

## **Информация по обеспечению информационной безопасности в сети Интернет**

Работа по обеспечению информационной безопасности детей в Чувашской Республике проводится в соответствии с Федеральными законами от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Законом Чувашской Республики от 24 июля 2009 г. № 43 «О некоторых мерах по защите детей от факторов, негативно влияющих на их физическое, интеллектуальное, психическое, духовное и нравственное развитие» и др.

В целях защиты детей от негативной информации в сети «Интернет» во всех 455 общеобразовательных организациях Чувашской Республики установлено программное обеспечение для исключения доступа учащихся к интернет-ресурсам, несовместимых с задачами образования и воспитания (интернет Цензор – 86,6%, NetPolice – 2,8%, другие – 10,6%), ведутся журналы учета выхода учителей и учащихся в сеть «Интернет», определены ответственные за реализацию единой политики по доступу в данную сеть, в должностные инструкции которых внесены соответствующие дополнения. С ответственными работниками проведены курсы повышения квалификации, семинары-совещания, в образовательные организации направлены методические рекомендации по организации контент-фильтрации.

Образовательными организациями ведется системная работа по защите детей от негативной информации, находящейся в сети «Интернет», обеспечению информационной безопасности обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде посредством проведения различных профилактических мероприятий.

Так, например, в образовательных организациях регулярно проводится месячник «Безопасный интернет», в рамках которого проводятся различные мероприятия: традиционные (классные часы, беседы, родительские собрания), интерактивные (выставки, просмотр видеороликов, презентаций и проектов), инновационные (уроки-практикумы, тематические интерактивные выставки, опросы с обсуждением).

С педагогическими работниками, ответственными за воспитательную работу, проводятся круглые столы и совещания по темам: «Защита детей от негативных аспектов работы в сети «Интернет», «Защитим наших детей в сети «Интернет», обсуждения Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Закона Чувашской Республики от 27 июля 2009 г. № 43 «О некоторых мерах по защите детей от факторов, негативно влияющих на их физическое, интеллектуальное, психическое, духовное и нравственное развитие» и др.

Кроме того, если педагог, родитель или сам ребенок считает, что увлеченность компьютером чрезмерна, что наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то с этой проблемой можно обратиться к специалистам-психологам по общероссийскому «Телефону доверия» (8-800-2000-122) . Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Звонки принимаются круглосуточно.

В республике ведется работа по вовлечению студентов и учащейся молодежи в федеральный молодежный проект «Медиа Гвардия», целью которого является выявление в сети «Интернет» сайтов, сообществ и групп в социальных сетях, специализирующихся на распространении противоправного контента. Участниками данного проекта являются 46 человек.

В настоящее время представители проекта «МедиаГвардия» сотрудничают с Федеральной службой по надзору в сфере связи, информационных технологий и массовых

коммуникаций по выявлению сайтов, сообществ и групп в социальных сетях, пропагандирующих распространение психоактивных веществ, детскую порнографию, призывающих к суицидальному поведению.

Вся собранная информация передается в профильные ведомства для принятия решений по блокированию работы таких источников. По итогам 2016 г. на территории республики выявлено 29 запрещенных страниц.

В целях освещения вопросов безопасности детей в Интернете в печатных СМИ Чувашии созданы рубрики: «Медиабезопасность», «Дети и Интернет», «Важно знать», «Берег детства», «Интернет и его безопасность». Размещаются правила по безопасной работе в сети для детей и родителей, анонсы и релизы тематических мероприятий. Широкое освещение в региональной прессе в этом году получил Единый урок по безопасности в сети Интернет, который третий год подряд проводился в российских школах.

На сайте Мининформполитики Чувашии размещен баннер «Защита детей от негативной информации», где можно ознакомиться с действующей нормативно-правовой базой, рекомендациями для детей и родителей по организации безопасного интернет-пользования, электронными адресами организаций и телефонами «горячих линий» для сообщений о противоправном контенте.

На Национальном телевидении Чувашии вопросы информационной безопасности детства поднимаются в телевизионной передаче об информационных технологиях «IT не обойти» и детском информационном выпуске новостей «Акилбупсер», на «Таван радио» – в познавательной программе для детей и взрослых «Азбука детской безопасности».

В региональном эфире телеканалов «Россия-1» и «Россия-24», а также на «Радио Чувашии» транслируется ролик «Интернет – территория повышенной опасности».

СМИ прикладывают максимальные усилия, чтобы привлечь внимание общественности к данной проблеме и повысить осведомленность школьников нашей республики и их родителей в вопросах безопасного пользования Интернетом, научить подрастающее поколение критически оценивать информацию в сети.

*Выдержки из Рекомендаций к проведению Урока по безопасности в сети Интернет, разработанный Минобрнауки России и Минкомсвязи России, ФГБУ «Российская академия образования» (РАО), ФГНУ «Институт информатизации образования» РАО и ФГАОУ ДПО «Академия повышения квалификации и профессиональной переподготовки работников образования»*

### **Предотвращение возможных негативных последствий использования Интернета**

Рассматривая возможности Интернета, уникальные с точки зрения образовательных применений, следует выделить его положительное влияние, которое обусловлено прямым воздействием на обучающегося в целях формирования позитивной траектории его социализации, обучения решению жизненно важных проблем, предоставления выбора «виртуального» социального окружения («виртуальных» сообществ) и пр.

Существующие риски негативного влияния Интернета обусловлены: нарушением правил и режимов использования с прямым и опосредованным воздействием на состояние физического и психического здоровья пользователя (например, прямое влияние на зрение и опосредованное – на формирование психологической Интернет-зависимости). Опосредованное влияние может также проявляться в нарушении осанки, в малоподвижном образе жизни, в замкнутости поведения личности.

Вообще в настоящее время использование Интернета порождает гораздо больше проблем, нежели радужных перспектив. Проблемы эти связаны, прежде всего, с изменением структуры и психологической составляющей устоявшегося веками информационного взаимодействия между обучающим и обучающимся. В условиях использования Интернета в образовательных целях оно строится не на абсолютизировании авторитета обучающего, а, скорее всего, на партнерских отношениях, которые в состоянии установить учитель со своими подопечными. Помимо этого, существуют еще более значительные трудности, связанные с возможными негативными последствиями психологического и медицинского характера. Последние связаны с вольным или невольным нарушением или пренебрежением пользователем режимами работы, которые необходимо соблюдать в процессе применения Интернета.

Не менее опасны возможные **негативные последствия психолого-педагогического воздействия**, оказываемого на ученика информационно емким и эмоционально насыщенным контентом различных сайтов Интернета. Опасность связана с: использованием недопустимого объема учебной информации, представленной на экране; несоответствием представляемой на экране информации (по структуре, качеству) возрастным и (или) индивидуальным возможностям обучающегося; необеспеченностью позитивным «психологическим климатом» информационного взаимодействия с объектами виртуальных экранных миров, которыми изобилует Интернет.

При этом особое внимание следует обратить на то, что информационная перегрузка при длительном использовании Интернета и, связанное с этим эмоциональное возбуждение, обманчивое повышение работоспособности непосредственно за экраном компьютера, опасны как для психического, так и физического здоровья молодого человека.

Решение проблем, связанных с **медицинскими вопросами**, осуществляется путем соблюдения ряда мер физиолого-гигиенического характера, описанных в специальных нормативно-методических документах, утвержденных соответствующими Государственными инстанциями.

Более сложными и трудноразрешимыми, по мнению современных психологов, педагогов и медиков, являются **возможные негативные последствия, связанные с активным вторжением в естественный внутренний мир современного человека неестественных, иллюзорных виртуальных впечатлений от виртуальных сюжетов и взаимодействий при «вхождении» в Интернет**. Вполне понятная и объяснимая психологией личности человека увлеченность яркими и необычными, порой

призрачными, впечатлениями, отличными от реальных, чревата многими опасностями для несформировавшейся психики обучающегося. К ним следует отнести, прежде всего, усиливающееся взаимодействие между современными молодыми людьми, обусловленное возможностью легкой «замены партнера» на киберпартнера и облегченной «коммуникацией без проблем». Вызывает не меньшее беспокойство опасность преднамеренного манипулирования сознанием молодого человека, выполняющего определенные действия и участвующего в реализации различных сюжетов, представляемых на сайтах Интернета.

Следует обратить особое внимание на *философские аспекты реализации информационного взаимодействия в Интернете*, при котором мир и коммуникации, сгенерированные современными технологиями, могут стать настолько реальными, что пользователь может в конце концов совсем оторваться от реального мира и перейти в «киберпространство».

*Для безопасного и педагогически целесообразного использования Интернета* основным принципом должно являться неукоснительное выполнение предложенных специалистами – медиками, психологами, физиологами и гигиенистами – требований по режимам работы, при педагогически целесообразном использовании информационного ресурса Интернет и осуществлении информационного взаимодействия как между обучающим и обучающимися, так и между ними и интерактивным контентом Интернета.

Наконец, не менее важной является *защита детей и подростков от негативного влияния вредоносного медиаконтента*, не только имеющегося в интернет-среде, но и в большом количестве представленного в современных СМИ, рекламных и иных материалах, с которыми дети сталкиваются повседневно. С целью защиты детей и подростков от такого рода вредоносной информации Распоряжением Правительства Российской Федерации от 2 декабря 2017 г. № 2471-р принята *Концепция информационной безопасности детей* (<http://government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf>).

Концепцией определены основные принципы обеспечения информационной безопасности детей, приоритетные задачи и механизмы реализации государственной политики в этой области, ожидаемые результаты.

Положения Концепции базируются на принципах признания детей и подростков активными участниками информационного процесса, ответственности государства за соблюдение законных интересов детей в информационной сфере, воспитания у детей навыков самостоятельного и критического мышления, создания в информационной среде благоприятной атмосферы для детей и подростков вне зависимости от их социального положения, религиозной и этнической принадлежности.

К приоритетным задачам государственной политики в области информационной безопасности детей в том числе относятся повышение уровня медиаграмотности детей и подростков, формирование у них чувства ответственности за свои действия в информационном пространстве, удовлетворение познавательных потребностей и интересов, минимизация рисков десоциализации, развития и закрепления девиантных и противоправных действий подростков.

Результатом реализации Концепции должно стать формирование к 2020 году поколения молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном пространстве. Планируется, что будет создана медиасреда с такими основными характеристиками, как свободный доступ детей к историко-культурному наследию, увеличение числа детей и подростков, разделяющих ценности патриотизма, популяризация здорового образа жизни, формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву.

## **Рекомендации родителям** **«Основные правила защиты наших детей от Интернет опасностей»**

Интернет постепенно проникает в каждую организацию, общественное и учебное учреждение, в наши дома. Число пользователей Интернета в России стремительно растет и молодеет, доля молодежи и совсем юной аудитории среди пользователей Всемирной сети очень велика. Для многих из них, он становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, в Интернете содержатся огромные массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию.

Согласно ст. 5 Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», к информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера.

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. И, это не удивительно: ведь в Интернете можно найти информацию для реферата или доклада, послушать любимую мелодию, проверить свои знания в интернет конкурсах или on-line тестированиях, 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.

**Правило 1.** Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – посещать нельзя. Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

**Правило 2.** Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

**Правило 3.** Объясните 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.

**Правило 4.** Не позволяйте ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с

новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

**Предупреждение груминга:** Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии. Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствие взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу; Интересуйтесь тем, куда и с кем ходит ваш ребенок.

**Кибербуллинг** — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов. **Предупреждение кибербуллинга:** Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать. Научите детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

***На что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:***

1) Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

2) Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

3) Нервозность при получении новых сообщений. Негативная реакция ребенка на звук электронного письма должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

**Правило 5.** Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

**Правило 6.** 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.

**Правило 7.** Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости. Предвестниками «интернет-зависимости» (синонимы: интернет-аддикция,

виртуальная зависимость) и зависимости от компьютерных игр («геймерство») являются: навязчивое стремление постоянно проверять электронную почту; предвкушение следующего сеанса онлайн; увеличение времени, проводимого онлайн; увеличение количества денег, расходуемых онлайн. Если Вы считаете, что ваши дети, страдают от чрезмерной увлеченности компьютером, что наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь\*.

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! Помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером

### ***Какие угрозы встречаются наиболее часто?***

Прежде всего:

- Угроза заражения вредоносным программным обеспечением (далее – ПО). Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, ПО для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

- Доступ к нежелательному содержимому. 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 Интернет 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;

- Неконтролируемые покупки. Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Именно обеспечению безопасности наших детей при пребывании в сети Интернет и будет посвящена наша статья. Интернет это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что как и наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна.

Приведем несколько рекомендаций, с помощью которых посещение Интернет может стать менее опасным для ваших детей:

1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;

2. Объясните детям, что если в Интернет 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.), использовании он-лайн 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 Интернет нет разницы между неправильными и правильными поступками;

6. Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;

7. Скажите им, что никогда не стоит встречаться с друзьями из Интернет. 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 – правда. Приучите их спрашивать о том, в чем они не уверены;

9. Не забывайте контролировать детей в Интернет 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 от лжи в Интернет?

Следует объяснить детям, что нужно критически относиться к полученным из Интернет материалам, ведь опубликовать информацию в Интернет может абсолютно любой человек. Объясните ребенку, что сегодня практически каждый человек может создать свой сайт и при этом никто не будет контролировать, насколько правдива размещенная там информация. Научите ребенка проверять все то, что он видит в Интернет. Как это объяснить ребенку?

- 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 от лжи;

- Не забывайте спрашивать ребенка об увиденном в сети Интернет. Например, начните с расспросов, для чего служит тот или иной сайт.

- Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в Интернет 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 Интернет. Покажите, как использовать различные поисковые машины для осуществления поиска;

- Объясните вашим детям, что такое расизм, фашизм, межнациональная ирелигиозная 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 Интернет. Если ваши дети хотят посещать Интернет, вам следует выработать вместе с нимисоглашение по использованию Интернет. 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 Интернет;

- Что делать, если ваших детей что-то беспокоит при посещении Интернет;

- 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 разговаривайте в Интернет 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 систему 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? Установите правила использования домашнего компьютера и постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка. Кроме того, добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых. Обратите внимание на себя, не слишком ли много времени вы проводите в Интернет.

## Советы по безопасности для детей разного возраста

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

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

### Возраст 5-6 лет

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов.

Как им помочь делать это безопасно?

- В таком возрасте желательно работать в Интернет только в присутствии родителей;
- Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира;
- Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети;
- Используйте специальные детские поисковые машины, типа MSN KidsSearch (<http://search.msn.com/kids/default.aspx?FORM=YCHM>);
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
- Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Ваши дети растут, а, следовательно, меняются их интересы.

### 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 Интернет 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 `c:\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 Интернет. 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 Интернет 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; 120
- Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее;
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;
- Используйте специальные детские поисковые машины, типа MSN KidsSearch (<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 позволить 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;
- Научите 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 <http://www.microsoft.com/rus/athome/security/email/fightsпам.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 Интернет, как если бы речь шла о друзьях в реальной жизни;
- Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. 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 9-12 лет

В данном возрасте дети, как правило, уже слышаны о том, какая информация существует в Интернет. 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 Интернет 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 в Интернет 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 Интернет;

- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет;
- 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 Интернет;
- 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 Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;
- Расскажите детям о порнографии в Интернет;
- 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 13-17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет 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 Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

*Советы по безопасности в этом возрасте:*

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте 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 Интернет.

Что посоветовать в этом возрасте?

- Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах);
- Компьютер с подключением к Интернет должен находиться в общей комнате. Часы работы в Интернет могут быть легко настроены при помощи средств Родительского контроля KasperskyInternetSecurity 7.0.
- Не забывайте беседовать с детьми об их друзьях в Интернет, 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 моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

- Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет.

- 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 Интернет.

- 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 Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

- Расскажите детям о порнографии в Интернет.

- Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального 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 по закону дети не могут играть в эти игры. Обеспечивать родительский контроль в Интернет можно с помощью различного программного обеспечения.

### «Опасные игры»

В социальных сетях стала популярна «детская» игра «Беги или умри». Ее суть в том, чтобы на спор или для видео перебежать дорогу перед транспортом, причем, как можно ближе к автомобилям. Так сказать, пробежаться по лезвию бритвы, оказавшись на самой грани жизни и смерти. Опасность дети явно не осознают.

Идти на игры со смертью, по словам психологов, в основном решаются дети от 9 до 14 лет. Это группа риска, к которой нужен особый подход. Зависимость от мнения сверстников, подростковая конкуренция могут подтолкнуть ребенка и не на такое. Они также считают, что новая смертельная забава компенсирует детям недостаток «острых» ощущений.

Неравнодушные родители сразу стали размещать информацию о предостережении: «Внимание родители и водители! Сейчас среди детей очень новомодной стала игра: «Беги или умри!». Эта игра уже популярна по всей России. Поэтому и водителям нужно быть предельно внимательными, когда видите детей у дороги, учитывайте тот факт, что они могут броситься бежать прямо под колёса. Проведите беседу с детьми».

По сообщениям родителей в социальных сетях, дети, участвующие в этой игре ведут себя следующим образом:

1. Подросток не высыпается, даже если рано ложится спать. Проследите, спит ли он в ранние утренние часы.
2. Рисует китов, бабочек, единорогов.
3. Состоит в группах, содержащих в названии следующее: «Киты плывут вверх», «Разбуди меня в 4.20», «f57», «f58», «Тихийдом», «Рина», «Няпока», «Море китов», «50 дней до моего...» и др.
4. Закрыв в Контакте доступ к подробной информации, в переписке с друзьями (на личной стене) есть фразы «разбуди меня в 4.20», «я в игре». И совсем уж страшно, если на стене появляются цифры, начиная от 50 и меньше.
5. Переписывается в вайбере (и др. мессенджерах) с незнакомыми людьми, которые дают странные распоряжения.