

Информационная безопасность образовательного учреждения. Использование компьютерных технологий и работа в сети Интернет

© Баданов А.Г. badanov1@YANDEX.RU 2010

Информационная безопасность образовательного учреждения. Использование компьютерных технологий и работа в сети Интернет.....	1
Введение.....	2
Сайт образовательного учреждения.....	4
О школьном сайте.....	5
Инструментарий, свободно доступный в сети Интернет для ОУ (хостинг, конструкторы сайтов и др).	6
Локальная сеть образовательного учреждения.....	8
Основы безопасности информации и рекомендации по использованию различных программ. Защита и восстановление целостности информации.....	12
Свойства информации, связанные с ее безопасностью:.....	12
Организация защиты информации:.....	12
Основные правила безопасности:.....	13
Наиболее распространенные симптомы заражения.....	18
Проверка компьютера на вирусы.....	19
До того, как приступить непосредственно к лечению (рекомендуется):.....	21
Что еще необходимо учесть, если на компьютере обнаружались вирусы:.....	22
Использование Диска Live CD «BART» или аналогичного по применению.....	23
Пример инструкции на АРМ ОУ по вопросам безопасности.....	24
Контроль над использованием не санкционированных к использованию программ в рамках ОУ.....	25
Виртуальные машины.....	26
Установка и настройка виртуальной машины SUN Virtualbox.....	27
Установка Операционной системы Windows XP на виртуальную машину.....	34
Установка виртуальной машины Virtual PC 2007.....	34
Установка Операционной системы на виртуальную машину.....	39
Свободное программное обеспечение, ориентированное для использования в образовательной среде и свободно распространяемые полезные программы для работы с информацией.....	40
Видеоролики, демонстрирующие установку, настройку различных программ для обеспечения информационной безопасности.....	40
Настраиваем интегрированный брандмауэр компании Microsoft.....	41
Использование антишпионской программы Comodo.....	42
Проверка съёмных носителей на вирусы.....	44
Резервное копирование данных с помощью программы Cobian Backup.....	46
Установка программы Cobian Backup.....	46
Настройка заданий Cobian Backup 8.....	47
Полезные ссылки.....	51
Литература и документы.....	54

Введение

Эта книга написана для практического использования в деятельности образовательного учреждения наиболее интересных и эффективных решений, как по организации безопасной единой информационной среды образовательного учреждения, так и по организации личной информационной безопасности. В книге приводятся ссылки на разнообразные программные продукты и технологические решения, которые можно использовать как лично, так и в образовательной или иной деятельности (кроме коммерческой), без дополнительных расходов на приобретение этих продуктов.

Материалы книги позволят вам рассмотреть различные варианты организации Единой информационно-образовательной среды (ЕИОС) и элементов ЕИОС в образовательном учреждении. Это организация Интернет - представительства ОУ (сайт школы), использование безбумажного документооборота, организация защищенных сегментов локальной сети, вопросы информационной защиты, защиты персональных данных и др...

Единая Информационно-образовательная среда – это совокупность (система) информационной, технической и учебно-методической подсистем, целенаправленно обеспечивающих учебный процесс, а также его участников.

Стратегическая цель информатизации – создание условий подготовки участников образовательного процесса к полноценной жизни и деятельности в информационном обществе за счет повышения качества образования посредством формирования единой информационно-образовательной среды и интенсивного внедрения информационно-коммуникационных технологий в образовательный процесс.

Как правило, в школах не всегда работают специалисты, способные быстро находить решение различных вопросов обеспечения информационной поддержки образовательной и административной деятельности, принимать действенные решения по постоянно возникающим проблемам организации информационной безопасности. Понятно, что все эти проблемы в каждой школе приходится тем или иным способом устранять, вне зависимости от того, есть подготовленные специалисты в школе или их нет. Чем больше в нашем образовании будет людей, знающих как справиться с возникающими сложностями в обеспечении информационной безопасности, тем комфортнее будет работать всем участникам образовательного процесса. Личную информационную безопасность также невозможно отделить от работы, хотя бы только по тому, что работа чаще всего продолжается и дома за компьютером... Поэтому предложенные материалы рассчитаны не только на технических специалистов или учителей информатики, а на всех, кого они заинтересовали. Для этого в отдельных разделах книги предложены очень подробные алгоритмы действий с полезными и ценными компьютерными программами, которые

позволят организовать свое защищенное информационное пространство, как дома, так и на рабочем месте.

Сайт образовательного учреждения.

О школьном сайте

Для того, чтобы появился эффективно работающий школьный сайт необходимо иметь четкое представление - для чего он нужен и какие задачи школа намерена с его помощью решать. Это вопрос главный, ибо без его решения проектировать меню, разрабатывать разделы, вводить сервисы – во всем этом смысла просто нет. Рассмотрим ряд целей, которые можно использовать за основу:

- **«Сайт - площадка внутришкольного взаимодействия».** Возможность общения между детьми, педагогами в неформальной обстановке. Возможность размещения и использования дистантных модулей и программ, возможность для детей, в силу различных причин, не посещавших занятия или не имеющих такой возможности усваивать рабочий материал. Комментируемые новости составят своеобразную летопись жизни школы. Это одновременно и выход во внешнее пространство. Возможность для педагогов, представляя свое образовательное учреждение, давать ответы на вопросы, которые в привычной, повседневной деятельности только внутри своего коллектива сложно осмыслить:
 - в каком направлении осуществляется развитие школы?
 - какова ценностная основа, педагогическая, методическая концепция (идея, кредо) школы?
 - в чем заключается характерное отличие нашего учебного заведения от другого (и есть ли оно вообще)? и др.

Школьный сайт может также рассматриваться в качестве коммуникативного инструмента не только администрации, педагогов и учеников, но и «внешних» по отношению к образовательному учреждению субъектов – родителей, работников образования и культуры и др. В этом качестве школьный сайт способствует повышению открытости образовательного учреждения, создает такие контактные возможности, которые в обычной жизни зачастую затруднены.

- **«Визитка школы».** Школьный сайт также может выполнять функцию визитной карточки школы – со своим уникальным стилем и характерной для данной школы формой подачи материала. Это своеобразная рекламная площадка для привлечения внимания к школе. Что позволит привлечь в школу больше детей. Поэтому так важно точно и корректно сформулировать для сайта, в чем

своеобразие данной педагогической системы, чем она отличается от других. Полная, конкретная и выгодная подача информации о специфике реализуемых в школе программ сможет привлечь к ней внимание, что поможет образовательному учреждению не потеряться в кругу подобных учреждений образования.

- **«Школьный сайт как элемент единой информационной образовательной среды города (района)».** Школьный сайт может выступать элементом образовательной Интернет-системы (естественно, при условии существования последней). Это, безусловно, не является конкретной целью школьного сайта, скорее, в этом качестве сайт может работать одним из информационных субъектов, комплекс которых в состоянии отражать динамически меняющуюся образовательную картину в рамках района, города, региона.

Инструментарий, свободно доступный в сети Интернет для ОУ (хостинг, конструкторы сайтов и др).

Для создания сайта всегда требовалось быть технически грамотным человеком, владеющим технологиями современного программирования в сети Интернет. Заведомо считалось, что это весьма дорогостоящее и трудоемкое дело. Да, сейчас эти знания так же важны, но вместе с тем прогресс в области сайтостроения не стоит на месте. Сейчас для того, чтобы создать Интернет-представительство школы не нужно ни денег, ни знания WEB программирования. В сети есть множество бесплатных сервисов, построенных на основе шаблонов, где достаточно только подобрать интересный шаблон и наполнить его своим содержанием. А по мере развития требований к сайту переводить его на более гибкие технологии, но думаю, к этому времени в каждом ОУ появятся энтузиасты и фанаты школьного интернет пространства и будут четко сформулированы цели, которые преследует школа, создавая собственный официальный сайт. Эти технологии будут постепенно подключаться к уже существующему сайту. Вот подборка ссылок на эти инструменты:

- <http://narod.yandex.ru/> - конструктор сайтов, доменное имя, шаблоны, до 100 мегабайт бесплатно.
- <http://www.proshkolu.ru> проект Учительской газеты. Набор сервисов и интерактивов, доменное имя и хостинг-бесплатно. Размер сайта не ограничен.
- <http://joomlaportal.ru/> Joomla – конструктор сайтов – бесплатно. Гигантское количество шаблонов. Сам сайт можно разместить на бесплатном хостинге и заниматься его наполнением.

- <http://agava.ru> Для бесплатного размещения сайтов учебных заведений и частных некоммерческих проектов AGAVA с 1 января 2010 г. запускает хостинг-тариф «Социальный». Параметры нового тарифа практически идентичны тарифу [Normal](#): 2Гб дискового пространства, FTP/SSH доступ, поддержка скриптов, MySQL 5.0, почтовые сервисы, ежедневный архив информации и круглосуточная техподдержка. бесплатно хостинг по тарифу «Социальный» учебным заведениям, а также сайтам, которые принадлежат физическим лицам и посвящены воспитанию, образованию, медицине или иной социально значимой теме. Клиенты могут выбрать бесплатные доменные имена в зонах hostedu.ru, sochost.ru, social-host.ru или использовать собственный домен.
- <http://edu.of.ru/default.asp> Проект Министерства образования РФ «Конструктор образовательных сайтов». Доменное имя, хостинг, система управления сайтом, шаблоны, помощь и консультации. В этой системе сделаны сайты множества ОУ, в том числе и отделы образования некоторых районов РФ.
- <http://dnevnik.ru> «Дневник.ру» - официально зарегистрированный [оператор персональных данных](#). "Дневник.ру" – всероссийская школьная образовательная сеть для педагогов, учеников и их родителей. Цель интернет-проекта - создание единой информационной и образовательной сети для учителей, учеников и их родителей. "Дневник.ру" предоставляет школам ряд бесплатных сервисов, в числе которых сервисы "Общение" (страницы школ и отдельных пользователей, обмен сообщениями), "Учеба" (расписание уроков, оценки, домашние задания и персональный календарь), "Электронный дневник учащегося", "Электронный журнал учителя", "Электронная библиотека", "Конструктор школьного сайта". Дневник.ру разработан совместно с Институтом стратегических исследований в образовании РАО.
- <http://ksdk.ru> Хостинг предназначен для создания сайтов детских творческих коллективов, относящихся к дополнительному образованию. Имеется конструктор сайтов, выделение доменного имени. Сайты можно делать для учреждений дополнительного образования и творческих коллективов. Оформление из шаблонов или собственное. Очень простая система управления. В комплекте адрес электронной почты.
- <http://www.ucoz.ru/> система управления сайтом, доменное имя и неограниченное дисковое пространство для хостинга. Все сервисы для школ бесплатны.

- <https://jlkhosting.com/> 200 мегабайт дискового пространства и хостинг бесплатно.
- <http://letopisi.ru/> -вики среда, в которой также можно создавать небольшие странички. Имеются шаблоны.

Платно. Их много. Вот, например школьный проект Национального фонда подготовки кадров:

«Школьный сайт» <http://www.edusite.ru/> Конструктор школьных сайтов Стоимость Конструктора и размещения сайта неограниченного размера составляет 1500 руб/год.

Локальная сеть образовательного учреждения.

В каждом ОУ, компьютеры которого подключены к сети Интернет, возникает вопрос, как организовать локальную сеть которая бы связывала ОУ и с помощью которой можно было бы организовать без больших финансовых затрат, что весьма немаловажно в нашем образовании, возможность реализации различных задач, возникающих внутри каждой школы. Это задачи административные и образовательные.

Вот перечень основных задач, которые ставятся в ОУ:

- Доступ к сети Интернет
- Организация файлообменной сети
- Автоматизация управления ОУ и организация безбумажного документооборота
- Медиабiblioteca
- Электронная почта
- Школьный форум
- Иные задачи, например использование сетевого принтера, организация беспроводной зоны доступа, организация беспроводного серфинга в сети Интернет и др.

Часть задач решается при создании простейшей локальной сети в которой компьютеры через сетевых концентраторов (Свич) соединены между собой с помощью кабеля (витая пара) оснащенного коннекторами. Для этого достаточно присвоить школьным компьютерам IP адреса из диапазона, предназначенного для использования в каждой школе. И назначить шлюз. Как правило, после того, как школы были отключены от централизованного подключения к сети Интернет, специалисты организаций, которые обеспечивают доступ к сети Интернет настроили Ваши ADSL модемы таким образом, что для подключения к сети Интернет других компьютеров нет необходимости вводить IP адреса персональных АРМ и шлюза и он генерируется для этих машин автоматически. Для примера приведу ручные настройки сетевого подключения.

IP адрес 192.168.1.* (автоматически он генерируется или вводится вручную в диапазоне от 2 до 255)

Маска подсети 255.255.255.0

Основной шлюз 192.168.1.1

Использовать следующие адреса DNS-серверов 77.40.0.2 и 77.40.0.3

На всех компьютерах реализуется только доступ к сети Интернет и будет возможно решение любых локальных задач на каждом отдельно взятом ПК.

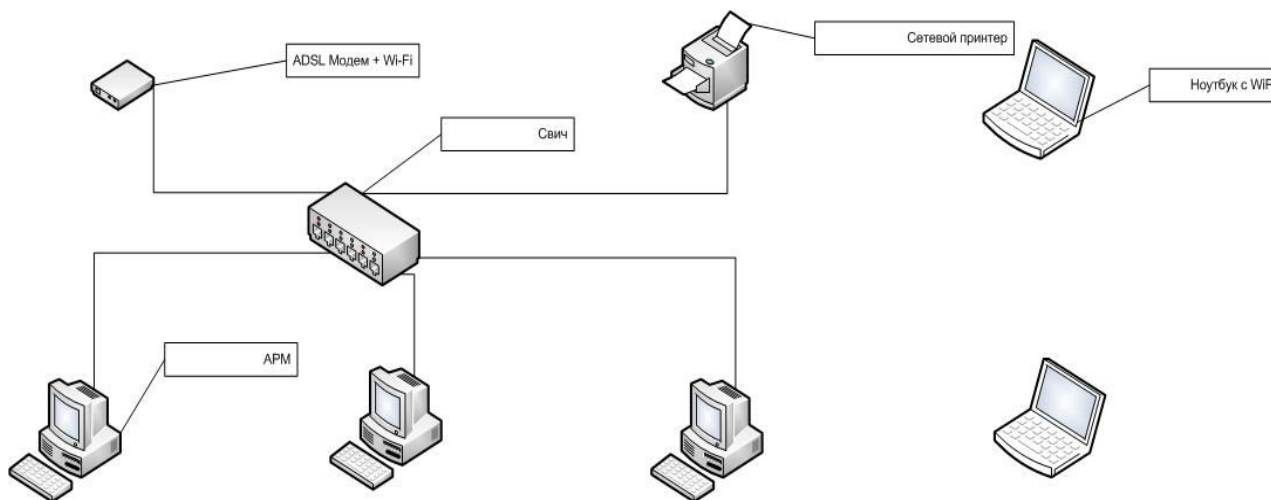


Рис1. Схема стандартной локальной сети ОУ

Если же открыть для общего использования отдельные папки («расшарить» их) на каждом компьютере можно таким образом организовать на этом же оборудовании и файлообменную сеть. Использование подобной структуры увеличит вероятность возникновения проблем сетевой безопасности. Когда ученик видит в сетевом окружении компьютер директора, он может испытать соблазн зайти к нему в гости, что в принципе возможно, при всех ограничениях прав и дроблении учетных записей. Поэтому совершенно излишня в учебном процессе та ситуация, когда на ученических дисплеях отображаются компьютеры школьной администрации или бухгалтерии. Помимо этого существует проблема «10 компьютеров», когда к одному и тому-же ресурсу в школьной локальной сети на может подключаться более 10 компьютеров, что создает серьезные трудности в использовании подобных ресурсов в образовательных или иных целях.

Решается эта проблема достаточно просто. На учительский компьютер, скажем, в

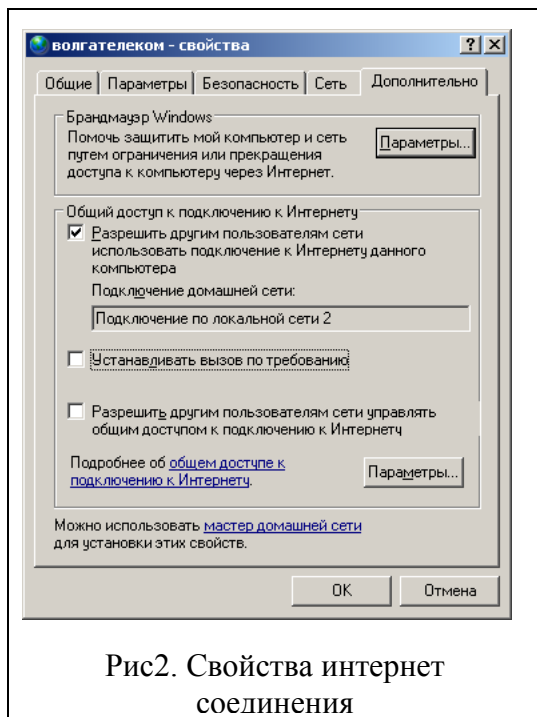


Рис2. Свойства интернет соединения

кабинете информатики, ставится вторая сетевая карта. Подключается к карте кабель и соединяется со свичем, через который подсоединены ученические компьютеры (Первая сетевая карта соединена с модемом и подключена к Интернету). Устанавливаются с диска или скачиваются с Интернета соответствующие драйвера. После этого в окне Сетевые подключения (Пуск-Панель управления- Сетевые подключения) появляется значок: Подключение по локальной сети2. Затем открываем Подключение по локальной сети(т.е. работаем с первой сетевой картой, которая подключена к Интернету)-Свойства-Дополнительно

и ставим галочку в чекбоксе Общий доступ подключения к Интернет.

После разрешения общего доступа появляется диалоговое окно, в котором говорится о том, что ip-адреса будут автоматически изменены у клиентских компьютеров, т.е тех компьютеров, которые будут подключаться к Интернету через вторую сетевую карту. Нажимаем ОК.

Остается только пройтись по ученическим компьютерам и установить на них получение ip-адреса из того диапазона адресов, которые вы будете генерировать с помощью второй сетевой карты в школьный класс. Эти адреса отличаются от тех, которые генерирует ADSL модем (они приведены выше).

Ученики получают через учительский компьютер выход в Интернет, а в сетевом окружении видят компьютеры только своего класса. Компьютер учителя играет роль сервера и диапазон адресов у него от 0 до 255. При этом нужно не забывать, что ученики не должны иметь административные права на своих рабочих местах. В этом случае у них будет отсутствовать возможность смены выделенных IP адресов на своей машине. А учитель всегда сможет регулировать подачу интернет к рабочим местам учеников по мере необходимости, включая или отключая вторую сетевую карточку в разделе Сетевые подключения, расположенной на Панели управления компьютера. При этом можно настроить Брандмауэр Windows на этом сетевом подключении, ограничив получение информации с различных сомнительных адресов.

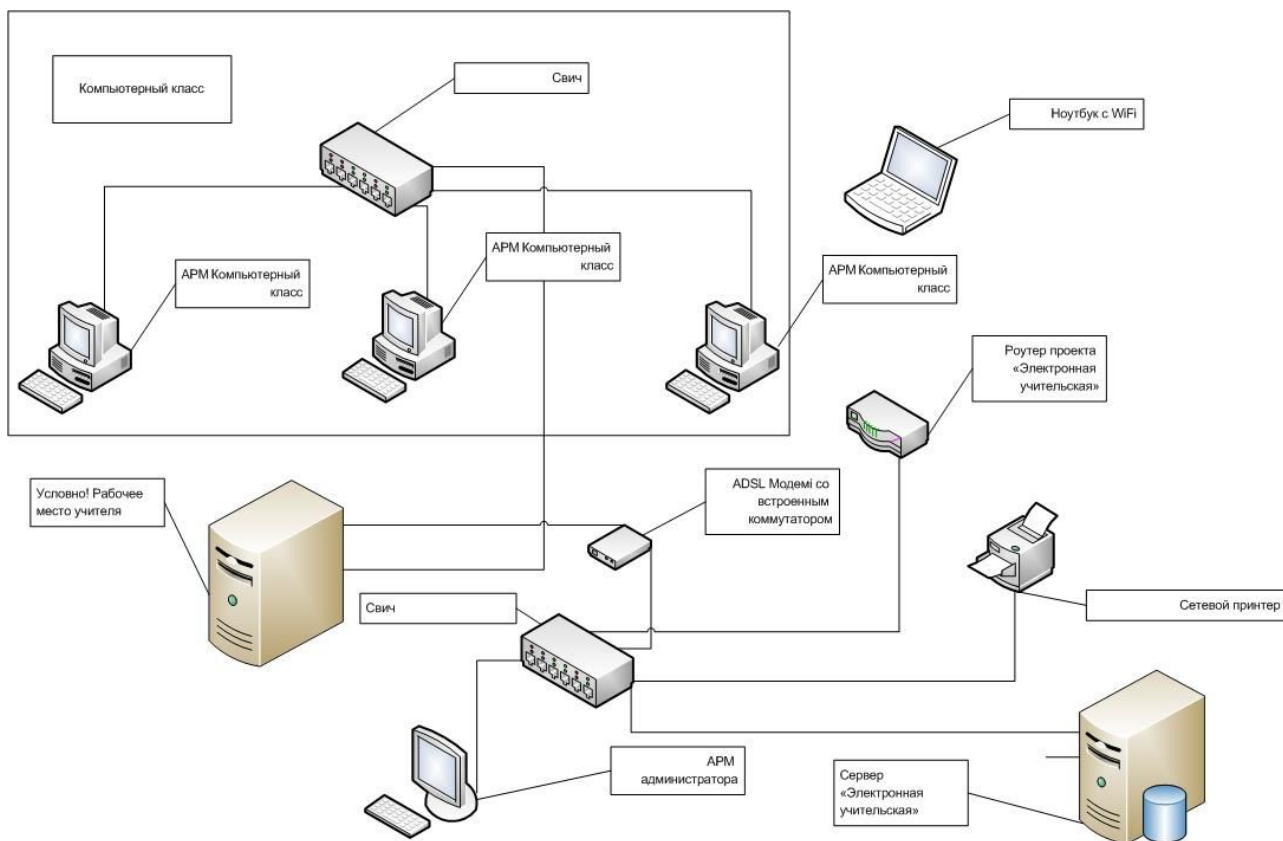


Рис3. Так выглядит предложенная выше конфигурация локальной сети

Существуют и более современные варианты организации локальных сетей, которые можно использовать в образовательном учреждении, все они используются в той или иной мере в различных регионах РФ. Все зависит от тех целей, которые поставила школа и финансовых возможностей которыми располагает школа. Это, например - вариант с выделенным сервером, через который организован доступ к сети Интернет, авторизация и раздача прав пользователям локальной сети. В случае использования сервера в школе легче будет организовать сетевую фильтрацию информационного содержимого сети Интернет, которая может отображаться на компьютерах школьников. Школы «миллионеры» и ресурсные центры получили помимо пакета «Первая помощь» еще и дополнительный пакет, где имеется дистрибутив Windows Server 2003. Хотя всем остальным можно использовать серверные возможности программ с открытым кодом Linux. Это наиболее защищенный в вопросах безопасности вариант организации локальной сети образовательного учреждения.

Внимание! При работе в локальной сети компьютеров с XP и VISTой настроить сеть будет значительно сложнее.

Проблему большого количества проводов (которые придется тянуть по всей школе), можно решить с помощью организации беспроводной сети с правильно установленными маршрутизаторами (появились стабильно работающие маршрутизаторы с аббревиатурой N,

которые обеспечивают по своим каналам большую скорость, пригодную даже для трансляции видео высокой четкости), которые позволят охватить всю школу хорошо работающей локальной сетью. Для разграничения пользователей, которых необходимо будет подключать к беспроводным точкам доступа при приобретении такой точки доступа обратите внимание на ее многодиапазонность, это как раз и позволит разграничить полномочия клиентов. Уровень защищенности определяется ключами шифрования, которые будут использоваться в работе локальной сети. А на стационарные компьютеры просто напосто устанавливаются либо PCI, либо USB адаптеры, на современных ноутбуках эти возможности технически сразу реализованы. Это позволит в буквальном слове окутать школу «дымкой Интернета». Сеть будет доступна (и подконтрольна) в любой точке школы и части школьного двора. Для этого необходимо только настроить, в зависимости от того какие возможности нам будут необходимы, точки доступа, которых на типовое школьное здание достаточно 4-6. И никакие ремонты здания, обрывы проводов, проблемы переноса компьютерной техники из помещения в помещение не будет пугать нас своей дополнительной работой по ремонту или монтажу/демонтажу большого количества проводов. Есть небольшой нюанс. Для организации беспроводной сети необходимо будет получить разрешение на использование беспроводных точек доступа, эти разрешения оформляются в Россвязьнадзоре и действуют в течение 10 лет.

Основы безопасности информации и рекомендации по использованию различных программ. Защита и восстановление целостности информации.

Свойства информации, связанные с ее безопасностью:

- Конфиденциальность.
- Целостность (некий набор фактов, не подлежащий изменению).
- Доступность (информация может быть доступна только определенному кругу людей).

Организация защиты информации:

- Технические средства. В настоящее время существует большое разнообразие технических средств защиты. К числу таких средств относятся программные, аппаратные и программно-аппаратные комплексы, обеспечивающие выполнение различных функций защиты информации. К ним относятся системы разграничения доступа и аудита доступа, обеспечивающие упорядочивание и отслеживание операций, производимых пользователями над объектами (файлами и папками).

- Криптографические средства, обеспечивающие шифрование информации и механизмы проверки подлинности (цифровая подпись и сертификаты).
- Антивирусные мониторы, фильтры, сканеры.
- Межсетевые экраны (брандмауэры) и шлюзы.
- Средства обеспечения отказоустойчивости и резервного копирования. Регулярное резервное копирование и архивирование наиболее важной информации – один из основных способов ее сохранения.

Основные правила безопасности:

Для того чтобы защитить свой компьютер нужно совсем не так много усилий, как кажется некоторым на первый взгляд. Главное, прилагать эти усилия заблаговременно (т.е. заранее), а не тогда, когда у вас начнут появляться проблемы... И не менее важно быть всегда последовательным и аккуратным в вопросах организации защиты информации на собственном ПК. Я очень быстро пройду по основным «бастионам» защиты и подробнее на особенностях тех или иных программ.

1. Регулярная установка всех критических обновлений ОС (операционной системы).

Это обычно производится с помощью сайта компании Microsoft Update: <http://update.microsoft.com> комментировать процедуру обновления операционной системы нет необходимости. Все это происходит, как правило, в автоматическом режиме. Пользователю потребуется только ответить на несколько вопросов и предложений. Для школ более приемлемым может быть вариант, когда скачиваются с портала компании Microsoft все критичные обновления и Сервис Паки и затем локально устанавливаются на все школьные компьютеры. Это позволяет экономить трафик (соответственно и деньги за Интернет) а при медленном и не стабильном подключении к сети Интернет будет более эффективно. Потому что при обрыве соединения всю работу придется переделывать снова и снова, пока не закачается обновление

2. Установка антивирусной программы. Одна из самых популярных в России

антивирусных программ - Антивирус Касперского (имеется в пакете Первая Помощь). К сожалению, на слабых машинах (а их большинство, особенно в регионах) антивирус Касперского заметно тормозит работу системы и программ. Хотя, как советуют специалисты «Лаборатории Касперского» (<http://www.openclass.ru/forums/100862>) ускорить работу антивируса можно, для этого нужно будет его тщательно перенастроить под возможности своего компьютера. Это не всегда устраивает пользователей, поэтому попробуйте присмотреться к альтернативным, бесплатным

программам. Популярны бесплатные программы:
avast! Home Edition <http://www.avast.com/eng/download-avast-home.html>
AntiVir® PersonalEdition Classic <http://free-av.com/en/download/index.html>
AVG Free <http://free.grisoft.com>; Microsoft Security Essentials
http://www.microsoft.com/Security_essentials/.

Не за горами тот день, когда пакет программ «Первая помощь» станет невозможно использовать в полном объеме. И проблема использования и выбора антивируса перед не самым богатым российским образованием действительно станет проблемой! За каждый платный антивирус на 1 компьютер в год придется платить около 800 рублей. И так каждый год. Посчитайте, сможет ли школа эту финансовую нагрузку потянуть. Кроме этого важно иметь в виду, что антивирусная программа на компьютере должна быть только одна. Компьютер просто перестанет работать, если на нем, например, с целью большей защищенности будут поставлен еще один или больше антивирусов. Не забывайте, что антивирусные базы требуют ежедневного обновления. Обновление, как баз вирусов, так и самих программ происходит в основном с помощью сети Интернет. Программы "сами об этом знают" и самостоятельно (по вашему разрешению либо отдельно, либо в процессе установки) будут обновлять базы и версии программ. Хотя есть и среди бесплатных программ, такие программы, которые позволяют эти обновления скачивать и затем уже локально устанавливать на свои компьютеры, не тратя трафика.

3. Использование фэйервола (встроенный брандмауер есть в Windows и можно им воспользоваться) или попробовать использовать бесплатный фэйервол, например Comodo Firewall <http://www.personalfirewall.comodo.com/>. Это один из популярных в сети Интернет фэйерволов.
4. Установка операционной системы в нестандартный каталог, например OS, MyWindows и т.д. Это позволит ввести в заблуждение отдельные вредоносные программы, которые используют жестко закрепленные пути, например C:\Windows. Правда как бы и самому не запутаться, где тут у меня установлена операционная система.
5. Использование альтернативного браузера, так как большинство вирусов написаны в расчете на использование пользователем стандартной программы Internet Explorer то большинство случаев заражения происходит через уязвимости этого популярного браузера. Хотя с 1 марта 2010 года компания Microsoft в комплект дистрибутива операционной системы включила и альтернативные браузеры. Использование альтернативной программы позволит резко снизить вероятность поражения компьютера через браузер. Хотя IE так же придется оставить на компьютере, так как

отдельные интерактивные формы, заполняемые в сети Интернет могут не работать с бесплатными альтернативными браузерами. Вот ссылки на наиболее популярные программы:

Mozilla Firefox <http://www.mozilla.ru/>; Opera <http://www.opera.com/download/>.

***Внимание!** Для более эффективной организации информационной безопасности при использовании браузера Mozilla Firefox можно добавить браузеру с помощью меню Инструменты – Дополнения специальные модули. Их множество. Вот большой перечень рекомендуемых <https://addons.mozilla.org/ru/firefox/browse/type:1/cat:12>*

Наиболее востребованы:

***Adblock Plus** – не пропускает и (или) блокирует нежелательные окна, рекламу;*

***NoScript**–регулирует исполняемость скрытых команд- скриптов на веб страницах.*

6. Использовать вспомогательные программы для обеспечения защиты своего компьютера. Одна из наиболее популярных программ **Spybot - Search & Destroy** (**Спайбот - найти и уничтожить**) поможет обнаруживать и удалять с Вашего компьютера различного рода шпионское программное обеспечение. Сайт поддержки - <http://www.safer-networking.org/ru/home/index.html>. На странице <http://www.safer-networking.org/ru/tutorial/index.html> размещён учебник с почти пошаговой инструкцией установки и использования данной программы.

7. Отключить возможность автозапуска и автозагрузки на компьютере, эти функции используют вирусы, которые приходят к нам с помощью носителей информации. Это легко можно сделать, воспользовавшись программой **Autorun Guard**. Это бесплатная программа для управления автозапуском на внешних носителях в ОС Windows. Она позволяет полностью отключить автозапуск в Windows и тем самым **защититься от проникновения autorun-вирусов**, она также позволяет восстановить работу автозапуска, если автозапуск или автозагрузка были нарушены сторонними программами. <http://autorunguard.com/ru/>. Эту операцию можно сделать и вручную с помощью использования параметров групповой политики для отключения всех функций автозапуска (пример для ОС Windows XP):

- Выберите в меню **Пуск** пункт **Выполнить**, введите Gpedit.msc в поле **Открыть** и нажмите кнопку **ОК**.
- Последовательно разверните узлы **Конфигурация компьютера**, **Административные шаблоны** и **Система**.

- В области **Параметры** щелкните правой кнопкой мыши элемент **Отключить автозапуск** и выберите пункт **Свойства**.

Примечание. В системе Windows 2000 параметр политики называется **Отключить автозапуск**.

- Щелкните элемент **Включено**, а затем выберите вариант **Все диски** в окне **Отключить автозапуск**, чтобы отключить автоматический запуск для всех дисков.
- Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Свойства выключения автозапуска**.
- Перезагрузите компьютер.

8. Архивирование важных данных. Особенно **важно** работая с базами, например с базой ОУ Хронограф Школа 2,5, которая активно используется многими школами, с целью сохранения информации необходимо регулярно сохранять копию этой информации на отдельном жестком диске или удаленном компьютере (можно ежедневно). В случае возникновения либо технических, либо программных проблем с сервером либо локальным компьютером на котором так же может храниться важная информация использование пользователем программы для **архивного копирования** позволит избежать потерь рабочей информации. А это большой человеческий труд и временные издержки, которые непременно бы возникли. Ярким примером подобных программ может служить свободная программа **Cobian Backup** <http://www.cobian.se>. Эта программа может работать как автоматически – по расписанию или в ручном режиме - по требованию пользователя АРМ.

9. Оптимизация операционной системы и наиболее часто использующихся программ. Программа **Xp-AntiSpy** <http://www.xp-AntiSpy.org> поможет изменить некоторые настройки операционной системы Windows и пакета программ Microsoft Office с целью отключения не нужных вам в вашей работе сервисов, в частности: **автозагрузки**, ограничение количества ПК в локальной сети (свыше 10 машин в случае одноранговой сети), отчетов об ошибках, работы с мультимедиа и др. **Оптимизировать** систему и работу отдельных программ можно при помощи программ - твикеров, позволяющих в считанные минуты устранить неполадки в системе и ускорить работу. Одной из них является **BoostSpeed**. <http://www.auslogics.com>. Lite версия этой программы бесплатна, в ней есть все необходимое для комплексной оптимизации системы. Программа может постоянно работать с ядром операционной системы, удерживая системные файлы в оперативной

памяти. Саму оперативную память пользователь может высвободить под любые нужды в любой момент. Также программа оптимизирует файловую систему и автоматически или по вашему требованию отключит невостребованные системные службы. Кроме этого пользователь может увеличить скорость загрузки Windows, выбрать оптимальный по скорости работы внешний вид операционной системы, ускорить работу почтовых и офисных программ, браузеров и некоторых системных компонентов. Помимо выше перечисленного BoostSpeed имеет несколько дополнительных утилит, среди которых есть Banner Killer — утилита, блокирующая нежелательную рекламу. В ее постоянно обновляемой базе данных имеется список сайтов, с которых обычно загружаются всплывающие окна.

10. Схема распределения ролей в сети: т.е. для каждой группы пользователей свои настройки. Вход, естественно, под паролем. Рекомендуется пароль администратора – не менее 10 символов, а пароли пользователей не менее 6 символов. Т.е. возникают группы учитель, ученик, администратор. В рамках этих групп устанавливаются ограничения на пользование сетью и доступ к определенным ресурсам и возможностям. Там же может быть ограничено время пребывания в сети, доступ к ряду "опасных" сайтов, например, для учеников. Вариантов может быть несколько: администратор; учитель; ученик старшей школы, среднего звена, начальной школы. Наиболее полно можно настроить ограничения на отдельных компьютерах и в случае с одноранговой сетью при использовании ОС Vista и 7. При использовании выделенного сервера настроить взаимоотношения с пользователями можно максимально эффективно для обеспечения условий безопасности работы с информацией.

11. Осуществлять режим жесткого входного контроля всей информации, которая поступает на ваш компьютер, от электронной почты до любых документов, которые вам принесли на флешке. Для того чтобы обезопасить себя от случайного поражения вирусами вашего компьютера необходимо быть внимательным в общении и не общаться со случайными людьми (электронная почта) и различными сайтами. Это может произойти в основном в двух случаях: если вы посещаете сайты сомнительного содержания и открываете постороннее вложение в электронных письмах (программы, документы, картинки и др). В первом случае достаточно свести к минимуму посещение сомнительных сайтов. Правда для этого существует система СКФ, которую тоже необходимо настраивать и регулярно пополнять базу программы ссылками на недопустимые адреса, установленная на каждом компьютере в школе. Интернет в школе можно «раздавать» (осуществлять входной контроль и запросы пользователей) с помощью бесплатного варианта программы NetPolice Lite

<http://www.netpolice.ru/filters/netpolice-lite/>. Это контент фильтр, который позволяет весьма эффективно ограничивать посещение нежелательных сайтов. Возможность ограничения нежелательного контента можно организовать с помощью дополнения к известному браузеру Mozilla Firefox в виде детского браузера Гогуль <http://www.gogul.tv/>, который обеспечит контроль посещения ребёнком сайтов в Интернете. Для контроля запуска других браузеров возможно использование бесплатной программы [Angry Duck](#) (необязательный компонент). Со вторым случаем сложнее. Письма с вирусами могут приходить как от незнакомых, так и от знакомых людей. Если пришло письмо от незнакомого человека, и в письме есть вложение, открывать его можно, лишь в том случае, если из текста письма вы чётко поняли: что это письмо для вас; что именно находится во вложенном файле; что содержимое вложения вам нужно. Никогда не следует открывать файлы, которые случайно попали к вам.

Наиболее распространенные симптомы заражения

Их может быть гораздо больше, но это наиболее часто встречающиеся, причем отдельные проблемы могут быть вызваны неправильной работой отдельных программ на вашем компьютере и проблемами в оборудовании системного блока или периферийного оборудования:

1. Спонтанная перезагрузка компьютера, без вашего в этом участия.
2. Появление критических и системных ошибок там, где их раньше никогда не было.
3. Частые зависания и сбои в работе компьютера без видимых на то причин.
4. Резко увеличилось время загрузки операционной системы.
5. Повседневные задачи выполняются компьютером гораздо медленнее, чем обычно.
6. Программы, которые раньше работали, внезапно перестали нормально функционировать или значительно возросло время их обычной загрузки.
7. Ненормальная сетевая активность и обращение по нетипичным вам сетевым адресам.
8. Предупреждения файрвола о попытке выйти в интернет незнакомых вам приложений.
9. Постоянные перебои в работе интернет-соединения или частые зависания браузера.
10. Нет доступа к некоторым сайтам, либо при обращении вместо нужного - открывается совсем другой.
11. Изменились настройки вашего браузера (к примеру, домашняя страница), и вернуть их в желаемое состояние обычными способами не получается.
12. Неожиданное открытие и закрытие CD-ROM'a, либо вообще отказ работать.
13. Стремительное уменьшение свободного места на дисках.

14. Перестали функционировать некоторые системные утилиты (диспетчер задач; regedit; check disk; дефрагментатор и т.д.). Либо по каким-то причинам к ним заблокирован доступ (при этом администратором компьютера являетесь вы).
15. Непонятное завершение антивирусной программы или файрвола.
16. Перезапуск системы в безопасном режиме (Safe Mode) приводит к ее полному зависанию.
17. Компьютер перестает отвечать на ваши запросы и часто блокируется.
18. Невозможность загрузки операционной системы.

Проверка компьютера на вирусы

Теперь самое важное! Все системы защиты информации будут работать действительно на сто процентов, только если вы установите эти программы на чистый без вирусов компьютер. Для того, чтобы убедиться в том, что он чист существуют специальные программы- утилиты, которые к тому же распространяются бесплатно и не требуют установки на компьютер. Эти программы можно запускать с диска (CD или DVD), защищенной от модификаций флешкой (с ключом защиты от записи) или с помощью загрузочного диска (так называемого Live CD)

Теперь попробуем проверить свой компьютер на вероятность его поражения вирусами. Не стоит уповать на уже установленный у вас антивирус, это, к сожалению, не гарантирует компьютер от внедрения вирусов. Только комплексные меры и собственная «чистоплотность» в какой то мере даст вам возможность безопасно работать с информацией.

Проверяем все локальные диски антивирусной программой. Очень удобно здесь как раз и воспользоваться утилитой **CureIt** <http://www.drweb.com>. При обнаружении вируса мы предложим антивирусу попробовать вылечить файл. Если это не получится, то удаляем его совсем. Обычно легко лечатся документы MS Word, Excel и другие документы MS Office. Программные и системные файлы лечатся с большим трудом. Велика доля вероятности, что они не поддадутся лечению. Тогда их надо удалять без сожаления. Потому что это уже не те программы, которые работали на вас. Это уже мутанты, которые никогда не будут делать то, что делали раньше, а будут выполнять новые задачи, поставленные вирусом-писателем, либо компьютер будет вести себя не адекватно вашим действиям с информацией.

Если антивирус будет сообщать о невозможности удаления каких-либо файлов, приготовьтесь перезагрузить компьютер в безопасный режим Safe Mode (Защищенный режим) и повторить сканирование сначала. Хотя есть специальные программы именно для удаления таких проблемных файлов, например Unlocker <http://ccollomb.free.fr/unlocker>

Проанализировать состояние компьютера можно также с помощью утилиты **AVZ** <http://z-oleg.com/secur/avz/> . Антивирусная утилита AVZ является инструментом для исследования и восстановления системы, и предназначена для автоматического или ручного поиска и удаления:

- SpyWare, AdvWare программ и модулей (это одно из основных назначений утилиты);
- Руткитов и вредоносных программ, маскирующих свои процессы;
- Сетевых и почтовых червей;
- Троянских программ (включая все их разновидности, в частности Trojan-PSW, Trojan-Downloader, Trojan-Spy) и Backdoor (программ для скрытного удаленного управления компьютером);
- Троянских программ-звонилки (Dialer, Trojan.Dialer, Porn-Dialer);
- Клавиатурных шпионов и прочих программ, которые могут применяться для слежения за пользователем;

Эта утилита **не лечит компьютер**, а только помогает найти уязвимости и вирусы, которые потом **придется убрать вручную** или с помощью других программ.

Для того, чтобы перевести компьютер в безопасный режим необходимо в момент включения компьютера при появлении меню загрузки Windows нажимать на клавишу "**F8**", чтобы на экране появилось меню дополнительных режимов загрузки. Теперь передвигаемся с помощью клавиш вверх/вниз и, остановившись на надписи "**Safe Mode**" (Защищенный режим), нажимаем "Enter"

Когда сканирование будет закончено, и все найденные антивирусом вредоносные файлы вылечены/удалены, перезагружаем компьютер, и восстанавливаем поврежденную защиту (переустановка антивирусов и вспомогательных программ).

Если после антивирусной чистки перестали работать какие-то нужные вам программы, следует переустановить их с имеющихся у вас дистрибутивов.

Внимание! Например, на сайте поддержки антивирусных продуктов Касперского <http://www.kaspersky.ru/> можно проверить как компьютер целиком, так и отправить отдельный файл на проверку.

Так же имеется сервис <http://www.VirusTotal.com> который анализирует подозрительные файлы и облегчает быстрое обнаружение вирусов, червей, троянов и всех видов

вредоносных программ, определяемых антивирусами. На этом сервисе **можно проверить файл сразу несколькими антивирусами.**

Существует портал «Антивирусная школа» <http://av-school.ru>. Данный портал создан с целью информирования интересующихся пользователей о возможностях использования персонального компьютера в повседневных делах и учебном процессе, формирования понимания роли информационных технологий, получения новых знаний и навыков для работы с компьютером, общения и обмена опытом между участниками. Этот портал создан специалистами «Лаборатории Касперского». Это возможность **получать современные знания в области информационных технологий, компьютерной безопасности**, расширять умения и навыки грамотного пользователя ПК, постоянно обновлять и совершенствовать свои знания в быстро развивающейся области знаний. Работает форум на котором можно задать любой вопрос о проблемах в информационной безопасности.

Форум «VirusInfo» <http://virusinfo.info/forum.php?referrerid=775> здесь также можно получить ответы и помощь в решении проблем информационной безопасности.

Сайт «Безопасность в Интернет» который создан специально для детей, родителей и учителей, на котором можно найти много интересной информации и советов http://www.e-teaching.ru/SiteCollectionDocuments/pil/inet_safety/html/etusivu.htm

До того, как приступить непосредственно к лечению (рекомендуется):

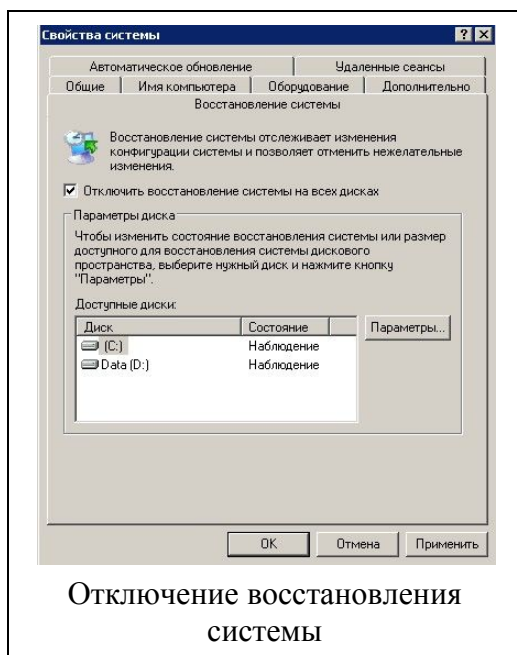
- Пуск > Выполнить впишите **msconfig** и нажмите ОК. В последнем разделе - **Автозагрузка (StartUp)** - уберите галочку напротив всех приложений, в автозапуске которых нет необходимости. Этим вы уменьшите общее время загрузки системы, плюс вполне возможно, предотвратите автоматический запуск потенциально вредоносных программ. Сохраните сделанные изменения - Применить и ОК.
- Удалите все временные файлы системы. Во-первых, это улучшит общую работоспособность компьютера, а во-вторых, автоматически избавит вас от инфекций, которые гнездятся именно во временных файлах (а таких немало). Для этого лучше воспользоваться специальной программой (свободна в использовании и бесплатна), например CCleaner http://www.filehippo.com/download_ccleaner/ или просто удалить все содержимое временных папок (**TMP**, **TEMP** в папке Windows и содержимое папки **Document and setting – Local Setting-Temp** (для этого нужно в свойствах папки убрать галочку скрывающую системные папки и файлы)). Удобнее работать с защищенными и скрытыми файлами используя альтернативный файл-менеджер, где имеется подсветка системных и скрытых файлов. Наиболее популярны Far-manager

<http://www.farmanager.com/download.php>, начиная с версии 2.0 эта программа бесплатна для всех пользователей и Total Commander <http://www.ghisler.com/> которая является условно-бесплатной, интересен бесплатный вариант FileComander <http://www.godlikesoft.de>. Стандартный проводник менее удобен в этой работе. Хотя его тоже можно настроить. Для этого необходимо изменить стандартные настройки проводника. **Пуск- Панель управления- Сервис- Свойства папки** и снять галочки с настроек, которые позволяют скрывать скрытые и системные файлы и добавить галочки, разрешающие эти действия.

Что еще необходимо учесть, если на компьютере обнаружались вирусы:

Для того, чтобы процесс лечения был успешным и достаточно быстрым, компьютер нужно предварительно подготовить:

- Выключите любые приложения, защищающие реестр от изменений (например, модуль программы Ad-Aware - Ad-Watch), иначе они не дадут вам ничего сделать.
- Если у вас Windows XP, то на время лечения **желательно** отключить функцию Восстановление Системы (System Restore). Кликаем на "Панель управления" заходим



в "Свойства системы". Находим закладку "Восстановление Системы" ("System Restore") и ставим галочку напротив "Отключить восстановление системы на всех дисках" ("Turn off System Restore on all drives"). Нажать "Применить" ("Apply"). Появится сообщение, предупреждающее об удалении всех точек восстановления - нажимаем "ОК".

- Сделайте все необходимые обновления антивируса и антишпионского ПО, а также заранее скачайте любые программы, которые вам могут пригодиться в процессе лечения. Можно записать их на компьютер, предварительно переименовав, так как есть ряд вирусов способных заблокировать работу антивирусов с типовым именем антивирусной программы. Лучше всего записать их на диск или защищенную флешку.

- Отключиться от сети Интернет. Отключиться от локальной сети. Лучше выдернуть из компьютера кабель локальной сети

Использование Диска Live CD « BART» или аналогичного по применению

Если вы очистили компьютер от вирусов, но через день-другой ваша антивирусная программа может снова выдать сообщение о наличии вирусов, то здесь вам обязательно понадобится загрузочный диск с операционной системой (Live CD). Очень хорошо подойдет диск Bart PE, Live Linux и др.... Кстати на современных компьютерах есть возможность загрузки с флешек и создав такую флешку можно загружать компьютер с этого устройства. Кстати, многие антивирусные компании, которые производят коммерческие продукты, выкладывают на своих сайтах образы таких дисков, которые специально организованы для поиска и решения проблем на зараженных компьютерах. Эти диски можно скачать и использовать совершенно бесплатно. Вот несколько ссылок:

- продукты компании AVAST <http://www.avast.com/other-products>
- продукты компании DrWEB антивирус <http://products.drweb.com/> в разделе бесплатные утилиты
- продукты компании AVIRA <http://free-av.com/en/products/index.html>
- и другие.

Если ваш ПК перестал загружаться с жёсткого диска, то для загрузки компьютера им также можно будет воспользоваться и поработать с компьютером или переписать сохранившиеся документы на диск или флешку.

Но для того, чтобы операционная система загрузилась с диска необходимо, чтобы в BIOS очередность загрузки начиналась с компакт диска.

Компьютер может загружаться с жесткого диска, с дискеты или с компакт-диска. Очередность загрузки указывается в BIOSe. Чтобы попасть в BIOS необходимо при перезагрузке нажать клавишу **Del** на клавиатуре (либо иную – зависит от конкретного компьютера, например в ноутбуках бывает зарезервирована клавиша F2).

Примерные действия таковы (просто в разных версиях меню BIOS может быть организовано по другому):

На голубом фоне перейти в меню Boot. Далее найти строчку Boot device order (в некоторых BIOS - "Boot device priority"). В этом списке указаны устройства, с которых компьютер может загрузиться: Hard Disk Drive – жесткий диск; Floppy Drive - дискета; CD/DVD-ROM Drive – CD/DVD привод; Ethernet - сеть. Для того, чтобы загрузка пошла с диска - первым в этом списке поставьте CD/DVD-ROM Drive. Потом перейти в меню Exit, и выбрать Exit Saving Changes. (Y/N) нажать Y на клавиатуре.

Внимание! После того, как вы выполните очистку компьютера от вирусов с использованием диска **Bart PE** обязательно верните в BIOSе прежние параметры загрузки (с жесткого диска) Это позволит предотвратить заражение компьютера в момент включения от случайных дисков, дискет и флешек, если вы их случайно оставили в выключенном компьютере.

После этого операционная система загрузится с диска. После загрузки можно открыть рабочий диск. Лучше это сделать с помощью встроенного файлового менеджера, например Total Commander в котором на экране (настроено по умолчанию) отображаются скрытые и системные файлы. Открыть папки RECYCLER и System Volume Information и очистить их содержимое (потому что в основном вирусы, из этих папок при стандартной процедуре удаления вирусов отсюда не удаляются и вновь возвращаются на только что «пролеченный» компьютер). Если винчестер разбит на несколько дисков – необходимо повторить эту операцию на всех дисках. По окончании этой процедуры запустить любую утилиту, которая позволит проанализировать компьютер на наличие вирусов. Это можно сделать с помощью **CureIt** <http://www.freedrweb.ru>, либо утилиты лаборатории Касперского **AVZ** <http://www.kaspersky.ru>, либо любой другой, которая интегрирована в содержимое Live-CD. Если таких программ в найденном вами загрузочном диске нет, то можно использовать флешку, на которую вы можете записать эти или подобные программы. Практически все загрузочные диски позволяют подмонтировать подключаемую флешку к компьютеру.

Пример инструкции на АРМ ОУ по вопросам безопасности.

На каждом рабочем месте в образовательном учреждении должна находиться на видном месте инструкция, с помощью которой пользователь всегда будет оповещен о правилах безопасной работы с информацией и средствами вычислительной техники и Интернет.

ИНСТРУКЦИЯ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1. Регулярно, не менее 1 раз в неделю производить обновления операционной системы Windows <http://update.microsoft.com> если это не производится автоматически. Сообщение о наличии обновлений обычно появляется в виде значка на панели задач.
2. Встроенный брандмауэр Windows должен быть активирован.
3. Ежедневно проверять состояние антивирусного программного обеспечения, а именно:
 - режим автоматической защиты должен быть включен постоянно;

- дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты;
 - просматривать журналы ежедневных антивирусных проверок;
 - контролировать удаление вирусов при их появлении.
4. При работе с электронной почтой категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц файлы.
 5. Контролировать посещение Интернет сайтов пользователями (Значок системы СКФ на панели задач должен быть зеленого цвета).
 6. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними (автозагрузка со сменных носителей информации на компьютере должна быть отключена).
 7. Не запускать файлы, попавшие на ваш компьютер независимо из какого источника (Интернет; P2P сети; почта...), предварительно не проверив их антивирусом (это же касается и архивов).
 8. Регулярно проводить сохранение рабочих документов на внешние носители (не реже 1 раз в неделю). Либо настроить автоматическое сохранение важных папок на компьютере с помощью специальной программы (указываем имя программы)
 9. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от локальной сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры пригласить специалиста в области компьютерной безопасности для дальнейших действий.

Контроль над использованием не санкционированных к использованию программ в рамках ОУ.

В компьютерном классе, да и не только (компьютеры в компьютерном классе наиболее часто имеют программы установленные школьниками без ведома и разрешения учителя) необходимо регулярно проверять компьютеры на наличие нелегального программного обеспечения (ПО) и ПО сомнительного происхождения. Нелегальное ПО необходимо немедленно деинсталлировать с компьютера, ПО сомнительного происхождения - проверить лицензионное соглашение (ПО может быть бесплатным или условно-бесплатным) и для каких целей оно используется в образовательном учреждении. Для того, чтобы быстро проверить какие программы установлены на вашем компьютере можно

воспользоваться утилитой Aida 32, которая также бесплатна для некоммерческого использования <http://www.aida32.hu/> . AIDA32 - профессиональный инструмент для диагностики оборудования и анализа системной конфигурации. Отчеты AIDA32 содержат данные об оборудовании: информация о CPU, материнской плате, памяти (в том числе количество и тип модулей), HDD (IDE и SCSI), CD-ROM, звуковой карте и других устройствах в том числе и о программном обеспечении установленном на конкретный компьютер. AIDA32 получает данные об оборудовании на низком уровне (а не только по системному реестру Windows, как большинство Win32-информеров), используя собственную базу данных (около 21 000 устройств). AIDA32 позволяет собирать информацию с удаленных компьютеров по сети TCP/IP. AIDA32 во всех вариантах (в том числе Enterprise Edition и Network Edition) распространяется бесплатно для частных и корпоративных пользователей.

Использование этой программы не требует особенных знаний и у вас всегда будет под рукой информация об оборудовании (причем вскрывать для проверки компьютер не требуется), установленном в школе и программных продуктах имеющихся на школьных компьютерах. Помимо этого данные собранные со школьных компьютеров можно экспортировать в формате базы данных, что позволит использовать эти данные в организации учета и сроков обслуживания компьютерной техники. Да и для учета комплектации рабочих мест в учете материальных ценностей. Для этого можно воспользоваться программой «База ПК», которая также <http://hajam2.narod.ru> распространяется бесплатно и использование этой программы позволит упорядочить обслуживание компьютерной техники в школе. Импортировав отчет AIDA32 в программу, вы внесете компьютер в базу данных инвентаризации, не заполняя руками ни одной формы.

Виртуальные машины

Наиболее динамично в последние годы развиваются компьютерные сети, Интернет, мультимедиа технологии и программное обеспечение. Однако очень часто в учебных заведениях в целях безопасности школьникам предоставляется доступ к компьютеру из под учетной записи с ограниченными правами и возможностями. Это резко ограничивает практическую ценность работы в условиях развитой ЕИОС. Это связано с вопросами обеспечения информационной безопасности в среде ОС Windows. Но сегодня наряду с Windows существует альтернативная полноценная операционная система Linux (набор СПО получили все ОУ РФ), отвечающая всем современным требованиям. Linux представляет собой быстро развивающееся ПО, распространяемое на условиях лицензии GNU GPL, т.е. она бесплатна и общедоступна. Эта система также как и Windows имеет графический интерфейс. Linux можно интегрировать в любую локальную сеть, поддерживаются все

сетевые протоколы и службы, работа в TCP/IP-сетях. Использование этой операционной системы в учебных заведениях могло бы существенно снизить затраты на приобретение программного обеспечения. Однако, на сегодняшний день среди преподавателей и школьников очень мало тех, кто знаком с этой операционной системой и имеет какие-то навыки работы в ней. Значительную помощь при изучении операционных систем и компьютерных сетей могут оказать так называемые виртуальные машины. Под виртуальной машиной понимается программная среда, позволяющая запускать на компьютере одновременно несколько разных операционных систем и переключаться из одной ОС в другую без перезапуска компьютера. Виртуальная машина в точности эмулирует работу полноценного компьютера. На виртуальную машину можно установить фактически любую современную операционную систему при этом, не нарушая работоспособности основной операционной системы. В большинстве компьютерных классов в настоящее время установлена операционная система Windows XP. Для комфортной работы с виртуальной машиной потребуется 512 Мбайт оперативной памяти и больше.

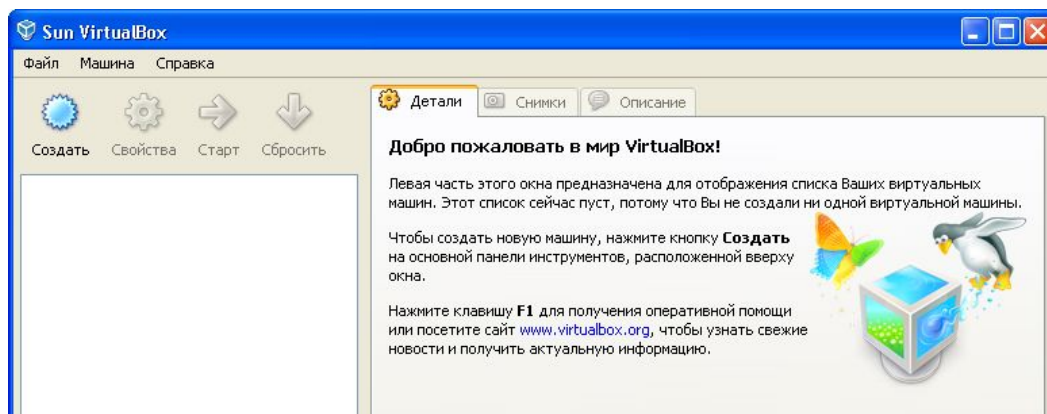
Наиболее удобны и что не маловажно бесплатны две виртуальные машины. Одна от компании SUN <http://www.virtualbox.org/> **Sun Virtualbox** и другая от компании Microsoft. <http://www.microsoft.com/windows/downloads/default.aspx> **Virtual PC 2007**. Виртуальная машина Virtual PC 2007 ориентирована в основном на свои продукты от компании Microsoft и не очень хорошо поддерживают другие программные продукты. «Виртуалка» от компании SUN весьма эффективна и поддерживает продукцию всех разработчиков ОС. В ней больше возможностей для работы. К сожалению, когда пользователь работает на компьютере со значительно урезанными правами, предпочтительнее использовать Virtual PC 2007. В школе можно использовать их для работы в сети Интернет, с распределенными сетевыми ресурсами, файл-серверами, прокси- серверами и др. Учителям информатики понравится возможность использования виртуальных машин для проведения уроков по настройке, установке ОС, инсталляции и деинсталляции программ, освоения ОС Linux и др, потому что основная операционная система в компьютерном классе никак не пострадает от неумелых действий школьников. Практически на виртуальных машинах можно проводить любые курсы с использованием средств вычислительной техники. Это позволит использовать любые программы не прибегая к помощи системного администратора для получения разрешений и установки различных программ.

Установка и настройка виртуальной машины SUN Virtualbox.

1. Устанавливаем на свой компьютер виртуальную машину, используя дистрибутив Sun VirtualBox <http://www.virtualbox.org/>. Все настройки используем по умолчанию(этого

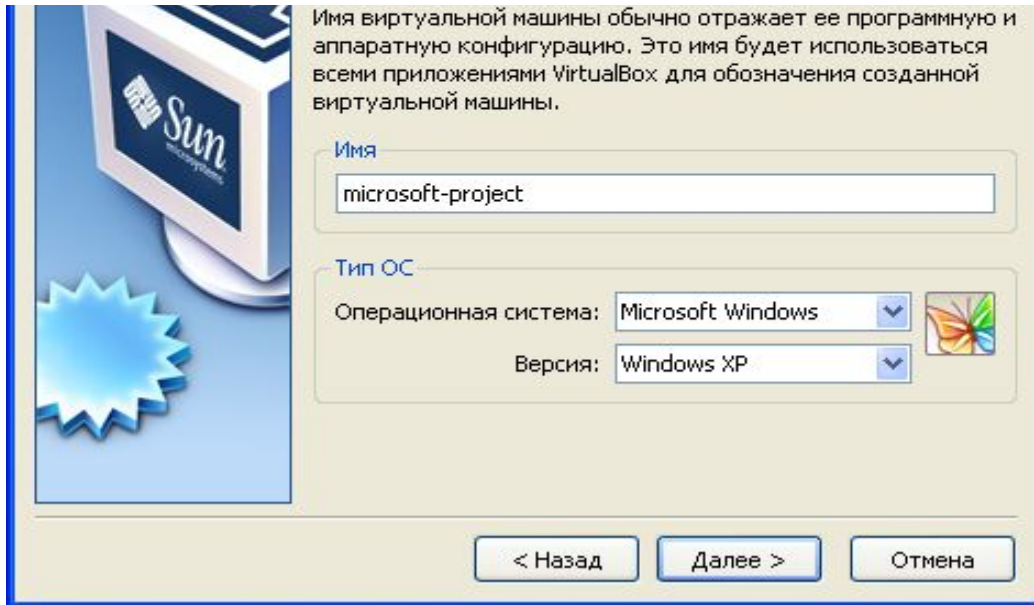
вполне достаточно для того чтобы полноценно установить на виртуальную машину любую операционную систему). В процессе установки, как правило, не возникает вопросов и проблем, просто щелкаем установить и ждем. После установки система предложит зарегистрировать установленную виртуальную машину. Вы можете немедленно это сделать, при этом вы получите бесплатный аккаунт от компании SUN и на ваш почтовый ящик будут приходить информационные письма о новостях виртуальной машины (обновления, новые версии). И вполне вероятно виртуальная машина предложит обновиться, если на сайте компании есть новая версия виртуальной машины.

2. После установки виртуальная машина предложит создать новую машину.



3. С помощью мастера создания виртуальных машин «по шагам» создаем новую машину.

4. Дадим название своей виртуальной машине, например Microsoft-project. Выбираем тип «операционной системы» и «Версию»



5. Выбираем основной раздел, который будет использоваться как оперативная память. Если на вашей физической машине объем памяти достаточно большой, то рекомендуется сделать размер памяти не менее 512 мб. Это позволит более комфортно работать с ней. Здесь как и на реальной машине от размера свободной памяти резко зависит быстродействие компьютера с виртуальной операционной системой.

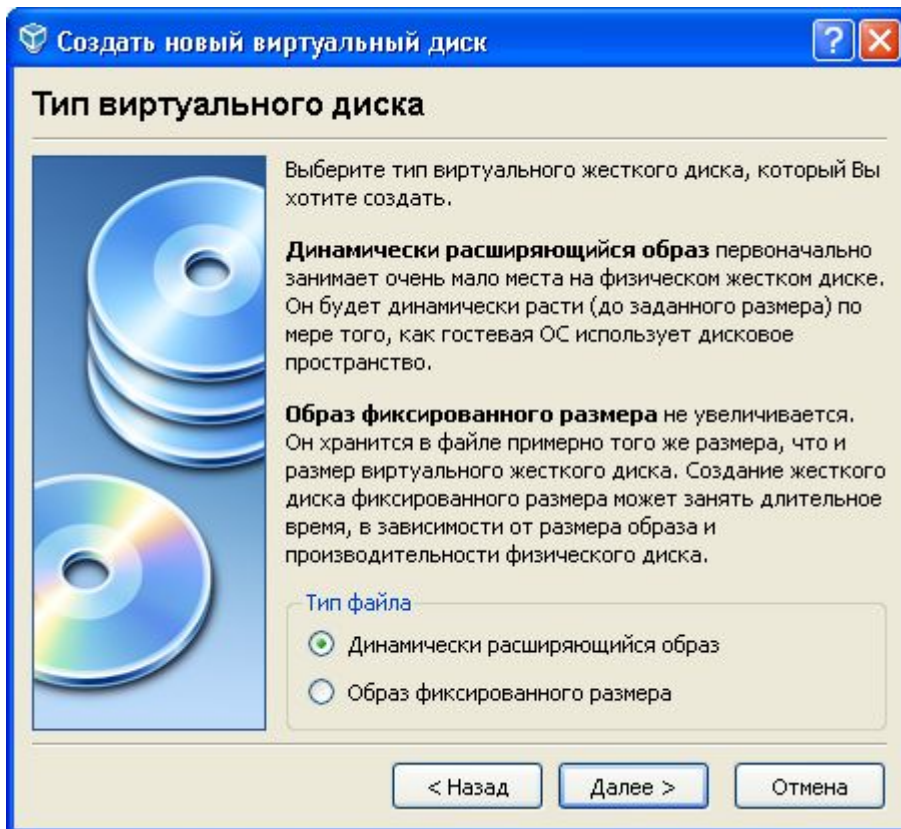


6. Шагаем дальше, для того чтобы на следующем этапе создать виртуальный загрузочный диск.



7.

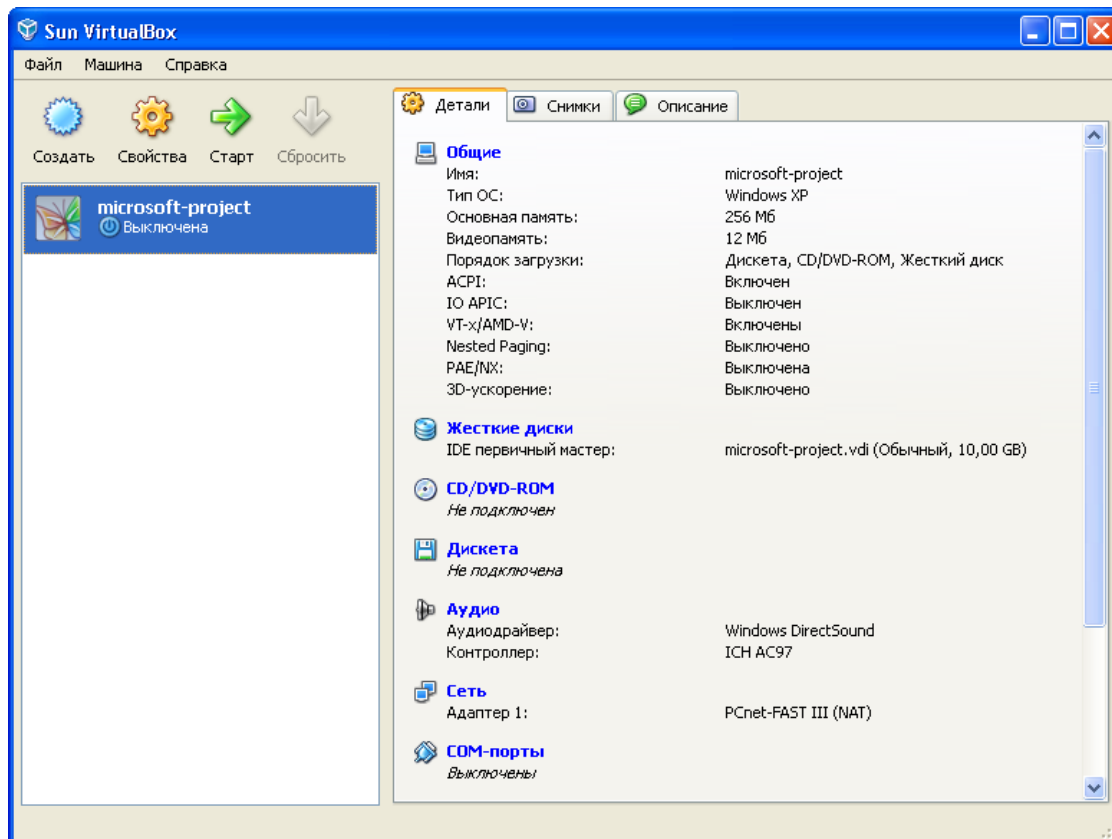
8. Выбираем тип диска (динамически расширяющийся образ)



9. Выбираем местоположение и размер диска (Они либо используются по умолчанию, либо вы выбираете диск, на котором у вас есть немного свободного места для расположения созданных виртуальных машин.

10. В последнем окне мастера подтверждаем сделанный выбор, щёлкнув по кнопке Готово.

11. Еще одно Готово и виртуальная машина для установки на неё операционной системы Microsoft Windows XP создана.

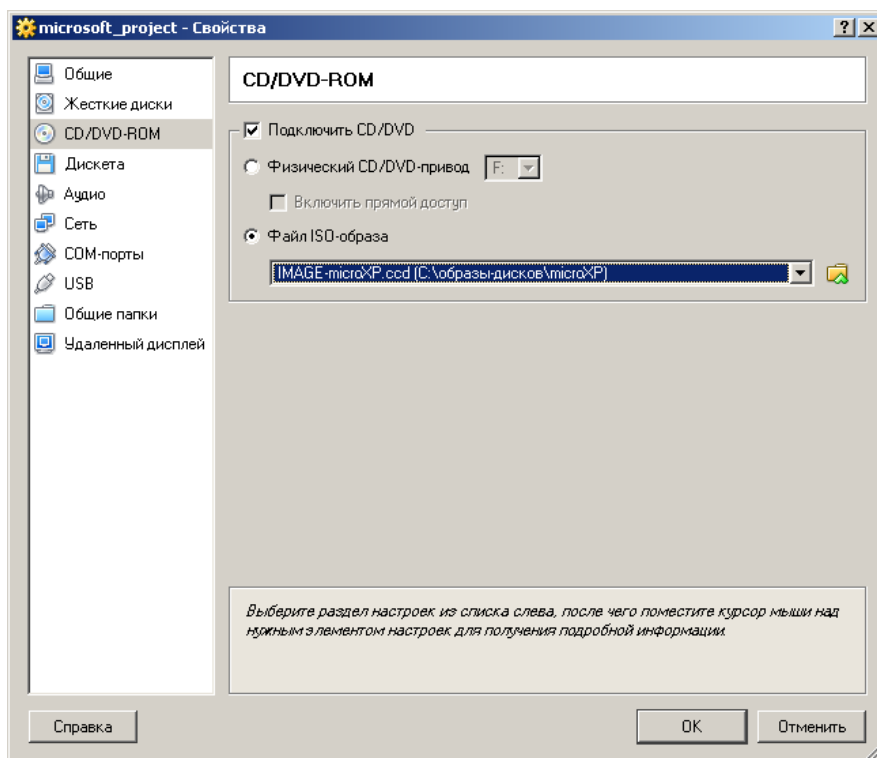


Эта, созданная нами виртуальная машина, позволит с успехом отрабатывать навыки установки на компьютер операционной системы, установки любых других программ и отработки навыков настройки и отладки операционной системы.

Настройка виртуальной машины

Производим настройку виртуальной машины с помощью меню **свойства**





Подключаем к машине образ установочного диска (который подготовлен заранее в формате ISO) с которого и будем устанавливать операционную систему (как на изображении) на виртуальную машину. Здесь наша задача состоит в том, что нужно просто указать путь, до того места на компьютере или в локальной сети, где хранится образ подключаемого установочного диска (дистрибутива).

А где взять образы дисков?

Есть несколько вариантов:

1. Изготовить самостоятельно, использовав собственный загрузочный диск и программу (также бесплатную) *MagicDisk* <http://www.magiciso.com/download.htm>

2. **Скачать готовый образ на сайтах:**

<http://khodarev.narod.ru/OS.html> много различных образов

<http://ubuntu.ru/get> Linux Ubuntu-ru

<http://www.altlinux.ru/go/download/> Alt Linux

и другие, которых можно найти множество в сети Интернет.

Подключаем звук (аудиодрайвер)

Если нужна сеть. - Устанавливаем сетевые подключения

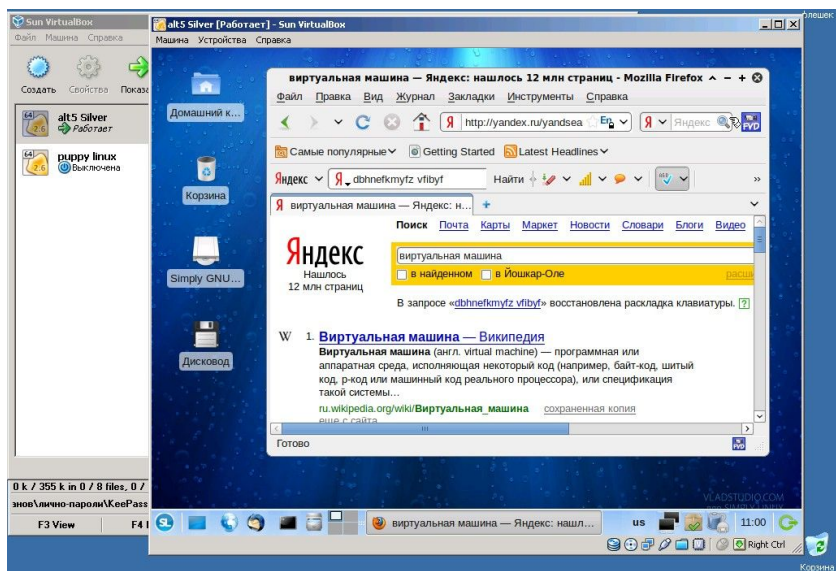
Причем эти устройства после установки операционной системы можно откорректировать, причем, если вы сделали ошибки послу установки, то многие проблемы решатся автоматически в момент установки операционной системы на виртуальную машину.

Установка Операционной системы Windows XP на виртуальную машину.

Нажимаем на кнопку **СТАРТ**

Начинается установка операционной системы на виртуальный диск компьютера. При этом на экране в стандартной последовательности будут появляться текущие вопросы к пользователю.

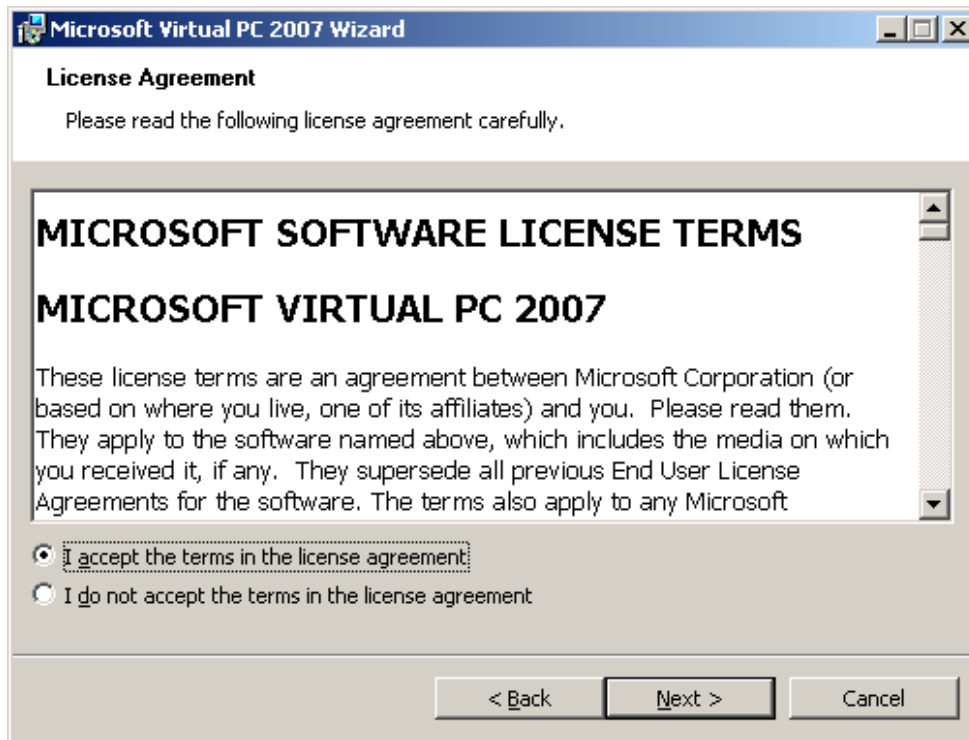
В процессе установки вам придется отвечать на стандартные вопросы, например: дата, государство, язык и др. Обычно у пользователей это не вызывает никаких вопросов. По окончании установки на экране появляется приглашение операционной системы. Интернет настраивается автоматически, если основной компьютер имеет подключение к сети Интернет. С программами и ресурсами Интернет можно начать работать сразу же после установки ОС. Вся процедура установки ОС на этом закончена. Если требуется установить любые дополнительные программы, устанавливаются они также как и на физическую машину с помощью дистрибутивных файлов, имеющих на флешке или компакт диске(ах).



На этой копии экрана видна установленная и запущенная на компьютере виртуальная машина с ALT-Linux. На ОС запущен браузер с поисковой машиной Yandex.

Установка виртуальной машины Virtual PC 2007

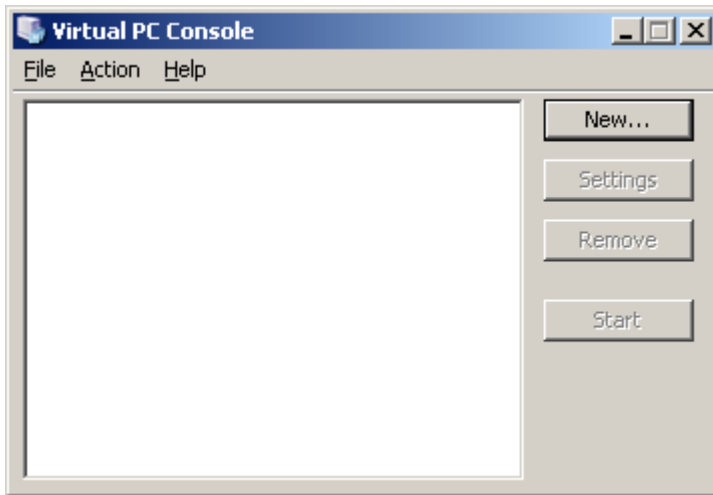
Установка Virtual PC 2007 <http://www.microsoft.com/windows/downloads/default.aspx> Эта программа будет общаться с вами только на английском языке.



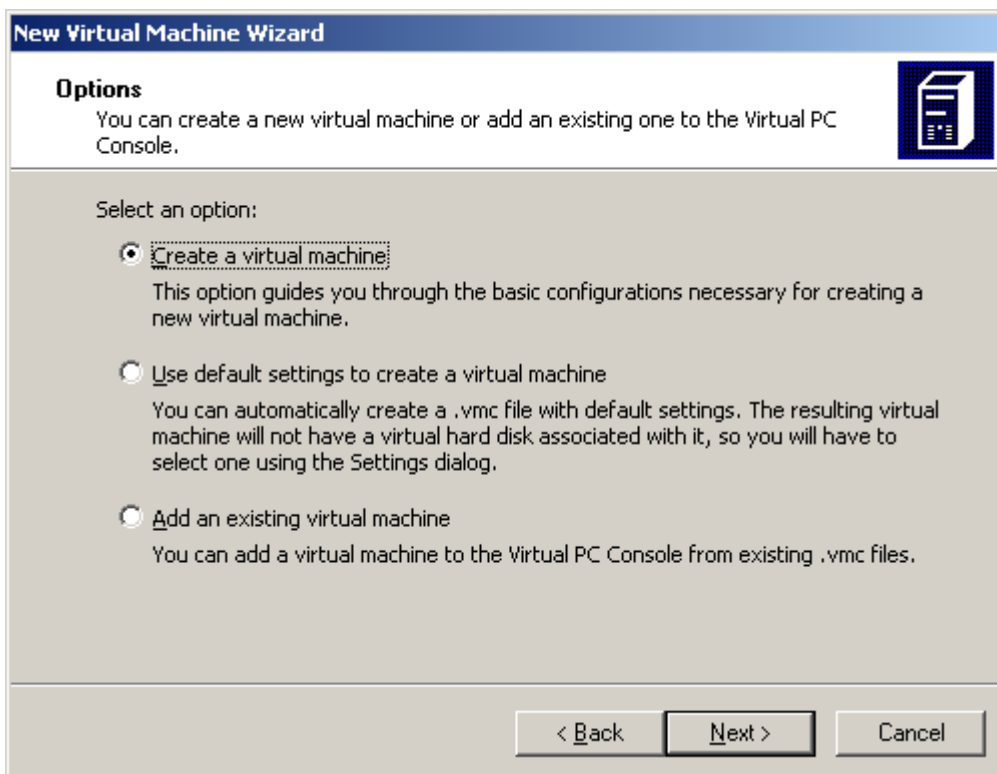
2. Несмотря на то, что программа распространяется бесплатно - у нее все равно есть свой ключ. Он формируется автоматически. Наша задача ввести имя пользователя и наименование организации. Далее переходим по умолчанию через несколько окон. И вот он **Finish**. Машина установлена на компьютер. Настроек «по умолчанию» достаточно для полноценной работы с виртуальными машинами.

Запуск и настройка виртуальной машины

1. Запускаем виртуальную машину

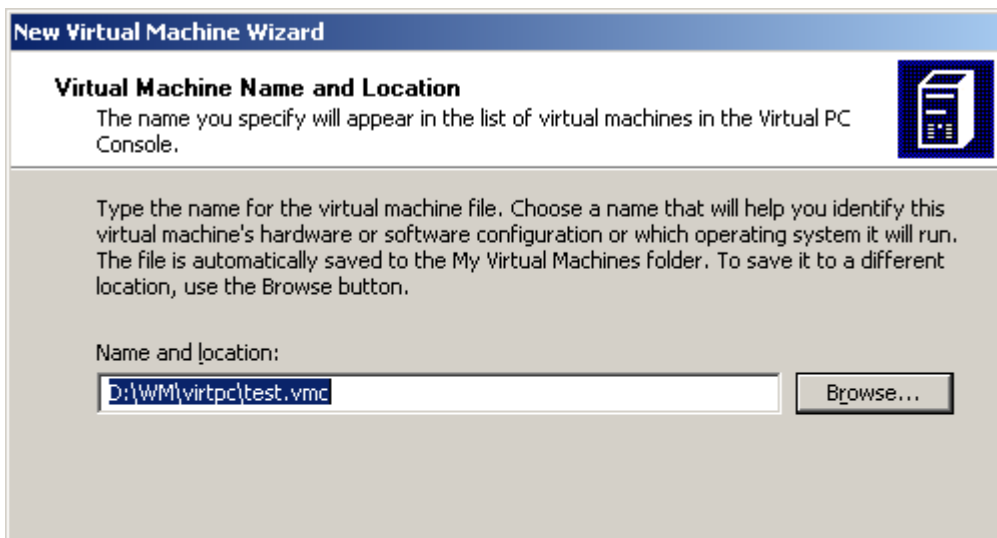


2. После первого запуска запускается мастер создания новых виртуальных машин:



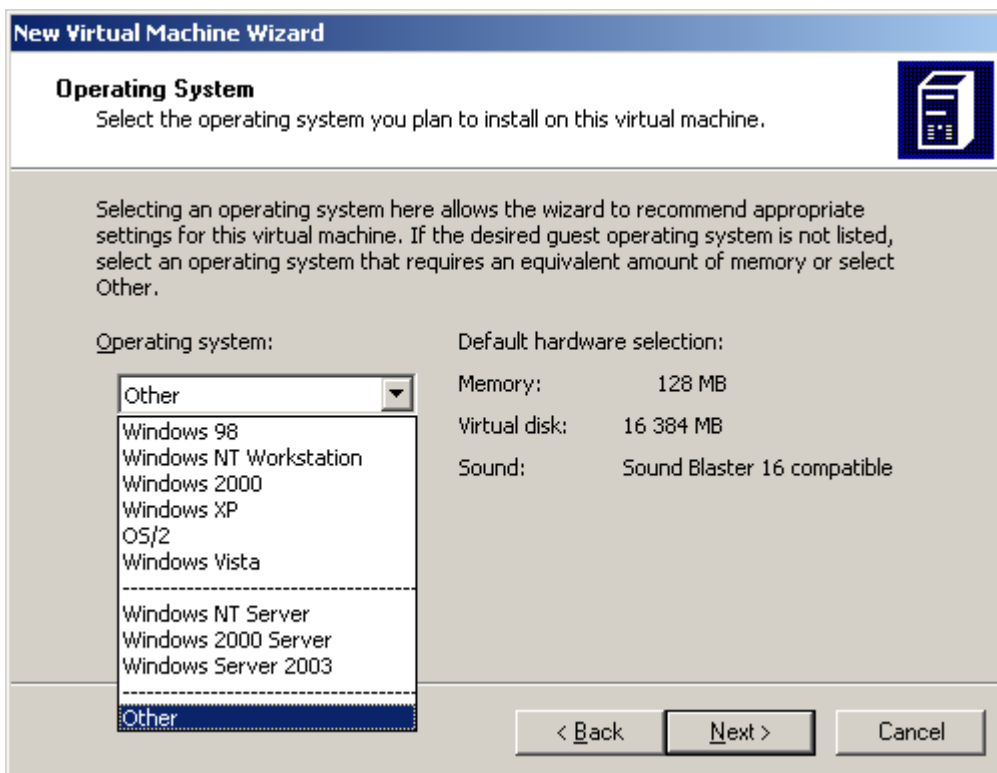
3. Первый вопрос - чего же мы хотим: создать виртуальную машину; создать виртуальную машину, используя предустановленные настройки; просто добавить уже существующую виртуальную машину.

4. Выбираем пункт Create a virtual machine. Создаем новую машину:

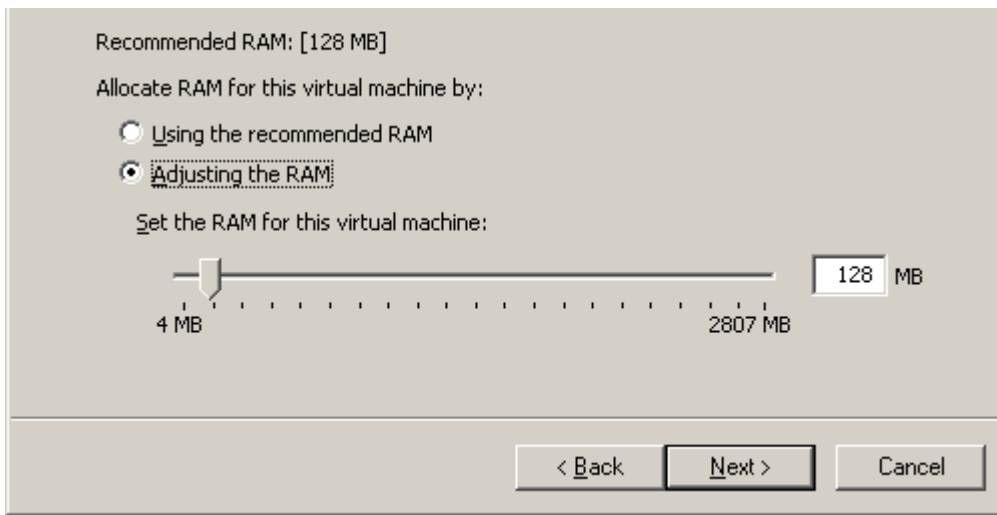


5. Мы выбираем названия машины и расположение ее файла настройки. По-умолчанию, файл образа новой машины будет создан в специализированном каталоге "My Virtual Machines" в папке "Мои документы". В данном случае наша виртуальная машина называется test.

6. Следующим шагом будет выбор операционной системы, которую предполагается установить на компьютер:

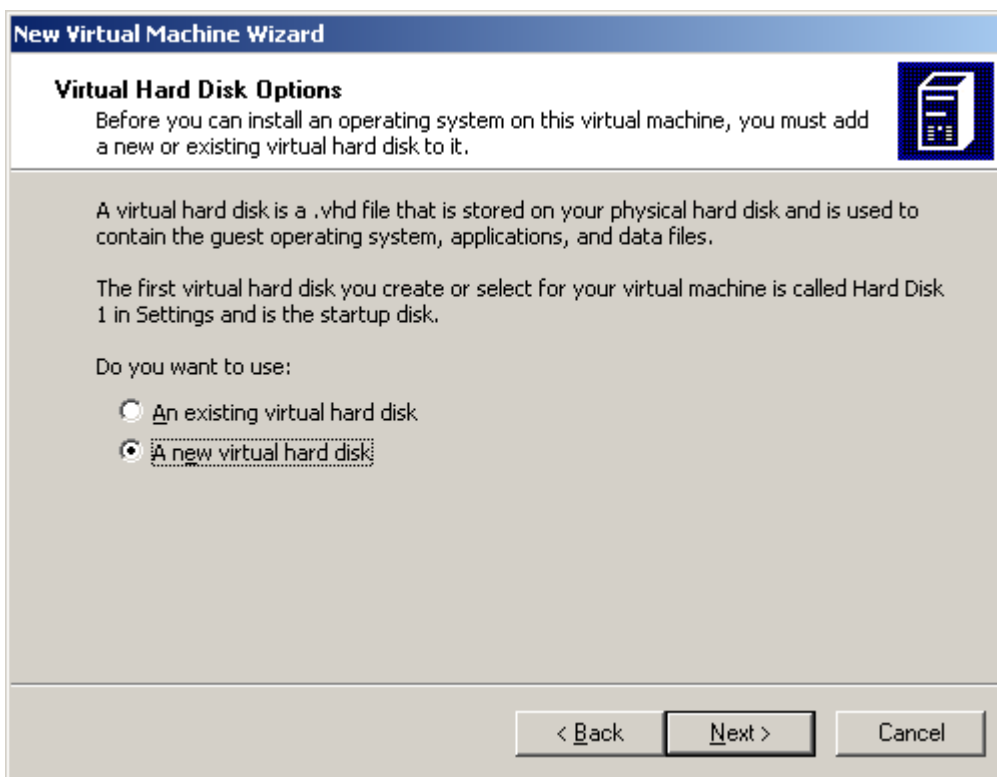


7. В зависимости от выбора будет меняться количество выделяемой оперативной памяти, размер диска и способ эмулирования звуковой карты. Эти настройки можно будет поменять:

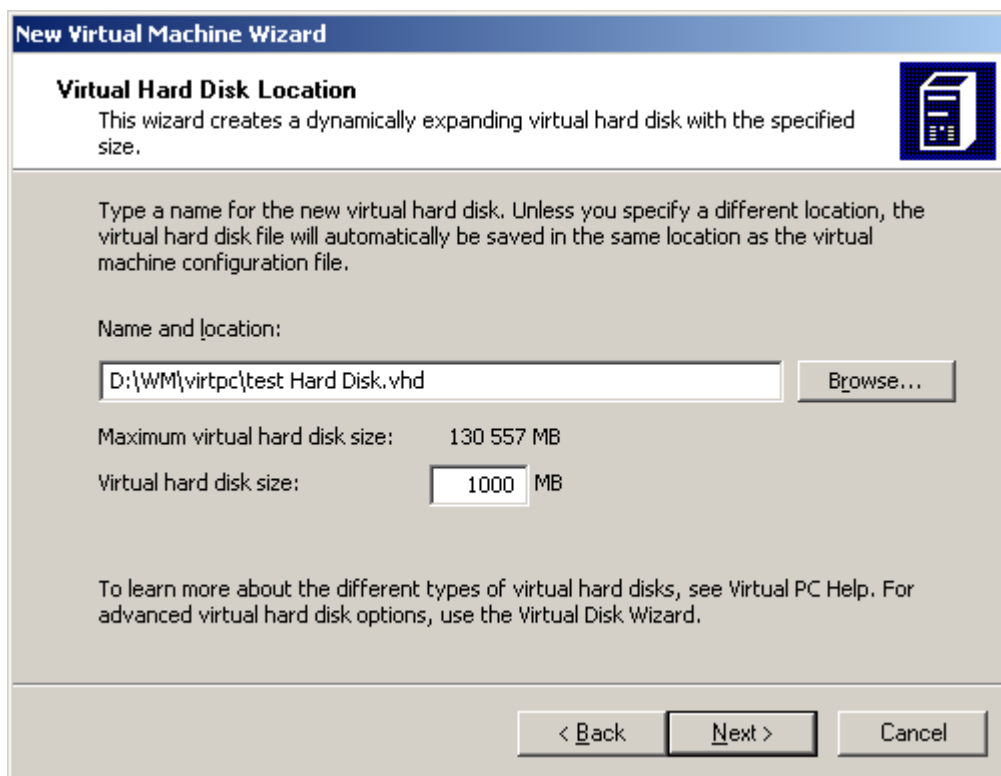


Например, размер оперативной памяти легко увеличить с помощью ползунка.

8. Следующий шаг - создание или добавление жесткого диска:



9. Если выбираем "Создать новый" (A new virtual hard disk), то следующим шагом будет его конфигурация:

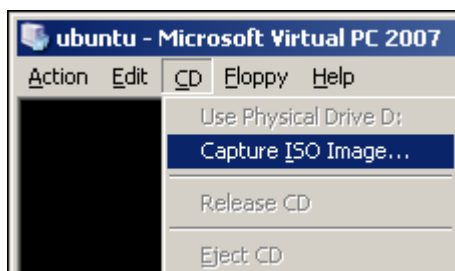


10. Выбираем место размещения и размер. Машина создает диск с динамически изменяемым размером.

11. Нажимаем **Finish**. Машина сконфигурирована (настроена) под будущую установку ОС.

Установка Операционной системы на виртуальную машину

Запускаем машину и с помощью меню CD подключаем образ диска(о том где его брать рассказано чуть выше по тексту), с которого и будет устанавливаться операционная система.



После монтирования диска перезагружаем «виртуалку» и устанавливаем ОС, как на обычный компьютер или любую другую виртуальную машину. На экране появится приглашение системы, и мы можем приступить к работе. Из недостатков следует отметить то, что интерфейс программы не поддерживает русский язык и в основном она предназначена для работы с образами продуктов компании Microsoft. Рекомендуется скачать с сайта компании максимально свежую версию.

Свободное программное обеспечение, ориентированное для использования в образовательной среде и свободно распространяемые полезные программы для работы с информацией.

Здесь я попробую рассказать поподробнее об особенностях установки, настройки, использования различных программ, о которых говорилось в предыдущих разделах этой книги. С помощью пошаговых инструкций и детализации действий с программами вы сможете произвести настройку и установку программного обеспечения на свой компьютер и обеспечите его надежную защищенность. Все эти программы активно используются, проверены в работе и не требуют дополнительных специальных знаний для их обслуживания. В первую очередь – это бесплатный софт (Open Source). А в целом вся ваша успешность в организации безопасного информационного пространства, как на работе, так и дома, напрямую зависит от вашей аккуратности, как пользователя, от выполнения всех необходимых нормативов и правил безопасности, В этом случае ваша жизнь вместо постоянной борьбы с вирусами, рисками потери рабочей и личной информации, проблемы с собственными нервами и драгоценным потерянным временем превратится в безопасную и комфортабельную работу с информацией и информационными ресурсами.

Видеоролики, демонстрирующие установку, настройку различных программ для обеспечения информационной безопасности.

В сети Интернет на видеосервисах YouTube мною размещены видеоролики на которых снят процесс инсталляции, обновления и использования различных программ, о которых говорится в этой книге, предназначенных для обеспечения информационной безопасности. При наличии подключения к сети Интернет на экране монитора вы подробно познакомитесь с видеороликами, снабженными подробными комментариями.

Ссылки на ролики:

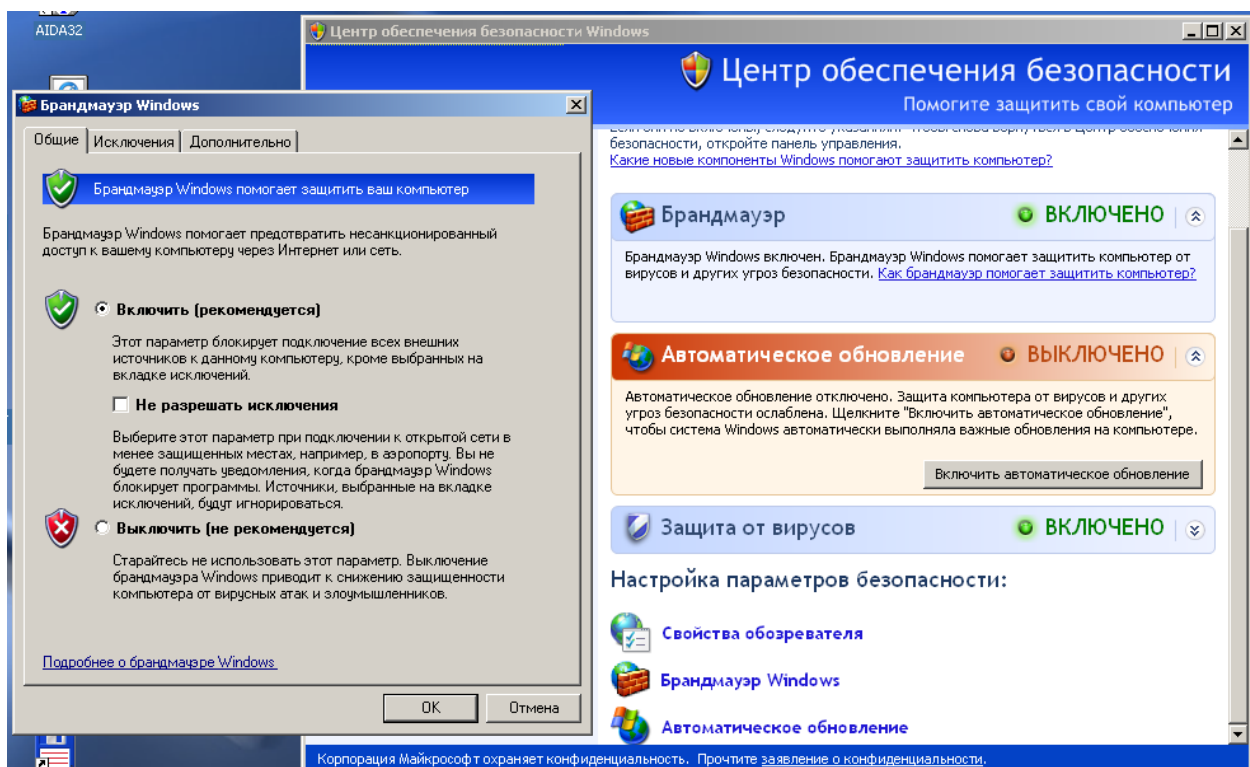
- Обновление браузера Internet Explorer <http://www.youtube.com/watch?v=IX6o3nsmzaU>
- Установка альтернативного браузера на Windows XP, настройка безопасности и дополнений. http://www.youtube.com/watch?v=C_aF8EB7fbA
- Установка операционной системы Windows XP на виртуальную машину. Особенности и правила установки. <http://www.youtube.com/watch?v=Mptz5knKFNA>
- Как установить виртуальную машину на компьютер. Настройка и особенности. Виртуалка от компании Microsoft PC2007. <http://www.youtube.com/watch?v=qYBnjAHRcmo>

- Работаем с флешками. Ограничение функций автозапуск и автозагрузка. Защита флешек. <http://www.youtube.com/watch?v=U12iLfwVDhU>
- Установка и настройка детского браузера Гогуль. Примеры использования. <http://www.youtube.com/watch?v=40sZIPADeGE>
- Установка, настройка антишпионской программы Spyboot Search&Destroy на компьютер с операционной системой Windows. <http://www.youtube.com/watch?v=t5dq0uNlqKE>
- Установка антивируса на компьютер с операционной системой Windows XP. http://www.youtube.com/watch?v=ifit6PpQ_uI Запущена виртуальная машина.
- Установка дополнений для браузера Mozilla Firefox. Запущена Sun виртуальная машина и операционная система Alt Linux. <http://www.youtube.com/watch?v=mK1iDdGxhjY>

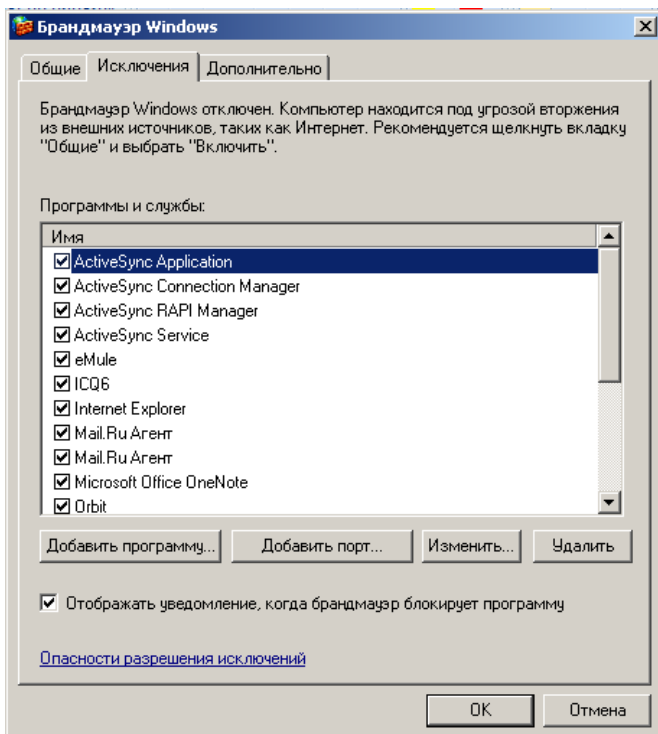
Настраиваем интегрированный брандмауэр компании Microsoft

Выбираем ПУСК - ПАНЕЛЬ УПРАВЛЕНИЯ - ЦЕНТРОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Убеждаемся, что Брандмауэр включен, если он выключен, включаем его.

Переходим к настройке параметров безопасности. Щелкаем по надписи Брандмауэр Windows – открывается окно, в котором мы будем настраивать параметры брандмауэра.

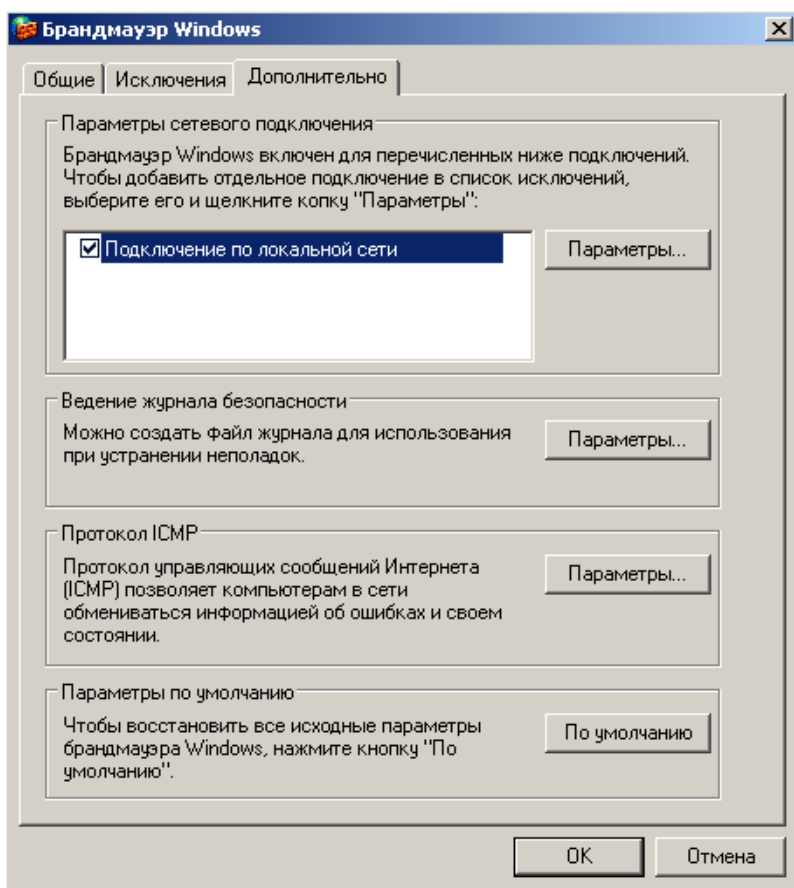


Вкладка ИСКЛЮЧЕНИЕ



Добавляем программу, которой доверяем, например программа АИДА-32, с помощью которой можем собирать информацию о устройствах и программах компьютера. Соответственно добавляем в перечень программ, которым вы доверяете.

Вкладка ДОПОЛНИТЕЛЬНО

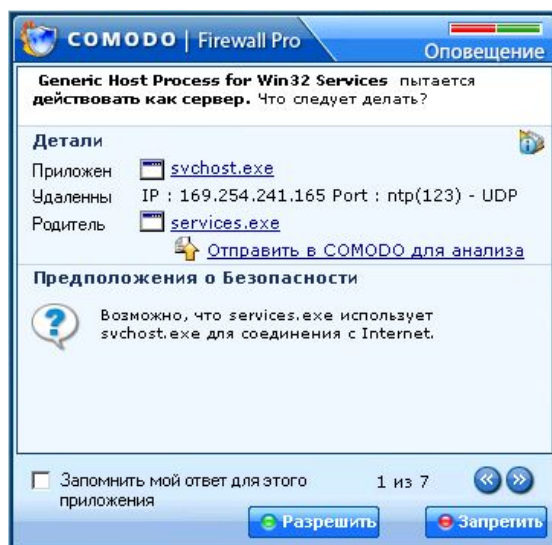


С помощью этой вкладки можно выбрать подключения к компьютеру для контроля их с помощью брандмауера. При выборе параметров по умолчанию, все стандартные настройки брандмауера будут восстановлены.

Использование антишпионской программы Comodo

1. Запустите установку программы Comodo;

2. В диалоговом окне COMODO Firewall Pro Installer на вопрос отвечаем *Да* → *Next>>* → *Yes* → *Next>>* → пишем свой адрес электронной почты (не обязательно) → *Далее* → *Далее* → *Finish* (т.е. устанавливаем всё по умолчанию). Компьютер перезагрузится.
3. На рабочем столе появится ярлык программы COMODO Firewall Pro.
А в нижнем правом углу после перезагрузки появится окно-оповещение,

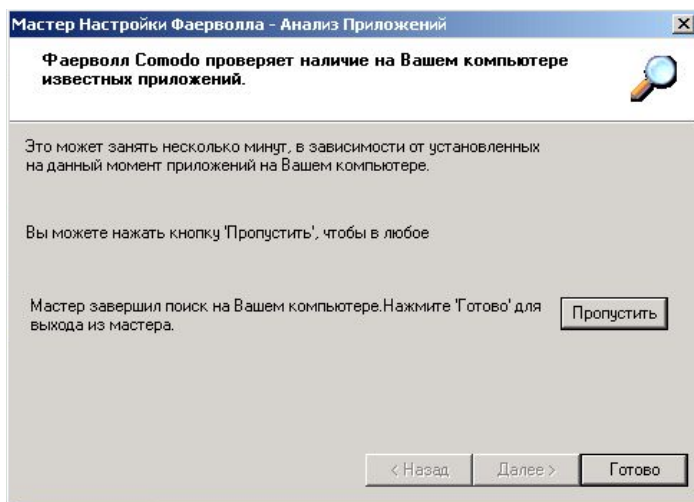


спрашивающее, что следует сделать: Разрешить или Запретить.

4. Внимательно читаем вопрос и если Вы уверены, что это не шпионская программа пытающаяся проникнуть на Ваш компьютер, тогда ставим галочку *Запомнить мой ответ для этого приложения* и щелкаем по нужной кнопке. Прodelываем это действие столько раз, в зависимости от количества активных программ установленных на Вашем компьютере.
ВНИМАНИЕ! Пользователь должен быть достаточно опытным для первоначальной настройки программы. Дальше в режиме самообучения вы последовательно организуете защиту вашего компьютера.
5. Изменяем способы оповещения Центром обеспечения безопасности, для этого отключаем Брандмауэр:
Пуск → *Панель управления* → *Центр обеспечения безопасности* → *Изменить способ оповещений* Центром обеспечения безопасности.
Убираем галочку Брандмауэр → *ОК*. Закрываем все окна.
6. Перезагружаем компьютер.
!!! Если к Вашему компьютеру подключен Интернет, то будет спрашиваться доступность обновления программы, отвечаем *Да*.
7. На панели задач в области уведомлений появится значок программы COMODO, щелкаем по нему правой кнопкой мыши → *Открыть...*



8. В диалоговом окне COMODO Firewall Pro переходим на вкладку *ЗАЩИТА* → *Поиск известных приложений*. Ждём, когда мастер прогонит поиск и щелкаем *Готово*.



9. Чтобы изменения вступили в силу, Вам будет предложено перезагрузить Фаерволл Comodo, но не сам компьютер. Щёлкаем *ОК*.
10. Закрываем программу и выходим из неё, для этого в области уведомлений правой кнопкой щёлкаем по значку программы → *Выход* → *Да*.
11. Для активации программы, вновь запускаем её.

Проверка съёмных носителей на вирусы

Если при включении флешки у Вас срабатывает автозагрузка и на экране появляется приглашение системы с предложением выбрать программу для просмотра содержимого

носимого устройства хранения информации, то на ваш компьютер срочно нужно установить программу Autorun Guard (о ней писалось выше). После установки нужно снять две галочки, которыми отмечены автозапуск и автозагрузка. Либо воспользоваться другим способом отключения этих функций. Эта операция позволит резко снизить опасность автоматического заражения вашего компьютера только от того, что вы вставили в него флешку.

Прежде чем начать работать со съёмным носителем НЕОБХОДИМО проверить его (просканировать) на вирусы. Здесь предложены 2 варианта антивирусных программ. С опытом у вас появится возможность просматривая визуально содержимое флешки в файл-менеджере (Far-manager, TotalComander и др. у которых включена возможность отображения скрытых и системных файлов, как правило вирусы используют эти возможности чтобы замаскироваться) удалять наиболее опасные вирусы вручную. Это позволит экономить время на проверку носителей. От вашей аккуратности и последовательности зависит напрямую и ваша информационная безопасность.

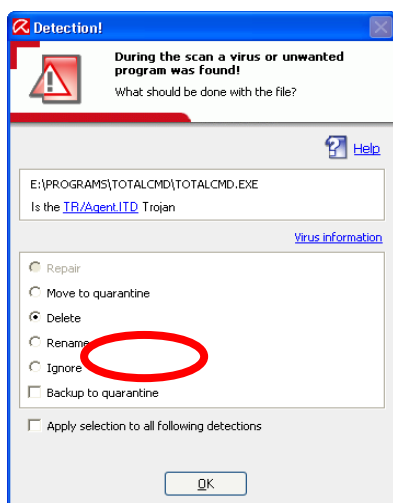
Проверка на вирусы в программе Avira AntiVir Personal

Открываем Мой компьютер;

Щёлкаем правой кнопкой мыши по съёмному носителю;

Из выпадающего меню выбираем команду Scan selected files with AntiVir.

Если обнаружен вирус, антивирусная программа выдаёт соответствующее сообщение:



Щёлкаем Delete---OK

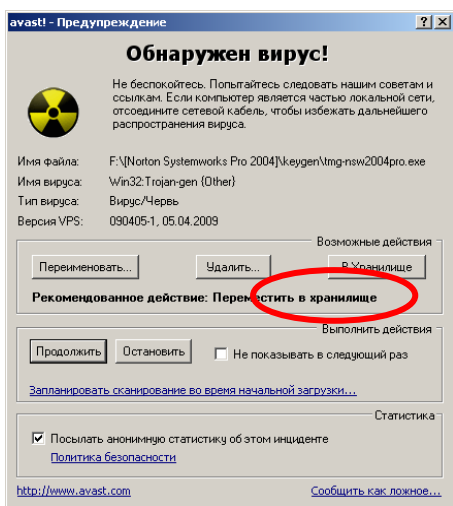
Проверка на вирусы в программе Avast

Открываем папку Мой компьютер;

Щёлкаем правой кнопкой мыши по съёмному носителю;

Из выпадающего меню выбираем команду Сканировать.

Если обнаружен вирус, антивирусная программа выдаёт соответствующее сообщение:



Щёлкаем Удалить.

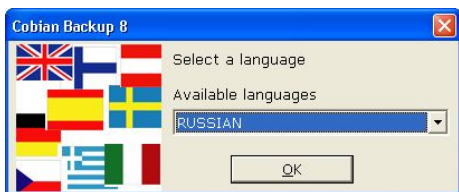
Если вирусы не обнаружены можете спокойно использовать флешку для работы.

Резервное копирование данных с помощью программы Cobian Backup.

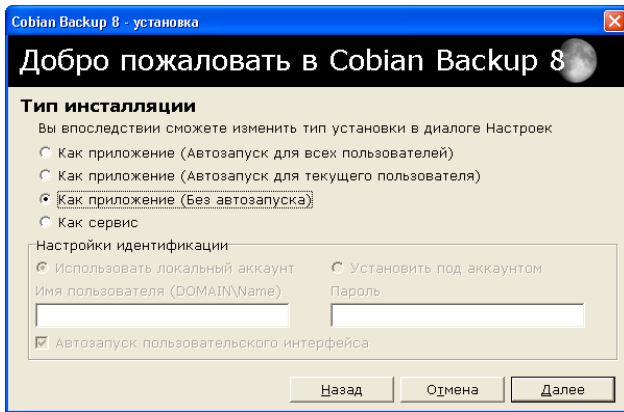
Эта бесплатная утилита предназначена для резервного копирования файлов и папок, которые часто изменяются. Программа может создавать копии заданных элементов в автоматическом режиме по заданному расписанию. Cobian Backup может сохранять копии объектов не только на вашем компьютере, но и в локальной сети, на FTP-сервере. При создании резервных копий используется интегрированный zip-архиватор.

Установка программы Cobian Backup

1. Запускаем инсталляционный файл
2. Выбираем из списка **Russian** (на этом языке будет с вами общаться программа)



3. Щёлкаем по кнопке **OK**
4. В окне *Cobian Backup 8 – установка* ставим галочку на *я принимаю условия*
5. Щёлкаем по кнопке **Далее**
6. Путь к директории (папке) оставляем по умолчанию и щёлкаем по кнопке **Далее**
7. Тип инсталляции выбираем **Как приложение (без автозапуска)**



8. Щёлкаем по кнопке **Далее**

9. Щёлкаем по кнопке **Готово**

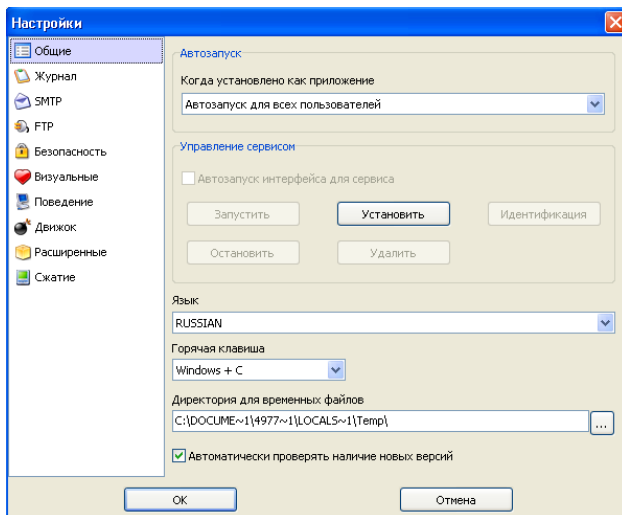
В области уведомлении появится значок 

10. Двойным щелчком запускаем программу из области уведомлении

11. Из меню **Инструменты** выбираем команду **Настройки**

12. В открывшемся окне *Настройки* в поле *Автозапуск* из выпадающего списка выбрать **Автозапуск для всех пользователей**

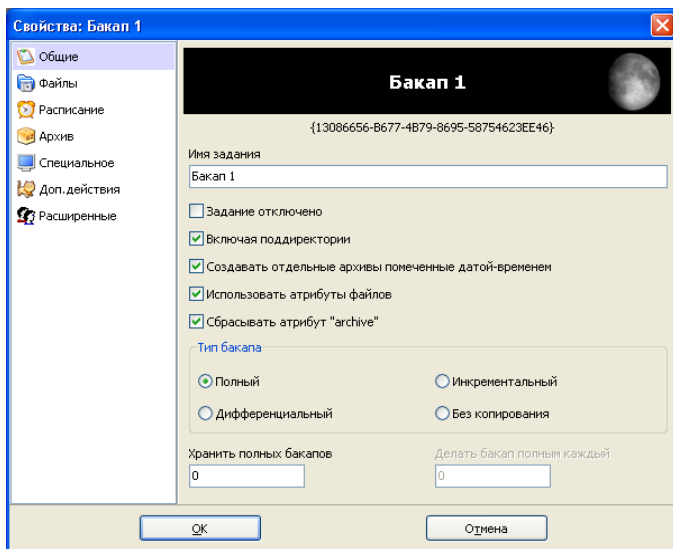
13. Щёлкните по кнопке **ОК**.



Настройка заданий Cobian Backup 8

1. Из меню **Задание** выбираем команду **Новое задание**

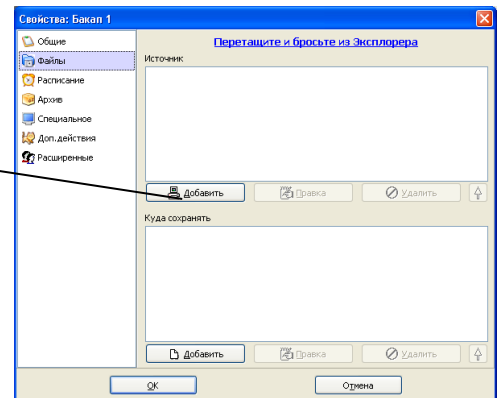
2. Откроется окно *свойства: Бэкап 1*



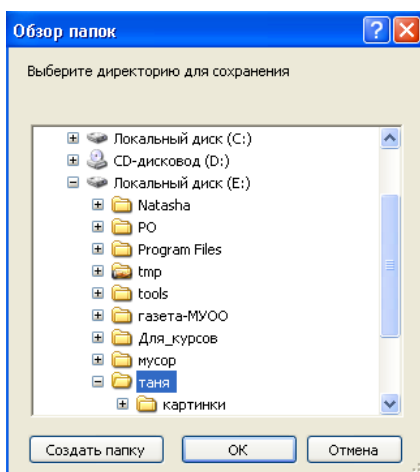
3. В меню расположенной с левой стороны выбираем **Файлы** и щёлкаем по кнопке **Добавить** в поле *Источник*

4. В выпадающем меню выберите **Директория**


Примечание: Можно создавать резервные копии не только своей личной папки, но и различных файлов и папок, FTP сайтов.



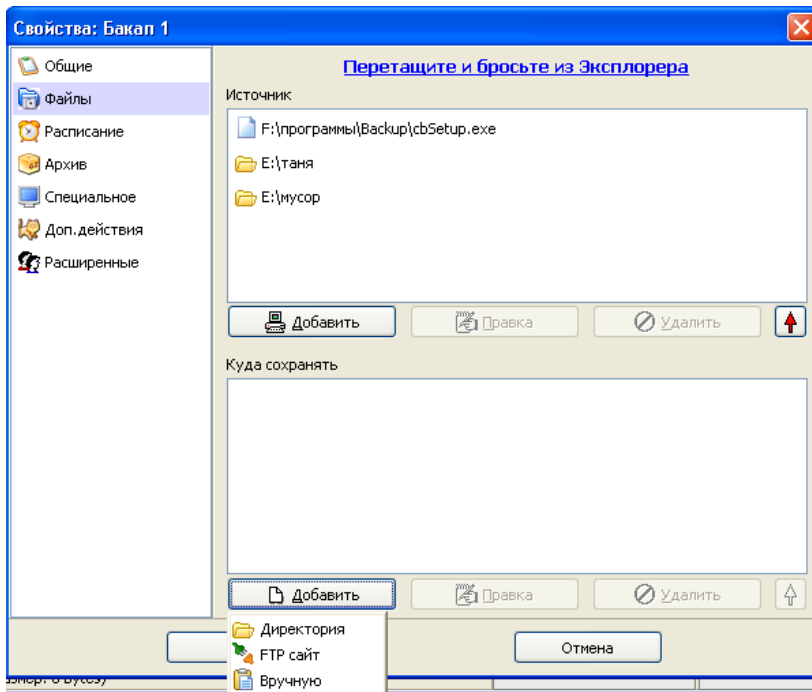
5. В окне *Обзор папок* найдите свою личную папку, в которой собираетесь хранить архивы.



6. Щёлкните по кнопке **OK**

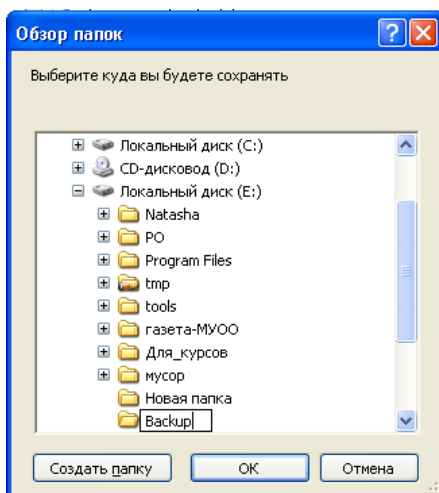
- Если Вы ошиблись в выборе папки, то её можно удалить с помощью кнопки **Удалить**, либо отредактировать с помощью кнопки **Правка**.
- С помощью кнопки  можно расположить папки, файлы:
 - а) Расположить по типу;
 - б) Расположить по алфавиту.

8. В поле *Куда сохранять* щёлкните по кнопке **Добавить**




9. Из выпадающего меню выберите **Директория**

В окне *Обзор папок* укажите диск *D* (допустим) и создайте новую папку *Backup* с помощью кнопки **Создать папку**



10. Щёлкните по кнопке **ОК**

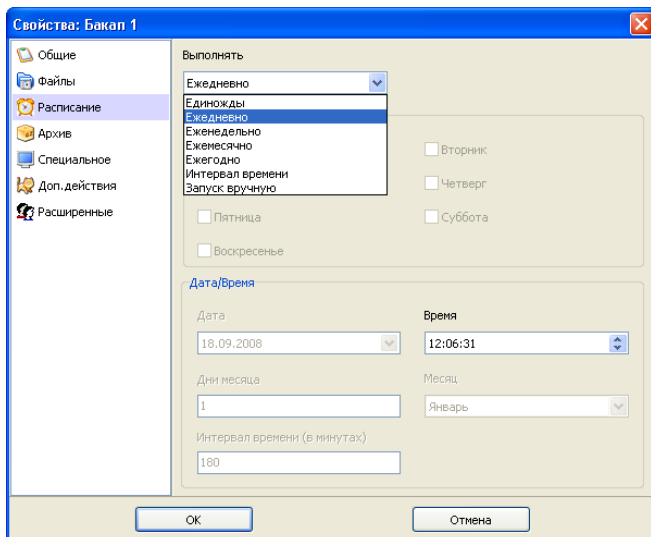
- Если Вы ошиблись в выборе папки, то её можно удалить с помощью кнопки **Удалить**, либо отредактировать с помощью кнопки **Правка**.

- С помощью кнопки  можно расположить папки, файлы:

- c) Расположить по типу;
- d) Расположить по алфавиту.

12. В меню расположенной с левой стороны выбираем **Расписание**

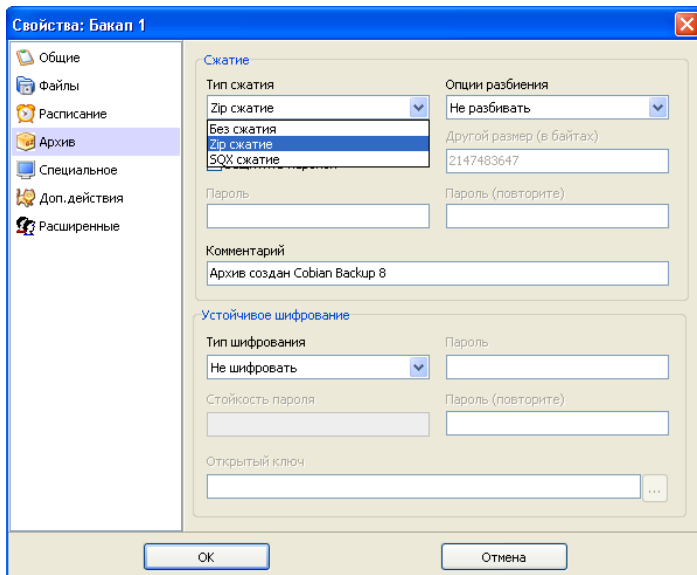
13. В поле *Выполнять* Вы можете установить единожды, ежедневно, еженедельно, ежемесячно, ежегодно, интервал времени, запуск вручную. Установите **ежедневно**.



14. В поле *Время* установите с помощью стрелок время, когда бакап будет запущен.

15. В меню (с левой стороны) выбираем **Архив**

16. В поле *Тип сжатия* из выпадающего списка выберите **Zip сжатие**



17. Щёлкните по кнопке **OK**.

Этот алгоритм расписан для использования с 8 версией программы, сейчас существуют более свежие версии, в них алгоритм действий будет несколько отличаться от предложенного вам.

Полезные ссылки

- Обеспечение информационной безопасности в учебных заведениях. На портале Сети творческих учителей. http://www.it-n.ru/communities.aspx?cat_no=71586&tmpl=com
- Вопросы обеспечения информационной безопасности от компании **Microsoft**
<http://www.microsoft.com/rus/protect/default.mspx#>
- Вопросы безопасности - сайт от компании **Semantec**
http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids
- Ребенок в сети. Сайт от компании **Panda** <http://www.detionline.ru/>
- Специальный портал созданный по вопросам безопасного использования сети Интернет. **Безопасный Интернет** <http://www.saferinternet.ru/>. Документы, материалы и мн. другое.
- **ТЫРНЕТ - Детский Интернет** (<http://www.tirnet.ru/proxy>) сетевой инструмент для организации безопасного серфинга детей в сети Интернет.
- [securelist.com](http://www.securelist.com) (<http://www.securelist.com/ru/encyclopedia>)- Энциклопедия информационной безопасности.
- **Антивирусная Школа** (<http://av-school.ru/>) Антивирусная школа от Касперского
- **Интернет-СМИ "Ваш личный Интернет"** (<http://www.content-filtering.ru/>) помощь родителям в организации безопасного доступа детей в сеть Интернет.
- **InternetSecure.ru - безопасность в интернет** (<http://internetsecure.ru/>) Набор технологий и программ для работы в сети и с компьютером.
- **Безопасность наших школ** (<http://www.schoolsave.ru/>) Портал «Безопасность наших школ» призван обеспечить общественный контроль за мерами пожарной и антитеррористической безопасности, здоровьем школьников и состоянием зданий школ, а также способствовать вовлечению граждан в обсуждение вопросов, связанных с безопасностью российских школ.
- **Security Portal .RU** (<http://www.securityportal.ru/>) Вы найдете информацию по защите информации, защите приватности, безопасным сетевым взаимодействиям, криптографии.
- **Обеспечение безопасности детей при работе в Интернет** (<http://www.oszone.net/6213/>) Обеспечение безопасности детей при работе в Интернет статья, ссылки, материалы.
- **Anti-Malware.ru - независимый информационно-аналитический портал по безопасности** (<http://www.anti-malware.ru/>)
- **Школьный Яндекс** (<http://school.yandex.ru/>) Школьный поисковик

- [Защита детей от интернет угроз](http://www.securitylab.ru/software/1423/) (<http://www.securitylab.ru/software/1423/>) Каталог программ Защита детей от интернет угроз на SecurityLab.ru. Описание, сравнение, оценки
- [Семейная безопасность - Windows Live](http://download.live.com/familysafety) (<http://download.live.com/familysafety>) программа от компании Microsoft.
- <http://nicekit.ru/> -программа родительского контроля. <http://www.kidscontrol.ru/> -Еще один вариант программы для организации родительского контроля. Сегодня многие из нас встают перед проблемой - как же ограничить доступ ребенка к компьютеру, как ограничить время и защитить от порно-наркотиков-матов
- [Этика](http://www.etika.ru/) (<http://www.etika.ru/>) Сайт создан специально для пользователей Рунета, которые хотят работать в этичной, корректной и безопасной среде и готовы участвовать в создании такой среды.
- [Сетевой этикет — Википедия](http://ru.wikipedia.org/wiki/Netiquette) (<http://ru.wikipedia.org/wiki/Netiquette>)
- [WWW.PSYHELP.RU](http://www.psyhelp.ru/texts/iad_test.htm) (http://www.psyhelp.ru/texts/iad_test.htm) Тест Интернет зависимость Кимберли Янг.
- [Проект Антиспам.Ру](http://www.antispam.ru/) (<http://www.antispam.ru/>) Проект Антиспам.Ру
- [Основы безопасности в Интернете для молодежи](http://laste.arvutikaitse.ee/rus/html/etusivu.htm) (<http://laste.arvutikaitse.ee/rus/html/etusivu.htm>) интерактивный курс по Интернет-безопасности.
- CITFORUM <http://www.citforum.ru/security/> Информационная безопасность большое количество материалов
- [Родители, дети, компьютер. Программа контроля использования компьютера ребенком - КиберМама™](http://cybermama.ru/) (<http://cybermama.ru/>) КиберМама - программа для родительского контроля за использованием домашнего компьютера детьми
- [Компьютер и здоровье: болезни от компьютера, профилактика и лечение. Здоровый образ жизни и профессиональные заболевания пользователей компьютеров](http://www.comp-doctor.ru/) (<http://www.comp-doctor.ru/>) Компьютер и здоровье. Болезни, вызываемые компьютером, их профилактика и лечение. Как выбрать безопасные для здоровья компьютер и программы, правильно организовать рабочее место.
- [\[Клякс@.net\]\[Информатика и ИКТ в школе. Компьютер на уроках.\]\[Комплексы упражнений\]](http://www.klyaksa.net/html/pc_and_health/exercise/index.htm) (http://www.klyaksa.net/html/pc_and_health/exercise/index.htm) Сайт для учителей информатики и не только. Комплексы упражнений физкультминутки
- <http://reality.isgreat.org/> Online test на Интернет аддикцию.
- Инфосекьюрити <http://www.infosecurity.ee/> Эстонский сайт о безопасности, но интересен и для российских пользователей сети Интернет.

- [4 этапа защиты компьютера](#) Советы от компании Microsoft.
- [Nachalka.com \(http://www.nachalka.com/\)](http://www.nachalka.com/)- сайт для людей от 6-и лет и старше, имеющих отношение к начальной школе. Для детей это безопасная площадка, где можно узнавать что-то интересное, создавать что-то новое, играть в умные игры, общаться со сверстниками, участвовать в проектах и конкурсах. Родителям интересно обменяться советами о воспитании детей, получить при необходимости консультацию учителей, узнать больше о своих собственных детях. *"Пока мы спорим "пуцать" или "не пуцать" учеников начальной школы в Интернет - они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык "безопасного" поведения в Интернете. Как?"* Этому и не только посвящен раздел сайта "Безопасность детей в Интернет" <http://www.nachalka.com/bezopasnost>
- <http://www.gogul.tv/> Детский браузер Детский интернет браузер Гогуль. Защита детей от нежелательного контента, контроль за интернет-серфингом.
- [Through the Wild Web Woods - A game by the Council of Europe based on the Internet Literacy Handbook \(http://www.wildwebwoods.org/popup.php?lang=ru\)](http://www.wildwebwoods.org/popup.php?lang=ru) Through the Wild Web Woods is an online game for teaching basic Internet safety in a fun and friendly fairy tale environment. The game is available in 14 European language versions. The game was supported by and created in the spirit of 'Building a Europe for and with children'.
- [Поиск детских сайтов. Визуальный Детский поисковик ага \(http://www.agakids.ru/\)](http://www.agakids.ru/) Визуальный Детский поисковик - АГА. В базе данных только детские сайты. Для детей: детское радио, раскраски, игры, учимся рисовать. Поиск сайтов с детской тематикой для детей и родителей. В том числе сайты для родителей по воспитанию, здоровью детей. Клуб международных детских знакомств. Всё лучшее только детям!
- [Мир Бибигона. Социальная сеть для всей семьи \(http://www2.mirbibigona.ru/cgi-bin/sd.fcgi\)](http://www2.mirbibigona.ru/cgi-bin/sd.fcgi)
- [KIDO'Z - Safe,easy and fun internet for kids \(http://kidoz.net/\)](http://kidoz.net/)The KIDO'Z Kid's Web Environment is the safe, easy and fun way for young kids to surf their favorite sites, watch videos, play games, send emails, create and communicate without knowing how to read and write!.
- Интерактивная игра «Джунгли Интернета» <http://school-sector.relarn.ru/wps/?p=1706> Игра предназначена для детей в возрасте от 7 до 10 лет и создавалась в духе программы » Строим Европу для детей и вместе с детьми».
- Сетевые технологии в помощь учителю. <http://www.openclass.ru/wiki-pages/26731>

Литература и документы

- Информационные технологии в управлении образованием «Национальный фонд подготовки кадров» Москва УМП 2006г.
- Соглашение об организации проведения работ по подключению образовательных учреждений к сети Интернет в рамках реализации мероприятия «Развитие технической основы современных информационных образовательных технологий» направления «Внедрение современных образовательных технологий» приоритетного национального проекта «Образование» 2006 г с приложениями.
- Проект Федерального закона N 155219-5 "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию" http://www.pravinfo.ru/dn_2009_30.shtml
- Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных. <http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html>
- Федеральный закон Российской Федерации от 9 февраля 2009 г. N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" <http://www.rg.ru/2009/02/13/dostup-dok.html>
- Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 г. № 3523—1) <http://www.consultant.ru/online/base/?req=doc;base=LAW;n=58240>
- Закон Российской Федерации от 09.07.93г. №5351-1 “Об авторском праве и смежных правах” http://www.copyright.ru/ru/library/zakonodatelstvo/avtorskoe_pravo_i_smezhnye_prava/ob_avtorskom_prave_i_smezhnih_pravah/
- Федеральный закон Российской Федерации от 24 февраля 2010 г. N 17-ФЗ "О внесении изменения в статью 1501 части четвертой Гражданского кодекса Российской Федерации" С текстом части четвертой ГК. <http://www.rg.ru/2010/02/26/izmenenie-dok.html>
- Федеральный Закон «О государственной тайне» №5485-1 http://svr.gov.ru/svr_today/doc05.htm
- Федеральный закон "О связи" № 126-ФЗ <http://ham-cq.pnz.ru/files/mainlaw.html>
- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации. <http://www.rg.ru/2006/07/29/informacia-dok.html>

- Типовая инструкция по охране труда при работе на персональном компьютере ТООИ Р-45-084-01. <http://mvf.klerk.ru/spr/spr89.htm>
- Сайт Безопасность наших школ. Нормативная документация. <http://www.schoolsave.ru/documents/>
- Локальные акты образовательного учреждения (материалы Российского образовательного портала). http://zakon.edu.ru/catalog.asp?cat_ob_no=12712
- Права и дети в Интернет. <http://school-sector.relarn.ru/prava/>
 - Безопасная работа в Интернет. (памятка) Какие программы следует использовать для защиты компьютера. http://www.openclass.ru/sites/default/files/panel/2009/06/___18416.pdf