Утверждаю Принято на заседании совета школы

Директор школы \_\_\_\_\_\_\_\_Е.А. Веселова протокол № 08 от «03» октября 2016 г.

Приказ № 178/5 от «04» октября 2016г.

Программа

муниципального общеобразовательного

учреждения средней общеобразовательной

школы №2 п. Селижарово обучения правилам безопасного поведения в Интернет-пространстве, профилактики Интернет-зависимости на 2016-2022 года

**Содержание**

|  |  |  |
| --- | --- | --- |
| 1. | Паспорт программы муниципального общеобразовательного  учреждения средней общеобразовательной школы №2 п. Селижарово обучения правилам безопасного поведения в Интернет- пространстве, профилактики Интернет- зависимости на 2016-2022 года | 3-5 |
| 2. | Пояснительная записка | 5-6 |
| 3. | Цель и задачи | 6 |
| 4. | Сроки и этапы реализации программы | 6 |
| 5. | Участники программы | 6 |
| 6. | Функциональные обязанности участников программы | 7 |
| 7. | Формы проведения мероприятий в ходе реализации программы | 7-9 |
| 8. | Основные мероприятия по обеспечению защиты детей от информации, причиняющей вредих здоровью и развитию | 9-11 |
| 9. | Основные мероприятия по обучению безопасному использованию сети Интернет | 11-12 |
| 10. | Результаты выполнения программы | 12-13 |
| 11. | Методические рекомендации «Безопасный интернет» | 13-22 |
| 12. | Приложения | 22-52 |

**1.Паспорт программы муниципального общеобразовательного** учреждения средней общеобразовательной школы №2 п. Селижарово обучения правилам безопасного поведения в Интернет- пространстве, профилактики Интернет- зависимости на 2016-2022 года

|  |  |
| --- | --- |
| **Наименование программы** | Программа муниципального общеобразовательного учреждения средней общеобразовательной школы № 2 п. Селижарово обучения правилам безопасного поведения в Интернет-пространстве, профилактики Интернет-зависимости на 2016-2022 года |
| **Назначение программы** | Программа является организационно-правовой основой в сфере обучения правилам безопасного поведения в Интернет-пространстве, профилактики Интернет-зависимости в школе |
| **Основание для разработки программы** | Программа разработана в соответствии с:  Федеральным законом РФ «О защите детей от информации, причиняющей вред их здоровью и развитию»  Федеральным законом "Об образовании в Российской Федерации";  Учетом санитарно-эпидемиологических правил и норм;  Законодательством РФ, нормативными муниципальными правовыми актами. |
| **Заказчик программы** | Администрация школы |
| **Основной разработчик программы** | Заместители директора по УВР и ВР |
| **Исполнители программы** | Муниципальное общеобразовательное учреждение средняя общеобразовательная школа №2 п. Селижарово |
| **Цель программы** | Обеспечение информационной безопасности детей и подростков при обучении, при организации внеурочной деятельности и свободном использовании современных информационно-коммуникационных технологий (в частности сети Интернет) |
| **Задачи программы** | Реализация Программы предполагает решение следующих задач:  -формирование и расширение компетентностей работников школы в области медиабезопасного поведения детей и подростков;  -формирования информационной культуры как фактора обеспечения информационной безопасности;  -изучение нормативно-правовых документов по вопросам  защиты детей от информации, причиняющей вред их здоровью и развитию;  -формирование знаний в области безопасности детей использующих Интернет;  -организация просветительской работы с родителями (законными представителями). |
| **Основные направления деятельности** | 1.Создание организационно-правовых механизмов защиты детей от распространения информации, причиняющей вред их здоровью и развитию.  2.Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно - программных и технико - технологических устройств  3.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  4.Информационное просвещение участников образовательного процесса о возможности защиты детей от информации, причиняющей вред их здоровью и развитию |
| **Сроки реализации программы** | Октябрь 2016 года - декабрь 2022 года |
| **Этапы реализации программы развития** | I этап: октябрь-декабрь 2016 г. Диагностико - прогностический, подготовительный.  II этап: январь 2017- сентябрь 2022 г.г.Организационно – практический.  III этап: октябрь-декабрь 2022 г. Контрольно – обобщающий. |
| **Ожидаемые результаты** | - формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;  - формирование информационной культуры как фактора обеспечения информационной безопасности;  - изучение нормативно-правовых документов по вопросам  защиты детей от информации, причиняющей вред их здоровью и развитию;  - формирование знаний в области безопасности обучающихся, использующих Интернет;  - организация просветительской работы с родителями (законными представителями). |
| **Механизм реализации программы** | Программа реализуется через запланированные мероприятия. |
| **Финансирование программы** | Выполнение Программы обеспечивается за счет различных источников финансирования: областной бюджет, районный бюджет, и дополнительные привлеченные средства (спонсорские средства, доходы от дополнительных образовательных услуг, добровольные пожертвования и т.д.). |
| **Контроль исполнения программы** | Администрация школы. |

**2.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 (законных представителей) и самих школьников.

**3. Цель и задачи**

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

Задачи:

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

-формирование информационной культуры как фактора обеспечения информационной безопасности;

-изучение 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 (законными представителями).

**4.Сроки и этапы реализации программы**

*I этап: октябрь-декабрь 2016 г. Диагностико - прогностический, подготовительный.*

*II этап: январь 2017- сентябрь 2022 г.г. Организационно – практический.*

*III этап: октябрь-декабрь 2022 г. Контрольно – обобщающий.*

**5.Участники программы**

Участниками программы являются:

* администрация школы;
* классные руководители, учителя-предметники;
* родители (законные представители) обучающихся;
* обучающиеся школы;
* медицинский работник;
* социальные партнеры.

**6.Функциональные обязанности участников программы**

*Функциональные обязанности администрации школы:*

-общее руководство реализацией программы: организация, координация, контроль;

-организация преподавания вопросов правил безопасного поведения в Интернет-пространстве на уроках;

* обеспечение порядка в ИЦШ;

- контроль проведения воспитательной работы со школьниками по обучению правилам безопасного поведения в Интернет-пространстве.

*Функциональные обязанности классных руководителей, учителей-предметников:*

- проведение бесед о соблюдении правил безопасного поведения в Интернет-пространстве;

воспитание навыков культуры поведения при работе с компьютером;

- проведение мероприятий по преодолению негативного воздействия сети Интернет на детей.

- проведение бесед с родителями (законными представителями) по соблюдению правил детьми безопасного поведения в Интернет-пространстве;

- преподавание вопросов правил безопасного поведения в Интернет-пространстве на уроках;

*Функциональные обязанности родителей (законных представителей) обучающихся :*

-привитие навыков детям соблюдения правил безопасного поведения в Интернет-пространстве;

- проведение мероприятий по преодолению негативного воздействия сети Интернет на детей.

-выполнение рекомендаций классных руководителей и медработников по соблюдению правил безопасного поведения в Интернет-пространстве;

* *Функциональные обязанности обучающихся:*

-соблюдение правил безопасного поведения в Интернет-пространстве;

- соблюдение культуры поведения при работе с компьютером;

*Функциональные обязанности медицинского работника:*

- проведение бесед с обучающимися о нанесении вреда здоровью при несоблюдении правил безопасного поведения в Интернет-пространстве;

- проведение мероприятий по преодолению негативного воздействия сети Интернет на детей.

*Функциональные обязанности социальных партнеров:*

- оказание содействия в реализации программы;

- проведение совместно со школой мероприятий по преодолению негативного воздействия сети Интернет на детей.

**7.Формы проведения мероприятий в ходе реализации программы**

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 оказываются не всегда готовыми 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:

«Школьный сектор. Права и дети в Интернете» <http://schoolsectorp.wordpress.com> ,

«Безопасность» <http://sos-ru.info>,

«Безопасный Интернет» <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 (обществознание, право, ОБЖ и т.д.), а также и во внеурочной деятельности.

Планируется создать в школе «Совет по Интернет – безопасности», в рамках которого обучающиеся будут изучать и создавать проекты по данной тематике, проводить доклады и заседания, что позволит воспитать в школьниках не только культуру общения в сети, но и привить нравственность, ответственность за использование и передачу информации.

Достичь высоких результатов в воспитании невозможно без привлечения родителей (законных представителей). Очень часто родители (законные представители) 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 (законные представители), 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 (законными представителями) проводится разъяснительная работа, т.к. без понимания родителями (законными представителями) данной проблемы невозможно ее устранить силами только образовательного учреждения. Формы работы с родителями (законными представителями) разнообразны: выступления на родительских собраниях, индивидуальные беседы, информация на сайте школы, встречи со специалистами, семинарские занятия.

Разработаны методические рекомендации для родителей (законных представителей) 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 (законных представителей)).

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 МОУ СШ № 2 п. Селижарово 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;

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

-назначены лица, ответственные за организацию доступа к сети Интернет;

-регулярно проводится мониторинг качества предоставления провайдером услуги доступа к сети Интернет школы с обеспечением контент-фильтрации Интернет — трафика.

2.Во исполнение Национальной стратегии действий в интересах детей , 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;

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

**8.Основные мероприятия**

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №  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 программы обучения детей и подростков правилам безопасного поведения в интернет -пространстве, профилактики интернет -зависимости, предупреждения рисков вовлечения в противоправную деятельность, порнографию. | | | 2017-2022 | | | Администрация школы |
| 1.2. | Изучение методических рекомендаций по проведению внеурочных занятий с обучающимися по теме «Приемы безопасной работы в Интернет-пространстве» | | | 2017-2022 | | | Администрация школы |
| 1.3. | Изучение педагогами школы вопросов обеспечения мер информационной безопасности, проблем безопасного поведения в сети Интернет и т.д.. | | | 2017-2022 | | | Администрация школы |
| 1.4. | Разработка информационного курса для родителей (законных представителей) по защите детей от распространения вредной для них информации | | 2017 | | | | Администрация школы |
| 1.5. | Проведение родительских собраний о безопасности детей  в информационно-телекоммуникационной сети Интернет | | 2017-2022 | | | | 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 | | ежегодно | | | | Заместитель директора по УВР |
| 2.2. | Мониторинг функционирования и использования в школе программного продукта, обеспечивающего контент- фильтрацию Интернет-трафика | | 2017-2022 | | | | Ведущий программист |
| 2.3. | Мониторинг качества предоставления провайдером услуги доступа к сети Интернет школы с обеспечением контент- фильтрации Интернет - трафика | | 2017-2022 | | | | Ответственный за использование сети Интернет |
| 2.4. | Стимулирование родителей (законных представителей) к использованию услуги «Родительский контроль», позволяющей устанавливать ограничения доступа к информационно-телекоммуникационной сети Интернет. | 2017-2022 | | | | | Администрация школы |
| **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 медиа-уроков по теме «Информационная безопасность» | | | 2017-2022 | | | Заместитель директора по УВР |
| 3.2. | Проведение ежегодных мероприятий в рамках недели «Интернет-безопасность» для учащихся школы и их родителей | | | 2017-2022 | | | Заместитель директора по УВР |
| 3.3. | Участие в обучающих семинарах по созданию надежной системы защиты детей от противоправного контента в образовательной среде школы и дома. | | | 2017-2022 | | | Заместитель директора по УВР |
| 3.4. | 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 | | | 2017-2022 | | | Заместитель директора по УВР |
| 3.5. | Внедрение и использование программно-технических средств, обеспечивающих исключение доступа обучающихся школы к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания | | | 2017-2022 | | | Заместитель директора по УВР |
| 3.6. | **Мероприятия по антивирусной защите компьютерной техники школы** | | | | 2017-2022 | | Ведущий  Программист |
| **IV. Информационное просвещение участников образовательного процесса 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 | | | 2017-2022 | | Заместитель директора по ВР | |
| 4.2. | Размещение на сайте школы ссылок на электронные адреса по проблемам информационной безопасности для всех участников образовательного процесса | | | 2017-2022 | | Заместитель директора по УВР | |
| 4.3 | Проведение бесед с участием специалистов МУП «Селижаровская ЦРБ» | | | 2017-2022 | | Заместитель директора по ВР | |
| 4.4 | Проведение Дней правовых знаний в рамках гражданско-правового образования | | | 2017-2022 | | Заместитель директора по УВР | |
| 4.5 | Проведение мероприятий в рамках федерального закона «Об ограничении курения табака», борьба с курением и его профилактика | | | 2017-2022 | | Социальный педагог | |
| 4.6 | Проведение мероприятий по профилактике употребления алкоголя | | | 2017-2022 | | Социальный педагог | |
| 4.7 | Проведение мероприятий по противодействию потребления наркотических средств и их незаконному обороту | | 2017-2022 | | | Социальный педагог | |
| 4.8 | Осуществление других мероприятий по реализации программы | | 2017-2022 | | | Заместитель директора по УВР | |

**9. Основные мероприятия по обучению безопасному использованию сети Интернет**

Перечень мероприятий по обучению школьников безопасному использованию сети Интернет:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Мероприятия | Сроки проведения | Ответственные |
| 1 | Уроки безопасности работы в Интернет для учащихся 1–4, 5–9, 10– 11 классов. | Ежегодно, в соответствии с планом работы школы | Заместитель директора по ВР |
| 2 | Изучение нормативных документов по организации безопасного доступа к сети Интернет | Ежегодно, в соответствии с планом работы школы | Администрация школы |
| 3 | Организация и проведение конкурса детских работ «Мой безопасный Интернет» с номинациями:  Рисунок (1-4 классы),  Плакат (5-7 классы),  Рассказ о позитивном контенте («Мои любимые сайты», «Любимые сайты нашей семьи») и т.д. | Ежегодно, в соответствии с планом работы школы | Заместитель директора по ВР |
| 4 | Круглый стол «Основы безопасности в сети Интернет» и т.д. | Ежегодно, в соответствии с планом работы школы | Заместитель директора по УВР |
| 5 | Классные часы в 1- 11 классах.  Цель: ознакомление учащихся с опасностями, которые подстерегают их в Интернете.  «Сказка о золотых правилаз безопасности в сети Интернет» (1 кл.)  «Чем опасен интернет» (1-4 кл.); «Безопасность в сети Интернет» (5-6 кл.); «Компьютерные сети» (5-8 кл.);  «Темная сторона Интернета» (7-8 кл.), «Опасности в Интернете», «Остерегайся мошенничества в Интернете»  (9-11 кл.) и другие | Ежегодно, в соответствии с планом работы школы | Заместитель директора по ВР |
| 6 | На уроках информатики проведение бесед, диспутов: «Безопасность при работе в Интернете», «О личной безопасности в Интернет», «Сетевой этикет», «Этика сетевого общения » (7-8 классы), «Форумы и чаты в  Интернет», «Информационная безопасность сетевой технологии работы» (9-11 классы) и т.д. | Ежегодно, в соответствии с планом работы школы | Заместитель директора по УВР |
| 7 | Родительское собрание на тему: «Быть или не быть Интернету в компьютере вашего ребенка?»  Анкетирование «Знают ли родители, с кем общается их ребенок в сети?» | Ежегодно, в соответствии с планом работы школы | Заместитель директора по ВР |
| 8 | Изготовление памяток и буклетов для детей:  а) «Защити себя сам!» (советы детям для безопасного поиска в Интернете). б) «Интернет-ресурсы для детей» (полезные сайты) и т.д. | Ежегодно, в соответствии с планом работы школы | Заместитель директора по ВР |

**10. 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, при организации внеурочной деятельности и свободном использовании современных информационно-коммуникационных технологий, в том числе в сети Интернет. | |
| Задача №1: формирование и расширение компетентностей работников школы в области медиабезопасного поведения детей и подростков; | - Использование всеми педагогами современного коммуникационного взаимодействия (доля педагогов, использующих современных коммуникационных взаимодействий в процентах ежегодно) |
| - Умение использовать и интегрировать разнотипную информацию ( доля педагогов, умело использующих разнотипную информацию в процентах ежегодно) . |
| Задача № 2: формирование информационной культуры как фактора обеспечения информационной безопасности; | - Использование всеми педагогами сетевых технологий, современных средств связи и прикладных программ в области профессиональной деятельности (доля педагогов использующих сетевые технологии, современные средства связи и прикладные программы в области профессиональной деятельности в процентах ежегодно). |
| Задача № 3: изучение нормативно-правовых документов по вопросам  защиты детей от информации, причиняющей вред их здоровью и развитию; | - Владение правовыми знаниями в области информатизации ( доля участников образовательного процесса владеющих правовыми знаниями в области информатизации в процентах ежегодно). |
| 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 ( доля участников образовательного процесса владеющих знаниями о защите компьютера от вредоносных программ, о нелегальном, пиратском контенте и об опасности его скачивания в процентах ежегодно). |
| Задача № 5: организация просветительской работы с родителями (законными представителями). | - Включение родителей (законных представителей) в совместную со школой деятельность по обеспечению безопасности детей в Интернет пространстве ( доля родителей (законных представителей), включенных в совместную со школой деятельность по обеспечению безопасности детей в Интернет пространстве в процентах ежегодно) |

**11.Методические рекомендации «Безопасный Интернет»**

В наши дни компьютер становится привычным элементом не только в научных лабораториях, но и дома, в школьных классах. Так, например, в Российской Федерации в настоящее время уже эксплуатируется не менее 5 млн. персональных компьютеров. В Западной Европе компьютер используют свыше 60% взрослого населения. Людей, ежедневно проводящих за компьютером по нескольку часов, становится все больше. При этом уже мало кто сомневается, что работа на персональном компьютере влияет на физическое и психологическое здоровье человека не самым лучшим образом. Длительное пребывание у экрана, неподвижность позы пользователя ПК, электро­магнитные поля и излучения, мелькание изображения на экране – все это небез­вредно для здоровья.

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет - это не только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них - дети, которые могут не знать об опасностях мировой паутины. Одним из средств решения этой проблемы может стать просвещение общественности и специальная подготовка профессионалов, в первую очередь, педагогов в сфере безопасного поведения человека, специалиста, школьника в мире компьютерных технологий и Интернет. Интернет должен быть максимально безопасным для подрастающих поколений. Эта цель осуществима, если родители осознают свое главенство в обеспечении безопасности детей. В данных методических рекомендациях представлены материалы для разработки уроков, классных часов, направленные на обеспечение необходимыми знаниями в области психолого-педагогического и здоровье-сберегающего сопровождения образовательного процесса школьников, использующих персональные компьютеры и Интернет в профессиональной, учебной и внеучебной деятельности, родительских собраний. Методические рекомендации содержат советы, как сделать компьютер и Интернет безопасным для своего ребенка.

Данные рекомендации - практическая информация для родителей (законных представителей) и классных руководителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

**Анкетирование учащихся.**

Для изучения безопасности в сети Интернет и отношения к ней подростков разрабатываются анкеты, позволяющие проанализировать современную ситуацию в образовательной среде.Анкетирование предполагается проводить в форме анонимного опроса как на бумажных носителях, так и в электронном виде. Примерные формы анкет представлены в Приложении 1 и Приложении 2.

**Проведение круглого стола**

**«Основы безопасности в сети Интернет»**

Цель: формирование устойчивых жизненных навыков при работе в сети Интернет.

Работе круглого стола предшествует предварительная подготовка учащихся по предложенной тематике. Перечень вопросов для обсуждения выявляется в результате анкетирования учащихся.

Примерные вопросы для обсуждения:

1. Для чего нужен Интернет?

2. Какие существуют риски при пользовании интернетом, и как их можно

снизить?

3. Какие виды мошенничества существуют в сети Интернет?

4. Как защититься от мошенничества в сети Интернет?

5. Что такое безопасный чат?

6.Виртуальный собеседник предлагает встретиться, как следует поступить?

7. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений.

При подведении итогов круглого стола обучающимся можно предложить правила поведения в сети Интернет (Приложение 3).

**Проведение компьютерной игры для младших школьников**

В рамках классного часа или урока информатики (окружающего мира) обучающимся 2-4 классов целесообразно предложить компьютерную игру о правилах поведения в сети Интернет Прогулка через ИнтерНетЛес (<http://www.wildwebwoods.org/popup.php?lang=ru>), где в игровой форме показано какие опасности могут встречаться при работе в сети Интернет, рассказано о сетевом взаимодействии и об этикете, а также о защите прав детей.

**Конкурс буклетов "Правила поведения в сети Интернет"**

Целью данного конкурса является формирование у учащихся четкого представления о правилах поведения в сети Интернет.

Данный конкурс проходит в два этапа: заочный и очный. За 14 дней предлагается определенная тематика конкурсных заданий, разрабатывается критериальный аппарат, даются методические рекомендации по составлению буклета. Данный конкурс проходит в два этапа: заочный и очный. За 14 дней предлагается определенная тематика конкурсных заданий.

Заочный этап предполагает анализ и отбор 20 лучших работ, отобранных экспертной комиссией, в состав которой входят как педагоги, так и учащихся.

Очный этап конкурса предполагает публичную защиту буклета и

ответы на вопросы одноклассников. По результатам данного этапа определяется победитель.

**Проведение тематического классного часа**

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

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

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

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

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

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

**Ожидаемые результаты:**

В ходе проведения классного часа дети должны научиться делать более безопасным и полезным свое общение в Интернете и иных информационно- телекоммуникационных сетях, а именно:

-критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

-отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;

-избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

-распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

-распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;

-критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

-анализировать степень достоверности информации и подлинность ее источников;

применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

При организации классного часа важно исходить из возрастных особенностей учащихся, учесть уровень их знакомства с Интернетом.

Организовать проведение классного часа необходимо таким образом, чтобы несовершеннолетние не только получили необходимый минимум знаний об информационной безопасности, но смогли *высказать свою точку зрения на указанную проблему.*

При определении **содержания, форм и методики** проведения единого классного часа важно учитывать:

необходимость деятельностного подхода в учебной работе учащихся в активном и интерактивном режиме;

целесообразность использования методик учебного сотрудничества, различных вариантов работы в группах, кооперации, моделирования жизненных ситуаций.

**Образовательные технологии**

|  |  |  |
| --- | --- | --- |
| № п/п | Виды учебной работы | Образовательные технологии |
| 1 | Лекция | *Проблемное обучение, визуализация* |
| 2 | Практические занятия | *Деловая игра, разбор конкретных ситуаций, практическая работа, технология развития критического мышления, технология Дебаты, авторская мастерская* |
| 3 | Реферат, проектирование | *Проектная деятельность,*  *исследовательская работа.* |

При определении тематики бесед для единого классного часа Безопасный Интернет необходимо исходить:

-из понимания важности и значимости для каждого человека основ медиакультуры;

-из возможности в доступных игровых ситуациях знакомить обучающихся с основами медиакультуры;

-из необходимости приобретения обучающимися первичного опыта регулирования медиаотношений;

-из необходимости получения обучающимися знаний и навыков использования конкретных правил и норм медиаобразования и первичного опыта разработки собственных правил медиакультуры.

Темы бесед с 1 по 11 класс могут быть следующие:

- Интернет среди нас.

- Я и мои виртуальные друзья.

- Интернет в моей семье.

- Мой Интернет.

- Интернет и природа.

- Мой социум в Интернете.

- Интернет и моя будущая профессия.

- Интернет в современной школе.

- Интернет и мое здоровье и т.д.

Освоение медиа–безопасности наиболее эффективно в совместной деятельности со взрослыми. Поэтому желательно привлечь родителей (законных представителей), представителей органов исполнительной власти, правоохранительных, органов, общественных организаций.

При проведении уроков в начальной школе рекомендуется использовать материалы, размещенные:

- на сайте интерактивного курса по Интерент-безопасности (<http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu>. htm) в разделе Для учащихся рассказы для детей 7-10 лет, а также в разделе Тесты (можно организовать on-line тестирование школьников 7-10 лет);

- на сайте (http://www.onlandia.jrg.ua/ru-RU/) On-ляндия. Безопасная

веб-страна в разделе Для детей 7-10 лет рассказы в картинках, задания и вопросы;

- на сайте (<http://content-filtering.ru/aboutus/>) Информационно- аналитический ресурс Ваш личный Интернет в разделе Юным пользователям - Дошкольники и младшие классы подсказки и советы по безопасному поведению в сети Интернет;

- на сайте (<http://stopfraud.megafon.ru/>) федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах Виды мошенничества и Наши рекомендации , а также советы родителям;

- на портале Безопасный интернет (<http://www.saferinternet.ru/>) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме Безопасный интернет .

- в качестве видео заставки для классного часа или урока можно использовать <http://youtu.be/789j0eDglZQ> мультфильм Безопасный интернет , который разработала студия Mozga.ru.

- на сайте Началка.ком материалы по безопасному интернету (<http://www.nachalka.com/taxonomy/term/335>).

При проведении уроков в 5-9 классах рекомендуется использовать материалы, размещенные:

- на сайте интерактивного курса по Интерент-безопасности (http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu. htm) в разделе Для учащихся рассказы для детей 11-16 лет, а также в разделе Тесты (можно организовать on-line тестирование школьников 11- 14 лет);

- на сайте (<http://www.onlandia.org.ua/ru-RU/>) On-ляндия. Безопасная веб-страна в разделе Для детей 11-14 лет рассказы в картинках, задания и вопросы; в разделе Для учителей опасности в сети и поведение в сети;

- на сайте (<http://content-filtering.ru/aboutus/>) Информационно- аналитический ресурс Ваш личный Интернет в разделе Юным пользователям - Средние классы подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;

- на сайте <http://stopfraud.megafon.ru/> федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах Виды мошенничества и Наши рекомендации , а также советы родителям;

- на портале Безопасный интернет (<http://www.saferinternet.ru/>) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме Безопасный интернет.

При проведении уроков в 10-11 классах рекомендуется использовать материалы, размещенные:

- на на сайте интерактивного курса по Интерент-безопасности (http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu. htm) в разделе Для учащихся рассказы для детей 11-16 лет, а также в разделе Тесты (можно организовать on-line тестирование школьников 11-14 лет);

- на сайте (<http://www.onlandia.org.ua/ru-RU/>) On-ляндия. Безопасная веб-страна в разделе Для подростков советы по безопасному общению и работе в режиме on-line; в разделе Для учителей опасности в сети и поведение в сети;

- на сайте (<http://content-filtering.ru/aboutus/>) Информационно- аналитический ресурс Ваш личный Интернет в разделе Юным пользователям - Старшие классы подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;

- на сайте <http://stopfraud.megafon.ru/> федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах Виды мошенничества и Наши рекомендации, а также советы родителям;

- на портале Безопасный интернет (<http://www.saferinternet.ru/>) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме Безопасный интернет.

**Дополнительные Интернет-ресурсы для проведения классного часа:**

- Справочник по детской безопасности в Интернет от Google (<http://www.google.ru/familysafety/>);

- Сайт советов по работе на компьютере ([http://shperk.ru/sovety/kak-sdelat-internet-dlya-detej-bolee bezopasnym.html](http://shperk.ru/sovety/kak-sdelat-internet-dlya-detej-bolee%20bezopasnym.html));

- Сайт Компьютерная безопасность. Безопасность жизни (<http://blog.chljahsoft.net/3167>);

- Сайт Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт (<http://i-deti.org/>);

- Буклет Безопасный интернет детям Министерства внутренних дел РФ (<http://www.mvd.ru/userfiles/liflets_k_deti_06.pdf>);

- Материалы III ежегодного Форума Безопасного Интернета (<http://safor.ru/prezentacii11.php>);

- Сайт Дети России Онлайн (<http://detionline.com/>).

**Проведение родительских собраний**

Родительские собрания целесообразно проводить по ступеням возрастного развития учащихся (начальная ступень образования, основная ступень образования, старшая ступень образования).

В начале родительского собрания рекомендуется провести анонимное анкетирование, которое позволит выявить отношение родительской общественности к внедрению в образовательный процесс ИКТ. По результатам анкетирования будет определена дальнейшая стратегия работы ОУ по безопасности детей в сети Интернет. Примерный перечень вопросов анкетирования в Приложении 4.

После анкетирования проводится беседа по проблеме доступа ребенка к сети Интернет, в которой поднимаются наиболее актуальные вопросы.

Далее даются рекомендации родителям по работе детей в сети Интернет (с учетом возрастных особенностей) (Приложение 5).

В конце родительского собрания всем родителям предлагается памятка по безопасности детей в сети Интернет при помощи программных средств (Приложение 6).

**Урок Интернет-безопасность**

(на всех уровнях обучения)

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

1) информирование обучающихся о видах информации, способной

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

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

3) ознакомление обучающихся с международными принципами и

нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

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

5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

В ходе уроков Интернет - безопасности учащиеся должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно:

критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;

избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;

критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

анализировать степень достоверности информации и подлинность ее источников;

применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

**В рамках урока Интернет-безопасность в начальных классах** целесообразно ознакомить обучающихся:

– с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Рекомендуется продемонстрировать возможности детских поисковых систем: <http://kids.quintura.ru>, <http://agakids.ru> и детского браузера <http://www.gogul.tv>, а также познакомить с детскими социальными сетями: http://cyberpapa.ru/, http://interneshka.net/, http://kinder- online.ru/detskiy\_portal.html, http://1dnevnik.ru/, http://www.detkino.ru.

Для отбора содержания урока могут быть использованы материалы сайта www.detionline.com (видеоматериалы, материалы электронного журнала Дети в информационном обществе , материалы Линии помощи), а также материалы других сайтов, содержащих информацию по безопасному использованию сети Интернет.

Большое значение для эффективности урока Интернет-безопасности имеет не только содержание, но и форма его проведения. Целесообразно использовать для 1-4 классов – урок-путешествие, урок-викторину, урок- соревнование, урок-игру, беседу.

**Полезные ссылки:**

- [http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon\_ metsa.html](http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon_%20metsa.html) – о правилах безопасного поведения в сети Интернет с элементами интерактива;

- <http://www.nachalka.com/node/948> - учебное видео Как обнаружить ложь и остаться правдивым в Интернете ;

- <http://content-filtering.ru/aboutus/> - информационно-аналитический

ресурс Ваш личный Интернет.

**В ходе урока Интернет-безопасность в среднем звене** целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве: Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.); № 252-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки.)

Ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможны следующие формы проведения урока: урок - пресс- конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными администраторами и т.д.

**Полезные ссылки:**

1) [http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma\_ro oma.html](http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_ro%20oma.html) - молодежная история с элементами интерактива;

2) <http://content-filtering.ru/aboutus> - информационно-аналитический

ресурс Ваш личный Интернет;

3) [www.icensor.ru](http://www.icensor.ru) - Интернет-фильтр.

**В рамках урока Интернет-безопасность в старших классах** целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве (см. рекомендации для проведения урока Интернет–безопасности в среднем звене).

Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:

- информация, запрещенная для распространения среди детей;

- информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:

- перечень рисков, подстерегающих ребенка в сети Интернет;

- рекомендации по грамотному использованию электронной почты;

- технологии безопасного общения в средах мгновенного обмена

сообщениями;

Необходимо обеспечить обучающихся инструкциями по безопасному общению в чатах; советами по профилактике и преодолению Интернет - зависимости; общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете: нежелательные программы; защита личных данных; мошенничество; виртуальные “друзья”; пиратство; on-line-игры; этика; критический подход к информации.

Обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации.

Ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм Интернет-безопасность, дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

**Полезные ссылки:**

1) <http://www.kaspersky.ru> – антивирус Лаборатория Касперского ;

2) <http://www.onlandia.org.ua/rus/>- безопасная web-зона;

3)http://www.interneshka.net международный онлайн-конкурс по безопасному использованию Интернета;

4) http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета;

5) <http://content-filtering.ru> – Интернет СМИ Ваш личный Интернет;

6) <http://www.rgdb.ru> – Российская государственная детская библиотека.

Примерный план-конспект урока на тему БезОпасный Интернет приведен в Приложении 7.

По итогам проведения уроков проводится итоговое анкетирование по теме Безопасный интернет (Приложение 8).

**Проведение внеклассного мероприятия**

**Сказка о золотых правилах безопасности в сети Интернет**

Сказку целесообразно подготовить силами обучающихся 5-6 классов и представить ее обучающимся начальной школы.

При разработке сценария внеклассного мероприятия Сказка о золотых правилах безопасности в сети Интернет значимую роль играет сам педагог, так как именно от него зависит своевременность и актуальность представленного материала.

Обсуждение сказки позволит младшим школьникам определить собственную позицию организации работы в сети Интернет. Примерный сценарий сказки приведен в Приложении 9.

По окончании внеклассного мероприятия обучающимся раздаются памятки с семью золотыми правилами работы в сети Интернет. (Приложение 10).

**Список используемой литературы**

1.П.Н.Дерянин, О.О.Михальский, Д.И.Правиков, А.Ю.Щербаков. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.

2**.** А.Г.Асмолов, А.Л.Семенов, А.Ю.Уваров.Российская школа и новые информационные технологии: взгляд в будущее десятилетие.- М.:, 2010

3. Г.У.Солдатов, М.И.Лебешева. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников?//Журнал «Дети в информационном обществе» - М., 2011, №8 – СС.46-55.

4. Г.У.Солдатов, Е.И.Рассказова. Из-за интернета я не ел и не спал». Зависимость или новый образ жизни?//Журнал «дети в информационном пространстве - М., 2011, №9 – СС. 22-29

5. Г.У.Солдатов, Е.И.Рассказова. Как им помочь. Ребенок к Интернете: запрещать, наблюдать или объяснять?//Журнал «дети в информационном пространстве - М., 2011, №10 – СС. 26-33

6. Интернет-ресурсы:

<http://ipk.68edu.ru/docs/bezopasnostdeti/bezopasnyi-internet-dlya-pedagogov.pdf>

<http://orgpsiholog.ru/pr.bezop.htm>

<http://gldn.ur.ru/support/security/work/>

<http://www.kuzbass.net/security.html>

[http://www.interneshka.net](http://www.interneshka.net/)

[http://www.saferinternet.ru](http://www.saferinternet.ru/)

[http://content-filtering.ru](http://content-filtering.ru/)

<http://www.pkdb.ru/detyam/gostinaya/web-resursy.html>

<http://i-deti.org/>

<http://mvd.ru/userfiles/liflets_k_deti_06.pd>

<http://ppt4web.ru/informatika/pravila-bezopasnosti-v-internete.html>

<http://www.myshared.ru/slide/265508/>

<http://www.kultura.kurganobl.ru/assets/files/pdf_dokument/2013/04-13/Bezop_int.pdf>

**12.Приложения**

**Приложение 1**.

Анкета №1 Осторожно, вирус!

Что является основным каналом распространения компьютерных вирусов?

1. Веб-страницы

2. Электронная почта

3. Флеш-накопители (флешки)

Для предотвращения заражения компьютера вирусами следует:

1. Не пользоваться Интернетом

2. Устанавливать и обновлять антивирусные средства

3. Не чихать и не кашлять рядом с компьютером

Если вирус обнаружен, следует:

1. Удалить его и предотвратить дальнейшее заражение

2. Установить какую разновидность имеет вирус

3. Выяснить как он попал на компьютер

Что не дает хакерам проникать в компьютер и просматривать файлы и документы:

1. Применение брандмауэра

2. Обновления операционной системы

3. Антивирусная программа

Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?

1. Уничтожение компьютерных вирусов

2. Создание и распространение компьютерных вирусов и вредоносных программ.

3. Установка программного обеспечения для защиты компьютера.

**Приложение 2**.

Анкета №2 Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?

1. Свои увлечения

2. Свой псевдоним

3. Домашний адрес

2. Чем опасны социальные сети?

1. Личная информация может быть использована кем угодно в разных целях

2. При просмотре неопознанных ссылок компьютер может быть взломан

3. Все вышеперечисленное верно

3. Виртуальный собеседник предлагает встретиться, как следует поступить?

1. Посоветоваться с родителями и ничего не предпринимать без их согласия.

2. Пойти на встречу одному

3. Пригласить с собой друга

4. Что в Интернете запрещено законом?

1. Размещать информацию о себе

2. Размещать информацию других без их согласия

3. Копировать файлы для личного использования

5. Действуют ли правила этикета в Интернете?

1. Интернет - пространство свободное от правил

2. В особых случаях

3. Да, как и в реальной жизни.

**Приложение** **3.**

Круглый стол Основы безопасности в сети Интернет

Правила работы в сети Интернет

1. Не входите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.

3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.

4. Никогда не посылайте никому свой пароль.

5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. При общении в Интернет не указывать свои личные данные, а использовать псевдоним (ник).

7. Без контроля взрослых ни в коем случае не встречаться с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.

9. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.

10. Не всей той информации, которая размещена в Интернете, можно верить.

11. Не оставляйте без присмотра компьютер с важными сведениям на экране.

12. Опасайтесь подглядывания через плечо.

13. Не сохраняйте важные сведения на общедоступном компьютере.

**Приложение 4.**

Материалы для проведения родительского собрания.

Анкета для родителей.

Уважаемые родители! В школе информационные технологии применяются в различных направлениях: учебная деятельность (урочная и внеклассная), воспитательная (классные часы и различные школьные мероприятия), ИКТ являются основой единого информационного пространства школы (администрация школы, учитель, ученик, родитель) - сайт школы, работа "Электронного журнала", учебно-материальная база школы, цифровые образовательные ресурсы и т.п. В том числе, информационные технологии прочно вошли в деятельность и досуг детей. Просим Вас ответить на несколько вопросов. (Все вопросы не являются обязательными для ответа. Если Вы выбираете "другое" - не забудьте поставить напротив галочку).

1. В каком классе учится Ваш ребенок?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Отношение к внедрению ИТ в образование. Внедрение информационных технологий (ИТ) в образование относится к числу крупномасштабных инноваций, пришедших в российскую школу в последние десятилетия. Среди ИТ, внедряемых в сфере образования, можно выделить следующие: обучающие, тренажеры, справочные, единые информационными образовательные пространства (сайт школы, дистанционное обучение, электронные дневники), техническое обеспечение кабинетов и др.

скорее положительно

скорее отрицательно (не вижу необходимости) Другое:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Использование информационные технологии в школе

- различные мероприятия с применением информационных технологий (проектная деятельность, уроки, классные часы и родительские собрания)

- урок, с применением новых информационных технологий более

популярен у моего ребенка (более интересен, понятен и т.п. - со слов

ребенка)

- ребенок с интересом и удовольствием выполняет проекты (рефераты, доклады), используя компьютер

- ребенок готовится к уроку, используя компьютер (Интернет, полезные ссылки на сайте школы, рекомендуемые учителем сайты и т.п.)

- классный руководитель проводит родительские собрания с использованием компьютера

Другое: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Работа "Электронного журнала".

Одной из возможностей ресурса является просмотр на страницах этого ресурса в Интернете оценок учащегося, которые выставляют учителя на уроках и их комментарии, домашнего задания... (пароль доступа индивидуален для каждого пользователя)

- в нашем классе есть "Электронный журнал", его работа очень важна для нас

- в нашем классе есть "Электронный журнал", но в его работе нет необходимости

- возможности "Электронного журнала" очень важные, но в нашем классе он не работает

- в нашем классе он не работает и думаю, что нет в нем необходимости

Другое:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5. Посещение Школьного сайта

- часто посещаем (в том числе раздел Новости)

- очень редко посещаем

- не посещаем

Другое:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Школьный сайт.

Напишите, пожалуйста, что бы Вы хотели бы изменить в работе сайта. Ваши предложения и рекомендации Вы можете написать в этом разделе\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Есть ли у Вас дома компьютер?

- да (один)

- да (несколько)

- нет

Другое:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Кто пользуется компьютером у Вас дома?

- только родители

- только ребенок

- все члены семьи (родители и дети)

Примерный список вопросов, которые планируется обсудить на

родительском собрании

1. В каком возрасте следует разрешить детям посещение интернета?

2. Следует ли разрешать детям иметь собственные учетные записи электронной почты?

3. Какими внутрисемейными правилами следует руководствоваться при использовании интернета?

4. Как дети могут обезопасить себя при пользовании службами

мгновенных сообщений?

5. Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, Mail Agent)?

6. Могут ли дети стать интернет-зависимыми?

7. Что должны знать дети о компьютерных вирусах?

8. Как проследить какие сайты посещают дети в интернете?

9. Что следует предпринять, если моего ребенка преследуют в интернете?

10. Помогает ли фильтрующее программное обеспечение?

11. На какие положения политики конфиденциальности детского сайта нужно обращать внимание?

12. Какие угрозы встречаются наиболее часто?

13. Как научить детей отличать правду ото лжи в Интернет?

**Приложение 5.**

Рекомендации для родителей (законных представителей)

детей различных возрастных категорий.

Возраст от 7 до 8 лет

Находясь в Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интеренета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.

Запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

Советы по безопасности в сети Интернет

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый белый список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте специальные детские поисковые машины, типа MSN Kids Search (<http://search.msn.com/kids/default.aspx?FORM=YCHM>).

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

Научите детей не загружать файлы, программы или музыку без вашего согласия.

Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

Подробнее о таких фильтрах

http://www.microsoft.com/rus/athome/security/email/fightspam.mspx

Не разрешайте детям использовать службы мгновенного обмена сообщениями.

В белый список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.

Не делайте табу из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты для взрослых.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах.

Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Не забывайте беседовать с детьми об их друзьях в Интернет.

Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.

Позволяйте детям заходить только на сайты из белого списка, который создайте вместе с ними.

Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

Приучите детей не загружать программы без вашего разрешения.

Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Расскажите детям о порнографии в Интернет.

Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст от 13 до 17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок для взрослых . Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов ( черный список ), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).

Компьютер с подключением к сети Интернет должен находиться в общей комнате.

Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни.

Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

Используйте средства блокирования нежелательного контента, как дополнение к стандартному Родительскому контролю.

Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

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

Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

Приучите детей не загружать программы без вашего разрешения.

Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Расскажите детям о порнографии в Интернет.

Расскажите детям о порнографии в Интернет.

Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

Приучите себя знакомиться с сайтами, которые посещают подростки.

Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

**Приложение 6.**

**Примерный макет памятки**

****



**Приложение 7.**

**План - конспект урока на тему: БезОпасный Интернет**

**9-11 классы**

**Цель:** обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

**Задачи:**

- изучение информированность пользователей о безопасной работе в сети Интернет;

- знакомство с правилами безопасной работы в сети Интернет;

- ориентироваться в информационном пространстве; способствовать ответственному использованию online-технологий;

- формирование информационной культуры обучающихся, умения самостоятельно находить нужную информацию, пользуясь web-ресурсами;

- воспитание дисциплинированности при работе в сети.

*Учащиеся должны знать:*

перечень информационных услуг сети Интернет;

правилами безопасной работы в сети Интернет;

опасности глобальной компьютерной сети.

*Учащиеся должны уметь:*

ответственно относиться к использованию on-line-технологий;

работать с Web-браузером;

пользоваться информационными ресурсами;

искать информацию в сети Интернет.

**Тип урока:** урок изучения нового материала.

**Методы и формы обучения:** словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

**Ссылки на web-ресурсы:**

1) <http://www.kaspersky.ru> – антивирус Лаборатория Касперского ;

2) <http://www.onlandia.org.ua/rus/> - безопасная web-зона;

3) <http://www.interneshka.net> – международный онлайн-конкурс по

безопасному использованию Интернета;

4) http://www.saferinternet.ru - портал Российского Оргкомитета по

безопасному использованию Интернета;

5) <http://content-filtering.ru> – Интернет СМИ Ваш личный Интернет ;

6) <http://www.rgdb.ru> – Российская государственная детская библиотека.

**Этапы урока:**

1. Организация начала урока. Постановка цели урока.

Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/\_myvideo/1.html

Постановка темы и главного вопроса урока.

2. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).

3. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.

4. Закрепление изученного материала. Рекомендации по правилам

безопасной работы. Тестирование.

5. Подведение итогов урока. Оценка работы группы. Домашнее задание.

**Ход урока**

**1. Организация начала урока. Постановка цели урока.**

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всем мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И ни когда-то, а прямо сейчас. (Просмотр видеоролика Дети и Интернет – 1 мин. (по выбору) (<http://www.youtube.com/watch?v=HbVgg6->

3EWo&feature=autoplay&list=PLD70B32DF5C50A1D7&playnext=1 Как оставаться в безопасности на YouTube

http://www.youtube.com/watch?v=AMCsvZXCd9w&feature=BFa&list=PLD70B

32DF5C50A1D7&lf=autoplay Остерегайся мошенничества в Интернете

<http://www.youtube.com/watch?v=xRSnLKveMpY&feature=relmfu> Мир глазами Gmail - ЗАЩИТА ОТ СПАМА)

Как не стать жертвой сети Интернет? Тема нашего урока - Безопасный Интернет.

Главный вопрос урока: Как сделать работу в сети безопасной?

**2. Изучение нового материала.**

Игра За или против.

Учитель предлагает игру За или против . На слайде - несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!

2. Интернет – это глобальный рекламный ресурс. И это хорошо!

3. Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.

4. Интернет является мощным антидепрессантом.

5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли

Учитель предлагает обучающимся ответить на вопросы Какие опасности подстерегают нас?, Какие виртуальные грабли лежат у нас на пути? (Целесообразно заранее нескольким обучающимся подготовить короткие сообщения по темам: Интернет-зависимость, Вредоносные и нежелательные программы, Психологическое воздействие на человека через Интернет , Материалы нежелательного содержания , Интернет-мошеники.)

**Физкульт. минутка**. Соберите рукопожатия.

Участникам предлагается в течение 10 секунд пожать руки как можно большего числа других людей.

Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Если – да, то чем он был вызван?

Анализ ситуации.

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия? Однако, очень важно знать, что есть рядом люди, готовые выслушать, оказать поддержку, помочь в трудную минуту

Учитель предлагает ответить на главный вопрос урока – Как сделать работу в сети безопасной?

**3. Практическая часть.**

- Что можно? Что нельзя? К чему надо относиться осторожно?

Обучающимся предлагается посмотреть ресурсы

http://content-filtering.ru/aboutus,

<http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_rooma.ht> ml,

http://www.youtube.com/watch?v=y37Ax5TPc3s&feature=related.

Учитель спрашивает, что об этом можно прочитать на web-страницах и просит обучающихся сформулировать правила безопасной работы.

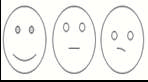
Резюме (обсуждение найденной информации). Какие правила безопасной работы выбрали учащиеся, посещая web-сайты?

**4. Закрепление изученного материала.**

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет-общение будет приносить пользу.

Рефлексия. На данном этапе предлагается подвести итоги урока Интернет- безопасности: на столе лежат три смайлика, обучающимся необходимо выбрать и положите перед собой тот, который соответствует настроению школьника.



Урок понравился. Узнал что-то новое.

Урок понравился. Ничего нового не узнал.

Урок не понравился. Зря время потерял.

***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!***

Оценивание обучающихся.

Информация о домашнем задании, инструкция о его выполнении:

1. Дать определение понятию информационная безопасность.

2. Составить информационный лист Моя безопасная сеть.

**Приложение 8.**

**Примерные материалы итогового анкетирования обучающихся**

**по теме "Безопасный Интернет"**

1. Укажите свой возраст\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Что такое Интернет?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Какие опасности существуют в Интернете?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Использование Интернета является безопасным, если: \* выберите один или несколько вариантов из списка ответов

а)защитить свой компьютер, защитить себя в Интернете, соблюдать правила

б) разглашать личную информацию, заботиться об остальных, регулярно обновлять операционную систему

в) защитить компьютер, создавать резервные копии документов, закону надо подчиняться даже в Интернете

5. Как защитить себя в Интернете? \* выберите один или несколько ответов

а) защитить свой компьютер, расширять круг знакомств с неизвестными людьми

б) стараться давать как можно меньше информации о себе

в) размещать фотографии свои, друзей и родственников

6. Как обезопасить свой компьютер? \* выберите один вариант из списка ответов

а) выключить и спрятать в шкаф

б) установить антивирусную программу

7. Что надо делать, чтобы антивирусная программа была эффективной \* выберите один или несколько вариантов из списка ответов

а) лучше не иметь антивирусную программу

б) обновлять антивирусную базу

в) не посещать сайты, где нет достоверности, что сайт находится под защитой

8. Кто создаёт опасные программы? \* выберите один или несколько вариантов из списка ответов

а) чёрный властелин

б) хакеры

в) шпионы

г) пожиратели смерти

9. Перечислите правила поведения в Интернете \* если вы не знаете ответа на этот вопрос, то напишите "Без ответа»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. А что для вас является "Безопасным Интернетом?" \* если вы не знаете ответа на этот вопрос, то напишите "Без ответа»\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Приложение 9.**

**Сказка о золотых правилах безопасности в Интернет**

В некотором царстве, Интернет - государстве жил-был Смайл-царевич- Тьютор-Королевич, который правил славным городом СоцОБРАЗом. И была у него невеста– прекрасная Смайл-царевна-Он-лайн-Королевна, день и ночь проводившая в виртуальных забавах. Сколько раз предупреждал е царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город СоцОБРАЗ, заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве. И не заметил он, как Интернет- паутина вс -таки затянула Смайл-царевну в свои коварные сети. Погоревал – да делать нечего: надо спасать невесту. Собрал он рать королевскую- СоцОбразову – дружину дистанционную и организовал "Регату" премудрую.

Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они Семь золотых правил безопасного поведения в Интернет, сложили их в котомку Смайл-царевичу, и отправился он невесту искать. Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: порно-сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловья-разбойника, товары заморские купцов шоповских, сети знакомств-зазывалок русалочьих. Как же найти-отыскать Смайл-царевну? Крепко задумался Тьютор-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, отбиваясь от реклам шоповских зазывающих и спамов завлекающих. И остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне, мохом заросшим: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей разомкнувшихся Смайл - царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!

Всегда помни своё Интернет-королевское имя (E-mail, логин, пароли) и не кланяйся всем подряд (не регистрируйся везде без надобности)!

Не поддавайся ярким рекламам-указателям и не ходи тропками путанными на подозрительные сайты: утопнуть в трясине можно!

Если пришло письмо о крупном выигрыше – это Обман-грамота: просто так выиграть невозможно, а если хочешь зарабатывать пиастры, нужно участвовать в полезных обучающих проектах – в Регате, например!

Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)!

Если хочешь дружить с другими царствами-государствами, изучай полезные социальные сервисы Web 2.0: они помогут тебе построить Мой королевский мир, свой царский блог, форум для глашатаев важных – друзей званных Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер!

Не скачивай нелицензионные программные продукты – иначе пираты потопят твой корабль в бурных волнах Интернет!

Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего СоцОБРАЗа, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образовательные.

**Приложение 10.**

**Памятка для учащихся начальной школы**

***Контентные риски***

 Для того, чтобы избежать встречи с неприятной информацией в интернете, установи на свой браузер фильтр или попроси сделать это взрослых – тогда ты сможешь смело путешествовать по интересным тебе страницам.

 Всегда спрашивай родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.

***Электронные риски***

 Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу –антивирус!

 Если твой компьютер заблокирован, то попроси взрослых разблокировать твой компьютер с помощью антивируса. Если твой компьютер заблокировался картинкой с требованием отправить смс, позвони на Линию помощи «Дети Онлайн» (8-800-25-000-15, бесплатно), и тебе помогут решить проблему!

***Коммуникационные риски***

 Прежде чем начать дружить с кем-то в интернете, спроси у родителей, как безопасно общаться в сети.

 Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

 Не отправляй свои фотографии, а также фотографии своей семьи и своих друзей незнакомым людям. Они могут использовать их так, что это навредит тебе или твоим близким.

 Не встречайся без родителей с людьми из интернета в реальной жизни. В интернете многие люди рассказывают о себе неправду.

 Общаясь в интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека. Читать грубости также неприятно, как и слышать.

 Если тебя кто-то расстроил или обидел в интернете, обязательно расскажи об этом родителям.

***Потребительские риски***

 Если хочешь скачать картинку или мелодию, но тебя просят отправить смс – не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс, и не обманут ли тебя. Сделать это можно на специальных сайтах: http://smscost.ru, <http://smswm.ru>, http://smsnumbers.ru.

Более подробно узнать об интернет-рисках, правилах безопасности, ознакомиться с другими важными материалами, можно на порталах: www.detionline.com, www.fid.su, <http://www.google.ru/familysafety>, http://safety.mts.ru.

**Приложение 11**

**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)

**Приложение12.**

**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!

**Приложение 13.**

**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.

|  |
| --- |
| 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. |

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:

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.

**Приложение 14**

**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.

**Приложение 15**

**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:

У вас на домашнем компьютере установлен Интернет?

Что вам больше всего нравится в Интернете?

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?»**

**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.

**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.

**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.

**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.

**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.

**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.

**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.

**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.

**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?»**

**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.

**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.

**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.

**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.

**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.

**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.

**Интернет-хулиганство.**

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

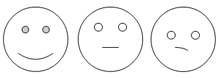
**Недостоверная информация.**

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

**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.