Павшим в борьбе с вирусами ПК,
посвящается

Здравствуйте! Перед Вами первая статья из цикла статей, посвящённых установке и настройке самых распространённых антивирусов. Надеюсь, данные руководства будут полезны многим, особенно новичкам в мире информационных технологий.

Сегодня практически все у кого есть ПК, знают, что в системе должен быть установлен антивирус. Вирусы могут проникнуть в Вашу систему не только в том случае, если Вы подключены к сети Интернет. Это может быть флэшка друга, CD с зараженными файлами и т.д. Но как показывает практика, даже если антивирус присутствует в системе, то он либо не обновлён, либо настроен неправильно, либо и то, и другое вместе, что в результате сводит присутствие антивирусной программы к 0. Я постараюсь максимально просто показать, как желательно, настроить тот или иной антивирус.

Естественно, я не претендую на абсолютную истину и, кому-то, мои советы покажутся нелепыми. Я понимаю, что не все будут согласны со мной, это логично, сколько людей, столько и мнений. Замечу одно: выбор антивируса – личное дело каждого, я не буду никому навязывать тот или иной продукт, поэтому все попытки уличить меня в пиаре того или иного вендора считаются бессмысленными ☺. Собственно пиарить смысла нет, ибо в зависимости от ситуации, я могу пользоваться абсолютно различными продуктами.

Итак, начнём. Первым антивирусом, который я рассмотрю, будет Norton AntiVirus 2008 (первым я его взял не из-за особого пристрастия, а из-за того, что я не пользовался NAV года, так, с 2004, стало интересно, что там появилось и чего убралось). Бодрым шагом идём на www.symantec.com. Заглянув в раздел For Home, находим ссылку на NAV 2008, смотрим, чего пишут.

Системные требования:

Windows Vista® Home Basic/ Home Premium/Business/Ultimate
Windows® XP with Service Pack 2 Home/XP Pro/XP Media Center Edition;
Процессор с тактовой частотой 300MHz или выше;
256MB ОЗУ;
300MB на жестком диске;
(также должны быть удовлетворены минимальные системные требования для ОС).

Ключевые особенности:

Antispyware;
Антивирус
Защита от интернет-червей; (Firewall, который контролирует входящие соединения)
Обнаружение Rootkit.

Цена: 39,99$.

Интерфейс: англоязычный

Загрузить пробную версию сроком на 15 дней можно по адресу:
http://spftrl.digitalriver.com/pub/symantec/2004/NAV081500.exe (~56MB)

Приступим к установке. Запускаем тот пакет, что мы скачали, соглашаемся с лицензионным соглашением. Сразу же приходится провести некоторые настройки (рис.1):

Destination Folder – По умолчанию предлагается установка на диск C:\ в папку Program Files. Вы можете согласиться с этим, а можете выбрать другой каталог для установки, нажав кнопку Browse (1).

Norton Community Watch – Присоединиться к сообществу Norton. Как нам сообщают, это поможет общему делу, а также лично нам, ускоряя время реакции сотрудников Symantec на новые угрозы. Эта опция позволяет автоматическую передачу зараженных, подозрительных и проблемных файлов в лабораторию Symantec, что позволит оперативно отреагировать на угрозы безопасности. Решать лично Вам, оставлять ли эту опцию включенной. На мой взгляд, лучше оставить её включённой, хотя, если Вам дорог каждый мегабайт трафика, отключайте.

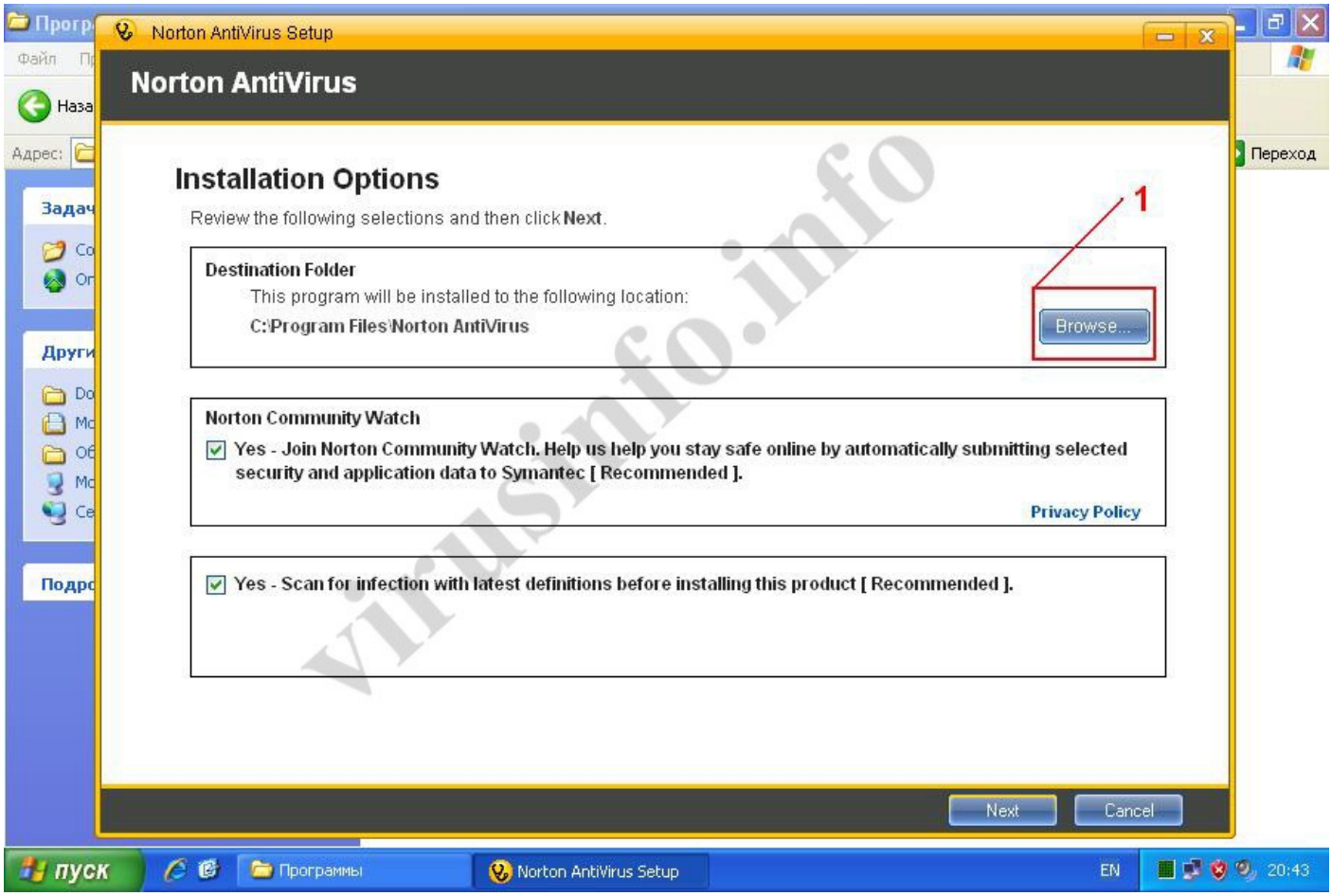

Рис. 1

Последняя опция позволяет провести сканирование ПК, с целью обнаружения и лечения возможного заражения. Действительно полезная опция, так как мы не знаем, заражен наш ПК или нет. Оставляем её включённой, пусть сканирует, хоть это и увеличит время установки. При этом программа установки попросится в интернет для получения самых свежих антивирусных баз. (рис. 2) Список проверенных объектов не выводится, похоже на то, что проверяются наиболее критические области системы, такие как автозапуск, папка system32 и др.

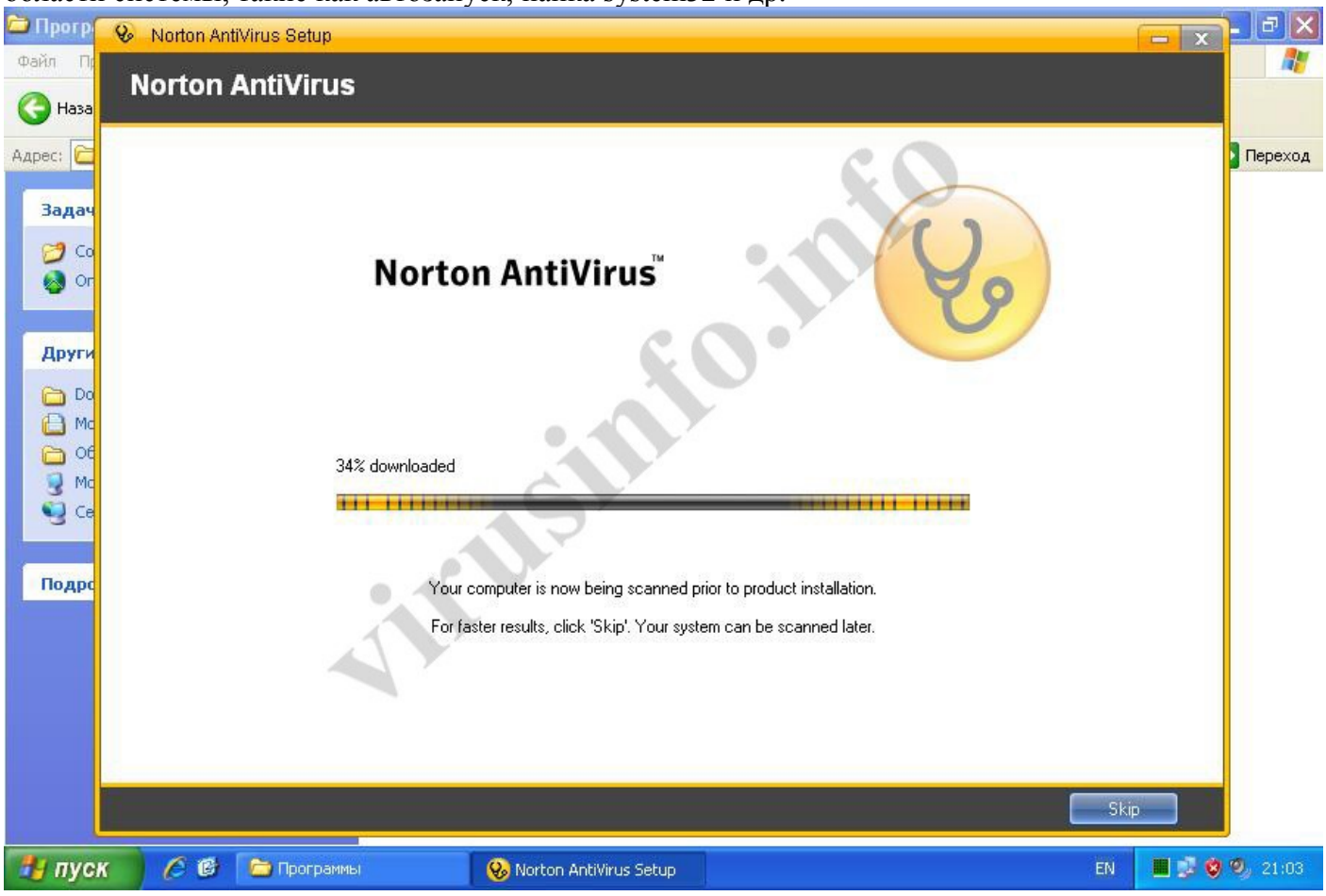

Рис. 2

По окончанию установки появляется окно (рис. 3), в котором предлагаются 3 варианта:
- Использовать продукт 15 дней (пробный период);
- Купить продукт;
- Ввести полученный ранее код активации.

Я выбрал использование пробного периода.

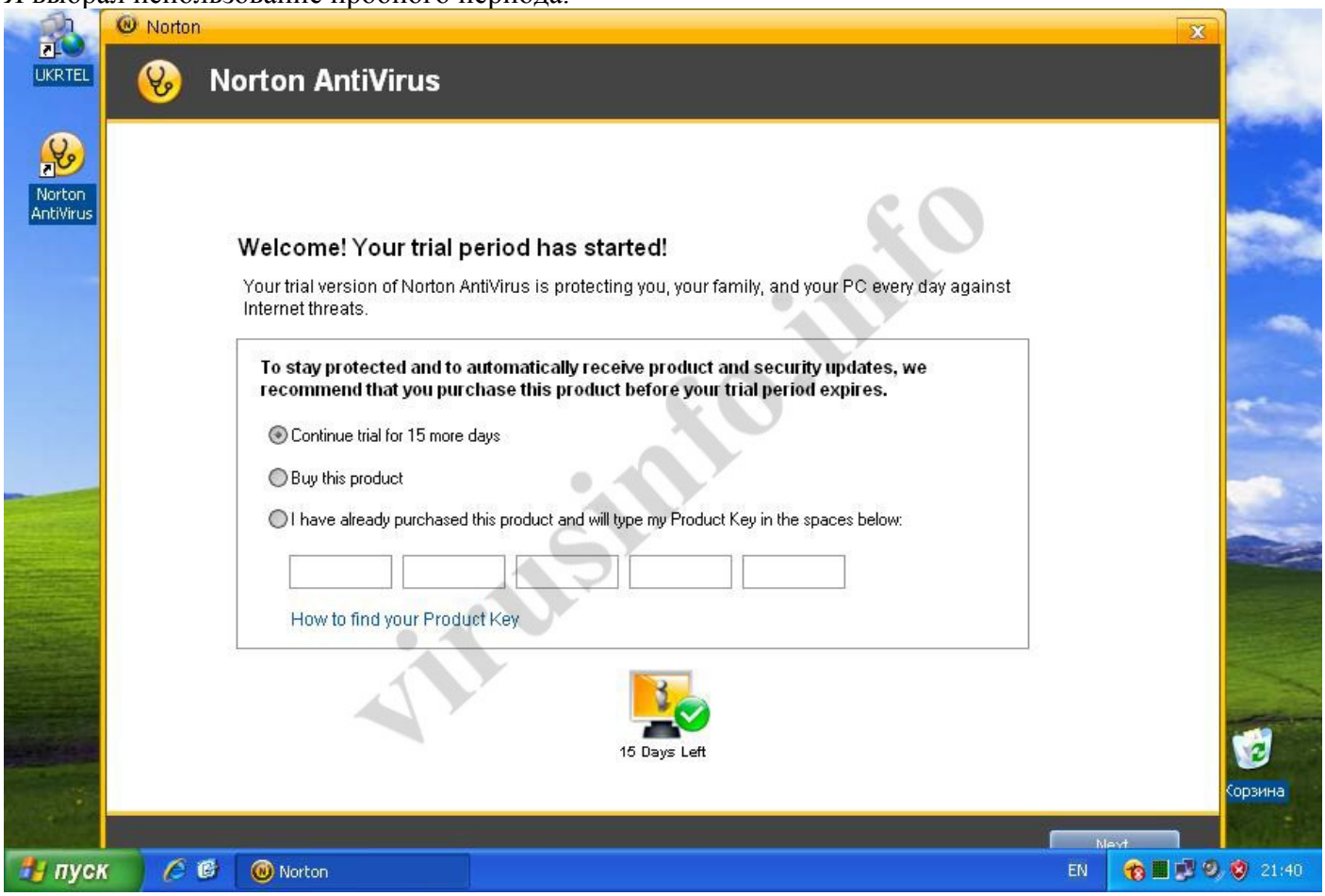

Рис. 3

Жмём кнопку **Next.**

Появляется ещё одно окно, в котором нам предлагают ввести данные для регистрации своего аккаунта. (рис.4) Собственно он, по большому счёту, не нужен, это чистая формальность. Единственное зачем он нужен, так это для сохранения лицензионного ключа, но поскольку эта версия пробная, то и беспокоиться особо не о чем. Выбираем (1), жмём кнопку **Next.** Вам сообщат, что Вы не заполнили необходимые поля, но так как мы не хотим подписываться, то нажимаем появившуюся кнопку **SKIP.**

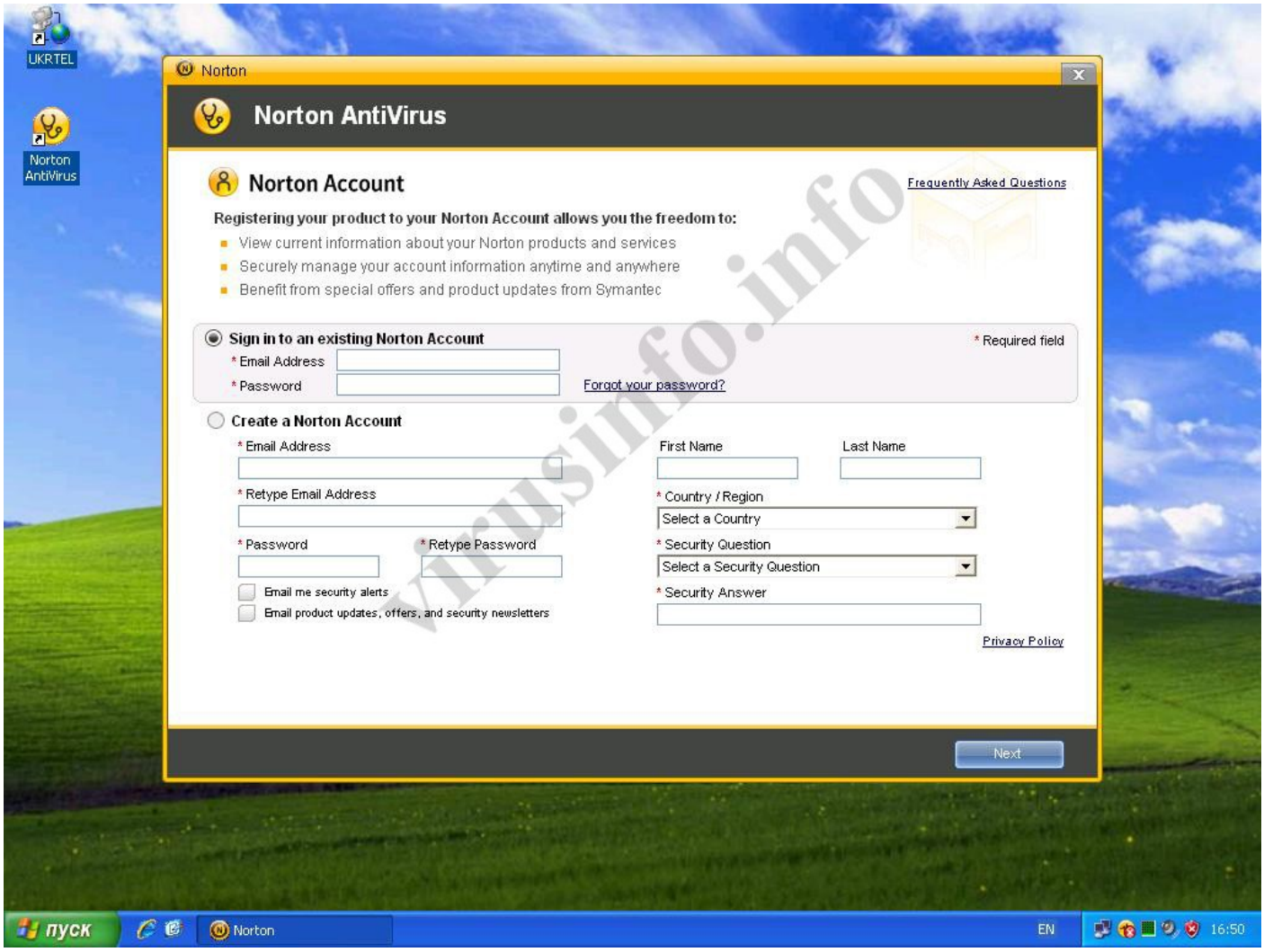

Рис. 4

Последнее окно сообщает нам о том, что у нас есть 15 дней на то, чтобы убедиться в том, что NAV это то, что нужно и по окончанию пробного периода мы с радостью побежим его покупать. ☺

На рисунке 5, мы видим всплывающее предупреждение (1), в котором сообщается, что у нас отключено автоматическое обновление Windows и то, что антивирусные базы устарели.

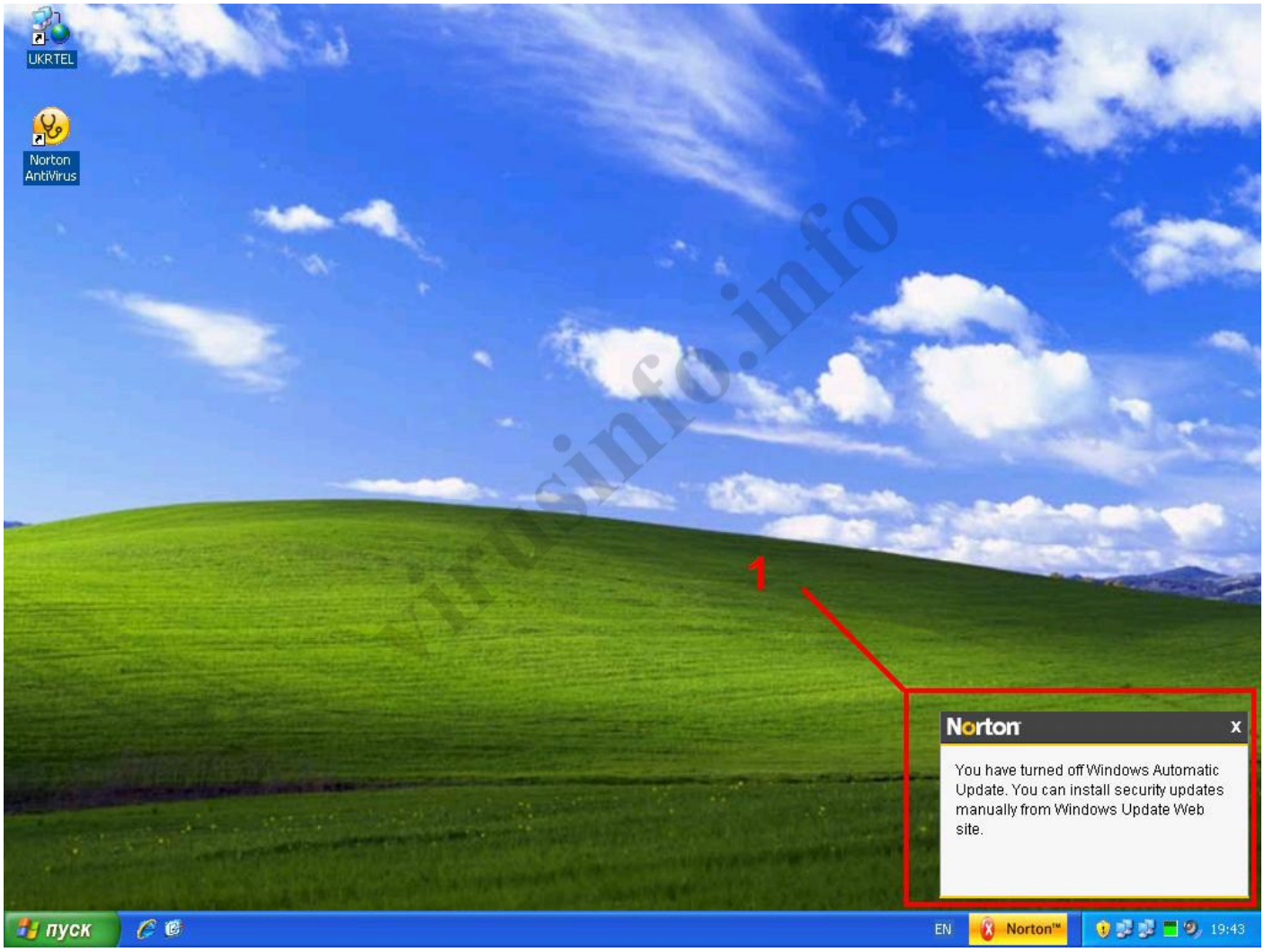

Рис. 5

Возле системного лотка, появилась желтая табличка с бодрой надписью **Norton** и большим крестиком в красном кружочке, что означает, что система подвержена угрозам. Нажимаем на эту табличку, и открывается главное окно программы (рис. 6).

Рис. 6

Мы видим, что попали в **Norton Protection Center.** Давайте разберёмся, что нам дальше делать… Первое, что нам бросается в глаза – большая надпись (1) **At Risk** и кнопка под этой надписью **Fix Now**. Смотрим (2), что же у нас **At Risk**:

Раздел **Computer**. Красное **At risk,** показывает, что не в порядке, это **Protection Updates** (обновления защиты) и **Windows Automatic Updates** (Автоматическое обновление Windows). Всё остальное в норме, о чём нам говорит зелёная надпись **Secure**. Жмём кнопку **Fix Now,** дабы Norton сам исправил проблемы с безопасностью.

Norton сам включил автоматическое обновление Windows и начал обновлять свои базы. Обновляться будет долго, размер обновлений не маленький. После обновления будет предложено перезагрузиться.

На рис. 6, смотрим (3). Есть 4 пункта меню:

- **Run LiveUpdate** (Запустить обновление)
- **Scan Now** (Просканировать систему)
- **View History** (Посмотреть журнал событий)
- **Options** (Опции)

Далее нас интересует (4)… Это карта сети. Вообще, это нужно настраивать, если у Вас несколько ПК с установленными продуктами Norton, если же этого у Вас нет, то и настраивать незачем.

Ну что ж, более-менее разобрались, приступаем к настройке всего нашего хозяйства. Переходим на закладку (5) рис.6.

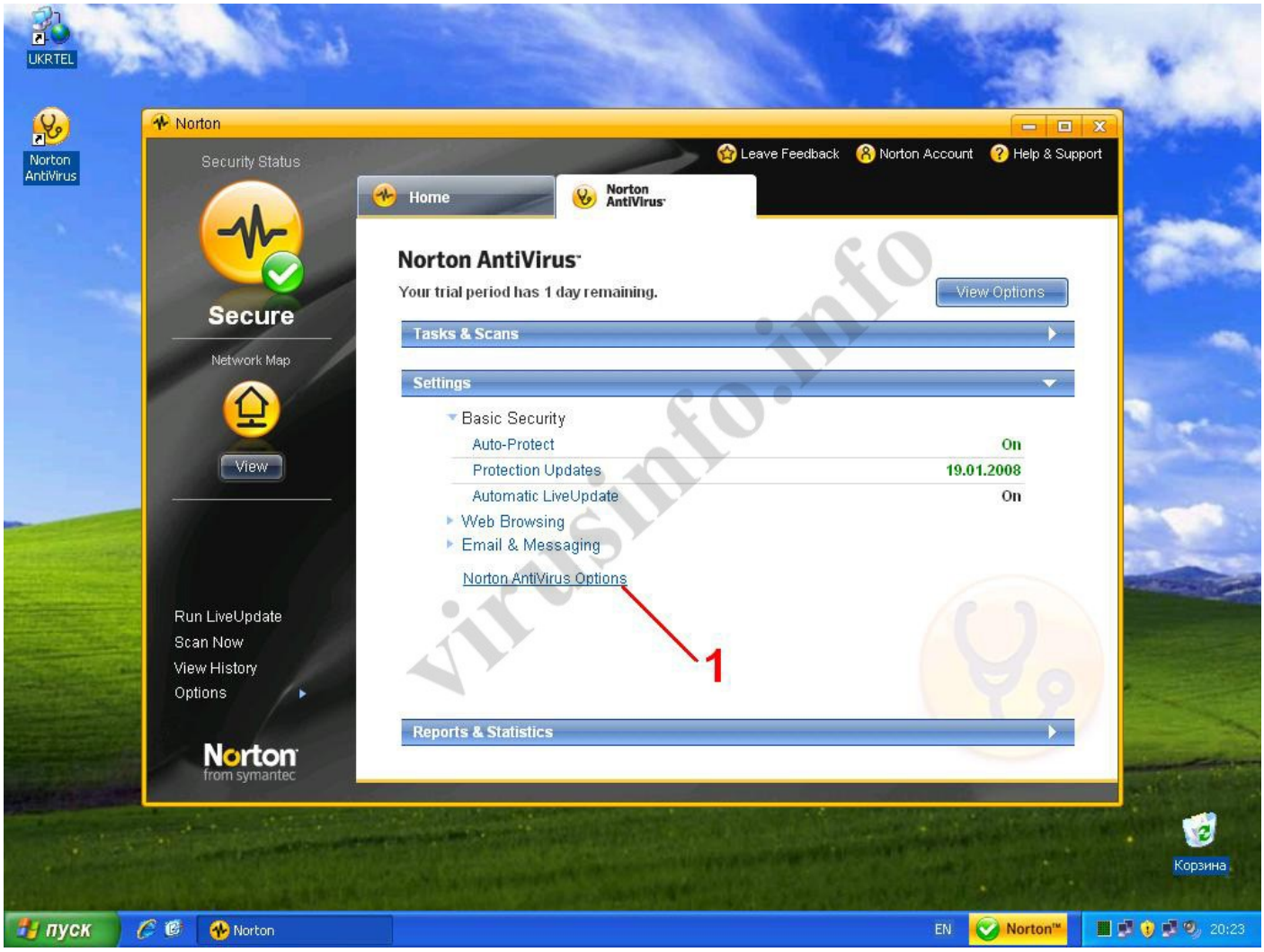

Рис. 7

На рис.7 мы видим следующее:

- **Tasks&Scans** (Задания и сканирование)
- **Settings (**настройки**)**
- **Reports & Statistics** (отчёты и статистика)

Для начала идём в **Settings.** Сделаю оговорку, все подразделы, которые открылись, доступны в подразделе **Norton Antivirus Options (1)**, смело нажимаем на эту надпись. Открывается окно настроек всего комплекса.

Начнём по порядку. Сперва идём в **General Settings** (общие настройки).

Turn on password protection (включить парольную защиту настроек) – Если активировать эту опцию, то при нажатии кнопки **Apply** (применить), будет предложено создать пароль. Не зная этого пароля, получить доступ к настройкам антивируса будет невозможно. Весьма полезная опция, если Ваш компьютер использует несколько человек.

Turn on protection for Norton products (включить защиту продуктов Norton) – Рекомендую включить эту опцию Это не что иное, как самозащита. Включение этой опции активирует защиту процессов и настроек антивируса от несанкционированного доступа со стороны других процессов, что не позволит вредоносному ПО принудительно завершить работу модулей антивирусной защиты или изменить настройки антивируса таким образом, что сделает его работу неэффективной.

Display the Auto-Protect icon in the system tray (отображать иконку в системном лотке) – Если Вы включите эту опцию, то в системном лотке (возле часов) появится жёлтенький кружочек со стетоскопом, это значок NAV. Влияния на работу не оказывает, опция для эстетов.

Join Norton Community Watch (присоединиться к сообществу Norton) – Позволяет автоматически отсылать выбранные отчёты безопасности и подозрительные файлы. В целом, полезная опция. Можно оставить включенной.

Переходим к разделу **Live Update** (автоматическое обновление). Раздел весьма важный потому, что надёжность работы антивируса и защита Вашего ПК напрямую зависит от своевременного обновления антивирусных баз и программных модулей защитного комплекса.

Turn on Automatic Live Update (включить автоматическое обновление) – Настоятельно рекомендую оставить эту опцию включённой, если, конечно, Вы не хотите познакомиться с представителями семейства троянообразных вплотную.

Notify me when updates are available (Уведомлять меня о доступности обновлений) – Рекомендую отключить эту опцию, пусть обновление работает полностью на автомате.

Run Quick Scan whenever protection updates have been received (запустить быстрое сканирование после обновления) – Рекомендую включить эту опцию. После того как будет произведено обновление, NAV начнет проверять критически важные области системы на наличие вредоносных программ (а вдруг чего завелось?)

Дальше идёт самый интересный раздел, **Real-Time Protection** (Активная защита).

Подраздел **General Settings** (общие настройки).

Turn on Suspicious Activity Monitoring (Включить мониторинг подозрительной активности) – Рекомендуется включить. Если будет замечена активность приложений, которая является подозрительной с точки зрения NAV, она будет заблокирована, а в журнал событий будет занесена запись об этом событии. (данная опция не работает на Windows Vista 64bit).

Turn on Advanced Mode (включить расширенный режим) – Если же Вы хотите вручную управлять блокировкой подозрительной активности, то эта опция для Вас, смело включайте. Если же Вы не любите заморачиваться с рассматриванием алертов и раздумыванием над вопросом блокировать - не блокировать, то оставьте эту опцию выключенной. (данная опция не работает на Windows Vista 64bit).

Scan removable media for boot viruses when media is inserted (Сканировать сменные носители на наличие загрузочных вирусов, когда носитель вставлен). - Дополнительный рубеж обороны. Рекомендую включить, хотя включение данной опции замедляет начальную работу с CD и DVD.

Turn on scanning for Microsoft Office documents (Включить сканирование документов Microsoft Office). – Данная опция требует наличия установленного пакета Microsoft Office версии не ниже 2000. Не лишним будет активировать эту опцию.

Подраздел **Auto-protect** (резидентная защита)

Turn on Auto-protect (включить резидентную защиту) – Собственно эта опция ОБЯЗАНА быть включена, иначе зачем нам антивирус вообще? ☺

Load Auto-Protect during system startup (загружать резидентную защиту во время загрузки системы) – Желательно включить эту опцию, хотя она несколько замедляет загрузку системы. Смысл этой опции в том, что чем раньше загрузиться антивирус, тем меньше шансов того, что лютый вирус проникнет в систему.

Turn on Bloodhound heuristics (включить эвристический анализатор) – Настоятельно рекомендую включить эту опцию. 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.

Turn on caching (включить кэширование) – Включение этой опции улучшает производительность системы. Смысл заключается в том, что NAV следит за наиболее часто используемыми файлами и не сканирует их даже после перезагрузки компьютера. На мой взгляд, это минус в защите. Моё мнение, эту опцию лучше отключить.

Подраздел **Email Protection** (защита электронной почты).

Scan incoming email messages (сканирование входящей электронной почты) – Если Вы пользуетесь почтовым клиентом (The BAT!, Outlook Express, Mozilla Thunderbird и др.) то обязательно включайте эту опцию! Современные реалии таковы, что даже от Вашего знакомого может придти письмо с вирусом. Поэтому сканировать входящую электронную почту на наличие вирусов просто необходимо.

Scan outgoing email messages (сканирование исходящей электронной почты) – Опция полезная в плане заботы о других. Если Вы не хотите по ошибке отправить коллеге, другу или партнёру по бизнесу неприятный подарок, то включайте эту опцию, лишним не будет.

Scan outgoing messages for suspected worms (сканировать исходящие сообщения на наличие подозрительных файлов) – Желательно включить.

Automatically remove (автоматически удалить) – При обнаружении вредоносного кода NAV автоматически удалит зараженный файл.

Ask me what to do (Спросить меня что делать) – При обнаружении вредоносного кода в исходящем электронном сообщении NAV запросит у Вас, что с ним делать. Включение этой опции отменяет опцию **Automatically remove.**

Protect against timeouts (защита от ошибки по таймауту) – Крайне желательно включить эту опцию. Дело в том, что прежде чем письмо попадёт к почтовому клиенту, его должен получить NAV и проверить его. Если размер сообщения не маленький и у Вас медленный канал связи, то по прошествии определённого периода времени (обычно 1-3 минуты) почтовый клиент сочтёт, что приём письма не удался и завершит сеанс работы с ошибкой «Истекло время соединения» (ну или нечто близкое по духу). Чтобы такие ошибки не возникали по вине проверки письма антивирусом и была придумана данная опция.

Display icon in System Tray (отображать иконку в системном лотке) – Если включить эту опцию, то при проверке электронной почты, в системном лотке будет отображаться иконка, уведомляющая о том, что проверяется почта.

Display progress indicator (отображать индикатор состояния) – Если включить эту опцию, то при приёме/отправке почты будет отображаться индикатор, который будет показывать сколько ещё нам ждать и как быстро идёт процесс. Опция в целом эстетическая и особой смысловой нагрузки не несёт.

Подраздел **Instant Messenger** (средства обмена сообщениями). NAV может взять под защиту Ваше любимое средство обмена сообщениями, но только при условии, что это Yahoo messenger (версии не ниже 5.0), AOL IM (версии не ниже 4.7), MSN Messenger (версии не ниже 6.0), Trillian (версии не ниже 3.1). Как видим, выбор не богатый. И, к сожалению, аськи, квипы, миранды и прочее популярное у нас - идёт лесом. Жаль.

Подраздел **Internet Worm Protection** (настройка фаерволла). Вкратце, фаерволл (он же брандмауэр) - комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Основной задачей брандмауэра является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Во как ☺ Отличие NAV от других антивирусов – это наличие встроенного брандмауэра (не люблю я слово фаерволл, трудное оно какое-то). Не только NAV имеет в своём составе брандмауэр, У Avast тоже есть (модуль "сетевой экран"), хотя и более примитивный. Но антивирусов с брандмауэрами мало (я не говорю о комплексных решениях типа KIS, NIS, ESS). Сразу сделаю оговорку, брандмауэр в NAV контролирует только входящие соединения (аналог брандмауэра в Windows XP SP2, но на пару порядков мощнее). Конечно, полноценный брандмауэр это более полезная вещь, но с учётом того, что за 40$ (средняя цена всех антивирусов) мы получаем помимо антивируса ещё и средство защиты от сетевых атак извне, то это весьма неплохо. Итак, переходим к настройке.

Обратим внимание на (рис. 8)

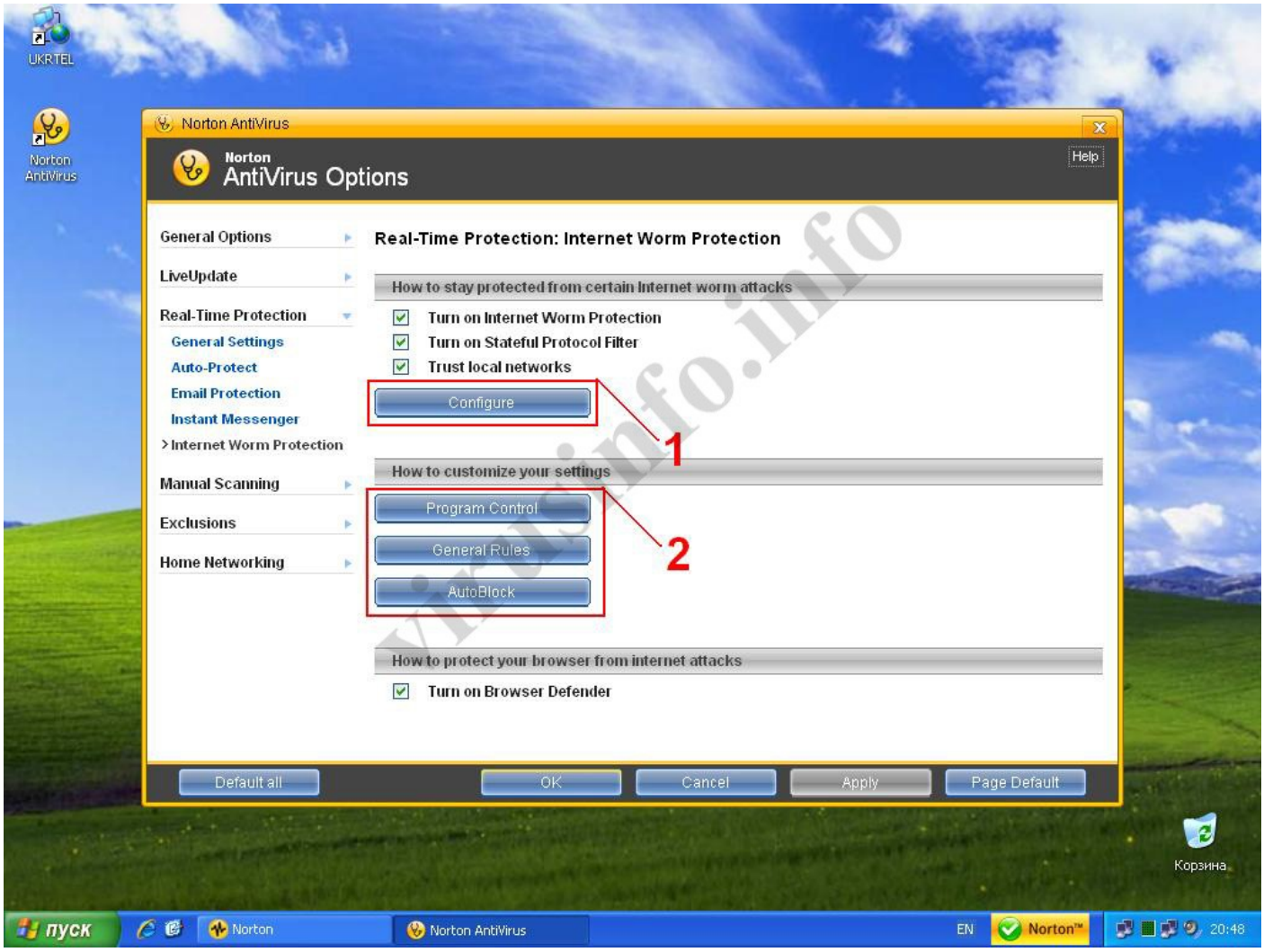

Рис. 8

Turn on Internet Worm Protection (включить защиту от интернет-червей) – Эта опция должна быть включена.

Turn on Stateful Protocol Filter (включить анализатор трафика) – Эта опция также должна быть включена. Её смысл в том, что брандмауэр начинает не только проверять на какой порт (разрешённый/неразрешённый) пришли пакеты, но также проверять содержимое самих пакетов, что весьма полезно, с учётом того, что на разрешённый порт могут прийти «вредные» пакеты, которые могут нести угрозу безопасности Вашему ПК.

Trust local networks (доверять локальной сети) – А вот с этой опцией всё несколько сложнее. Включать её или отключать зависит от того есть ли у Вас локальная сеть или нет. В моём случае – у меня АДСЛ подключение и естественно доверять каким-либо сетям смысла нет, поэтому я её отключил. Если же Вы подключены к домашней сети, то включать это опцию или отключать зависит от того, хотите ли Вы, чтобы к Вашему ПК подключались другие машины сети или нет.

Если нажать кнопку (1) рис. 8, то откроется окно с кучей строчек, это список сигнатур, по которым брандмауэр в NAV может определить активность интернет-червей при проверке трафика. Каждую из сигнатур можно отключить, но особого смысла в этом нет, так что оставляем всё как есть.

Теперь обратим внимание на группу кнопок (2) рис.8.

Первая кнопка, **Program Control (**Контроль программ**)**. Позволяет создавать правила контроля входящих соединений для тех программ, которые Вы укажите в списке. Может пригодиться для разрешения открытия портов для таких программ как eMule, uTorrent и других, которые требуют контроля входящих соединений.

General Rules (общие правила). В отличие от правил созданных индивидуально для программ в **Program Control, в General Rules** задаются глобальные правила доступа к Вашему ПК, они перекрывают правила заданные в **Program Control**. Давайте посмотрим этот список. (рис.9)

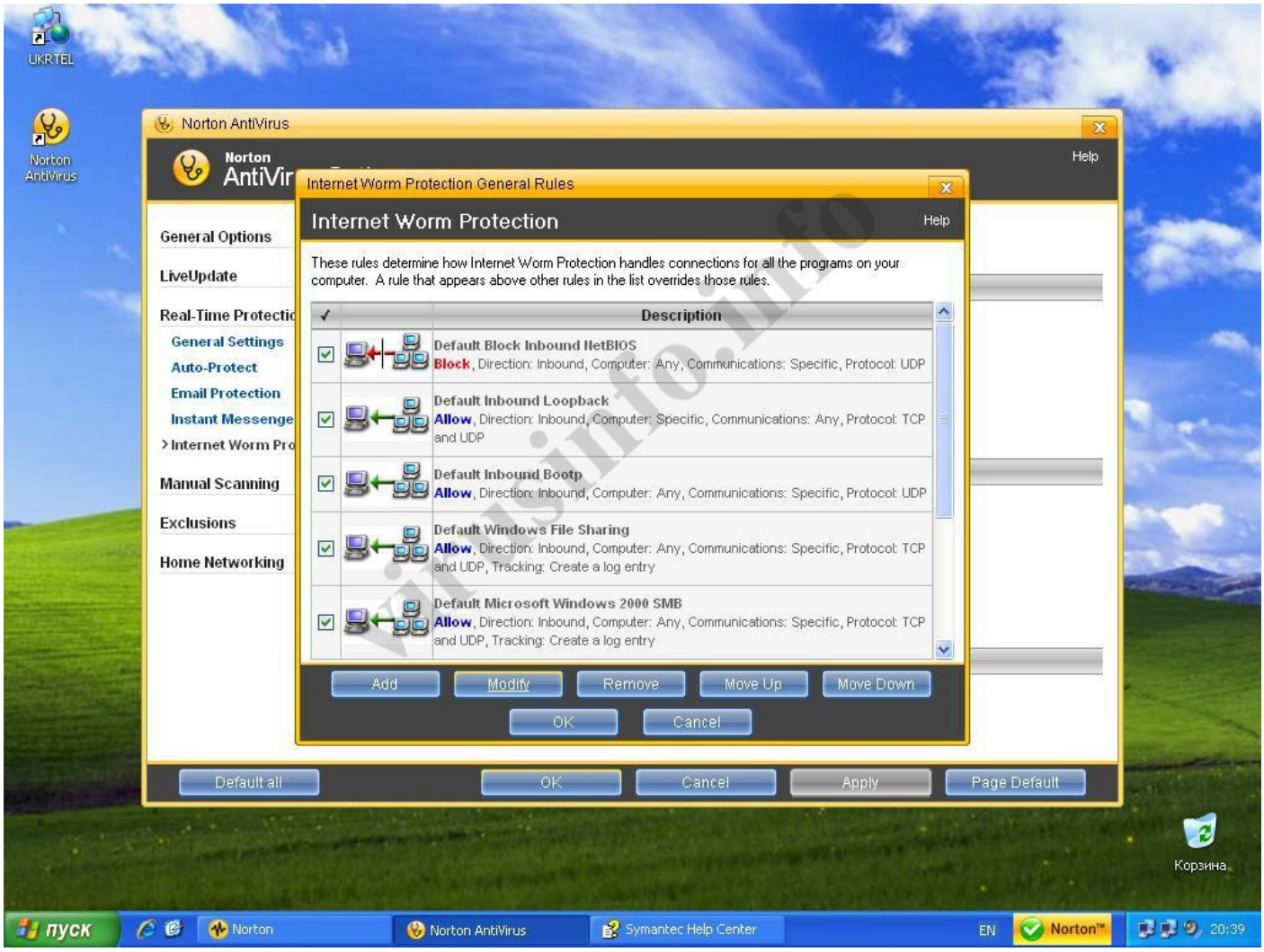

Рис.9

В открывшемся списке перечислены правила, которые определяют, на какие порты возможен доступ к Вашему ПК из интернет. Список составленных правил будет зависеть от многих факторов: подключен ли Ваш ПК к локальной сети, работает ли на Вашей машине ftp или www сервер и др. Рассмотрим обычный случай, у Вас (как и у меня) ADSL-подключение. По хорошему, доступ к Вашему ПК из интернет должен быть полностью запрещён. Конечно, у Вас могут быть установлены клиенты файлообменных сетей и прочее, тогда придётся добавлять ещё правила.

Итак, рассмотрим правила более детально. Как видно из рисунка, правила в NAV отличаются большой наглядностью. Даже новичок может понять, что первое правило запрещает входящие соединения от других компьютеров к Вашему. Галочка слева от правила указывает на то, что правило включено. Более детальную информацию о правиле можно получить выделив это правило (щёлкнуть на нём левой кнопкой мыши) и нажав кнопку **Modify**. Смело нажимаем эту кнопку и видим диалог создания/модификации правила. (Рис.10)

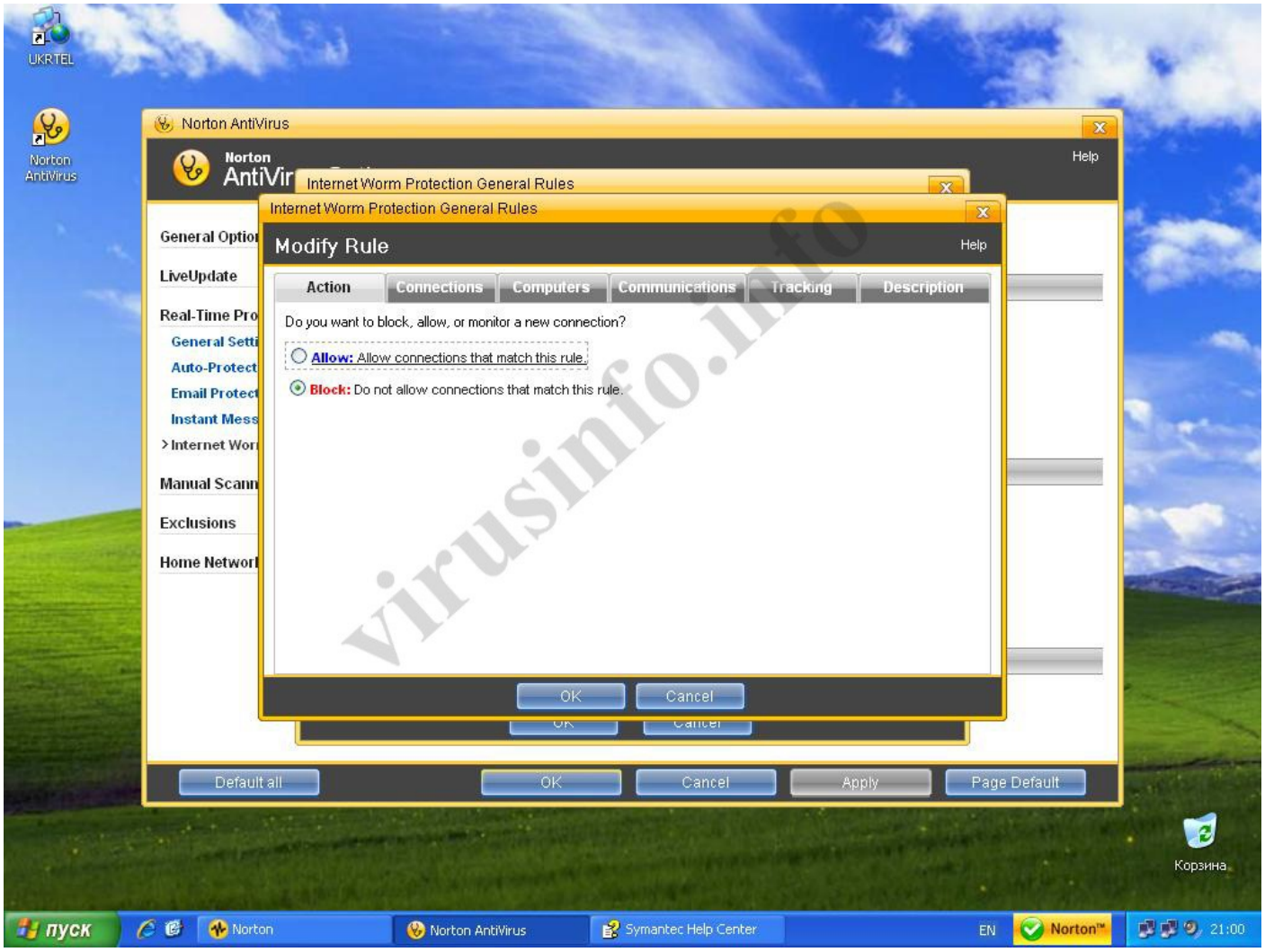

Рис.10

У нас есть ряд закладок сверху **Action** (действие), **Connections** (соединения), **Computers** (компьютеры), **Communications** (протоколы и порты), **Tracking** (отслеживание), **Description** (описание). Рассмотрим их по порядку.

Action (действие) – Доступны два действия или **Allow** (разрешить), или **Block** (запретить). В этом правиле стоит запрещающее действие.

Connections (соединения) – На этой закладке и выбирать то нечего, возможно только одно **Connections From other computers** (соединения от других компьютеров), потому что брандмауэр в NAV контролирует только входящие соединения.

Computers (компьютеры) – На этой закладке задаётся уточняющее условие для входящего соединения. Вы можете выбрать либо от всех машин (**Any Computer**), либо с какого именно IP-адреса, диапазона адресов или определённой подсети будет идти соединение (**Only the computers and sites listed below**)

Communications (протоколы и порты) – На этой закладке задаются номера портов и типы протоколов соединений. В этом правиле мы видим, что заданы порты 137,138 и протокол UDP.

Tracking (отслеживание) – Если включить опцию **Create an event log entry** (записать событие в журнал), то будет происходить следующее. Если входящее соединение соответствует заданным условиям, то запись об этом событии будет занесена журнал событий, что бывает весьма полезно.

Description (описание) – Собственно, имя правила.

Итак, в целом, что же у нас за правило? А правило такое: Запрещать входящие соединения от любых компьютеров на портах 137 и 138, протокол UDP, событие не регистрировать в журнале.

Теперь жмём Cancel.

Как я уже говорил, у меня ADSL-подключение. Я не хочу, чтобы кто-то подключался к моему ПК. Я отключу все правила в списке (рис.9), оставлю только правило **Default inbound loopback** и добавлю ещё одно правило **Deny All.**

Учтите, что порядок следования правил очень важен! Я собираюсь создать правило **Deny All**, которое будет запрещать любые входящие соединения, оно должно идти самым последним. Для изменения следования правил есть кнопки **Move Up** (переместить вверх) и **Move Down** (переместить вниз).

Итак, чтобы добавить правило, нажимаем кнопку **Add** и задаём следующие условия: **Block**, **Connections From other computers, Any Computer, The protocol you want block** ставим **All,** не включаем протоколирование этого правила, имя правила **Deny All**.
После ввода имени правила, открывается окно с полным описанием созданного правила и есть кнопка **Finish.** Жмём её. Теперь у нас есть наше собственноручно созданное правило, которое должно стоять самым последним в списке созданных правил. Любые другие правила должны стоять выше его. Вообще, всегда при построении правил брандмауэра, лучше всего создать глобальное запрещающее правило, а потом по необходимости добавлять разрешающие правила.
Таким же образом создаются правила для конкретных программ в **Program Control**. Единственное отличие в том, что NAV предлагает либо автоматически сконфигурировать доступ (рекомендуется), либо запретить/разрешить весь доступ или сконфигурировать правила вручную.
Следующая кнопка **AutoBlock** (автоблокировка атакующего компьютера). Можно нажать эту кнопку и посмотреть, что там интересного. По умолчанию автоблокировка включена. Смысл этой функции в следующем, если атакующий выполнит определённые действия, то NAV заблокирует соединение с атакующим на 30 минут (интервал можно изменять). Следующую попытку атаки можно будет повторить с этого IP-адреса только через 30 минут. Функция, что говорится, палка о двух концах. Примером вредоносного действия можно считать сканирование портов. Да, действие вредное, сканируя Вашу систему на наличие открытых портов, злоумышленник, таким образом, проводит подготовительные действия для атаки. Но с другой стороны, некоторые провайдеры тоже сканируют порты на машинах клиентов (зачем они это делают – непонятно, вполне возможно, что ищут противоречащие договору предоставления услуг вещи (прокси, open relay)), в таком случае есть шанс заблокировать всяческие соединения с сервером провайдера и остаться без интернета ☺ Для разблокировки заблокированных IP-адресов предназначены кнопки **Unblock** (снять блокировку с одного IP) и **UnblockAll** (разблокировать всех). Моё мнение, лучше эту опцию отключить.
Осталась опция **Turn on Browser Defender** (включить защиту браузера). – Если включена данная опция, то NAV проверяет браузер Internet Explorer версий 6 и 7 на наличие уязвимостей, даже неизвестных. Для тех, кто пользуется данным браузером – включить!
Переходим к разделу **Manual scanning** (ручное сканирование). В этом разделе доступен только один подраздел **General settings** (общие настройки). Рассмотрим, какие опции нам доступны.
Scan within compressed files (сканировать сжатые файлы) – Включение данной опции увеличит время сканирования запущенного вручную, потому что начнут проверяться файлы в архивах. С учётом быстродействия современных ПК эту опцию можно оставить включенной, дополнительная безопасность не помешает.
Scan active programs and start-up files (сканировать запущенные программы) – Оставляем включённой. При запуске ручного сканирования NAV проверит все запущенные программы и процессы, а также все файлы, которые с ними связаны.
Turn on SONAR scan (включить SONAR сканирование) – Название этой опции для меня вначале было совершенно непонятным и ассоциировалось как нечто среднее между ГЛОНАСС и СОИ. Пришлось лезть в справку по NAV и смотреть, что же это за опция такая военная. Разгадка оказалась простой, SONAR – Symantec Online Network for Advanced Response (звучит, правда, как глобальная инициатива превентивного удара ☺) обеспечивает защиту на основе поведения, способную обнаруживать новые шпионские программы и вирусы еще до появления традиционных определений на основе сигнатур. Нечто похожее на эвристический анализатор, но с более широкими возможностями. Говоря современным языком – проактивная защита. Собственно, грозное название соответствует поставленным задачам. Оставляем включённой.
Turn on keylogging detection (включить обнаружение кейлоггеров) – Эта опция должна быть включена. Кейлоггеры – маленькие вредные программы, которые перехватывают вводимую с клавиатуры информацию и отправляют её нехорошим людям. Одно дело, если перехватили Ваше послание турецкого султана, а другое – если это был пароль на Ваш почтовый ящик, платёжный счёт и др.
Scan for rootkits and other stealth items (включить обнаружение руткитов и других замаскированных объектов) – Опция полезная со всех сторон, просто обязана быть включена.
Краткая справка, Rootkit (руткит, от англ. root kit, то есть «набор root'a») — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе. В наше время, всё больше заразы старается попасть на ПК и мало того что натворить гадостей, да ещё и спрятаться так, чтобы никто не нашёл, ни пользователь, ни антивирус. Вот эта опция как раз и предназначена для обнаружения скрытых вредоносных процессов в Вашей системе, дабы

доблестный NAV смог найти хулигана, вытащить его на свет божий и бить ногами до потери сознания подозреваемого ☺.

Scan for tracking cookies (включить обнаружение печенюшек ☺) – Что такое печенюшки?

Cookie – это небольшая порция текстовой информации, которую сервер передает браузеру. Сами по себе cookies не могут делать ничего, но когда пользователь обращается к серверу (набирает его адрес в строке браузера), сервер может считывать информацию, содержащуюся в cookies, и на основании ее анализа совершать какие-либо действия. Например, в случае авторизованного доступа к чему-либо через веб, в cookies сохраняется логин и пароль в течение сессии, что позволяет пользователю не вводить их снова при запросах каждого документа, защищенного паролем.

На всякий случай, пусть эта опция будет включённой.

Раздел **Exclusions** (исключения).

Подраздел **Scans** (сканирования) – В этом разделе задаются пути к файлам и папкам, которые не должны проверяться антивирусом не при каких обстоятельствах. Исключения вещь хорошая, есть программы, такие как Radmin, которые могут использоваться со злым умыслом, но прямой угрозы они не несут, всё зависит от того, кто их использует. Если у Вас установлен Radmin и Вы точно знаете, что это Вы его ставили (ну мало ли зачем он Вам понадобился), то Вам придётся добавлять в исключения файлы Radmin, иначе он будет безжалостно пристрелен антивирусом. Смотрим рис.11

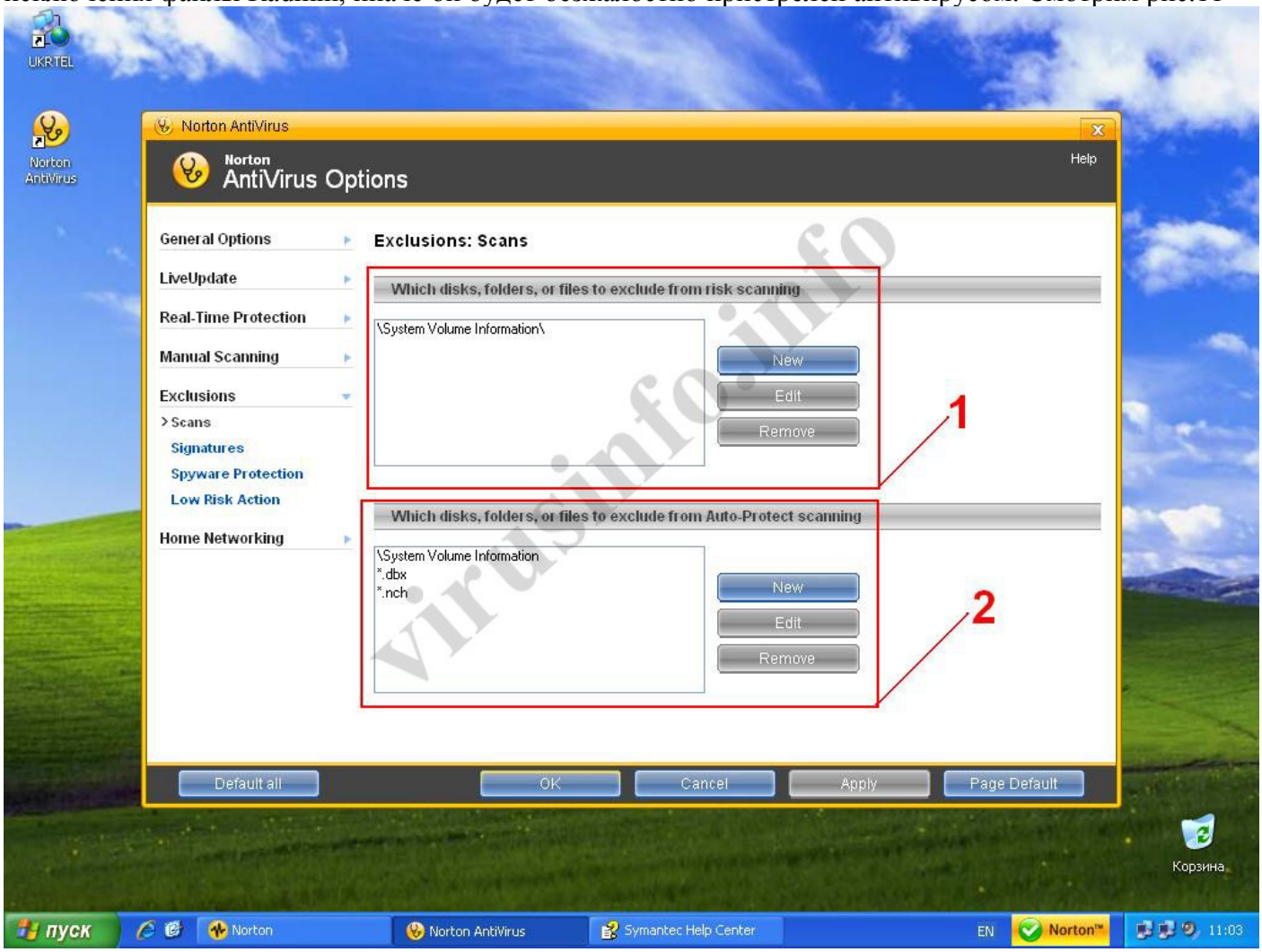

Рис.11

В окне (1) задаются пути к файлам и папкам, которые не должны проверяться антивирусом при ручном сканировании. В окне (2) задаются пути к файлам и папкам, которые не должны проверяться резидентным монитором. Для создания, изменения и удаления исключений предназначены кнопки New, Edit, Remove соответственно. Видно, что в исключениях присутствует папка System Volume Information. По-хорошему, эту папку надо удалить из исключений, потому что в ней очень часто любят селиться зловреды. Для того чтобы удалить исключение, надо его выделить и нажать кнопку Remove.

Следующий подраздел, **Signatures** (сигнатуры) – Вот тут я уже удивился. Оказывается в NAV можно задавать в исключения сигнатуры зловредов! (не всех правда, но список внушительный). Смотрим рис.12

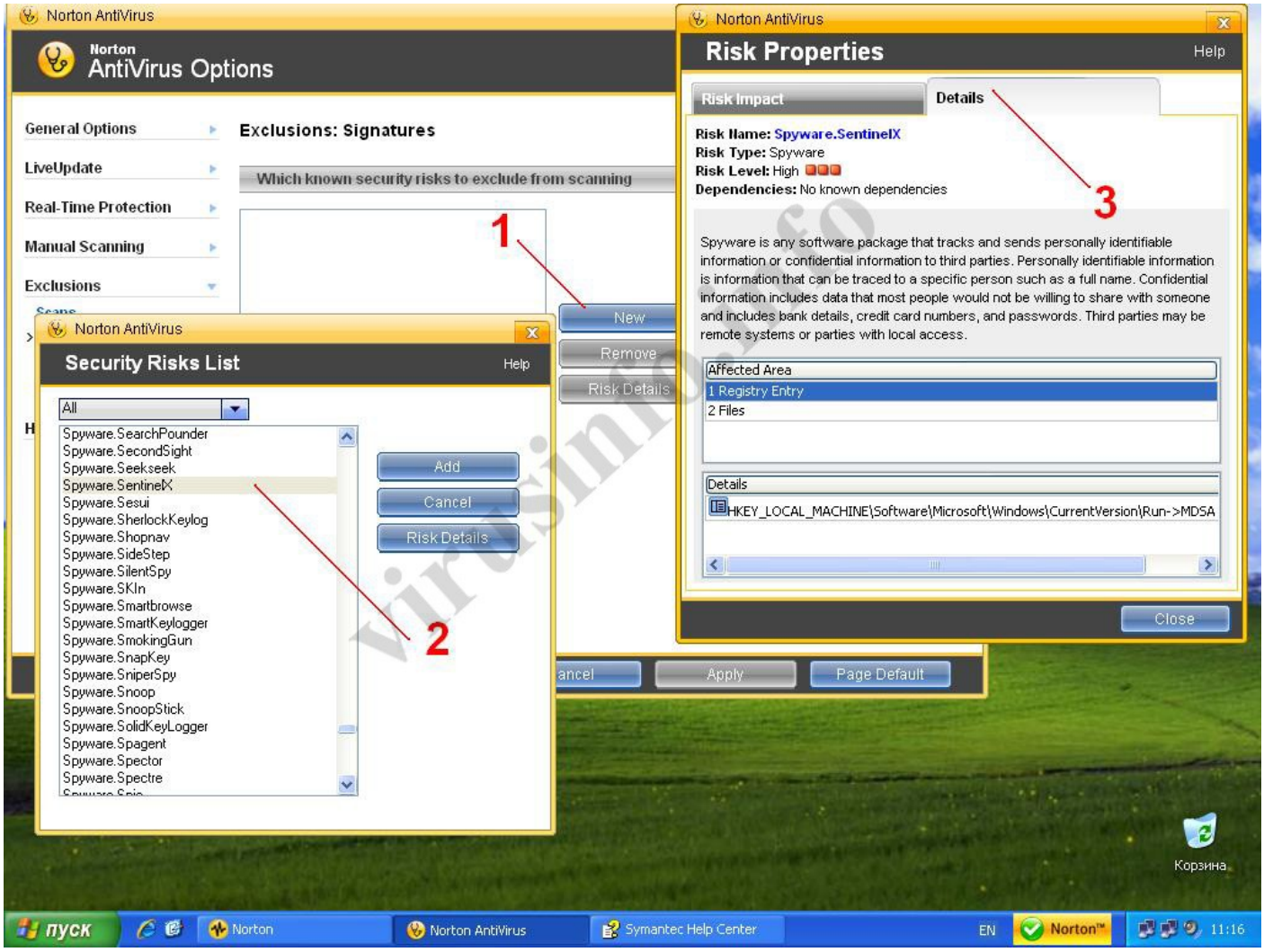

Рис.12

Нажав кнопку New(1), открывается список сигнатур, в котором мы можем выбрать интересующую нас (2). Если нажать кнопку Risk Details, то откроется окно, в котором мы можем просмотреть детальную информацию о выбранном зловреде (3).

Лучше всего не добавлять в исключения никаких сигнатур, пусть этот список будет пустым. Причина добавления сигнатуры в исключения должна быть ну очень специфичной.

Подраздел **Spyware Protection** (защита от Spyware) - Spyware - это мониторинговый программный продукт, установленный и применяемый без должного оповещения пользователя, его согласия и контроля со стороны пользователя, т.е. несанкционированно установленный. Именно в этом узком смысле термин Spyware (англ. Spy — шпион и англ. (Soft)ware — программное обеспечение) соответствует своему дословному переводу, т.е. шпионское программное обеспечение.

В этом подразделе перечислены виды Spyware, которые может обнаруживать NAV. Желательно, чтобы все галочки были установлены, пусть NAV детектирует все виды Spyware.

Подраздел **Low-Risk Action** (реакция на угрозы низкого уровня опасности) – У нас есть три варианта, что делать с угрозами низкого уровня опасности (угрозы среднего и высокого уровня опасности будут удаляться автоматически). По умолчанию стоит **Ask me what to do** (запрос о действии). Можно так же выбрать **Automatically remove low-risk items** (прибить не спрашивая) и **Always ignore low-risk items** (всегда игнорировать угрозы такого класса). Оставляем значение по умолчанию, пусть NAV предупреждает нас, а там мы сами разберёмся чего делать.

Последний раздел в настройках это **Home Network** - дает возможность видеть подключенные устройства на схеме локальной сети. Также эта функция следит за состоянием безопасности компьютеров, на которые установлен Norton AntiVirus 2008 или Norton Internet Security 2008. Собственно здесь ничего не трогаем. Нам эти функции не нужны.

Вот, с настройками разобрались. Как видим, «гаек» в NAV предостаточно. Стоит отметить, что настройки по-умолчанию являются весьма оптимальными и эффективными. Пользователям, которые любят залазить под капот, хватит работы ☺

Теперь вернёмся к рис.9 и перейдём к разделу **Tasks&Scans** (Задания и сканирование). Есть три подраздела.

Первый из них это **Run a scan** (запустить сканирование). Посмотрим на рис. 13

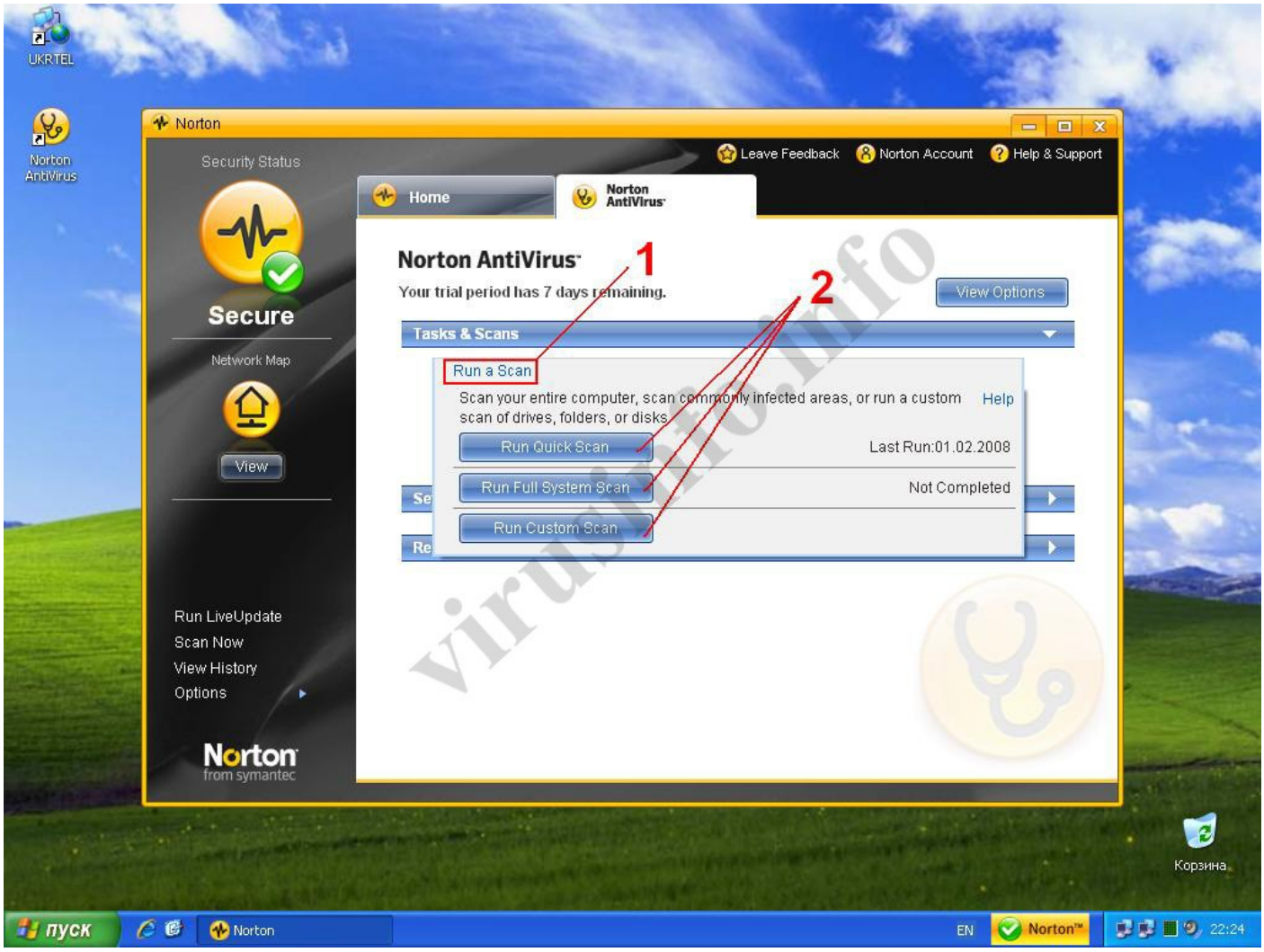

Рис.13

При нажатии на (1) открывается меню с тремя кнопками:

Run Quick Scan (запустить быстрое сканирование) – Проверка критически важных областей системы.

Run Full System Scan (запустить полное сканирование системы) – Ну тут, я думаю всё понятно.

Run Custom Scan (выбор областей проверки вручную) – При нажатии этой кнопки откроется меню, в котором мы можем выбрать, что именно мы хотим сканировать: диск, несколько папок, отдельный файл. (рис.14)

Рис.14

После чего остаётся лишь нажать кнопку Scan.

В подразделе **Shedule a Scan** (запланировать сканирование) можно задать выполнение проверки по расписанию. Это может быть или полная проверка компьютера или же выборочная (к примеру проверка диска С по пятницам в 12:30).

Подраздел **Manage Quarantined Items** (управление объектами, помещёнными на карантин).

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 можно указать, чтобы файл был удалён с диска, дабы никто не смог его случайно открыть или запустить. Данные из карантина можно восстановить, что тоже весьма полезно. Итак, нажимаем **Manage Quarantined Items** и затем кнопку **Go To Quarantine**, смотрим на рис. 15

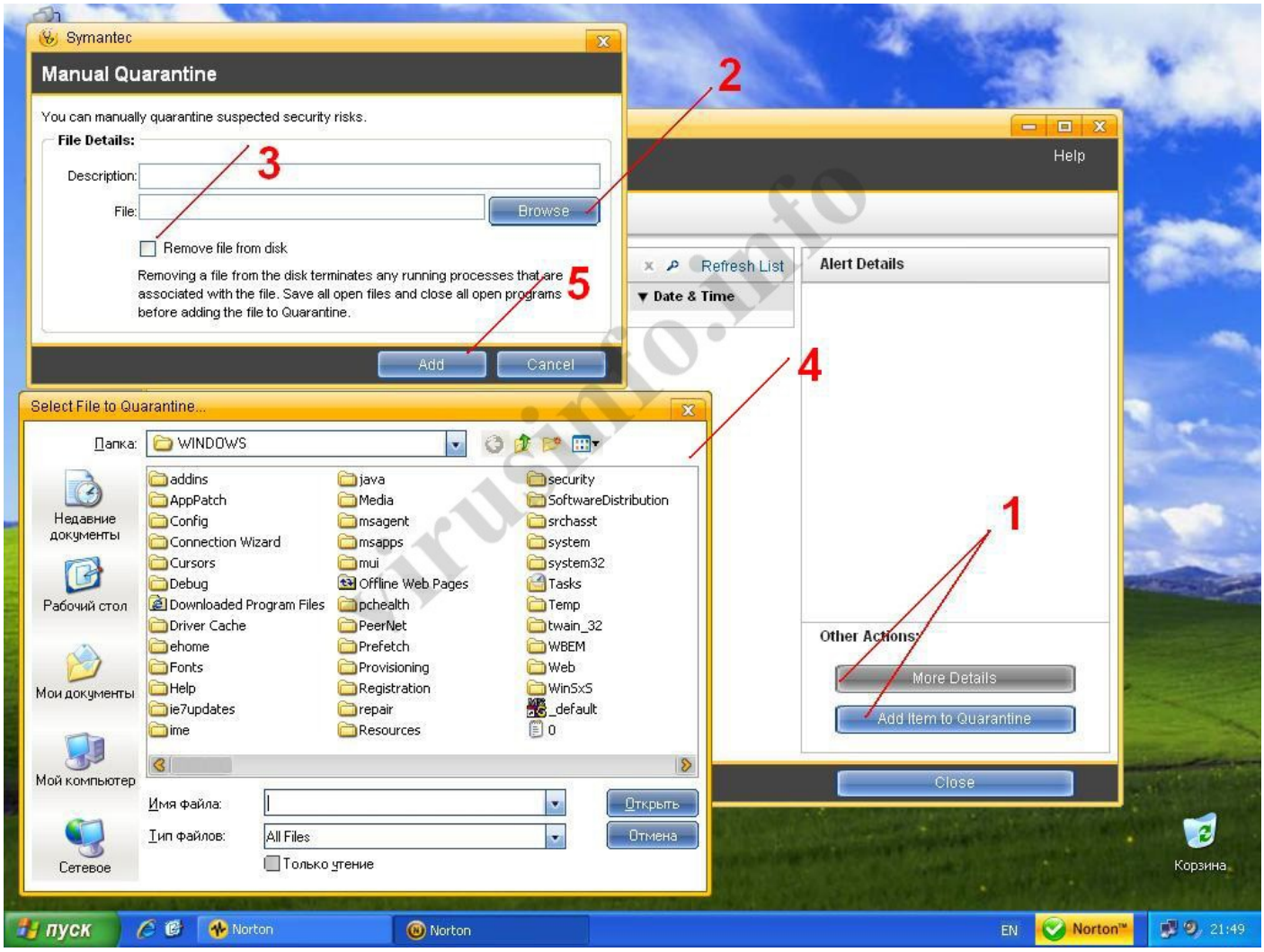

Рис.15

На данный момент у меня карантин чист, там ничего нет. Обратим внимание на две кнопки (1) **More Details** (детально) и **Add Item to Quarantine** (добавить объект на карантин). При условии, что в карантине что-то есть, будет активна кнопка **More Details,** при нажатии на которую, можно будет просмотреть детальную информацию о помещённом на карантин объекте.

Кнопка **Add Item to Quarantine** предназначена для добавления в карантин объектов вручную. При нажатии этой кнопки открывается окно, в котором можно выбрать объект, для просмотра дерева каталогов предназначена кнопка **Browse** (2). Также можно указать, чтобы файл был удалён с диска, для этого надо поставить галочку в (3). После чего в окне (4) выбираем нужный нам файл, затем жмём кнопку **Add** (5). У нас есть объект в карантине. Что же можно с ним сделать? А сделать с ним можно следующее, выделяем наш объект, жмём кнопку **More Details** и смотрим рис.16

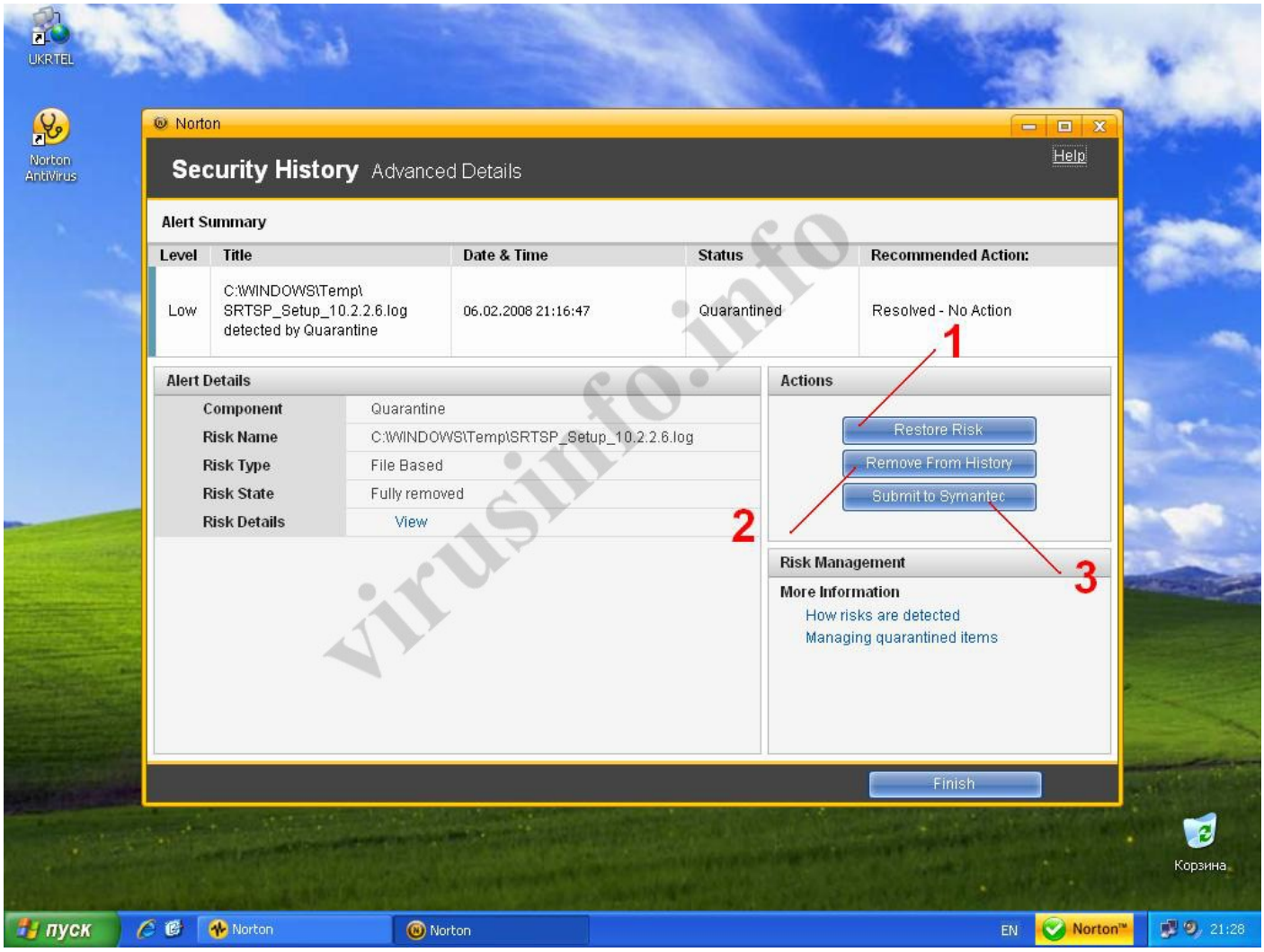

Рис. 16

Как видно, о каждом объекте в карантине можно просмотреть детальную информацию.

Restore Risk (1) (восстановить) – Нажатие кнопки приведёт к восстановлению объекта в его исходное месторасположение.

Remove From History (2) (удалить из истории) – удалить объект из карантина, удалённый объект восстановить нельзя.

Submit to Symantec (3) (отправить в Symantec) – очень полезная кнопка. Если Вы подозреваете, что объект заражен, или Вы поместили на карантин вирус, который Norton ещё не знает, то Вы можете отправить файл прямо в лабораторию Symantec. Специалисты исследуют его и если объект действительно несёт угрозу, то его сигнатура будет добавлена в антивирусные базы.

Переходим к последнему разделу - **Reports & Statistics** (отчёты и статистика) (см. рис.7)

Доступно два подраздела: **View Activity Log** (просмотр журнала событий) и **View Online Virus Encyclopedia** (просмотр онлайновой вирусной библиотеки).

Начнём с **View Activity Log** – Вот то, что мне всегда особенно нравилось в NAV. Ребята из Symantec правильно решили, что журнал событий должен хранить и отображать всю информацию, которая проходит через NAV. Отчёты о событиях подробны, но не перегружены лишними данными. Многие подумаю «в пень эти отчёты», но я скажу, Вы не правы! Благодаря хорошей системе отчётов можно проконтролировать правильно ли работает защита, установить причину, почему не работает какая-то программа, которой нужен доступ в сеть, что за вирусные события были (возможно, кто-то из членов семьи случайно попытался подцепить заразу, но Вам об этом не сказал). Да мало ли чего.

Смотрим на рис.17

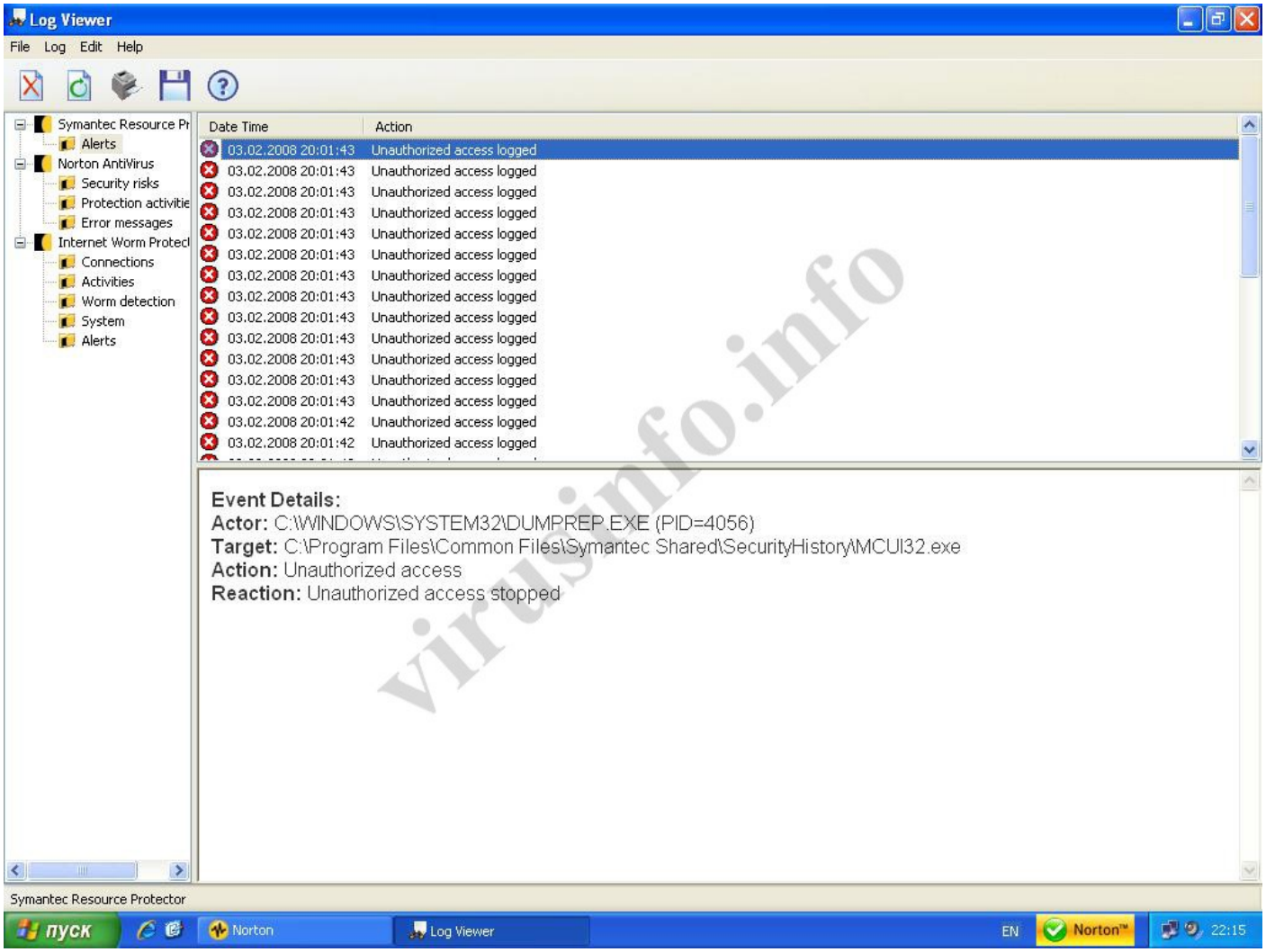

Рис.17

Журнал событий поделен на три части со своими подразделами: **Symantec Resource Protector** (запись событий о неавторизованном доступе к процессам и модулям NAV), **Norton Antivirus (**запись событий об обнаруженной заразе, результатах сканирования и ошибках в работе**)**, **Internet Worm Protector** (все, что касается работы брандмауэра).

Как видно на рис.17, зафиксирована попытка неавторизованного доступа к процессу NAV MCUI32.exe со стороны процесса DUMPREP.exe. Попытка доступа заблокирована.

Если посмотрим записи **Security Risks** (угрозы безопасности) (рис.18), то увидим (1), что 06.02.2008 в 20:20 был пойман и пристрелен (выполнено действие **Blocked**) лютый вирус, под названием Trojan.Horse (2), вдобавок приведена ссылка на описание этого вируса в вирусной библиотеке (2).

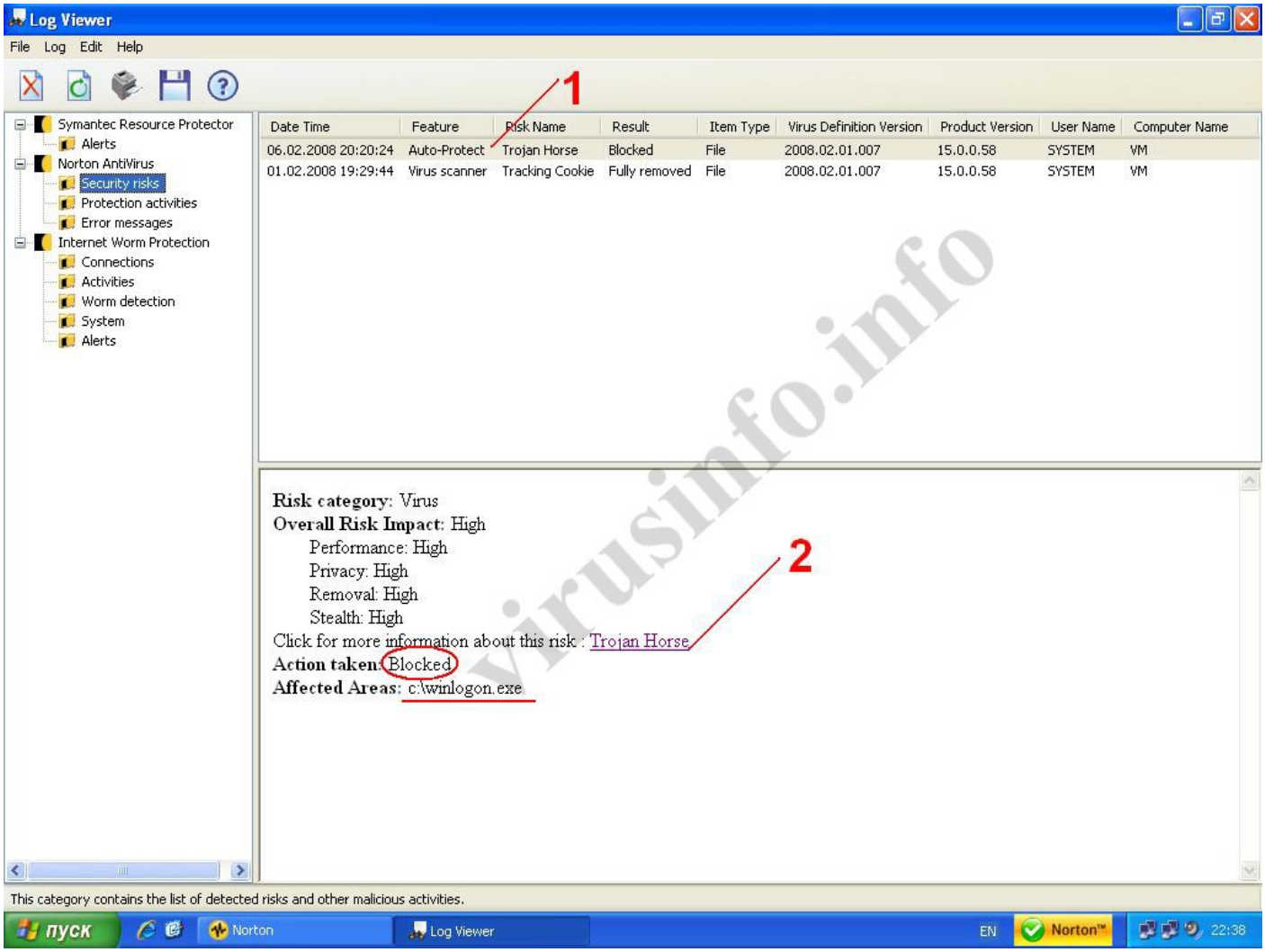

Рис.18

Также указан путь к файлу, который оказался вирусом.

На данный момент это всё по данному продукту. Возможно, я упустил некоторые детали (скорее всего это так, но существенными они не будут). Как всегда, замечания - учитываются, конструктивная критика – приветствуется. Человеков с красными глазами и лозунгом «Нортон - ацтой», просьба не беспокоить. Есть люди интересующиеся, данная статья предназначена им. Обсуждение статьи будет вестись на портале virusinfo.info.

Отдельное СПАСИБО команде портала virusinfo.info, которые участвовали в обсуждении статьи.