МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ УРОКОВ **«БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ» В НАЧАЛЬНОЙ И СРЕДНЕЙ ШКОЛЕ**

Ростелеком
Больше возможностей

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Стремительно развивающийся современный мир выдвигает новые требования к развитию личности человека. Современное образование рассматривается во всём мире как важный фактор становления и развития личности, как неотъемлемая часть социокультурной среды, в которой живёт человек.

Новые федеральные государственные образовательные стандарты (ФГОС), разрабатываемые в соответствии с решением Правительства РФ, – это один из основных элементов управления развитием российского образования. Федеральные государственные стандарты устанавливаются в Российской Федерации в соответствии с требованием статьи 7 «Закона об образовании» и представляют собой «совокупность требований, обязательных при реализации основных образовательных программ начального общего образования (ООП НОО) образовательными учреждениями, имеющими государственную аккредитацию».

С официальным приказом о введении в действие новых стандартов и текстом стандарта можно ознакомиться на сайте Минобрнауки России: http://www.edu.ru/db-mon/mo/Data/d_09/m373.html.

В связи с переходом на новые ФГОС учителю необходимо будет изменить методы работы с классом и каждым учащимся в отдельности с позиции новых требований, предъявляемых современным обществом к выпускнику школы.

В основу разработки стандарта положена целевая установка, предусматривающая переход от «догоняющей» к «опережающей» модели развития российского образования.

При разработке Стандарта был полностью учтён объективно происходящий в условиях информационного общества процесс формирования новой дидактической модели образования, основанной на компетентностной образовательной базе. Главным образовательным результатом здесь является формирование мотивированной компетентной личности.

Обязательной составной частью основной образовательной программы начального общего образования являются планируемые результаты, которые можно разделить на три группы: личностные, метапредметные и предметные.

Под предметными результатами понимается освоенный обучающимися в ходе изучения учебного предмета опыт специфической для данного предмета деятельности и получение нового предметного знания.

Под метапредметными результатами понимаются как универсальные способы деятельности — познавательные, коммуникативные, так и способы регуляции своей деятельности (планирование, контроль), применяемые не только в рамках одного или нескольких учебных предметов, но и при решении проблем в реальных жизненных ситуациях.

Под личностными результатами понимается развитие мотивов и смыслов

учебной деятельности, формирование внутренней позиции школьника.

Предполагается, что в результате изучения всех предметов в начальной школе у учащихся будут сформированы личностные, регулятивные, познавательные и коммуникативные универсальные учебные действия (УУД) как основа умения учиться.

В сфере личностных УУД будут сформированы внутренняя позиция школьника, адекватная мотивация учебной деятельности, включая учебные и познавательные мотивы, ориентация на традиционные моральные нормы и их выполнение.

В сфере регулятивных УУД школьники овладевают всеми типами учебных действий, включая способность принимать и сохранять учебную цель и задачу, планировать её реализацию, контролировать и оценивать свои действия, вносить соответствующие коррективы в их выполнение.

В сфере познавательных УУД учащиеся научатся использовать знаково-символические средства, в том числе овладеют действием систематизации и моделирования, а также широким спектром логических действий и операций, включая общие приёмы решения задач.

В сфере коммуникативных УУД младшие школьники приобретут умения учитывать позицию собеседника, организовывать и осуществлять сотрудничество и взаимодействие с учителем и сверстниками, адекватно воспринимать и передавать информацию и отображать предметное содержание и условия деятельности в речи.

Существующая система образования не подвергается резким изменениям её установок и структур. Альтернативой является использование в обучении приёмов и методов, которые формируют умение самостоятельно находить и усваивать новые знания, собирать необходимую информацию, формируя у школьников умения и навыки самостоятельности и саморазвития. Активность обучающегося является целью обучения.

Для того чтобы реализовать новый подход в образовании, учителю необходимо не только подобрать новые методы обучения, научиться сотрудничать, но и иметь в руках учебно-методический комплект (УМК), помогающий достичь высоких результатов. Особенность нового стандарта заключается в том, что он не содержит определённого УМК – меняется сам подход, вводится внеучебная деятельность в количестве 10 часов.

Стандарт предполагает реализацию в образовательном учреждении как урочной, так и внеурочной деятельности. Внеурочная деятельность организуется по направлениям развития личности (спортивно-оздоровительное, духовно-нравственное, социальное, общеинтеллектуальное, общекультурное).

Содержание занятий должно формироваться с учётом пожеланий обучающихся и их родителей (законных представителей). Содержание

внеурочной деятельности должно быть отражено в основной образовательной программе образовательного учреждения.

Время, отведённое на внеурочную деятельность, не входит в предельно допустимую нагрузку обучающихся. Чередование урочной и внеурочной деятельности определяется образовательным учреждением и согласуется с родителями обучающихся.

Именно в эти часы мы и рекомендуем включить занятия по очень актуальной теме нашего времени – теме безопасности детей в Интернете.

Важность этого вопроса обусловлена тем, что информационно-коммуникационные технологии (ИКТ) в новых условиях позиционируются как образовательная технология, а не как отдельный предмет «Информатика». И умение работать с технологичной информацией, с информационными компьютерными сетями становится важнейшим моментом образовательного процесса в целом.

В новом стандарте ИКТ рассматривается как активный инструмент деятельности, в том числе познавательной, – умение пользоваться различными прикладными программами и техническими мультимедийными информационно-коммуникационными средствами. Здесь и возникает проблема безопасности школьника в Интернете.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ УРОКОВ «БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ» В ОБЩЕОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

1. Общие рекомендации

В наши дни компьютер становится привычным элементом не только дома и в научных лабораториях, но и в школьных классах. Людей, ежедневно проводящих за компьютером по нескольку часов, становится все больше. При этом уже мало кто сомневается, что длительное пребывание у экрана, неподвижность позы пользователя ПК, электромагнитные поля и излучения, мелькание изображения негативно влияют на физическое и психологическое здоровье человека.

Разработаны гигиенические требования, которые необходимо соблюдать при работе с компьютером:

– школьникам среднего и старшего возраста можно разрешить проводить перед монитором до двух часов в день, устраивая 10–15-минутные перерывы каждые полчаса;

– ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности – не более одного урока, а при наличии противопоказаний офтальмолога – только 10 минут не более 3 раз в неделю;

– лучше работать за компьютером в первой половине дня;

– комната должна быть хорошо освещена;

– мебель должна соответствовать росту ребенка;

– расстояние от глаз ребенка до монитора – 60 см;

– периодически нужно делать зарядку для глаз;

– непосредственное сидение за компьютером необходимо перемежать физическими упражнениями.

По данным Института возрастной физиологии, чем младше современные школьники, тем раньше они начали пользоваться компьютером: 9–10-летние впервые сели за компьютер в 7–8 лет, а 7–8-летние – в 5–6 лет. Количество времени, проводимое ежедневно подростками за компьютером, достигает 1–3 часов (65,61 % исследуемых). В части использования сети Интернет исследования института показывают, что 72 % школьников предпочитают общение в Интернете, 51 % – поиск информации, 24 % – выполнение учебных заданий, 52 % – прослушивание музыки, 26 % – просмотр фильмов.

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Однако доступность и проницаемость глобальной коммуникационной сети дает возможность и для нежелательных воздействий.

Сегодня количество пользователей российского сектора сети Интернет составляет десятки миллионов людей, и немалая часть из них – дети, которые могут не знать об опасностях Мировой паутины.

Одним из средств решения этой проблемы может стать просвещение общественности, участников образовательного процесса и специальная подготовка профессионалов, в первую очередь педагогов, в сфере безопасного поведения человека – специалиста и школьника в мире компьютерных технологий и Интернета.

Мы хотим сделать Интернет максимально безопасным и удобным для подрастающих поколений. Эта цель осуществима, если государство, представители бизнеса, правоохранительные органы и общественность объединят усилия, а родители осознают свою роль в обеспечении безопасности детей.

В данном методическом пособии представлены методические рекомендации для разработки классных часов для школьников двух возрастных групп, направленные на обеспечение необходимыми знаниями в области психолого-педагогического и здоровьесберегающего сопровождения образовательного процесса школьников, использующих персональные компьютеры и Интернет в учебной и внеучебной деятельности. Кроме того, пособие может быть интересно для организации работы с родителями школьников, так как содержит советы и рекомендации, как сделать компьютер и Интернет безопасными для своего ребенка.

Данные рекомендации – практическая информация для учителей-предметников и классных руководителей по организации внеурочной деятельности в части использования сети Интернет, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

Как правило, ребенка в сети Интернет привлекает возможность общения и игр. Виртуальная среда так же, как и реальный мир, обладает своими законами и правилами поведения. Основную опасность представляет её глобальность и, как следствие, возможность общения ребенка не только со сверстниками, но и с личностями – потенциальными источниками разрушающего социального и психологического поведения. Одновременно опасность представляет собой анонимность собеседника. При повышенном уровне доверия младших школьников велика вероятность социально деструктивного поведения неизвестного участника коммуникации. Поэтому, прежде чем отпускать ребенка в самостоятельное путешествие по бескрайним просторам Интернета, следует научить его основам безопасного и грамотного пользования Сетью. И в дальнейшем не прекращать контролировать процесс использования Интернета подростком.

Решающим фактором безопасного поведения ребенка в Интернете

является внимание со стороны родителей к проблеме взаимодействия ребенка с компьютерным миром вообще и сетью Интернет – в частности. Педагогам необходимо обратить внимание родителей на эту специфическую проблему киберопасности, подчеркнуть важность участия родителей в безопасной коммуникации ребенка в Сети и организовать периодические встречи, посвященные теме взаимодействия ребёнка с сетью Интернет.

Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие программные фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык безопасного поведения в Интернете.

Проблема относительно свежая, но решается старыми методами.

Задача организации участников образовательного процесса, заинтересованных в безопасном использовании Интернета подростками и детьми, заключается в следующем.

1. Родители должны знать, чем заняты их дети. Самое простое – разговаривать с детьми: чем живет, чем интересуется, какие сайты любит посещать и почему, с кем дружит, в том числе и в Интернете. Кроме того (не вместо – кроме!), семейный фильтр на поисковой машине, контроль по журналам посещённых страниц, логам и проч.

Дети должны владеть основами безопасного пользования интернет-сетями. Мы учим их не разговаривать с незнакомцами? Мы объясняем, что нельзя называть незнакомцам свой домашний адрес? В глобальной сети действуют все те же правила.

2. Учитель должен понимать, зачем он отправляет детей в Интернет. Учить «с Интернетом» нынче модно. Всегда ли это оправдано? Предположим, учитель сформулировал конкретные задачи урока, реализуемые с помощью интернет-ресурсов. Какие здесь могут быть варианты обеспечения безопасности:

а) закрытые среды обучения, например, учебные блоги, где могут оставлять свои комментарии только те, кто получил соответствующий доступ от учителя, ведущего блог;

б) постановка конкретной учебной задачи: что хочу найти, где, как использую;

в) формирование навыков критического мышления;

г) список проверенных учителем ресурсов, с которых предлагается использовать информацию;

д) все те же фильтры и контроль системного администратора, если таковой в школе имеется.

Самое главное – приучать детей не «проводить время» в Интернете, а активно пользоваться полезными возможностями Сети.

Тем не менее, есть и несколько технологических и методологических основ, рекомендуемых настоящим пособием, которые необходимо знать и выполнять учителю.

Основная программа, первой устанавливаемая на компьютер и определяющая в числе прочего особенности работы с сетью Интернет, называется «Операционная система». Распространены и используются операционные системы семейства Windows компании Microsoft, разновидности Linux и семейство MacOS. В случае если ваши учебные, домашние или рабочие компьютеры используют в качестве операционной системы Windows, то риск заражения компьютера нежелательной или вредоносной программой существенно выше, чем у компьютеров, использующих в качестве операционной системы семейство MacOS или Linux. Архитектура операционных систем MacOS и Linux изначально разрабатывалась в соответствии с явным разделением прав и возможностей для всех прикладных программ. То есть на бытовом уровне можно сказать, что компьютеры под управлением операционной системы семейства MacOS и Linux не подвергаются заражению вирусами. Что, несомненно, является привлекательным фактором для использования данных систем для работы в Интернете. Однако повседневное использование подобных систем по широкому кругу задач требует определенной подготовки и наличия специальных умений и навыков в связи с не очень широкой распространенностью и методологической подготовленностью использования компьютеров с операционными системами MacOS и Linux в России.

Компьютеры под управлением операционной системы семейства Windows на этапе проектирования предусматривали максимальное удобство использования всех программ, не делая разделения на «правильные» и «неправильные», что привело к возможности заражения вирусами и другими нежелательными программами. Поэтому оправданным требованием к компьютерам, оснащённым системой Windows, является обязательная установка программ антивируса и сетевого «защитника» – иначе называемого брандмауэр или фаервол. В настоящее время производители программ антивирусов объединяют свои программы с возможностями «защитника» от заражения нежелательными программами, такими как «черви», «трояны». Подобные программы широко представлены на рынке программного обеспечения и предлагаются для свободного домашнего использования. Под домашним использованием понимается установка на один компьютер и регистрация по адресу электронной почты. Среди отечественных производителей известны «Лаборатория Касперского», «Доктор Веб», среди иностранных – Eset Nod32, Avast, Avira и другие. В случае если в вашем учебном заведении все компьютеры подключаются к сети через один шлюз, возможна установка одной серверной программы антивируса / фаервола на компьютер шлюза-выхода в Интернет.

К сожалению, установка и использование программ антивируса / фаервола не гарантирует непроникновения на ваш компьютер вирусов. Во-первых, вы используете во время учебы переносные устройства – флеш-карты, CD или DVD-диски, которые могут быть заражены вирусами. Есть общее правило: все, что вы скачиваете из Интернета, приносите на диске или флеш-карте, перед использованием обязательно проверяйте программой антивируса. Если программа браузера интернет-страниц задает вопрос при открывании неизвестного файла «Открыть или скачать на компьютер?», обязательно скачивайте во временную папку на вашем компьютере и проверяйте этот файл антивирусом. Во-вторых, вирусные программы постоянно усложняются и изменяются, и с ними могут не справиться даже установленные на ваши компьютеры антивирусные программы. Поэтому постоянно обновляйте базы своих антивирусных программ. Как правило, в настройках программ делается установка на постоянное периодическое обновление баз.

Вредоносные программы, кроме нанесения вреда хранящимся на компьютере данным, могут снижать скорость работы в Сети и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Суммируем вышесказанное по пунктам.

1. Установите на все домашние и школьные компьютеры специальные защитные программы, почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за интернет-активностью и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

3. Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не использовать нелицензионные программы, в том числе скачанные из Интернета.

4. Периодически старайтесь полностью проверять свои рабочие компьютеры.

5. Делайте резервную копию важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жёстком диске.

6. Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли. То есть пароль должен быть не меньше 6 знаков, с использованием букв, в том числе заглавных, а также – цифр.

Для наглядности в классе сделайте вместе с ребятами специальный стенд с памяткой по безопасному поведению в Интернете (см. Приложение №1) и периодически обновляемым материалом по данной теме. Этот стенд можно сделать в классе детей любого года обучения – с 1-го до 11-го. Но обязательно совместно с учениками. Продумайте обновляемую часть стенда. Это могут быть новости с игровых и досуговых сайтов для младших классов и новинки мира программ, геймерские новости, забавные случаи социальных сетей, интернет-юмор и курьёзы – для более старших школьников. Облегчённый контент будет уравновешивать дидактический характер памятки, но всё же будет заставлять постоянно обращаться к ней как к информации, соседствующей с забавным и постоянно обновляемым блоком.

С первых дней пребывания школьника в учебном заведении, находясь в тесном контакте с родителями (а именно в начальной школе контакт с родителями бывает наиболее частным и плотным, к старшим же классам он естественно ослабевает), постоянно ведите с родителями разъяснительную работу по проблеме безопасности ребёнка в Интернете. Об этом подробнее будем говорить далее.

2. Методические рекомендации для учителей начальной школы

С 1 сентября 2011 года все образовательные учреждения России переходят на новый федеральный государственный образовательный стандарт начального общего образования (ФГОС НОО). А с 1 сентября 2012 года все первоклассники начнут учебный год с ноутбуком или планшетником на своём учебном месте.

Важным элементом формирования универсальных учебных действий (УУД) обучающихся на ступени начального общего образования, обеспечивающим его результативность, являются ориентировка младших школьников в информационных и коммуникативных технологиях (ИКТ) и формирование способности их грамотно применять в учебе и на практике (ИКТ-компетентность). Использование современных цифровых инструментов и коммуникационных сред указывается как наиболее естественный способ формирования УУД.

Реализация программы формирования УУД в начальной школе – ключевая задача внедрения нового образовательного стандарта. Отличительной особенностью начала обучения является то, что наряду с традиционным письмом ребенок сразу начинает осваивать клавиатурный набор текста.

Ряд дисциплин начального образования позволяет привлекать использование Интернета для осуществления учебной деятельности. Изучение окружающего мира предполагает не только изучение материалов учебника, но и наблюдения и опыты, проводимые с помощью цифровых измерительных приборов, цифрового микроскопа, цифрового фотоаппарата и видеокамеры. Наблюдения и опыты фиксируются, их результаты обобщаются и представля-

ются в цифровом виде.

Изучение искусства предполагает изучение традиционных видов искусства наравне с современными, в частности, цифровой фотографии, видеофильма, мультипликации.

В контексте изучения всех предметов должны широко использоваться различные источники информации, в том числе в доступном Интернете.

В современной школе широко применяется проектный метод. Средства ИКТ являются наиболее перспективным средством реализации проектной методики обучения. Имеется цикл проектов, участвуя в которых дети знакомятся друг с другом, обмениваются информацией о себе, о школе, о своих интересах и увлечениях. Это проекты «Я и мое имя», «Моя семья», совместное издание азбуки и многое другое.

Интегрированный подход к обучению, применяемый при создании нового стандарта, предполагает активное использование знаний, полученных при изучении одного предмета, на уроках по другим предметам. Так, если на уроке русского языка идет работа над текстами-описаниями, то эта же работа продолжается на уроке окружающего мира, например, в связи с изучением времен года. Результатом такой деятельности может стать, к примеру, видеорепортаж, описывающий картины природы, природные явления и т. п. Но неизменным для всех предметных уроков является необходимость школьника начальных классов пользоваться информационными ресурсами Интернета.

Хотя дети в этом возрасте уделяют Интернету мало внимания, онлайновые изображения и звуки могут стимулировать воображение и развивать фантазию.

У детей этого возраста обычно открытая натура и положительный взгляд на мир. Они гордятся приобретенным умением читать и считать и любят делиться идеями. Они не только хотят вести себя хорошо, но и доверяют авторитетам и редко в них сомневаются.

Дети могут быть очень способными в играх, выполнении команд на компьютере и работе с мышью. Однако они сильно зависят от взрослых при поиске сайтов, интерпретации информации из Интернета или отправке электронной почты.

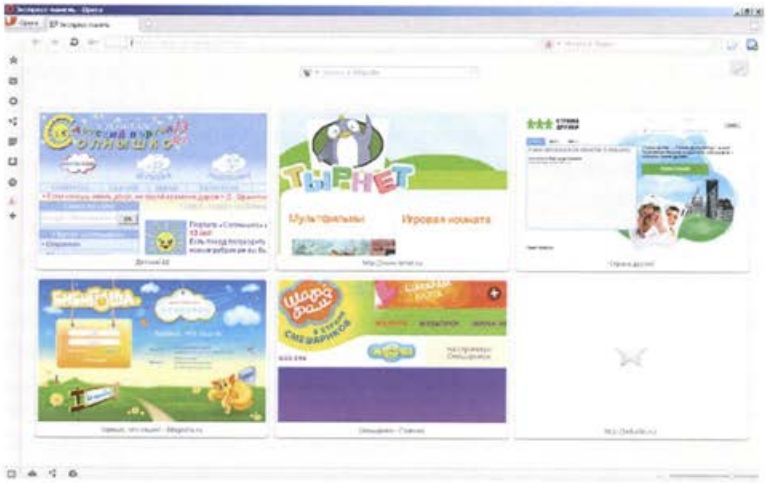
Необходимо обращать повышенное внимание на нравственное воспитание младших школьников.

Дети этого возраста должны выходить в Интернет первоначально только под присмотром учителей или родителей на сайты, которые соответствуют возрасту и культурному развитию ребенка.

Информационная политика учебных учреждений, как правило, жестко регламентируется. То есть учителя не имеют возможности устанавливать на школьные компьютеры различные программы и производить настройки. Однако учителя-предметники должны иметь представление о безопасном использовании Интернета для возможного изменения информационной

политики своего учебного заведения и для организации рекомендаций при общении с родителями учеников. Дальнейшая рекомендация предназначена для учителей начальных классов с учетом вышесказанного.

Если вы по каким-то причинам решили, что ребенок младшего возраста должен иметь доступ в Интернет, то для комфортного и безопасного способа, позволяющего просматривать интернет-страницы, можно установить специальный детский браузер Gogul.tv, который является дополнением к известному браузеру Firefox. На странице www.gogul.tv достаточно подробно рассказывается о возможностях и правилах использования данной программы. Если же вы решили использовать стандартные браузеры, то можно порекомендовать программу Opera с настроенной экспресс-панелью. Экспресс-панель представляет собой панель закладок на интернет-ресурсы в виде очень крупных и четких значков, по которым невозможно промахнуться курсором.



Закладки вы определяете сами, тем самым задавая страницы, которые может посещать ребенок. Подобие экспресс-панели под названием Fast Dial или Speed Dial существует у браузеров Firefox и Chrome, но с меньшей четкостью изображения.

Несмотря на то что системой закладок, представленной на экспресс-панели, вы задаёте интернет-ресурсы, которые рекомендуете детям для посещения, установите, настройте и используйте средства блокирования нежелательного материала (например, отечественные ICensor, NetPolice, KidGid или иностранные локализованные программные продукты, такие как ContentKeeper, K9 Web Pro-

tection и другие) как дополнение, но не замену непосредственному родительскому контролю и надзору (Приложение 4).

Принцип работы этих программных систем основан на составлении так называемых «чёрных» и «белых» списков, которые предлагаются разработчиками, но и вы сами можете дополнять и изменять их. В списки входят слова, нежелательные для прочтения, и, соответственно, происходит блокирование просмотра интернет-страницы, содержащей «запрещённые» слова. К сожалению, рисунки, фотографии или видео- и флеш-ролики невозможно таким образом блокировать, если только они не содержат в описании текст, сопровождаемый «запрещёнными» словами. Доступ к управлению подобными программами-фильтрами осуществляется по паролю, который вы должны запомнить и записать, но не сообщать детям. Удаление подобных программ возможно только по данному паролю, поэтому ваш ребёнок без пароля не сможет остановить или удалить фильтр.

К сожалению, даже на рекомендованных детских интернет-ресурсах бывает размещена реклама, содержащая непристойные или даже запрещённые изображения. Программы-фильтры работают, как было указано, только по словам и не имеют возможности блокировать просмотр подобных интернет-страниц.

Также существует встроенная в операционные системы или программы-фильтры и защитные программы возможность «родительского контроля». Это позволяет ограничить по времени использование компьютера ребёнком. Например, вы можете задать только два часа каждый день – с 12.00 до 14.00 –

Наркотики

Интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья».

Сайты знакомств, социальные сети, блоги и чаты

Виртуальное общение разрушает способность к общению реальному, модифицирует и дисгармонирует коммуникативные навыки, которые мы естественно приобретаем в процессе социализации в живом человеческом общении.

Секты

Виртуальный собеседник не схватит за руку, но ему вполне по силам «проникнуть в мысли» и повлиять на взгляды на мир.

Экстремизм, национализм, фашизм

Все широкие возможности Интернета используются представителями экстремистских течений для того, чтобы заманить в свои ряды новичков.

Прежде всего надо разобраться с рассчитанными на детей поисковыми машинами или поисковыми машинами с фильтрами информации.

Все вышеизложенные технические и методологические рекомендации для школьников младшего школьного возраста остаются в силе и для подростков.

Но это не панацея от всех бед, ибо подчас школьники являются гораздо более продвинутыми пользователями, способными обойти любые ограничения по сёрфингу в Интернете. Более того, с определённого возраста они, наоборот, активно противятся любым ограничениям, в том числе и ограничениям, связанным с Интернетом. Поэтому фильтры – это лишь временная и не слишком эффективная мера. Прежде всего необходимо усилить воспитательные меры работы с учениками: говорить с ними на языке, показывающем, что вы более или менее «в материале», то есть пользуетесь Интернетом и знаете о нём, об особенностях работы в Сети, о специфике и опасностях сетевого общения и пр. Для этого вам необходимо стать если не продвинутым пользователем, то, во всяком случае, хотя бы просто регулярным пользователем Интернета и сетевых сервисов: социальных сетей, чатов, форумов профессиональной направленности или связанных с вашими личными увлечениями. Но, помимо этого, надо стараться отслеживать появление новых тенденций в Сети, заглядывая на те сайты, о которых вы можете узнать от своих учеников. Старайтесь наладить с ними виртуальное общение по электронной почте, по skype, задавайте им задания, связанные с необходимостью налаживания такого рода общения. Например, преподаватель биологии может попросить своих учеников,

для использования компьютера ребенком для выхода в Сеть.

Когда маленькие дети начинают осваивать Сеть, остальные члены семьи должны служить для них примером.

Расскажите детям о недоверии к неизвестному собеседнику и конфиденциальности. Если на сайте необходимо, чтобы ребёнок придумал себе логин, или так называемое «имя пользователя», помогите ему выбрать псевдоним, не раскрывающий никакой личной информации.

Невозможно закрыть все ресурсы, содержащие негативный контент, и полностью оградить ребёнка от столкновения с вредоносным содержимым, но возможно предупредить его, научить справляться с угрозой и в спорных ситуациях в первую очередь обращаться за помощью к взрослым.

Использование даже специальных детских социальных сетей или детских многопользовательских игр позволяет ребёнку общаться с неизвестными участниками, среди которых могут оказаться не только дети, но и социально нежелательные личности.

Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Итак, резюмируем всё вышеизложенное.

1. Перед первым выходом вашего ученика в Интернет как можно чётче оговорите правила пользования Сетью. Обсудите с ребенком, куда ему можно заходить (возможно, на первых порах стоит составить список сайтов), что можно и что нельзя делать, сколько времени можно находиться в Интернете.

2. Сообщите ему о том контроле, который вы намерены осуществлять: проверка посещённых ребёнком страниц, контроль времени, проведённого в Сети, проверка адресов электронной почты. Объясните ребёнку, что вы доверяете ему и заботитесь о его безопасности.

3. Договоритесь с ребёнком о соблюдении им следующих правил:

- сообщить родителям своё регистрационное имя и пароль, если ребёнку разрешено участвовать в чатах или блогах, e-mail адрес и пароль почтового ящика;
- никому, кроме родителей, эти сведения сообщать категорически нельзя;
- не сообщать без разрешения родителей для каждого отдельного случая личную информацию (домашний адрес, номер телефона, номер школы, место работы родителей);
- не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет;
- сразу обратиться к родителям, если ребенок увидит нечто неприятное,

тревожащее, угрожающее на сайте или в электронной почте;
- не соглашаться лично встретиться с человеком, с которым ребёнок познакомился в Сети;
- если кто-то предлагает ребёнку какой-то необычный «секрет», тут же сообщить об этом родителям;
- не скачивать, не устанавливать, не копировать ничего с дисков или из Интернета без разрешения родителей на каждый отдельный случай;
- не делать без разрешения родителей в Интернете ничего, что требует оплаты;
- проявлять уважение к собеседникам в Интернете, вести себя так, чтобы не обидеть и не рассердить человека.

4. В течение некоторого времени сопровождайте ребенка в его путешествиях по Сети для того, чтобы убедиться, что ребенок соблюдает ваш уговор.

5. Периодически проверяйте в браузере журнал посещённых ребёнком интернет-страниц. Конечно, журнал можно очищать, но не всякий ребёнок умеет это делать.

3. Методические рекомендации для учителей средней школы

Именно с переходом в возрастную категорию «подросток» проблемы, связанные с Интернетом, становятся действительно острыми и глобальными. Что же это за проблемы, с которыми именно школа должна вовремя сразиться и постараться их вовремя локализовать? И как именно это должно происходить?

Дополнительная психологическая и социальная проблема детей подросткового возраста заключается в возрастном становлении характера и скептическом и недоверчивом отношении к замечаниям и рекомендациям родителей и учителей. А техническая подготовленность к использованию возможностей сети Интернет уже достаточна высока на фоне несформировавшейся психики и неустойчивого социального поведения школьников средней школы.

Что же подстерегает детей подросткового возраста, проводящих у компьютера достаточно много времени, с экрана монитора?

Порнография

Опасна избыточной информацией и грубым, часто извращённым, натурализмом. Мешает развитию естественных эмоциональных привязанностей.

Депрессивные молодежные течения

Ребенок может поверить, что шрамы – лучшее украшение, а суицид – всего лишь способ избавления от проблем.

посадивших семена огородных растений дома для домашнего наблюдения за их ростом, присылать фотографии стадий роста растений по электронной почте. Таким образом, отрабатываются не только домашние задания непосредственно по программе курса, и имеет место внедрение ИКТ в образовательный процесс, но и формируется элемент электронной учебной коммуникации с преподавателем, повышающий авторитет учителя и заставляющий ученика осознанно работать с образовательными возможностями ИКТ.

Одна из основных проблем современных подростков, связанная именно с развитием цифровых коммуникаций, – это коммуникативный дисбаланс. Почти все современные дети говорят, что у них нет друзей в школе, во дворе, где они должны бы гулять, как это было раньше, даже в кружковых и хобби-секциях. Есть сверстники, с которыми они общаются на уровне «здравствуй – до свидания». Но друзей или хотя бы приятелей – нет. В то же время в социальных сетях у этих же самых подростков десятки, а то и сотни «френдов», которыми они гордятся и с которыми часами готовы общаться, не выключая настольного компьютера даже тогда, когда делают уроки, не связанные с поиском информации в Сети. И это является огромной социальной и психологической проблемой для всего общества. Бороться с этим трудно, если не сказать более – бесполезно. Можно лишь чуть корректировать ситуацию. И, самое главное, постараться обеспечить безопасность ребёнка в этом вопросе. Для этого надо постоянно говорить с ребёнком об этом в школе и дома. Что же надо знать самому учителю и рассказать в классе в первую очередь?

Преступники устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются прельстить свою цель вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей.

Некоторые преступники действуют быстрее других и сразу же заводят сексуальные беседы. Такой более прямолинейный подход может включать решительные действия или скрытое преследование жертвы. Преступники могут также рассматривать возможность встречи с детьми в реальной жизни.

Кому из молодых людей угрожает опасность?

Подростки являются наиболее уязвимой группой и подвергаются наибольшей опасности. Подростки стремятся исследовать свою сексуальность, уйти

из-под контроля родителей и завязать новые отношения вне семьи. Несмотря на то что общение в Интернете может быть полностью анонимным, они больше подвержены опасности, даже если до конца не осознают возможные последствия.

Молодые люди, наиболее уязвимые для злоумышленников, – это, как правило:

- новички в Интернете, не знакомые с сетевым этикетом;
- недружелюбные пользователи;
- те, кто стремится попробовать всё новое, связанное с острыми ощущениями;
- активно ищущие внимания и привязанности;
- бунтари;
- одинокие или брошенные;
- любопытные;
- испытывающие проблемы с сексуальной ориентацией;
- те, кого взрослые могут легко обмануть;
- те, кого привлекает субкультура, выходящая за рамки понимания их родителей.

Универсальных рецептов избежать всех вышеперечисленных проблем нет и быть не может. В этой работе важнее всего согласованная работа школы и родителей и усиление воспитательной общегуманитарной работы. Что является идеалом, скорее всего, недостижимым. Существует весьма ограниченное количество плодотворных гуманитарноцентричных способов организации использования интернет-возможностей в образовании. Одним из эффективных способов является метод высокотехнологичных учебных проектов.

Учителю любой дисциплины необходимо инициировать большие и малые телекоммуникационные учебные проекты.

Учебный телекоммуникационный проект – это совместная учебно-познавательная, творческая или игровая деятельность учащихся-партнеров, организованная на основе компьютерной телекоммуникации, имеющая общую цель, согласованные способы деятельности, направленная на достижение общего результата деятельности.

Метод проектов как совокупность определенных действий, документов, замыслов для создания реального объекта в результате творческой деятельности способствует

– формированию базовых знаний, умений и навыков;

– устойчивой мотивации и ощущению потребности в приобретении новых знаний, необходимых для реализации проекта;

– активизации познавательной деятельности учащихся;

– развитию творческих способностей, позволяющих реализовать проектную задачу в соответствии с собственным видением;

– воспитанию инициативности;

– рефлексии учащихся при осознании себя творцами новых знаний.

Именно такого рода мультимедийные телекоммуникационные проекты и стали основным вектором научной работы авторов данного пособия.

Школьной проектной деятельностью учитель решает сразу несколько проблем:

во-первых, учащиеся приобретают навык практического применения полученных теоретических знаний по использованию компьютеров, компьютерных технологий и Интернета;

во-вторых, и это самое главное, школьник начинает видеть в компьютере и Интернете не только игрушку и поток непотребных ресурсов, но инструмент создания нового, интересного и нужного не только ему, но и окружающим его в школе и дома людям пространства. И в этом пространстве ребёнок подобен творцу: каким он его создаст, таким его мир и будет. Будь то красивый проект по рыбкам или птичкам, по панк-группам или готам, эмо, другим молодёжным субкультурам, или это предметно-ориентированные ресурс по литературе, математике и пр. Ребёнок должен сам выбрать то, что в данный момент его больше всего волнует и захватывает. Но выбрать под чутким руководством и при ненавязчивой корректировке учителя. Для ребёнка это форма откровенного разговора с одноклассниками и учителями, которым интересно и важно узнать об увлечениях и мыслях конкретно этого маленького, но чрезвычайно значимого для окружающих человека. Для учителя это форма современной коммуникации со своим учеником и поле для воспитательной работы с ним.

Лучше всего инициировать глобальный (на один или несколько классов) проект, связанный с усиленной необходимостью коммуникации. То есть каждый школьник выполняет часть работы по общему учебному телекоммуникационному проекту. Чем глобальнее и трудозатратнее проект, тем лучше. Надо добиваться того, чтобы школьнику просто некогда было бы заниматься в Интернете чем-то иным, кроме работы по реализации проекта. Для этого проект должен быть

а) интересен самим детям и, желательно, и предложен же ими, чтобы они позднее не могли отказаться от того, что сами же и предложили;

б) очень высокотехнологичным, чтобы для его реализации школьнику было необходимо полностью проявить свою компьютерную «продвинутость», да ещё и подучиться разным сложным технологиям, общаясь со своими виртуальными друзьями: здесь пройдёт естественный отсев пустопорожних коммуникаций в социальных сетях: человеку творческому некогда и не о чем разговаривать на уровне междометий о несущественных пустяках;

в) долгосрочным и предусматривающим дальнейшее коммуникативное

дополнение. Необходимо разместить проект хотя бы на специально организованной странице школьного сайта или не пожалеть времени и средств (родители, думаю, не откажутся поучаствовать в этом) и зарегистрировать отдельно наиболее значимый ресурс. И после размещения его в Сети у детей, гордящихся проделанной работой, должен быть стимул общаться в Интернете на тему своего проекта и постоянно дополнять и дорабатывать его.

Для этого же очень важно устраивать публичные показы проектов школьников на классных часах, на предметных уроках, в рамках программы которых сделаны эти проекты.

Итак, что учитель должен сказать своим ученикам?

– Относись к информации осторожно. То, что веб-сайт эффектно выглядит, еще ни о чём не говорит. Спроси себя: для чего этот сайт сделан? В чём меня хотят убедить его создатели? Чего этому сайту недостает? Узнай об авторах сайта: зайди в раздел «О нас» или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надёжный, например, университет, то вполне возможно, что информации на сайте можно доверять.

– Часто в Сети можно столкнуться с подделками под известные сайты социальных сетей или почтовых сервисов, так называемым «фишингом». После неосторожного ввода имени пользователя и пароля на страницах ненастоящих, поддельных сайтов, злоумышленники используют пароли в своих целях на реальных сайтах. Например, для рассылки спама от имени владельца почтового ящика или злоумышленного обращения в социальных сетях от имени владельца аккаунта. Каждый сайт в Интернете имеет свой уникальный адрес. Необходимо проверять именно адрес страницы, не доверяя внешнему оформлению, которое может быть скопировано с оригинального.

– Используя информацию из Интернета в своей работе, следуй правилу трёх источников: организуй поиск и сравни три разных источника информации, прежде чем решить, каким источникам можно доверять. Не забывай, что факты, о которых ты узнаешь в Интернете, нужно очень хорошо проверить, если ты будешь использовать их в своей работе.

– Хотя Интернет – специфическая среда для общения, в ней существуют определённые правила вежливости, которые широко обсуждаются в Интернете, но, к сожалению, культура общения остается на низком уровне. В Сети нередко можно наблюдать грубость, речевую агрессию, нетерпимость к чужим мнениям. Желательно сохранять правила человеческого общения даже в случае анонимной коммуникации. На эмоциональное послание лучше отвечать не мгновенно, а через некоторое время, чтобы не плодить излишний негатив в общении.

Работая в Интернете, учащиеся обязательно должны столкнуться с проблемой

виртуального общения (чат, форум, электронная почта, телеконференции). Если мы общаемся с незнакомыми людьми, то возникает ситуация разговора с виртуальными личностями. Человек может изменять свой статус, скрывать возраст, пол, преувеличивать силу, красоту, а также почти безнаказанно проявлять агрессивные черты характера, которые он вынужден подавлять в повседневной жизни. Для того чтобы избежать отрицательных последствий общения в Интернете, следует придерживаться определенных правил:

1) не нужно слепо верить в то, что собеседник говорит о себе;

2) следите за своими словами (не употребляйте грубых выражений);

3) не сообщайте незнакомому лично человеку ваш домашний адрес, телефонный номер;

4) если вы чувствуете дискомфорт в общении, уходите.

Можно предложить учащимся составить свои принципы общения в Интернете.

Рассмотрите совместно с учащимися подробнее неформальный кодекс поведения в сети Интернет, регулирующий общение пользователей друг с другом и так называемый нетикет (netiquette – от слияния англ. слов net – сеть и etiquette – этикет), или сетевой этикет. Сетевой этикет – это некоторое количество базовых правил поведения в Сети, однако эти правила время от времени подвергаются изменениям, что-то устаревает и теряет свою актуальность в связи с развитием интернет-технологий, а что-то добавляется новое.

Сетевой этикет регулирует

- правила обмена сообщениями по электронной почте,
- стилистику сетевой коммуникации при коллективных обсуждениях,
- общие правила написания публикуемых текстов в Сети и пр.

При переписке по электронной почте каждый пользователь должен помнить о некоторых правилах:

– Приветствуйте собеседника в начале письма и прощайтесь в конце.

– По электронной почте можно обращаться к незнакомым людям, но при условии, что адрес был опубликован его владельцем.

– Пишите кратко, грамотно и аккуратно.

– Отвечая на сообщение, необходимо цитировать его наиболее существенные места.

– Удобно, когда письма пользователя заканчиваются краткой «подписью», автоматически добавляемой к каждому сообщению, отправляемому пользователем, однако эта подпись не должна быть длиннее четырех – пяти строк. Очень важно указать в подписи своё имя-отчество полностью, чтобы получателю было удобно обратиться к вам. Если указаны только инициалы, то

отвечающему придётся искать имена в других источниках, на это потребуется время. Подразумевать же, что все точно помнят наше имя-отчество, – это неверно. У всех свои особенности памяти и объёмы информации, а также круг общения. Например:

С уважением,
Комарова Наталия Ивановна,
старший научный сотрудник Научно-исследовательского института столичного образования ГОУ МГПУ.

E-mail: N.Komarova@mail.ru

– В переписке личного характера можно придерживаться разговорного стиля.

– Не следует переправлять чьё-то личное сообщение другим людям или в телеконференцию без предварительного согласия его автора.

– Если вы заняты и не можете быстро ответить на поступившее сообщение, отправьте пару строк с подтверждением получения и обещанием ответить при первой возможности.

– Если сообщение поступило от незнакомого лица, следует понять, обосновано оно или нет. В первом случае – ответить в течение трех дней. Во втором – не отвечать.

– Текст письма нужно структурировать по смыслу, абзацы отделять пустой строкой.

– Если вы отправляете заархивированный файл, поинтересуйтесь заранее, сможет ли получатель письма его распаковать (то есть имеет ли он на своем компьютере нужную программу-архиватор). Предпочтительным является использование zip-архивации как наиболее распространённой.

– Строка текста должна ограничиваться 60–70 символами, справа без выравнивания.

– Нежелательно посылать письма большого объема – около одного мегабайта, поскольку пользователь, работающий с бесплатным почтовым ящиком, может такое послание не прочитать из-за ограничений на объем входящей корреспонденции.

– К незнакомым людям можно обращаться с просьбами о консультации, с вежливыми предложениями и пожеланиями, не претендуя на получение ответа.

– Неполучение ответа следует рассматривать как нежелательность или невозможность установления контакта и повторять не следует.

– При обращении к незнакомым людям следует воздерживаться от просьб, вызывающих необходимость использования других средств связи, отличных от электронной почты.

– Если в письмо вложен файл, то в тексте письма обязательно должно был указано, что приложено и зачем.

- Будь ответственным и в реальной жизни, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайне.
- Не занимайся плагиатом. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его – спроси разрешения. Иногда достаточно указать ссылку на использованный источник.
- Сообщая учителям или родителям о неприемлемом контенте, ты помогаешь делу безопасности Сети.
- Когда ты грубишь в Интернете собеседнику, ты провоцируешь его на такое же поведение. Попробуй оставаться вежливым или просто не реагировать.
- Всё, что ты размещаешь в Интернете, навсегда останется с тобой, как татуировка. Только ты не сможешь эту информацию удалить или контролировать её использование. Ты ведь не хочешь оправдываться за свои фотографии перед будущим работодателем? Подумай, прежде чем разместить в Интернете какую-то интимную или персональную информацию о себе.

4. Работа с родителями

Специальные классные часы необходимо посвятить беседам с родителями о правилах обеспечения безопасности их детей в работе с Интернетом дома. И хотя многие родители считают себя продвинутыми пользователями и уверены в том, что с их детьми ничего плохого в Сети произойти не может, это не так. Даже такие родители должны понимать, что выскакивающие сами по себе рекламные баннеры порносайтов, навязчивые торговые слоганы и призывы получить «бесплатно» рецепт для похудения – это опасные ловушки прежде всего для их не подготовленных пока к социально агрессивному миру Интернета детей.

Что родители могут сделать для повышения безопасности пребывания своих детей в сети Интернет? Действия родителей должны быть скоординированы с рекомендациями учителей.

Надо напомнить родителям о том, чтобы они, подтверждая информацию, данную учителем, также рассказали своим детям о существовании злоумышленников и о потенциальных опасностях Интернета.

Надо спросить родителей: вот вы, родители, на данный момент знаете, какими сайтами пользуются ваши дети? Нет? Очень печально. Именно с этого надо начинать работу с безопасным Интернетом.

В Интернете пользователя-подростка могут обидеть, запугать или даже оскорбить. Лучшей защитой является руководство собственным здравым смыслом. Наиболее важной задачей является предупреждение детей

об опасностях Интернета, неоднократное напоминание о том, чтобы они вели себя осторожно. Кроме того, необходимо обсуждать с детьми все вопросы, которые могут у них возникнуть при использовании Интернета. Не только учитель, но и родители не должны дистанцироваться от вопросов детей, а, наоборот, надо стараться максимально завоевать их доверие, постоянно интересуясь их времяпрепровождением в Сети. Тогда вы будете в курсе той информации, которой владеют ваши дети.

Даже если ребенок не сталкивался с оскорблениями в Интернете, рекомендуется объяснить ему следующее.

- Не распространяй контактную или личную информацию, например, фотографии, без тщательного обдумывания возможных последствий. Сетевая дружба может закончиться, а личная информация может быть скопирована и использована злоумышленниками.
- В Интернете, как и в жизни, каждый человек имеет право на уважительное отношение.
- Лучше человеческие отношения переносить в сетевое общение, а не наоборот.
- Родители — твои друзья, которые больше всех заинтересованы в физическом и эмоциональном здоровье ребенка.

КРАТКОЕ ИЗЛОЖЕНИЕ. ОСНОВНЫЕ ВОЗРАСТНЫЕ РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ПОЛЬЗОВАНИЮ ИНТЕРНЕТОМ

Дети до 7 лет

Во время первого знакомства с Интернетом закладывается фундамент для его последующего использования и формирования хороших манер у детей. Детям дошкольного возраста нравится установленный порядок, и это является идеальным способом развития у детей навыков безопасного использования Интернета.

Дети до 7 лет могут не полностью понимать информацию, доступную в Интернете, и, например, не отличать рекламу от действительного содержимого. В этом возрасте родителям необходимо помогать детям в поиске подходящего материала. Дети часто не видят разницы между использованием Интернета и играми или рисованием на компьютере.

На этом этапе вы можете установить первые внутренние правила использования компьютера и Интернета.

Время, проводимое за компьютером, необходимо ограничить по причинам, связанным со здоровьем.

Поместите компьютер, например, в гостиной. При использовании Интернета дошкольниками рекомендуется присутствие взрослого.

Доступ к Интернету для дошкольников необходимо ограничить до списка знакомых веб-сайтов, выбранных заранее. Более подготовленные дети могут найти знакомые сайты в меню «Избранное» обозревателя Интернета.

Самым безопасным решением является создание для ребенка персональной рабочей среды, в которой выбор сайтов ограничивается только указанными сайтами.

Дети 7–9 лет

Юные школьники имеют дело с Интернетом не только у себя дома, но и в школе и у друзей. Родители вместе с детьми должны обсудить, как использовать Интернет надлежащим образом, и согласовать правила, которым необходимо следовать. Дети 7–9 лет уже могут иметь относительно хорошее представление о том, что они видят. Тем не менее, они не готовы к обращению со всем материалом, доступным в Интернете, особенно с эмоционально вызывающим или неуместным материалом (изображения, текст или звук). Разговор об этих материалах и объяснение различных вещей, с которыми дети могут столкнуться в Интернете, поможет детям более осмысленно и безопасно работать в Интернете. Родители могут поделиться собственными мнениями и взглядами на использование Интернета, чтобы помочь своим детям.

В этом возрасте ограничения, защита и использование Интернета под

присмотром по-прежнему являются первостепенными. Родителям и детям рекомендуется согласовать правила использования Интернета и пересматривать их по мере взросления детей.

Использование Интернета дома по-прежнему разрешено только в присутствии родителей. Это обеспечивает получение помощи в любой проблемной ситуации.

Сделайте естественным использование Интернета путём установки компьютера в комнате, которой пользуется вся семья.

Ребёнок ещё не может определить надёжность веб-сайта самостоятельно, поэтому родители должны контролировать публикацию личной информации в Интернете.

Для предотвращения доступа к неуместным сайтам можно также применять программы фильтрации (см. выше), но важно, чтобы родители по-прежнему активно участвовали в использовании Интернета ребенком.

Дети 10–12 лет

Школьники, как правило, умеют пользоваться Интернетом. Родители могут поддержать ребенка, выяснив, какие сайты могут помочь с домашним заданием, содержат информацию о хобби или других увлечениях ребенка. Интернет может также использоваться для решения вопросов, касающихся всей семьи. Это дает возможность родителям и детям обсудить надежность разных сайтов, а также источники поиска полезной и качественной информации.

Ребёнку необходим родительский присмотр и контроль, а также знание правил безопасной работы в Сети. Тем не менее, ребёнок может узнать, как избавиться от присмотра и обойти правила, если он будет считать их слишком ограничивающими его свободу или не соответствующими его потребностям.

Родителям и детям необходимо прийти к соглашению относительно разрешённых и запрещённых действий в Интернете, а также его использования. В соглашении должны быть учтены все потребности и мнения. Объясните родителям, что необходимо «по-взрослому» договориться с детьми, какую личную информацию можно разглашать и в каких случаях, а также поговорить об опасности размещения личной информации. Если ребенок уже заинтересовался общением на форумах или в социальных сетях, родителям следует обсудить с детьми безопасность и комфортность общения и продолжать проявлять внимание, соответствующее возрасту, и контролировать их.

Многие дети любопытны и любознательны, поэтому родителям необходимо акцентировать внимание на необходимости осторожного и корректного использования информации, взятой в Интернете.

Дети 13–15 лет

В этом возрасте Интернет становится частью социальной жизни детей:

в Интернете они знакомятся и проводят время, ищут информацию, связанную с учебой или увлечениями. При более высоком уровне компьютерной грамотности использование Интернета открывает множество возможностей. Родителям уже может быть сложно узнать о том, чем их ребенок занимается в Интернете. В этом возрасте дети также склонны к риску и выходу за пределы дозволенного. Технические ограничения и запреты могут оказаться неэффективным способом повышения уровня безопасности в Интернете.

Дети 13–15 лет могут захотеть сохранить свои действия в тайне, особенно если родители раньше не интересовались и не узнавали о способах использования Интернета ребенком. Важным моментом для всей семьи становится участие в открытых дискуссиях, а для родителей – заинтересованность в том, что ребенок делает и с кем и для чего использует интернет-ресурсы.

По-прежнему важным остается принцип доверия подростка к родителям и учителям при решении проблем, вызванных использованием Интернета.

Нижеследующие рекомендации относятся как родителям, так и учителям.

1. Убедите своих детей делиться с вами впечатлениями от работы в Интернете. Выберите время для неконфликтного совместного просмотра интернет-страниц.
2. Научите детей доверять интуиции. Если что-нибудь в Интернете будет вызывать у них психологический дискомфорт, пусть дети рассказывают вам об этом.
3. Если ваши дети регистрируются на форумах, в чатах или сетевых играх, что требует указания идентификационного имени пользователя, помогите им выбрать это имя и убедитесь в том, что оно не содержит никакой личной информации.
4. Запретите своим детям сообщать другим пользователям Интернета адрес, номер телефона и другую личную информацию, в том числе номер школы и любимые места для игр.
5. Объясните детям, что нравственные принципы в Интернете и реальной жизни одинаковы.
6. Научите детей уважать других пользователей Интернета. Разъясните детям, что при переходе в виртуальный мир нормы поведения нисколько не изменяются.
7. Добейтесь от детей уважения к собственности других пользователей Интернета. Расскажите детям, что незаконное копирование продуктов труда других людей, в том числе музыки, видеоигр и других программ, почти не отличается от воровства в магазине.
8. Убедите детей в том, что они не должны встречаться с интернет-друзьями лично. Скажите, что интернет-друзья могут на самом деле быть не теми, за кого

пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми.

Официально медицина пока не признала интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления.

Зависимость (наркотическая) в медицинском смысле определяется как навязчивая потребность в использовании привычного вещества, сопровождающаяся ростом толерантности и выраженными физиологическими и психологическими симптомами. Также зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определённой деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр, обжорства или гиперрелигиозности. Очевидно, его можно употреблять и при рассмотрении интернет-зависимости. Здесь характер зависимости иной, чем при употреблении наркотиков или алкоголя, то есть физиологический компонент полностью отсутствует. А вот психологический проявляется очень ярко. Таким образом, можно определить интернет-зависимость как нехимическую зависимость – навязчивую потребность в использовании Интернета, сопровождающуюся социальной дезадаптацией и выраженными психологическими симптомами.

По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4–6 %. Несмотря на отсутствие официального признания проблемы, интернет-зависимость уже принимается в расчёт во многих странах мира. Например, в Финляндии молодым людям с интернет-зависимостью предоставляют отсрочку от армии.

Основные 5 типов интернет-зависимости таковы:

1. Навязчивый веб-серфинг – бесконечные путешествия по Всемирной паутине, поиск информации.
2. Пристрастие к виртуальному общению и виртуальным знакомствам – большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.
3. Игровая зависимость – навязчивое увлечение компьютерными играми по Сети.
4. Навязчивая финансовая потребность – игра по Сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.

они себя выдают.

9. Объясните детям, что верить всему, что они видят или читают в Интернете, нельзя. Скажите им, что при наличии сомнений в правдивости какой-то информации, им следует обратиться за советом к вам.

10. Продолжайте контролировать действия своих детей в Интернете с помощью специализированного программного обеспечения. Средства родительского контроля помогают блокировать вредные материалы, следить за тем, какие веб-узлы посещают ваши дети, и узнавать, что они там делают.

11. Если ваши дети пользуются чатами, вам следует знать, какими именно и с кем они там беседуют. Лично посетите чат, чтобы проверить, на какие темы ведутся дискуссии. Внушите детям, что никогда нельзя покидать общий чат. Многие сайты имеют «приватные комнаты», где пользователи могут вести беседы наедине – у администраторов нет возможности читать эти беседы. Такие «комнаты» часто называют «приватом».

13. Компьютер, подключенный к Интернету, должен находиться в общей комнате; по возможности не устанавливайте его в спальне ребенка.

14. Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев. Если дети пользуются компьютерами в местах, находящихся вне вашего контроля: общественной библиотеке, школе или дома у друзей, – выясните, какие защитные средства там используются.

В таком возрасте подросток может столкнуться с кибермошенничеством – это один из видов киберпреступления, целью которого является причинение материального или иного ущерба путём хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

- Проинформируйте ребенка о самых распространённых методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.
- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.
- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надёжности и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности:

1. Ознакомьтесь с отзывами покупателей.
2. Проверьте реквизиты и название юридического лица – владельца

магазина.

3. Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whols).
4. Поинтересуйтесь, выдает ли магазин кассовый чек.
5. Сравните цены в разных интернет-магазинах.
6. Позвоните в справочную магазина.
7. Обратите внимание на правила интернет-магазина.
8. Выясните, сколько точно вам придется заплатить.

Объясните ребенку, что нельзя отправлять слишком много информации о себе при совершении интернет-покупок: данные счетов, пароли, домашние адреса и номера телефонов. 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.

Ещё одной немаловажной проблемой, связанной с развитием ИКТ, стала так называемая «интернет-зависимость» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимость от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты. Сейчас же это явление стало массовым социальным феноменом во всём мире.

Психологическую в своей основе интернет-зависимость сравнивают с наркоманией – физиологической зависимостью от наркотических веществ, где также присутствует психический компонент. Интернет-зависимость определяется как навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета.

Интернет-зависимость – психическое расстройство, навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. Интернет-зависимость является широко обсуждаемым вопросом, но её статус пока находится на неофициальном уровне: расстройство не включено в официальную классификацию заболеваний DSM-IV.

Информация для человека имеет огромное значение. Компьютер и Интернет являются мощным инструментом обработки и обмена информацией, кроме того, благодаря компьютеру стали доступными различные виды информации. Это и считается первопричиной компьютерной или интернет-зависимости, так как в определённом смысле они страдают нарушением процессов обмена информацией.

Проблема интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным

пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми.

Официально медицина пока не признала интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления.

Зависимость (наркотическая) в медицинском смысле определяется как навязчивая потребность в использовании привычного вещества, сопровождающаяся ростом толерантности и выраженными физиологическими и психологическими симптомами. Также зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определённой деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр, обжорства или гиперрелигиозности. Очевидно, его можно употреблять и при рассмотрении интернет-зависимости. Здесь характер зависимости иной, чем при употреблении наркотиков или алкоголя, то есть физиологический компонент полностью отсутствует. А вот психологический проявляется очень ярко. Таким образом, можно определить интернет-зависимость как нехимическую зависимость – навязчивую потребность в использовании Интернета, сопровождающуюся социальной дезадаптацией и выраженными психологическими симптомами.

По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4–6 %. Несмотря на отсутствие официального признания проблемы, интернет-зависимость уже принимается в расчёт во многих странах мира. Например, в Финляндии молодым людям с интернет-зависимостью предоставляют отсрочку от армии.

Основные 5 типов интернет-зависимости таковы:

1. Навязчивый веб-серфинг – бесконечные путешествия по Всемирной паутине, поиск информации.
2. Пристрастие к виртуальному общению и виртуальным знакомствам – большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.
3. Игровая зависимость – навязчивое увлечение компьютерными играми по Сети.
4. Навязчивая финансовая потребность – игра по Сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.

ЗАКЛЮЧЕНИЕ

Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», принятый для защиты детей от разрушительного, травмирующего воздействия информации на их психику, а также от информации, способной развить в ребёнке порочные наклонности, вступает в силу с 1 сентября 2012 года и будет распространяться на все виды информации: на СМИ, книги, аудиовизуальные произведения и интернет-порталы. В настоящее время безопасность в школах обеспечивается в основном за счёт использования чёрных и белых списков, ограничивающих доступ к негативному контенту и определяющих сайты, доступные для посещения. В дальнейшем планируется введение интеллектуальной системы оценки информации, реализуемой не только за счёт автоматического сканирования содержимого сайтов, но и за счёт экспертной оценки спорных ресурсов.

Но никакая даже самая совершенная система высокотехнологичных фильтров и программных средств не защитит нас и наших детей от ещё более быстрыми темпами развивающейся виртуальной среды глобальных компьютерных сетей. Необходимо понять несколько основополагающих моментов:

1. Остановить прогресс невозможно, и его не надо бояться. Современному учителю надо принимать информационно-коммуникационный поток с достоинством и вооружившись не только знаниями, умениями и навыками, но и компетентностью, инициативой, творческим настроем.
2. Самую важную роль в деле обеспечения безопасности детей в Интернете играет именно учитель, который выполняет функцию воспитателя не только для своих учеников, но и для их родителей.
3. Академик Н. Н. Моисеев говорил: «Когда я произношу слово «УЧИТЕЛЬ», то имею в виду не только педагогов, работающих в средней или высшей школе, а саму систему формирования, сохранения и развития коллективных знаний, нравственности и памяти народа, передачи всего накопленного следующим поколениям... Человечество подошло к порогу, за которым нужны и новая нравственность, и новые знания, новый менталитет, новая система ценностей. Кто их будет создавать и пестовать? От того, как следующие поколения смогут усвоить эту тревогу за будущее, понять и реализовать собственную Ответственность, и зависит это будущее».
4. Учителю надо понять и прочувствовать свою огромную роль в современном мире, в том числе и виртуальном, и подстраивать виртуальный мир под себя, а не самому подстраиваться под него. Ведь, в конце концов, именно мы, люди, создали этот цифровой мир. Значит, мы и в ответе за всё, что там происходит. Значит, мы можем управлять им, внося в него гармонию и красоту. Всё в наших руках!

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Ахрямкина Т. А., Матасова И. Л. Особенности проявления и факторы формирования компьютерной зависимости различных возрастных групп: методическое пособие для студентов психологического факультета и практикующих психологов. – Самара, 2005.

2. Безопасный компьютер и Интернет для детей: новая программа повышения квалификации преподавателей АПКиППРО // Microsoft в образовании [Электронный ресурс]. – Электрон. дан. – сор. 2008. – Режим доступа: http://www.ms-education.ru.

3. Бочаров М. И. Комплексное обеспечение непрерывной информационной безопасности школьников // Применение новых технологий в образовании: материалы XX международной конференции. – Троицк, 2009. – С. 17–19.

4. Ваш личный Интернет [Электронный ресурс]. – Электрон. дан. – М., сор. 2008. – Режим доступа: http://www.content-filtering.ru.

5. Гаянова Т. И. Дети в Интернете: библиотека в помощь формированию культуры использования информационного пространства Интернета // Школьная библиотека. – 2011. – № 1/2. – С. 129–136.

6. Гончаров Д. К. Веб – это платформа образования // Социология ИКТ: сборник научных статей. Выпуск 1 [Электронный ресурс]. – М., 2010. – Режим доступа: http://screen.ru/ikt.

7. Джонсон С. Как защитить детей от опасностей Интернета. – СПб. : НТ Пресс, 2006. – 304 с.

8. Зеркина Е. В. Совместная работа учителя и родителей по преодолению негативного воздействия ИКТ-среды на школьника // Применение новых технологий в образовании: материалы XIX международной конференции. – Троицк, 2008. – С. 130–132.

9. Кобзева С. Модели защиты прав несовершеннолетних в сети Интернет: мировой опыт и рекомендации для России // Информация для всех [Электронный ресурс]. – Электрон. дан. – [М.], сор. 2002–2009. – Режим доступа: http://www.ifap.ru/pi/10/sr04.rtf.

10. Комарова Н. И. Гуматитаризация техногенной сферы как методологическая база социологического исследования ИКТ // Социология ИКТ: сборник научных статей. Выпуск 1 [Электронный ресурс]. – М., 2010. – Режим доступа: http://screen.ru/ikt.

11. Кормушин Ю. В. Уберечь своего ребёнка от опасностей. Как ? – М. : Эксмо, 2010. – 320 с.

12. Проект Федерального закона «О защите детей от информации, наносящей вред их здоровью, нравственному и духовному развитию». «Законодательство и практика

масс-медиа» // Право и СМИ [Электронный ресурс]. – Электрон. дан. – [М.], Институт проблем информационного права, cop. 1995–2006. – Режим доступа: http:// www.medialaw.ru/publications/zip/128/1.htm.

13. Федосов А. Ю. Система воспитательной работы в едином информационном пространстве сельской школы // Педагогическая информатика. – 2006. – № 4. – С. 82–88.

14. Шорохова О. А. Жизненные ловушки зависимости и созависимости. – СПб. : Речь, 2002. – 136 с.

15. Фонд развития Интернет. Дети России онлайн [Электронный ресурс]. – Режим доступа: http://www.detionline.com.

16. Программы mail.ru [Электронный ресурс]. – Режим доступа: http://www.soft.mail.ru.

17. Бесплатный интернет-фильтр для детей «Интернет Цензор» [Электронный ресурс]. – Режим доступа: http://www.icensor.ru.

18. Представительство microsoft в Сети [Электронный ресурс]. – Режим доступа: http:// www.microsoft.com.

19. Ежегодный форум бесплатного Интернета [Электронный ресурс]. – Режим доступа: http://www.safor.ru.

20. Интернет СМИ «Ваш личный Интернет» [Электронный ресурс]. – Режим доступа: http://www.content-filtering.ru.

21. Центр безопасности Microsoft [Электронный ресурс]. – Режим доступа: http://www. microsoft.com/rus/childsafety.

22. Центр безопасности Microsoft [Электронный ресурс]. – Режим доступа: http://www. microsoft.com/rus/security.

23. Центр анализа интернет-ресурсов [Электронный ресурс]. – Режим доступа: http:// www.cair.ru.

24. Портал российского оргкомитета по проведению года безопасного Интернета [Электронный ресурс]. – Режим доступа: http://www.saferinternet.ru.

25. Интернет-портал «Справедливая жизнь в России» (посвящен вопросам семьи и демографии) [Электронный ресурс]. – Режим доступа: http://www.ruslife.ru.

26. Онлайновая игра, созданная в рамках программы Совета Европы «Строим Европу для детей и вместе с детьми» [Электронный ресурс]. – Режим доступа: http://www. wildwebwoods.org.

Антивирусная программа
Программа, предназначенная для предотвращения доступа к персональному компьютеру вредоносных программ. Программа обнаруживает заражённые компьютерным вирусом файлы и удаляет их.

Всплывающее окно
Новое окно, которое открывается поверх активного окна обозревателя Интернета. Как правило, такое окно не содержит видимого веб-адреса. Во всплывающих окнах, которые открываются без запроса пользователя, обычно содержится реклама.

Загрузка
Сохранение файлов из Интернета на собственном компьютере.

Защита данных
Набор правил, которые обеспечивают сохранение конфиденциальности информации. Безопасность данных распространяется на конфиденциальную информацию, например, личную информацию, и поддерживается политикой информационной безопасности или заявлением о конфиденциальной информации.

«Защитник», «защитная» программа, фаервол, брандмауэр
Программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельным компьютером. Например, с помощью настройки фаервола по правилам можно запретить некоторым или всем программам выходить в Интернет. Можно настроить фаервол на запрет запуска скриптов при просмотре страниц в Интернете.

Информационная безопасность
Политика мер, реализуемая для обеспечения контроля над рисками информационной стабильности и безопасности.

Опасные программы: вирусы, черви и трояны
Программа или часть программы, которая предназначена для распространения нежелательных событий в компьютерной или информационной системе, например, подбор паролей, уничтожение компьютерных данных. Обладают возможностями по самостоятельному распространению себя в Сети путём копирования.

Операционная система
Главная программа, которая работает «между» компьютером и прикладным программным обеспечением. С помощью операционной системы компьютер управляет установленным программным обеспечением, а также контролирует и использует его. К распространенным операционным системам относятся семейства программ Microsoft® Windows®, Apple® Mac OS и Linux®. Под словом «семейство» подразумевается выпуск новых версий программ.

Почта; электронная почта; сообщение электронной почты
Электронная передача текста или мультимедийной информации между компьютерами.

Сервер
Программа, которая распределяет файлы по компьютерам в Сети на основе предварительно заданных правил. Например, в Интернете пользователи получают сообщения электронной почты от сервера электронной почты Сети. Сервером часто называют компьютер, на котором установлена серверная программа.

Серфинг
Просмотр содержания интернет-страниц.

Сетевой дневник, или блог
Общественный интерактивный дневник, расположенный в сети Интернет, имеющий возможность открытого и ограниченного доступа.

Скайп
Специальная программа, наиболее часто используемая в Интернете для организации голосовой связи. Имеет дополнительные возможности текстового и видеообщения, посылки файлов.

Спам
Нежелательная электронная почта, которая, как правило, рассылается в целях прямой почтовой рекламы и других предложений коммерческого характера. Спам почти всегда единовременно рассылается большому кругу получателей.

Фишинг
Поддельный сайт в Интернете. Внешне по дизайну полностью совпадающий с известным сайтом, например, mail.ru, yahoo.com, odnoklassniki.ru, но в строке браузера содержится адрес, похожий на оригинальный, но ненастоящий. Цель

создания таких сайтов состоит в хищении чужого пароля.

Форум
Место обсуждения в Интернете, часто посвящённое определенной теме. Здесь люди могут оставлять сообщения в интерактивном режиме, отвечать на чужие сообщения, используя форматы, указанные поставщиком данной услуги. Для некоторых дискуссионных форумов требуется регистрация.
В некоторых форумах имеется архив, который можно использовать для поиска определенной темы. Некоторые форумы контролируются администратором, который имеет право удалять и редактировать любые размещенные сообщения или запрещать доступ для пользователей, которые оскорбляют своих собеседников.

«Френд»
Дословный перевод с английского – друг. В социальных сетях – участник этой же сети, которому можно присвоить статус «френд», после чего у него появляются дополнительные возможности для чтения закрытых для других сообщений и другие возможности.

Хакер, взломщик
Человек, взламывающий информационные сети или системы организации либо использующий их без разрешения. В последнее время основное распространение получили не физические персонажи, взламывающие компьютерные программы и сети, а написанные этими хакерами программы, которые автоматически, без непосредственного участия человека, осуществляют взлом, подбор паролей, уничтожение или порчу компьютерной информации и другую нежелательную и несанкционированную деятельность.

Чат
Способ виртуальной коммуникации в текстовом виде, работающий в режиме реального времени. В нем пользователи поочередно пишут сообщения, сразу отображающиеся на экране. Сообщения заменяются по мере написания новых, поэтому отображаются только самые последние сообщения. Бывают управляемые «живым» человеком, который имеет право на запрет общения временно (kick — кик, пинок) или навсегда (бан), и неуправляемые. Соответственно, модерируемые и немодерируемые.

ПАМЯТКА ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

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

- По возможности не сообщайте свои личные данные: имя, номер телефона, адрес проживания или учёбы, любимые места отдыха или проведения досуга. Помните, что всё, что вы о себе сообщите в социальных сетях, чатах или форумах, становится доступным и может быть прочтено и использовано любым человеком в мире: Интернет прозрачен и глобален.

- Никогда не сообщайте в открытых источниках конфиденциальные данные: пароли или номера кредитных карт, пин-коды и другую финансовую информацию.

- При регистрации на интернет-страницах используйте нейтральное имя, а если потребуется выбрать пароль, используйте комбинацию из строчных и заглавных букв и цифр, по возможности сложную.

- Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу. И советуйтесь по сложным ситуациям, когда вы сталкиваетесь с чем-то необычным.

- Используйте защитные программы, антивирусы, фильтры электронной почты, программы для блокирования спама и нежелательных сообщений.

- Никогда не соглашайтесь на индивидуальные личные встречи с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.

- Будьте сдержанны и по возможности вежливы в интернет-общении. Прекращайте любые контакты с теми, кто начинает задавать вам вопросы раздражающие, личного характера или содержащие сексуальные намеки. Обязательно расскажите об этом родителям.

ТЕСТ ДЛЯ РОДИТЕЛЕЙ НА НАЛИЧИЕ ИГРОВОЙ ИНТЕРНЕТ-ЗАВИСИМОСТИ ИХ РЕБЁНКА

Поставьте в соответствующую графу один балл за каждый вопрос, на который вы ответили положительно.

Вопросы	Балл
Много ли времени ребёнок проводит за компьютером, игровой панелью, планшетом, карманным персональным компьютером, смартфоном, играя в компьютерные игры?	
Легко ли он прекращает игру по вашему требованию?	
Часто ли бывают ситуации, когда ребенок прячется от вас и играет в компьютерные игры?	
Часто ли он рассказывает вам о персонажах из компьютерных игр и игровых ситуациях?	
Часто ли ребёнок с друзьями обсуждает игровые ситуации?	
Изменился ли резко его внешний вид, одежда?	
Появились ли у него странные и нетипичные предметы: меч, плащ, необычные аксессуары, обувь?	
Просит ли он у вас обновить компьютер? Сделать его мощнее, быстрее?	
Просит ли ребёнок деньги на игры или на непонятные вам цели?	
Изменились ли резко его привычки?	

Если сумма баллов дает больше 5, то вам надо обратить внимание на возможную игровую зависимость вашего ребёнка.

ПЕРЕЧЕНЬ ПРОГРАММ-ФИЛЬТРОВ ИНТЕРНЕТ-КОНТЕНТА

Если вы волнуетесь за безопасность своих детей, которые остаются «один на один» с компьютером, ознакомьтесь с основными способами «фильтрации» интернет-контента:

Название	Описание	Сайт разработчиков
Kaspersky Internet Security KASPERSKY lab	Kaspersky Internet Security предлагает запретить доступ к нежелательным сайтам	www.kav.ru
KinderGate Родительский контроль KinderGate PARENTAL CONTROL	С помощью KinderGate Родительский Контроль родители смогут не только запрещать сайты взрослого содержания, но и блокировать массу других категорий по своему усмотрению	www.usergate.ru
Фильтр «Семейная безопасность»	Веб-фильтр в Семейной безопасности Windows Live помогает защитить вашего ребёнка путём ограничения доступа к определённым веб-сайтам	download.ru.msn.com
StaffCop Home Edition STAFFCOP	Программа сохраняет сайты, посещаемые пользователями	www.staffcop.ru/home/
«Один Дома» Один дома	Данное ПО предназначено специально для защиты детей от просмотра нежелательного контента	www.odindoma.org

«Интернет Цензор» 	Главная задача пакета – сделать пребывание детей и подростков в Интернете безопасным, оградив их от вредных ресурсов	www.icensor.ru
Avira Premium Security Suite 	Пакет программ, которые, будучи используемыми в комплексе, позволяют защитить личный компьютер от большинства современных угроз	www.avira.com
BitDefender Internet Security 2011 	BitDefender Internet Security 2011 защищает ПК от вирусов, хакеров, взлома и попытки кражи персональных данных	www.bitdefender.ru
Dr.Web Security Space 	Помимо сильного модуля родительского контроля, это также комплексное решение проблемы защиты ПК	www.drweb.com
F-Secure Internet Security 2009 	Комплексное решение защиты от всех видов интернет-угроз	www.f-secure.com