

АНТИВИРУСНАЯ ЗАЩИТА В ШКОЛЕ

Автор: учитель информатики
МБОУ Тёпловская СОШ
Карачевского района Брянской области
Федоров Александр Николаевич

Антивирусная защита персональных компьютеров – задача, которая стоит не только перед обычными пользователями, но и учителями информатики и лаборантами, которым необходимо защитить десятки компьютеров в школе. И этот вопрос не настолько тривиален, как может показаться, поскольку его решение лежит не только (и не столько) в технической плоскости, сколько в плоскости правовой.

После того, как государство массово оплатило годовые лицензии на **Антивирус Касперского** несколько лет назад, оно отказалось от подобной практики, оставив выбор антивирусного ПО на откуп школам. Учителям информатики, в том числе и мне, пришлось выбирать антивирус для школы.

Казалось бы, что здесь выбирать – на рынке присутствует множество бесплатных решений, только выбирай. И многие коллеги, я это точно знаю, решили вопрос очень просто – установив, наверное, самый известный из бесплатных антивирусов – **AVAST Free Antivirus**.

Однако же это решение, являясь удачным с технической точки зрения, совершенно никуда не годится с точки зрения правовой, поскольку в данном случае идет прямое нарушение лицензии данного продукта, который бесплатен лишь для домашнего применения. Таким образом, первая же проверка прокуратуры может вызвать ряд весьма неприятных переживаний.

Другой вариант, сам просящийся на ум – решение от **Microsoft**. Действительно, **Microsoft Essentials Security** тоже – бесплатный продукт. Но, читая лицензию, мы видим, что установка его в учебных и иных государственных учреждениях запрещена. Значит, и данное решение нам не подходит.

То же самое касается и большинства других антивирусов, допустим, продукта от **Avira**. Набирающий популярность китайский **360 Total Security**, во-первых, слишком завязан на облако, что крайне негативно скажется на пропускной способности и без того еле дышащей школьной сети (не знаю, у кого как, а в нашем районе норма для сельской школы – 256 кбит/сек, и это гордо именуется «широкополосным доступом в Интернет»), а во-вторых использует движки других антивирусов, что так же, думаю, приведет к правовым нестыковкам (см. выше).

Собственно, я сумел найти лишь два продукта, которые действительно можно без всяких проблем использовать в учебных заведениях – антивирус от моих земляков из Брянска под трендовым названием **NANO Antivirus** (http://www.nanoav.ru/index.php?option=com_content&view=article&id=4&Itemid=78&lang=ru), а также продукт весьма известного вендора в мире IT-безопасности – **COMODO Antivirus** (<https://www.comodo.com/home/internet-security/free-internet-security.php?key5sk0=2128&key5sk1=e340515d16fa1aa8f71dbcbdddb8d98c249bb709>). О них и поговорим.



COMODO
Creating Trust Online®

Увы, годичный опыт работы с отечественным продуктом оставил достаточно негативные ощущения. В целом, неплохой антивирус, справляющийся со своими обязанностями вполне успешно, но при этом – слишком прожорлив к системным ресурсам. Даже не самые слабые компьютеры заметно проседали под его «тяжестью», а старички (коих в наших школах предостаточно) так и вовсе едва дышали после его установки. Правда, с тех пор, как я в последний раз пользовался данной программой, прошло более двух лет. Может быть (я даже надеюсь на это) за это время с ней произошли значительные изменения к лучшему. Тем более, там было весьма удобно создавать локальное зеркало для обновлений по сети, что было весьма весомым плюсом к данному продукту.

Однако, попользовавшись год этим антивирусом, я понял, что надо что-то менять. Директор, который сам изнемогал от тормозности своего компьютера, не справляющегося с аппетитами **NANO Antivirus**, согласился выбить деньги в бухгалтерии на приобретение моего любимого **ESET NOD32**. Тем более, у них есть акция «Антивирусная перемена», позволяющая приобрести лицензию на 1 компьютер в школе всего за 175 рублей в год. В общем, 2 года мы безбедно прожили под защитой **NOD32**, компьютеры обрели словно вторую молодость.

Но вот в этом году директор сказал, что ждать денег от бухгалтерии явно не приходится, и нужно искать что-то иное. Таким образом, пришла моя очередь присмотреться к антивирусу от компании **COMODO**.

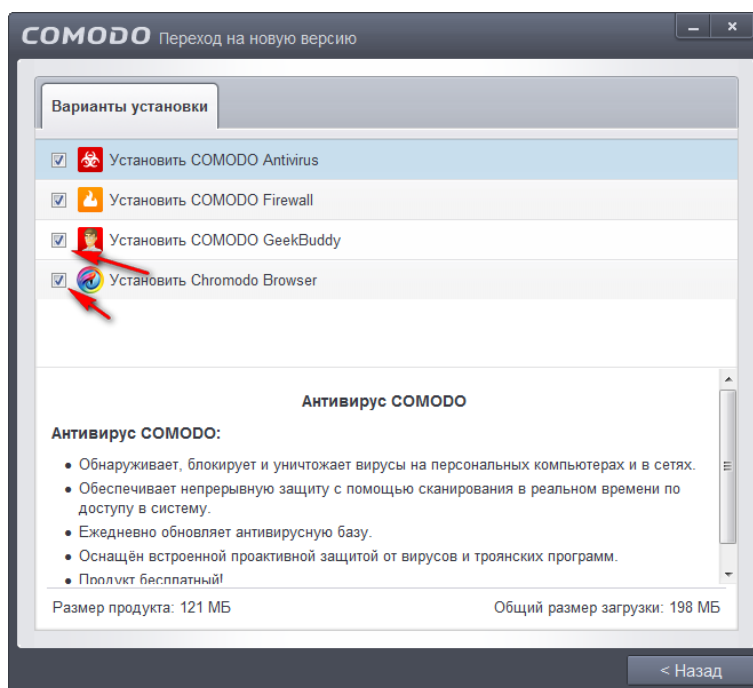
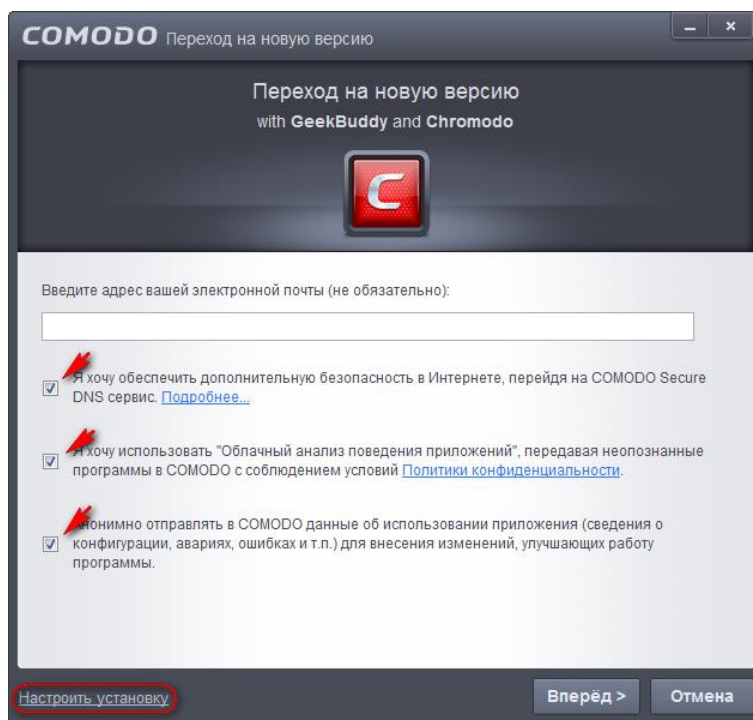
Я уже много лет дома пользуюсь файерволлом от данной компании, и очень доволен. Однако с антивирусом сталкиваться еще не приходилось. Меня интересовало, насколько он лоялен к системным ресурсам, и можно ли обновлять его из локального зеркала.

Итак, установив на рабочий компьютер **Comodo Antivirus** актуальной на момент написания данной статьи версии 8.2.0.4674, обратил внимание, что изменений в скорости работы компьютера не заметил. Правда, мой компьютер не самый маломощный, а вот слабые машины, конечно, не слишком обрадовались. По крайней мере, при установленном **ESET32** версии 3 они работали куда как шустрее. Возможно, можно попытаться найти более старую версию **Comodo**, допустим, порядка 5.8 (кажется, именно с этой версии они изменили структуру баз и все остальное). В конечном итоге все снова упрется в объем скачиваемых обновлений. Но по большому счету, по загрузке процессора и памяти на старых компьютерах последняя версия **Comodo** не дает особого преимущества перед тем же **NANO Antivirus**, при том, что последний настраивается более гибко в том числе и в плане зеркала обновлений. Поэтому можете попробовать именно его, возможно, вы не разочаруетесь.

Но вернемся к **Comodo Antivirus**. Главное же, что меня интересовало – обновление из зеркала. Увы, но подобной опции в данном антивирусе не предусмотрено. Правда, есть возможность импорта антивирусных баз, но это очень неудобно для конечного пользователя (допустим, учителю нашей школы, на ноутбуке которого будет установлен данный продукт придется выполнять ряд манипуляций по импорту, причем для него не всегда очевидных, что вызовет ненужные проблемы и ему и мне), да и качать всякий раз свыше 200 МБ представляется не слишком радужной перспективой.

Однако, решение было найдено. Им оказалась программа **Comodo Offline Updater**, работающая по принципу кэширующего прокси-сервера и создающая зеркало для обновлений вышеозначенного антивирусного продукта. Поскольку у меня возникли некоторые проблемы, пока не удалось все сделать как надо, я думаю, что описав эти проблемы и их решение, я смогу облегчить жизнь кому-нибудь. Поэтому дальнейшая часть статьи будет, по сути, пошаговым руководством по созданию локального зеркала для обновлений антивируса **COMODO**.

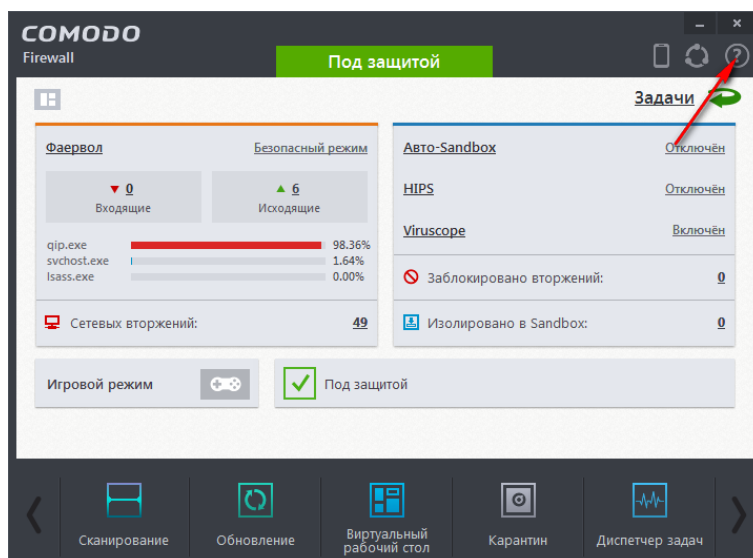
Итак. Каков же порядок действий. Во-первых, устанавливаем сам антивирус. Дабы не установить лишнего, при установке следует снять несколько галочек, а также обратить внимание на неприметную ссылку. Лично я убираю все галки в основном окне, хотя если бы обладал скоростным интернетом, вероятно, облачный анализ оставил бы...



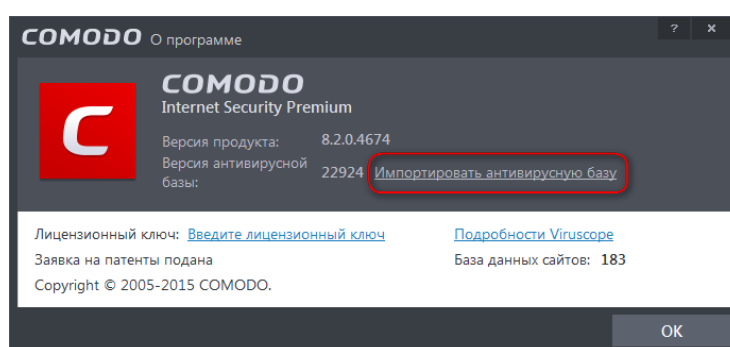
В дополнительных настройках я убираю GeekBuddy и Chromodo, но это уже вопрос вкусов. Также можно снять галку и с файерволла, если нет желания обеспечить себя дополнительным уровнем защиты и гибким инструментом по контролю за сетевыми соединениями.

После установки программы она тут же попытается обновиться. При скоростном интернете это – не проблема, кроме того, избавит от той проблемы, с которой столкнулся я. Но если Вы – мой товарищ по несчастью, и также маетесь на медленном интернете, то на данном этапе лучше отключить соединение с интернетом и не дать ему обновляться. Вместо этого нужно заранее скачать кумулятивное обновление с официального сайта **Comodo**: <https://www.comodo.com/home/internet-security/updates/vdp/database.php>

После установки и перезагрузки импортируйте базу данных. Для этого нажмите на значок со знаком вопроса в верхнем правом углу и выберите пункт «О программе».



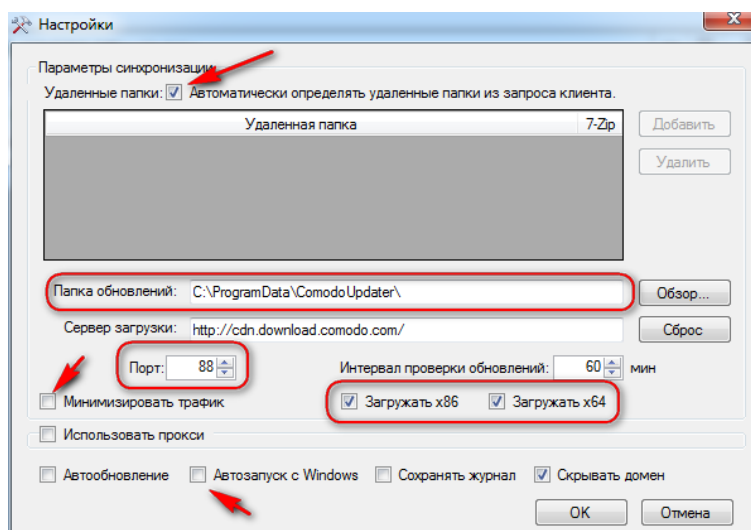
В появившемся окне нажмите пункт «Импортировать базу», и укажите путь к скачанному вами файлу bases.cav.



Сразу поясню – зачем такие сложности. Просто если давать каждому установленному антивирусу обновляться самостоятельно – представьте, сколько это займет времени, если у вас, допустим, порядка 20 машин. А так – достаточно один раз скачать 200-мегабайтный файл, и затем импортировать его на любое количество компьютеров. А если оставить антивирусную базу пустой, то лично у меня не вышло обновить ее через **Comodo Offline Updater** – программа выдавала ошибку на этапе применения обновлений. Только когда я импортировал базу, установка обновлений с зеркала стала успешной. Может быть, я что-то не так делал, или это какие-то частные проблемы, но у меня это было на трех разных компьютерах.

Теперь пришла пора настройки зеркала. Для начала нужно скачать и установить саму программу **Comodo Offline Updater**. Это можно сделать, посетив официальный форум **Comodo**: <https://forums.comodo.com/10551086108810911089108910821080-russian/comodo-offline-updater-t54363.0.html>

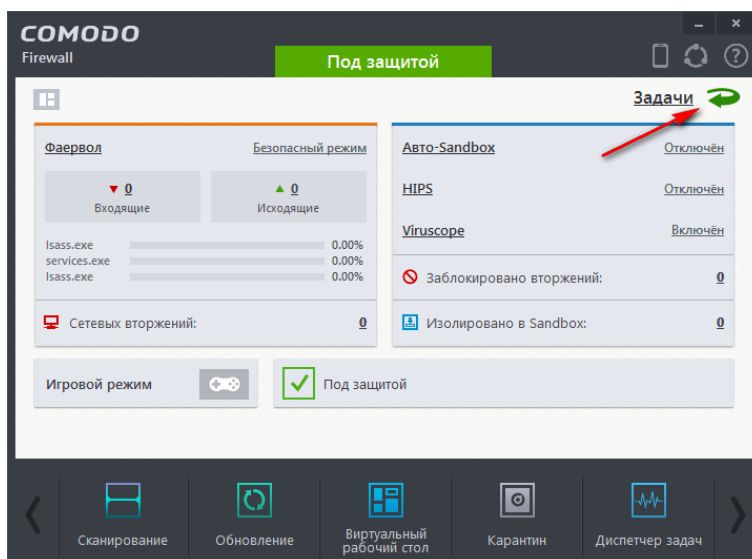
Распаковав программу, запустите ее и зайдите в настройки.



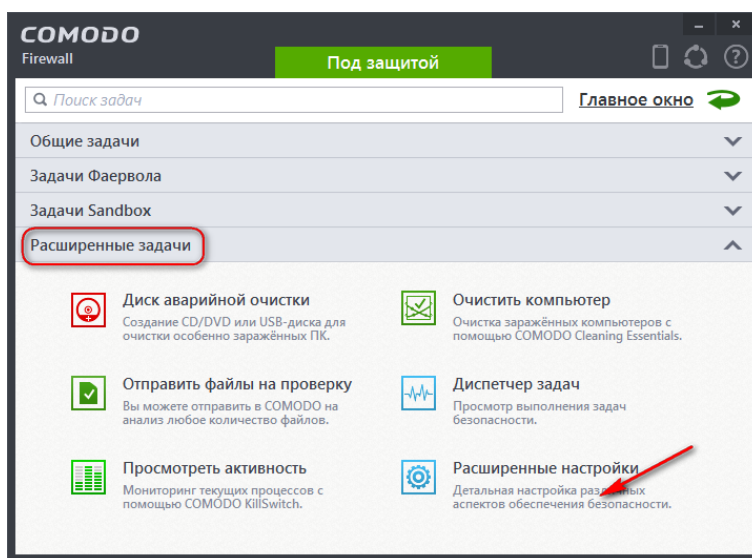
По большому счету, тут уже все настроено так, что нам практически ничего и делать не нужно. Обязательно убедитесь, что у вас установлена галочка «Автоматически определять удаленные папки»! Порт оставляем тот, что по умолчанию – 88. Я бы изменил путь к папке обновлений – поместил бы не на системном диске. Если у вас, как в моем случае, все компьютеры работают под управлением 32-разрядных систем, то есть смысл снять галку с «Загружать x64». Ну и поставьте галочку на автозапуск с Windows, поскольку антивирусы смогут обновляться только при запущенном приложении.

Отдельно хочется сказать по поводу опции «Минимизировать трафик». Изначально я ее включил, поскольку думал, что это как-то отразится на количестве скачанной из интернета информации. Но оказалось – никак. Если кумулятивное обновление весит порядка 200 МБ, то **Comodo Offline Updater** выкачивает порядка 800 – вероятно, для всех версий продукта. Однако, эта опция негативно сказывается на скорости обновления внутри локальной сети. Насколько я понимаю, смысл данной опции – сжимать файлы обновлений при помощи архиватора **7-zip**, передавать их по сети, и на стороне клиента разархивировать обратно. В общем, это занимает невероятную кучу времени, и обновление по локальной сети идет в разы медленнее, чем даже через интернет-соединение 256 кбит/сек. В общем, я снял эту галку, и все стало нормально. Думаю, она имеет смысл лишь в крупных сетях на многие десятки машин, когда их постоянные обращения к серверу обновлений могут забивать сеть.

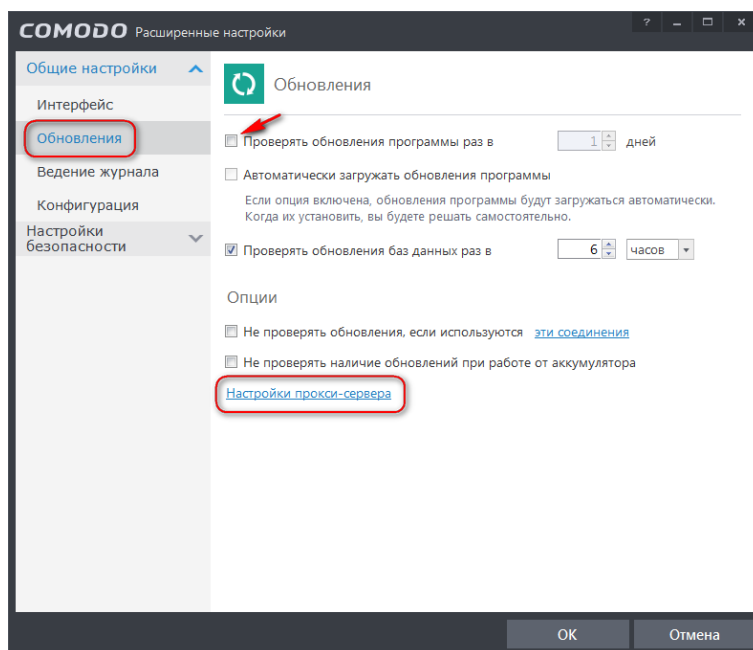
Перечень удаленных папок пуст. Так и должно быть. Эти папки чуть позднее будут определены автоматически. Что для этого нужно? Теперь пришла пора настроить антивирус. Для этого откроем окно приложения, и выберем пункт Задачи.



Затем в Расширенных задачах выберем пункт Расширенные настройки.

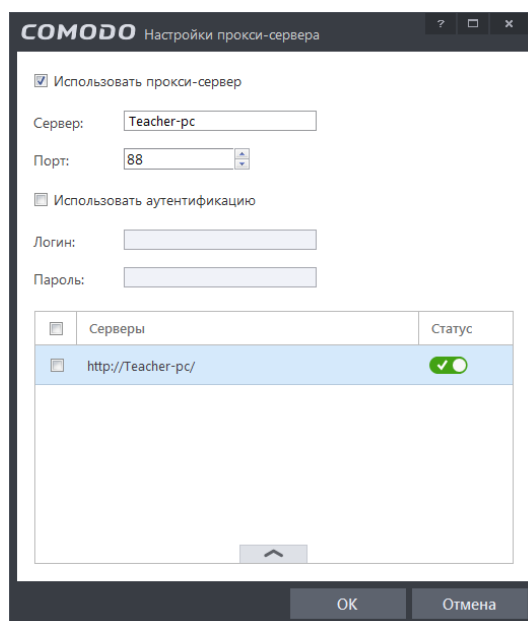


В появившемся окне выберем слева пункт Обновления.



Если честно, не знаю, входят ли обновления программы в контент, скачиваемый **Comodo Offline Updater**, есть небольшое подозрение, что – да, поскольку мне думается, что вряд ли сами вирусные сигнатуры имеют деление на 32- и 64-битные. Так что, думаю, есть смысл не убирать галку «Проверять обновления программы». Но это – не более, чем мои размышления.

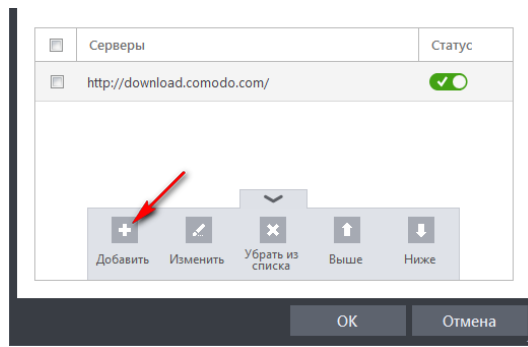
Нас же будет интересовать настройка «Настройки прокси-сервера».



Здесь включаем опцию «Использовать прокси-сервер», ведь, как мы говорили выше, **Comodo Offline Updater** как раз и является таким прокси-сервером. Теперь по настройкам. В поле «Сервер» нужно ввести либо имя компьютера, на котором установлен **Comodo Offline Updater**, либо его IP-адрес. Я заметил у себя, что когда обновляется антивирус, установленный на том же компьютере, он замечательно работает с именем (как на скриншоте), а вот на других компьютерах я вбивал IP-адрес, потому что не все они почему-то принимали имя. По большому счету, и на том же компьютере можно использовать IP – это никак не повредит.

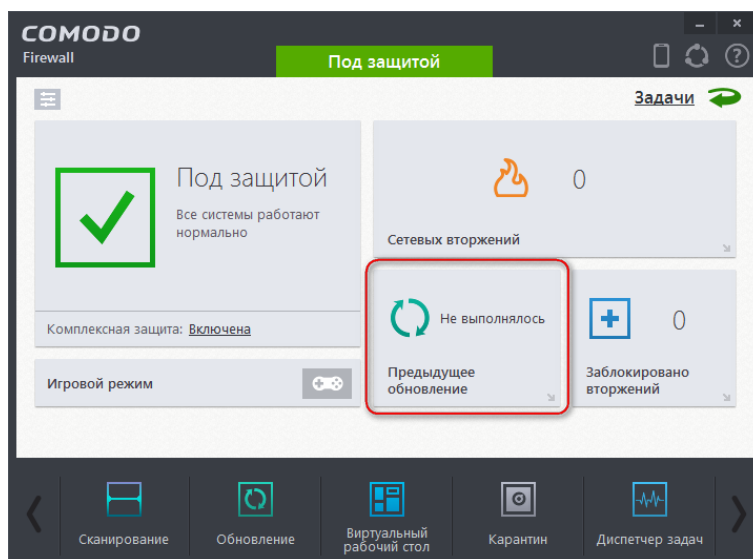
Порт – 88, поскольку именно этот порт указан в настройках **Comodo Offline Updater**, и именно этот порт данный прокси-сервер будет «слушать» на предмет обращений антивируса за обновлениями.

В поле «Серверы» нажимаем на стрелочку вниз, и в открывшемся меню нажимаем «Добавить»

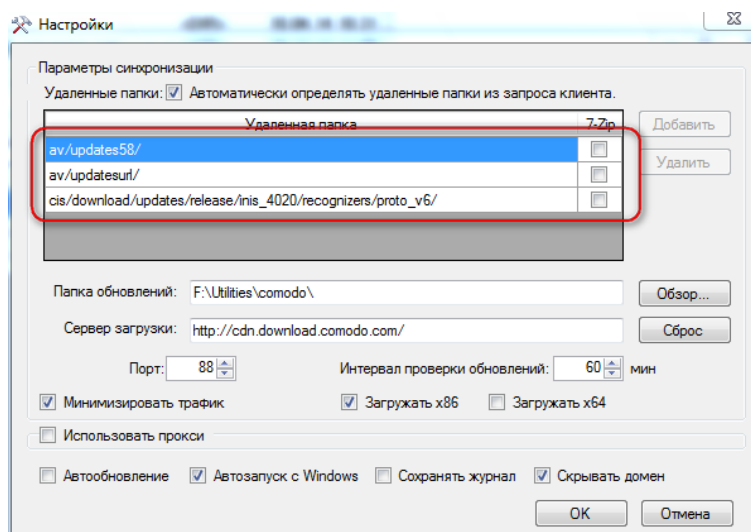


В появившееся окно вбиваем адрес сервера вида `http://[имя_компьютера]/` или `http://[IP-адрес]/`. В любом случае обратите внимание на слеш в конце! После того, как сервер добавлен, сервер обновлений Comodo можно либо вовсе удалить (включаем галку напротив него, и жмем «Убрать из списка» в том же выпадающем меню, где мы нашли «Добавить»), либо поместить ниже созданного нами. Все, настройка обновлений антивируса завершена.

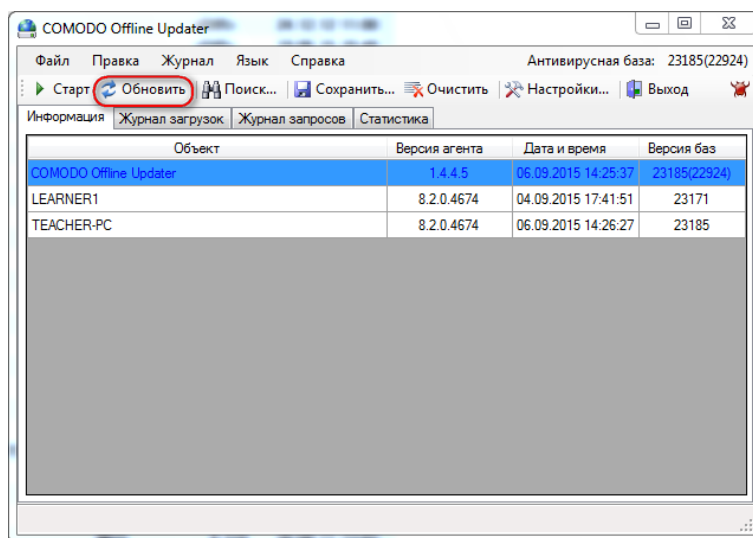
Теперь запускаем обновление антивируса.



Оно завершится ошибкой, поскольку никаких баз антивирус, естественно, не найдет. Но это хорошо, это так и должно быть! Зачем нам это нужно? Дело в том, что на данном этапе **Comodo Offline Updater** зафиксирует попытку обновить базы от нашего антивируса, и сможет считать его версию, а, следовательно, те необходимые обновления, которые ему нужны и те самые удаленные папки, в которых на сервере **Comodo** лежат эти обновления. Действительно, если мы откроем настройки, **Comodo Offline Updater**, то мы убедимся, что список удаленных папок больше не пуст. Он сформирован исходя из запроса клиента.



Вот теперь можно запускать обновления в **Comodo Offline Updater**.



За ходом обновления можно следить по журналу загрузок. Когда обновление будет завершено, запустите обновление базы на антивирусе, и вы увидите, что он теперь обновляется с сервера обновлений **Comodo Offline Updater**. Что и требовалось доказать, как говорится!

Попробуем подвести краткие итоги этой совсем не маленькой статьи.

1. Не каждый бесплатный антивирус в действительности можно устанавливать на учебные компьютеры. В большинстве случаев это ведет к нарушению законодательства.
2. В числе антивирусов, которые могут быть установлены на компьютеры в учебном заведении, можно назвать:
 - **NANO Antivirus**
(http://www.nanoav.ru/index.php?option=com_content&view=article&id=4&Itemid=78&lang=ru)
 - **COMODO Antivirus**
(<https://www.comodo.com/home/internet-security/free-internet-security.php?key5sk0=2128&key5sk1=e340515d16fa1aa8f71dbcbdddb8d98c249bb709>).
3. Оба данных антивируса вполне справляются с поставленными задачами, оба достаточно требовательны к системным ресурсам и не очень уютно чувствуют себя на устаревших машинах (возможно, **NANO Antivirus** в чуть большей степени, нежели **Comodo**).
4. В **NANO Antivirus** есть встроенная возможность создать при обновлении локальное зеркало, которое затем можно при помощи общего доступа сделать доступным для обновления всех компьютеров локальной сети. В этом – несомненный плюс данного антивирусного продукта.
5. В **Comodo Antivirus** подобной возможности нет, но она может быть реализована сторонним приложением **Comodo Offline Updater**, которое после небольших манипуляций становится отличным сервером обновлений.

Надеюсь, эта статья окажется полезной для Вас. С удовольствием отвечу на вопросы и комментарии.