Памятка для родителей и педагогов по безопасности работы детей в интернет-пространстве на разных возрастных этапах

(по материалам В. Ф. Безмалого)

Подключаясь к сети Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать

Какие угрозы встречаются наиболее часто?
— доступ к нежелательному содержимому. Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики, порнография, страницы, подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернете без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера;
— контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.

Рекомендации по безопасности использования сети Интернет детьми
1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернета.
2. Объясните детям, что если в Интернете что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством.
3. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, MicrosoftMessenger и т. д.), использования Online-игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.
4. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т. д.
5. Объясните своему ребенку, что в реальной жизни и в Интернете нет разницы между неправильными и правильными поступками.
6. Научите ваших детей уважать собеседников в Интернете. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернете и в реальной жизни.
7. Скажите им, что никогда не стоит встречаться с друзьями из Интернета. Ведь люди могут оказаться совсем не теми, за кого себя выдают.
8. Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернет-пространстве — правда. Приучите их спрашивать о том, в чем они не уверены.
9. Не забывайте контролировать детей в Интернете с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.
Как научить детей отличать правду ото лжи в интернет-пространстве?
— Начните, когда ваш ребенок еще достаточно мал. Ведь сегодня даже дошкольники уже

успешно используют сеть Интернет, а значит нужно как можно раньше научить их отделять правду ото лжи.
Никто не будет контролировать, насколько правдива размещенная там информация. Научите ребенка проверять все то, что он видит в Интернете.

Как это объяснить?
— Не забывайте спрашивать ребенка об увиденном в Интернете. Например, начните с расспросов, для чего служит тот или иной сайт.
— Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в Интернете информацию по другим источникам (по другим сайтам, газетам или журналам). Приучите вашего ребенка советоваться с вами. Не отмахивайтесь от их детских проблем.
— Поощряйте ваших детей использовать различные источники, такие как библиотеки или подарите им энциклопедию на диске, например, «Энциклопедию Кирилла и Мефодия» или MicrosoftEncarta. Это поможет научить вашего ребенка использовать сторонние источники информации.
— Научите ребенка пользоваться поиском в Интернете. Покажите, как использовать различные поисковые машины для осуществления поиска.
— Объясните вашим детям, что такое расизм, фашизм, межнациональная и религиозная вражда. Несмотря на то, что некоторые подобные материалы можно заблокировать с помощью специальных программных фильтров, не стоит надеяться на то, что вам удастся отфильтровать все подобные сайты.

Семейное соглашение о работе в Интернете.

Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение по использованию Интернета. Учтите, что в нем вы должны однозначно описать права и обязанности каждого члена вашей семьи. Не забудьте четко сформулировать ответы на следующие вопросы:

— Какие сайты могут посещать ваши дети и что они могут там делать?
— Сколько времени дети могут проводить в Интернете?
— Что делать, если ваших детей что-то беспокоит при посещении Интернета?
— Как защитить личные данные?
— Как следить за безопасностью?
— Как вести себя вежливо?
— Как пользоваться чатами, группами новостей и службами мгновенных сообщений?

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы должны проверять выполнение соглашения вашими детьми.

Научите вашего ребенка использовать службу мгновенных сообщений.

При использовании службы мгновенных сообщений напомните вашему ребенку некоторые несложные правила безопасности:

— никогда не заполняйте графы, относящиеся к личным данным, ведь просмотреть их может каждый;
— никогда не общайтесь в Интернете с незнакомыми людьми;
— регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;

— внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает;
— не следует использовать системы мгновенных сообщений для распространения слухов или сплетен.

Родителям не стоит надеяться на тайную слежку за службами мгновенных сообщений, которыми пользуются дети. Гораздо проще использовать доброжелательные отношения с вашими детьми.

Может ли ваш ребенок стать интернет-зависимым?

Не забывайте, что Интернет это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию интернет-зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не становится очень серьезной. Да и, кроме того, факт наличия такой болезни как интернет-зависимость не всегда признается. Что же делать?

Советы по безопасности для детей разного возраста.

Как показали исследования, проводимые в сети Интернет, наиболее растущим сегментом пользователей Интернета являются дошкольники.

В этом возрасте взрослые будут играть определяющую роль в обучении детей безопасному использованию Интернета.

Возраст от 7 до 8 лет.
Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернете ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.
Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах интернет-папки: /Users/User/AppData/Local/Microsoft/Windows/TemporaryInternetFiles(в операционной системе WindowsVista).
В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок.
Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернету. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.
По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.
Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как KasperskyInternetSecurity версии 7.0 со встроенным родительским контролем.

Что можно посоветовать в плане безопасности в таком возрасте?
— Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
— Требуйте от вашего ребенка соблюдения временных норм нахождения за

компьютером.
— Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
— Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т. е. создайте им так называемый «белый» список Интернета с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее.
— Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
— Используйте специальные детские поисковые машины, типа MSNKidsSearch(http://search.msn.com/kids/default.aspx?FORM=YCHM).
— Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
— Создайте семейный электронный ящик, чтобы не позволять детям иметь собственные адреса.
— Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
— Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
— Приучите детей не загружать файлы, программы или музыку без вашего согласия.
— Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы. Подробнее о таких фильтрах httg://www.microsoft.com/rus/athome/security/email/fightspam.mspx.
— Не разрешайте детям использовать службы мгновенного обмена сообщениями.
— В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
— Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
— Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».
— Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст от 9-12 лет.
В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте.
— Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
— Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.
— Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
— Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
— Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
— Не забывайте беседовать с детьми об их друзьях в Интернете.

— Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
— Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
— Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
— Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
— Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
— Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
— Расскажите детям о порнографии в Интернете.
— Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
— Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст от 13-17 лет.
В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила интернет-безопасности — соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.
В 13-17 лет подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Советы по безопасности в этом возрасте.
— Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
— Компьютер с подключением к Интернету должен находиться в общей комнате, часы работы в Интернете могут быть легко настроены при помощи средств Родительского контроля.
— Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
— Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
— Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
— Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из

Интернета.
— Приучайте детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
— Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
— Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если вами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
— Расскажите детям о порнографии в Интернете.
— Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
— Приучите себя знакомиться с сайтами, которые посещают подростки.
— Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям.
— Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Как проводить Родительский контроль над поведением детей в Интернете?

Обеспечивать родительский контроль в Интернете можно с помощью различного программного обеспечения, например, Родительский контроль в WindowsVista, средства Родительского контроля, встроенные в KasperskyInternetSecurity.

МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ РАБОТЕ В ИНТЕРНЕТЕ

Интернет дает вам возможность, не выходя из дома, быстро находить необходимую информацию, участвовать в обсуждениях интересующих вас проблем на различных форумах и в интернет-конференциях, приобретать товары и услуги, осуществлять платежи, обмениваться сообщениями по электронной почте. Однако, пользуясь Интернетом, нельзя забывать о безопасности. Помните:
• в ваш компьютер может попасть компьютерный вирус;
• ваш электронный адрес может оказаться в базе данных для рассылки рекламы;
• сведения, которые вы сообщаете о себе в Интернете, могут стать известны посторонним лицам;
• информация, которую вы находите в сети, может быть недостоверной;
• вы можете стать жертвой мошенников.
Все это ни в коем случае не значит, что нужно отказаться от использования Интернета. Просто необходимо знать о том, какие опасности вас подстерегают, и уметь их распознавать и предупреждать их последствия.

Спам и кибермошенничество
Спам (англ. spam, сокращение от self-promotion and marketing) – это массовая, иногда сразу по нескольким миллионам адресов, рассылка рекламных сообщений. Тех, кто распространяет по электронной почте такие письма, называют спамерами.
Отличительные черты спама – отсутствие предварительного согласия адресата на получение сообщения, невозможность отказаться от получения аналогичных сообщений в будущем, фальсифицированный адрес отправителя.

Спамерские письма обычно бывает легко узнать по теме сообщения. Чаще всего в них рекламируются юридические, бухгалтерские, туристические, медицинские и косметические услуги, методы быстрого похудения, курсы иностранных языков, бизнес-семинары, порнографические интернет-сайты и издания, интимные услуги. Нередко также встречаются предложения баз данных с электронными адресами, т.н. «спам про спам» Обнаружив в поступившей почте сообщение с подобной темой, подумайте, может ли оно представлять для вас какой-то интерес, и если нет – смело его удаляйте.

Виды спама

• Реклама. Это письма типа «сдаем в аренду офис» или «Верный способ повысить ваши доходы», а также предложения улучшить ваш персональный сайт, изменить пропорции тела, вывести волосы на ушах и тому подобное. Именно с помощью такого рода спама рекламируют продукцию, о которой нельзя сообщить потенциальным потребителям иным способом: порнографию, лекарственные препараты, оборот которых не лицензирован или ограничен законом, добытую незаконным путем информацию (различные базы данных), контрафактные компьютерные программы.

• «Нигерийские письма». Мошенники часто используют спам с целью выманить у легковерного получателя деньги. Наиболее распространенный способ такого рода жульничества известен как «нигерийские письма», поскольку вначале большинство подобных сообщений приходило из Нигерии. Содержание «нигерийского письма» сводится к следующему: вам сулят возможность без особого труда заработать много денег, но при этом отправитель просит перевести на указанный счет небольшую сумму, необходимую для оформления документов или покрытия каких-то других расходов. Обещание легкого обогащения, естественно, всего лишь приманка, задача мошенника – получить ваши деньги.

• Фишинг (англ. phishing, по аналогии с fishing – «рыбалка») – еще один способ мошенничества с помощью спама, только в этом случае у ас пытаются выманить не деньги, а номер кредитной карты, банковского счета или пароль доступа к системе платежей через Интернет. Письмо обычно выглядит как официальное уведомление от банка, где говорится, что получатель должен подтвердить сведения о себе, иначе его счет будет заблокирован. Тут же приводится адрес принадлежащего спамерам сайта. Чтобы жертва не догадалась об обмане, оформление подставного сайта имитирует дизайн официального сайта банка. Среди данных, которые требуется указать в размещенной там онлайн-форме, присутствуют и те, что нужны преступникам, вознамерившимся вас обокрасть.

• Предложения принять участие в финансовых пирамидах. Такие послания тоже редко отличаются друг от друга. Обычно сначала вас заверяют в том, что «это не спам», а а затем предлагают работу, за которую вы сможете получить баснословную сумму. Часто в поле «Тема» подобных сообщений пишут «Не удаляйте это письмо» или Please read It carefully («Пожалуйста, прочтите внимательно»).

• Предложения зайти на некий сайт. Цель таких писем – заставить вас щелкнуть по приведенной в тексте ссылке. Средства для этого выбираются самые разные. Например, в письме может быть сказано, что это рассылка, на которую вас подписали, но, если вы не хотите ее получать, подписку легко аннулировать, щелкнув по ссылке на соответствующий сайт, - разумеется, ни в какую онлайн-форму для отказа от рассылки вы при этом не попадете. Нередко подобные письма маскируются под личные и даже интимные послания, обращенные именно к вам: «Привет! У меня все нормально. Хочешь посмотреть мои новые фотки? Вот ссылка…». Главная отличительная особенность таких писем – наличие ссылки на неизвестный вам сайт. Кроме того, вместо вашего настоящего имени даже в приветствии стоит имя пользователя, т.е. часть вашего электронного адреса до знака @.

• Скам (англ. scam – «жульничество, обман») – еще один вариант письма с целью

выманить у вас деньги. В разосланном мошенниками письме получателям предлагают купить дешевые ноутбуки или, скажем, товары, конфискованные на таможне. Как правило, часть платежа просят перевести авансом, после чего контактные телефоны и указанный в письме сайт перестают работать. Товар-приманку вы, разумеется, никогда не получите.
Среди других видов спама можно назвать массовые рассылки писем религиозного содержания; сообщений, цель которых – вывод из строя почтовой сиситмы (denial of service); электронных писем от чужого имени с целью вызвать негативное отношение к «отправителю» (т.н. черный пиар); писем, содержащих компьютерные вирусы (таким образом обеспечивается их быстрое распространение).

Защита от спама

Превентивные методы
Самый надежный способ защиты от спама – не позволить спамерам узнать ваш электронный адрес. Для этого рекомендуется соблюдать следующие правила.
• Заводите электронный почтовый ящик не на бесплатном почтовом сервере, а в корпоративной сети или у интернет-провайдера (солидные провайдеры обычно предоставляют клиентам почтовый ящик на своем сервере). Как правило, такие электронные адреса к спамерам не попадают.
• При создании электронной почты выбирайте нестандартное имя пользователя. У спамеров имеются специальные словари, включающие простые слова английского языка, имена людей, названия географических объектов и некоторые наиболее распространенные выражения из сленга пользователей Интернета. Используя такой словарь и список доменных имен, которые открыто публикуются, несложно получить множество адресов для спамерских рассылок.
• Не сообщайте свой электронный адрес на интернет-сайтах, которые не дают гарантии неразглашения конфиденциальной информации. По возможности старайтесь не делать этого также на форумах, на собственном сайте и в электронных письмах.
• Если вам необходимо указать свой электронный адрес, например, в ответ на просьбу другого учасника форума, пишите его с пробелами перед знаком @ и после него. В этом случае адрес не попадет в базы данных спамеров, так как используемые ими специальные поисковые программы не смогут опознать эту запись как электронный адрес.
• При регистрации на различных сайтах указывайте в онлайн-формах не ваш основной адрес электронной почты, а адрес специально заведенного для этих целей бесплатного почтового ящика.
• Никогда не отвечайте на письма спамеров и не переходите на интернет-сайты по содержащимся в них ссылках. Такими действиями вы подтвердите, что активно пользуетесь своим электронным адресом, и станете получать еще больше спама.
Безусловно, даже строго выполняя эти простые правила, полностью от спама вы не избавитесь, но ваш личный почтовый ящик, по крайней мере, не будет переполняться ненужными рекламными сообщениями.
Фильтрационные методы
Сегодня существуют программы для автоматического распознавания спама и его фильтрации. Подобные фильтр широко применяются на почтовых серверах, но некоторые из этих программ предназначены и для индивидуальных пользователей и могут быть установлены на персональном компьютере.

Компьютерные вирусы

Классификация вредоносных программ

Назойливая реклама, рассылаемая по электронной почте, раздражает и мешает работе, но чаще всего спам не несет опасности для вашего компьютера. Другое дело вирусы, программы-шпионы и сетевые атаки, которые представляют серьезную угрозу компьютеру, подсоединенному к Интернету.

По способу распространения вредоносные программы можно разделить на следующие виды:

• вирусы – программы, способные размножаться внедрять свои копии в другие файлы;
• сетевые «черви» – программы, которые не изменяют файлы на жестком диске компьютера, а проникают в его операционную систему и затем, находя на компьютере адреса других пользователей, рассылают по этим дресам свои копии;
• «троянские» программы – исполняемые файлы, обычно маскирующиеся под новую версию какой-нибудь популярной программы или игры с целью заставить пользователя установить их на свой компьютер.

Вирусы и другие вредоносные программы могут попасть в ваш компьютер различным путем: при копировании программ с чужого компьютера без проверки на наличие в них вирусов; при открытии зараженных файлов, полученных по электронной почте; при посещении сомнительных сайтов, чаще всего порнографических или тех, с которых можно скачать пиратское программное обеспечение.

Как определить, что в ваш компьютер попал вирус

Запустив зараженную программу, вы, как правило, даже не заметите, что активировали вирус, и лишь позднее обнаружите, что с вашим компьютером что-то не так. Вот несколько признаков, свидетельствующих о том, что ваш компьютер, возможно, заражен вирусом:

• компьютер стал работать медленнее, чем раньше;
• компьютер не отвечает на запросы или часто зависает;
• компьютер каждые несколько минут дает сбои и сам перезагружается;
• компьютер перезагружается без вашей команды и после этого не может работать в нормальном режиме;
• программы на вашем компьютере работают неправильно;
• дисководы становятся недоступными;
• возникают проблемы при вводе текста с помощью клавиатуры;
• вам не удается нормально распечатать текст на принтере;
• компьютер выдает необычные сообщения об ошибках.

Антивирусные программы

Самое эффективное средство борьбы с вредоносными программами – применение антивирусных программ. Ни одна из таких программ (их для краткости часто называют просто антивирусами) е обеспечивает стопроцентной защиты, поэтому при выборе антивируса необходимо учитывать ряд параметров: надежность программы, удобство ее использования, скорость работы, способность идентифицировать максимальное количество распространенных типов вирусов, возможность «лечения» зараженных объектов, наличие других полезных функций. Правильно настроенная антивирусная программа способна проверять компьютер в автоматическом режиме и информировать вас о наличии вирусов.

Наиболее известные антивирусные программы

1. Norton AntiVirus. Разработанная компанией Symantec Corporation (www.symantec.ru)
2. Антивирус NOD32. Разработанная компанией Eset Software (www.esetnod32.ru)
3. Doctor Web. (www.drweb.ru)

4. Антивирус Касперского. Лаборатория Касперского (www.kaspersky.ru)
5. Антивирус AVG Free Edition. Бесплатная. (www.free.grisoft.com)