**УТВЕРЖДАЮ**

Директор школы \_\_\_\_\_\_\_\_ Семенова А.Д.

05.09.2015

Приказ № от 05.09.2015 г.

**МУНИЦИПАЛЬНОЕ КАЗЁННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ** «СШ№2 им М.И. Халилова г Теберды»

**Программа**

**обучения детей и подростков правилам безопасного поведения в Интернет - пространстве, профилактике Интернет - зависимости, предупреждения рисков вовлечения в противоправную деятельность**

**на 2015 – 2017 годы**

Программа предназначена для уч-ся 1-11 кл

г. Теберда

2015г

**Авторы программы:**

Доюнова Х.А. .,зам. директорпо УВР ; Глчияева М.К. ., педагог - психолог,Абазалиев Б.И. ., председатель Управляющего совета, Бостанова С.У.., учитель информатики.

**Пояснительная записка**

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более

актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем».

Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование.

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих

проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

В связи с этим необходимо направить все усилия на защиту детей от информации, причиняющей вред их здоровью и развитию. Просвещение

подрастающего поколения, знание ребенком элементарных правил отбора

информации, а также умение ею пользоваться способствует развитию системы защиты прав детей.

«Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные

техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать» (П.А.Астахов, уполномоченный

при Президенте Российской Федерации по правам ребенка).

Медиаграмотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

Развитие и обеспечение информационной грамотности признан эффективной мерой противодействия посягательствам на детей с использованием сети Интернет (Рекомендация Rec (2006) 12 Комитета министров государствам-членам Совета Европы по расширению возможностей детей в новой информационно-коммуникационной среде от 27.09.2006.)

Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права (**Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства** в Интернете, **Решение Европейского парламента и Совета № 276/1999/ЕС о** принятии долгосрочной плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).

Согласно российскому законодательству **информационная безопасность детей** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию").

Преодолеть нежелательное воздействие компьютера возможно только

совместными усилиями учителей, родителей и самих школьников.

**Программа разработана с учетом требований нормативно-правовых документов:**

* Федеральный закон от 29.12.2012 № 273 – ФЗ «Об образовании в Российской Федерации».
* Конвенция «О правах ребенка».
* Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" и от 29.06.2013 года № 135-ФЗ «О внесении изменений в статью 5 Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
* Указ Президента РФ от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей на 2012 – 2017 годы».
* Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете
* Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочной плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).
* «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10

**Программа.**

**Цель и задачи программы.**

Цель: обеспечения информационной безопасности детей и подростков при обучении, организации внеучебной деятельности и свободном использовании современных информационно-коммуникационных технологий (в частности сети Интернет)

Задачи:

-формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;

-формирования информационной культуры как фактора обеспечения информационной безопасности;

-изучение с нормативно-правовых документов по вопросам  защиты детей от информации, причиняющей вред их здоровью и развитию;

-формирование знаний в области безопасности детей использующих Интернет;

-организации просветительской работы с родителями и общественностью.

**Данная программа рассчитана на период** с 2015 по 2017 г.

**Сроки реализации программы:** 2015 – 2017 годы

**Программы рассчитана на** детей 7-17 лет.

**Формы проведения мероприятий в ходе реализации программы:**

медиауроки, тематические недели, дни, семинары, конкурсы, мониторинги, беседы, классные часы, практикумы, тренинги, конференции, родительские собрания и др.

Обеспечить безопасность детей, не способных иногда правильно оценить степень угрозы информации, которую они воспринимают или передают, так как темпы информатизации оказались столь быстрыми, что и семья и школа оказались не всегда готовы к угрозам нового типа, методы борьбы с которыми еще только разрабатываются.

Опасности, которые ждут школьника в сети Интернет (некоторые):

-***суицид-сайты, на которых дети получают информацию о «способах»***

***расстаться с жизнью;***

***-сайты-форумы потенциальных самоубийц;***

***-наркосайты. Интернет пестрит новостями о "пользе” употребления***

***марихуаны, рецептами и советами изготовления "зелья”;***

***-сайты, разжигающие национальную рознь и расовое неприятие:***

***экстремизм, национализм, фашизм;***

***-сайты порнографической направленности;***

***-сайты знакомств. Виртуальное общение разрушает способность к***

***общению реальному, "убивает” коммуникативные навыки подростка;***

***-секты. Виртуальный собеседник не схватит за руку, но ему вполне по***

***силам "проникнуть в мысли” и повлиять на взгляды на мир.***

Это не полный список угроз сети Интернет. Любой школьник может попасть на такие сайты случайно: кликнув по всплывшему баннеру или перейдя по ссылке. Есть дети, которые ищут подобную информацию специально, и естественно, находят. Кроме этого, появились психологические отклонения, такие как компьютерная и Интернет–зависимость, игромания (зависимость от компьютерных игр). Для преодоления негативного воздействия сети Интернет на детей, в образовательном учреждении проводится целенаправленная воспитательная работа учителей совместно с родителями. Выработана единая стратегия безопасности совместными усилиями педагогических работников, родителей и обучающихся.

Обучение педагогических работников проводится в форме семинаров, мастер – классов, круглых столов, в рамках которых рассматриваются проблемы информационной безопасности личности в сети Интернет, нежелательный контент и меры борьбы с ним, виды и формы информационно - психологического воздействия и методы защиты от него, правила и нормы сетевого этикета, причины возникновения девиантной формы поведения детей и методы работы по их профилактике и устранению.

Необходимая информация находится на сайтах:

«Безопасность» <http://sos-ru.info>,

«Безопасный Интернет» <http://www.i-deti.org/> <http://www.saferinternet.ru> и т.д.

Работа с обучающимися ведется в зависимости от возрастных особенностей: начальное звено (2-4 класс), среднее (5-9 класс) и старшее(10-11 класс). На каждом этапе осуществляются специальные формы и методы обучения в соответствии с возрастными особенностями. Формирование навыков информационной безопасности и культуры осуществляется не только на уроках информатики, но и на других предметах (обществознания, права, ОБЖ и т.д.), а также и во внеурочной деятельности.

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, между тем «выпуская» его в Интернет не представляют себе, что точно также нужно обучить его основам безопасности в сети. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети. Необходимо выработать в нем критическое мышление.

С родителями проводится разъяснительная работа, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения. Формы работы с родителями разнообразны: выступления на родительских собраниях, индивидуальные беседы, информация на сайте лицея, встречи со специалистами, семинарские занятия.

Разработаны 7 специальных методических рекомендаций для родителей по обеспечению информационной безопасности в сети Интернет. Они содержат классификацию Интернет угроз, рекомендации по обеспечению безопасности

ребенка в сети Интернет дома (в зоне ответственности родителей).

Комплексное решение поставленной задачи со стороны семьи и школы

позволит значительно сократить риски причинения различного рода ущерба

ребенку со стороны сети Интернет.

Для организации безопасного доступа к сети Интернет в МКОУ «СШ №2 им М.И. Халилова Г Теберда »

1.Применяются административные и организационные меры, технические и программно-аппаратные средства защиты детей от вредной информации в местах доступных для детей:

- провайдером услуги доступа к сети Интернет школы с обеспечением контент-фильтрации Интернет — трафика ;

-функционирование и использование в лицее программного продукта, обеспечивающего контент-фильтрацию Интернет-трафика, в том числе SkyDns, бесплатных контент-фильтров;

-стимулирование родителей к использованию услуги «Родительский контроль», позволяющей устанавливать ограничения доступа к информационно-телекоммуникационной сети Интернет;

-назначены лица, ответственные за установку программного продукта для реализации контектной фильтрации доступа к сети Интернет;

-регулярно проводится мониторинг качества предоставления провайдером услуги доступа к сети Интернет школы с обеспечением контент-фильтрации Интернет — трафика и мониторинг функционирования и использования в школе программного продукта, обеспечивающего контент-фильтрацию Интернет-трафика.

2.Во исполнение Национальной стратегии действий в интересах детей на 2012-2017 годы, утвержденной Указом Президента РФ от 01.06.2012г. №761 и Федеральнго закона "О защите детей от информации, причиняющей вред их здоровью и развитию"от 29.12.2010г. № 436-ФЗ запланировано:

-создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность, порнографию с использованием справочников по детской безопасности в Интернете (своего рода электронных учебников для педагогов и родителей, которые содержат не только полезные советы, в том числе видеосоветы, но и различные настройки для безопасного поиска, ссылки для подачи сообщения о незаконном контенте на сервисах YouTube, Живая лента и др.); сайта МОО "Информация для всех", который распространяет помимо прочего информацию о мероприятиях, например, о Заочной всероссийской научно-практической конференции с международным участием "Детство. Медиакультура. Информационное общество", в которой на обсуждение среди различных проблем вынесены проблемы защиты детей от негативного воздействия медиа и актуальные проблемы современного медиаобразования и др.

-внедрение системы мониторинговых исследований по вопросам обеспечения безопасности образовательной среды образовательных учреждений, а также по вопросам научно-методического и нормативно-правового обеспечения соблюдения санитарно-гигиенических требований к использованию информационно-компьютерных средств в образовании детей.

**План мероприятий**

**по обеспечению защиты детей от информации, причиняющей вред их здоровью и развитию**

**в МКОУ «СШ №2 им М.И. Халилова г Теберды » на 2015 – 2017 г. г.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование мероприятия | | | Срок испол  нения | Ответственные за  реализацию  мероприятия, организаторы |
| **I. Создание организационно-правовых механизмов защиты детей от распространения информации,**  **причиняющей вред их здоровью и развитию** | | | | | |
| 1.1. | Создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет -пространстве, профилактики интернет -зависимости, предупреждения рисков вовлечения в противоправную деятельность, порнографию. | | | 2015-  2017 | Бостанова С.У. . |
| 1.2. | Разработка и реализация целевых программ обеспечения информационной безопасности детей | | | 2015-  2017 | Администрация |
| 1.3. | Изучение методических рекомендаций по проведению внеурочных занятий с обучающимися по теме «Приемы безопасной работы в Интернете» | | | 2015-  2017 | Кл рук-ли  Бостанова С.У.. |
| 1.4. | Изучение педагогами вопросов обеспечения мер информационной безопасности, проблем безопасного поведения в сети Интернет и пр. | | постоянно | | Зам. директора по УВР |
| 1.5. | Реализация информационного курса для родителей по защите детей от распространения вредной для них информации | | 2015-2017 | | Бостанова С.У. |
| 1.6. | Проведение родительских собраний о безопасности детей  в информационно-телекоммуникационной сети Интернет | | 2015 | | Классные руководители |
| **I I. Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно - программных и технико - технологических устройств** | | | | | |
| 2.1. | Функционирование контент- фильтра в школе | | 2015 | | Бостанова С.У.  Байчоров Р. |
| 2.2. | Мониторинг функционирования и использования в школе программного продукта, обеспечивающего контент- фильтрацию Интернет-трафика | | 2015-  2017 | | Бостанова С.У. |
| 2.3. | Мониторинг качества предоставления провайдером услуги доступа к сети Интернет школыс обеспечением контент- фильтрации Интернет - трафика | | 2015-2017 | | Бостанова С.У. |
| 2.4. | Мониторинговые исследования по вопросам научно-методического и нормативно-правового обеспечения соблюдения санитарно-гигиенических требований к использованию информационно-компьютерных средств в образовании детей. | 2015-  2017 | | | Бостанова С.У.  Доюнова Х.А. |
| 2.5. | Стимулирование родителей к использованию услуги «Родительский контроль», позволяющей устанавливать ограничения доступа к информационно-телекоммуникационной сети Интернет. | 2015-  2017 | | | Классные руководители |
| **III. Профилактика у детей и подростков интернет-зависимости, игровой зависимости и правонарушений с использованием информационно - телекоммуникационных технологий, формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно - телекоммуникационной среде через обучение их способам защиты от вредной информации** | | | | | |
| 3.1. | Проведение медиауроков по теме «Информационная безопасность» | | | 2015- 2017 | Бостанова С. |
| 3.2. | Проведение ежегодных мероприятий в рамках недели «Интернет-безопасность» для учащихся и их родителей | | | 2015- 2017 | Бостанова С. |
| 3.3. | Участие в Международном Дне безопасного Интернета для учащихся школы и их родителей | | | 2015- 2017 | Бостанова С.У.  Байчоров Р. |
| 3.4. | Участие во Всероссийском конкурсе сайтов для детей и юношества «Позитивный контент» | | | 2015- 2017 | Бостанова С.У.  Байчоров Р. |
| 3.5. | Участие в обучающих семинарах по созданию надежной системы защиты детей от противоправного контента в образовательной среде школы и дома. | | | 2015- 2017 | Бостанова С.У. Байчоров Р. |
| 3.6. | Организация свободного доступа обучающихся и преподавателей к высококачественным и сетевым образовательным ресурсам, в том числе к системе современных учебных материалов по всем предметам общеобразовательной школы | | | 2015- 2017 | Байчоров Р. |
| 3.7. | Внедрение и использование программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания | | | 2015- 2017 | Бостанова С.У. |
| 3.8. | **Мероприятия по антивирусной защите компьютерной техники школы** | | | | Байчоров Р. |
| **IV. Информационное просвещение граждан о возможности защиты детей от информации, причиняющей вред их здоровью и развитию** | | | | | |
| 4.1. | Проведение различных мероприятий (лекториев, семинаров, практикумов, тренингов, круглых столов, конференций и т.п.), в том числе с применением дистанционных технологий, по проблемам информационной безопасности для всех участников образовательного процесса | | | 2015- 2017 |  |
| 4.2. | Размещение на сайте лицея ссылок на электронные адреса по проблемам информационной безопасности для всех участников образовательного процесса | | | 2015- 2017 |  |
| 4.3 | «Школа здоровья»: проведение бесед с участием специалистов детской поликлиники, школьного медицинского работника | | | 2015- 2017 |  |
| 4.4 | Проведение Дней правовых знаний в рамках гражданско-правового образования | | | 2015-  2017 | классные руководители, лекторские группы |
| 4.5 | Проведение мероприятий в рамках федерального закона «Об ограничении курения табака», борьба с курением и его профилактика | | | 2015-  2017 | Волонтерская группа |
| 4.6 | Проведение мероприятий по профилактике употребления алкоголя | | | 2015-  2017 | Волонтерская группа |
| 4.7 | Осуществление мероприятий по реализации школьных программ «Общение», «Досуг» | | 2015-  2017 | |  |
| 4.9 | Проведение мероприятий по реализации Программы духовно-нравственного развития и воспитания обучающихся | | 2015-  2017 | |  |

**Результаты выполнения программы**

Повышение грамотности по проблемам информационной безопасности всех участников образовательного процесса

|  |  |
| --- | --- |
| **Цели и задачи программы** | **Перечень показателей** |
|
| **Цель:** Обеспечение информационной безопасности обучающихся при обучении, организации внеучебной деятельности и свободном использовании современных информационно-коммуникационных технологий в том числе сети Интернет. | |
| Задача №1: формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков; | -Все педагоги, используют современные коммуникационные взаимодействия. |
| -Умение использовать и интегрировать разнотипную информацию. |
| Задача № 2: формирования информационной культуры как фактора обеспечения информационной безопасности; | -Почти все педагоги используют сетевые технологии, современные средства связи и прикладные программы в области профессиональной деятельности. |
| Задача № 3: изучение нормативно-правовых документов по вопросам  защиты детей от информации, причиняющей вред их здоровью и развитию; | -Владение правовыми знаниями в области информатизации. |
| Задача № 4: формирование знаний в области безопасности обучающихся, использующих Интернет; | -Владение знаниями о защитите компьютера от вредоносных программ, о нелегальном, пиратском контенте и об опасности его скачивания. |
| Задача № 5: организации просветительской работы с родителями и общественностью. | - Включение родителей в совместную со школой деятельность по обеспечению безопасности детей в Интернет пространстве. |

**Список использованных материалов**

* Федеральный закон от 29.12.2012 № 273 – ФЗ «Об образовании в Российской Федерации».
* Конвенция «О правах ребенка».
* Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" и от 29.06.2013 года № 135-ФЗ «О внесении изменений в статью 5 Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
* Указ Президента РФ от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей на 2012 – 2017 годы».
* Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете
* Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочной плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).
* «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10
* Дети в интернете: как научить безопасности в виртуальном мире. И. В. Литовченко и др. –К.:Издательство ООО «Издательскийдом“Аванпост-Прим”,2010.–с.48.–Пособие для родителей.

**Приложение**

**Психологические и физические симптомы Интернет-зависимости**

**Психологические симптомы**

Хорошее самочувствие или эйфория вовремя работы за компьютером.

Невозможность остановиться.

Увеличение количества времени, проводимого в интернете.

Пренебрежение семьей и друзьями.

Возникновение ощущения пустоты, тревожности, раздражения в периоды пребывания вне интернета.

Ложь близким о своей деятельности.

Проблемы в учебе.

**Физические симптомы**

Боль в кисти руки–(из-за длительного перенапряжения мышц).

Сухость в глазах.

Головные боли.

боли в спине.

Нерегулярное питание, пропуск приемов пищи.

Пренебрежение личной гигиеной.

Нарушения режима сна.

**Опасные сигналы (предвестники интернет-зависимости)**

Навязчивое стремление постоянно проверять электронную почту

Предвкушение следующего сеанса онлайн.

Увеличение времени, проводимого онлайн.

Возрастание финансовых трат на интернет-услуги.

**Признаками наступившей интернет-зависимости являются:**

-полная поглощённость интернетом;

-потребность неуклонного увеличения времени онлайн-сеансов;

-наличие неоднократных, малоэффективных попыток сокращения времени пребывания в интернете;

-появление симптомов абстиненции при прекращении интернет-связи (повторная тяга,возникновение и усиление напряжения через определённое время);

-возникновение проблем с ближайшим окружением(одноклассниками, членами семьи, друзьями);

-стремление к сокрытию реального времени, проводимого в интернете;

-зависимость настроения от использования интернета (выражается эмоциональными двигательным возбуждением, тревогой, навязчивыми размышлениями о том, что сейчас происходит в интернете, фантазиями и мечтами об интернете, произвольными или непроизвольными движения пальцев, напоминающими печатание на клавиатуре)

**Памятка для обучающихся начальной школы**

[smile235.gif]1. Всегда помни своѐ Интернет-королевское имя (e-mail, логин,

пароли) и не кланяйся всем подряд (не регистрируйся везде без

надобности)!

* 2. Не поддавайся ярким рекламам-указателям и не ходи тропками,

путанными на подозрительные сайты: утопнуть в трясине можно!

[033.gif]3. Если пришло письмо о крупном выигрыше – это «Лохотрон-

грамота»: просто так выиграть невозможно, а если хочешь

зарабатывать пиастры, нужно участвовать в полезных обучающих

проектах – в «Регате…», например!

* 4. Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой

Клубок волшебный (заводи себе будильник, садясь за компьютер)!

* 5. Если хочешь дружить с другими царствами-государствами,

изучай полезные социальные сервисы Web2.0: они помогут тебе

построить «Мой королевский мир», свой царский блог, форум для

глашатаев важных – друзей званных!

[smile287.gif] 6. Не забывай обновлять антивирусную программу – иначе вирус

Серый Волк съест весь твой компьютер!

[smile207.gif]7. Не скачивай нелицензионные программные продукты – иначе

пираты потопят твой корабль в бурных волнах Интернета!

**Родительское собрание**

Тема:  «Интернет: плюсы и минусы»

Цель:  **рассказать родителям, какие угрозы существуют и как их избежать.**

«Ваши дети дома?»

Незатейливый вопрос, адресованный родителям, каждый вечер звучит в телеэфире. Дети дома, но в безопасности ли они?

С тех пор, как Интернет перестал быть роскошью и пришел буквально в каждый дом, он стал неотъемлемой частью жизни не только взрослых, но и детей.

**+** Даже родители, некогда расценивавшие доступ во Всемирную сеть как баловство, вынуждены признать: Интернет содержит массу полезной для ребенка информации, помогает в выполнении школьных заданий, расширяет кругозор и является своеобразным «окном в большой мир».

**-**  С другой стороны, только очень наивный взрослый не знает, сколько в Сети ресурсов, которые отнюдь не назовешь безопасными – особенно для детей, любопытных и жадных до новых знаний. Судите сами: программы, запрещающие доступ к «плохим» ресурсам, не оправдывают надежд, поскольку просто не в силах фильтровать все вредоносное содержимое.

Как должны родители помочь детям снизить эти риски? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка. Вот вы, родители, на данный момент знаете, какими  сайтами пользуются ваши дети? Нет? Очень печально. Именно с этого надо начинать работу с безопасным интернетом.

Для детей и молодежи Интернет главным образом является социальной средой, в которой можно не только встречаться с друзьями, но и с незнакомцами. В Интернете пользователя могут обидеть, запугать или даже оскорбить. Лучшей защитой является руководство собственным здравым смыслом. Наиболее важной задачей является предупреждение детей об опасностях Интернета, чтобы они вели себя осторожно. Кроме того, необходимо обсуждать с детьми все [вопросы](http://shperk.ru/tag/voprosy), которые могут у них возникнуть при использовании Интернета. Не отвергайте детей, а наоборот, постарайтесь как можно ближе расположить их доверие. Тогда вы будете в курсе той информации, которой владеют ваши дети.

Даже если ребенок не сталкивался с оскорблениями в Интернете, рекомендуется обсудить с ним  следующие вопросы:

                        Не распространяйте контактную или личную информацию, например, фотографии, без тщательного обдумывания возможных последствий. Интерактивная дружба может закончиться. Когда это произойдет, личная информация может быть отправлена злоумышленникам.

                        В Интернете каждый человек имеет право на уважительное отношение.

                        Детям должна быть предоставлена возможность поговорить с родителями об отрицательном опыте.

# *Безопасное использование в соответствии с возрастом*

## 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.

  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 будут иметь дело с Интернетом не только у себя дома, но и в школе, и у друзей.  Вы 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 пугающим или неуместным материалом (изображения, текст или звук). Разговор об этих материалах и объяснение различных вещей, с которыми дети могут столкнуться в Интернете, поможет детям стать ответственными и способными самостоятельно и безопасно работать в Интернете.  Вы можете 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.

  Если компьютер установлен в комнате, которой пользуется вся семья, использование Интернета становится естественным для повседневной жизни.

  Ребенок еще не может определить надежность веб-сайта самостоятельно, поэтому ему всегда следует спрашивать разрешения у родителей перед публикацией личной информации.

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

## Дети 10–12 лет

Школьники уже могут знать, как использовать Интернет в различных целях. 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 планирования вопросов, касающихся всей семьи. Это дает возможность родителям и детям обсудить надежность разных сайтов, а также источники поиска полезной и качественной информации.

Ребенку необходим родительский присмотр и контроль, а также знание правил правильной работы в Сети. Тем не менее, ребенок может узнать, как избавиться от присмотра и обойти правила, если он будет считать их слишком ограничивающими или несоответствующими его потребностям.

  Родителям и детям необходимо прийти к соглашению относительно разрешенных и запрещенных действий в Интернете, а также его использования. В соглашении должны быть учтены все потребности и мнения. Договоритесь, какую личную информацию можно разглашать и в каких случаях, а также поговорите о рисках, связанных с разглашением информации.  
Если ребенок уже заинтересовался общением в чатах или IRC,  вам  следует обсудить с детьми их безопасность и контролировать их опыт в интерактивных обсуждениях.

  Многие дети любопытны и любознательны, поэтому родителям необходимо акцентировать внимание на необходимости безопасного и осторожного использования.

  Систему безопасности информации также необходимо обновлять.

## 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 грамотности использование Интернета открывает множество возможностей. Родителям, может быть, очень 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 семьи становится участие в открытых дискуссиях, а для родителей — заинтересованность в том, что ребенок делает и с кем использует интернет ресурсы.

Что за угрозы подстерегают наших детей в виртуальном мире? Этот вопрос задают многие родители, которые ещё не сталкивались с проблемами использования интернета. Поэтому **целью собрания является рассказать, какие угрозы существуют и как их избежать.**

Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержимым!

Итак,  что же подстерегает наших детей с экрана монитора:

|  |
| --- |
| **Порнография**                                  Опасна избыточной информацией и грубым, часто                                 извращенным, натурализмом. Мешает развитию естественных                                 эмоциональных привязанностей. |
| **Депрессивные молодежные течения**                                  Ребенок может поверить, что шрамы – лучшее украшение, а                                 суицид – всего лишь способ избавления от проблем. |
| **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, “убивает” коммуникативные навыки, которые мы                                  невольно приобретаем с самого раннего детства. |
| **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. |

  Если вы не знаете с чего начать, ознакомьтесь с приведенными ниже советами, которые помогут вам научить детей принципам безопасной работы в Интернете.

|  |  |
| --- | --- |
| 1. | Убедите своих детей делиться с вами впечатлениями от работы в Интернете. Путешествуйте в Интернете вместе с детьми. |
| 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 общаются в чатах, пользуются [программами мгновенной передачи сообщений](http://www.microsoft.com/protect/products/computer/imsafety.mspx), играют в сетевые игры или занимаются в Интернете чем-то другим, 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 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. | Контролируйте 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. |

 Представьте себе Интернет, в котором нет порнографических сайтов, сомнительных социальных сетей, откровенных блогов, онлайн-казино, страниц, пропагандирующих фашизм, насилие и религиозную нетерпимость – словом, представьте себе действительно безопасный Интернет, в который вы спокойно «отпустите» своего ребенка одного. Недавно об этом можно было только мечтать, сейчас же каждый может убедиться в том, что мечта стала явью – достаточно скачать с сайта [www.icensor.ru](http://www.icensor.ru/) и установить на домашнем компьютере программу «Интернет Цензор».                                      Безусловный плюс «Интернет Цензора» в том, что программу эту каждый родитель может «подстроить» под себя и своего ребенка, адаптировать к его интересам и увлечениям. Вам понадобится лишь пара минут на то, чтобы разрешить доступ к той или иной страничке. С другой стороны, если тот или иной «открытый» сайт покажется вам вредным для ребенка, запретить доступ к нему тоже не составит труда.

«Интернет Цензор» — удобная и простая программа, не требующая мощного компьютера и специальных знаний. Распространяется она бесплатно, так же бесплатны и все обновления – это принципиальная позиция создателей программы, изменять которой они не собираются.

Говоря о безопасности детей в Интернете, акцент следует  сделать на то, что самое главное – это доверие между родителями и ребенком, готовность взрослых к диалогу, обсуждению непростых вопросов, да и просто разговорам о том, «что такое хорошо и что такое плохо».

**Рекомендуем!**  
[Школьный Яндекс](http://school.yandex.ru/) - это полнофункциональная поисковая система для школьников

**Памятка**

**по безопасному**

**поведению в Интернете**

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

• Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

• Используйте нейтральное экранное имя, не содержащее сексуальных 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 сексуальные намеки. Расскажите об этом родителям.

**Соблюдая эти простые правила безопасной работы в интернете**, вы избавите себя от множества серьезных проблем и опасностей, существующих в сети.

* Поступайте и пишите в Сети так, как поступили бы в реальной жизни и как хотели бы, чтобы поступали с вами. Помните – все, что вы сделаете в Интернете, будет иметь последствия в реальной жизни. Анонимность в Интернете не гарантирует, что любые поступки сойдут с рук. Стоит вспомнить хотя бы то, сколько хакеров и Интернет-мошенников уже оказались за решеткой. Вычислить человека по его виртуальным следам (IP, cookies, мак-адрес) не так уж сложно.
* Уважайте своих собеседников и чужую собственность в Интернете, за ними скрываются настоящие люди и реальный труд. Вы общаетесь не с абстрактным псевдонимом, а с человеком – даже за ботом стоит человек. Кстати, у всех материалов, находящихся в Сети, есть авторы и хозяева.
* Не сохраняйте на своем компьютере неизвестные файлы, не переходите по ссылкам от незнакомцев, какими бы заманчивыми они не были. Такая ссылка может оказаться вирусом, трояном или, если «повезет», рекламой порносайта. 80% ссылок, присылаемых незнакомцами, являются рекламой. А 20% - вредоносными объектами.
* Обязательно установите антивирус и фаервол и регулярно обновляйте их базы. Необновленные и устаревшие базы не смогут гарантировать вам стопроцентную защиту от вредоносных объектов. Дело в том, что ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу необходимо как можно чаще получать информацию о методах борьбы с ними.
* Не запускайте неизвестный файлы, особенно с расширением \*.exe. Старый совет, но по-прежнему актуальный. Файл с таким разрешением не может являтья картинкой или фильмом. Это всегда программа, в крайнем случае флеш-анимация. Поэтому велика вероятность, что такой файл является вирусом или Трояном.
* Старайтесь давать как можно меньше информации о себе в Интернете. «Что написано пером – не вырубить топором» - эта мудрость актуальна и для Интернета. Например, 90% мошенничеств происходит из-за утечки информации по вине пользователя.
* Будьте осторожны при общении с незнакомыми людьми. Ничто не мешает сорокалетнему извращенцу прикидываться в чатах пятнадцатилетней школьницей и заводить знакомства со «сверстницами». Опросы показывают, что каждый пятый пользователь Сети выдавал себя за другого человека (реально существующего или придуманного).
* Не открывайте сразу файлы, скаченные из Интернета, скопированные с диска или флэшки. Сначала скопируйте файлы на рабочем столе, проверьте антивирусной программой и только после этого решайте – открывать их или нет.

**Как защититься от хамства и оскорблений в Интернете**

В зависимости от типа ресурса, на котором вы столкнулись с киберхамами, подходящими могут быть различные действия.

Чат. Если при общении в тематическом чате к вам пристает пользователь с оскорблениями, злыми шутками или издевательствами, отправьте его в игнор-лист (персональный «черный список») или сообщите администратору чата о его неприемлемом поведении. Скорее всего, грубиян будет забанен, то есть исключен из числа пользователей. Грубить хаму в ответ чревато получением того же бана. Icq и прочие онлайн-месседжеры.

Отвязаться от нежелательного собеседника в аське проще всего. Добавив его в «черный список», вы больше никогда не увидите и не услышите его. Чтобы предотрватить дальнейшие беседы с «клонами» хама (то есть его «реинкарнациями» под другими номерами icq), необходимо поставить в настройках клиента запрет на получение сообщений от неавторизованных пользователей. Тогда вы будете получать сообщения только от тех контактов, которые одобрите сами.

Социальные сети. Решить проблему хамства в социальных сетях обычно помогают модераторы ресурса, которые обязаны внимательно следить за публичными сообщениями пользователей. В случае добросовестной работы модераторов вы даже не успеете прочитать оскорбительное послание. Если же сетевой грубиян донимает вас по личной почте, вы всегда можете пожаловаться тому же модератору в индивидуальном порядке. Сайты знакомств. К сожалению, заметная часть посетителей сайтов знакомств приходят туда вовсе не для того, чтобы найти себе друга или любимых.

Сайты знакомств являются излюбленным местом обитания сетевых хамов, любителей онлайновых издевательств и розыгрышей. Поэтому, пользуясь подобными ресурсами, нужно быть предельно внимательным и быть морально готовым к неадекватным сообщениям. Отвечать на провокации и грубости вовсе не обязательно. А кнопка для отправки жалобы администрации всегда под рукой.

Форумы. Пытаться доказать что-то таким людям совершенно бесполезно, так как они преследуют единственную цель – позлить вас. Лучше представьте, что этого пользователя вовсе не существует на форуме и его сообщений тоже. Продолжайте беседу в привычной манере, не реагируя на попытки «тролля» вывести вас из себя. Вероятно, вскоре ему надоест тратить время зря и он оставит вас в покое. Если же вы сами не прочь сорвать злость и плохое настроение в Интернете, может рискнуть пообщаться с сетевым хамом на его языке. В конце концов, он первый начал и вы не обязаны быть вежливым. Однако опускание до уровня банального грубияна – занятие не делающее чести никому, поэтому куда лучше будет не обращать на него внимания. Если вы оставались в таком общении относительно корректны, ваша моральная правота позволяет вам прибегнуть к методам «сетевого саморегулирования» - написать модераторам форума. «Стукачеством» подобные действия называют теперь только сами «тролли», ибо на практике большая часть форумистов заинтересованы в нормальной и спокойно атмосфере для общения и молчаливо поддержит забанивание тролля. Если же на этом форуме «троллинг» возведен в культ, то лучше оттуда уйти – немного потеряете.

ОБЩИЕ ПРАВИЛА ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

1. По возможности используйте псведонимы.

2. Указывайте лишь электронные способы связи, причем созданные специально для таких контактов. Например, специально выделенный для подобного общения e-mail или номер icq. Если собеседник окажется интересным и безопасным, ничто не мешает поделиться с ним потом «более реальными» электронными координатами, а то и телефон или адресом.

3. Тщательно обдумайте, какую информацию о себе загружать в Интернет. В Интернете действует принцип «все, что вы выложили, может быть использовано против вас”. Даже если вы удалите фото, его уже могли скопировать – а значит, оно по-прежнему ходит по Интернету. Например, фото разгульной вечеринки может вызвать разрыв с близким человеком, видеоролик драки – стать доказательством для суда, демонстрация богатства наведет на вас грабителей. А подробные данные о себе подскажут им, где и как вас лучше ограбить.

4. Осторожно подходите к выбору друзей, не принимайте все заявки подряд для количества. Радость от большого числа «друзей» быстро омрачится неприятностями. Другом в соцсети может быть только тот, кто хорошо известен – желательно в реальной жизни.

5. Не открывайте доступ к своим личным страничкам незнакомым людям. Есть те, кто специально ходит по социальным сетям с целью сбора информации. Затем ее используют для киберпреследования или подготовки серьезных преступлений. Чем меньше вы дадите информации о себе – тем безопаснее.

КАК НЕ СТАТЬ ЖЕРТВОЙ «ТРОЛЛЯ»

1. Игнорируйте оскорбителя. Самый простой и действенный способ. Просто представить, что данного пользователя не существует. Добавить его в игнор-лист («черный список») и мысленно удалить его из Интернета. Не отвечать ему и не поддаваться на провокации. Продолжать общаться на этом же ресурсе с людьми, приятными и близкими вам по духу.

2. Сообщите модератору. Это можно сделать с помощью специальной формы на форуме (она обычно выглядит как кнопочка «пожаловаться на сообщение») или личным письмом. Если это популярный и уважаемый ресурс или если модераторская служба на нем поставлена на высоком уровне, его хозяева обязательно примут меры и воздействуют на сетевого агрессора (предупредят или вообще заблокируют ему доступ). В случае, если агрессором является сам модератор – воспользуйтесь третьим советом.

3. Найдите другой ресурс. Ничего не мешает вам покинуть сайт, на котором процветают хамство и оскорбления, и найти аналогичный, где можно спокойно общаться. Сделать это особенно просто, если вы не успели освоиться на сайте и привыкнуть к нему. Однако никто не гарантирует, что на новом месте не найдется своих местных хамов.

4. «Задавите интеллектом». Можно попытаться задавить сетевого хама интеллектом, показать, что с вами шутки плохи и, дескать, шел бы он оттачивать способности на ком-нибудь другом. Делается это лаконичными негрубыми ответами, высмеивающими грубияна и его действия.

5. Не нужно грубить в ответ. Если вы опуститесь до уровня не очень умного человека, то будете выглядеть ничуть не лучше его.

6. Не угрожайте хаму противозаконными последствиями в реальной жизни. Подобные вещи чреваты наказанием согласно Уголовному кодексу. Хамы обычно люди весьма подлые и могут такую угрозу повернуть против вас. А получить судимость из-за сетевого хама – дело совсем не перспективное.

7. Не создавайте на форуме тему с жалобами. Если вас обидели – свяжитесь в администрацией сайта. Ни к чему засорять ресурс пустыми темами. Не теряйте уважение к себе и окружающим вас людям. Ведите себя в Интернете так, как хотите, чтобы вели себя с вами. Тогда вы обязательно найдете интересных собеседников и существование различных агрессивных личностей перестанет вас беспокоить.

**Безопасность при on-line играх**

Так же, как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Сети. Их называют гриферами. Есть вероятность, что один из таких злодеев по крайней мере единожды может побеспокоить в таких многопользовательских играх, как Halo 2, EverQuest, The Sims Online, SOCOM и Star Wars Galaxies. Гриферы получают удовольствие, хамя и грубя окружающим. Обычно они издеваются над другими, особенно над начинающими: мешают играть товарищам по команде, используют нецензурную лексику, жульничают, создают вместе с другими гриферами бродячие банды, блокируют выходы из комнат, выманивают монстров на неосторожных игроков или используют игру, чтобы досаждать кому-то или изводить конкретного человека.

Хотя гриферы составляют лишь малую часть от общего числа пользователей, из-за них некоторые компании потеряли клиентов. Поэтому многие разработчики игр не жалеют средств и используют любые методы для вычисления гриферов. Как поступать, если Вы столкнулись с гриферами? Игнорируйте их. Если Вы не будет реагировать на воздействия гриферов, большинству из них это в конце концов надоедает, и они уходят. Измените параметры игры.

Играйте в игры, правила или режимы, которых можно изменить (например, невозможность убить товарищей по команде). Таким образом, тактика гриферов становится бессмысленной. Создайте частную игру. Большинство многопользовательских игр позволяет создавать закрытые комнаты, куда можно пускать только друзей. Играйте на сайтах со строгими правилами. Там, где установлены строгие правила, тогда администратор сможет немедленно заблокировать хулиганов. Играйте в игры, где от гриферов можно легко избавиться: сообщения хулиганов можно отключить или проголосовать за их исключение из игры.

Поищите уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору. Если обидчик продолжает беспокоить, смените игру или сделал перерыв и вернулся позже. Воздерживайтесь отвечать огнем на огонь.

Не используйте против обидчиков их же тактику: скорее всего, это спровоцирует гриферов на еще более озлобленное поведение.

БЕЗОПАСНОСТЬ ОБЩЕНИЯ В ЧАТАХ

На многих Web-узлах имеются комнаты для бесед, доступ к которым может получить каждый посетитель узла. Каждый, у кого есть доступ в Интернет, может воспользоваться старомодной системой под названием IRC Chat — посиделки в Интернете, которая остается достаточно популярной и в наше время, хотя пользоваться ею достаточно затруднительно.

Сущность сеансов бесед в целом не зависит от типа используемых систем. Каждая комната для бесед имеет свое название, которое обычно определяет тему беседы и по которому иногда можно судить о том, какого типа люди ее ведут. Независимо от того, какая система используется для ведения бесед, каждый участник должен выбрать себе псевдоним (на сленге — ник), который был бы достаточно колоритным и одновременно служил маской истинного имени пользователя. Ввиду тотальной анонимности сеансы бесед являются местом, где, с одной стороны, следует соблюдать особую осторожность поведения.

С другой стороны, беседы ведутся для того, чтобы познакомиться с новыми интересными людьми. Много теплых и чудесных дружеских связей развилось из случайных встреч в комнатах для бесед. Когда вы подключаетесь к группе уже после начала беседы, на экране отображены псевдонимы людей, которые участвуют в беседе, и окно текущего разговора. Если группа дружелюбная, то после вашего появления в группе кто-нибудь наверняка пошлет вам приветствие.

При знакомстве с новым человеком в интерактивной дискуссионной группе, возможно, захочется перейти от общения в общественном чате к более личной беседе с глазу на глаз. Например, можно начать беседу в общей комнате чата, а затем перейти к общению с помощью программы мгновенного обмена сообщениями или переписке по электронной почте.

При использовании этих средств можно по-прежнему обеспечить защиту своей личности путем использования псевдонима (например, псевдоним01@домен.ru). Кроме того, такой тип адреса проще предоставить на случай, если новым контактом окажется человек, с которым необходимо будет прекратить общение.

Взрослым следует быть осторожными и не позволять детям принимать участие в подобных беседах без их наблюдения. Так как, несмотря на то, что существуют специально предназначенные комнаты для бесед детей, в которых предпринимаются некоторые меры предосторожности с целью безопасного общения, в них все равно иногда проникают люди, общение с которыми может оказаться вредным для ребенка. Люди в комнатах для бесед часто говорят неправду о своих занятиях, возрасте, месте жительства и, увы, даже скрывают свой пол.

Кто-то считает себя очень остроумным, кто-то фантазирует, а кто-то по-настоящему болен. Дети, которые общаются в чатах, должны знать, как сделать такое общение безопасным: - не доверять никому личную информацию: место жительства, почтовый адрес, фамилию или телефонный номер, адрес школы, которую посещает ребенок, личные сведения о членах своей семьи, даже если за заполнение подобной формы предложат какой-нибудь приз, и т. п.; - сообщать администратору чата о проявлениях оскорбительного поведения участников; - если ребенку неприятно находиться в чате, его следует покинуть; - если ребенку что-то не понравилось, обязательно следует рассказать об этом родителям; - детям рекомендуется отказываться от участия в личных интерактивных беседах с людьми, которых они не знают в жизни.

Кроме того, если система для ведения бесед поддерживает создание профилей, а кто-то, не имеющий профиля, желает с ребенком пообщаться, следует быть вдвойне осторожным. - не встречаться без ведома и согласия родителей с человеком, с которым познакомились в on-line режиме. 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.

ЗНАКОМСТВА В ИНТЕРНЕТЕ. БЕЗОПАСНОСТЬ ОБЩЕНИЯ,

Безопасность у одних ассоциируется с личной неприкосновенностью, у других с безопасным сексом, у третьих с защитой конфиденциальной информации. Все эти аспекты прямо или косвенно имеют отношение и к Интернет-знакомствам, особенно тем, которые перемещаются в реальную жизнь. Чтобы реальное знакомство оказалось действительно приятным и безопасным, нужно соблюдать несколько простых правил. Прежде всего, не открывать свои личные данные до тех пор, пока вы не уверены в собеседнике. Сюда относятся имя и фамилия, возраст, дата рождения, телефон (сложнее всего с мобильным, поскольку именно он используется для связи, но и здесь можно что-то придумать – например, завести отдельный номер или использовать антиАОН), адрес, место работы или учебы. Сочините небольшую легенду, которую без труда можно будет развеять при более близком знакомстве, удостоверившись в порядочности человека, с которым вы познакомились. Это справедливо при любых целях знакомства – от дружеского общения до создания семьи. И почти всегда встречается с пониманием. Размещение фотографий на сайтах знакомств, безусловно, увеличивает ваши шансы познакомиться, но одновременно и шансы быть узнанными коллегами, если они также посещают их, или недоброжелателями, если таковые у вас есть. Отправка фотографий по почте конкретному адресату – более безопасный вариант. К тому же совсем не обязательно пассивно ждать приглашений к знакомству – можно предпринять собственный поиск и, заинтересовав человека, обменяться фотографиями. Всегда старайтесь до первой реальной встречи убедиться в том, что человек, с которым вы общаетесь, действительно тот, за кого себя выдает. Хотя бы выясните, мужчина это или женщина. Проще всего это сделать по телефону, но можно также исследовать другие источники – например, информацию в ICQ, ЖЖ, на персональном сайте, проверить адреса электронной почты, – в зависимости от того, что вам доступно. Сопоставляйте данные из разных источников и, если обнаружите серьезные расхождения, поинтересуйтесь у вашего нового знакомого или знакомой, почему они не совпадают. Реакция на подобный вопрос тоже достаточно информативна. С людьми, которые не предоставляют о себе вообще никаких сведений, общаться потенциально небезопасно. Хотя вовсе не факт, что они обязательно окажутся маньяками или террористами, но с ними нужно быть предельно осторожными и открываться хотя бы не в большей степени, чем ваш собеседник. Отмечайте неадекватные реакции в процессе виртуального общения, чересчур сильное «застревание» на какой-то определенной теме или замечания о вашем сходстве с каким-либо человеком (кроме политиков, известных спортсменов, фотомоделей и артистов). Все эти признаки могут свидетельствовать о психологических проблемах, которые при непосредственном общении когда-нибудь отразятся и на вас. В лучшем случае ваш собеседник окажется дурно воспитанным или чересчур застенчивым человеком, в худшем – может оказаться психически неуравновешенным или садистом. Назначайте встречи в публичных местах и преимущественно в светлое время суток, или хотя бы не слишком поздно, до тех пор, пока не познакомитесь ближе. Отклоняйте предложение пойти в гости или принять гостей при первой же встрече. Лучшим выбором для нее будут кафе, кино, парк развлечений, любое мероприятие вроде концерта или театрального представления. Наименее безопасны поездки за город. Соблюдение этих мер не гарантирует абсолютную безопасность, но позволяет отсечь наиболее очевидные угрозы, с которыми можно столкнуться при знакомстве в Интернете.

**Материалы для разработки классного часа.**

**Интернет для обучающихся начальных классов.**

***Безопасность детей в Интернете***

Пока мы спорим "пущать" или "не пущать" учеников начальной школы в Интернет - они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык "безопасного" поведения в Интернете. Как?

Проблема относительно «свежая», но, решается «старыми» методами.

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 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? Ну, и в сети все то же самое.

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:

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

- постановка конкретной учебной задачи: что хочу найти? где? как использую?

- формирование навыков критического мышления;

- список проверенных учителем ресурсов, с которых предлагается использовать информацию;

- 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.*

Вступительное слово учителя.

Как вы думаете, ребята, для чего школьникам нужен Интернет?

Варианты ответов:

как площадка для общения (школьные сайты, блоги, форумы; сайты\блоги\форумы по интересам; электронная почта\ аська);

источник информации (использовать Интернет кроме\вместо учебника, графика, справочная информация, литература);

дистанционное обучение (дистанционные курсы, мастер-классы, консультирование болеющих детей и детей на домашнем обучении);

участие в сетевых конкурсах, олимпиадах, проектах.

Послушаем стихотворение о том, как правильно и безопасно пользоваться Интернетом:

***Несколько правил Интернет-безопасности***

1-й чтец:

Интернет бывает разным:

Другом верным иль опасным.

И зависит это все

От тебя лишь одного.

Если будешь соблюдать

Правила ты разные-

Значит для тебя общение

В нем будет безопасное!

Будь послушен и внимательно

Прочти, запомни основательно

Правил свод, что здесь изложен,

Для детишек он не сложен!

2-й чтец:

Если ты не в первый раз

Компьютер сам включаешь

И легко без лишних фраз

Сайты, чаты посещаешь,

Себя в нем мастером считаешь.

Вдруг однажды сам решил

В тайне от родителей

Потихоньку завести

Для общения в сети электронный адрес.

3-й чтец:

Указал без разрешения

Адрес, улицу и дом, и квартиру в нем.

Разместил на сайте ты фотографии семьи.

Не забыл секреты старших - все в анкете указал,

Все, что вспомнил, все, что знал!

Переписываться стал, подписался на рассылку,

Фильмы разные качал.

В общем, пока взрослых нет, заходил ты в Интернет.

4-й чтец:

И теперь сидишь довольный: стал мгновенно знаменит!

О тебе все знают в школе! Что там в школе и в районе,

Во всем мире знаменит! От друзей секретов нету -

Это всем давно известно.

Все тебе охотно пишут

И секреты узнают. Целый мир про вас всё знает

И при встрече сообщает:

«Знаем, знаем, мы читали, фотографии видали.

Прочитали, что твой папа на работу опоздал,

А у мамы из кастрюли суп на плитку убежал.

И про школьные проблемы всё читали и всё знаем!»

5-й чтец:

А по почте счёт пришёл вам за работу Интернета.

Там стоят такие цифры! Что у мамы почему-то

Враз глаза большими стали и обратно не встают.

Потихоньку плачет мама, и сердитый ходит папа.

Ведь они не знают правду, почему их узнают?

Почему по счету нужно им вложить такие деньги?!

6-й чтец:

Все при встрече, сразу быстро им твердят одно и то же:

- Знаем, знаем, прочитали, фотографии видали!...

И воришка, к сожаленью, всё найдёт без промедленья,

Где и что у вас лежит.

А теперь запомни, Друг мой!

Правила не сложные: В Интернете, как и в жизни,

Должен ты всё понимать:

Информацию и фото с мамой вместе размещать.

На рассылку подписаться или мультики скачать,

Должен с нею всё решать!

Хочешь с мамой или с папой - это сам ты выбирай.

В Интернете, как и в жизни, **Безопасность** соблюдай!

- О каких несложных, но очень важных и нужных правилах пользования Интернетом говорится в этом стихотворении?

- Какие еще советы и предложения вы могли бы сами дать своим сверстникам, чтобы их нахождение в сети Интернет было полезным и безопасным?

Ну, и в заключение беседы можно использовать так называемое

***Джентельменское соглашение родителей(учителей) и детей***

Перед первым выходом в Интернет как можно четче 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.

Сообщите ему о том контроле, который Вы намерены осуществлять: проверка посещенных ребенком страниц, контроль времени, проведенного в Сети, проверка адресов электронной почты. Объясните ребенку, что Вы доверяете ему и заботитесь о его безопасности.

Договоритесь с ребенком о соблюдении им следующих правил:

1. Сообщить родителям свое регистрационное имя и пароль, если ребенку разрешено участвовать в чатах или блогах, e-mail адрес и пароль почтового ящика.

2. Никому, кроме родителей, эти сведения сообщать категорически нельзя.

3. Не сообщать без разрешения родителей для каждого отдельного случая личную информацию (домашний адрес, номер телефона, номер школы, место работы родителей).

4. Не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет.

5. Сразу обратиться к родителям, если ребенок увидит нечто неприятное, тревожащее, угрожающее на сайте или в электронной почте.

6. Не соглашаться лично25,26,27,28,29 встретиться с человеком, с которым ребенок познакомился в Сети.

7. Если кто-то предлагает ребенку какой-то "секрет" - тут же сообщить об этом родителям.

8. Не скачивать, не устанавливать, не копировать ничего с дисков или из Интернета без разрешения родителей на каждый отдельный случай.

9. Не делать без разрешения родителей в Интернете ничего, что требует оплаты.

10.Проявлять уважение к собеседникам в Интернете, вести себя так, чтобы не обидеть и не рассердить человека.

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

**Методическая разработка классного часа на тему:**

**«БезОпасный Интернет»**

**(5 – 7 класс)**

**Цель**: Познакомить учащихся с опасностями, которые подстерегают их в Интернете и помочь избежать этих опасностей.

**Подготовительная работа**: классный руководитель проводит опрос учащихся по вопросам:

1. У вас на домашнем компьютере установлен Интернет?
2. Что вам больше всего нравится в Интернете?
3. Как ваши родители воспринимают ваши занятия в  Интернете? Почему?

**Оборудование:** компьютер, проектор, [презентация](file:///C:\Documents%20and%20Settings\Client%205\Local%20Settings\Temp\Rar$DI06.370\Презентация1.pptx), памятка учащимся.

**Ход занятия**

**Учитель:** Раньше подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. И начать наш классный час я хочу с обработанных данных проводимого опроса. Давайте обратим внимание, что наибольший процент ответов на последний вопрос связан с безопасностью в Интернете. И ваши родители во многом правы! Очень большое внимание при работе с Интернетом необходимо уделять именно вопросам безопасности.  И ответить на вопросы: «Какие опасности подстерегают нас в Интернете?» и «Как их избежать?» нам поможет этот классный час.

**Вопрос 1. «Какие опасности подстерегают нас в Интернете?»**

1. **Преступники в Интернете.**

**ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ**.

Преступники преимущественно 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. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим 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 свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

1. **Вредоносные программы.**

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Cети.

1. **Интернет-мошенничество и хищение данных с кредитной карты.**

В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing»,состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

1. **Азартные игры.**

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. В отличие от игровых сайтов, сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

1. **Онлайновое пиратство.**

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и дляличных целей) материалов, защищенных авторскимправом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

1. **Интернет-дневники.**

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут интернет-дневники без ведома взрослых. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

1. **Интернет-хулиганство.**

Так же, как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета. По сути, они те же дворовые хулиганы, которые получают удовольствие, хамя и грубя окружающим.

1. **Недостоверная информация.**

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

1. **Материалы нежелательного содержания.**

К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

**Учитель:** А сейчас мы немного отдохнём. Музыкальная пауза.

(Во время музыкальной паузы учащиеся выполняют движения)

Частушки:

(Руки на пояс, поднимаем плечи по очереди, голову слегка влево, вправо).

Пропоем сейчас частушки,  
Чтоб чуть-чуть нам отдохнуть.  
Про здоровый образ жизни  
Не забудем намекнуть.

(На первые две строчки частушки закрывать глаза руками и открывать, на другие две - потягиваться).

На компьютере играли,  
Наши глазоньки устали,  
А теперь мы отдохнем  
И опять играть начнем.

(Руки на поясе, наклоны влево, вправо).

Нужно спортом заниматься   
И в жару нам, и в мороз,   
Если где-то ты не сможешь,  
То не хмурь уж ты свой нос.

(Хлопать в ладоши).

Мы пропели вам частушки  
Хорошо ли, плохо ли,  
А теперь мы вас попросим,  
Чтобы вы похлопали.

**Учитель:** Мы с вами уже рассмотрели те опасности, которые нам могут встретиться в Интернете. А теперь давайте посмотрим, как этих опасностей можно избежать.

**Вопрос 2. «Как этих опасностей избежать?»**

1. **Преступники в Интернете.**

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 сексуальные намеки. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

1. **Вредоносные программы.**

А) Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла.

Б) Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности.

В) Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.

1. **Интернет-мошенничество и хищение данных с кредитной карты.**

А)Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Б) Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют многие банки в России.

1. **Азартные игры.**

Помните, что нельзя играть на деньги. Ведь, в основном, подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, те, которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

1. **Онлайновое пиратство.**

Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

1. **Интернет-дневники.**

Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

1. **Интернет-хулиганство.**

Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

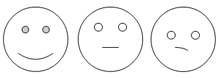
1. **Недостоверная информация.**

Всегда проверяйте собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам.

1. **Материалы нежелательного содержания.**

Используйте средства фильтрации нежелательного материала (например, MSN Premium’s Parental Controls или встроенные в Internet Explorer®). Научитесь критически относиться к содержанию онлайновых материалов и не доверять им.

**Учитель:** А теперь подведём итоги нашего классного часа. У вас на столе лежат три картинки. Выберите и положите перед собой ту, которая соответствует вашему настроению.



* Классный час понравился. Узнал что-то новое.
* Классный час понравился. Ничего нового не узнал.
* Классный час не понравился. Зря время потерял.

**Учитель:** А на память об этом классном часе я хочу подарить каждому из вас [памятку](file:///C:\Documents%20and%20Settings\Client%205\Local%20Settings\Temp\Rar$DI06.370\памятка.docx) по безопасному поведению в Инернете.

В Сети ты можешь встретить все, что угодно – от уроков истории и новостей до нелепых картинок. Но не стоит думать, что, раз информация появилась в Интернете, она является достоверной.

Чтобы разобраться, какой информации в Сети можно, а какой нельзя доверять, следуй простым советам:

1. Относись к информации осторожно. То, что веб-сайт здорово сделан, еще ни о чем не говорит. Спроси себя: за что этот сайт выступает? В чем меня хотят убедить его создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайди в раздел “О нас” или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.

2. Следуй правилу трех источников. Проведи свое расследование и сравни три 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 домашней работе.

3. Как предоставлять достоверную информацию?

Будь ответственным – и в реале, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайне.

4. Не занимайся плагиатом. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его - спроси разрешения.

5. Сообщая о неприемлемом контенте, ты не становишься доносчиком. Наоборот, ты помогаешь делу безопасности Сети.

6. Когда ты грубишь в Интернете, ты провоцируешь других на такое же поведение. Попробуй оставаться вежливым или просто промолчать. Тебе станет приятнее.

7. Все, что ты размещаешь в Интернете, навсегда останется с тобой – как татуировка. Только ты не сможешь эту информацию удалить или контролировать ее использование. Ты ведь не хочешь оправдываться за свои фотографии перед будущим работодателем?

8. Защищай себя – сейчас и в будущем. Подумай, прежде чем что-либо разместить в Интернете.

***И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!***

***Методические материалы для разработки классного часа***

***«Что нужно знать старшекласснику об Интернете?»***

**Юридические аспекты и общие свойства:**

- У Интернета нет собственника, так как он является совокупностью сетей, которые имеют различную географическую принадлежность.

- Интернет нельзя выключить целиком, поскольку маршрутизаторы сетей не имеют единого внешнего управления.

- Интернет стал достоянием всего человечества.

- У Интернета имеется много полезных и вредных свойств, эксплуатируемых заинтересованными лицами.

- Интернет, прежде всего, средство открытого хранения и распространения информации. По маршруту транспортировки незашифрованная информация может быть перехвачена и прочитана.

- Интернет может связать каждый компьютер с любым другим, подключённым к Сети, так же, как и телефонная сеть. Если телефон имеет автоответчик, он способен распространять информацию, записанную в него, любому позвонившему.

- Сайты в Интернете распространяют информацию по такому же принципу, то есть индивидуально, по инициативе читателя.

- Спам-серверы и «зомби-сети» распространяют информацию по инициативе отправителя и забивают почтовые ящики пользователей электронной почты спамом точно так же, как забивают реальные почтовые ящики распространители рекламных листовок и брошюр.

- Распространение информации в Интернете имеет такую же природу, как и слухи в социальной среде. Если к информации есть большой интерес, она распространяется широко и быстро, нет интереса — нет распространения.

- Чтение информации, полученной из Интернета или любой другой сети ЭВМ, относится, как правило, к непубличному воспроизведению произведения. За распространение информации в Интернете (разглашение), если это государственная или иная тайна, клевета, другие запрещённые законом к распространению сведения, вполне возможна юридическая ответственность по законам того места, откуда информация введена.

**Сервисы**

В настоящее время в Интернет существует достаточно большое количество сервисов, обеспечивающих работу со всем спектром ресурсов. Наиболее известными среди них являются:

*электронная почта (E-mail),* обеспечивающая возможность обмена сообщениями одного человека с одним или несколькими абонентами;

*телеконференции, или группы новостей (Usenet),* обеспечивающие возможность коллективного обмена сообщениями;

*сервис FTP* — система файловых архивов, обеспечивающая хранение и пересылку файлов различных типов;

*сервис Telnet*, предназначенный для управления удаленными компьютерами в терминальном режиме;

*World Wide Web (WWW, W3)* — гипертекстовая (гипермедиа) система, предназначенная для интеграции различных сетевых ресурсов в единое информационное пространство;

сервис DNS, или система доменных имен, обеспечивающий возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов;

*сервис IRC*, предназначенный для поддержки текстового общения в реальном времени (chat);

Перечисленные выше сервисы относятся к стандартным. Это означает, что принципы построения клиентского и серверного программного обеспечения, а также протоколы взаимодействия сформулированы в виде международных стандартов. Следовательно, разработчики программного обеспечения при практической реализации обязаны выдерживать общие технические требования.

Наряду со стандартными сервисами существуют и нестандартные, представляющие собой оригинальную разработку той или иной компании. В качестве примера можно привести различные системы типа Instant Messenger (своеобразные Интернет-пейджеры — ICQ, AOl, Demos on-line и т. п.), системы Интернет-телефонии, трансляции радио и видео и т. д. Важной особенностью таких систем является отсутствие международных стандартов, что может привести к возникновению технических конфликтов с другими подобными сервисами.

Для стандартных сервисов также стандартизируется и интерфейс взаимодействия с протоколами транспортного уровня. В частности, за каждым программным сервером резервируются стандартные номера TCP- и UDP-портов, которые остаются неизменными независимо от особенностей той или иной фирменной реализации как компонентов сервиса, так и транспортных протоколов. Номера портов клиентского программного обеспечения так жестко не регламентируются. Это объясняется следующими факторами:

во-первых, на пользовательском узле может функционировать несколько копий клиентской программы, и каждая из них должна однозначно идентифицироваться транспортным протоколом, то есть за каждой копией должен быть закреплен свой уникальный номер порта;

во-вторых, клиенту важна регламентация портов сервера, чтобы знать, куда направлять запрос, а сервер сможет ответить клиенту, узнав адрес из поступившего запроса.

**Услуги**

Сейчас наиболее популярные услуги Интернета — это:

*Всемирная паутина*

*Веб-форумы*

*Блоги*

*Вики-проекты*

*Интернет-магазины*

*Интернет-аукционы*

*Социальные сети*

*Электронная почта и списки рассылки*

*Группы новостей (в основном, Usenet)*

*Файлообменные сети*

*Электронные платёжные системы*

*Интернет-радио*

*Интернет-телевидение*

*IP-телефония*

*Мессенджеры*

*FTP-серверы*

*IRC (реализовано также как веб-чаты)*

*Поисковые системы*

*Интернет-реклама*

*Удалённые терминалы*

*Удалённое управление*

*Многопользовательские игры*

*Web 2.*

**Интернет-зависимость**

С возрастанием популярности Интернета проявились и негативные аспекты его применения. В частности, некоторые люди настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. 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. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в стране таковых 4—6 %.

***Интерне́т-зави́симость*** — 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.

***Происхождение проблемы***

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.

***Интернет-зависимость и официальная медицина***

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. Рост толерантности означает привыкание ко всё бо́льшим и бо́льшим дозам [1]. 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.

***Интернет-зависимые***

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.

***Классификация интернет-зависимости, её причин и симптомов***

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.

5. Киберсексуальная зависимость — навязчивое влечение к посещению порносайтов и занятию киберсексом[3].

***Интернет-зависимость и проблемы в семье***

Проблемы в семье, как правило, возникают в результате недостатка внимания к тому или иному члену семьи. Ссоры и непонимание проблем зависимого человека только усугубляют положение отношений в семье. Так как интернет-зависимый человек поглощает много информации и, возможно, знаний, подобные изменения вызывают внутреннюю напряжённость и обеспокоенность. Семейные скандалы могут лишь еще больше повредить психику человека. Лучший способ решить проблемы семьи — это и любовь, и взаимопонимание, и мудрость домочадцев. Плавно выводить человека на семейное позитивное общение и, главное, увеличивать совместное общение с живой природой, к примеру: с помощью прогулок.

***Пути решения проблемы***

Самый простой и доступный способ решения зависимости — это приобретение другой зависимости. Любовь к здоровому образу жизни, общение с живой природой, творческие прикладные увлечения, такие, как рисование, как правило, выводят человека из зависимости.

Ведущим специалистом в изучении интернет-зависимости сейчас считается Кимберли Янг — профессор психологии Питсбургского университета в Брэтфорде (США), автор известной книги «Пойманные в Сеть» (англ. «Caught in the Net»), переведённой на многие языки. Она также является основателем Центра помощи людям, страдающим интернет - зависимостью (англ. Center for On-Line Addiction). Центр, созданный в 1995 году, консультирует психиатрические клиники, образовательные заведения и корпорации, которые сталкиваются со злоупотреблением интернетом. Центр свободно распространяет информацию и методики по освобождению от интернет-зависимости.