

Информационный курс для родителей

«Управление безопасностью детей в Интернете»

План

1. Введение
2. Советы по созданию безопасного Интернета
3. Повышение уровня безопасности детей в Интернете при помощи технических средств

1. Введение

Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям работать в Интернете самостоятельно, им следует уяснить некоторые моменты.

Дети должны знать об опасностях, существующих в Интернете, должны уметь правильно выходить из неприятных ситуаций. Дома должны быть установлены определенные ограничения на использование Интернета, о которых дети должны знать.

2. Советы по созданию безопасного Интернета

Сделать посещение Интернета для детей полностью безопасным можно при выполнении следующих положений.

- Дома установлены определённые правила работы в Интернете для детей. Родители непреклонны в требованиях их выполнения.
- Дети научены предпринимать следующие меры предосторожности по сохранению конфиденциальности личной информации:
 - представляясь, следует использовать только имя или псевдоним;
 - никогда нельзя сообщать номер телефона или адрес проживания или учебы;
 - никогда не посылать свои фотографии;

- никогда не встречаться со знакомыми по Интернету без контроля со стороны взрослых.

- Дети должны понимать, что разница между правильным и неправильным одинакова как в Интернете, так и в реальной жизни.

- Если их в Интернете что-либо беспокоит детей, то им следует сообщить об этом родителям.

- Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, родители должны помочь ребенку его выбрать и убедиться, что оно не содержит никакой личной информации.

- Дети должны уважать других в Интернете, знать о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

- Дети должны уважать собственность других в Интернете: незаконное копирование чужой работы - музыки, компьютерных игр и других программ - является кражей.

- Детям никогда не следует встречаться с друзьями из Интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают.

- Дети должны понимать, что не все, что они читают или видят в Интернете, - правда. Необходимо спрашивать родителей, если дети в чём - то не уверены.

- Родители должны контролировать деятельность детей в Интернете с помощью современных программ, которые помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

- Родители должны поощрять детей делиться с ними опытом работы в Интернете, посещать Сеть вместе с детьми, регулярно посещать Интернет-дневник своего ребенка, если он его ведет, для проверки.

- ***Родители должны быть внимательны к своим детям!***

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

Интернет предоставляет детям доступ к играм и фильмам, а также бесконечные возможности для получения новых знаний и развития исследовательских навыков. Но эти преимущества сопровождаются и рядом сложных проблем. Однако можно предпринять некоторые шаги, которые помогут защитить детей от опасностей в Интернете. Не следует забывать при этом, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются ваши дети за компьютером.

1. Родителям необходимо повысить уровень общей безопасности 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 трех наиболее важных компонентов.

Для того чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующее:

- *нажать* кнопку *Пуск/Start*, в открывшемся меню выбрать *Панель управления/Control Panel*;
- в панели управления открыть *Центр обеспечения безопасности/Security Center*;
- убедиться, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).

Включить или отключить брандмауэр и автоматическое обновление можно непосредственно в *Центре обеспечения безопасности*. Для управления защитой от вирусов необходимо обратиться к настройкам установленного антивирусного программного обеспечения.

2. Родителям необходимо блокировать доступ к неподходящим материалам.

Один из наилучших способов защиты от нежелательной информации - это блокирование доступа еще 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:

- нажать кнопку *Пуск/Start*, в открывшемся меню выбрать *Панель управления/ Control Panel*;
- в панели управления открыть *Свойства обозревателя/Internet Options*;
- в появившемся окне перейти на вкладку *Содержание/Content*;
- в разделе *Ограничение доступа/Content Advisor* нажать кнопку *Включить/Enable*;
- в появившемся окне ввести пароль, который будет защищать вводимые родителями ограничения от изменения детьми;
- в окне *Ограничение доступа/Content Advisor* можно блокировать доступ к нежелательной информации.

3. Родителям целесообразно повысить уровень безопасности при работе ребенка с электронной почтой outlook® express.

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

При помощи переключателя *выберите зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use* можно уменьшить вероятность появления вирусов на 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 в компьютер, ограничить его дальнейшее распространение можно, 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 *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.*

4. Заблокируйте поступление спама.

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

Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере hotmail.com, необходимо зайти в этот почтовый ящик и перейти по ссылке Options и в вертикальном меню выбрать вкладку Mail.

Перейдя по ссылке *Junk E-mail Filter*, можно изменить настройки фильтра нежелательной почты.

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

В случае, если почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.

Для настройки этого фильтра в меню Microsoft Outlook выбрать *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 можно внести изменения в настройки фильтра нежелательной почты.

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

5. Создайте отдельные учетные 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, дающую 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 ребенка с ограниченными правами доступа для работы в Интернете, необходимо выполнить следующие действия:

- нажать кнопку *Пуск/Start*, в открывшемся меню выбрать *Панель управления/Control Panel*;
- в панели управления открыть *Учетные записи пользователей/User Accounts*;
- в открывшемся окне выбрать *Создание учетной записи/Create a new account*, ввести ее имя;
- на этапе выбора типа учетной записи установить переключатель в положение *Ограниченная запись/Limited*;
- после нажатия кнопки *Создать учетную запись/ Create Account* процесс создания учетной записи с ограниченными правами будет завершен и ребенок сможет выбрать ее при следующем входе в систему.

6. Родители могут повысить уровень конфиденциальности при общении ребенка в Интернете с помощью Internet Explorer.

Сохранение конфиденциальности личной информации ребенка при его работе в Интернете является важным механизмом безопасности.

Для того чтобы повысить уровень конфиденциальности при общении ребенка в Интернете, родителям необходимо выполнить следующие действия:

- нажать кнопку *Пуск/Start*, в открывшемся меню выбрать *Панель управления/Control Panel*;
- в панели управления открыть *Свойства обозревателя/Internet Options*;
- в появившемся окне перейти на вкладку *Конфиденциальность/Privacy*;
- при помощи ползунка выбрать необходимый уровень конфиденциальности.

7. Родители должны контролировать то, что делают в Интернете дети.

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

Когда человек перемещается по Интернету, браузер (например, Internet Explorer или Netscape Navigator) собирает всю информацию о посещенных местах и сохраняет ее на компьютере. Современные браузеры обычно ведут журнал последних посещенных сайтов.

Проверить, чем ребенок занимался в Интернете, можно следующим образом:

- запустить *Internet Explorer®*;
- в его меню выбрать раздел *Вид/View*, в нем - раздел *Панели обозревателя/Explorer Bar*. В этом разделе выбрать команду *Журнал/History*.

В окне Internet Explorer появится журнал, в котором можно увидеть список всех посещенных ребенком страниц.

8. Родителям необходимо помнить о том, что дети без труда могут отключать или изменять указанные функции контроля. В вопросах технологии они, скорее всего, всегда будут на шаг впереди родителей.

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

9. Родителям следует блокировать возможность неизвестных контактов в программах обмена мгновенными сообщениями.

Чаты и система обмена мгновенными сообщениями предоставляют детям замечательные возможности для обсуждения интересующих их тем и установления дружеских контактов. Однако анонимность Интернета может представлять серьезную опасность; ваш ребенок 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:

- в главном окне программы в меню *Сервис/ Tools* выбрать пункт *Параметры/Options*;
- на панели слева перейти на вкладку *Конфиденциальность/Privacy*;
- установить флажок *«Видеть мое состояние и отправлять мне сообщения могут только люди, внесенные в белый список/Only people on my Allow list can see my status and send me messages»*.

10. Необходимо создавать надежные пароли.

Пароли - это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться личными данными человека в корыстных целях, например, открыть новые счета

кредитных карт, обратиться за ипотекой или даже общаться через Интернет от его имени. Человек может 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.msp>

Список использованной литературы

- 1.Безопасность детей в Интернете. М: Корпорация Microsoft, 2006. – 36 с.