

Пошаговые Руководства
Сам Себе Админ
системное администрирование
Microsoft Windows



Практика использования лицензионного антивируса

Приветствую, друзья! Сегодня я хочу поделиться с Вами опытом установки и использования лицензионного антивируса «Kaspersky Internet Security 2012».

Случилось так, что один человек купил себе домой лицензионный антивирус, но поскольку лицензий две, а вторая ему явно не нужна, то я решил установить этот антивирус от лаборатории Касперского и на своем домашнем компьютере. Чтобы лицензия зря не пропадала ☺

Вроде как отдельным полноценным уроком это назвать сложно: что тут такого особенного в этой теме? Но в процессе установки и ознакомления лично для себя я узнал несколько полезных вещей. Может быть, они и Вам пригодятся? ☺

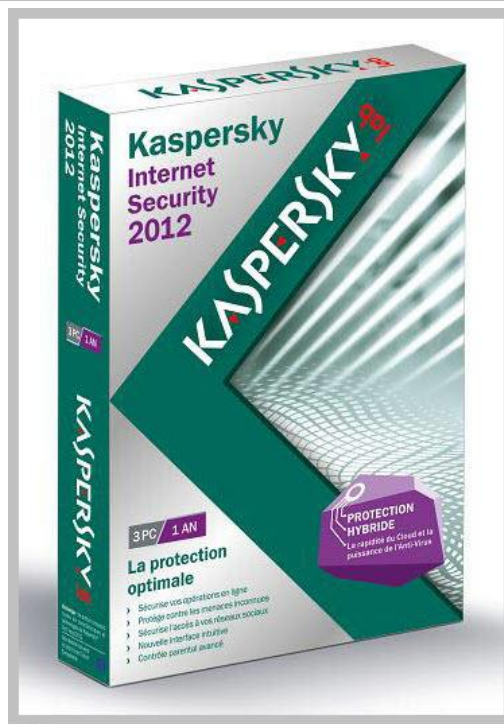
Разберем весь процесс подробно, поэтому будет много скриншотов. Для начала — ознакомимся с ценовой политикой лаборатории Касперского относительно данного программного продукта.

Так вот, наша версия стоит вот столько:



Это — в гривнах, в рублях получается что-то в районе 2200 рублей (60 долларов).

Теперь, о внешнем виде нашего антивируса. Ну, понятно, что за такие деньги по крайней мере упаковка должна быть красивой ☺ Вот что мы имеем снаружи:



Распечатываем коробку и видим, что внутри находится сам диск с антивирусом и бумажное руководство пользователя, на которое наклеен стикер с ключом активации.

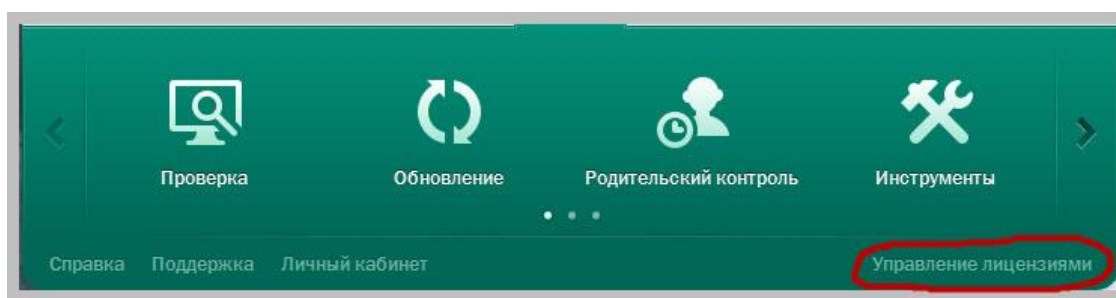


Сам диск также выглядит достаточно внушительно!

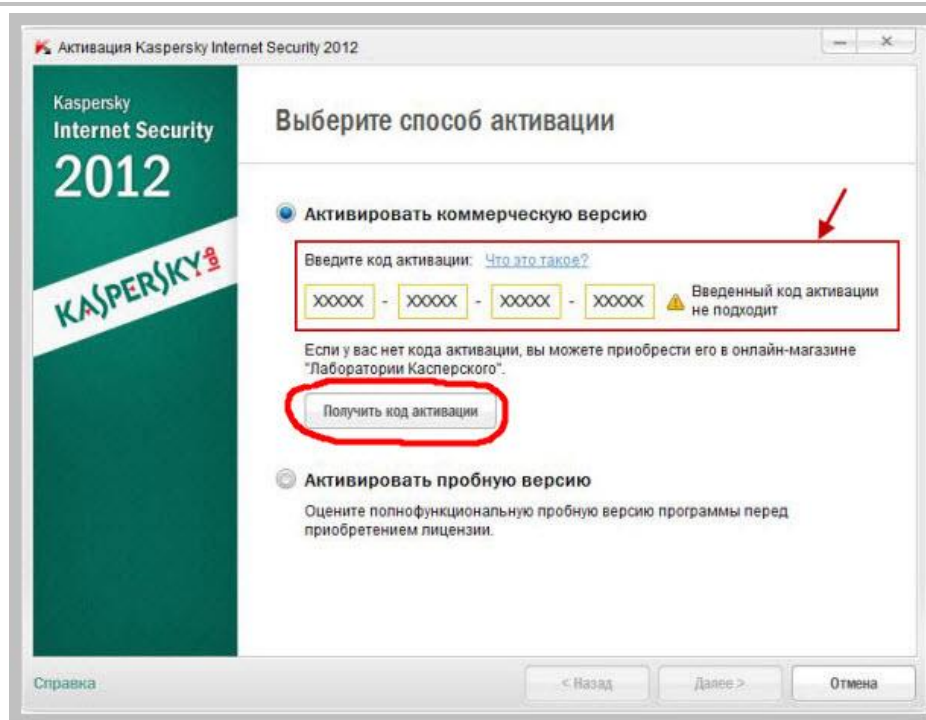


Итак, вставляем диск в привод для оптических дисков, бегло (из любопытства) пробегаем глазами руководство пользователя и приступаем к установке антивируса.

После завершения процесса в первую очередь, как и положено, пытаемся активировать продукт с помощью оригинального серийного номера. Сразу скажу, что выход в Интернет из дома у меня осуществляется напрямую (без прокси, фаервол доступ к сети для Касперского не блокирует). Заходим в раздел программы, где мы можем ввести лицензионный ключ в специальные поля. Туда можно попасть из главного окна программы, нажав на ссылку «Управление лицензиями» в правом нижнем углу.



Нажимаем и... сталкиваемся вот с такой неприятностью:



Буквально – «введенный код активации не подходит». Странно видеть подобное в случае с официально купленным продуктом, но что поделаешь? Перепроверил вводимые данные и начал искать альтернативный вариант.

Кнопка «Получить код активации» ведет нас в Интернет-магазин лаборатории Касперского и это нам не подходит. Немного “осмотревшись” на сайте производителя, находим ссылку на форму получения от лаборатории Касперского специального активационного файла, с помощью которого можно активировать данный программный продукт в автономном режиме, без подключения к Интернету.

Добро пожаловать на страницу активации продуктов Лаборатории Касперского! Для начала процедуры активации продукта, пожалуйста, введите ваш код активации в поле "Activation Code".
Если Вы уже являетесь нашим зарегистрированным пользователем, пожалуйста, укажите дополнительно Ваш идентификатор (Номер клиента) и пароль. В этом случае шаг 2 будет пропущен.

Замечание: настоятельно рекомендуем вам использовать в качестве браузера **Internet Explorer**, так как при использовании альтернативных браузеров могут возникнуть проблемы с получением ключевого файла к вашему продукту Лаборатории Касперского

Код Активации	<input type="text"/>
Номер клиента	<input type="text"/>
Пароль	<input type="text"/>
Если у Вас еще нет Номера клиента, то необходимо ввести только код активации.	
Введите изображенную на картинке надпись	<div>4 6 8 w</div> <input type="text" value="468w"/>
<input type="button" value="Дальше"/>	

Здесь в поле «Код активации» вводим наш номер с коробки (номер клиента и пароль указывать не нужно), вводим капчу (проверочные цифры с картинки) и нажимаем кнопку «дальше».

Переходим на следующий шаг мастера получения файла:

Пожалуйста, укажите данные о себе. Собранная на этом шаге информация будет использоваться только для Вашей идентификации и общения со службами технической поддержки.	
E-mail	<input type="text"/>
User name	<input type="text"/>
Country	<input type="text"/>
<input type="button" value="Дальше"/>	

Здесь нас просят ввести наш адрес электронной почты и клятвенно заверяют, что не будут использовать его для непотребных действий ☺ Что ж, поверим!

Нажимаем кнопку «дальше» и видим вот такое окно.

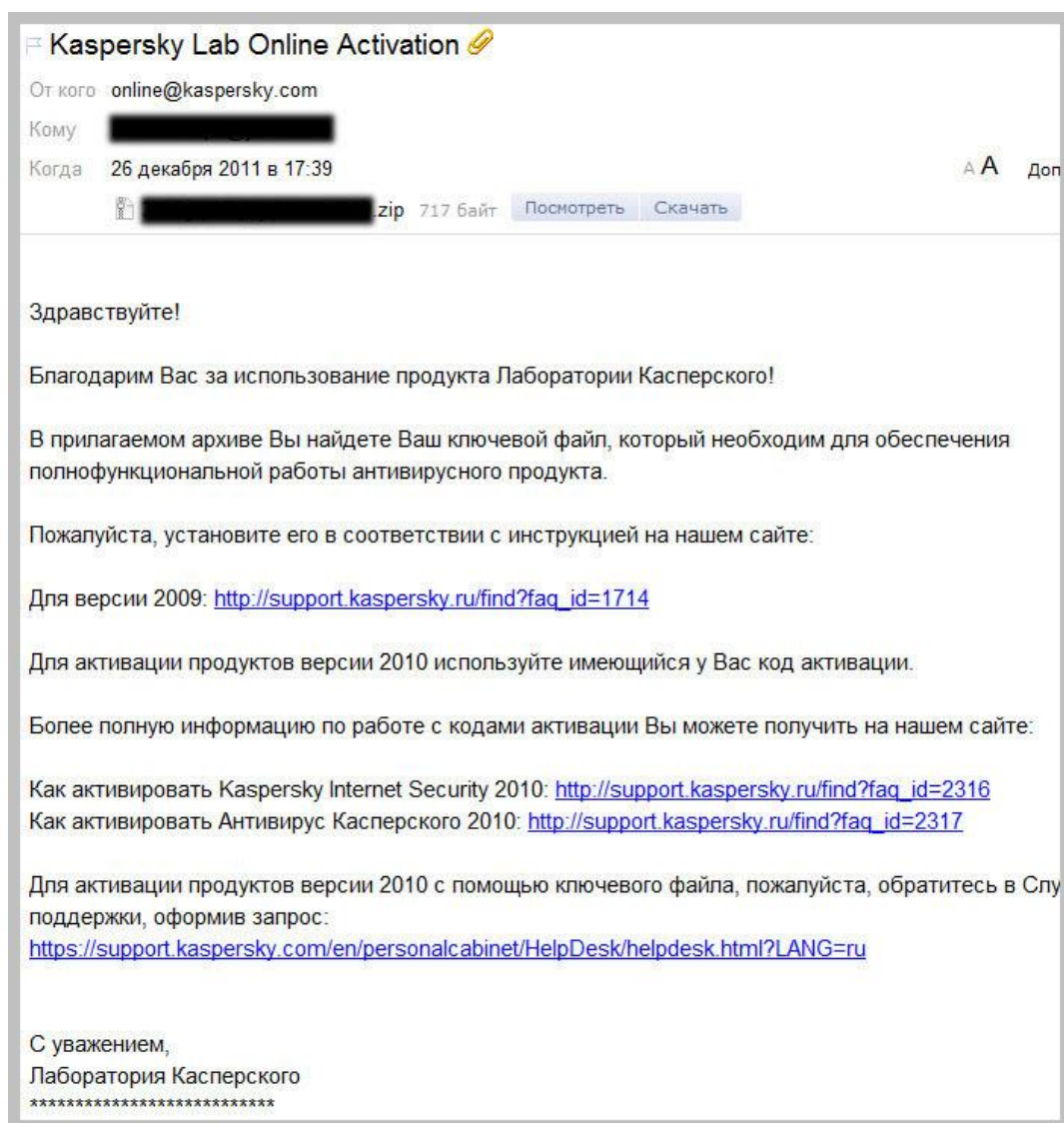
Данные отправлены

База знаний:

- [как активировать версию 2009](#)
- [вернуться на главную страницу](#)
- [перейти на страницу технической поддержки](#)

Наши данные (лицензионный ключ и почтовый адрес) получены лабораторией Касперского и на «e-mail» нам в скором времени должен будет прийти тот самый файл активации продукта.

Вот как в моем случае выглядело это письмо:

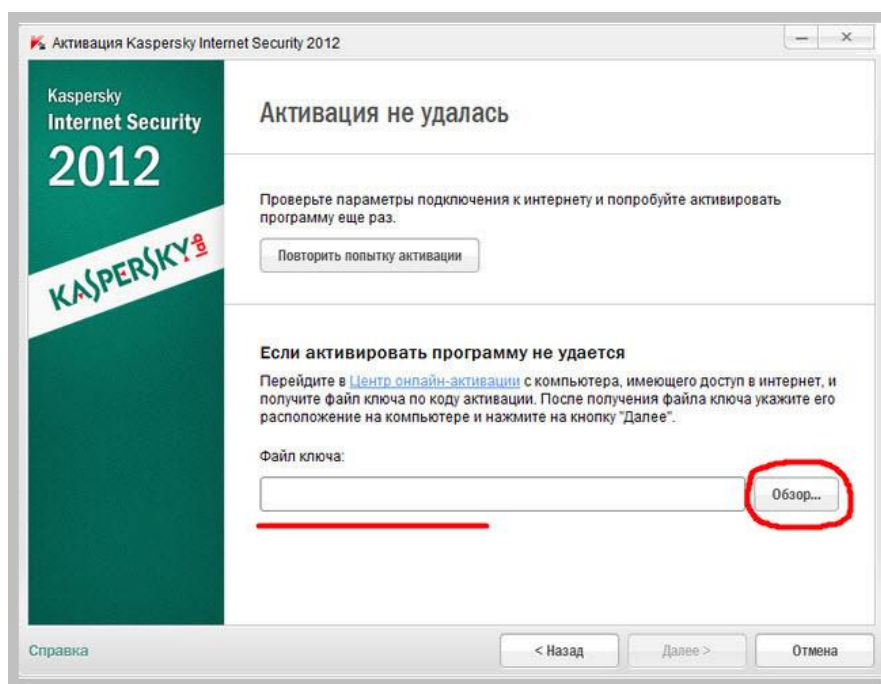


К письму прикреплен маленький «zip» файл. После скачивания на компьютер и разархивирования он оказался REG файлом (файлом данных реестра, который добавляет

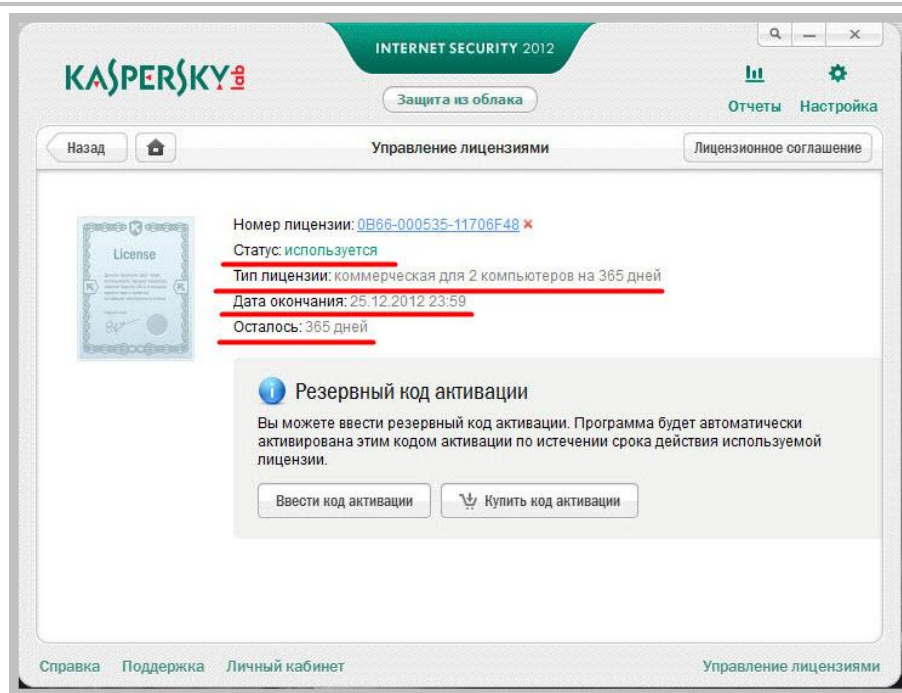
какие-то бинарные данные в системный реестр Windows). В данном случае, понятно, что данные эти касаются сроков истечения лицензии для антивируса.

Но не будем забегать вперед! Что мы имеем на данный момент? Файл реестра для активации и установленный, но не активированный антивирус. Давайте совместим эти две вещи и получим, наконец, одну нормально работающую 😊

Заходим в раздел программы, касающийся активации продукта, (ссылка «Управление лицензиями») нажимаем кнопку «Обзор» и в открывшемся проводнике выбираем скачанный нами из Интернета REG файл. После этого он появится в поле «Файл ключа».

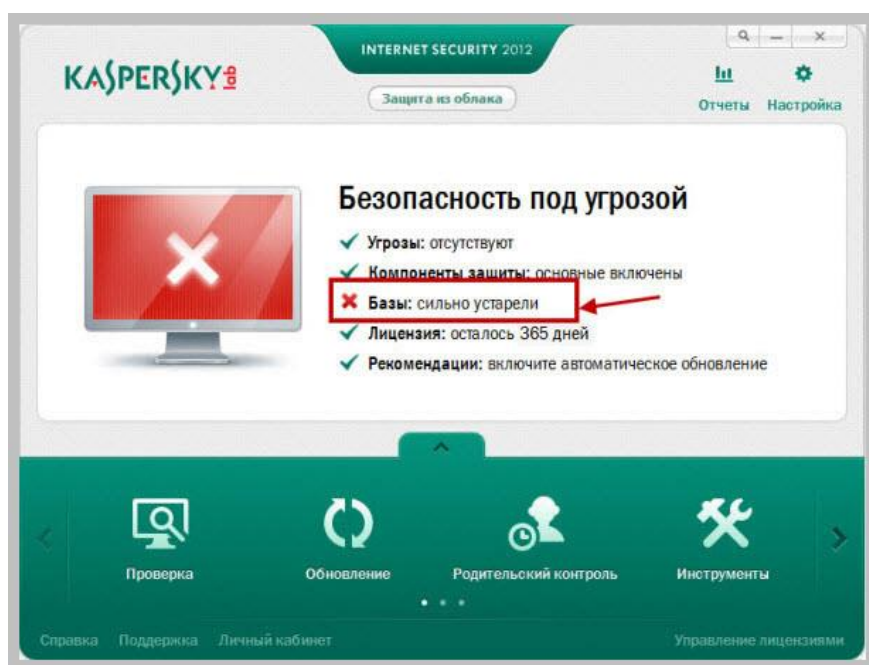


Нажимаем кнопку «Далее». И чрезвычайно радуемся тому обстоятельству, что активация прошла успешно. Мы можем убедиться в этом, посмотрев на скриншот ниже:



Статус лицензии – «используется», указана дата окончания ее действия – 25-е декабря 2012-го года и общее количество оставшихся дней до истечения срока использования.

Вроде все замечательно, но есть еще один немаловажный момент! Нам нужно теперь обновить антивирусные базы программы. На что, собственно, нам недвусмысленно и намекает сам антивирус.



И это – очень важный момент! Настолько, что я, пожалуй, остановлюсь на нем отдельно. Важно понять следующее: Какой бы ни был хороший, надежный и лицензированный антивирус он – **не сможет защитить Вас от вирусов, если его антивирусные базы устарели!** Часто почему-то бывает так: человек поставил себе

«хороший» антивирус, потом (через несколько месяцев) звонит и спрашивает почему у него компьютер плохо работает? Спрашиваешь: у тебя базы антивируса за какое число? И слышишь примерно следующее: не знаю, он ведь сам должен обновляться?!

Поймите, друзья и смиритесь с этим фактом, ☺ никому он ничего не должен (я бы сам хотел, чтобы было иначе) и если мы сами не будем контролировать этот процесс и следить за своевременным обновлением вирусных сигнатур (образцов кода, по которым программа и распознает вирусы), то и последствия заражения полностью ложатся на нас и только на нас!

Насколько часто нужно проводить обновление? Лично я у себя дома могу месяц не обновлять антивирус и считаю что это нормально (для дома). Вряд ли только что запущенный в сеть новомодный вирус успеет добраться до Вас за такое время. Другое дело – офисная корпоративная сеть. Здесь мы централизованно обновляем антивирусные базы через день, потому как очень не охота бегать потом «с мухойбойкой» по отдельным компьютерам территориально распределенной сети, если что-то вдруг да проскочит ☺

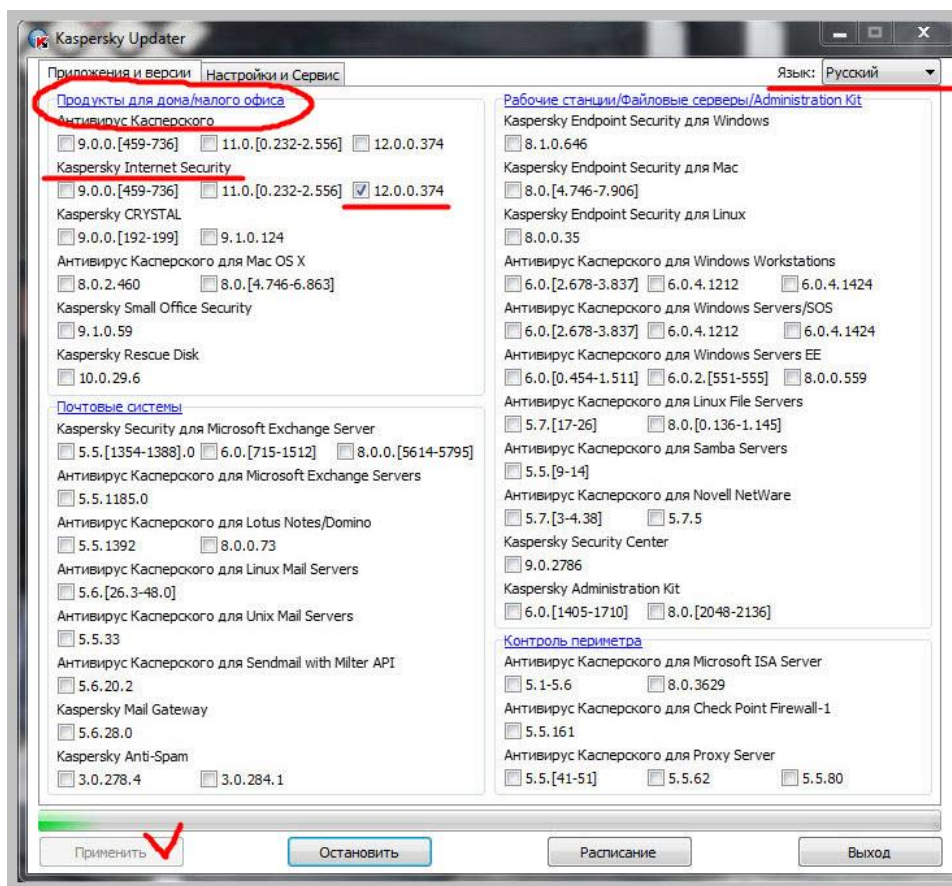
Так вот, давайте сейчас и обновим эти самые вирусные сигнатуры («зародыши» вирусов, которые программа сличает с оригиналом и на основании этого сопоставления принимает решение о том, вирус это или нет).

Конечно, обновляться напрямую из Интернета проще, я же хочу показать Вам другой вариант, освоив который Вы более наглядно увидите, как работает процесс обновления и заодно познакомитесь с очень полезной бесплатной утилитой от лаборатории Касперского. Называется она «KLUpdater».

Примечание: графический интерфейс утилиты «KLUpdater» периодически меняется разработчиками, поэтому Вы можете визуальнo увидеть другую ее версию (не такую, как на скриншотах ниже), но суть от этого не меняется. Старую версию, которую я предлагаю использовать можно скачать с нашего сайта <https://sebeadmin.thelogos.in.ua/soft/klupdater.zip> Она прекрасно работает и нравится мне больше, чем новая.

Итак, что же делает эта утилита? Она дает возможность загрузить последние обновления антивирусных баз на Ваш компьютер в отдельную папку. Причем скачать, таким образом, Вы можете обновление практически **к любому антивирусному продукту** лаборатории Касперского! В список обновления входят как продукты для дома и малого офиса, так и корпоративные серверные решения, также – антивирусы для

рабочих станций. Программа замечательна еще тем, что ее не нужно устанавливать. Просто запускаете «KasperskyUpdater.exe» и видите вот такое окно:

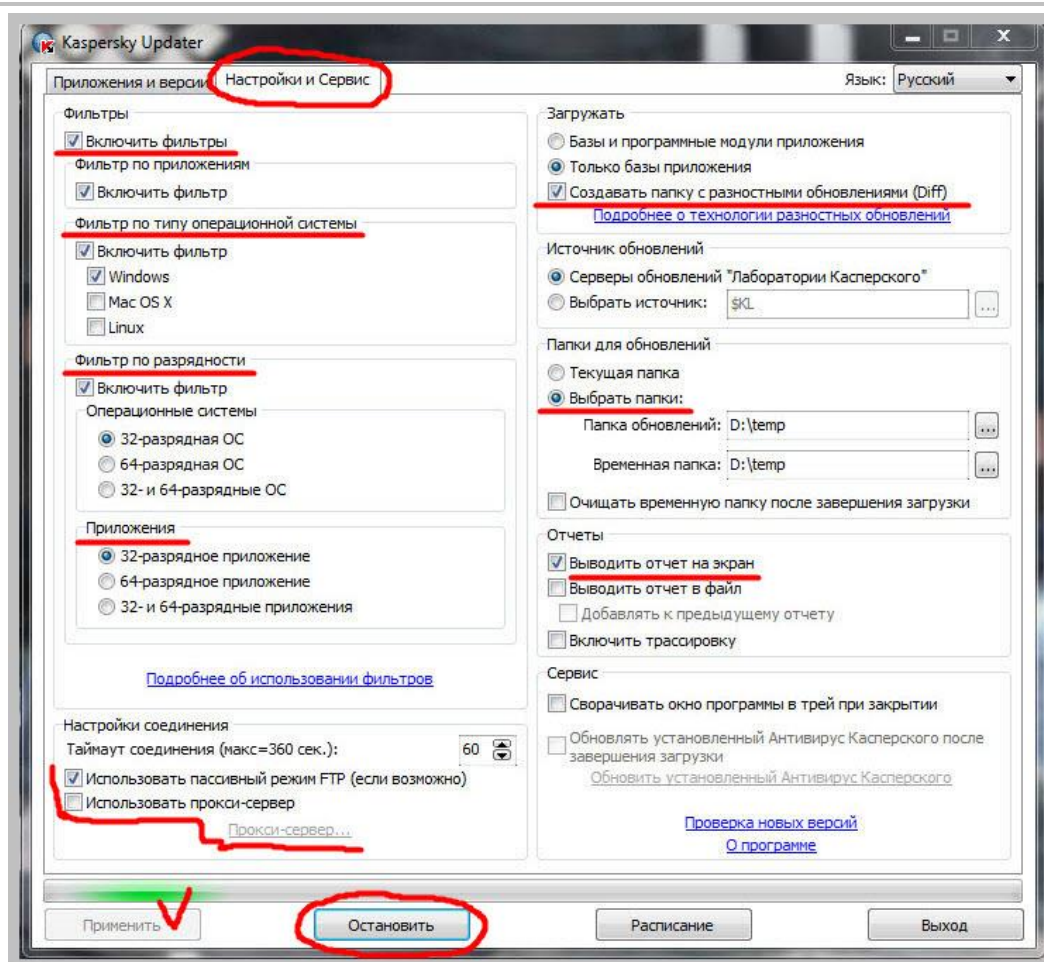


Для большей наглядности можете сразу выбрать в правом верхнем углу программы русский язык, чтобы все надписи были на русском.

Мы видим, что главное окно условно разделено на четыре части, в каждой из которых собраны продукты лаборатории Касперского, относящиеся к одному из классов. Нас будет интересовать класс «Продукты для дома/малого офиса», ведь именно к нему относится наш антивирус.

Отмечаем галочкой наш антивирус и версию, к которой мы хотим скачать обновления. Для нас это «Kaspersky Internet Security» версии «12» и нажимаем кнопку «Применить» в левом нижнем углу. Теперь программа запомнила, что мы будем скачивать обновления именно для указанного типа и версии антивируса.

Далее нам нужно будет произвести еще кое-какие дополнительные настройки. Для этого переходим во вторую вкладку программы «Настройки и сервис»



Здесь мы более тонко можем настроить параметры того, что конкретно мы будем зачислять с серверов лаборатории Касперского? Поскольку утилита может скачивать обновления к любым типам антивирусов и операционных систем, то именно здесь ей надо указать, что именно нам нужно.

Мы, конечно, можем ничего здесь и не указывать и все равно получим свое законное обновление для «Kaspersky Internet Security 2012» (мы ведь поставили соответствующую галочку в предыдущем окне), но вместе с ним мы также загрузим на свой компьютер большое количество других ненужных нам данных. Да и само скачивание будет происходить **гораздо** дольше. Вот именно чтобы этого не происходило в данной вкладке и существуют фильтры, которые призваны отфильтровать все для нас лишнее и загружать только то, что действительно необходимо.

Итак, смотрим на фото выше и разбираем важные для нас моменты. Сначала ставим галочку напротив пункта «Включить фильтры». Этим мы говорим программе, что мы адекватный пользователь и сами понимаем, что нам скачивать, а что нет ☺

«Фильтр по типу операционной системы» – «Включить». Сразу становится активной область, в которой мы можем указать, для каких операционных систем мы

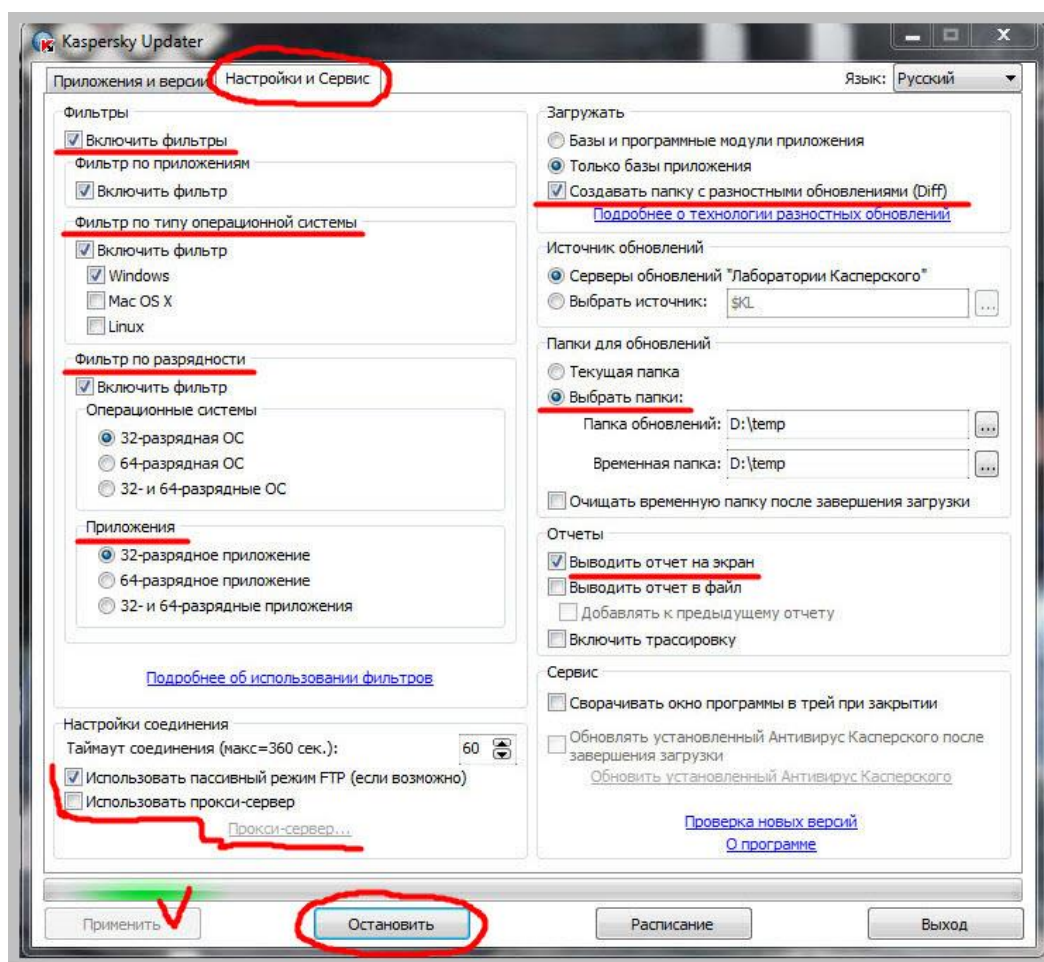
будем загружать обновления антивирусных баз: «Windows», «Mac OS X» или «Linux»? Думаю, в нашем случае – первый вариант, отмечаем его галочкой.

Следующая секция – «Фильтр по разрядности», включаем его установкой галочки и в разделе «Операционные системы» выбираем ту, которая у нас используется (32-двух или 64-ти четырех битная).

«Приложения» – 32-х разрядное (битное) приложение самого антивируса.

Ниже у нас секция, которая позволяет подключаться к серверам Касперского через прокси-сервер. Если не знаете что это такое – поставьте галочки, как показано на скриншоте и не заморачивайтесь 😊

Разберем правую сторону окна программы. Продублируем (для наглядности) еще раз скриншот, расположенный выше:



Секция «Загружать» дает нам возможность выбрать, что мы будем скачивать: базы и программные модули приложения или только сами антивирусные базы? Лично я выбрал второй вариант. Также советую Вам поставить галочку напротив пункта «Создавать папку с разностными обновлениями». Таким образом мы сэкономим сетевой трафик и время загрузки.

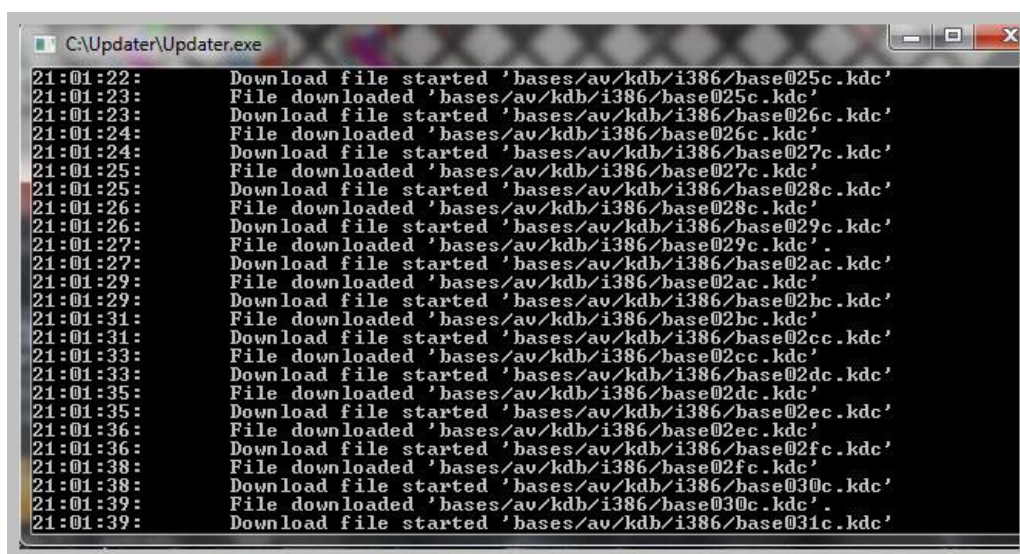
Вот что говорится на сайте лаборатории Касперского по поводу этого вида обновления: «Технология разностных обновлений, которая используется в последних версиях приложений позволяет значительно сократить трафик при обновлении антивирусных баз. Благодаря ей, если в базу была добавлена новая запись (т.е. в файл добавилась запись о новой вредоносной программе), то модуль обновления скачает не весь файл целиком, а только разницу между новым (измененным) файлом и одноименным файлом на локальной машине. Эта разница и называется "diff". После скачивания на локальной машине diff "приклеивается" (добавляется) к соответствующей базе.»

Двигаемся дальше. «Источник обновлений», понятное дело – серверы обновлений лаборатории Касперского.

Следующий пункт – важный! Здесь мы должны указать, куда мы будем скачивать обновления антивирусных баз (потом из этой папки мы будем обновлять наш антивирус). Создаем на диске произвольную папку (у меня это папка «temp» на диске «D») и выбираем ее, нажав на кнопку с тремя точками. Временную папку я указал ту же.

Галочка «Выводить отчет на экран» позволит нам визуально следить за процессом обновления, что достаточно удобно.

Вот и все! Программу мы настроили. Теперь пришло время испытать ее в действии. Нажимаем внизу кнопку «Запустить» (на скриншоте она у меня имеет надпись «Остановить», так как обновление уже запущено ☺) и видим вот такое появившееся окно:

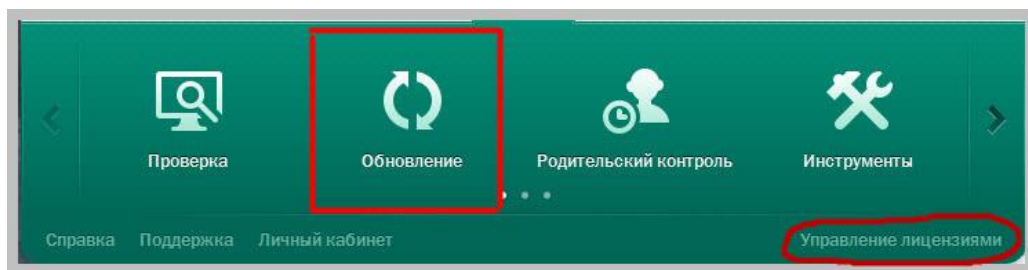


```
C:\Updater\Updater.exe
21:01:22: Download file started 'bases/av/kdb/i386/base025c.kdc'
21:01:23: File downloaded 'bases/av/kdb/i386/base025c.kdc'
21:01:23: Download file started 'bases/av/kdb/i386/base026c.kdc'
21:01:24: File downloaded 'bases/av/kdb/i386/base026c.kdc'
21:01:24: Download file started 'bases/av/kdb/i386/base027c.kdc'
21:01:25: File downloaded 'bases/av/kdb/i386/base027c.kdc'
21:01:25: Download file started 'bases/av/kdb/i386/base028c.kdc'
21:01:26: File downloaded 'bases/av/kdb/i386/base028c.kdc'
21:01:26: Download file started 'bases/av/kdb/i386/base029c.kdc'
21:01:27: File downloaded 'bases/av/kdb/i386/base029c.kdc'
21:01:27: Download file started 'bases/av/kdb/i386/base02ac.kdc'
21:01:29: File downloaded 'bases/av/kdb/i386/base02ac.kdc'
21:01:29: Download file started 'bases/av/kdb/i386/base02bc.kdc'
21:01:31: File downloaded 'bases/av/kdb/i386/base02bc.kdc'
21:01:31: Download file started 'bases/av/kdb/i386/base02cc.kdc'
21:01:33: File downloaded 'bases/av/kdb/i386/base02cc.kdc'
21:01:33: Download file started 'bases/av/kdb/i386/base02dc.kdc'
21:01:35: File downloaded 'bases/av/kdb/i386/base02dc.kdc'
21:01:35: Download file started 'bases/av/kdb/i386/base02ec.kdc'
21:01:36: File downloaded 'bases/av/kdb/i386/base02ec.kdc'
21:01:36: Download file started 'bases/av/kdb/i386/base02fc.kdc'
21:01:38: File downloaded 'bases/av/kdb/i386/base02fc.kdc'
21:01:38: Download file started 'bases/av/kdb/i386/base030c.kdc'
21:01:39: File downloaded 'bases/av/kdb/i386/base030c.kdc'
21:01:39: Download file started 'bases/av/kdb/i386/base031c.kdc'
```

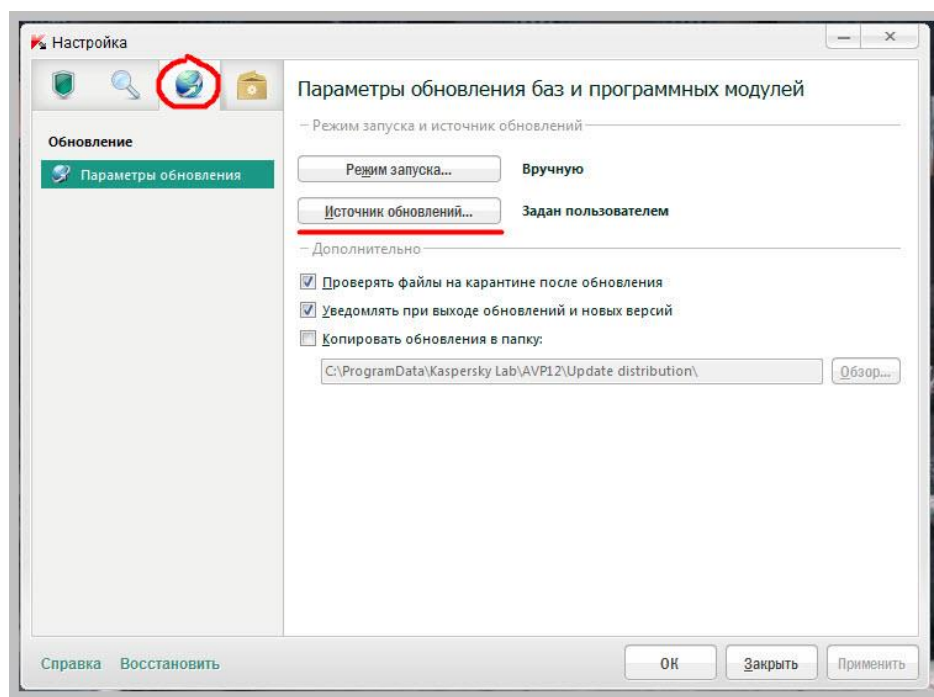
Если оно выглядит примерно так: появляются бегущие строчки с надписью «Download file started» (начало загрузки файла) и «File downloaded» (файл загружен),

значит все работает нормально – программа начала загрузку файлов с серверов обновления лаборатории Касперского в указанную нами папку на компьютере. Остается дождаться окончания этого процесса (когда окно пропадет). Это может занять от 15 до 30-ти минут. В зависимости от объема скачиваемых данных и скорости Вашего Интернет-соединения.

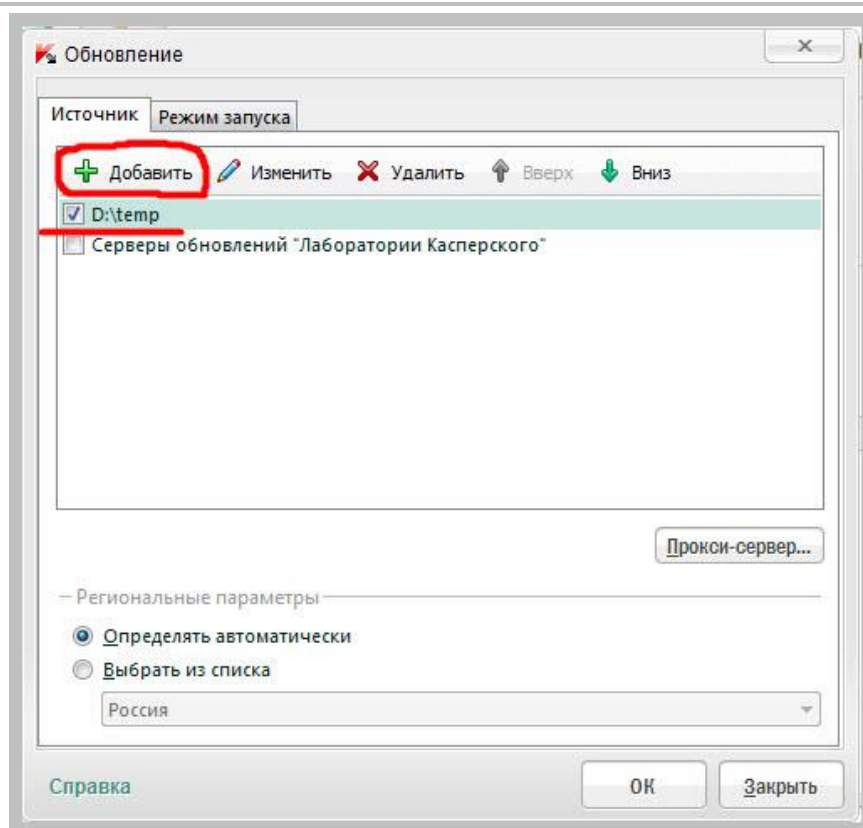
После того, как загрузка завершилась, нам надо указать нашему антивирусу, откуда брать обновления (указать ту локальную папку на нашем диске, в которую мы их сохранили). Для этого – в основном окне программы нажимаем кнопку «Обновление».



Затем – переходим во вкладку, касающуюся обновления антивирусных баз и нажимаем кнопку «Источник обновлений».



Появится еще одно окно, показанное на фото ниже:

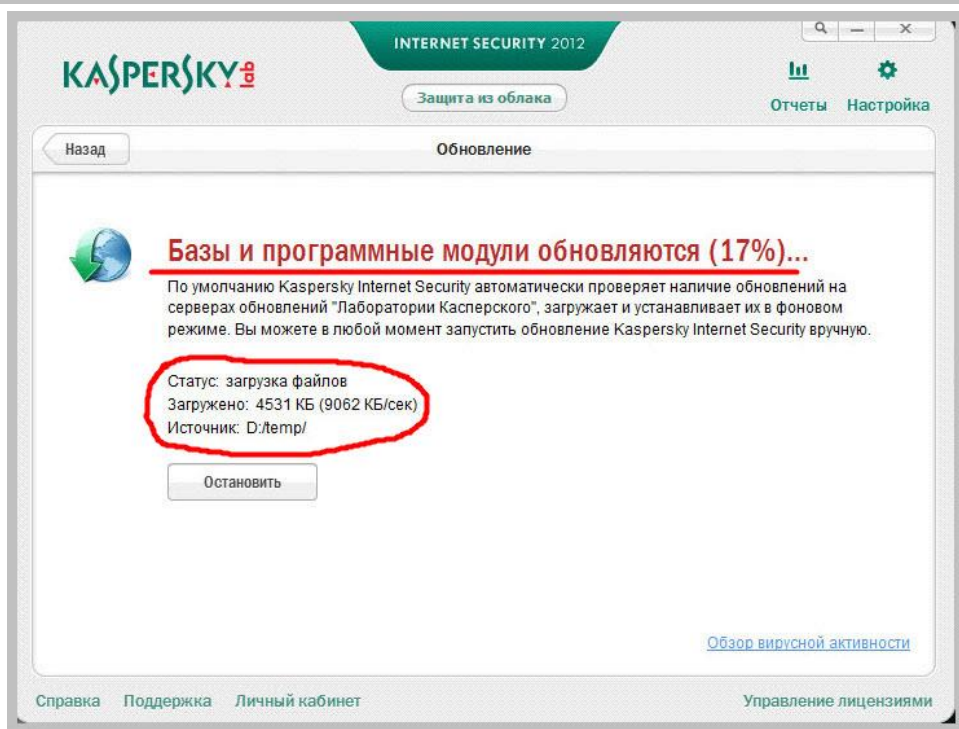


В этом окне нажимаем кнопку «Добавить» и в обзорном окне выбираем папку, в которую мы сохранили наши обновления (у меня это – D:\temp). Ставим напротив нее галочку, а галочку напротив «Серверы обновлений Лаборатории Касперского» убираем. И с помощью кнопок «Вверх» и «Вниз» перемещаем нашу локальную папку вверх списка.

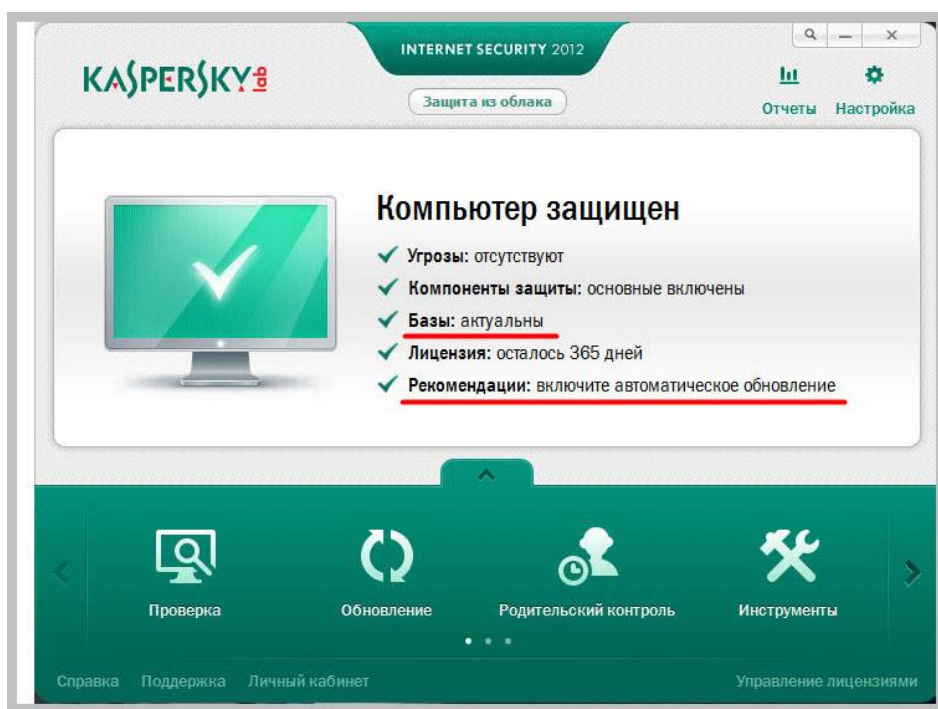
Также, перейдя во вкладку «Режим запуска», мы можем выставить опцию «Вручную» и в будущем самим решать, когда обновлять антивирус.

Вот теперь (имея сохраненные на компьютере файлы обновления антивирусных баз и настроенный на папку с ними антивирус) мы можем запустить сам процесс обновления!

Запускаем и убеждаемся в том, что процесс идет нормально:



После его завершения в главном окне программы контролируем результат обновления:



Как видим, – все нормально. Правда, нам рекомендуют включить автоматическое обновление. Но, **понимая** теперь механику его работы и **зная**, куда смотреть для контроля за этим процессом, мы можем сами составить график обновления программы (скажем, раз в две недели), скачивать базы в папку и с нее же обновляться, еще и друзьям раздавать на флешке 😊

Вот, собственно, и все что я хотел рассказать Вам относительно самого антивируса и обновления его антивирусных баз.

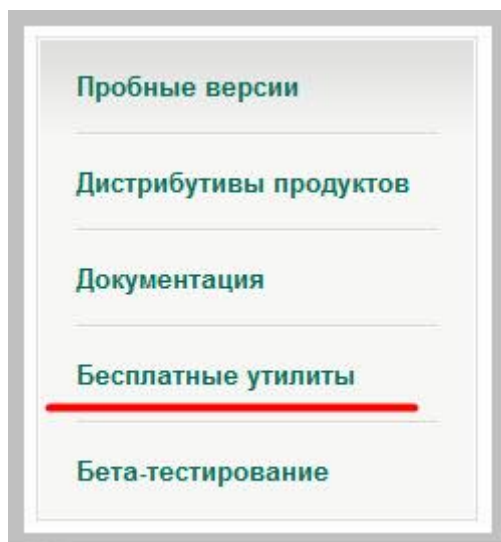
Сейчас же я хочу рассмотреть еще два инструмента от лаборатории Касперского, которые могут здорово помочь нам в случае серьезного заражения компьютера. Это – «Kaspersky Rescue Disk» и «Kaspersky Virus Removal Tool».

Сразу скажу, что загрузить их можно совершенно бесплатно с официального сайта. Причем «Kaspersky Rescue Disk» (диск спасения Касперского) можно создать прямо в нашем антивирусе. Единственный нюанс – нам перед этим придется скачать его образ с родительского сайта.

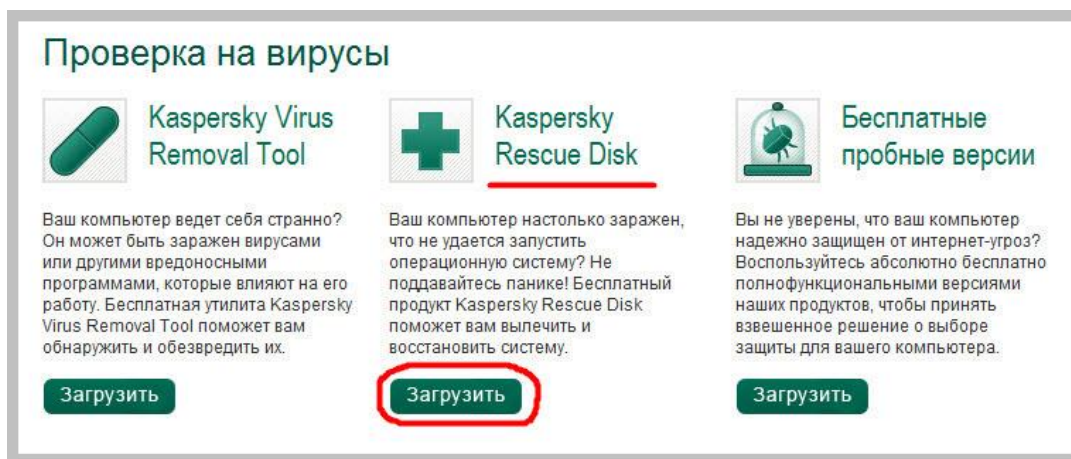
Но, давайте все по порядку 😊 Заходим на сайт разработчика ПО и ищем раздел «Загрузить».



Дальше в левом боковом меню выбираем «Бесплатные утилиты»:



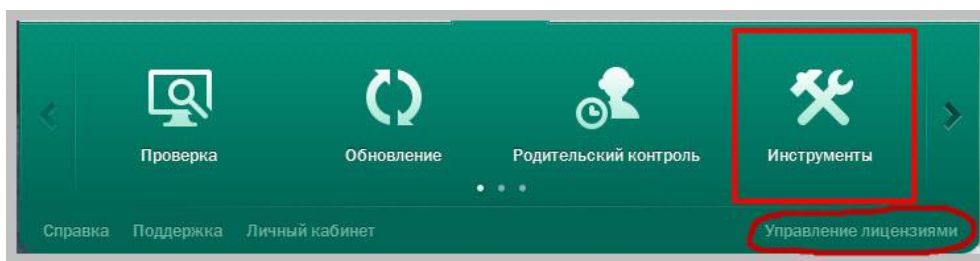
Здесь нам предлагают выбрать продукт для загрузки. Пробные версии нас не интересуют. Сейчас разберем «Kaspersky Rescue Disk».



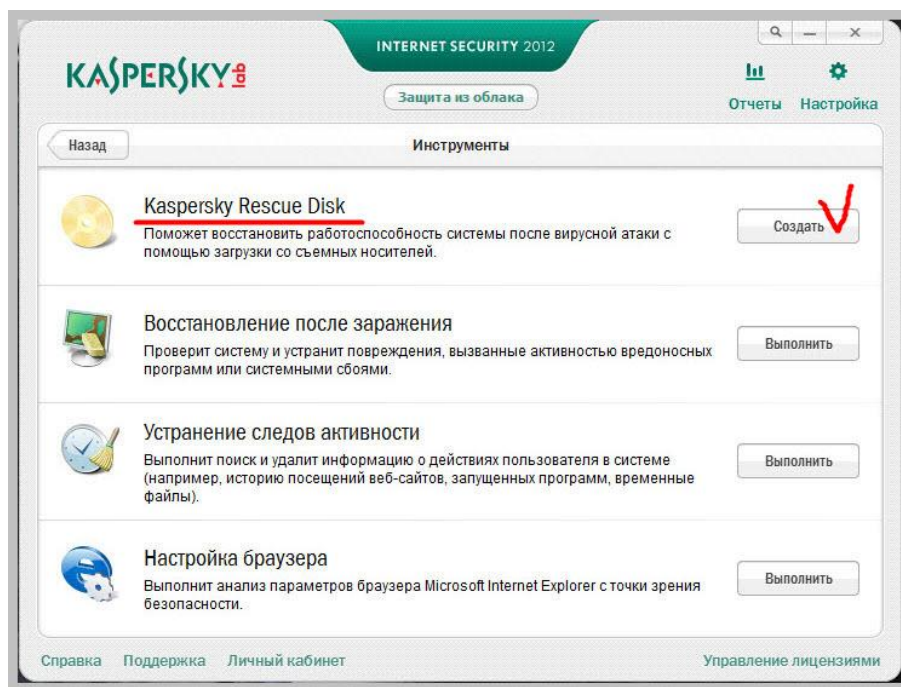
Нажимаем кнопку «Загрузить» и выбираем место на компьютере, куда мы будем сохранять загружаемый образ.

В двух словах, что мы вообще делаем и зачем? Сейчас нам нужно скачать себе на компьютер образ загрузочного (спасительного) диска, а затем – записать его на CD диск. После этого у нас в руках окажется загрузочный диск от лаборатории Касперского, содержащий последние (на момент его скачивания) антивирусные базы. Мы сможем загрузить с него наш компьютер и проверить его на вирусы, не загружая нашу рабочую операционную систему.

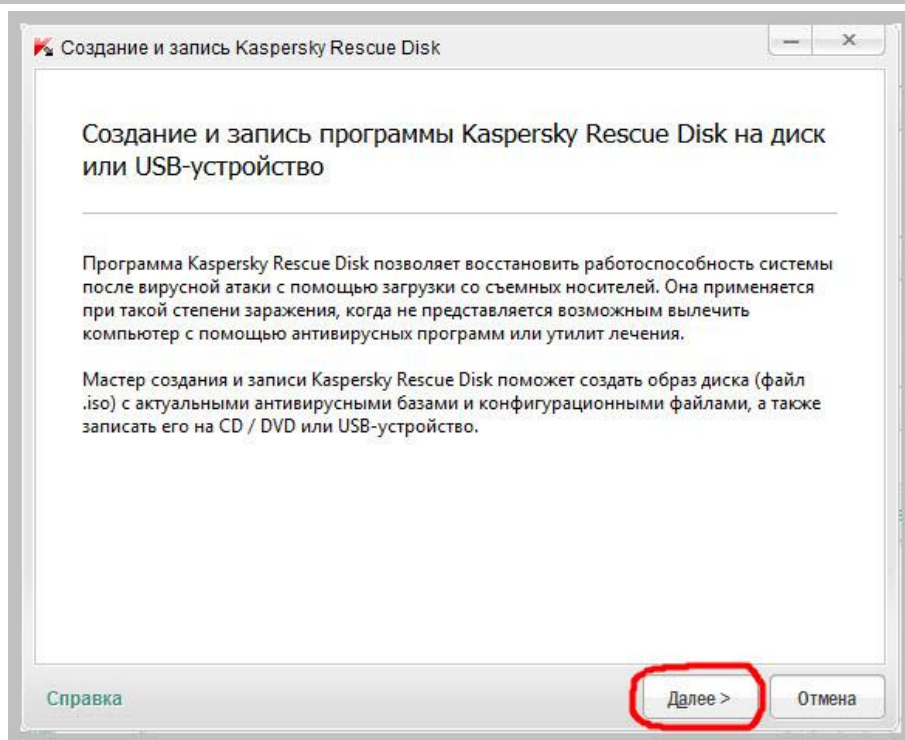
Итак, мы скачали «iso» файл в несколько сотен мегабайт и сохранили его в заранее подготовленную папку на жестком диске. Затем – «идем» в главное окно программы и нажимаем кнопку «Инструменты».



Попадаем вот в такое окно, где нам нужно будет нажать кнопку «Создать» в разделе «Kaspersky Rescue Disk».

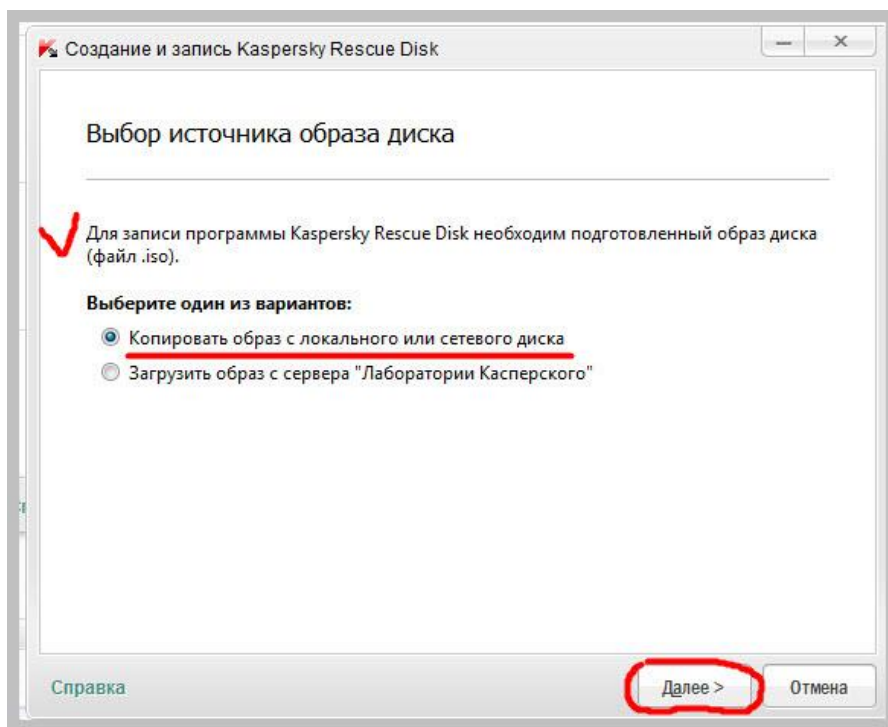


После этого запустится «мастер» создания загрузочного спасительного диска.

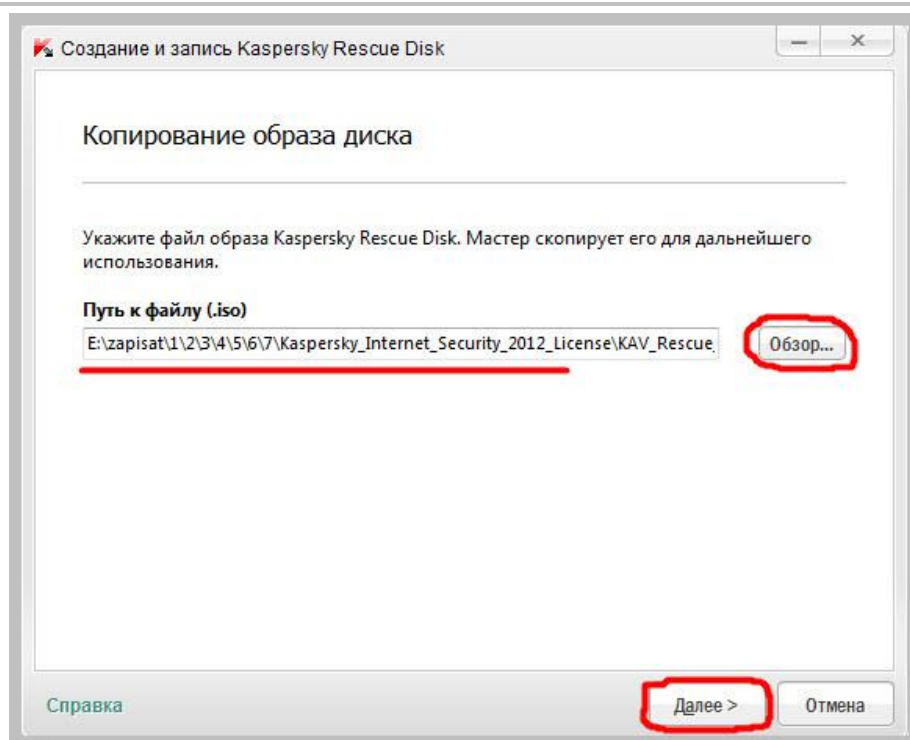


Как видите, мы можем создать либо диск, либо загрузочное USB устройство (флешку).

Нажимаем кнопку «Далее» и попадаем в окно выбора «iso» файла образа.

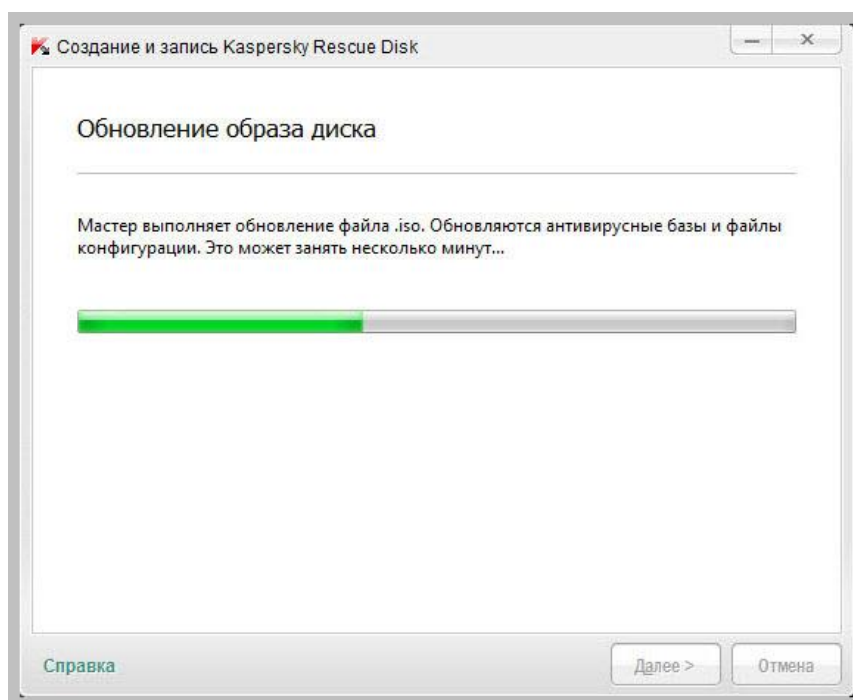


Поскольку мы его уже загрузили, нам остается лишь указать нужный вариант и нажать кнопку «Далее».

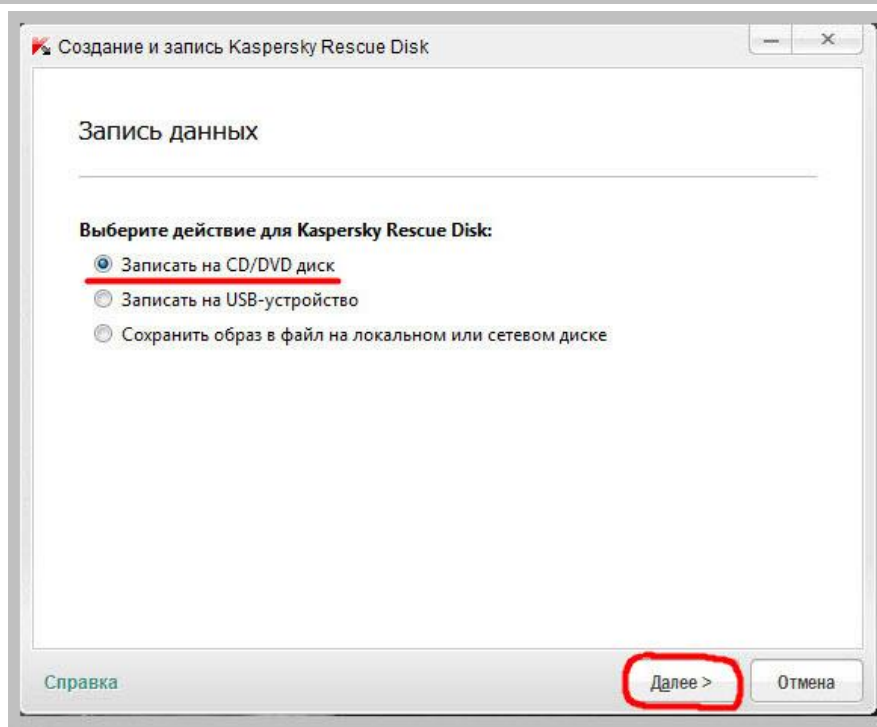


В этом окне через кнопку «Обзор» выбираем скачанный нами файл и еще раз нажимаем «Далее».

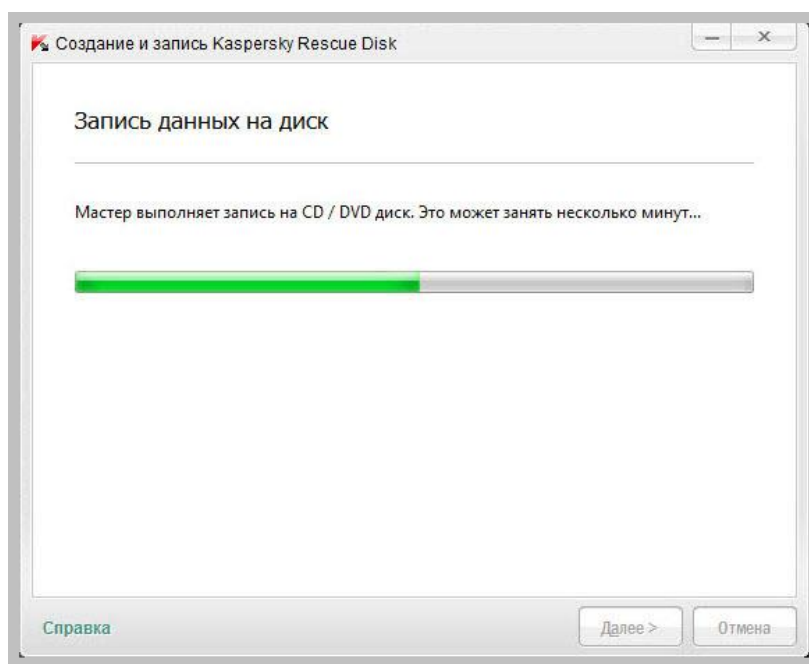
И видим, вот такое окно:



Что именно делает программа в этот момент – трудно сказать, но по завершении этого процесса нас спросят о том, хотим ли мы создать загрузочный диск или флешку? Лично я выбрал первый вариант.



Нажимаем «Далее» и (наконец-то!) программа приступает к записи нашего загрузочного диска! 😊



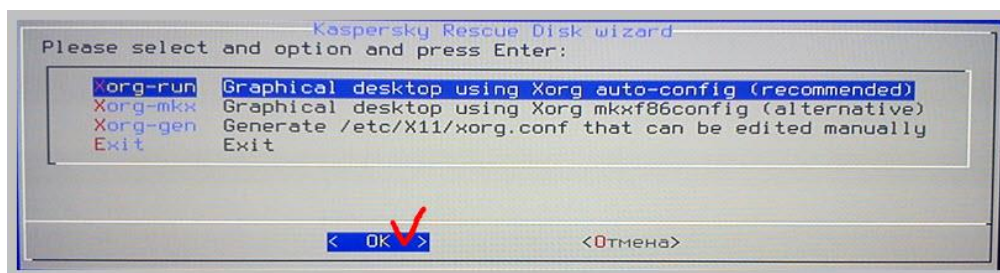
После того, как диск будет записан, нам нужно будет выставить в BIOS загрузку с CD или DVD, вставить в компьютер наш диск и перезагрузиться.

Если мы все сделали правильно, то должна начаться загрузка непосредственно со спасительного диска Касперского.

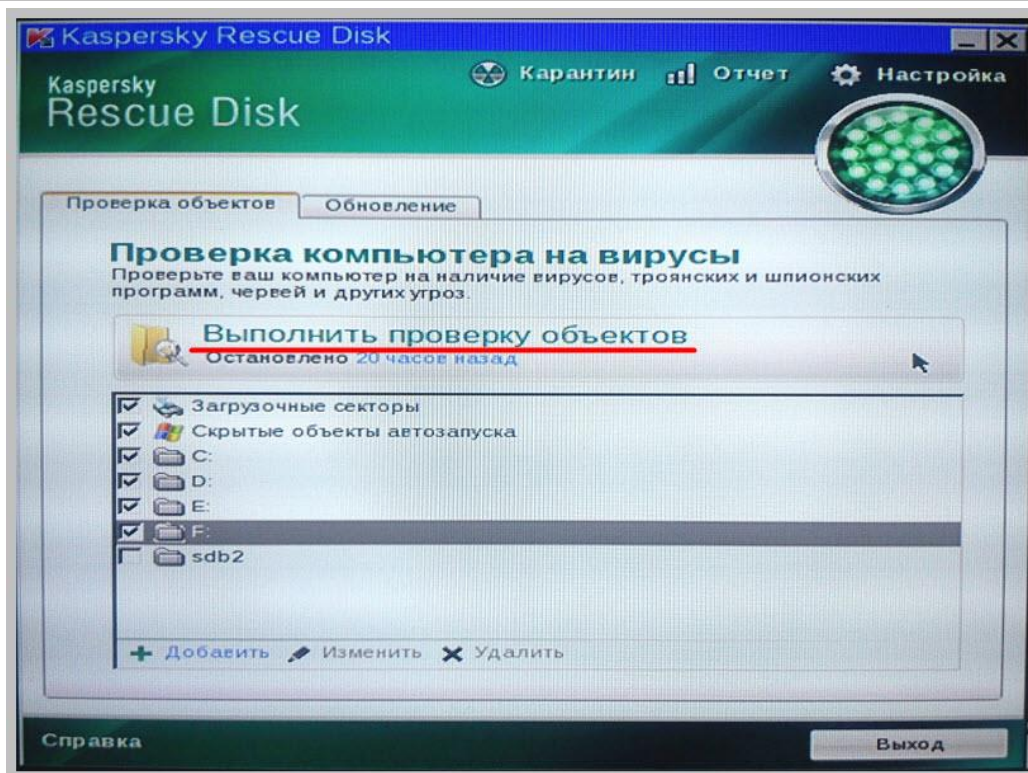
```
OpenRC 0.7.0 is starting up Gentoo Linux (i686)
* Mounting /proc ...
* Caching service dependencies ...
* Mounting /sys ...
* Mounting security filesystem ...
* Mounting debug filesystem ...
* Mounting /dev ...
* Starting udevd ...
* Populating /dev with existing devices through uevents
* Waiting for uevents to be processed ...
* Mounting /dev/pts ...
* Mounting /dev/shm ...
* Setting system clock using the hardware clock [UTC] ..
* Updating /etc/mtab ...
* Setting terminal encoding [UTF-8] ...
* Setting console font [ter-v16n] ...
* Checking local filesystems ...
* Setting hostname to kavrescue ...
* Bringing up interface lo
* Caching network module dependencies
```

Как мы можем видеть из фото выше, загружается программная оболочка на основе ядра «Linux», а именно – одна из ее разновидностей – «Gentoo Linux».

В появившемся окне делаем все так, как показано на фото ниже. Нажимаем кнопку «OK».

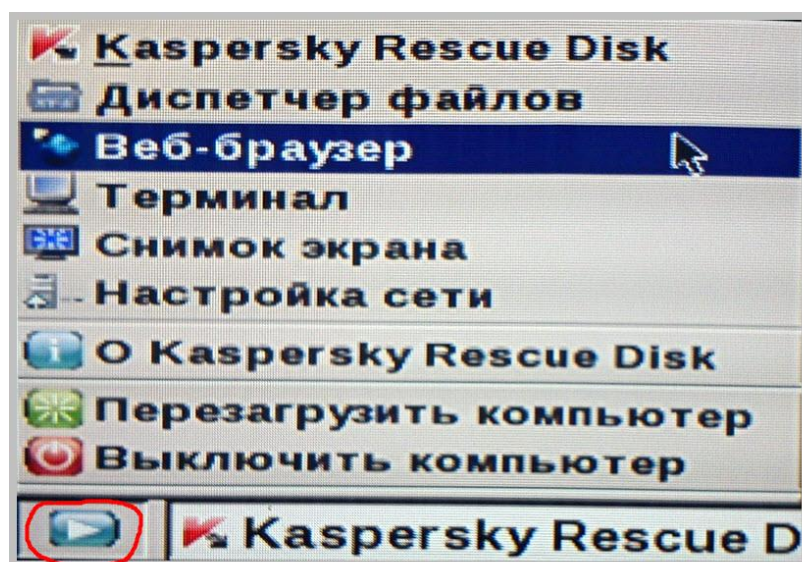


Это приведет к запуску графического интерфейса диска.

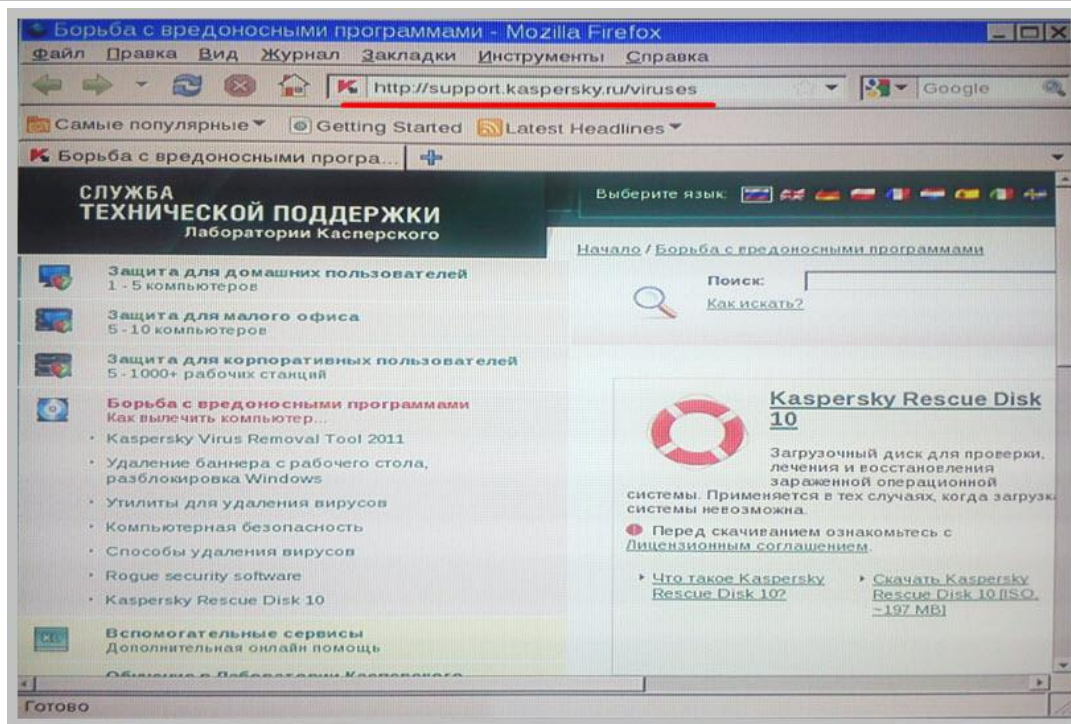


Здесь мы можем задать область проверки на вирусы (лучше отметьте все галочки) и нажать надпись «Выполнить проверку объектов». После чего начнется сканирование системы.

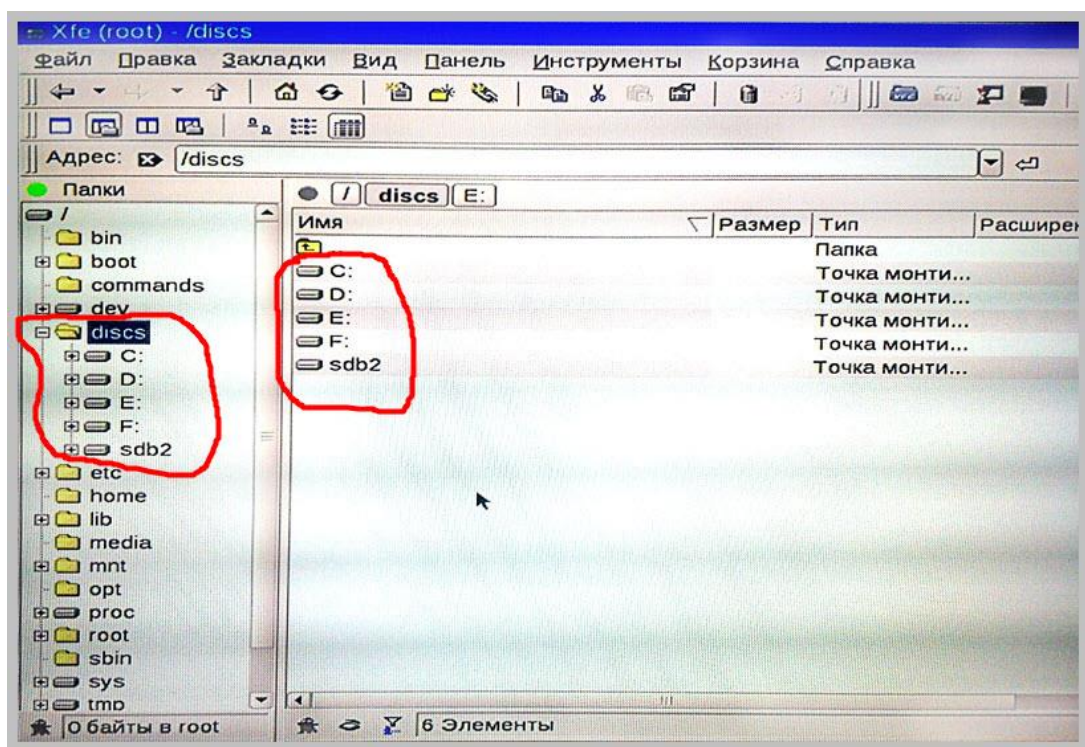
Также здесь присутствует еще несколько утилит, список которых отображается после нажатия на кнопку, заменяющую собой кнопку «Пуск» в системе Windows.



Можно запустить из меню веб-браузер «Mozilla Firefox», с помощью которого выйти в Интернет прямо из оболочки данного диска, зайти на сайт лаборатории Касперского и выполнить там любые действия, необходимые для восстановления работоспособности системы.



Также можно запустить встроенный файловый менеджер (проводник), который в данном меню называется «Диспетчер файлов» и получить в нем доступ к файловой системе нашего винчестера.



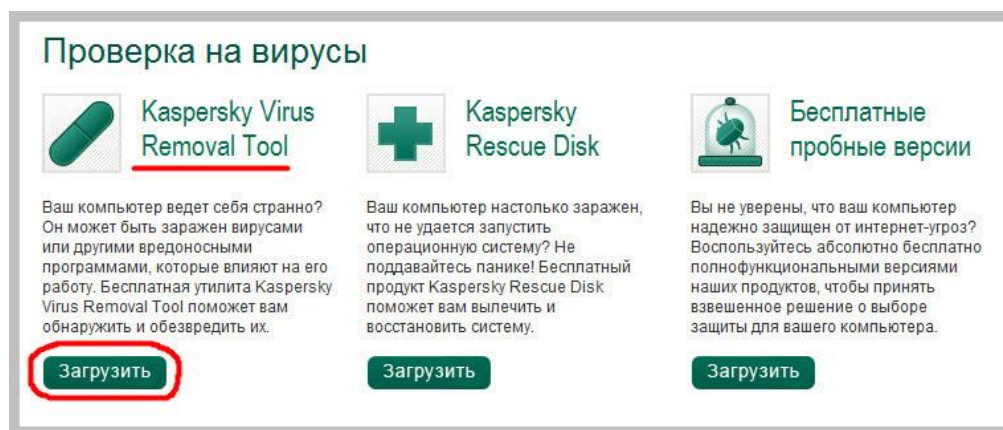
Все диски находятся (монтируются) в папке «Discs». Для того, чтобы получить к ним доступ, надо нажать на значок «+» слева от изображения папки и в правом окне проводника мы увидим содержимое наших дисков. Естественно, что после этого можно выполнять все привычные дисковые операции: копирование файлов, их перемещение или удаление.

Согласитесь, это – удобная и очень нужная дополнительная функция к самой антивирусной проверке, осуществляемой с загрузочного диска.

Представьте что (не дай бог!) ☺ Ваша операционная система перестала загружаться, а данные с системного диска надо как-то извлечь. Можно, конечно, физически вытащить сам диск, подсоединить его к другому компьютеру и перекопировать информацию на него. А можно поступить и более элегантно: загрузиться со спасительного диска и оперативно переместить нужные данные.

Это – что касается данной разработки лаборатории Касперского. В заключительной части нашей статьи хочу познакомить Вас с еще одним программным средством, которое можно также абсолютно бесплатно загрузить с сайта Касперского.

Заходим на сайт лаборатории. Переходим в «Загрузки» – «Бесплатные утилиты». Нас будет интересовать продукт «Kaspersky Virus Removal Tool».



Нажимаем кнопку «Загрузить». Нам нужно будет скачать примерно 100 мегабайт данных. И пока идет процесс загрузки, давайте поговорим о том, в чем нам может помочь данный продукт?

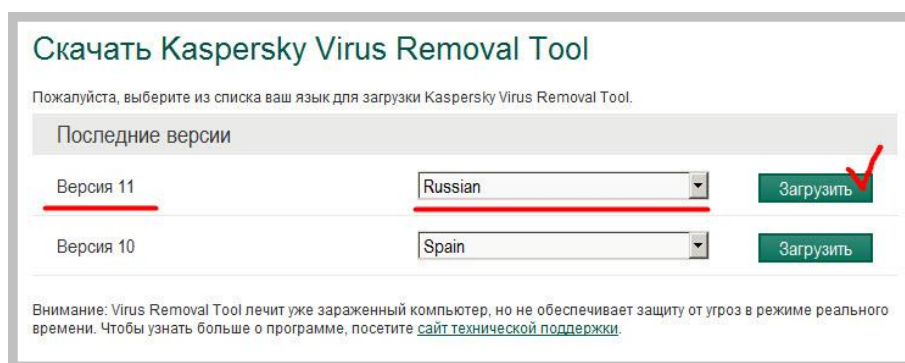
Это – разновидность антивируса для быстрой проверки. Он не обеспечивает защиты в реальном времени, поскольку не устанавливается на компьютер (не устанавливает своих служб, а запускается в оперативной памяти), и служит именно для однократной проверки и оперативного «лечения» компьютера.

Давайте снова смоделируем какую-нибудь «страшную» ситуацию ☺ К примеру, Ваш знакомый просит Вас очистить его компьютер от вирусов, и у него уже установлен другой антивирус (к примеру «Symantec Norton»). Но в силу того, что он давно не обновлялся, компьютер серьезно заражен несколькими разновидностями вирусов. Как быть в такой ситуации? Удалять «Symantec» знакомый не хочет, а просит найти другой

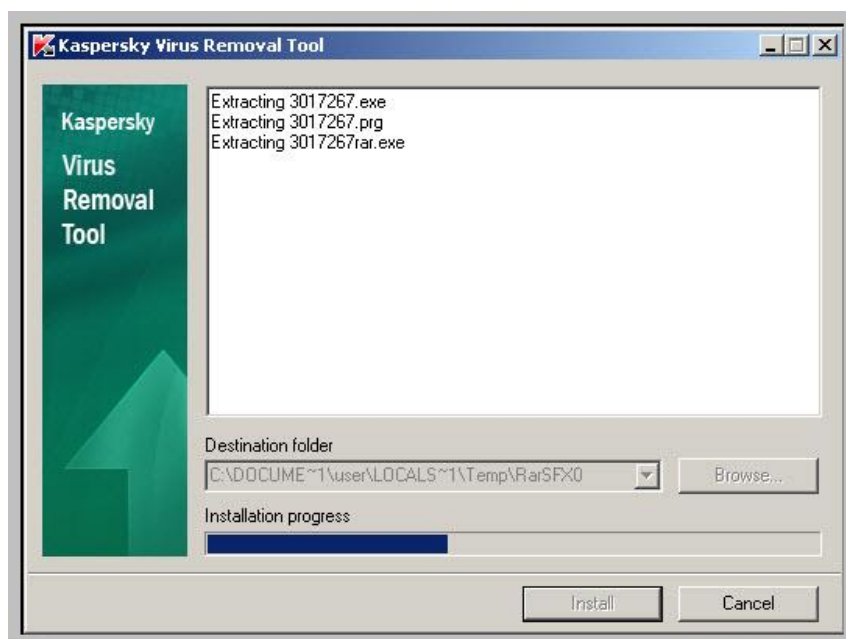
способ. Вот в такой ситуации идеально подойдет решение «Kaspersky Virus Removal Tool».

Единственное, надо понять, что актуальность антивирусных баз, содержащихся в пакете, будет соответствовать времени его загрузки. Но ничто нам не мешает в любой момент загрузить самую «свежую» его версию.

Итак, давайте подробно разберем, что произойдет после того, как мы нажмем на кнопку «Загрузить»? Нам предложат выбрать версию продукта и его язык. Тут, думаю, все понятно: номер версии выбираете самый больший, а язык – русский.



Сохраняем программу в отдельную папку на жестком диске и запускаем ее «exe» файл.

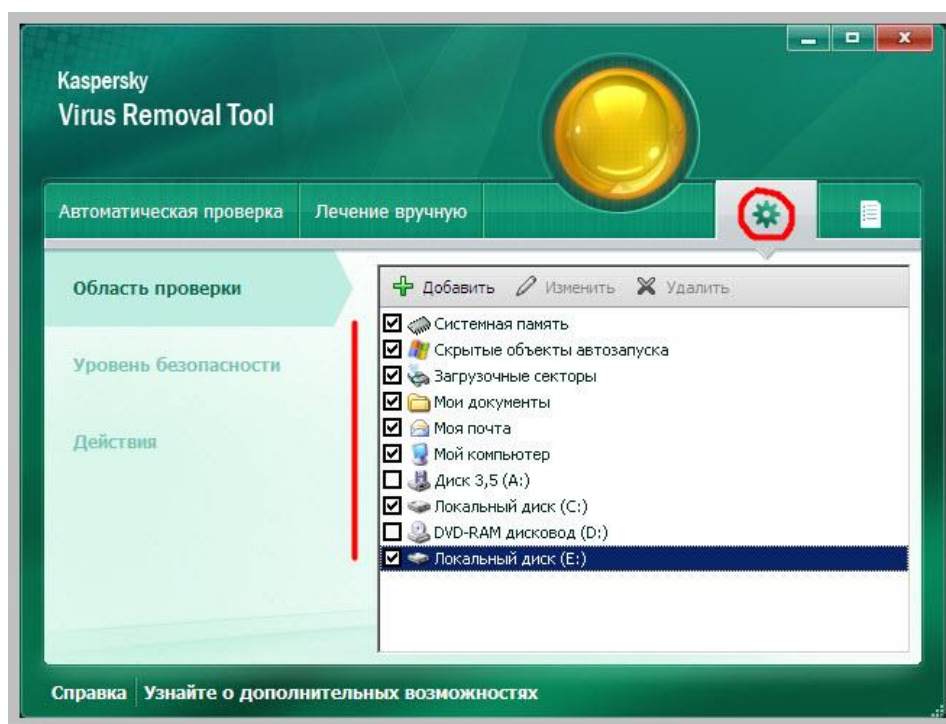


Как видим, начался процесс ее распаковки во временную папку, а затем – запуск программы.

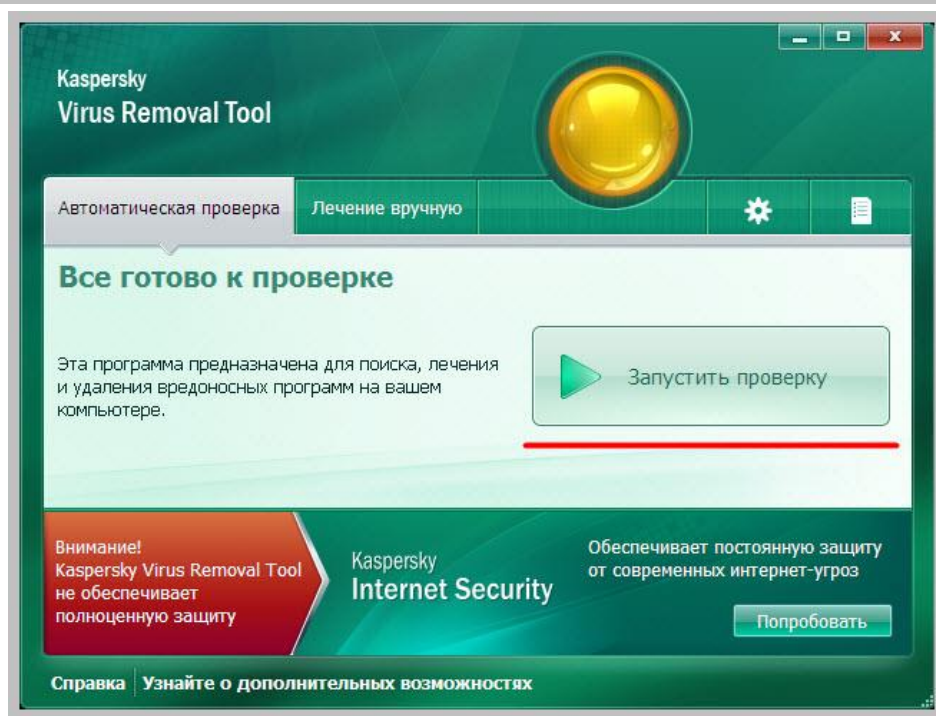


Программа очень проста в использовании. Нам просто надо задать область проверки (где мы будем искать вирусы) и запустить сам процесс поиска.

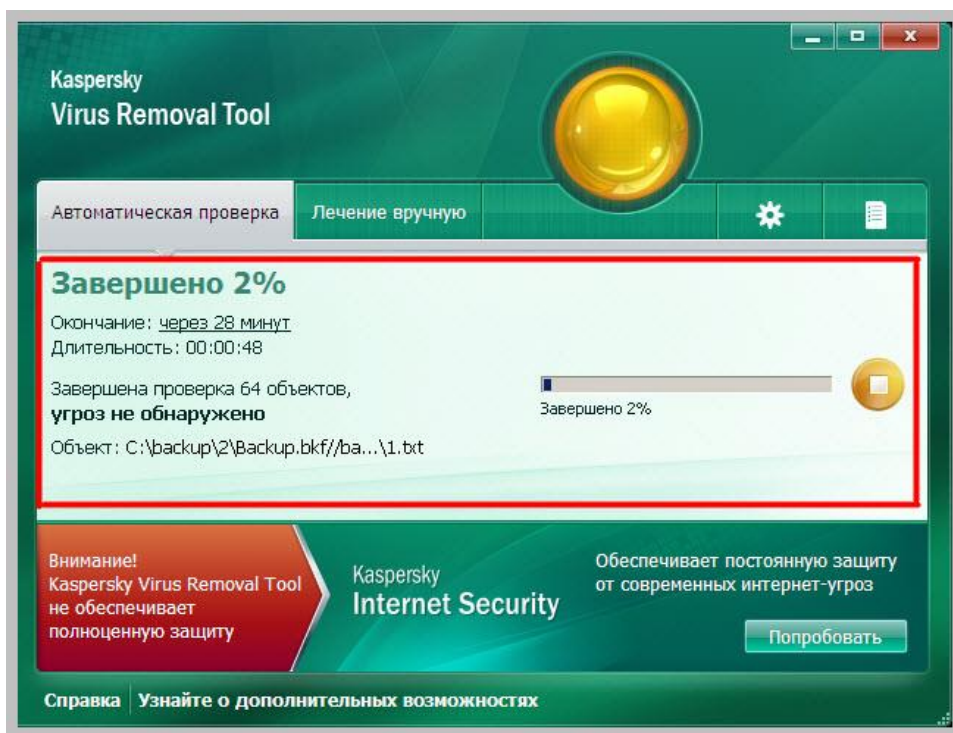
Для реализации первого этапа нажимаем на изображение шестерни и в появившемся окне ставим галочки напротив тех объектов, которые программа должна проверить.



Затем – возвращаемся в главное окно и нажимаем кнопку «Запустить проверку».



После запуска мы в режиме реального времени сможем наблюдать за статистикой сканирования и временем его окончания.



Как видите, все – очень просто! ☺

И уж совсем напоследок, я бы хотел сказать несколько слов о том постоянном споре, который можно наблюдать на различных компьютерных форумах, где люди пытаются доказать друг другу что их антивирус самый лучший, а остальные – ерунда полная.

Так какой же антивирус лучше? Думаю, правильным будет ответ: тот, который лично Вам больше нравится, лично для Вас более удобен в использовании и управлении и работой которого лично Вы остаетесь удовлетворены.

Вот он и будет – лучшим антивирусом!

Я говорю так потому, что на данный момент практически все известные антивирусы имеют более-менее одинаковую функциональность и достаточно хорошо справляются со своими задачами. И обращать внимание надо не на их названия и «брендовость», а на два очень простых, но важных фактора:

1. Своевременное обновление антивирусных баз (об этом мы говорили выше)
2. Версию самой антивирусной программы

Давайте остановимся на втором пункте более подробно. Наверное Вы помните, что пару лет назад почти все в один голос утверждали, что антивирус «Eset Nod 32» «не ловит вирусы» и вообще это не антивирус, а – сплошное недоразумение. В чем-то говорящие так были правы. Вполне «обычной» на тот момент могла быть ситуация, когда данный программный продукт (с самыми свежими антивирусными базами) умудрялся «пропускать» в систему все новые и новые вирусы. С большинством он успешно справлялся, но некоторые словно «просачивались» сквозь его защиту и «поселялись» на компьютерах пользователей. Я сам неоднократно сталкивался с этим явлением, поэтому знаю, о чем говорю.

Короче говоря, заслужил наш антивирус статус «дырявого». Отчасти справедливо, конечно. На то время это была антивирусная программа версии 2.0, затем вышла ее версии 2.5 и 2.7, не внесшие революционных изменений. Через некоторое время появилась полностью переработанная версия под номером 3.0. Изменилось практически все, начиная от графического интерфейса.

Я был, наверное, одним из первых, кто установил себе (и на компьютеры обслуживаемой мной тогда небольшой локальной сети) этот обновленный продукт. И Вы знаете, я сразу увидел огромную разницу в работе программы. Она перестала пропускать вирусы. Вот просто перестала и все! ☺ И это – на фоне непрекращающейся на тот момент в Интернете истерии по поводу того, что «Nod 32» это – плохой антивирус.

Я решил пообщаться на форумах с теми людьми, которые громче всех заявляли об этом. Оказалось именно то, что я и предполагал: у большинства из них либо была установлена на компьютере версия «Eset Nod 32» либо 2.5 (2.7) либо они уже давно «пересели» на что-то другое и говорили так по «старой памяти». Все дело было именно в версии антивирусной программы. Те немногие, у кого уже была установлена новая версия 3.0 никаких претензий к антивирусу не имели. Но «пена» негативного отношения к данному продукту в сети держалась еще почти год, вплоть до выхода версии программы 4.0, когда уже абсолютно всем стало ясно, что алгоритм поиска вирусов в «Nod 32» изменился полностью и он отлично справляется со своей задачей.

Так в чем же здесь дело? Что изменилось? Понятно, что обновленный графический интерфейс здесь не при чем. Так что же? Ответ – переработанное ядро программы, логика ее работы, то каким образом (**по какому алгоритму**) производится поиск вирусов в системе. Элементы данного подхода отражены в такой технологии, как эвристический анализ (сканирование).

Это метод обнаружения вредоносных программ, при котором антивирусная защита контролирует все действия, выполняемые проверяемой программой. В ходе эвристического анализа отслеживаются потенциально опасные действия, характерные для вирусов и вредоносных программ других типов. Эвристика призвана распознавать модифицированные версии вирусов в тех случаях, когда сигнатура (образцы из антивирусной базы) совпадает с телом неизвестной программы не на все 100%, но в подозрительной программе налицо более общие признаки вируса, на основе чего принимается решение о ее блокировании.

Сейчас существует большое количество разновидностей вирусов. К наиболее опасным можно отнести сетевых червей (вирусы, копирующие себя по сети), троянские программы, посредством которых злоумышленник может получить доступ к личным данным пользователя (клавиатурные шпионы, бэкдоры, почтовые троянские программы). Существуют также полиморфные вирусы, которые шифруют свой код, пытаясь таким образом «спрятаться» от антивирусных программ. Те люди, которые создают вирусы (уж не знаю зачем), тоже не сидят сложа руки, а постоянно ищут новые возможности спрятать код вируса от антивирусных программ или вовсе блокировать антивирусную защиту.

Все эти известные (и даже еще неизвестные) угрозы и должна уметь выявлять и устранять защита. И именно поэтому так важно (наряду со своевременным обновлением антивирусных баз) периодически обновлять и саму антивирусную программу с выходом ее новой версии. Так как в ней наверняка подправлен (или радикально переработан) алгоритм выявления и поиска новых вирусов.

Теперь – действительно все! ☺

Урок взят с сайта: <https://sebeadmin.thelogos.in.ua>

До встречи в следующих уроках !