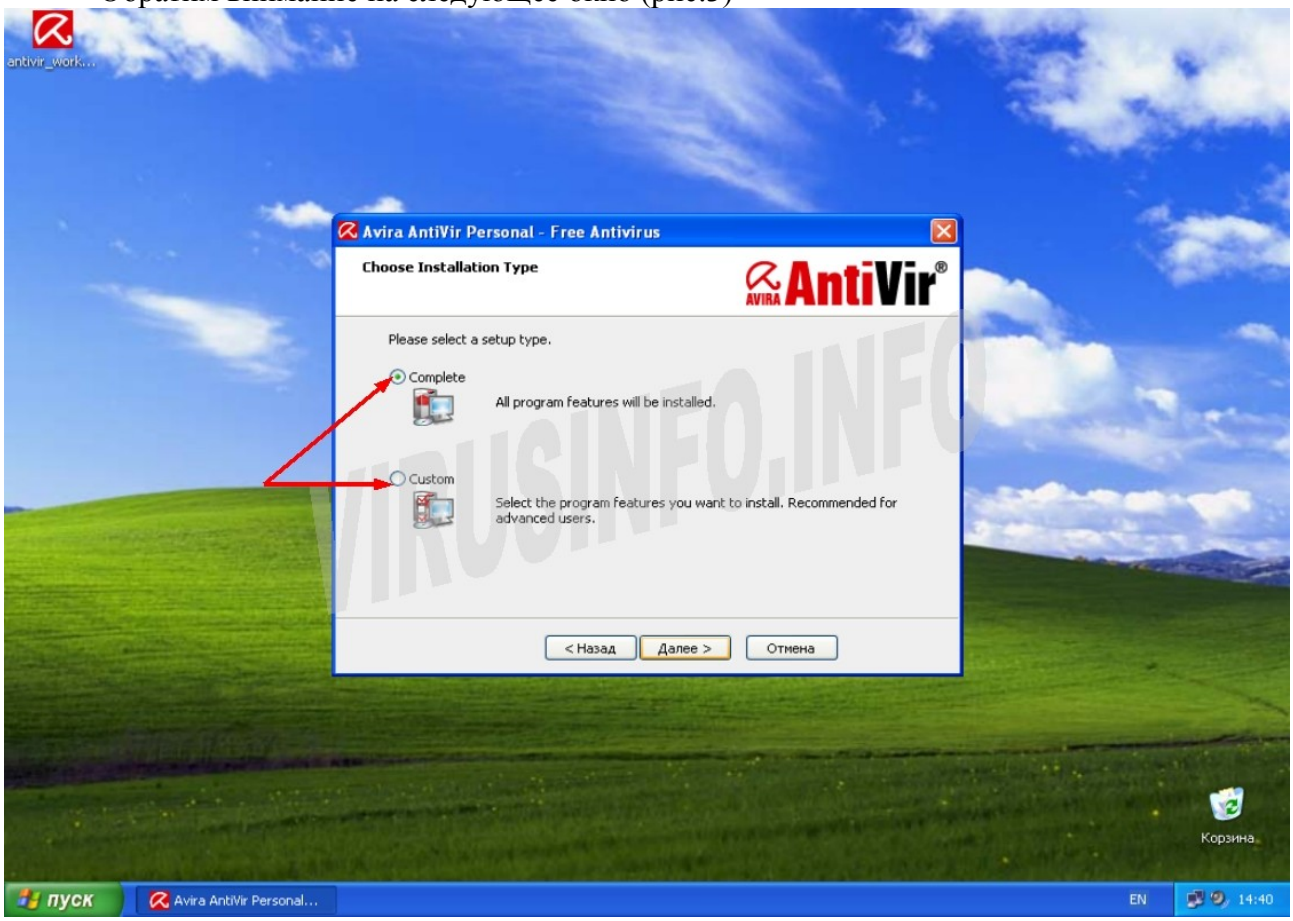

Рис.3

В этом окне нам предлагают 2 варианта установки: **Complete** (полный) и **Custom** (выборочный). Естественно же мы выбираем **Custom**, ведь мы же крутые пользователи, нам всё интересно и познавательно. :)

После принятия волевого решения выбрать **Custom** и нажатия кнопки далее, нам предлагают выбрать, куда мы будем ставить антивирус. (рис.4)

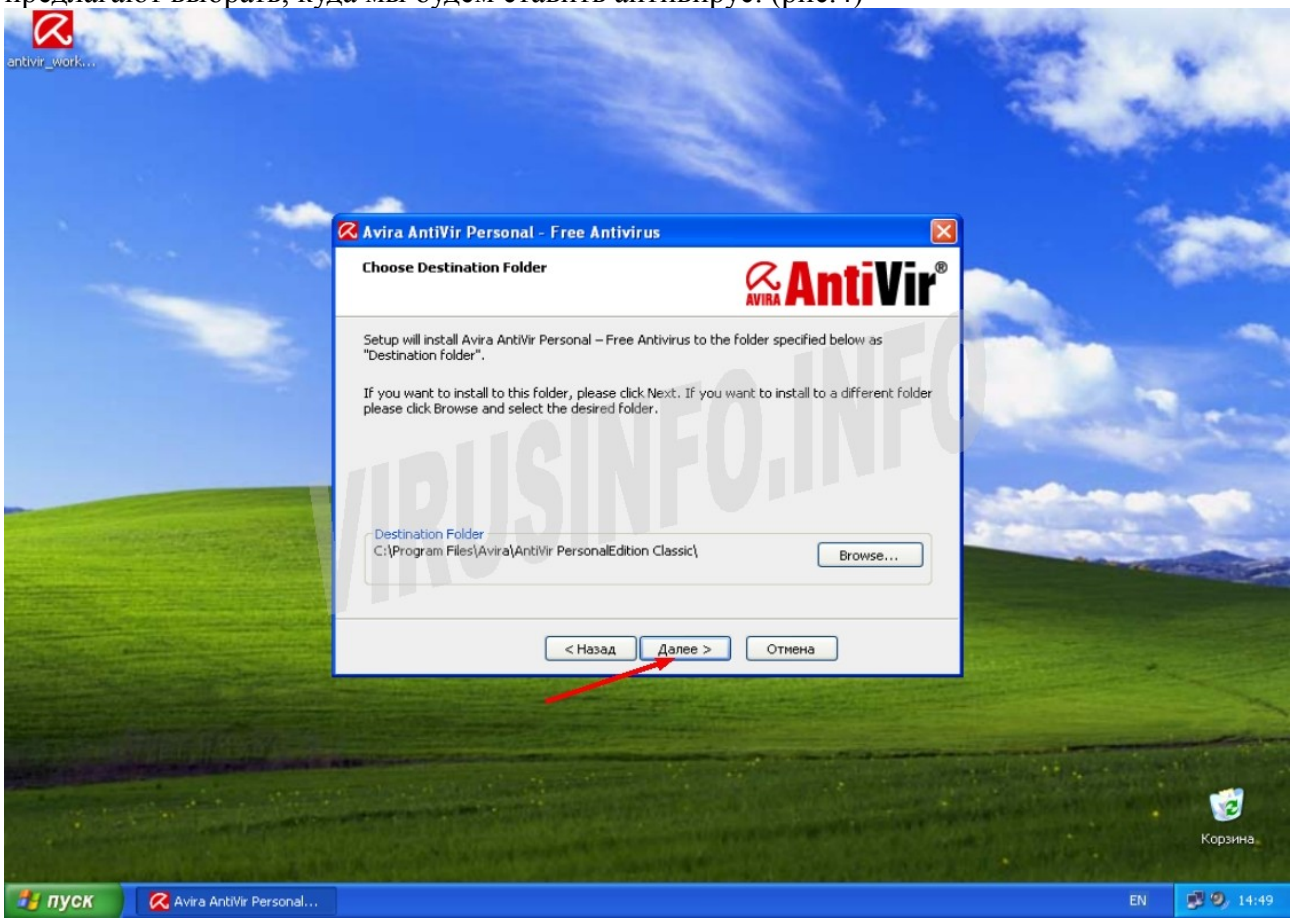

Рис.4

Согласно идеологии компании Microsoft и операционной системы Windows, все программы должны жить в одной большой дружной стране под названием Program Files. Так это всё дело и оставим, ибо программы, отделённые от своих собратьев, начинают скучать, болеть и умирать :) Соглашаемся с предложенным путём установки и жмём кнопку **Далее.**

В следующем окне (рис.5) выбрать компоненты антивируса, которые мы будем устанавливать.

Рис.5

Поясню для чего нужен тот или иной компонент:

- **Avira Antivir Personal** — Ядро антивируса. Отказаться от его установки нельзя, ибо это равносильно отмене установки вообще.
- **Antivir Guard** — Резидентный монитор, который оберегает наш ПК в реальном времени. От его установки можно отказаться в том случае, если Вы хотите установить Avira, как второй антивирус, который будет использоваться для проверки подозрительных файлов в том случае, если основной антивирус не обнаружил ничего, а Вы всё ещё сомневаетесь в надёжности файла. Если же Вы устанавливаете Avira как основной антивирус, то я крайне настоятельно рекомендую устанавливать этот компонент.
- **Antivir Rootkit Detection** — Модуль поиска руткитов. Тоже очень нужный компонент. Обязательно устанавливаем. На данный момент руткиты получили очень широкое распространение и борьба с ними это очень серьёзный и острый вопрос.
- **Shell Extension** — Если включен этот компонент, то в контекстное меню проводника добавляется пункт «Scan with Avira», весьма удобное расширение меню проводника. Оставляем включенным.

Жмём кнопку **Далее** и смотрим, что нам предлагают дальше (рис.6). А дальше нам предлагают включать или нет эвристический анализатор (1) и если да, то насколько подозрительным он должен быть (2). Вкратце поясню что такое эвристика. **Эвристика** – механизм, который позволяет антивирусу обнаруживать новые не известные ему вирусы. За эту возможность мы расплачиваемся небольшой частью производительности системы, но поверьте, оно стоит этого. Дело в том, что без эвристического анализатора, антивирус может обнаружить лишь тот вирус, сигнатура которого занесена в его базу. А для того чтобы сигнатура появилась в базе, образец вируса должен попасть вирусным аналитикам под

микроскоп. Но ведь может быть такая ситуация, что прежде чем вирус попадёт аналитикам, он может попасть на Ваш компьютер. В таком случае эвристический анализатор может спасти Вас. Естественно, что эвристикой мы не отловим все неизвестные вирусы, но в качестве дополнительной защиты это средство выгодно. Уровень эвристики определяет, насколько подозрительным будет антивирус. Если уровень минимальный, то эвристический анализатор сможет обнаружить лишь очень простых зверюк, которых не знает антивирус, а работа на максимальном уровне будет напоминать придирчивость полковника КГБ в отставке, который работает на проходной режимного предприятия, конечно, это повысит уровень обнаружения заразы, но одновременно с этим и повысит кол-во ложных срабатываний. Хотя уровень ложных срабатываний зависит от разработчиков антивируса. Есть некоторые антивирусы, которые на максимальной защите будут ругаться на всё, что можно, но толку от этого 0.

Итак, посмотрим на рис.6

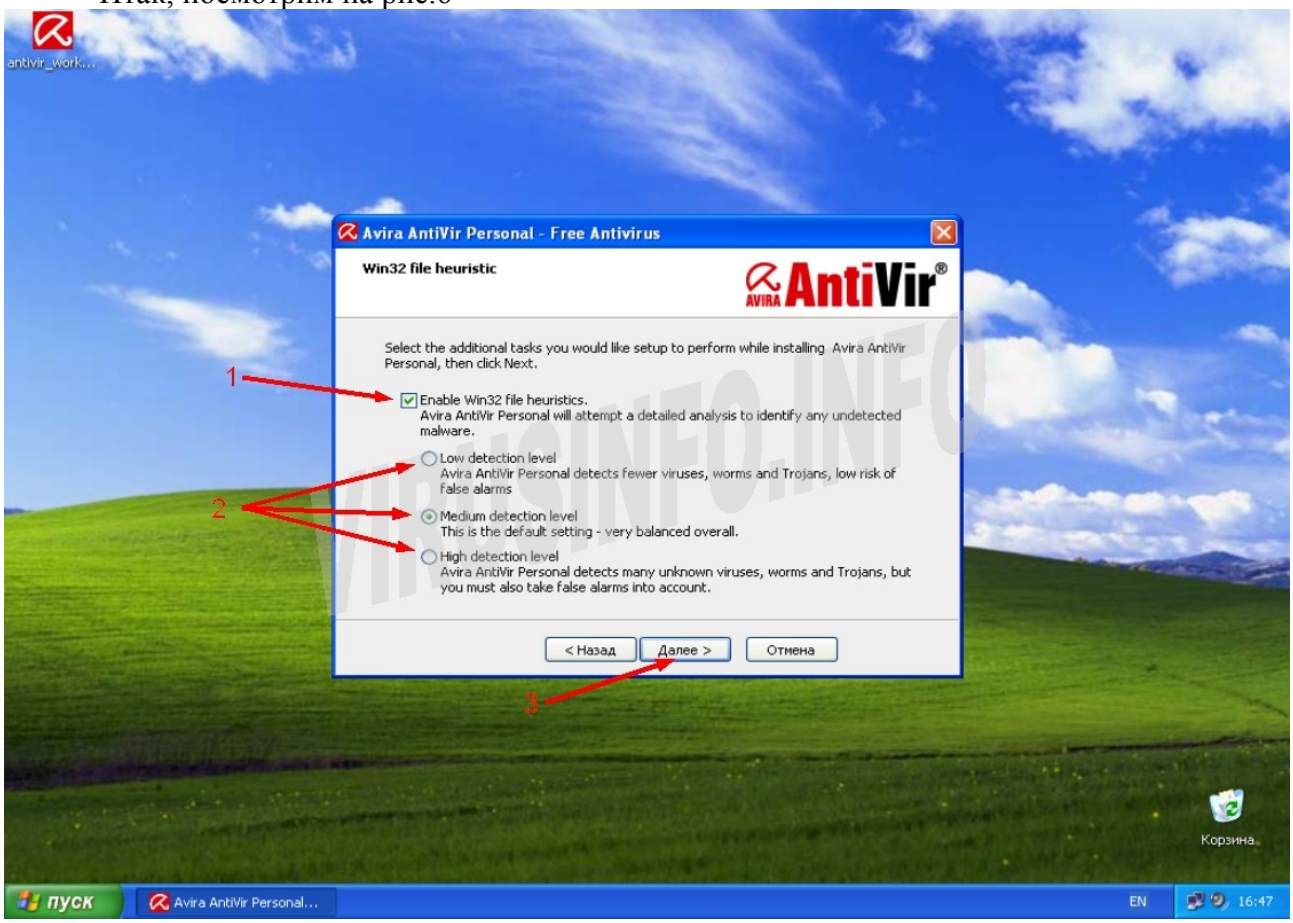

Рис.6

Нам предлагают три уровня работы эвристического анализатора: **Low** (низкий), **Medium** (средний), **High** (высокий). Какой же выбрать? Я советую включать высокий уровень. Почему? Потому что в современном мире замечательно действует принцип «сначала стреляй, потом разбирайся». Но в этом случае Вы должны более внимательно смотреть на какие файлы будет ругаться антивирус. Последнее — жмём на кнопку **Далее**. (3)

В следующем окне ничего интересного, по умолчанию предлагают создать ярлыки на рабочем столе и в меню «Пуск». Жмём **Далее** и не заморачиваемся. И вот оно, идёт установка антивируса :)

Финальный результат :) (рис.7)

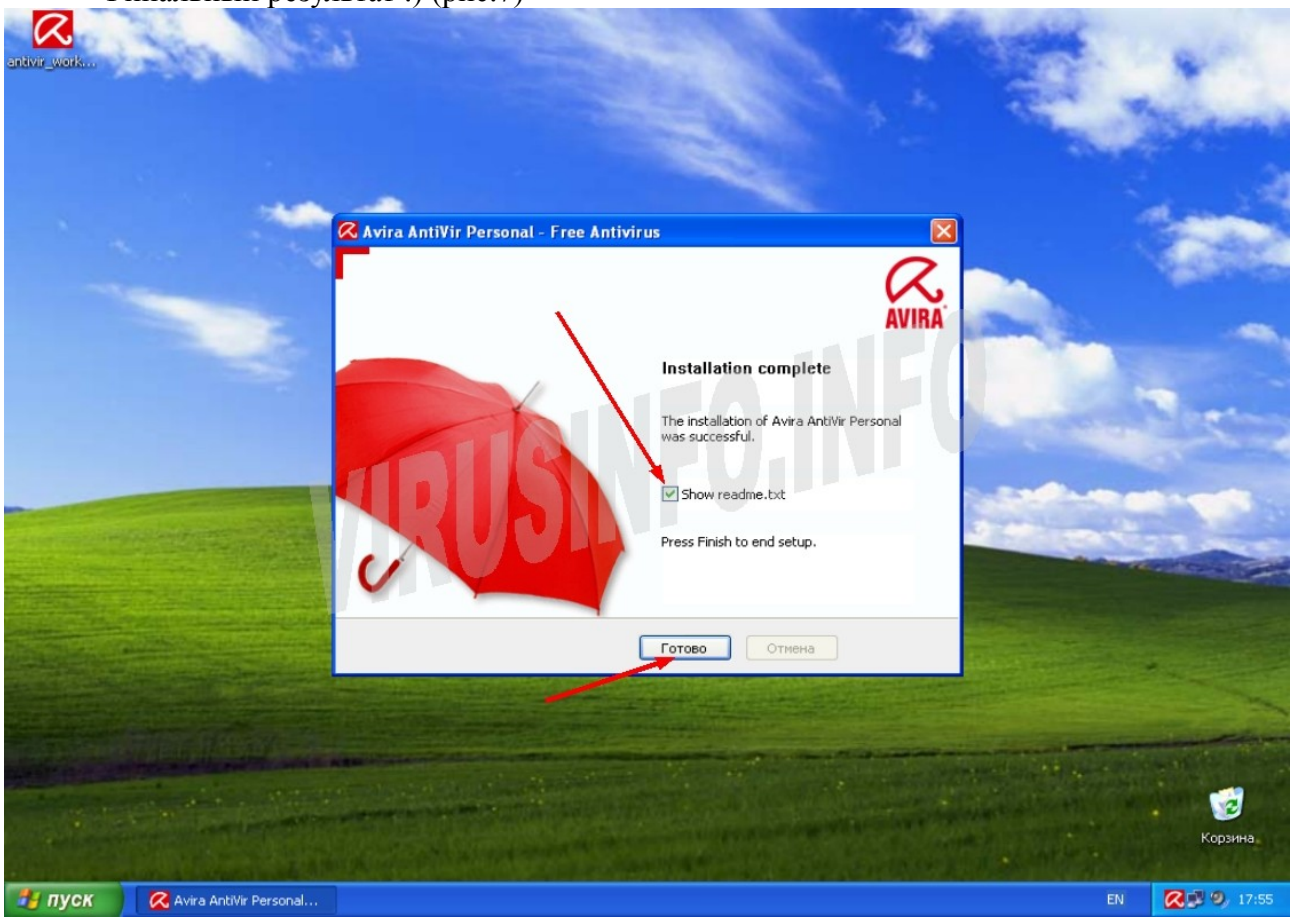

Рис.7

Убираем галочку с readme.txt (конечно, быть может Вы хотите почитать этот файл, тогда оставляйте эту галочку. Лично я эти файлы читать не люблю) и жмём кнопку **Готово.**

У нас спросят, хотим ли мы обновить антивирус? (рис.8)

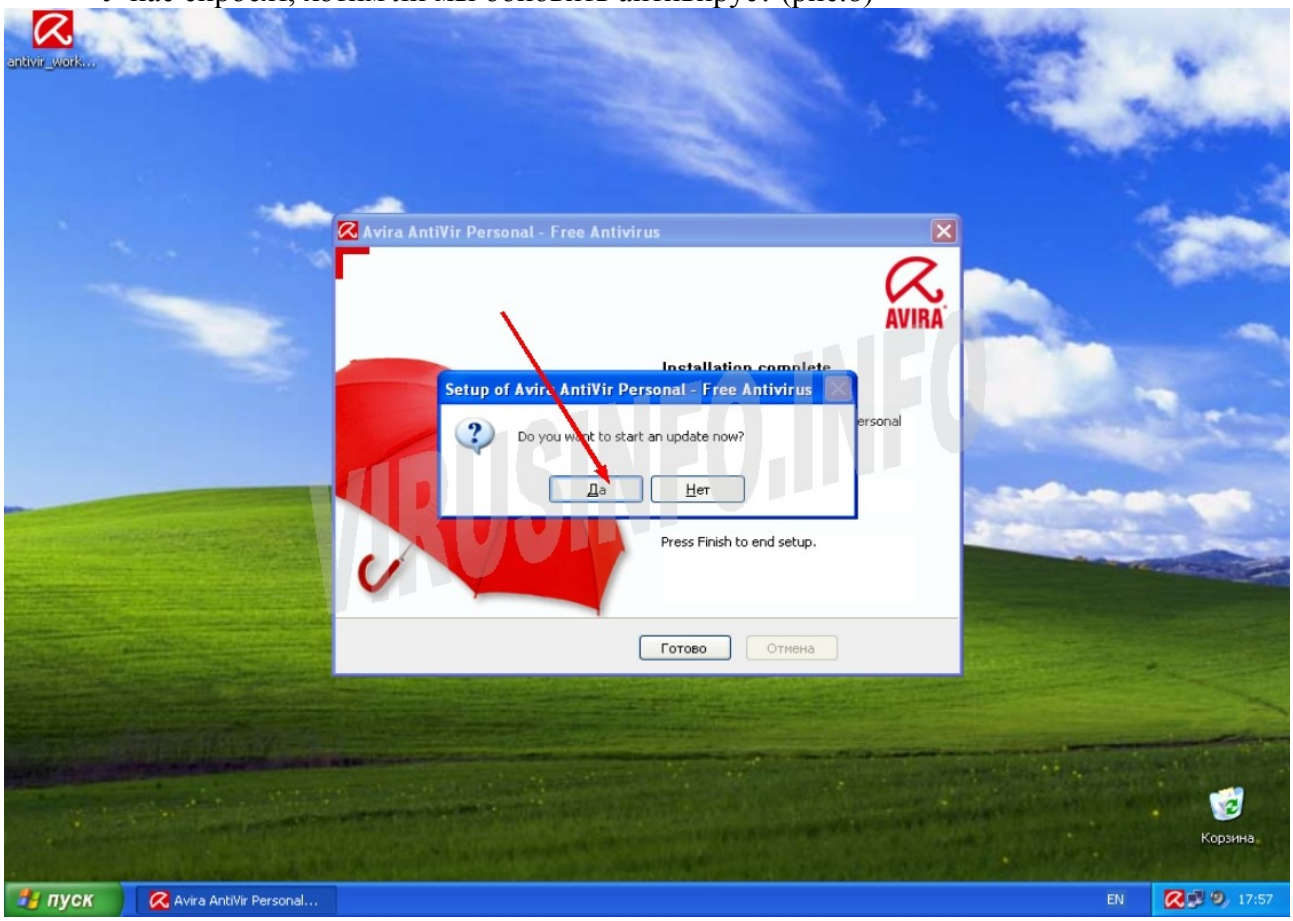

Рис.8

Обязательно отвечаем **Да**, своевременно обновлённый антивирус хорошая гарантия безопасности. Подождём, пока обновиться антивирус. По окончанию обновления, будет произведён перезапуск антивируса, поэтому в настройки ломиться сейчас нет смысла :) ***Если у Вас вдруг Авира не смогла соединиться с сетью, то посмотрите сюда и почитайте (там пара страниц про настройки доступа в сеть)***

Ну что же, антивирус обновился и готов к настройке, но прежде чем перейти к описанию настроек я расскажу про небольшой минус **Avira Personal**. Дело вот в чём, поскольку версия бесплатная, то есть реклама. При каждом обновлении, показывается окно с рекламой других продуктов Avira. Выглядит оно примерно так, как на рис.9

Рис.9

Окно надоедливое ибо при появлении все полнооконные приложения свернутся, но иногда в этом окошке бывают прикольные картинки: мужики в масках и с фомками, которые лезут к компьютеру, руки тянущиеся из розетки и прочие комиксы. Придётся смириться с этим окошком. Жмём ОК и забываем про него до следующего обновления.

Как видно на последнем скриншоте, в системном лотке появился красный значок с белым зонтиком. Если зонтик открыт, значит антивирусный монитор запущен, если зонтик закрыт — значит антивирусный монитор не работает. Кстати, старожилы должны помнить, что подобный зонтик показывался на заставке при старте антивируса Касперского 3-ей версии :)

Давайте щёлкнем на этом значке правой кнопкой мыши и посмотрим, что есть в открывшемся меню (рис.10):

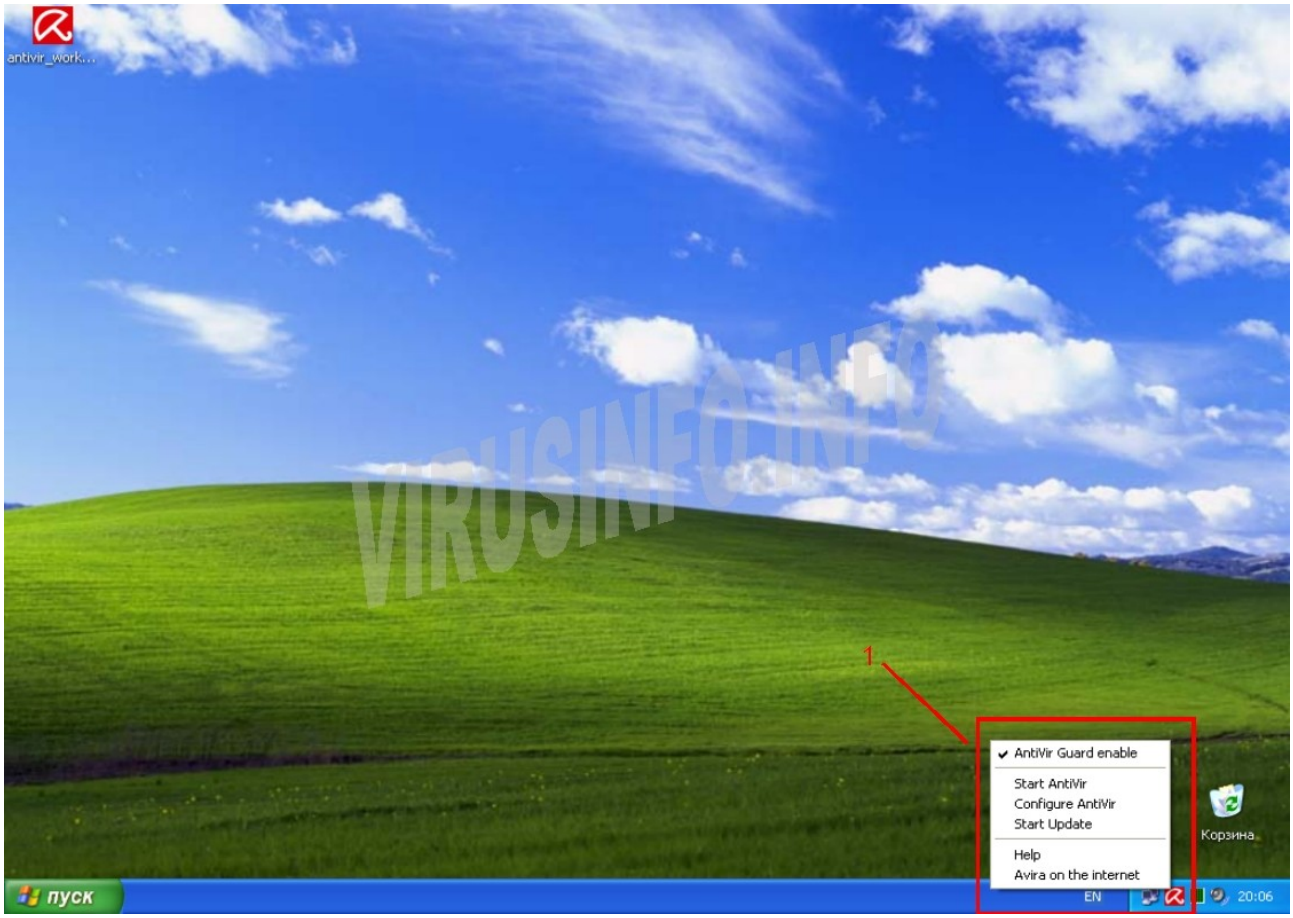

Рис.10

Итак, что мы видим (1) (начнём сверху вниз):

- **Antivir Guard enable** — Если возле этой надписи стоит галочка, то это значит, что антивирусный монитор работает. Щёлкая по этой надписи, можно включать/отключать резидентную защиту.
- **Start AntiVir** — Если щёлкнуть по этой надписи, то откроется главное окно антивируса (равносильно двойному щелчку левой кнопкой мыши по значку с зонтиком)
- **Configure Antivir** — Ну, это понятно, нажав на эту надпись, мы попадём в меню настроек антивируса.
- **Start Update** — Всё коротко и ясно, начать обновление
- **Help** — Хэлп, хэлп! Ну, помощь значит :)
- **Avira on the internet** — щёлкнув по этой надписи, мы перейдём на официальный сайт Avira.

Прежде чем перейдём к настройкам, давайте посмотрим на главное окно программы, для этого нажимаем **Start AntiVir** или делаем двойной щелчок левой кнопкой мыши по значку с зонтиком. Смотрим на рис.11

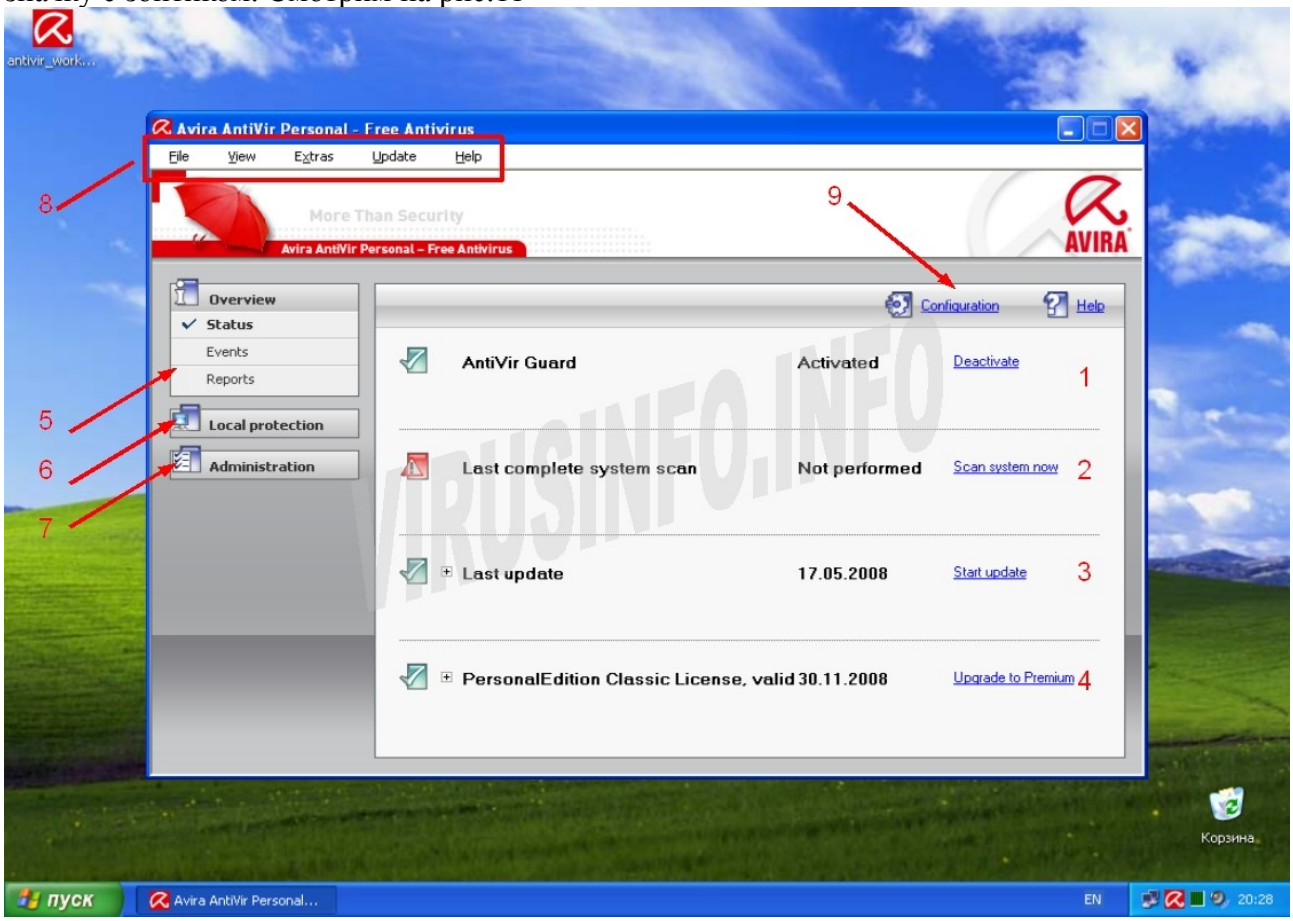

Рис.11

Давайте рассмотрим всё по-порядку.

- В строке (1) отображается статус **Avira Antivir**. Сейчас антивирус запущен, о чём свидетельствует зелёный цвет значка и слово **Activated**. Антивирус можно отключить, нажав на **Deactivate**.
- Строка (2) сразу заметна красным значком с восклицательным знаком. Возле значка написано «**Last complete system scan**» (Последнее полное исследование системы) и «**Not Perfomed**» (Не выполнено). Если нажать на **Scan system now**, то будет проведена полная проверка системы (все локальные и съёмные диски).
- Строка (3). Судя по значку, здесь всё в порядке. В этой строке отображается состояние обновлений. На скриншоте видно, что последнее обновление было выполнено 17.05.2008. (дата, естественно, может быть другой) Если нажать на **Start Update**, то будет выполнено обновление антивируса.
- В строке (4) отображается информация о сроке окончания лицензии. Как видно, лицензия действительна до 30 ноября 2008. Но не стоит переживать о том, что будет, когда наступит эта дата. За 4 недели до часа X, лицензия будет продлена автоматически. Надпись **Upgrade to Premium** ведёт на официальный сайт, где можно купить и скачать **Avira AntiVir Premium.**
- Меню **Overview** (5) это информационное меню. В нём можно посмотреть **Status** (это то, что мы только что детально разобрали). **Events** (журнал событий) — в этот журнал заносятся результаты выполнения запланированных заданий, информация о выполненных обновлениях, результатах сканирования различных объектов и протокол работы антивирусного монитора. Как это выглядит, можно посмотреть на рис.12

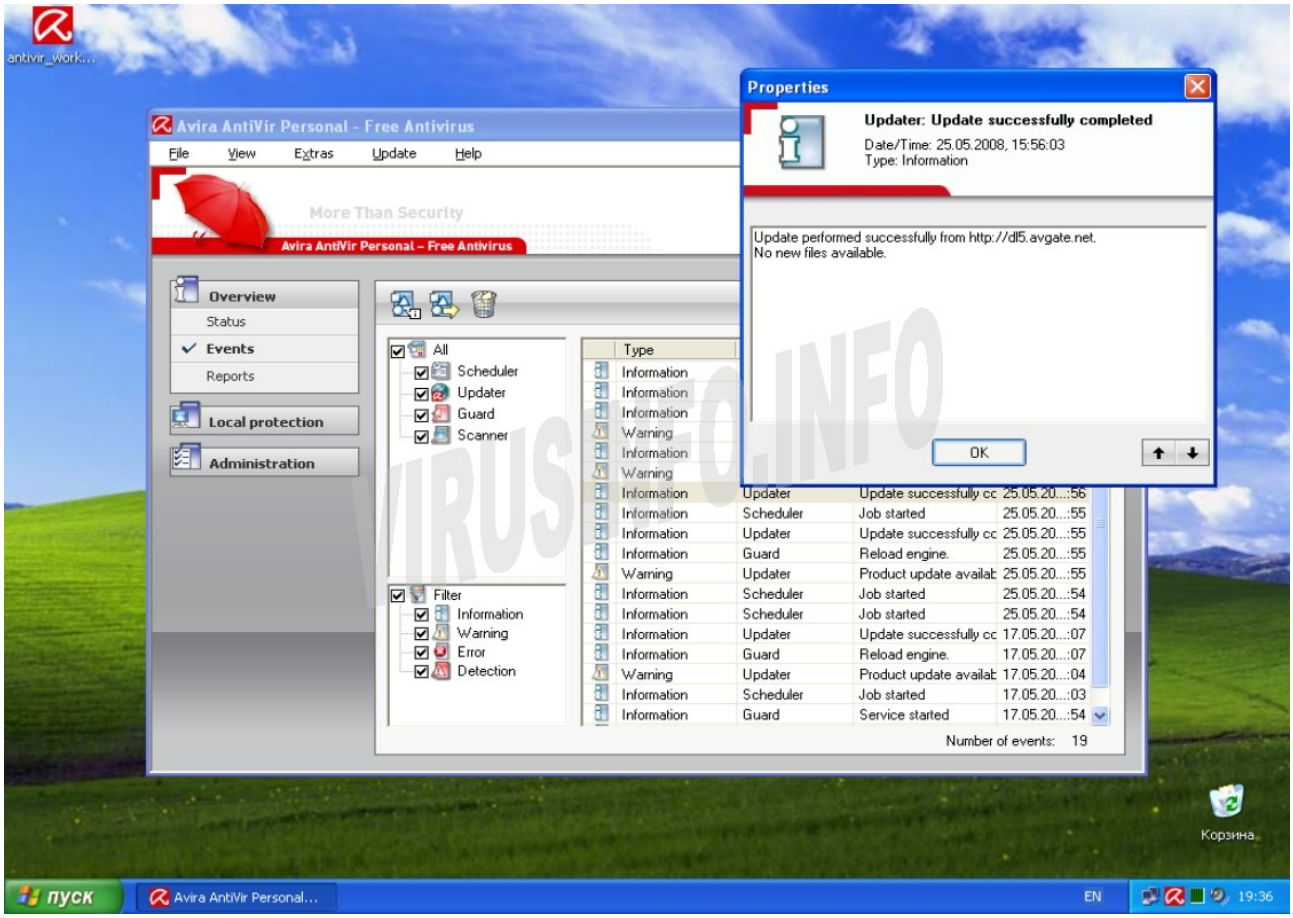

Рис.12

Кроме **Events** есть ещё и **Reports** (отчёты). Если в журнал событий заносятся записи с общей информацией, то раздел **Reports** содержит детальную информацию о выполненном действии. Пример такого отчёта виден на рис.13

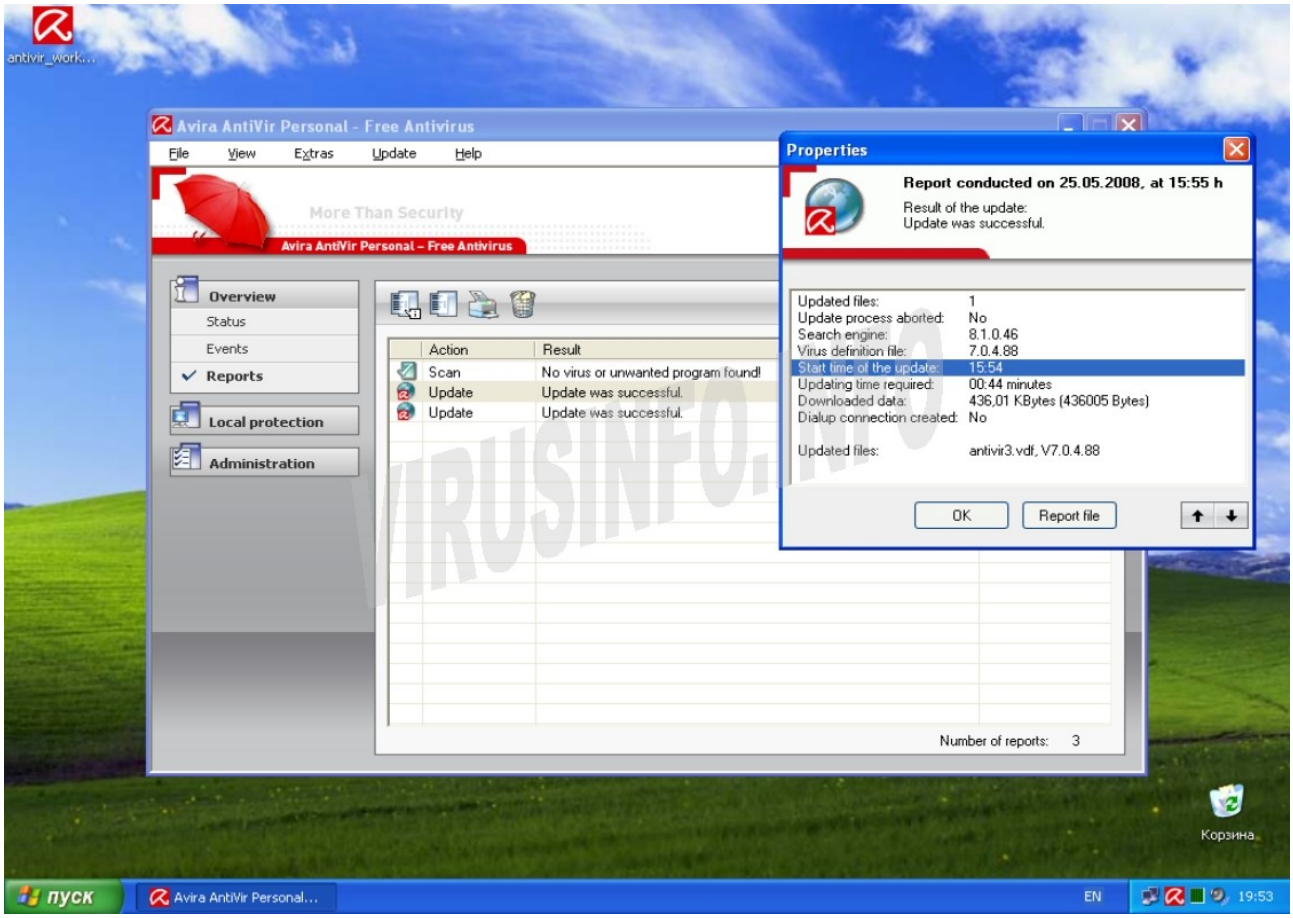

Рис.13

- Меню «**Local protection**» (6) (мы и далее рассматриваем рис.11). В этом меню есть два раздела: **Scanner** и **Guard**. В разделе **Scanner** предоставлен список (1) готовых профилей сканирования различных областей системы (рис,14):
  - **Local Drives** (Локальные носители) — Проверка всех жёстких дисков, флоппи-приводов, CD/DVD приводов, флэшек и т.п.
  - **Local Hard Disks** (Локальные жёсткие диски) — проверка всех жёстких дисков.
  - **Removable Drives** (Съёмные диски) — проверка флоппи-приводов, CD/DVD приводов, флэшек и т.п.
  - **Windows System Directory** - Проверка папки C:\Windows\System32.
  - **Complete System Scan** (Полная проверка системы) — Ну полная проверка, есть полная проверка :)
  - **My Documents** - Я думаю и так понятно, что это проверка папки «Мои документы»
  - **Active Processes** (Запущенные процессы) — проверка запущенных процессов
  - **Rootkit Search** - Проверка выбранных объектов на присутствие руткитов.
  - **Manual Selection** (Ручной выбор) — Проверка выбранных объектов. К примеру можно выбрать диски C:, E:, I.

Выбрав нужный профиль, нажимаем кнопку **Start scan with the selected profiles** (запустить сканирование с выбранным профилем) (2) рис.14

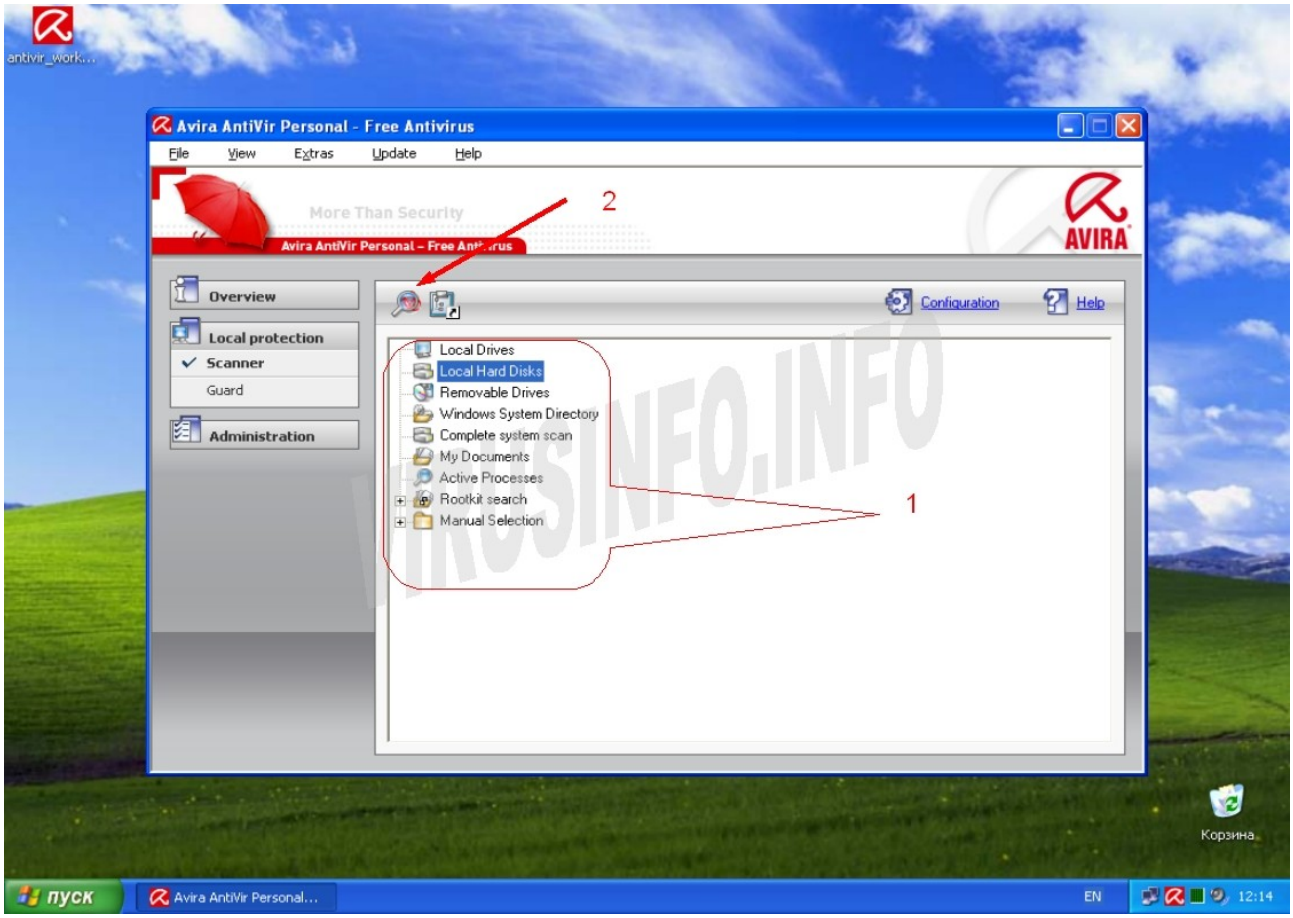

Рис.14

В разделе **Guard** меню **Local Protection** отображается путь к последнему зараженному файлу, название последнего обнаруженного вируса, последний проверенный файл и общая статистика работы антивирусного монитора. К тому же, есть интересная фича. Возле названия последнего обнаруженного вируса есть ссылка **Virus Information**, нажав на которую, можно посмотреть детальную информацию о найденной зверюке (если есть подключение к Интернет и если в базе есть описание этого вируса). Описания доступны на нескольких языках, в т.ч. и на русском. Пример можно посмотреть на рис.15

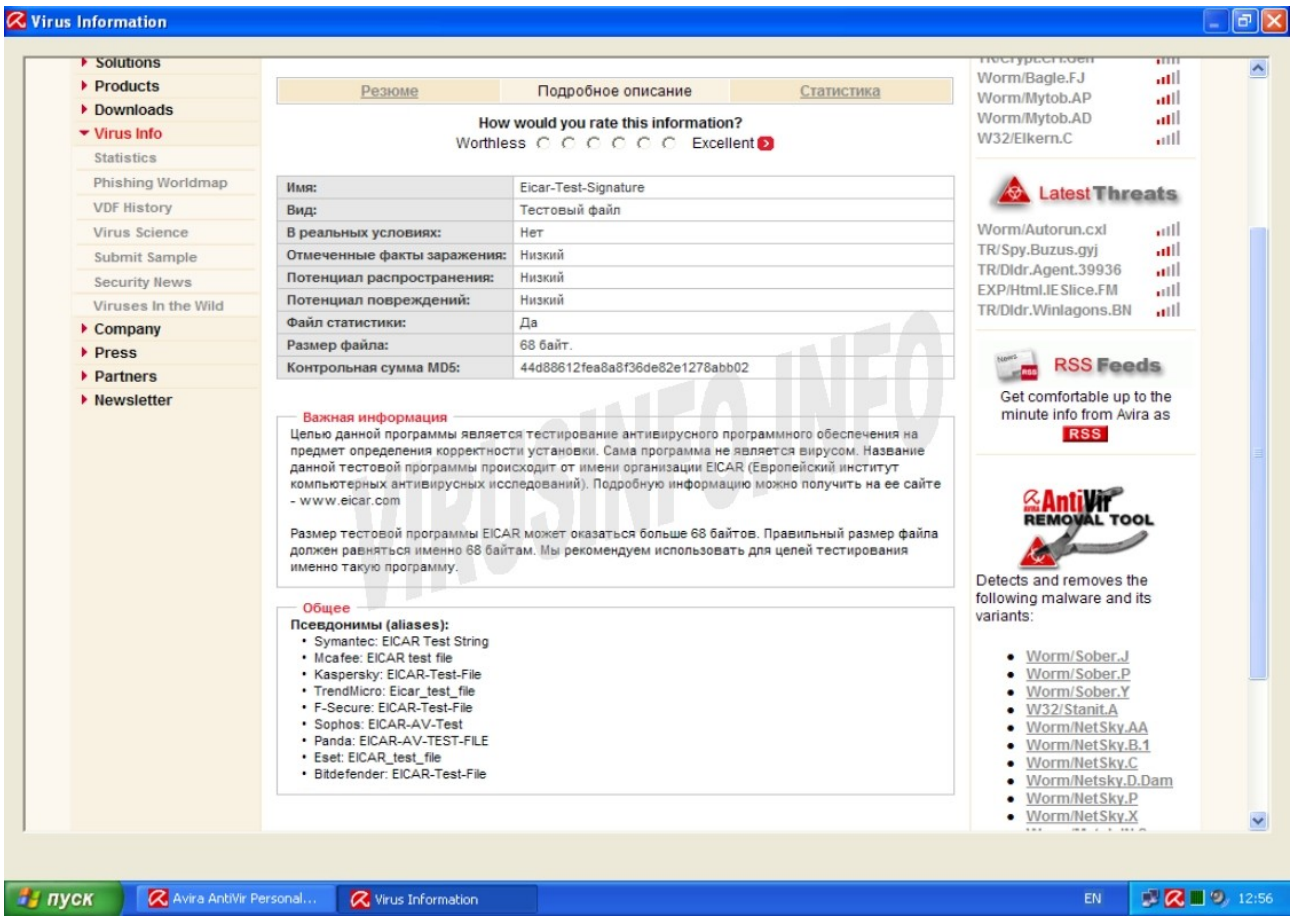

Рис.15

- Меню **Administration** (7) рис.11 содержит в себе два раздела: **Quarantine** (карантин) и **Sheduler** (планировщик). Карантин, это особая папка. Данные, помещенные на карантин, хранятся в закодированном виде, что препятствует запуску исполняемого кода и гарантирует стопроцентную безопасность от заражения. В карантин можно помещать файлы и вручную. Необходимость в этом может возникнуть и в том случае, если Вы подозреваете, что файл заражен. При помещении файла на карантин, файл удаляется из своего первоначального места хранения. Данные из карантина можно восстановить, что тоже весьма полезно. С объектами, которые находятся на карантине, можно проделать несколько операций. Для этого нужно на объекте щёлкнуть правой кнопкой мыши (в качестве примера смотрим рис.16)
    - **Rescan Object** — Пересканировать файл. Очень удобная опция. Во-первых, если антивирус сомневался в надёжности файла, а при очередном обновлении добавили сигнатуру этого вируса, то при повторным сканировании антивирус даст чёткое определение этому файлу. Во-вторых, если этот файл добавляли Вы, поскольку сомневались в его надёжности, то после каждого обновления, можно проверять этот файл.
    - **Restore Object** — Восстановить объект в начальное месторасположение. К примеру, если файл жил на рабочем столе, то восстановится он на рабочий стол.
    - **Delete Object** — Удалить объект. Ну, тут всё ясно :)
    - **Send Object** — Послать объект на исследование в антивирусную лабораторию. Очень полезная фича. Всегда бывает так, что антивирус не находит какую-то заразу. В этом случае мы кидаем зараженный файл в карантин и отправляем вирусным аналитикам. Если отправленный объект действительно вирус, то в ближайшее время сигнатуру добавят в

базы. А бывает так, что антивирус даёт ложное срабатывание на какой-то файл. В этом случае обязательно надо отправить образец аналитикам., дабы ложное срабатывание было устранено.

- **Restore Object to...** - Восстановить объект в месторасположение, отличное от первоначального. Бывает полезно в том случае, если Вы хотите собственноручно препарировать пойманного зверя :), а оставлять его, к примеру, на рабочем столе, опасно.
- **Add File** — Добавить файл в карантин.
- **Properties** — Свойства. Свойства они и в Африке свойства. Выбрав этот пункт, можно просмотреть детальную информацию об объекте.

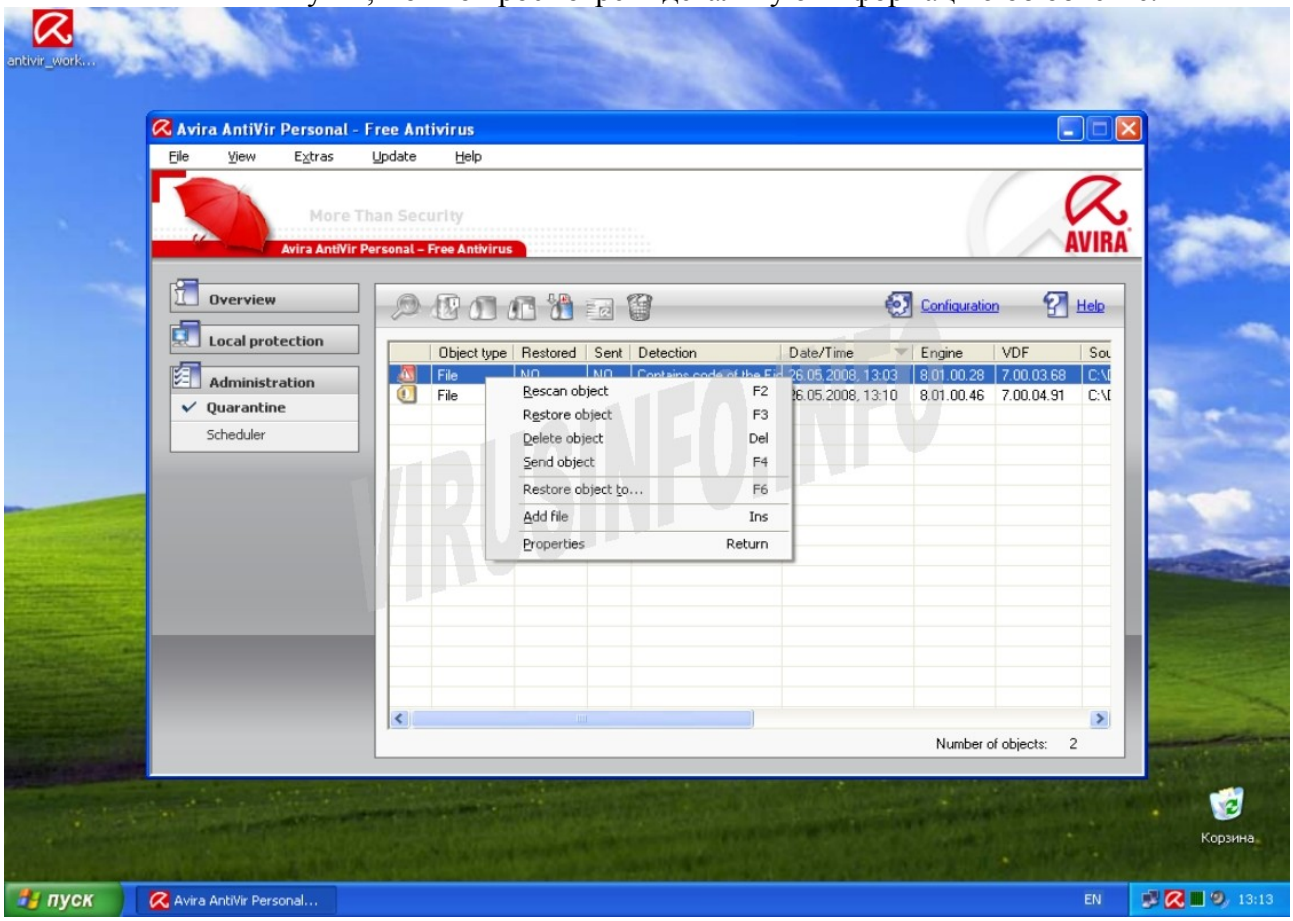

Рис.16

Раздел **Sheduler** (планировщик) предназначен для создания и управления запланированными заданиями. Есть два доступных вида заданий: задание обновления по расписанию и сканирование различных объектов (в зависимости от выбранного профиля) по расписанию.

Строка меню (8) рис.11 содержит в себе все те же самые меню, что и рассмотренные выше, но помимо них, есть ещё одна очень полезная функция, о которой я расскажу чуть позже. А сейчас приступим к подкрутке гаек, сбиванию костяшек пальцев и откручиванию приборной доски. Жмём заветную строку **Configuration** (конфигурирование) (9) рис.11 и вперёд под капот!!

Смотрим на рис.17, вот так выглядит окно конфигурирования антивируса.

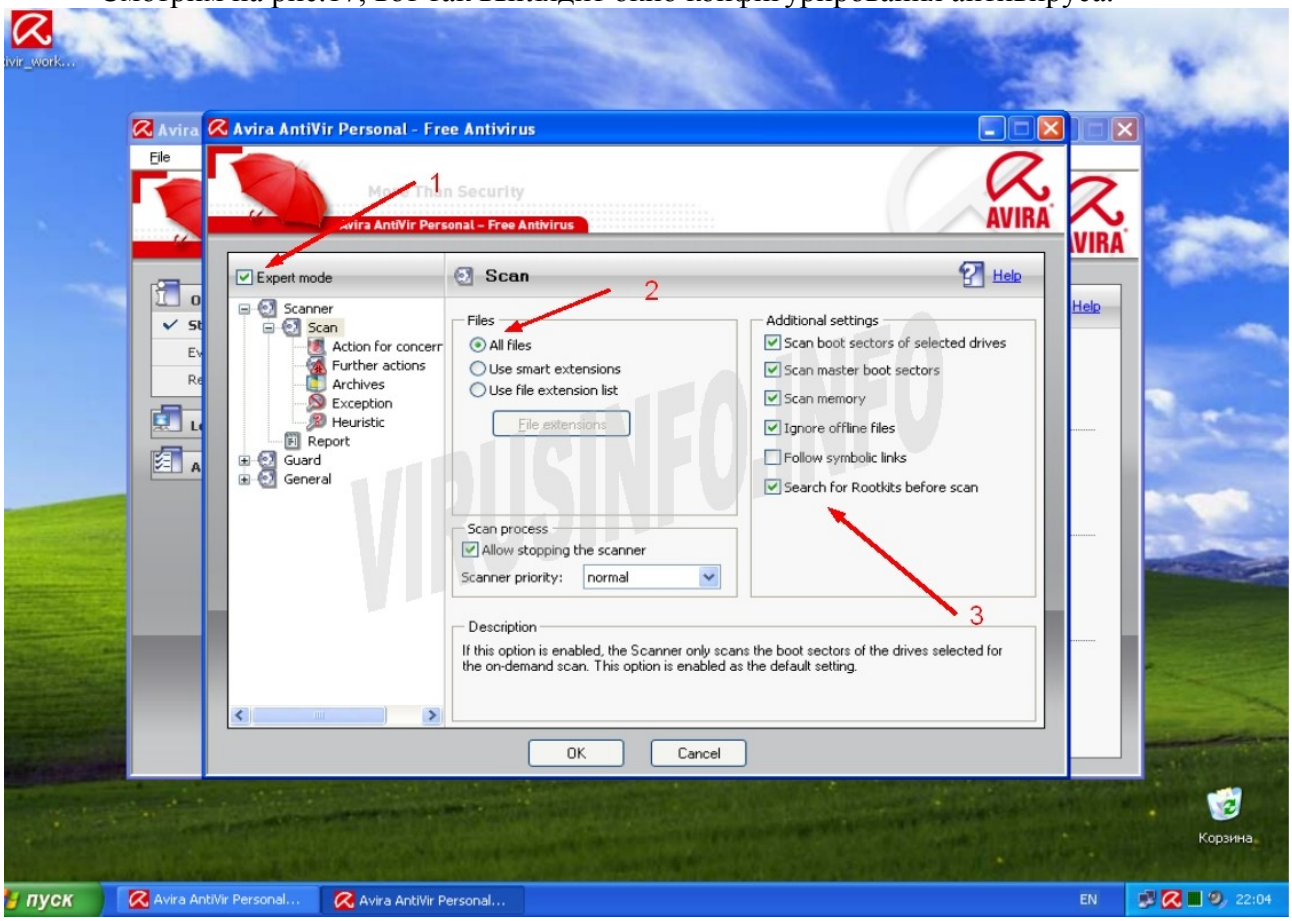

Рис.17

Сразу же ставим тыцку **Expert** (1). Слева видна деревовидная структура настроек. Основное это **Scan** (здесь находятся настройки сканера для проверки объектов по-требованию), **Guard** (эта группа настроек относится к антивирусному монитору) и **General** (общие, это довольно обширная группа настроек).

Начнём с первой группы настроек, которые относятся к сканеру. Обязательно ставим сканировать все файлы **All Files** (2), а в поле (3) ставим галочки так, как на скриншоте. Поясню, что каждая опция в поле (3) означает.

- **Scan boot sectors of selected drives** - Сканировать загрузочные сектора выбранных дисков. В загрузочных секторах могут быть вирусы, поэтому проверка этих мест отнюдь не лишняя.
- **Scan master boot sectors** - Сканировать главную загрузочную запись. Включение этой опции означает, что главная загрузочная запись будет проверена в любом случае, независимо от того, какой жёсткий диск был выбран.
- **Scan memory** - Сканировать оперативную память. При начале сканирования, сканер проверит оперативную память на наличие вирусов. Эта опция особенно актуальна, если Вы проводите сканирование при выключенном антивирусном мониторе.
- **Ignore offline files** - Не проверять автономные файлы. Включение этой опции запрещает прямое сканирование автономных файлов. Почитать об автономных файлах можно здесь. Эта опция включена по умолчанию. Оставляем её в таком же состоянии.
- **Follow symbolic links** - Следовать по ссылкам. Эта опция работает только на ОС Windows XP и Vista. По-умолчанию, она отключена. Её действия сводится к следующему: к примеру сканер проверяет диск C:, при проверке натыкается на ярлык, который указывает на файл, который находится на диске D:, сканер прочитает путь, указанный в ярлыке, и проверит этот файл. Смысл этой опции мне до конца не ясен, но время сканирования эта опция увеличит намного.
- **Search for Rootkits before scan** - Поиск руткитов перед сканированием. Рекомендую

включить эту опцию. Руткиты — это особый класс зловредов, они пытаются маскироваться от антивирусных и др. защитных программ всеми возможными способами. Поэтому, при этой включённой опции, сканер проведёт дополнительную проверку на наличие руткитов, чтобы в случае обнаружения суметь заблокировать работу руткита, нейтрализовать его и удалить все файлы, которые с ним связаны.

Идём дальше вниз по дереву настроек. Напоминаю, что мы сейчас рассматриваем подразделы, которые относятся к настройке ручного сканера (совсем ручной, даже не кусается :)).

Следующий подраздел — **Action for concerning files** (действия для обнаруженных зараженных файлов). Доступны 2 режима: **Interactive** (интерактивный) и **Automatic** (автоматический). Естественно, что сканер в интерактивном режиме будет задалбывать просьбами «Сделайте что-нибудь с этим файлом, ну пожалуйстаааа :)», а в автоматическом режим будет работать тихо и спокойно, пока не встретит файл, с которым он точно не будет знать, что делать. Я рекомендую переключить сканер в автоматический режим, но предварительно укажем, каким образом должен реагировать сканер на «плохие» файлы. Смотрим рис.18

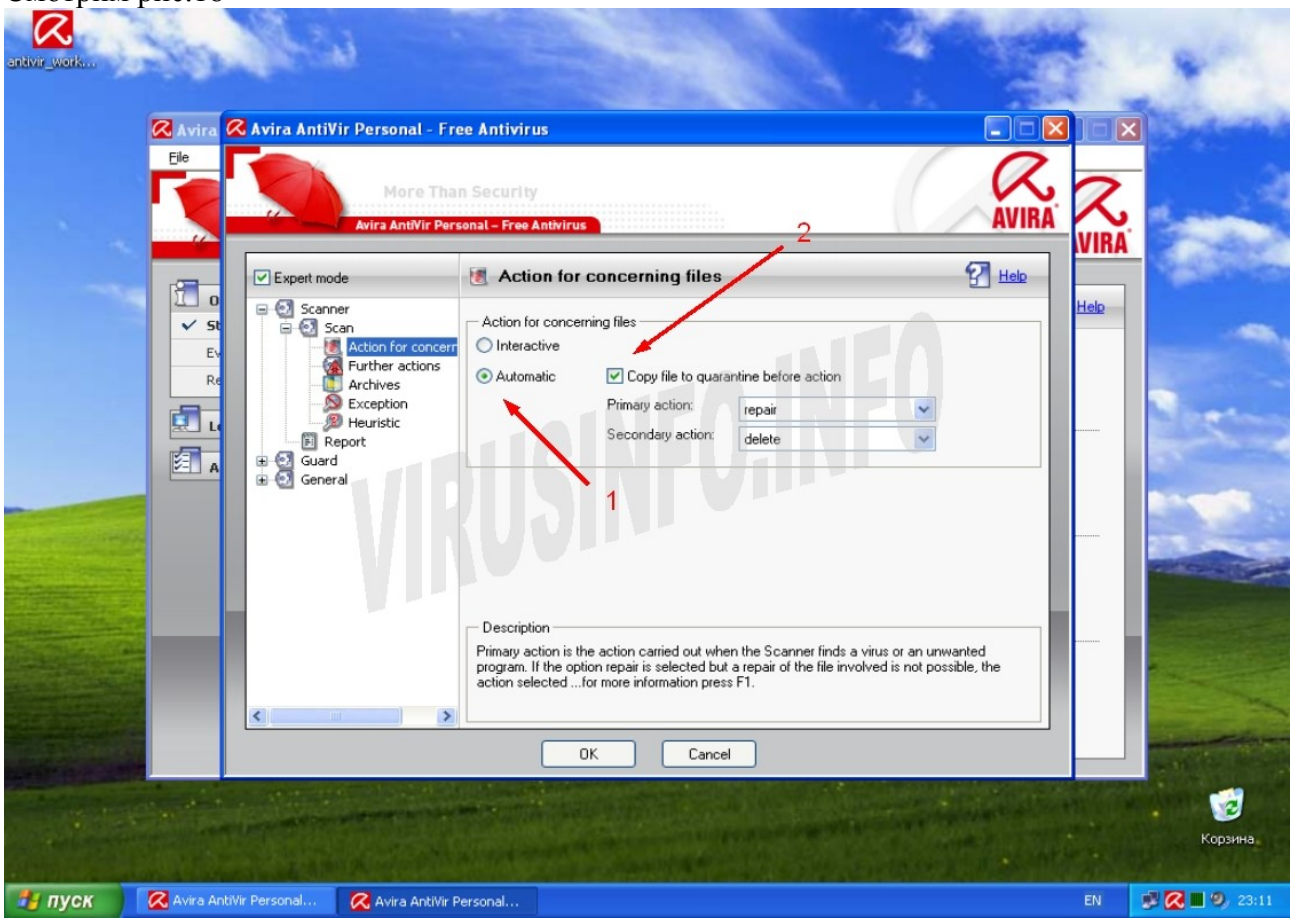

Рис.18

Переключаем в автоматический режим (1). (2) — обязательно указываем, чтобы файлы копировались в карантин перед любым действием, которое будет предпринято. Это очень полезная опция, не забудьте её включить. Видно, что есть первичное действие **Primary Action** и вторичное действие **Secondary Action**. Мы задаём первым действием «**лечение**» **Repair**, а вторым — «**удаление**» **Delete**. Для первичного действия доступны также варианты **Rename** (Переименовать), **Delete** (Удалить), **Ignore** (Игнорировать). А для вторичного действия доступны варианты (помимо **Delete**) **Ignore** и **Rename**. Если выбрать действие **Rename,** то антивирусный сканер переименует зараженный файл и это приведёт к тому, что, к примеру, запустить файл двойным щелчком мыши уже не получится. Это действие полезно в том случае, если файл заражен файловым вирусом, а алгоритм лечения ещё не добавлен в базы антивируса. В таком случае зараженный файл остаётся лежать до «лучших времён» и

как только антивирус сможет его вылечить, то можно будет вернуть файлу прежнее имя. Действия **Ignore** и **Delete** интуитивно понятны :) В первом случае антивирус просто-напросто пропустит этот файл, а во втором — беспощадно пристрелит. Действие **Repair** — я его поставил основным действием и вот почему. Антивирус может вылечить файл, если тот заражен, именно заражен, файловым вирусом. На данный момент файловые вирусы встречаются довольно редко, но встречаются, поэтому первичным действием надо ставить **Repair.**

Раздел **Further Actions** (Дальнейшие (другие?) действия, если я правильно перевёл). В этом разделе можно настроить какой звук будет издавать антивирусник при обнаружении заразы. ИМХО, опция для эстетов.

Следующий раздел — **Archives** (архивы). Если верить названию, то в этом разделе будет вестись речь о том, что сканер должен делать с архивами (проверять, не проверять и какие именно типы архивов проверять). Вдумчиво смотрим на рис. 19 и ищем знакомые буквы.

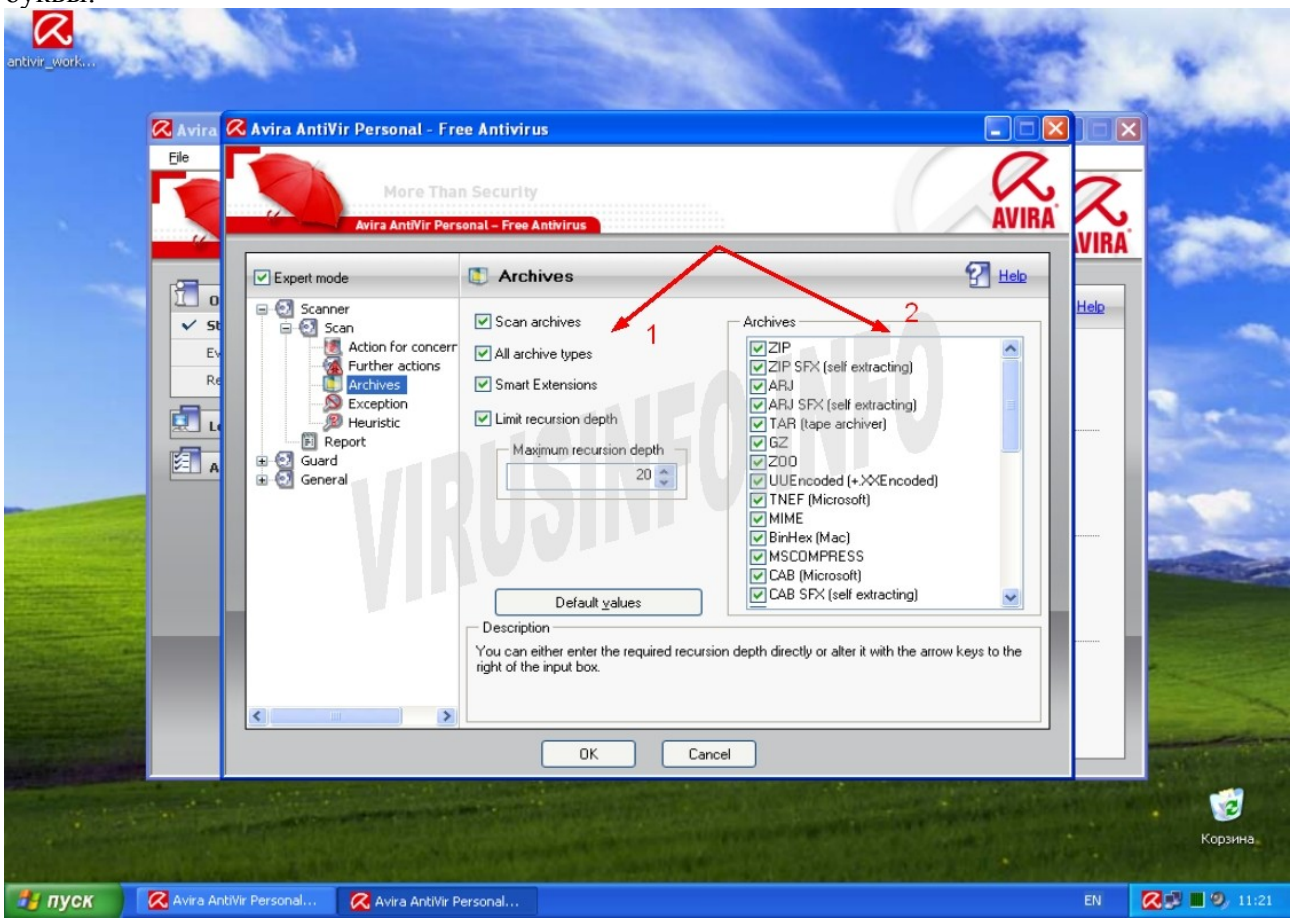

Рис. 19

Итак, смотрим в сторону 1. Я рекомендую, чтобы все галочки были выставлены. Кратко поясню назначение «этих гордых птыц»:

- **Scan archives** (проверять архивы) — Ну, тут, я думаю, всё понятно. Или проверять, или не проверять. Я рекомендую — проверять.
- **All archive types** (Все типы архивов) — Если мы посмотрим в сторону 2, мы увидим бааальшой список типов архивов, чего там только нет. Пусть сканер проверяет все типы архивов. Хуже от этого не будет.
- **Smart Extensions** (сканирование по содержимому) - Смысл этой опции в следующем: сканер будет определять (если включить эту опцию конечно) архив не по расширению, а по содержимому. То есть если zip-архиву сменить расширение с zip на ваоліоптіта, то умный сканер прочитает заголовок файла, определит, что это архив и проверит его. Во как! Так что эту опцию обязательно включаем.
- **Limit recursion depth** (ограничить глубину вложений) — Полезная опция,

обязательно включаем. Если обратите внимание на рисунок, то чуть ниже этой опции, есть счётчик и на нём число 20. Вот эта опция, указывает на как себя вести сканеру в ситуации «А за деревом — дерево...» То есть, если кому-то в голову придёт заархивировать файл, а потом этот архив ещё раз заархивировать, а потом ещё, ещё и ещё, и... Так, стоп, сканер максимум может обработать глубину в 99 вот таких вот перепакованых архивов. По умолчанию стоит значение 20. Его, ИМХО, и стоит оставить. (Хм, интересно, а что будет, если 99 раз перепаковать 700 метровый файл, типа кина и натравить на этот архив сканер? :))

Раздел **Exception** (Исключения) — Исключения, весьма полезная штука. Смысл в том, чтобы указать сканеру, какой файл или каталог не проверять. Частенько приходится пользоваться этой опцией. Простой пример. Я думаю многим известна программа Radmin, эта программа предназначена для удалённого управления ПК. Она может использоваться как в благих так и в злонамеренных целях. Если Вы используете эту программу, то Вам придётся добавлять её в исключения ибо она детектируется антивирусом . Как это сделать, смотрим на рис. 20

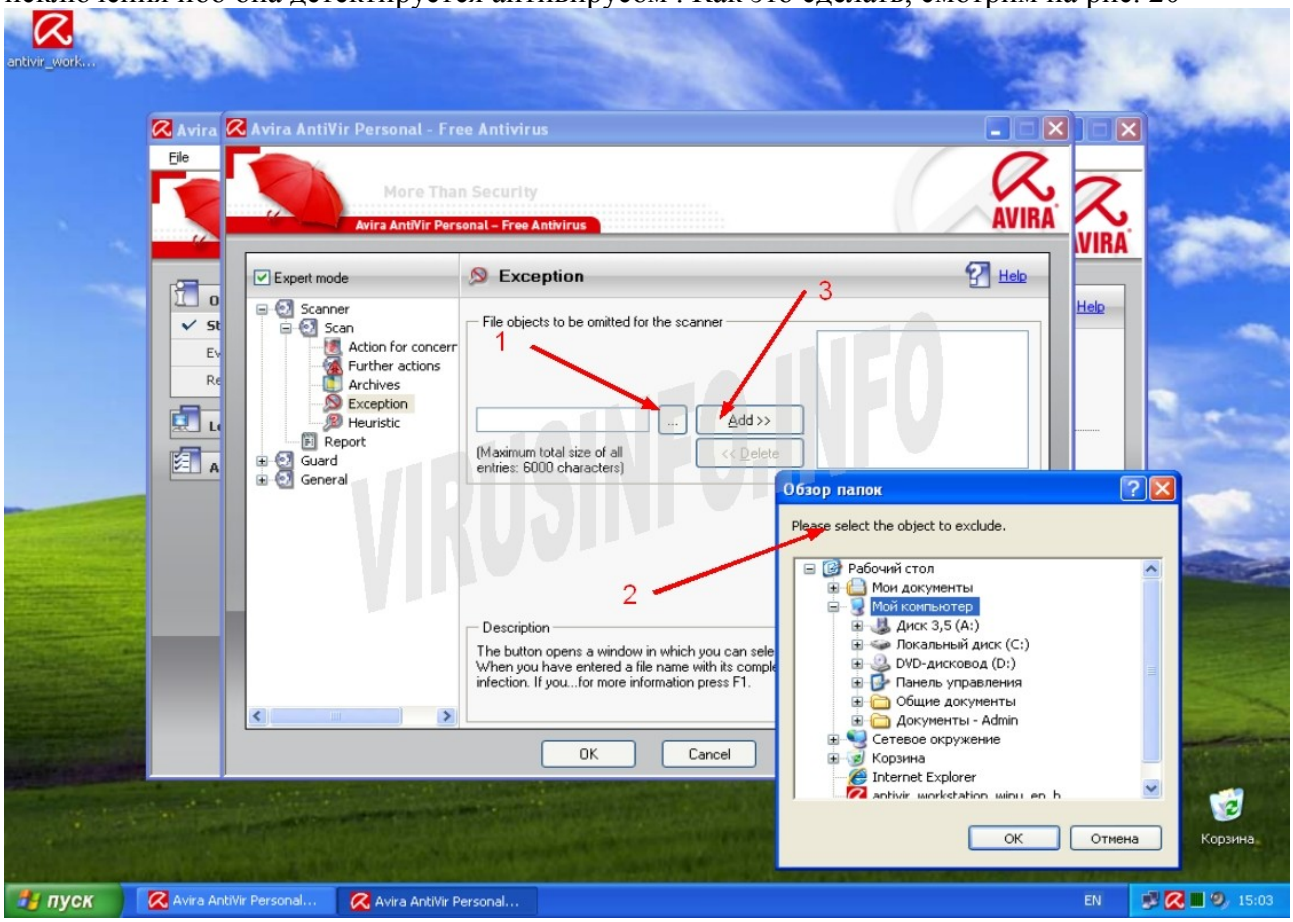

Рис. 20

Жмём на кнопку (1), откроется окно (2) в котором выберем нужную папку или файл, в этом же окне жмём ОК. После чего нажимаем кнопку **Add** (3). Вот и всё :) Всё просто.

Раздел **Heuristic** (Эвристика) — Что такое эвристика, я уже рассказывал вначале, когда мы начинали установку антивируса. Этот раздел посвящён настройке эвристического анализатора. Давайте посмотрим на рис. 21

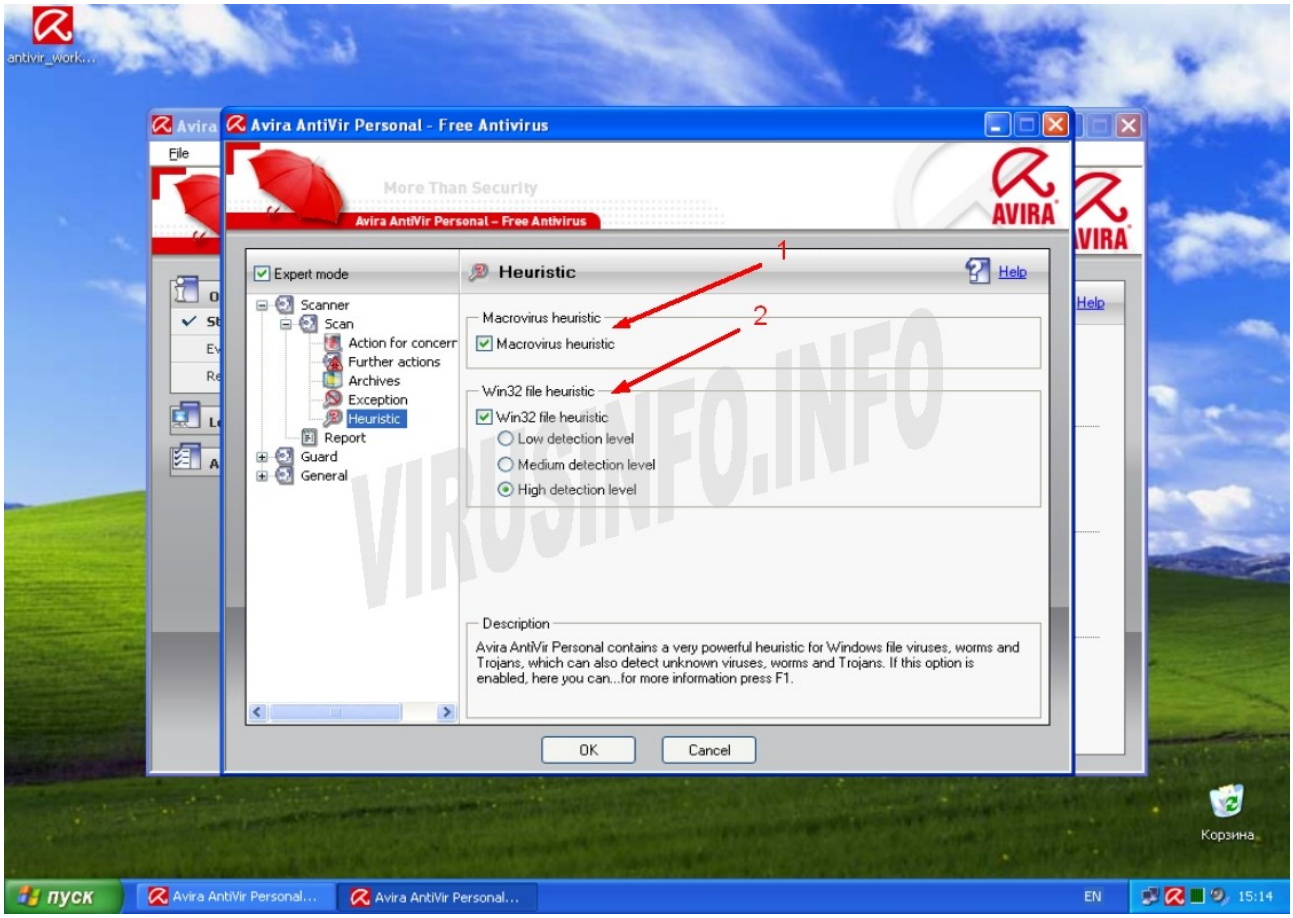

Рис. 21

Macrovirus heuristic (макровирусная эвристика) (1) — Если эта опция включена (а я рекомендую включить эту опцию), то будет идти проверка макросов в документах. Вредоносные макросы будут удаляться, а о подозрительных будет выдано предупреждение.

Win32 File Heuristic (2) — Это то, о чём мы уже говорили. Здесь можно порулить тремя уровнями эвристического анализатора, либо отключить его вообще. Я сторонник максимального уровня эвристического анализатора, как говорится «лучше перебдеть, чем недобдеть» :) Если же Вас не устроит повышенное кол-во ложных срабатываний, то поставьте уровень **Medium**.

Последний раздел — **Report** (отчёт). Тут ничего сложного. Отчёт можно отключить (**Off**), оставить по умолчанию (**Default**), расширенный (**Extended**), полный (**Complete**). Тут можете оставить по умолчанию или выбрать тот режим, какой Вам хочется.

Это мы сейчас настраивали ручной сканер. Теперь перейдём к следующему пункту нашей программы — настройке резидентной защиты (антивирусного монитора). Сворачиваем ветку **Scanner** и переходим к ветке **Guard**.

Смотрим раздел **Scan** (сканирование). (рис. 22)

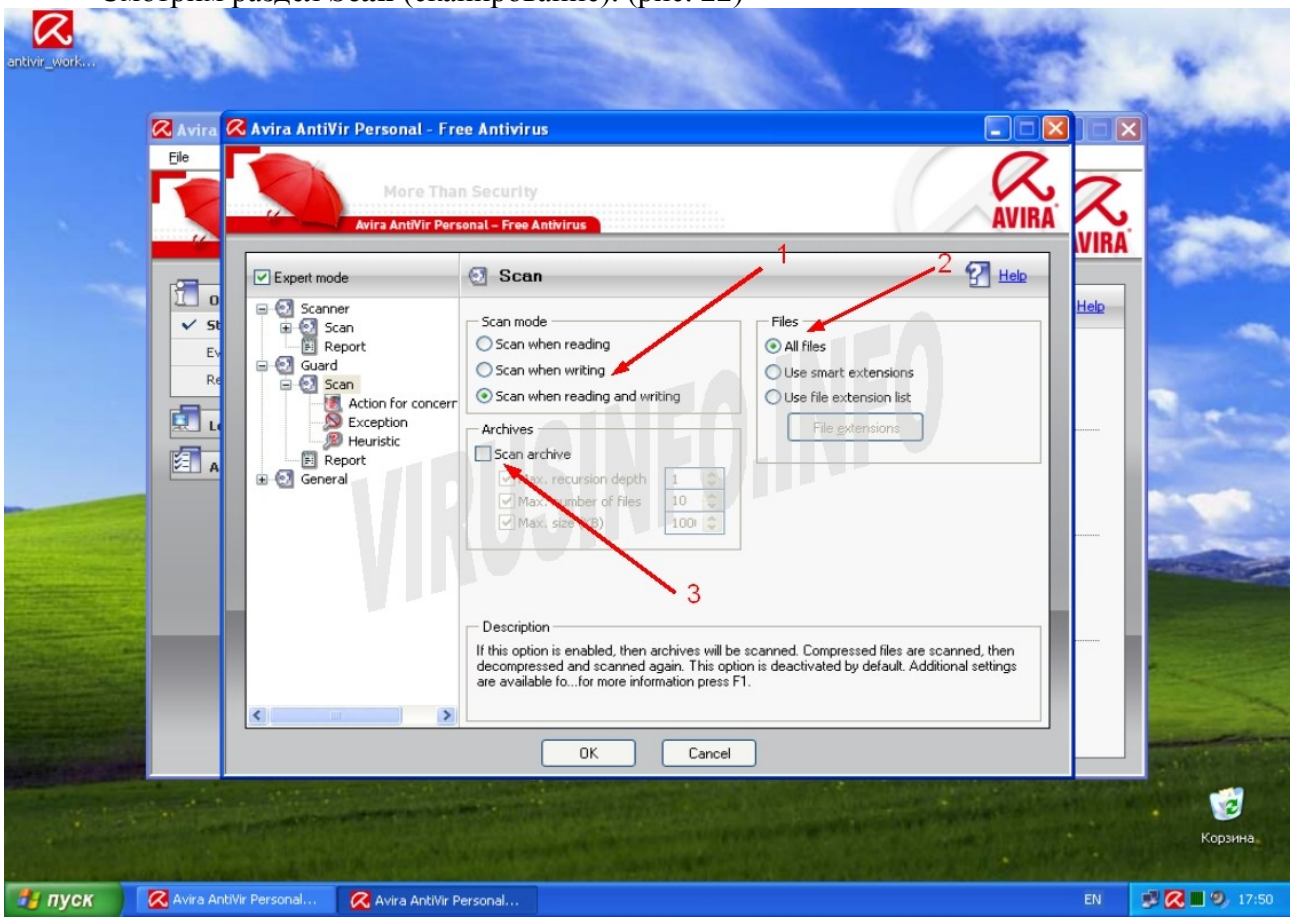

Рис. 22

Первое, что мы должны выбрать — это режим сканирования. (1).
Нам доступны 3 режима:

- **Scan wneh reading** (сканирование объекта при попытке его чтения)
- **Scan when writing** (сканирование объекта при попытке записи)
- **Scan when reading and writing** (сканирование объекта при попытке чтения и записи)

Я рекомендую ставить 3-й режим. Этот режим обеспечивает максимальную безопасность.

Дальше указываем какие типы файлов должны подвергаться проверке. (2). Опять же, доступны 3 режима:

- **All files** (все файлы)
- **Use smart extensions** («умное» сканирование по расширениям)
- **Use file extention list** (использовать список расширений)

Я рекомендую использовать 1-й режим (все файлы). Этот режим обеспечивает наилучшую безопасность, хоть и требует больше ресурсов ПК. Если же у Вас напряжёнка с ресурсами ПК, то можно выбрать второй режим. В этом режиме антивирусный монитор сам принимает решение какие файлы сканировать исходя из анализа содержимого файла и его расширения. Третий режим самый небезопасный, поскольку файлы сканируются только по расширению. То есть если файл леночка.exe переименовать в леночка.ttt, то монитор пропустит спокойно этот файл, будь он хоть трижды вирусом. Так что использовать этот режим не рекомендую вообще. (только если Вы не внесли расширение ttt в список расширений для анализа)

А вот опцию **Scan archive** (3) лучше вообще не включать, если не хотите наблюдать, как Ваш ПК из гоночного болида превращается в пример для пословицы «Кто понял жизнь, тот не спешит». Много где можно услышать мнения, что проверять архивы «на лету» просто обязательно!! Иначе апокалипсис и полный писец. Если Вы тоже такое читали, то вдумайтесь, Вы когда-нибудь видели файл, который сам бы вылез из архива?? Вот лежит себе заархивированый Ваш курсовик, а потом ни с того, ни с сего сам распаковался. Я такого ни

разу не видел. В зоопарке львы из клетки тоже не сами вылазят. Вирус в архиве абсолютно безопасен ровно до тех пор, пока Вы его сами не распакуете и не запустите, но как только Вы попытаетесь распаковать вирус, антивирусник тут же (если он конечно в курсе про этот вирус) его прибьёт. Так что включать проверку архивов «на лету» это просто издевательство над своим ПК :)

Следующий раздел **Action for concerning files** (фраза несколько загадочная, но по духу близкая к Действия для подозрительных и обнаруженных файлов). Там всего лишь две опции, которые включены по умолчанию: **Use event log** (использовать системный журнал событий) и **Acoustic Alert** (сигнал по тревоге). Если включена первая опция, то в системный журнал Windows будут записываться события о событиях «на фронте». А вот если включить вторую опцию, то при каждой найденной заразе системный динамик (пищалка) будет аццки пищать и подражать серенькому животному с хвостиком :)

Раздел **Exception** (исключения) нам уже знаком по настройке ручного сканера, но в отличии от сканера, здесь кроме файла или каталога можно задавать в исключения процессы. Смотрим рис. 23

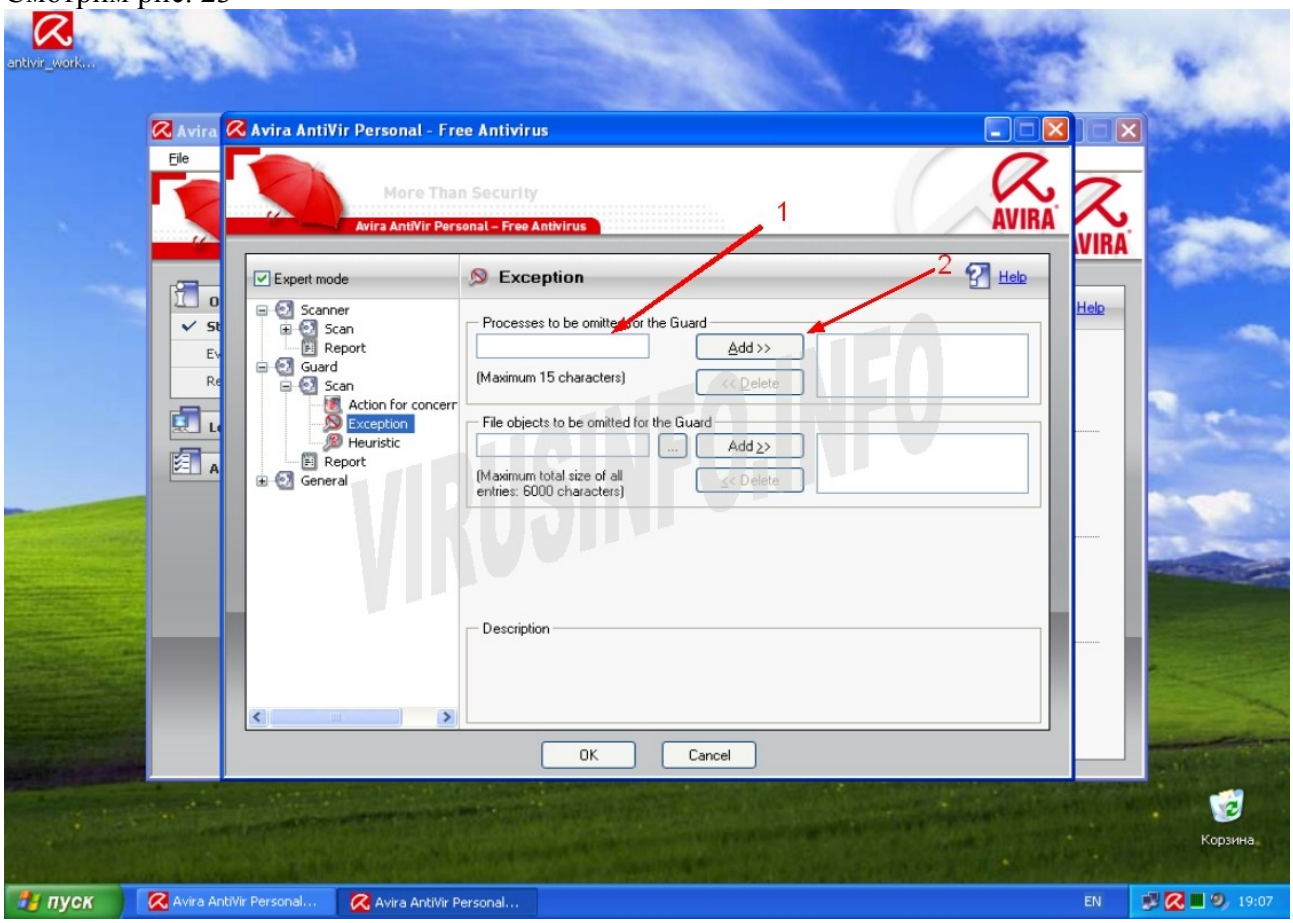

Рис. 23

В поле (1) вручную пишем имя процесса, к сожалению максимум 15 символов, а затем нажимаем кнопку **Add** (2)

Настройки раздела **Heurisctic** (эвристика) полностью аналогичны настройкам такого же раздела в ручном сканере.

Раздел **Report** мы уже настраивали, единственное что, так это есть возможность ограничения размера отчёта по размеру (от 1 до 100 мегабайт) (опция **Limit size to**), архивирование отчёта перед тем, как начать новый (опция **Backup report file before shortening**) и запись конфигурации антивируса в файл отчёта (опция **Write configuration in report file**). В данном разделе можно оставить всё как есть.

Переходим к ветке **General** (общие настройки).

Первое, что мы видим, это раздел **Email**. Здесь настраивается отправка сообщений о о найденных зловредах по электронной почте. Может быть полезно в том случае, если Вы

хотите знать, что на Вашем ПК пытаются поймать Ваши друзья или родичи :) пока Вы на работе или пошли в магазин за бубликами. Смотрим на рис. 24

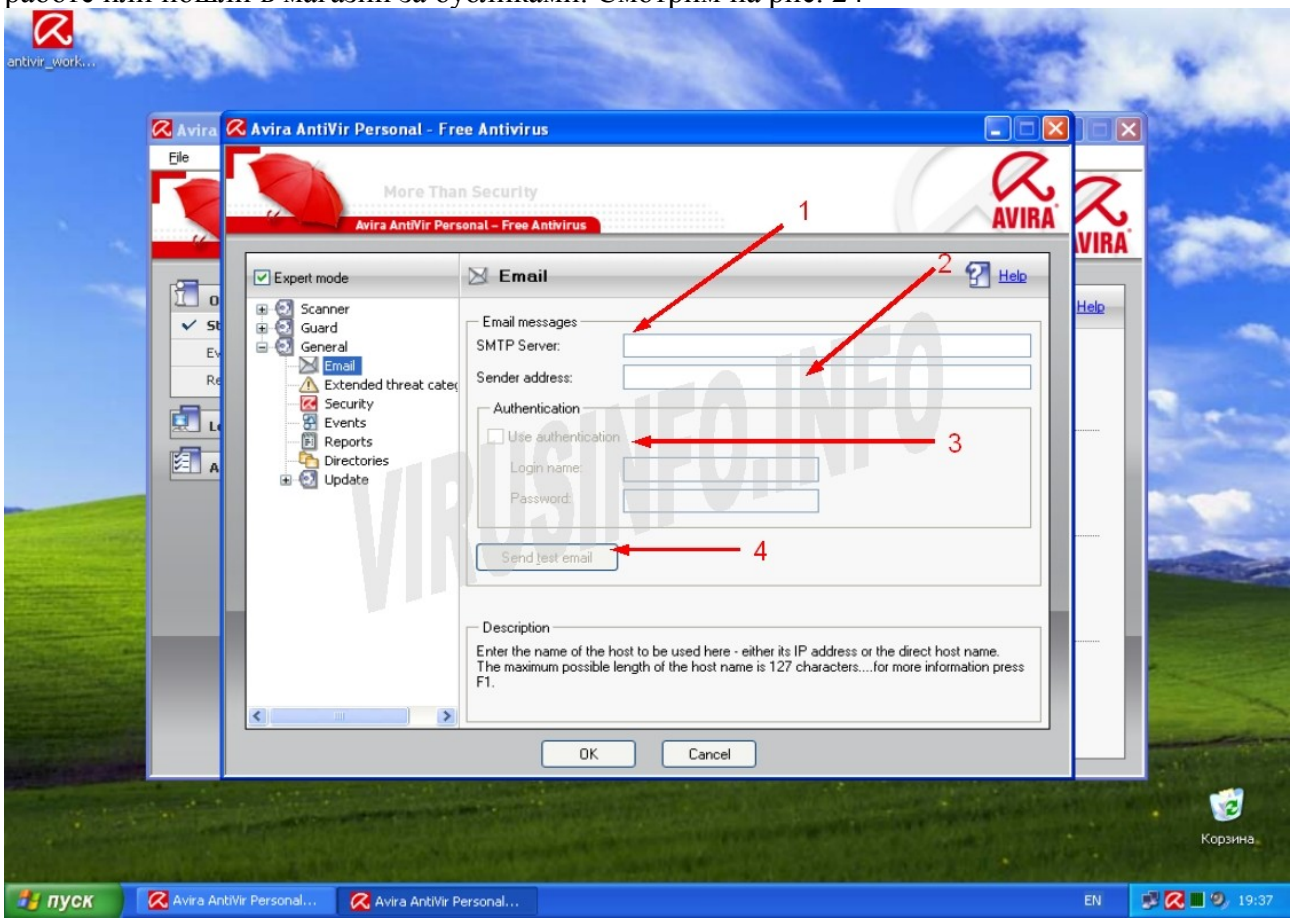

Рис. 24

В поле **SMTP Server** (1) пишем адрес этого самого сервера, в поле **Sender adress** (2) пишем адрес получателя. Если Ваш SMTP server требует аутентификацию, то ставим галочку (3) и в полях **Login name** и **Password** пишем имя пользователя и пароль соответственно. После того как все настройки указаны, можно нажать кнопку **Send test email** (послать тестовое сообщение) (4) и проверить почтовый ящик, на который должно придти письмо.

Раздел **Extended threat categories** (расширенный список угроз). В этом разделе указывается какие именно категории опасных угроз должны обнаруживаться антивирусом. По умолчанию часть категорий отключена, но для повышения личной безопасности рекомендую поставить галочку **Select All** (выбрать все). После этого Авира будет более ревностно относиться ко всяким подозрительным файлам :)

Раздел **Security** (безопасность) посвящён безопасности самого антивируса. Смотрим рис. 25

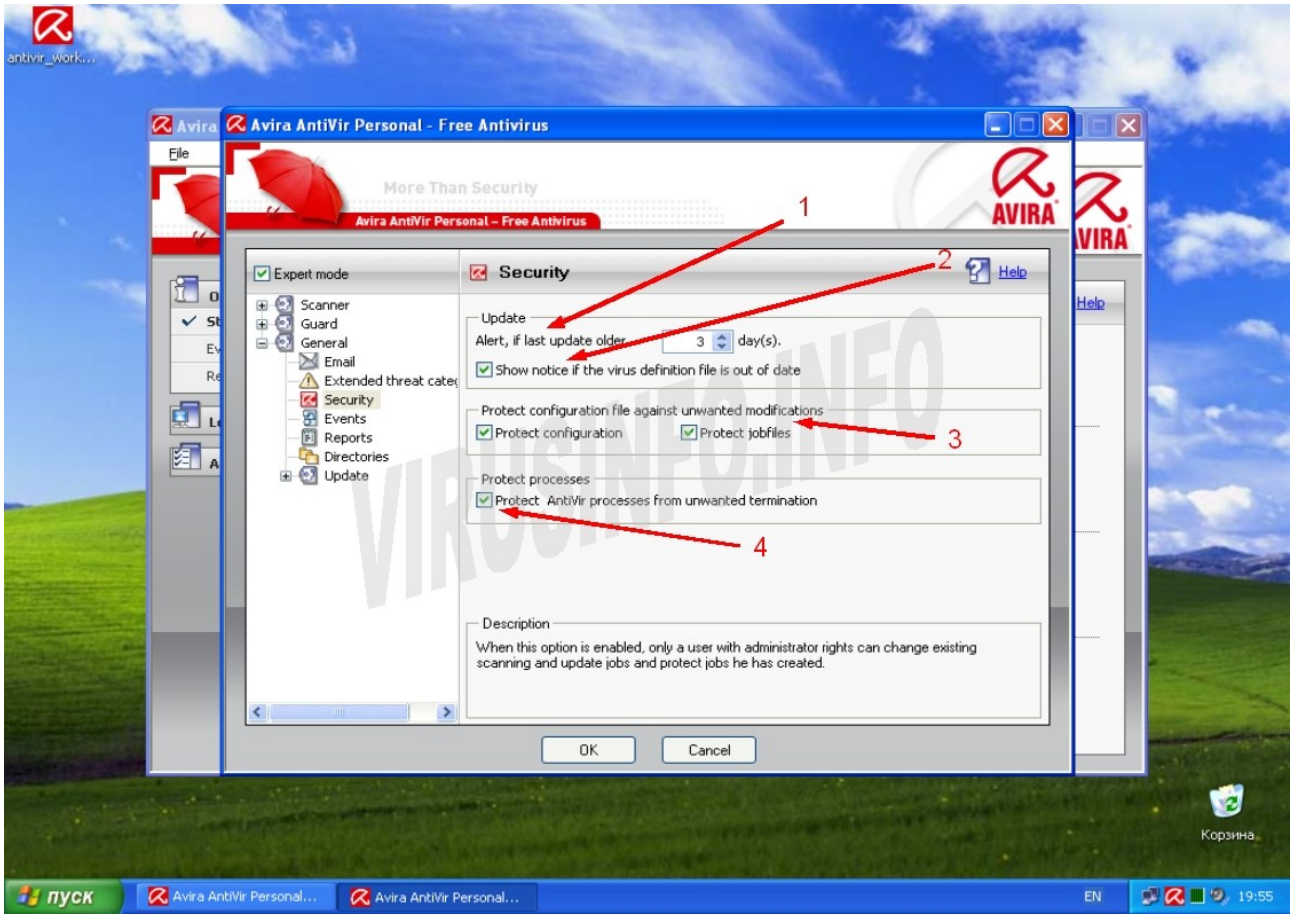

Рис. 25

(1) **Alert, if last update older** (предупреждать, если последнее обновление старше). Собственно, тут всё ясно, указываем кол-во дней, по истечении которых нас предупредят о устаревшей базе. Лучше поставить 1-2 дня. Чем чаще мы обращаем внимание на актуальность обновления антивирусных баз, тем для нас лучше :) Предупреждение будет отображаться в планировщике заданий

(2) Эту опцию тоже лучше включить. Если она включена, то будет показано всплывающее уведомление о устаревших базах.

Обязательно ставим галочки возле **Protect configuration** (защитить конфигурацию), **Potect JobFiles** (защитить рабочие файлы) и **Prevent AntiVir processes from being terminated** (препятствовать завершению процесса AntiVir) (3, 4) Эти опции предназначены для того, чтобы вирус не смог изменить настройки, удалить файлы антивируса или завершить процесс антивируса.

Раздел **Events** (события). Здесь можно указать сколько событий должно хранится в базе, старше какого периода удалять события и можно вообще отключить ограничения на кол-во хранимых событий. По умолчанию события старше 30 дней удаляются. Тут настраиваете как хотите, а можно оставить как есть.

Раздел **Reports** (отчёты) полностью аналогичен разделу **Events**.

В разделе **Directories** (каталоги) указывается путь к паке для хранения временных файлов антивируса. По умолчанию этот каталог находится в том каталоге, куда установлен сам антивирус. У меня это C:\Documents and Settings\All Users\Application Data\Avira\AntiVir PersonalEdition Classic\TEMP\ У вас этот путь может быть другим (смотря куда ставили). Также можно указать системную папку для хранения временных файлов **Use default system settings,** или указать вообще отдельную папку. Мой совет, оставляем всё как есть.

Раздел **Update** (обновления). Это очень важный раздел. Смотрим рис.26

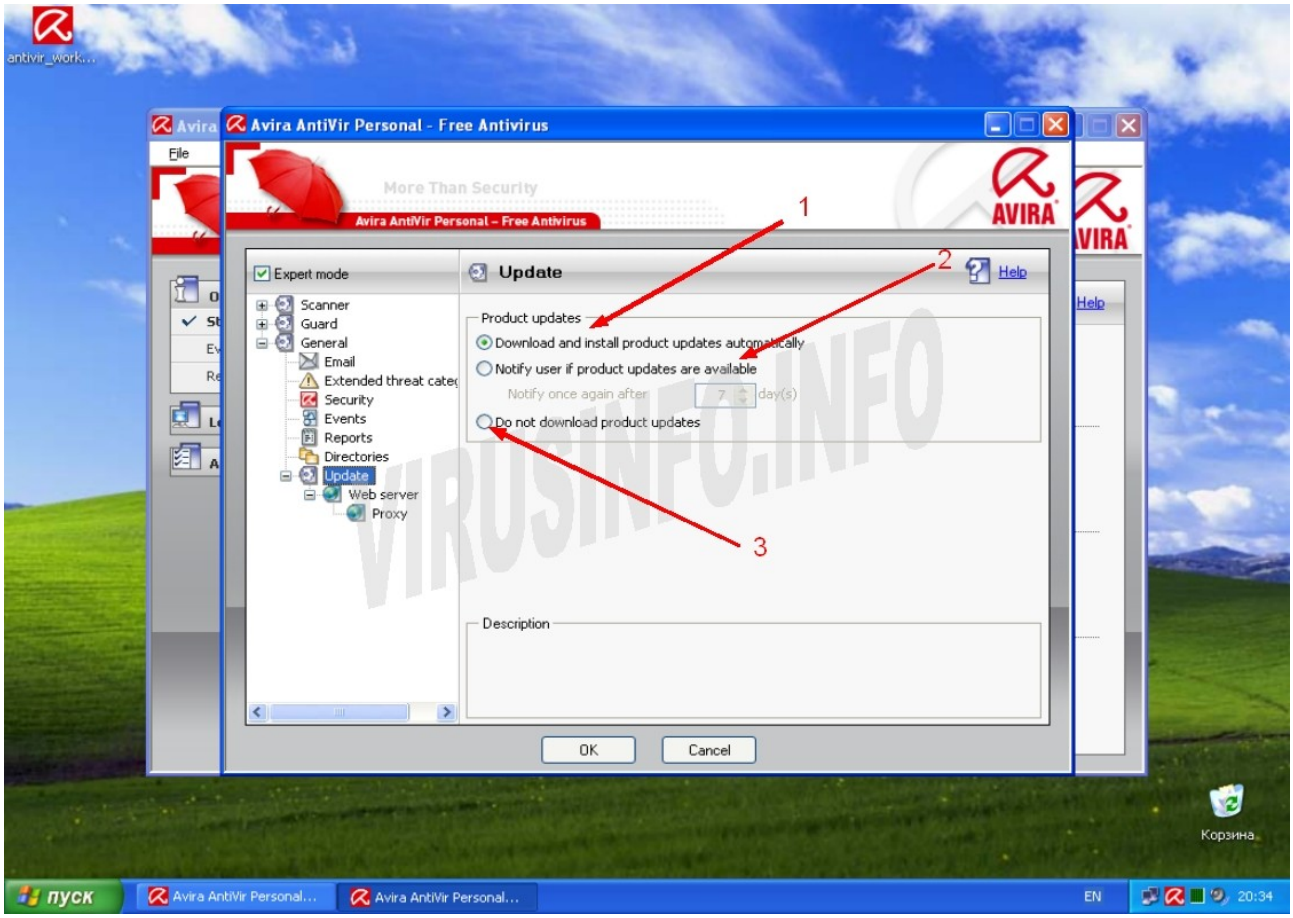

Рис. 26

Я рекомендую указать опцию **Download and automatically install product updates** (загружать и устанавливать обновления автоматически) (1).

Если Вы хотите просто получать уведомления о том, что обновления доступны, то указывайте опцию (2). Также можно настроить период, по истечении которого уведомление будет опять показано.

Опция (3) **Do not download product updates** (не загружать обновления). Её приходится включать в том случае, если у ПК нет доступа в сеть Интернет. Если же доступ в интернет есть, то эту опцию не стоит использовать.

Подраздел **Web Server**. Здесь указывается, как модуль обновления должен работать с сетью. Смотрим рис. 27

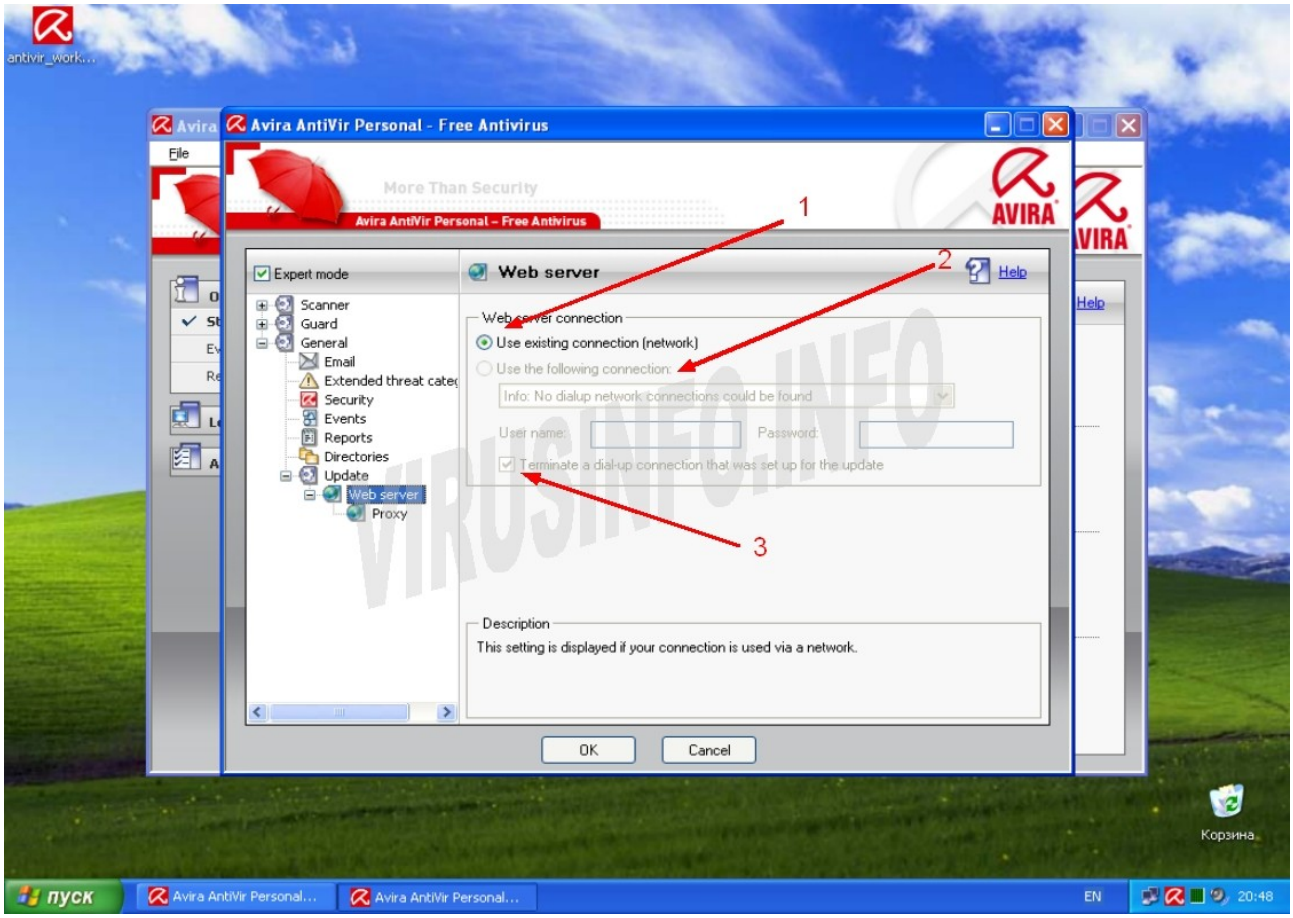

Рис. 27

Use existing connection (network) (использовать текущее соединение) (1) — Самый простой вариант. Ваш ПК в общей сети, все выходят через один шлюз.

Use the following connection: (использовать следующее соединение) (2) - Avira AntiVir может автоматически определять какой тип соединения с всемирной паутиной Вы используете. Если таких соединений нет, то эта опция неактивна. В противном же случае будет доступен список соединений. Если же у Вас dial-up, то будут доступны поля для логина и пароля и доступна опция **Terminate a dial-up connection that was set up for the update** (разорвать соединение по завершению обновления).

Подраздел **Proxy** (настройки для работы через прокси-сервер). Смотрим рис. 28

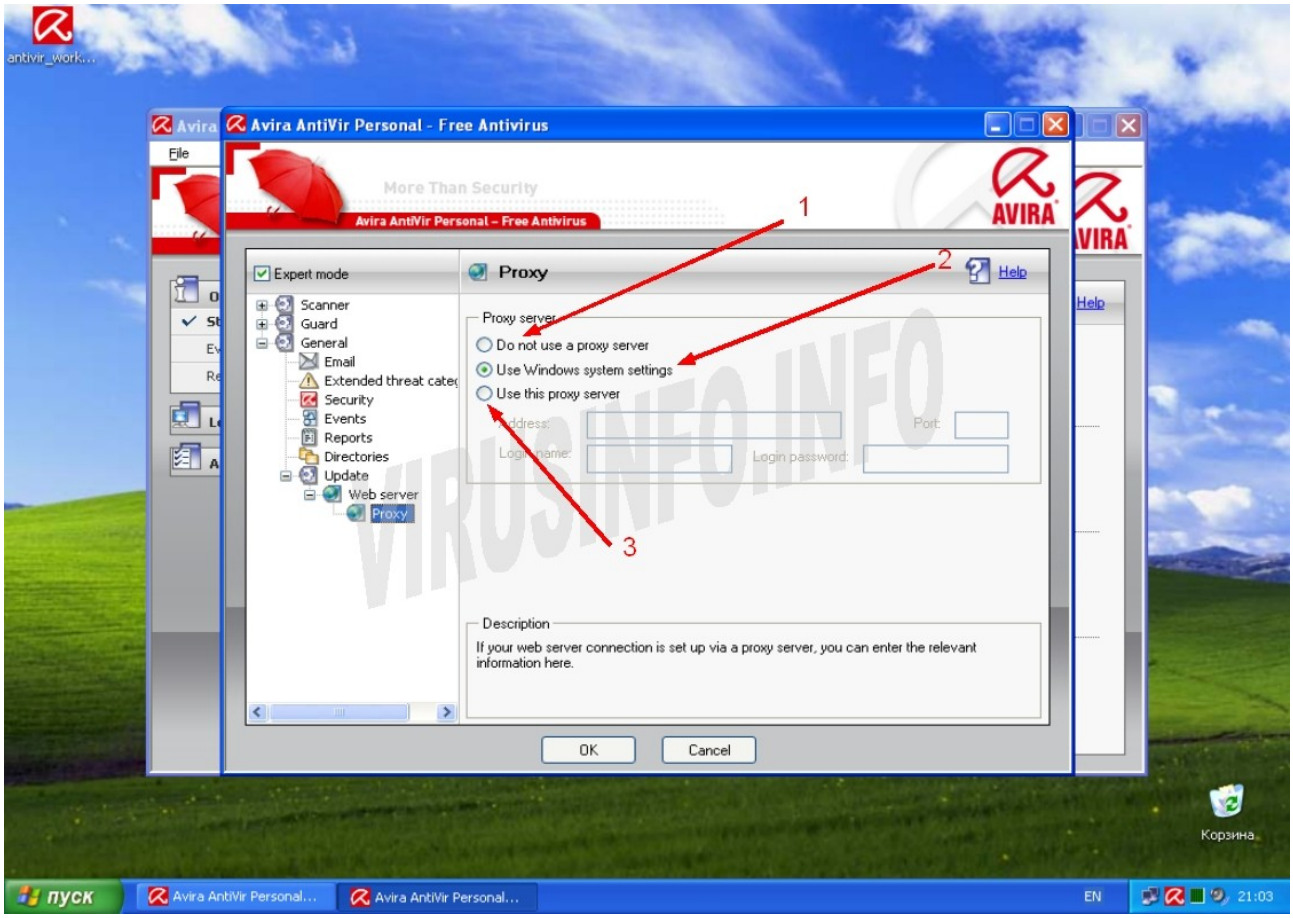

Рис. 28

Do not use a proxy server (не использовать прокси-сервер) — Ну, вроде как понятно, не использовать так не использовать; ломиться напрямую :)

Use Windows system settings (использовать настройки системы) — самый распространённый вариант. Будут автоматически прочитаны настройки ОС.

Use the following proxy server (использовать следующие настройки прокси-сервера) — тут прописываются настройки для получения доступа к прокси-серверу. Возможны такие ситуации, что необходимо задать настройки отличные от системных. К примеру Вы не хотите, чтобы Internet Explorer выходил в сеть и указываете ему адрес прокси-сервера 0.0.0.0. А по умолчанию стоит опция (2). Авира вычитает эти настройки и естественно не сможет обновиться.

Теперь расскажу о том, как обновить Avira Antivir в том случае, если ПК, на котором она установлена не имеет доступа к сети интернет. Для начала нам следует скачать базы. Скачать их можно отсюда или отсюда. Сохраняем архив в нужную нам папку. Далее с главном окне антивируса выбираем меню **update**, а в нём пункт **Manual Update** (рис. 29)

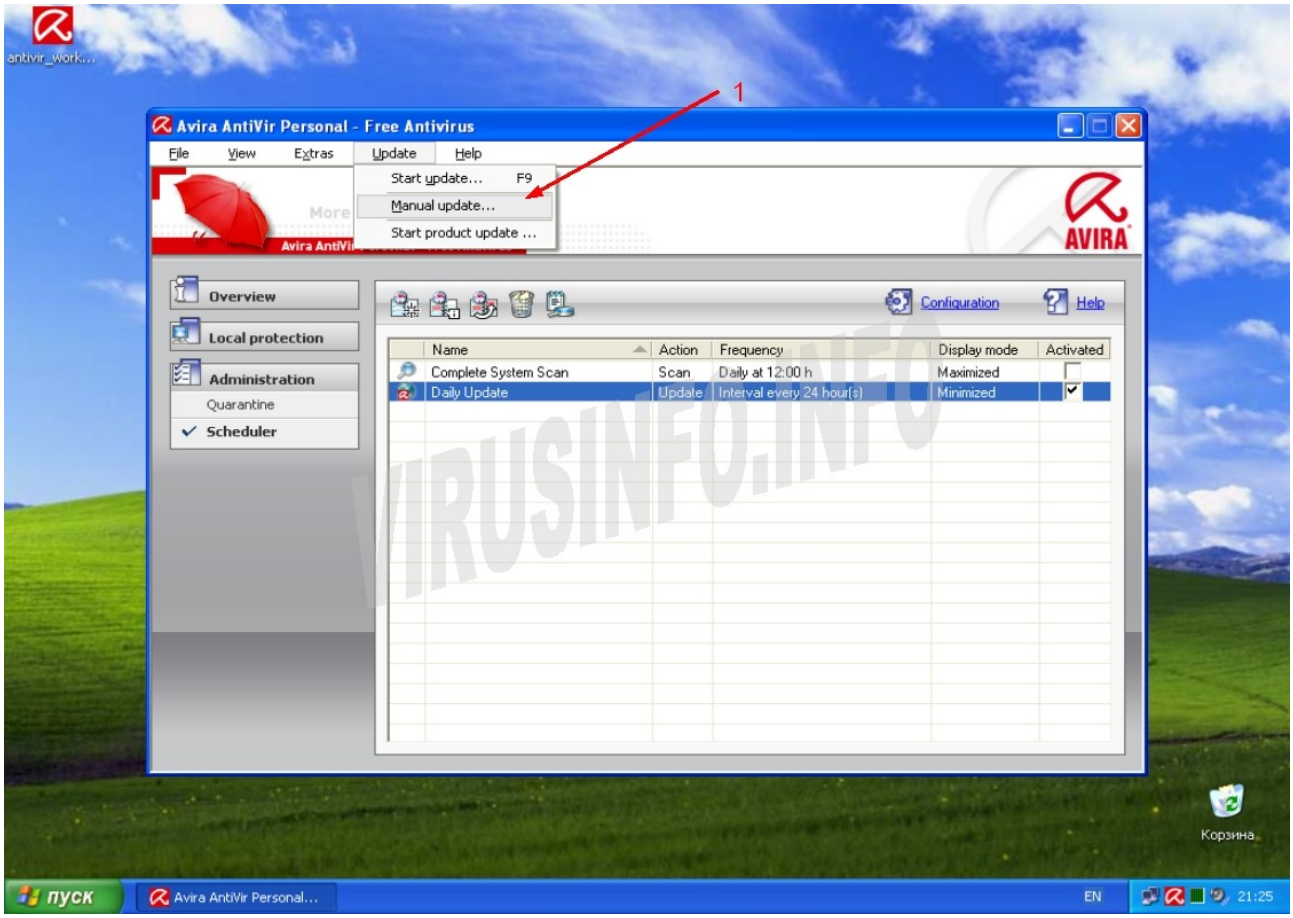

Рис. 29

Откроется окно (1), в котором мы выбираем тот каталог, куда мы сохранили скачанный архив с базами. Выбираем файл и жмём кнопку «Открыть» (2) (рис. 30). После чего антивирус обновится.

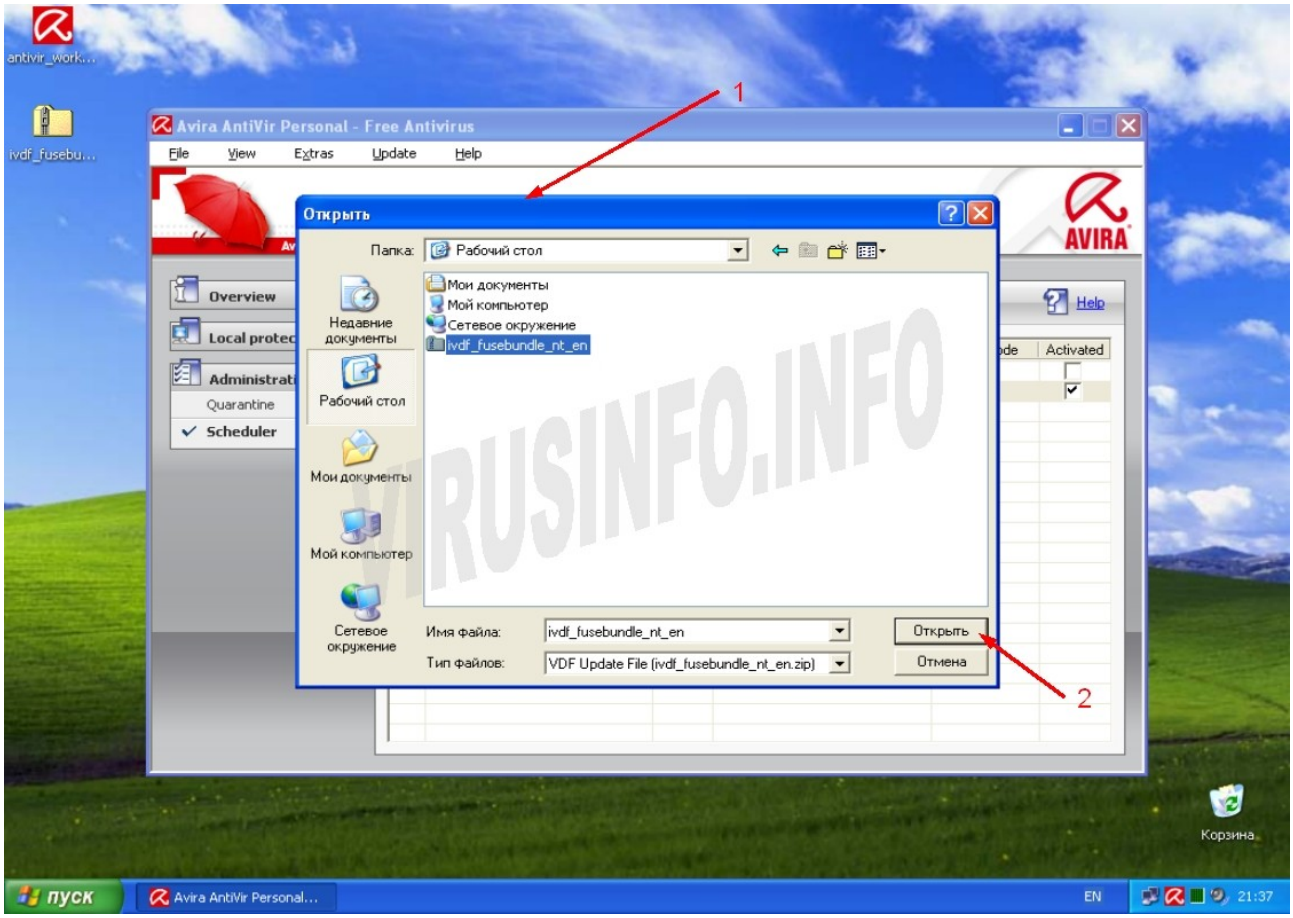

Рис. 30

Пора пить пиво :)

На данный момент это всё по данному продукту. Во второй части статьи, я расскажу о **Avira AntiVir Premium.** Возможно, я упустил некоторые детали (скорее всего это так, но существенными они наверное не будут). Как всегда, замечания - учитываются, конструктивная критика – приветствуется. Обсуждение статьи будет вестись на портале virusinfo.info.

Отдельное СПАСИБО команде портала virusinfo.info, которая участвовала в обсуждении статьи.

Также спасибо команде разработчиков Crysis, Battlefield 2 и C&C 3 Kane Wrath :)
Специальное спасибо всем пивзаводам Украины за любезно выпущенное и доставленное в магазины пиво :)