Безопасность детей в интернете.

Интернет постепенно проникает в каждую организацию, общественное учреждение, учебное заведение, в наши дома. Число пользователей Интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины очень велика. Для многих, особенно молодых людей, он становится информационной средой, без которой они не представляют себе жизнь. Для защиты детей от опасностей в Интернете необходима активная позиция родителей и это не удивительно: ведь в Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах.

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появилась своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

Защита детей в Интернете: что могут сделать взрослые?

Объясните детям и установите четкие правила – какие сайты они не должны посещать.

Помогите детям выбрать правильное регистрационное имя и пароль, если это необходимо для общения детей посредством программ мгновенного обмена сообщениями или сетевых игр. Убедитесь в том, что они не содержат никакой личной информации.

Объясните вашим детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

Объясните детям, что люди в Интернете не всегда являются теми, за кого они себя выдают.

Не позволяйте детям встречаться лично с их «знакомыми» по Интернету без вашего наблюдения. Научите детей уважать других в Интернете.

Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Настаивайте, чтобы дети уважали собственность других в Интернете.

Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости.

Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и с какой целью. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь.

Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет дневник, регулярно посещайте его.

Будьте внимательны к вашим детям!

**Возрастные особенности детей и Интернет**

Ребенок проходит в своем психологическом развитии определенные стадии, которые достаточно сильно отличаются друг от друга. Это также отражается и на интересах детей при пользовании Интернетом. Родителям важно понимать особенности формирования их характера и интересы в том или ином возрасте, для того чтобы правильно расставлять акценты внимания при своих беседах с детьми о правилах безопасности в Интернете.

**Повышение уровня безопасности детей в Интернете при помощи программных средств**

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. Пожалуйста, примите необходимые меры, чтобы защитить ваших детей при помощи программных средств. Но помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам (например, с помощью Internet Explorer®)

Увеличьте уровень защиты и конфиденциальности: используя возможности Microsoft® Windows, создайте отдельные учетные записи для разных пользователей настройте параметры безопасности Internet Explorer®

Следите за тем, какие сайты посещают ваши дети (например, с помощью Internet Explorer®) Напоминайте детям, чтобы они не общались в Интернете с незнакомцами. Помогите им оградить себя от неизвестных контактов (например, с помощью Microsoft Windows Messenger)

**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®7, 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 7, нужно проделать следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel; - и выбрать пункт Безопасность и Центр обеспечения безопасности;

- 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.

**УСТАНОВИТЕ 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 Remo-al 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:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel; - в панели управления откройте Свойства обозревателя/Internet Options;

- в появившемся окне перейдите на вкладку Содержание/Content; - в разделе Ограничение доступа/Content Ad-isor нажмите кнопку Включить/Enable;

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

- в окне Ограничение доступа/ Content Ad-isor 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 разделеСервис/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 sa-ed or opened that could potentially be a -irus.

Если же вирус все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочкуПредупреждать, 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 outgoingmessages 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 командуПараметры/Options. В открывшемся диалоговом окне перейдите на вкладку Настройки/Preferences и нажмите кнопку Нежелательная почта/JunkE-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 7 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:

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

- в панели управления откройте Учетные записи пользователей/User Accounts;

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

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

- 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:

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

- в панели управления откройте Свойства обозревателя/Internet Options;

- в появившемся окне перейдите на вкладку Конфиденциальность/Pri-acy;

- 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 Chrome) 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:

- запустите Internet Explorer®;

- в его меню выберите раздел Вид/-iew, в нем раздел Панели обозревателя/Explorer Bar.

- в этом разделе выберите команду Журнал/History.

- 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:

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

- на панели слева перейти на вкладку Конфиденциальность/Pri-acy;

- установите флажок Видеть моё состояние и отправлять мне сообщение могут только люди, внесённые в белый список/Only peopleon 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 адресуhttp://www.microsoft.com/rus/athome/security/pri-acy/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:

- Помните золотое правило: обращайтесь с другими так, как вы хотели бы, чтобы обращались с вами; - Помните о том, что ваше сообщение получает живой человек;

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

- Прощайте ошибки другим людям, в особенности новичкам;

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

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

- Не используйте неподходящую или оскорбительную лексику;

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

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

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

- Проверяйте правильность написанного, четко и коротко формулируйте свои сообщения;

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

- Придерживайтесь тех же правил хорошего тона, которым вы следовали бы в реальной жизни. **Обеспечение безопасности детей при работе в Интернет**.

**«БЕЗОПАСНЫЙ ИНТЕРНЕТ» - РЕКОМЕНДАЦИИ РОДИТЕЛЯМ**

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет – это не только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них – дети, которые могут не знать об опасностях мировой паутины. Мы хотим сделать Интернет максимально безопасным для подрастающих поколений. Эта цель осуществима, если государство, представители бизнеса, правоохранительные органы и общественность объединят усилия, а родители осознают свое главенство в обеспечении безопасности детей. Данные рекомендации – практическая информация для родителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

**Правило 1**. **Внимательно относитесь к действиям ваших детей в «мировой паутине»:**

• Не отправляйте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка с Интернетом, особенно на этапе освоения.

• Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернета, рассказывайте, как вовремя предупредить угрозы.

**Правило 2**. **Информируйте ребенка о возможностях и опасностях, которые несет в себе сеть**:

• Объясните ребенку, что в Интернете как в жизни встречаются и «хорошие», и «плохие» люди. Объясните, что если ребенок столкнулся с негативом или насилием со стороны другого пользователя Интернета, ему нужно сообщить об этом близким людям.

• Объясните ребенку, что размещать свои личные данные (адрес, телефон, место учебы) в социальных сетях и других открытых источниках нежелательно и даже опасно.

• Научите ребенка искать нужную ему информацию и проверять ее, в том числе с вашей помощью.

• Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернета, особенно путём отправки sms, – во избежание потери денег.

• Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться ваш ребенок, и посоветуйте их использовать.

• Объясните, что нежелательно переходить по ссылкам в Интернете. Доказано, что за шесть кликов можно перейти от «белого» сайта к «чёрному».

• Научите ребенка самостоятельно вносить адрес в адресную строку браузера. Это позволит избежать сайтов-клонов.

**Правило 3. Выберите удобную форму контроля пребывания вашего ребенка в Сети**:

• Установите на ваш компьютер необходимое программное обеспечение – решение родительского контроля, антивирус Касперского или Doctor Web.

• Простые настройки компьютера позволят вам быть в курсе того, какую информацию просматривал ваш ребенок. Регулярно отслеживайте ресурсы, которые посещает ребенок.

• Пользуйтесь программами семейной безопасности, которые позволяют полностью перекрыть доступ в Интернет или установить веб-фильтры, а также проверить, на какие сайты заходит ребенок, какие программы использует, сколько времени проводит в сети.

• Если ваш ребенок – учащийся младших классов и часто остается дома один, ограничьте ему время пребывания в Интернете.

• Если компьютер используется всеми членами семьи, установите его в месте, доступном для всех членов семьи, а не в комнате ребенка.

• Создавайте разные учетные записи на вашем компьютере для взрослых и детей. Это поможет не только обезопасить ребенка, но и сохранить ваши личные данные.

**Правило 4. Регулярно повышайте уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей:**

• Используйте удобные возможности повышения уровня компьютерной и Интернет-грамотности, например, посещение курсов, чтение специальной литературы, консультации с экспертами.

• Знакомьте всех членов вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете.

• Учитесь у ребенка! Дети XXI века нередко продвинутее родителей в вопросах компьютера и Интернета. В форме игры попросите ребенка показать свои возможности и научить вас незнакомым действиям.

**Правило 5. Будьте внимательны к поведению ребенка, отслеживайте признаки Интернет-зависимости:**

• Уясните, вредные привычки влияют на здоровье, а Интернет-зависимость наносит вред психике человека. По мнению врачей и психологов, зависимость от Интернета является «удобным» типом зависимости для родителей, так как носит неявный характер по сравнению с другими серьезными проблемами, к примеру, алкоголем и наркотиками.

• Будьте внимательны к переменам в поведении ребенка Раздражительность, рассеянность, замкнутость, потеря интереса к любимым занятиям, ложь о количестве времени, которое ребенок проводит в сети, частое употребление пищи перед компьютером – все это может быть признаками зависимости от Интернета.

• Придумайте полезную альтернативу Интернету. Это может быть увлекательное занятие, активный отдых, посещение спортивных секций и кружков, обычная прогулка с друзьями или родителями.

• Старайтесь распознать зависимость как можно раньше и при необходимости обратиться к специалисту. Правило 6. Руководствуйтесь рекомендациями педиатров:

• До 7 лет врачи не рекомендуют допускать детей к компьютеру/Интернету. 7-10 лет — время за компьютером рекомендовано ограничить 30 мин. в день. 10-12 лет — до 1 часа за компьютером. старше 12 лет – не более 1,5 часов с обязательными перерывами.

• Помните, что злоупотребление компьютером рискованно для физического здоровья и может вызвать у ребенка ухудшение зрения, гиподинамию, подверженность аллергиям и даже сердечно сосудистые заболевания.

**Полезные для ознакомления ресурсы**

<http://www.microsoft.com/eesti/haridus/-eebi-end/koomiksid/rus/html/etusi-u.htm>

http://www.wiki.-ladimir.i-edu.ru/index.php?title=%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D1%8B%D0%B9\_%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82\_%D0%B4%D0%BB%D1%8F\_%D0%B4%D0%B5%D1%82%D0%B5%D0%B9 Способы фильтрации

<http://www.ligainternet.ru/filtruyushchii-soft>

http://www.icensor.ru/ ТИПОВОЙ РЕГЛАМЕНТ по работе учителей и школьников в сети Интернет

http://gym1517sz.mskobr.ru/conditions/security/bezopasnost\_-\_internete/