**ПАМЯТКА**

***Повышение уровня безопасности детей в Интернете при помощи технических средств.***

**ПОВЫСЬТЕ УРОВЕНЬ ОБЩЕЙ БЕЗОПАСНОСТИ ВАШЕГО КОМПЬЮТЕРА**

Если на вашем компьютере установлена операционная система Microsoft®Windows®XP Service Pack 2, то можно использовать Windows Security Center. Эта программа позволяет просматривать информацию о состоянии защиты компьютера и изменять настройки, а также получать дополнительные сведения по вопросам безопасности.

Security Center показывает состояние трех важных компонентов безопасности: брандмауэра интернета, антивирусных программ и службы автоматического обновления. Кроме того, он служит для перехода к другим разделам безопасности, а также поиска технической поддержки и ресурсов, имеющих отношение к защите компьютера.

Security Center работает в фоновом режиме, постоянно проверяя состояние трёх наиболее важных компонентов. для того, чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующее:

v нажмите кнопку *Пуск/Start*, в открывшемся меню выберите *Панель управления/Control* *Panel*;

v в панели управления откройте *Центр обеспечения безопасности/ Security* *Center*;

v убедитесь, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).

Включить или отключить брандмауэр и автоматическое обновление вы можете непосредственно в *Центре обеспечения безопасности.*

Для управления защитой от вирусов обратитесь к настройкам установленного антивирусного программного обеспечения.

У**СТАНОВИТЕ НА ВАШЕМ КОМПЬЮТЕРЕ АНТИШПИОНСКИЕ НАСТРОЙКИ ИЛИ ДОПОЛНИТЕЛЬНОЕ АНТИШПИОНСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

Шпионскими называются программы, выполняющие определённые действия (например, сбор личной информации или изменение настроек) без согласия и контроля пользователя. Они могут существенно замедлить работу системы и привести к нежелательным изменениям в важных настройках.

Такие программы трудно удалить.

Антишпионское программное обеспечение поможет избавиться от шпионских и других нежелательных программ. Проверка компьютера может выполняться по расписанию в удобное для вас время.

Для того, чтобы предотвратить появление шпионского программного обеспечения на вашем компьютере, необходимо убедиться в том, что включены основные средства *Центра обеспечения безопасности* вашей операционной системы.

Для повседневной работы также рекомендуется использовать учетную запись с ограниченными правами.

Для удаления шпионского программного обеспечения, попавшего на ваш компьютер, следует воспользоваться специальным антишпионским программным обеспечениям, в частности, следующими программами:

*Windows* *Defender;*

*Malicious* *Software* *Removal* *Tool.*

Эти бесплатные программы вы можете загрузить с сайта htpp://www.microsoft.com/downloads. Для этого в строке *Search* в выпадающем списке выберите *All* *Downloads,* в строке справа введите название одного из указанных выше продуктов и нажмите кнопку *Go*.

**БЛОКИРУЙТЕ ДОСТУП К НЕПОДХОДЯЩИМ МАТЕРИАЛАМ**

Один из наилучших способов защиты от нежелательной информации – это блокировка доступа ещё до того, как она может быть получена.

Microsoft предлагает несколько таких способов.

Для того, чтобы блокировать доступ к нежелательной информации в *Internet* *Explorer®* и *MSN* *Explorer*, нужно выполнить следующее:

v нажмите кнопку *Пуск/Start*, в открывшемся меню выберите *Панель управления/Control* *Panel;*

v в панели управления откройте *Свойства обозревателя/Internet* *Options*;

v в появившемся окне перейдите на вкладку *Содержание/Content*;

v в разделе *Ограничение доступа/Content* *Advisor* нажмите кнопку *Включить/Enable*;

v в появившемся окне введите пароль, который будет защищать вводимые вами ограничения от изменения детьми;

v в окне *Ограничение доступа/ Content* *Advisor* вы можете блокировать доступ к нежелательной информации.

**ПОВЫСЬТЕ УРОВЕНЬ БЕЗОПАСНОСТИ**

**ПРИ РАБОТЕ РЕБЁНКА С ЭЛЕКТРОННОЙ ПОЧТОЙ**

Для повышения уровня безопасности при работе ребёнка с электронной почтой в меню программы Outlook®Express в разделе *Сервис/Tools* выберите команду *Параметры/Options*. перейдите на вкладку Безопасность/Security.

При помощи переключателя *Выберите зону безопасности для Internet* *Explorer/Select* *the* *Internet* *Explorer* *security* *zone* *to* *use* вы можете уменьшить вероятность появления вирусов на вашем компьютере. Для этих же целей служит переключатель *Не разрешать сохранение или открытие вложений, которые могут содержать вирусы/Do* *not* *allow* *attachments* *to* *be* *saved* *or* *opened* *that* *could* *potentially* *be* *a* *virus.*

Если же вирус все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочку *Предупреждать, если приложения пытаются отправить почту от моего имени/Warn* *me* *when* *other* *applications* *try* *to* *send* *mail* *as* *me.*

для защиты пересылаемых писем от подделки и от возможности перехвата и прочтения кем-либо кроме указанного получателя, есть возможность выбрать команды *Шифровать содержимое и вложения всех исходящих сообщений/Encrypt* *content* *and* *attachments* *for* *all* *outgoing* *messages* и *Подписывать все отправляемые сообщения/Digitally* *sign* *all* *outgoing* *messages.*

**ЗАБЛОКИРУЙТЕ ПОСТУПЛЕНИЕ СПАМА.**

Чтобы блокировать поступление спама (нежелательной почты), необходимо воспользоваться почтовым сервером, имеющим защиту от спама (например, normail.com), или почтовым клиентом, имеющим спам-фильтр (например, Microsoft Outlook).

Чтобы настроить спам-фильтр для почтового ящика, размещённого на серdере normail.com , необходимо зайти в это почтовый ящик, перейти по ссылке *Options* и в вертикальном меню выбрать вкладку *Mail*.

Перейти по ссылке *Junk* *E-mail* *filter*, вы можете изменить настройки фильтра нежелательной почты.

При помощи ссылки *Block* *Senders*, находящейся на вкладке *Mail*, вы можете добавить любого отправителя в список заблокированных, при этом почта от этого отправителя не будет поступать в ваш почтовый ящик.

Если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.

Для настройки этого фильтра в меню Microsoft Outlook выберите *Сервис/Tools*, в открывшемся меню выберите команду *Параметры*/*Options.* В открывшемся диалоговом окне перейдите на вкладку *Настройки/Preferences* и нажмите кнопку *Нежелательная почта/Junk* *E-mail.*

В появившемся диалоговом окне вы можете внести изменения в настройки фильтра нежелательной почты.

Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

**СОЗДАЙТЕ ОТДЕЛЬНЫЕ УЧЁТНЫЕ ЗАПИСИ ДЛЯ РАЗНЫХ ПОЛЬЗОВАТЕЛЕЙ.**

Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой *Мои документы*. Родитель может создать себе учетную запись администратора, дающий полный контроль над компьютером, а детям – ограниченные учетные записи. Пользователи с ограниченными учетными записями не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение включая большинство игр, медиаплееров и программ поддержки чатов.

Для того чтобы создать отдельную учетную запись для ребёнка с органиченными правами доступа для работы в интернете, необходимо выполнить следующие действия:

v нажмите кнопку *Пуск/Start,* в открывшемся меню выберите *Панель управления/Control* *Panel;*

v в панели управления откройте *Учетные записи пользователей/User* *Accounts*;

v в открывшемся окне выберите *Создание учетной записи/Create* *a* *new* *Accounts*, введите её имя;

v на этапе выбора типа учётной записи установите переключатель в положение *Ограниченная запись/Limited*;

v после нажатия кнопки *Создать учетную запись/Create* *Account* процесс создания учетной записи с ограниченными правами будет завершен, и ваш ребёнок сможет выбрать её при следующем входе в систему.

**ПОВЫСЬТЕ УРОВЕНЬ КОНФИДЕНЦИАЛЬНОСТИ**

**ПРИ ОБЩЕНИИ ВАШЕГО РЕБЁНКА В ИНТЕРНЕТЕ**

**С ПОМОЩЬЮ INTERNET EXPLORER.**

Сохранение конфиденциальности личной информации вашего ребёнка при его работе в интернете является важным механизмом безопасности.

Для того чтобы повысить уровень конфиденциальности при общении вашего ребёнка в интернете, выполните следующие действия:

v нажмите кнопку *Пуск/Start,* в открывшемся меню выберите *Панель управления/Control* *Panel;*

v в панели управления откройте *Свойства обозревателя/Internet* *Options;*

v в появившемся окне перейдите на вкладку *Конфиденциальность/Privacy*;

v при помощи ползунка выберите необходимый уровень конфиденциальности.

**КОНТРОЛИРУЙТЕ ТО, ЧТО ДЕЛАЮТ В ИНТЕРНЕТЕ ВАШИ ДЕТИ.**

Невозможно всегда находиться рядом с детьми, когда они путешествуют по интернету. Однако есть возможность проверить, на каких сайтах они проводят время.

Когда вы премещаетесь по интернету, браузер (например, Internet Explorer или Netscape Navigator) собирает всю информацию о посещённых местах и сохраняет её на компьютере. Современные браузеры обычно ведут журнал последних посещенных сайтов.

Проверить, чем ребёнок занимался в интернете, можно следующим образом:

v запустите *Internet* *Explorer®;*

v в его меню выберите раздел *Вид/View*, в нем раздел *Панели обозревателя/Explorer* *Bar.*

v в этом разделе выберите команду *Журнал/History*.

v в окне *Internet* *Explorer* появится журнал, в котором вы сможете увидеть список всех посещённых ребёнком страниц.

Помните о том, что дети без труда могут отключить или изменить указанные функции контроля. В вопросах технологии они, скорее всего, всегда будут на шаг впереди вас.

Мы должны понимать, что открытый и доброжелательный диалог с детьми гораздо конструктивнее, чем тайная слежка за ними. Хотя негласный, но ненавязчивый контроль часто делает своё доброе дело по своевременному обнаружению признаков нарушения безопасности вашего ребенка.

**БЛОКИРУЙТЕ ВОЗМОЖНОСТЬ НЕИЗВЕСТНЫХ КОНТАКТОВ**

**В ПРОГРАММАХ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ**

Чаты и система обмена мгновенными сообщениями предоставляют детям замечательные возможности для обсуждения интересующих их тем и установление дружеских контактов. Однако анонимность интернета может представлять серьёзную опасность: ваш ребёнок рискует стать жертвой обманщиков и преступников.

Для предотвращения попыток контакта с вашими детьми со стороны незнакомых людей во время обмена мгновенными сообщениями настройте программу так, чтобы были доступны только проверенные контакты.

Для того, чтобы блокировать возможность неизвестных контактов в MSN Messenger®, нужно проделать следующее:

v в главном окне программы в меню Сервис/Tools выберите пункт *Параметры/Options;*

v на панели слева перейти на вкладку *Конфиденциальность/Privacy*;

v установите флажок *Видеть моё состояние и отправлять мне сообщение могут только люди, внесённые в белый список/Only* *people* *on* *my* *Allow* *list* *can* *see* *my* *status* *and* *send* *me* *messages.*

**СОЗДАЙТЕ НАДЁЖНЫЕ ПАРОЛИ.**

Пароли – это ключи, которыми можно разблокировать компьютер и учетные записи в интернете. Чем надёжнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета кредитных карт, обратиться за ипотекой или даже общаться через интернет от вашего имени. Вы можете не подозревать о таких действиях до тех пор, пока не станет слишком поздно. Создавать надежные пароли несложно. Для укрепления безопасности компьютера достаточно приложить незначительные усилия, с которыми можно познакомиться на сайте Microsoft по адресу <http://www.microsoft.com/rus/athome/security/privacy/password.mspx>.

**ПРАВИЛА ИНТЕРНЕТ-ЭТИКЕТА**

Путешествие по Сети может быть и развлечением, и полезным занятием, и способом общения как для взрослых, так и для детей. Однако важно, чтобы все новые пользователи интернета, которых также называют Netizens, помнили о том, что они в интернете не одни, как и в реальной жизни, в Сети существуют правила поведения, или этикет, который необходимо соблюдать. Если вашим детям не удастся освоить правила существования в интернет, это будут не просто упущенные возможности: если они скажут неправильные слова в неправильный момент, то могут вызвать агрессию или спровоцировать возникновение других проблем.

Поэтому до того, как новый юный пользователь возьмёт в руки мышь, мы предлагаем ему изучить следующие рекомендации:

v *Помните золотое правило: обращайтесь с другими так, как вы хотели бы, чтобы обращались с вами;*

v *Помните о том, что ваше сообщение получает живой человек;*

v *Не забывайте о том, где вы находитесь, и ведите себя подобающим образом;*

v *Прощайте ошибки другим людям, в особенности новичкам;*

v *Всегда сохраняйте спокойствие, особенно если кто-нибудь вас обижает (или вы думаете, что вас обидели);*

v *Избегайте написания текста ТОЛЬКО ЗАГЛАВНЫМИ БУКВАМИ с целью усиления его значения – некоторые пользователи видят в этом способ выражения крика;*

v *Не используйте неподходящую или оскорбительную лексику;*

v *Пользуйтесь постоянным онлайновым именем или псевдонимом и подписывайте им все сообщения (и наоборот, чтобы защитить свои личные данные, никогда не пользуйтесь своим полным именем);*

v *Никогда не отправляйте и не пересылайте нежелательные электронные письма (обычно их называют спамом);*

v *Держитесь в стороне от затяжных, эмоциональных споров («флейма»);*

v *Проверяйте правильность написанного, четко и коротко формулируйте свои сообщения;*

v *Во время общения в чатах не прерывайте других и не уходите от темы;*

v *Придерживайтесь тех же правил хорошего тона, которым вы следовали бы в реальной жизни.*