1. **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...

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

Необходима для защиты от злоумышленников и вредоносных программ, использующих для своего несанкционированного доступа **уязвимости** Microsoft Windows. Через сайт Microsoft Update: http://update.microsoft.com или через функцию автоматического обновления Windows.

2. Установка антивирусной программы.

На компьютере **обязательно** должно быть установлено антивирусное программное обеспечение и программа запущена в режиме мониторинга. Одна из самых популярных в России антивирусных программ - Антивирус Касперского (имеется в пакете Первая Помощь). Можно воспользоваться и альтернативными программами. Так как на слабых машинах Антивирус Касперского будет очень заметно тормозить работу.

БЕСПЛАТНЫЕ:
avast! 4 Home Edition http://www.avast.com/eng/download-avast-home.html
AntiVir® PersonalEdition Classic http://free-av.com/antivirus/allinonen.html
Comodo AntiVirus http://antivirus.comodo.com/
AVG Free http://free.grisoft.com

Очень важно **регулярно обновлять** антивирусные базы. В противном случае толку от антивируса не будет никакого. **Не рекомендуется** включать одновременно два (и более) антивируса на одном персональном компьютере во избежание серьезных конфликтов в

системе. По тем же причинам перед установкой нового антивирусного продукта - не забудьте **удалить** старый. Вот тут при удалении Антивируса Касперского возникает ряд сложностей. Остается много «мусора»

3. Установка файрвола (он же брандмауэр и межсетевой экран).

Это необходимо для защиты компьютера от несанкционированного доступа и организации безопасного подключения к сети Интернет. Для минимальной защиты достаточно включить межсетевой экран, встроенный в Windows XP: **Пуск > Панель Управления > Центр обеспечения безопасности > Брендмауер**

БЕСПЛАТНЫЕ:
Comodo Firewall http://www.personalfirewall.comodo.com/
ZoneAlarm http://www.zonealarm.com/
Outpost Firewall FREE http://www.agnitum.ru/products/outpostfree/index.php

4. Установка альтернативного браузера.

Так как Internet Explorer является самым распространенным браузером в мире, большинство вредоносных программ пишутся именно под его уязвимости, и не работают в его альтернативных вариантах (т.е. опасны только лишь для IE). Хотя IE так же придется оставить на компьютере, так как отдельные интерактивные формы, заполняемые в сети Интернет могут не работать с альтернативными браузерами.

БЕСПЛАТНЫЕ:
Mozilla Firefox http://www.mozilla.ru/
Opera http://www.opera.com/download/

5. Кроме антивирусной программы рекомендуется установить дополнительные свободные программы-помощники.

- **Spybot - Search & Destroy (Спайбот - найти и уничтожить)** может 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.
- **StopAutorun.** Программа создана для защиты Вашего ПК от вторжений и проникновений всевозможных вирусов, которые распространяются посредством **сменных** носителей. Эта программа *не заменяет* антивирус, а лишь дополняет его. Она может обнаруживать новые неизвестные вредоносные программы и вести наблюдение за системной папкой Windows, обеспечивая большую защиту компьютера. StopAutorun будет постоянно наблюдать за жесткими дисками и сменными носителями и защищать Вас от троянов и вирусов. Для большой безопасности рекомендуется установить на каждый компьютер. Сайт поддержки http://makesoft.at.ua/load/1-1-0-4.

Важно! *Рекомендуется **регулярно** проверять компьютер утилитой **CureIt** загруженной с сайта http://www.FreeDrWeb.ru Причем та утилита бесплатна и ежедневно обновляется на сайте производителя. Либо Антивирусной утилитой лаборатории Касперского **AVZ** http://www.kasperski.ru*

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 нелицензионного ПО и ПО сомнительного происхождения. Нелицензионное ПО необходимо немедленно

деинсталлировать с компьютера, ПО сомнительного происхождения - проверить лицензионное соглашение (ПО может быть бесплатным или условно-бесплатным).

Для того чтобы обезопасить себя от случайного поражения вирусами необходимо быть внимательным в общении и не общаться со случайными людьми (электронная почта) и различными сайтами. Это может произойти в двух случаях: если вы посещаете сайты сомнительного содержания и как постороннее вложение в электронных письмах. В первом случае достаточно свести к минимуму посещение сомнительных сайтов. Правда для этого существует система СКФ, но наши «продвинутые» детишки знают, что эту систему очень легко обойти, воспользовавшись анонимайзером, которых множество в сети (в этом случае присвоенный ip- адрес подменяется случайным адресом и компьютер лишается защиты). Значит, учитель должен быть всегда начеку! 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

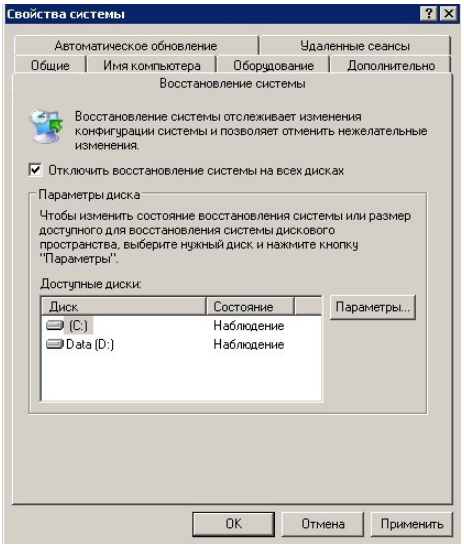
Их может быть гораздо больше, но это наиболее часто встречающиеся, причем отдельные проблемы могут быть вызваны неправильной работой отдельных программ на вашем компьютере:

2. Спонтанная перезагрузка компьютера, без вашего в этом участия.
3. Появление критических и системных ошибок там, где их раньше никогда не было.
4. Частые зависания и сбои в работе компьютера без видимых на то причин.
5. Резко увеличилось время загрузки операционной системы.
6. Повседневные задачи выполняются компьютером гораздо медленнее, чем обычно.
7. Программы, которые раньше работали, внезапно перестали нормально функционировать или значительно возросло время их обычной загрузки.
8. Ненормальная сетевая активность и обращение по нетипичным вам сетевым адресам.
9. Предупреждения файрвола о попытке выйти в интернет незнакомых вам приложений.
10. Постоянные перебои в работе интернет-соединения или частые зависания браузера.
11. Нет доступа к некоторым сайтам, либо при обращении вместо нужного - открывается совсем другой.
12. Изменились настройки вашего браузера (к примеру, домашняя страница), и вернуть их в желаемое состояние обычными способами не получается.
13. Неожиданное открытие и закрытие CD-ROM'a.
14. Стремительное уменьшение свободного место на дисках.
15. 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).
16. Непонятное завершение антивирусной программы или файрвола.
17. Перезапуск системы в безопасном режиме (Safe Mode) приводит к ее полному зависанию.
18. Компьютер перестает отвечать на ваши запросы и часто блокируется.
19. Невозможность загрузки операционной системы.

Ваши действия, если на компьютере обнаружились вирусы:

Для того, чтобы процесс лечения был успешным, 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 могут вам пригодится в процессе лечения. Можно записать их на компьютер, предварительно переименовав, так как есть ряд вирусов способных заблокировать работу антивирусов с типовым именем.
- Отключиться от сети Интернет. Отключиться от локальной сети. Лучше выдернуть из компьютера кабель локальной сети

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, после чего вам предложат перезагрузиться - **лучше немного повременить и сделать это после следующей процедуры**.
- 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, например CCleaner http://www.filehippo.com/download_ccleaner/

Проверяем все локальные диски антивирусной программой. Очень удобно здесь как раз и воспользоваться *утилитой* **CureIt** http://www.freedrweb.ru о которой говорилось ранее. 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 вирусописателем либо компьютер будет вести себя не адекватно.

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

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**", нажимаем "Enter"

Когда сканирование будет закончено, и все найденные антивирусом вредоносные файлы вылечены/удалены, перезагружаем компьютер, и после обязательно делаем повторную проверку системы.

Если при повторном сканировании антивирус больше ничего не найдет и симптомы заражения действительно исчезнут - включаем обратно всё то, что мы отключили (функцию Восстановление Системы, сеть, Интернет) и успокаиваемся.

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

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 (так называемый live CD). Очень хорошо подойдет диск Bart PE, Linux и др.. Например- Bart PE является несколько урезанной версией Windows XP, которая помещается на загрузочном диске CD-ROM или USB-накопителе. Если ваш ПК перестал загружаться с жёсткого диска, для загрузки им также можно будет воспользоваться и поработать с компьютером. Но для того, чтобы операционная система загрузилась с диска необходимо в BIOS изменить очередность загрузки (загрузка с CD), если это не произошло.

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 может быть расположено по разному):

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 BIOSe прежние параметры загрузки (с жесткого диска) Это позволит предотвратить заражение компьютера в момент включения от случайных дисков, дискет и флешек).*

После этого операционная система загрузится с диска. После загрузки можно открыть рабочий диск. Лучше это сделать с помощью файлового менеджера 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 процедуры запустить утилиту **CureIt** http://www.freedrweb.ru. либо утилиту лаборатории Касперского **AVZ** http://www.kaspersky.ru

После всего мы перезагружаем компьютер с жёсткого диска и можем продолжать работать с информацией.

Особенно **важно** работая с базами, например с базой ОУ Хронограф Школа 2,5, 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 программы для **архивного копирования** позволит избежать потерь 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 пользователем АРМ.