Муниципальное автономное образовательное учреждение дополнительного образования
«Дворец детского (юношеского) творчества» муниципального образования
города Чебоксары – столицы Чувашской Республики

«Дети и Интернет:
как создать безопасный виртуальный мир»
(материалы обучающего семинара для родителей учащихся)

Чебоксары
2016

Авторы-составители:

Карпович И.Е. – заведующая информационно-методическим отделом Дворца творчества;

Семенов А.Г. – педагог-организатор Дворца творчества;

Долгова М.В. – педагог-психолог Дворца творчества;

Самарина О.П. – методист Дворца творчества.

В методическом сборнике представлены материалы, используемые для проведения цикла обучающих семинаров с родителями учащихся Дворца творчества, посвященных теме информационной безопасности детей в сети Интернет. Методическое издание может быть полезно родителям, педагогам-психологам, работникам сферы дополнительного образования.

СОДЕРЖАНИЕ

Предисловие

«Мы считаем, что каждый - от пользователя домашнего компьютера до крупной компании и правительства - должен иметь возможность защитить то, что дорого для него. Неважно, идет ли речь о частной жизни, семье, финансах, бизнесе или критической инфраструктуре…»

Евгений Касперский,
генеральный директор «Лаборатории Касперского»

«Сегодня можно с уверенностью говорить о том, что в образовательных организациях налажена работа по оперативному реагированию на появляющиеся угрозы. Зачастую дети сталкиваются с негативной информацией дома. А родители меньше самих детей владеют знаниями об информационных технологиях, соответственно не могут обезопасить и проконтролировать их. Считаю, что необходимо провести серьезную работу именно в этом направлении…»

Михаил Игнатьев,
Глава Чувашской Республики (из выступления на заседании Координационного совета при Главе Чувашской Республики по реализации Национальной стратегии действий в интересах детей на 2012-2017 годы, 25 сентября 2015г.)

В МАОУДО «Дворец детского (юношеского) творчества» муниципального образования города Чебоксары – столицы Чувашской Республики особое внимание уделяется работе с родителями учащихся, т.к. семья не только влияет на формирование личности ребенка, но и выступает в роли социального заказчика образовательных услуг, определяющего цель деятельности учреждения и педагогов. Взаимодействие с семьей позволяет у лучше узнать ребенка, определить совместные действия, объединить усилия по обучению, воспитанию и развитию ребенка, а значит, семья и учреждение дополнительного образования должны также быть партнерами. Мы разделяем мнение, согласно которому, чтобы вырастить полноценного человека, культурную, высоконравственную, творческую и социально зрелую личность, необходимо, чтобы педагоги и родители действовали как союзники, делились с детьми своей добротой, опытом, знаниями.

С целью активизации и обогащения воспитательных умений родителей, создания в результате сотрудничества с родителями учащихся атмосферы общности интересов, поиска новых путей привлечения семьи к участию в учебно-

воспитательном процессе учреждения, нами организуются обучающие семинары для родителей учащихся Дворца творчества.

Цикл семинаров был посвящен теме информационной безопасности детей.

Цель, которую мы ставили: обеспечение информационной безопасности несовершеннолетних обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде, информирование и обучение родителей учащихся способам защиты ребенка от угроз сети Интернет.

Основные задачи:

1) информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сети Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) обучение учащихся правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

4) профилактика формирования у учащихся Интернет-зависимости и игровой зависимости (игромании, гэмблинга);

5) предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий;

6) выявление уровня компетентности родителей по вопросам информационной безопасности;

7) создание условий для осмысления родителями собственной Интернет-культуры;

8) создание информационного пространства для родителей, где бы они могли ознакомиться с материалами по информационной безопасности детей, а также задать вопросы и получить компетентные ответы на них;

9) разработка алгоритма действий родителей в целях обеспечения информационной безопасности детей;

10) обучение родителей формам осуществления родительского контроля над поведением детей в сети Интернет с помощью программного обеспечения.

На наш взгляд, только комплексное решение указанной проблемы со стороны семьи и образовательного учреждения позволит значительно сократить риски причинения различного рода ущерба ребенку со стороны сети Интернет. Обеспечение информационной безопасности и воспитание информационной культуры должно стать приоритетным направлением работы современного образовательного учреждения.

Материалы семинара представлены в данном издании.

Коммуникация в сети Интернет

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей. С каждым годом количество людей, попавших в сети Всемирной паутины, неуклонно растет. Если еще десять лет назад во всем мире Интернетом пользовались лишь 182 млн. человек, то сегодня только в России насчитывается свыше 10 млн. пользователей Интернета, из которых несколько миллионов - дети.

По данным всероссийских опросов, около 90% детей и подростков, так или иначе, соприкасаются с Интернетом в повседневной жизни. По статистике 60% мальчиков и 69 % девочек школьного возраста являются ежедневными пользователями Интернет. В наше время средний возраст для первого знакомства с Интернетом - 5-6 лет. В мегаполисах довольно много малышей получает доступ в интернет с 3-4 лет, и лишь немногие дети знакомятся с Интернетом в школьном возрасте.

Характерным признаком и главным достоинством коммуникации в Интернете является возможность общаться в устной и письменной форме с любым субъектом при отсутствии географических и временных границ, а также высокая скорость передачи информации. В Интернете мы делаем множество интересных и важных вещей: работаем и отдыхаем, получаем новые знания и встречаем новых друзей. Все это стоит того, чтобы позаботиться о защите и сохранить свою жизнь в Интернете в безопасности. Эта мысль, возможно, абсолютно понятна взрослым пользователям, но, к сожалению, не всегда ясна подрастающему поколению.

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье детей и подростков, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для ребенка угрозу. Так, например, по данным прокуратуры Чувашской Республики, в 2015 году в Чувашии зафиксирован рост подростковой преступности. За первые 6 месяцев текущего года в регионе несовершеннолетними совершено около 300 преступлений, что на 49% больше, чем в 1 полугодии 2014 года. В ряде случаев корни правонарушений кроются в социальных сетях, где подростки подбивают друг друга на совершение неправомерных действий, а позже размещают фотографии со своими «достижениями», такими как похищенные из супермаркетов и магазинов вещи, последствия «разборок» со сверстниками и т.д.

В связи с этим актуальной представляется проблема обучения грамотному и корректному поведению в сети Интернет, проблема защиты детей от информации, причиняющей вред их здоровью и развитию. Большой вклад в решение данной

проблемы может внести образовательное учреждение. Работа в этом случае должна вестись в нескольких направлениях, основные:

- информационная, профилактическая и обучающая работа с детьми;
- информационная, разъяснительная и обучающая работа с родителями.

Работа с детьми может реализовываться в форме бесед, лекториев, конкурсов и иных мероприятий, вызывающих интерес, заставляющих задуматься, позволяющих использовать полученные знания для собственной защиты в сети Интернет. С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения.

Все формы Интернет - общения, в связи с его опосредованностью компьютером, обладают некоторыми особенностями. Человек, погружаясь в виртуальную реальность, создает виртуальную личность, которая обладает определенным набором характеристик. Во-первых, это анонимность (и физическая непредставленность). Несмотря на то, что иногда есть возможность получить некоторые сведения анкетного характера и даже фотографию виртуального собеседника, этого недостаточно для реального и более - менее адекватного восприятия личности. Кроме того, при виртуальном общении наблюдается скрывание или презентация ложных сведений о себе. Вследствие подобной анонимности и безнаказанности в Сети проявляется и другая особенность, связанная со снижением психологического и социального риска в процессе общения - аффективная раскрепощенность, ненормативность и некоторая безответственность участников общения. Человек в сети может проявлять и проявляет большую свободу высказываний и поступков (вплоть до оскорблений, нецензурных выражений, сексуальных домогательств), так как риск разоблачения и личной отрицательной оценки окружающими минимален.

Коммуникация в сети Интернет характеризуется добровольностью и желательностью контактов. Пользователь Интернета добровольно завязывает всевозможные контакты или уходит от них, а также может прервать их в любой момент.

Интернет-общение характеризуется затрудненностью эмоционального компонента общения. Специалистами в области коммуникации подсчитано, что современный человек произносит за день около 30 тысяч слов или примерно 3 тысячи слов в час. Ученые установили, что с помощью языка мы передаем не более 35% информации своим собеседникам. На долю невербального языка приходятся оставшиеся 65% информации, передающейся в процессе коммуникации. Невербалика дает возможность выразить эмоции (отношение к собеседнику, к происходящему и пр.). При общении в Интернете эмоциональный компонент общения присутствует, но он чрезвычайно затруднен. Но, в то же время у человека может проявляться стойкое стремление к эмоциональному наполнению текста, которое выражается в создании специальных значков для обозначения эмоций или в описании эмоций словами (в

скобках после основного текста послания). Ученые называют это компенсаторной виртуальной эмоциональностью.

Общаясь в сети Интернет, человек нередко стремится к нетипичному, ненормативному поведению. Зачастую пользователи Интернета презентуют себя с иной стороны, чем в условиях реальной социальной нормы, проигрывают нереализуемые в деятельности вне сети роли, сценарии ненормативного поведения. Другое важное следствие физической непредставленности человека в текстовой коммуникации - это возможность создавать о себе любое впечатление по своему выбору. Действительно, в текстовой коммуникации в сети Интернет люди часто создают себе так называемые «виртуальные личности», описывая себя определенным образом. Виртуальная личность наделяется именем, часто псевдонимом (который еще называют - «ник»).

Интернет несет в себе большой информационный и образовательный потенциал, является средством гармонического развития, но, одновременно содержит и риски.

Можно выделить ряд *основных информационных угроз* в сети, представляющих опасность для детей и подростков.

Это:

<u>просмотр сайтов для взрослых</u>

По результатам исследования «Лаборатории Касперского», из всех сайтов с маркировкой 18+ наибольший интерес для российских детей представляют эротические и порнографические сайты - 46,4%, на втором месте оружейная тематика - 26,4%, на третьем - нецензурная лексика - 10,7%. Следует обратить внимание, что указанные проценты - это удельный вес не всех посещаемых несовершеннолетними сайтов, а только входящих в категорию нежелательных. Ещё точнее - в эти проценты вошли и неудачные попытки попасть на «взрослые» сайты, если они были заблокированы модулем «Родительский контроль». Что делать если ребенок смотрит сайты для взрослых? Например, на вопрос: "У меня сыну 12 лет, недавно обнаружила, что он смотрит порно, как быть, что делать?", - на сайте Liveexpert.ru был дан следующий ответ: 1. Включите на компе функцию «родительский контроль»; 2. Купите и положите ему на стол книгу «Сексуальная энциклопедия для подростков». Это как минимум; 3. Скажите отцу (или дедушке) пусть поговорят с сыном об интересующих мальчика вопросах секса. Здесь не место ханжеству.

<u>Кибер-террор (кибербуллинг) или «троллинг»</u>

Проще говоря, это травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди. «Троллинг» может принимать разные формы: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве. В Интернете, как правило, ребенок находится один на один с потенциальным

обидчиком, который к тому же уверен в своей анонимности и может действовать более нагло. Детей и подростков, сильнее, чем в предыдущие годы, стали беспокоить агрессия и киберпреследования при общении в интернете, социальных сетях и блогах (кибербуллинг). В 2014 году почти каждое второе обращение на линию оказания психологической помощи «Дети онлайн» было по этой теме, что на 10% больше по сравнению с 2013 годом. Данная тема на протяжении всех пяти лет работы совместного проекта МГТС и «Фонда развития Интернет» является одной из основных.

Помощь могут оказать на бесплатной горячей линии «Дети онлайн» 8–800–250–0015. Это первый в России общественный проект, целями которого является консультирование и оказание психологической помощи детям и подросткам, столкнувшимся со сложностями во время коммуникаций в Интернете. По мнению эксперта «Лаборатории Касперского», борьба с кибер-травлей технически не так проста, поэтому и программный родительский контроль не столь эффективен. При этом дети не способны справиться с агрессорами в одиночку, но зачастую не обращаются за помощью к взрослым, будучи запуганными угрозами, либо просто из-за отсутствия доверия к близким людям. Поэтому самую важную роль в защите ребенка от кибер-террора играют отношения с родителями. Старший научный сотрудник ESET Дэвид Харли советует родителям пользоваться интернетом и, в частности, соцсетями вместе со своими детьми, начиная с дошкольного возраста. Это наиболее тактичный способ познакомить их с основами онлайн-безопасности.

Кибермошенничество

Кибермошенничество - один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества. Для кражи личной информации пользователя, применяются все более сложные фишинговые схемы, в том числе с использованием узнаваемых брендов. В 2013 году число обращений по данному вопросу достигло 19%. Чаще всего Интернет-пользователи обращались на линию уже после столкновения с мошенниками, чтобы получить консультацию по дальнейшим действиям.

Некоторые правила, позволяющие предупредить кибермошенничество:

- проинформируйте ребенка о самых распространенных методах мошенничества в сети; всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в Интернете;

- не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки;

- не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны, помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды, если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники;

- установите на свои компьютеры антивирус или персональный брандмауэр, подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия;

- убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку.

Компьютерные игры

Компьютерная игра – это компьютерная программа, служащая для организации игрового процесса (геймплея), связи с партнёрами по игре, или сама выступающая в качестве партнёра.

Компьютерные игры часто создаются на основе фильмов и книг; есть и обратные случаи. С 2011 года компьютерные игры официально признаны в США отдельным видом искусства. Компьютерные игры можно делить на виды, исходя из различных оснований. Видов игр - великое множество. На психику человека (в т.ч. ребенка, подростка) они, как отмечают ученые, влияют по-разному.

Современные ученые многих стран сходятся во мнении, что играть в компьютерные игры можно с трех лет по 15 минут дважды в неделю. Именно время выступает на этом этапе определяющим фактором безопасности. С пяти до семи лет время игры можно увеличить до 20 минут, а с восьми - уже до получаса. В то же время российские врачи говорят, что шести-семилетние дети могут без ущерба для здоровья заниматься за компьютером не более 10 минут. Ученики 2–3 классов - 15 минут. В 4–6 классах норму можно повысить до 20 минут, в 8–9 - до 25 минут и только в 10–11 - до получаса.

Можно очень долго рассуждать на тему пользы и вреда компьютерных игр. Однако самое парадоксальное заключается в том, что сами они не обладают ни признаком вредности, ни признаком полезности, точно так же, как и любой другой предмет. Как отмечает автор одной из работ, посвященных проблеме влияния компьютерных игр на ребенка, - компьютерные игры можно сравнить с каким-либо предметом, например, ножом, и как любой предмет, сами по себе они и не полезны и не вредны: ведь ножом можно отрезать лимон, а можно и зарезать старушку, но почему-то еще никому не пришло в голову запретить ножи; дело не в предметах, а в том как, кем и с какой целью они используются.

Плохо, если у ребенка, увлекающегося компьютерными играми, начинает формироваться компьютерная зависимость. Основными признаками того, что не все благополучно, становится следующее:

1) нежелание отвлечься от игры на компьютере;

2) раздражение при вынужденном отвлечении;

3) неспособность спланировать окончание сеанса игры на компьютере;

4) расходование больших денег на постоянное обновление как программного обеспечения, так и компьютерных устройств;

5) забывание о домашних делах, учебе, встречах и договоренностях в ходе игры на компьютере;

6) пренебрежение собственным здоровьем, гигиеной и сном в пользу проведения большего количества времени за компьютером;

7) готовность удовлетворяться нерегулярной, случайной и однообразной пищей, не отрываясь от компьютера;

8) ощущение эмоционального подъема во время игры на компьютере;

9) обсуждение компьютерных игр, их тематики со всеми людьми, мало-мальски сведущими в этой области.

Игровая компьютерная аддикция (зависимость), по мнению ученых, может формироваться в любом возрасте, но наиболее актуальна эта проблема для подростков в силу сензитивности данного возрастного периода и их повышенного интереса к компьютерным играм.

Распространение в открытом доступе персональных данных несовершеннолетних

В мае 2014 года Роскомнадзор выявил более 200 сайтов, распространяющих в открытом доступе персональные данные несовершеннолетних россиян и их родителей.

Сайты, разместившие персональную информацию о детях, как правило, принадлежат школам, детским садам, интернатам, а также муниципальным образованиям и администрациям ряда субъектов Российской Федерации.

Обнаруженные данные содержали списки воспитанников детских садов и интернатов, учеников школ, с указанием их ФИО, даты рождения, места проживания, а также сведения о социальном статусе родителей и их принадлежности к той или иной льготной категории граждан. Речь идет о многодетных семьях, матерях-одиночках, безработных родителях, детях сотрудников правоохранительных органов, детях судей, детях, оставшихся без попечения родителей. На сайте одного из образовательных учреждений был опубликован список детей, направляемых на психоневрологическую комиссию.

Таким образом, Интернет – это глобальная компьютерная сеть, которая на сегодняшний день охватывает практически весь мир. В настоящее время существует очень много способов общения в Интернете, конечно же, не стоит полностью исключать компьютер из жизни ребенка. Просто необходимо внимательно следить за тем, как ваши дети пользуются Интернетом, научить их делать осознанный и грамотный выбор.

Психологические аспекты влияния Интернета на личность ребенка

С психологической точки зрения, негативное влияние интернета можно разделить на:

1. *Тактическое* – возникновение стрессов, актуальных для юных пользователей и их родителей.
2. *Стратегическое* – негативное влияние на психическое развитие ребенка или подростка.

Среди его составляющих, которые несут в себе негативный потенциал, необходимо отметить такие, как:

а) цифровая гипомнезия, или снижение эффективности запоминания (нет необходимости хранить информацию в долговременной памяти, если она всегда доступна по поисковому запросу в онлайне);

б) цифровое (клиповое) мышление, характеризующееся поверхностностью суждений, снижением критики и соответственно поспешностью принимаемых решений;

в) цифровая социализация - чрезмерное увлечение общением виртуальным, онлайновым общением в ущерб живому, офлайновому чревато развитием коммуникативной и эмоциональной некомпетентности, дефицита навыков взаимодействия с окружающими в реальном социуме и соответственно нарушением социально-психологической адаптации.

Регулярность повторения подобных состояний, их суммарная длительность (практически ежедневно, до нескольких часов в день, особенно если пользование интернетом оказывается вне родительского контроля и у ребенка возникает интернет-зависимость) могут быть достаточными для того, чтобы оказывать на психическое развитие ребенка/ подростка значимое влияние.

Таблица 1. Воздействие Интернета на личность

Три основных вида деятельности, осуществляемой в Интернете:	*Глобальные изменения (трансформации) личности:*
познавательная	Увлеченность познанием в сфере программирования и телекоммуникаций. Крайний вариант - *хакерство*
игровая	Увлеченность компьютерными играми. Крайний вариант - *игровая наркомания*
коммуникативная	Увлечение сетевой коммуникацией. Крайний вариант - *Интернет-аддикция* - своеобразная (нарко)зависимость от Интернета

По мнению психологов, пользование Интернетом должно дозироваться.

- *Ребенку до 7 лет* - интересно и даже необходимо играть, особенно — в развивающие и сюжетно-ролевые игры.
- *Ограничение по времени - не больше 30 минут в день!*
- *С 7 до 11 лет***,** дети по-прежнему любят играть и стремятся использовать интернет именно как площадку для игр. В этом возрасте у детей просыпается т. н. социальное «Я» => потребность в общении со сверстниками.
- *Ребенок в 11—14 лет* — это подросток. И самой главной, значимой, ведущей его деятельностью является общение с ровесниками. Здесь мобильный интернет может стать просто незаменимым помощником. Однако интерактивное общение нужно обязательно совмещать с реальным. Важно, чтобы ответы на свои вопросы подросток находил в первую очередь у родителей, а не на сомнительных сайтах.
- *Ребенок старше 14 лет* - уже достаточно взрослый человек. Интересуйтесь всем тем, чем интересуется Ваш ребенок. Начиная с этого возраста с ребенком можно говорить и о выборе будущей профессии. А в интернете можно найти множество информации, которая поможет ребенку определиться.

В каком возрасте ребенку лучше купить личный компьютер? Психологи считают, что по-настоящему он необходим только класса с 5-6-го, когда школьнику начинают задавать творческие работы, рефераты.

Стив Джобс запрещал своим детям слишком долго сидеть с айпадами и айфонами. Почему? Крис Андерсон (бывший редактор Wired, нынешний исполнительный директор 3D Robotics): «Это потому, что я вижу опасность чрезмерного увлечения интернетом как никто другой. Я знаю, с какими проблемами столкнулся я сам, и я не хочу, чтобы эти же проблемы были у моих детей».

Это может показаться странным. Но, судя по всему, генеральные директора IT-гигантов знают что-то, чего не знают обыватели…

Как уберечь ребенка от вреда Интернета? Психологи дают ряд советов.

- Обсудите с детьми опасности Интернета
- Держите устройства с подключением к Интернету в центре внимания
- Знайте, для чего Ваши дети используют Интернет
- Позвольте Вашим детям учить Вас. Это отличный способ общаться.
- Научите их доверять своим инстинктам и сообщать о любых неприятностях
- Научите детей советоваться с Вами, прежде чем предоставить личные сведения в Интернете
- Научите детей сообщать Вам о подозрительных действиях
- Помогите детям выбрать подходящие псевдонимы, адреса электронной почты и пароли
- Научите детей уважать других людей и соблюдать этикет в Интернете

- Установите четкие правила (распорядок) использования Интернета.

Одна из ошибок родителей – неумение правильно подбирать для своего ребенка программное обеспечение. Компьютер в первую очередь должен обучать, а уж потом развлекать. Воспитание ребенка должно сводиться по большей части к тому, что компьютер - это лишь часть жизни, а не самый главный подарок за хорошее поведение. Ребенок всегда считает, что запрещают самое интересное. Компьютер в таких случаях становится для ребенка просто самоцелью.

Риску стать интернет-зависимыми более всего подвержены дети, у которых не складываются отношения со сверстниками и родителями. Эти дети пытаются найти замену живому общению в виртуальных играх и чатах. «Уходят» также дети, испытывающие постоянный родительский прессинг: «Ты должен!». Нехватка эмоционального контакта, тех самых родительских объятий и поцелуев – тоже одна из причин ухода ребенка в виртуальный мир.

Как быстро формируется компьютерная зависимость? Достаточно полутора-двух месяцев!

Когда пора забеспокоиться?

- ребенок раздражается при необходимости отвлечься от работы или игры на компьютере;
- он не способен спланировать окончание сеанса работы или игры;
- расходует значительные суммы денег на обеспечение постоянного обновления как программного обеспечения (в том числе и игр), так и устройств компьютера;
- забывает о домашних делах, учебе и договоренностях в ходе работы или игры на компьютере;
- пренебрегает собственным здоровьем, гигиеной и сном в пользу проведения большего количества времени за компьютерными играми;
- ему все равно, что есть, лишь бы не отрываться от монитора, он вообще часто забывает о еде;
- ощущает эмоциональный подъем только во время работы с компьютером;
- обсуждает компьютерные проблемы со всеми мало-мальски сведущими в этой области людьми.

Основная рекомендация, гарантирующая безопасность ребенка в мобильном интернете – доверительное общение с родителями.

Родительский контроль, или как ограничить доступ ребенка к компьютеру и Интернету

«Лаборатория Касперского» является крупнейшей в мире частной компанией, занимающейся разработкой защитных решений для домашних пользователей и корпоративных IT-инфраструктур. Чтобы всегда предоставлять своим клиентам надежную и отвечающую их потребностям защиту, компания регулярно проводит специализированные исследования.

Летом 2013 года «Лаборатория Касперского» совместно с международной аналитической компанией B2B International провела исследование, в ходе которого было опрошено 8605 респондентов в возрасте 16+, проживающих в странах Латинской и Северной Америки, Ближнего Востока, Азии, Африки, Европы и России в частности.

Данные исследования:

Родители	*Мужчины*	*Женщины*
Переживают, что не контролируют, что видит/делает их ребенок в сети	21%	17%
Признались, что эффективные средства для защиты детей в Сети были бы очень полезны и востребованы ими	75%	83%
Используют программы с функциями родительского контроля	33%	21%
Стараются следить за детьми, когда они в сети	43%	36%
Добавили своих детей в друзья в социальных сетях	12%	19%

Методы родительского контроля:

- *Технические* - позволяют выстроить защищенный контур информационного пространства ребенка, используя технические возможности программных и аппаратных средств доступа в Интернет.
- *Воспитательные* - позволяют выстроить доверительные и взаимоуважительные отношения между родителем и ребенком в процессе обсуждения принимаемых ограничений доступа в Интернет и других защитных мер от Интернет-угроз.

Технические методы родительского контроля:

- Настройка безопасного поиска в Интернете.
- Контроль посещения сайтов.
- Фильтрация Интернет-трафика и защита от вирусов.
- Организация и контроль безопасного общения в социальных сетях.
- Контроль общения в чатах и по электронной почте.

- Безопасный Интернет-канал.
- Ограничение времени работы за компьютером.
- Настройка и защита мобильных устройств.
- Настройка ограничений теле/видео/игровых приставок и телевизоров с выходом в Интернет (XBOX, PlayStation, AppleTV, SmartTV и т.п.).

Безопасный поиск в Интернете

Сетевые ресурсы	Наличие системы безопасности
Yandex.ru	В настройках поиска можно установить режим фильтрации «Семейный поиск». Воспользоваться интерфейсом Семейного поиска также можно на сайте family.yandex.ru.
Google.ru	Информация в разделе «Центр безопасности» поможет: • настроить фильтрацию результатов поиска на сайте Google, видеороликов на YouTube.com, приложений в Google Play маркет. • настроить ограниченный доступ к приложениям на мобильных устройствах с ОС Android. Также размещены рекомендации по безопасной работе в Интернет.
Соцсеть «ВКонтакте»	Открытая группа «Безопасность» посвящена безопасности вашего аккаунта на сайте vk.com, а также советам по информационной безопасности в целом.
Соцсеть «Одноклассники»	На странице «Помощь» размещены рекомендации по безопасному использованию сайта и защиты профиля от вирусов и сомнительной рекламы.

Для контроля веб-трафика можно использовать специальные программы. Данная функция часто присутствует в многофункциональных антивирусных системах.
Основные возможности:

- Общий и детальный анализ посещений предпочитаемых сайтов.
- Подсчет потраченного времени.
- Блокировка доступа к запрещенным сайтам (черный/белый список настраивается вручную).

Для фильтрации интернет-ирафика и защиты от вирусов используются антивирусные системы, защищающие от таких Интернет-угроз, как вирусы, спам, рекламные баннеры, фишинговые сайты, программы-шпионы, сетевые атаки и т.п.

При работе в Интернет *важно*:

- Контролировать активность антивирусной системы.
- Проверять актуальность и обновлять базы данных.

– Уделять серьезное внимание всем сообщениям о выявленных угрозах. Научиться их понимать.

Способы безопасного общение в социальных сетях:

- Совместная регистрация в соцсетях. Настройка достоверного возраста (возможно, без раскрытия даты рождения).
- Добавиться в друзья/родственники к своим детям.
- Контролировать круг знакомств, темы и этическую сторону общения.
- Соблюдать на своей странице чистоту и правильную информацию, учитывая доступ к ней своего ребенка.
- Использовать настройки безопасности личной страницы в социальной сети для защиты от нежелательной информации и контактов.
- Создавайте сложные пароли (буквы, цифры, символы).

Безопасность Чатов.

Взрослые могут судить о степени безопасности чата, в котором общается ребенок, ответив утвердительно на три основных вопроса:

1. Предназначен ли чат для детей? В чатах, предназначенных для детей, вероятность неуместных тем или нежелательного контакта гораздо ниже.
2. Осуществляется ли контроль за чатом? Иногда в чатах работают добровольные модераторы, которые предотвращают случаи неуместного общения и могут заблокировать доступ в чат для хулиганов и других нарушителей порядка. Если контроль не осуществляется, в чате, по крайней мере, должна иметься кнопка для связи с администратором. Для детей предпочтительны контролируемые чаты. Уровень безопасности также повышается, если беседы сохраняются.
3. Возможно ли заблокировать доступ для пользователей? Блокировка доступа подразумевает запрет размещения в чате сообщений от конкретного пользователя. После блокировки доступа для пользователя его сообщения больше не отображаются на экране.

Безопасность использования электронной почты.

Используя настройки безопасности и правила получения/отправки электронной почты, можно организовать следующие возможности:

1. Настроить пересылку всех входящих писем с электронной почты ребенка на свою электронную почту. Следовательно вы всегда будете знать, кто и о чем пишет вашему ребенку.
2. Настроить разрешение получать (отправлять) письма только от ограниченного списка контактов.

Средства безопасности почтовых программ и антивирусные системы позволяют защищаться от спама и вирусов, передаваемых по электронной почте.

Важно соблюдать следующие правила безопасности:

- Не открывайте вложения в письмах, полученных от неизвестного Вам адресата или с сомнительным содержанием.
- Обращайте внимание на истинную цель отправителя. Переносите данное письмо в папку «СПАМ», чтобы очистить её позже, либо удаляйте его сразу.
- В некоторых программах можно использовать защищенный режим чтения писем, позволяющий понять цель и содержание.

Большинство Интернет-провайдеров предоставляют дополнительные услуги «Детский Интернет», который позволяет полностью исключить доступ Вашего ребёнка к ресурсам сети, которые: разжигают национальную рознь, пропагандируют насилие, распространяют порнографическую информацию, содержат нецензурную лексику.

В периоды отсутствия родителей, либо согласно введенному в семье распорядку, ограничить время работы за компьютером можно с помощью:

- настройки «Родительский контроль» в операционной системе (MS Windows 7 и выше, Mac OC X),
- настройки функций Родительского контроля в многофункциональных антивирусных системах,
- специальных программ, ограничивающих время работы компьютера.

Настройка и защита мобильных устройств:

- Смартфоны, коммуникаторы, планшеты, нетбуки, ноутбуки и т.п. мобильные устройства, имеющие выход в Интернет, должны быть настроены, аналогично персональному компьютеру.
- В основном современные мобильные операционные системы (Android, Apple iOS, Windows Phone и другие) имеют встроенный функционал Родительского контроля.
- Каждое устройство требует индивидуального подхода.
- Возможности контроля могут отличаться в зависимости от производителя устройства и версии программного обеспечения.
- Следует помнить, что многие теле/видео и игровые приставки, а также современные телевизоры могут быть подключены к Интернету. Следовательно являются источником потенциальных Интернет-угроз, среди которых видео-ролики, игры, чаты, развлекательные программы с возрастным ограничением.
- *ТВ и видео приставки с доступом в Интернет о*бычно имеют встроенный функционал родительского контроля. В основном требуется настроить

ограничения к некоторым каналам и приложениям и установить пароль для защиты настроекот изменений детьми.

- *Игровые приставки с доступом в Интернет* обычно связаны с настройкой профиля игрока, в котором указывается возраст и другие личные данные. Важно, контролировать настройки профиля вашего ребенка. С целью снять возрастное ограничение некоторые дети изменяют возраст в своих профилях.

Заключение

На наш взгляд, проведение семинаров по безопасной работе в сети Интернет дает родителям практические навыки, позволяющие:

- защитить своего ребенка от нежелательного влияния Интернета;
- уберечь ребенка от контактов с незнакомыми людьми в виртуальной реальности;
- осуществлять родительский контроль над поведением детей в сети Интернет с помощью программного обеспечения.

Получив необходимые знания, родители, в свою очередь, должны объяснить своим детям, как сделать более безопасным и полезным свое общение в Интернете и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную информацию от безопасной;
- избегать навязывания информации, способной причинить вред здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления неопытностью детей и их доверчивостью, попытки вовлечения детей в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательной информации и контактов в сетях.

Литература

1. Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт: [Электронный ресурс]. URL: http://i-deti.org.
2. Дети в информационном обществе: [Электронный ресурс]. URL: http://detionline.com/journal/.
3. Детская безопасность в глобальной сети. Видео (профессиональное и любительское): [Электронный ресурс]. URL: http://detionline.com/video/professional.
4. Детская безопасность/Центр безопасности GOOGLE: [Электронный ресурс]. URL: http://www.google.ru/safetycenter/families/start/basics.
5. Информационная безопасность бизнеса, 2013: [Электронный ресурс]. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2013.pdf
6. Национальный Узел Интернет-безопасности в России: [Электронный ресурс]. URL: http://saverunet.ru.
7. Образовательно-выставочный проект «Дети в интернете» (реализован МТС). Статистика и Исследования, посвященные изучению психологии цифрового поколения России: [Электронный ресурс]. URL: http://detionline.com/mts/about.
8. Родительский контроль / Лаборатория Касперского: [Электронный ресурс]. URL: www.kaspersky.ru/parental_control.
9. Фонд Развития Интернет: [Электронный ресурс]. URL:http://detionline.com.
10. Блог социального педагога, психолога: [Электронный ресурс]. URL:http://myblogіnfo.ru.

Глоссарий

Аккаунт – персональная информация пользователя, зарегистрированного на определенном ресурсе. Иногда путают с «личным кабинетом» и «персональной страничкой».

Антивирусная программа (антивирус) - любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики - предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Виртуальная реальность – искусственная реальность, электронная реальность, компьютерная модель реальности, созданный техническими средствами мир (объекты и субъекты), передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и другие.

Вирус - программа, способная к размножению и заражению файлов, программ и компьютерных систем. Некоторые вирусы могут самостоятельно реплицироваться и распространяться, другие также могут нанести ущерб компьютеру и данным.

Вредоносная программа – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам компьютера или к информации, хранимой на компьютере, с целью использования ресурсов компьютера или причинения вреда (нанесения ущерба) владельцу информации.

Груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети.

Интернет - всемирная система объединённых компьютерных сетей для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть. Построена на базе стека протоколов TCP/IP. На основе интернета работает Всемирная паутина (World Wide Web, WWW) и множество других систем передачи данных.

Кибермошенничество – один из видов киберпреступления, целью которого является умышленный обман или злоупотребление доверием пользователей с целью получения какой-либо выгоды.

Кибер-террор (кибербуллинг) или «троллинг» - травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

Компьютерная игра – это компьютерная программа, служащая для организации игрового процесса (геймплея), связи с партнёрами по игре, или сама выступающая в качестве партнёра.

Социальная сеть – программный сервис, площадка для взаимодействия людей в группе или в группах, сайт, объединяющий отдельных людей или организации. Ее участники реальны и связаны друг с другом теми или иными отношениями: от случайных знакомств до тесных семейных и дружеских связей. В качестве подобия социальной сети можно рассматривать любое онлайновое сообщество, члены которого участвуют, например, в обсуждениях на форуме. Социальная сеть также образуется читателями тематического сообщества, созданного на любом сервисе блогов. Многие профессиональные сообщества превратились в инструмент поиска людей, рекомендации сотрудников и поиска работы.

Спам (от англ. spam) – анонимная массовая не запрошенная рассылка по электронной почте коммерческой, политической и иной рекламы или иного вида сообщений от неизвестных людей или организаций без согласия получателя.

Троллинг - размещение в Интернете провокационных сообщений с целью вызвать флейм, конфликты между участниками, оскорбления и т. п.

Фишинг - попытка ввести пользователя в заблуждение с целью получения конфиденциальной информации, например номера страховки или паролей. Как правило, в атаках фишинга применяются якобы законные адреса электронной почты или мгновенные сообщения в сочетании с подложными веб-сайтами для отправки мошеннических запросов данных.

Флейм - обмен сообщениями в интернет-форумах и чатах, представляющий собой словесную войну, нередко уже не имеющую отношения к первоначальной причине спора.

Флуд - неоднократное повторение ненужной информации, размещение однотипной информации, одной повторяющейся фразы, символов, букв, одинаковых графических файлов или просто коротких бессмысленных сообщений на веб-форумах, в чатах, блогах.

Форум – интернет-сервис для общения (обычно на определенную тему), где каждый пользователь может оставлять свои текстовые сообщения, доступные для прочтения другим. Форум отличается от чата разделением обсуждаемых тем и возможностью общения не в реальном времени. Форумы часто используются для разного рода консультаций, в работе служб технической поддержки. В настоящее время форумы являются одним из наиболее популярных способов обсуждения вопросов в Интернете.

Холивар - обмен сообщениями в интернет-форумах и чатах, представляющий собой бессмысленные дискуссии, в которых участники пытаются доказать друг другу преимущество одной из нескольких похожих альтернатив (компьютерных программ, технологий, актёров, музыкальных групп и т. п.).

Чат – средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение.

Приложения

Приложение 1. Анкета для родителей

Анкета для родителей учащихся
«Мой ребенок и Интернет»

Уважаемые родители, просим Вас принять участие в анкетировании. Выберите и отметьте один ответ на каждый вопрос.

1. Защищаете ли Вы своих детей от негативного влияния Интернета и социальных сетей?

А. Да.

Б. Нет.

2. Разрешаете ли Вы своим детям бесконтрольно пользоваться выходом в Интернет с любого устройства?

А. Да.

Б. Нет.

3. Смогли бы Вы полностью ограничить выход в Интернет для своего ребенка?

А. Да.

Б. Нет.

4. Выделяете ли Вы время на приобретение знаний о негативном влиянии Интернета?

А. Да, регулярно.

Б. Да, но редко.

В. Нет.

СПАСИБО!

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ «КАК СДЕЛАТЬ ПОСЕЩЕНИЕ ИНТЕРНЕТА ДЛЯ ДЕТЕЙ БЕЗОПАСНЫМ»

1. Признайте право своего отпрыска на общение с кем-то, кого Вы не знаете. Даже если Вы в целях контроля и успокоения зарегистрируетесь на всех ресурсах, где зависает Ваш ребенок, Вы не сможете читать скрытые и личные сообщения. Однако, зарегистрироваться на этих ресурсах не запрещается: чтобы Ваше чадо не теряло ощущения с реальностью, стоит иногда появляться на его страничке, иногда писать комментарии (по делу, например, напомните ему о том, что пора делать уроки), чтобы он ощущал Ваше присутствие. Однако, не переборщите.
2. Выразите понимание и уважение склонностям ребенка вести онлайн-дневник. Похвалите его мысли, стихи, фотографии, или его стиль общения. Осведомитесь, можно ли Вам изредка заходить и читать те записи, которые он публикует для открытого просмотра. Если ребенку такое не понравится – согласитесь с его решением и не заходите в его дневник без необходимости.
3. Напоминайте ребенку, что пора прекращать общение и ложиться спать (идти кушать, учить уроки). Действуйте жестко – вплоть до выключения компьютера.
4. Если ребенок в гостях или у Вас на работе пытается сесть за компьютер, объясните ему, что углубляться в личное при посторонних неприлично. Научите ребенка терпеть неудобства, связанные с невозможностью выйти в сеть.
5. Объясните ребенку об опасностях, подстерегающих его на просторах сети. Запретите под любым эффективным страхом посылать смс на предлагаемые номера, давать незнакомым людям свои адрес и телефон, ругаться с людьми, даже если человек его оскорбляет (быть может, даже посоветуйте в этих случаях обратиться к родителям). У ребенка не должно быть иллюзий по поводу радужности и дружелюбности Интернета.
6. Поощряйте в ребенке склонность к хобби или спорту – в этом случае у него будет меньше вероятности заболеть Интернет-зависимостью.
7. Составьте список того, что нельзя делать за компьютером. Например, кушать, делать уроки, говорить по телефону, читать книгу, заниматься рукоделием.
8. Доведите до сознания ребенка, что реальный и виртуальный мир – разные вещи. Что люди ведут себя по-разному в сети и в жизни. Что аватар не является лицом человека, а его комментарии – его мыслями.
9. Устраивая счастье ребенка, не стоит давать ему полную свободу при общении онлайн. Однако, и запрещать такое общение категорично, без аргументов нельзя. Не отгоняйте ребенка от компьютера. Лучше – присядьте рядом и посмотрите в монитор вместе.

10. Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение 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.

Помните: смежная специальность современного родителя - Интернет-Ангел хранитель!

ПАМЯТКА ДЛЯ ДЕТЕЙ «БЕЗОПАСНОЕ ПОВЕДЕНИЕ В ИНТЕРНЕТЕ»

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, нужно предпринимать следующие меры предосторожности при работе в Интернете:

- Никогда не сообщать свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
- Необходимо использовать нейтральное экранное имя, не содержащее неприличных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.
- Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
- Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
- Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие непристойные намеки. Расскажите об этом родителям.

Приложение 4. Специальные службы для детей и родителей Чувашской Республики

№п/п	Наименование учреждения	Телефон	Время работы
1.	Республиканское государственное образовательное учреждение «Центр психолого-педагогической реабилитации и коррекции» Министерства образования и молодежной политики Чувашской Республики	(8352) 43-02-24	9.00-17.00
2.	МОУ для детей, нуждающихся в психолого-педагогической и медико-социальной помощи «Центр психолого-педагогической реабилитации и коррекции «Семья» г. Чебоксары	(8352) 63-37-17	8.00-17.00
3.	МОУ для детей, нуждающихся в психолого-педагогической и медико-социальной помощи «Центр психолого-медико-социального сопровождения «Содружество» г. Чебоксары	(8352) 62-24-37	8.00-17.00
4.	Экстренная психологическая помощь (служба, действующая круглосуточно под патронажем Министерства здравоохранения и социального Чувашии)	**(8352)58-31-31, 075**	круглосуточно
5.	Единый телефон доверия для детей, подростков и родителей, звонок бесплатный и анонимный для жителей России	**8-800-2000-122**	круглосуточно
6.	Единый телефон доверия (помощь по этому номеру оказывается АНОНИМНО)	**8-800-100-49-94**	круглосуточно