Муниципальное автономное общеобразовательное учреждение средняя общеобразовательная школа №73 г. Челябинска

Безопасность в сети интернет.

Методическое руководство для начальной школы

Учитель информатики
Ахатова Елена Владимировна

г. Челябинск, 2012г

Содержание.

Введение

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 признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет (Рекомендация Rec (2006) 12 Комитета министров государствам-членам Совета Европы по расширению возможностей детей в новой информационно-коммуникационной среде от 27.09.2006.) Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа - услугах и электронных СМИ – требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете, Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочной плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).

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

Преодолеть нежелательное воздействие компьютера возможно только совместными усилиями учителей, родителей и самих школьников. Наша задача сегодня – обеспечение безопасности детей, не способных иногда правильно оценить степень угрозы информации, которую они воспринимают или передают, так как темпы информатизации оказались столь быстрыми, что и семья и школа оказались не готовы к угрозам нового типа, методы борьбы с которыми еще только разрабатываются.

Какие же опасности ждут школьника в сети Интернет? Прежде всего можно выделить следующие: 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 далеко не весь 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 должна проводиться целенаправленная воспитательная работа учителей совместно с родителями.

Работа с обучающимися должна вестись в зависимости от возрастных особенностей: начальное звено (2-4 класс), среднее (5-9 класс) и старшее (10-11 класс). На каждом этапе необходимы специальные формы и методы обучения в соответствии с возрастными особенностями. Формирование навыков информационной безопасности и культуры должно осуществляться не только на уроках информатики, но и на других предметах (например, обществознания, права, ОБЖ и т.д.), а также и во внеурочной деятельности. Полезно 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. Очень часто родители не понимают и недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, между тем «выпуская» его в Интернет не представляют себе, что точно также нужно обучить его основам безопасности в сети. Ребенок абсолютно беззащитен перед потоком информации, сваливающейся на него из сети. Наша задача выработать в нем критическое мышление. С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения.

Комплексное решение поставленной задачи со стороны семьи и школы позволит значительно сократить риски причинения различного рода ущерба ребенку со стороны сети Интернет. Обеспечение информационной безопасности и воспитание информационной культуры должно стать приоритетным направлением работы современного образовательного учреждения.

Родительское собрание.

Первое родительское собрание.

Тема: «Безопасность детей в сети Интернет»

Цель: помочь родителям сориентироваться в мире подростковых влечений; выработать тактику педагогического воздействия, позволяющую сохранить взаимопонимание между родителями и подростками.

Задачи:

- обсудить с родителями проблему о зависимости детей от Интернета;
- познакомить родителей с угрозами, с которыми дети могут столкнуться в Интернете.
- совместно найти пути решения данной проблемы;
- познакомить родителей с советами специалистов по общению детей с интернетом;
- научить некоторым правилам и приемам, облегчающим общение с подростком;
- побудить родителей к полноценному общению со своими детьми;
- расширить объем знаний родителей о нормах и методах решения возникающих проблем с детьми.

Форма проведения: беседа.

Оборудование: компьютер; мультимедийный проектор

Участники: родители обучающихся, классный руководитель

Подготовительный этап: анкетирование обучающихся, анкетирование родителей, подготовка рекомендаций родителям о безопасном использовании Интернета детьми, создание презентации

Дидактический материал: Анкета для родителей , анкета для учеников (приложение 1), презентация (Приложение 2).

Ход собрания:

1. **Орг. Момент.** Приветствие, проверка готовности.

   Добрый день, уважаемые родители! Тема нашего разговора сегодня «Безопасность детей в сети Интернет».

2. **Мотивация и актуализация.**

Сегодня все больше и больше компьютеров подключаются к работе в сети Интернет. При этом все большее распространение получает подключение по высокоскоростным каналам, как на работе, так и дома. Все большее количество детей получает возможность работать в Интернет. Но вместе с тем все острее встает проблема обеспечения безопасности наших детей в Интернет. Так как изначально Интернет

развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и учитель?

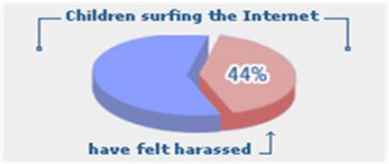
Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет (слайд № 1).

3. Результаты анкетирования.

В подготовительном этапе проводится анкетирование детей и родителей (анкеты - Приложение 1-2), родителям предоставляются результаты анкетирования с анализом. (слайд № 2-3)

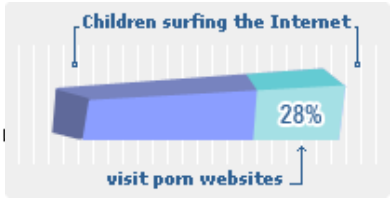
4. Выступление.

Тревожная статистика (слайд № 4):



44% детей подвергались сексуальным домогательствам в Интернете

28% детей посещают порнографические веб-стран



50% детей выходят в Интернет одни

Какие угрозы встречаются наиболее часто? Прежде всего: (слайд № 5-9)

- **Угроза заражения вредоносным ПО.** Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.
- **Доступ к нежелательному содержимому.** Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые

материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера;

- **Контакты с незнакомыми людьми с помощью чатов или электронной почты.** Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи;
- **Неконтролируемые покупки.** Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

(Слайд №10-20)

Интернет это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что как и наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна. Приведем несколько рекомендаций, с помощью которых посещение Интернет может стать менее опасным для ваших детей:

2. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;
3. Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;
4. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;
5. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.;
6. Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;
7. Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;
8. Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
9. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет – правда. Приучите их спрашивать о том, в чем они не уверены; Объясните ребенку, что сегодня практически каждый человек может создать свой сайт и при этом никто не будет контролировать, насколько правдива размещенная там информация. Научите ребенка проверять все то, что он видит в Интернет.
10. Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное

содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

(слайд № 21-29)

Как это объяснить ребенку? (рекомендации)

- **Начните, когда ваш ребенок еще достаточно мал**. Ведь сегодня даже дошкольники уже успешно используют сеть Интернет, а значит нужно как можно раньше научить их отделять правду от лжи;
- **Не забывайте спрашивать ребенка об увиденном в Интернет**. Например, начните с расспросов, для чего служит тот или иной сайт.
- **Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в Интернет информацию по другим источникам** (по другим сайтам, газетам или журналам). Приучите вашего ребенка советоваться с вами. Не отмахивайтесь от их детских проблем.
- **Поощряйте ваших детей использовать различные источники**, такие как библиотеки или подарите им энциклопедию на диске, например, «Энциклопедию Кирилла и Мефодия» или Microsoft Encarta. Это поможет научить вашего ребенка использовать сторонние источники информации;
- **Научите ребенка пользоваться поиском в Интернет.** Покажите, как использовать различные поисковые машины для осуществления поиска;
- **Объясните вашим детям, что такое расизм, фашизм, межнациональная и религиозная вражда.** Несмотря на то, что некоторые подобные материалы можно заблокировать с помощью специальных программных фильтров, не стоит надеяться на то, что вам удастся отфильтровать все подобные сайты.Родителям не стоит надеяться на тайную слежку за службами мгновенных сообщений, которыми пользуются дети. Гораздо проще использовать доброжелательные отношения с вашими детьми.

(слайд № 30-33)

Может ли ваш ребенок стать интернет - зависимым?

Не забывайте, что Интернет это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию Интернет - зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не становится очень серьезной. Да и кроме того, факт наличия такой болезни как Интернет-зависимость не всегда признается. Что же делать?

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

(слайд № 33-34)

5. Заключение.

Не стоит думать, что Интернет – это безопасное место, в котором ваши дети могут чувствовать себя защищенными. Надеюсь, что вы понимаете, что использование только средств воспитательной работы без организации действенного контроля – это практически бесполезное занятие. Точно так же как и использование репрессивных средств контроля без организации воспитательной работы. Только в единстве данных средств вы сможете помочь вашим детям чувствовать себя в безопасности и оградить их от влияния злоумышленников. На следующем родительском собрании мы рассмотрим несколько способов родительского контроля над проведением детей в интернете.

Второе родительское собрание.

Тема: «Родительский контроль над поведением детей в Интернет» (Практическое руководство)

Цель: помочь родителям сориентироваться в мире подростковых влечений; выработать тактику педагогического воздействия, позволяющую сохранить взаимопонимание между родителями и подростками.

Задачи:

- обсудить с родителями проблему о зависимости детей от Интернета;
- познакомить родителей с угрозами, с которыми дети могут столкнуться в Интернете.
- совместно найти пути решения данной проблемы;
- познакомить родителей с советами специалистов по общению детей с интернетом;
- научить некоторым правилам и приемам, облегчающим общение с подростком;
- побудить родителей к полноценному общению со своими детьми;
- расширить объем знаний родителей о нормах и методах решения возникающих проблем с детьми.

Форма проведения: беседа.

Оборудование: компьютер; мультимедийный проектор

Участники: родители обучающихся, классный руководитель

Подготовительный этап: создание презентации.

Дидактический материал: вопросы (Приложение 4), памятка для родителей (Приложение 5), презентация (Приложение 6).

Ход собрания:

1. **Орг. Момент.** Приветствие, проверка готовности.

2. **Мотивация и актуализация.**

Давайте ответим на вопросы письменно *(каждому родителю раздается лист с вопросами, где они и пишут свои ответы (Приложение 4), на ответы дается 5-10 минут):*

1. Как вам помогло предыдущее собрание, тема которого была «Безопасность детей в интернете?
2. Что бы вы еще хотели узнать о том как обеспечить безопасность детей при работе в интернете?

(возраст 9-12)

3. Выступление

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 *(памятка для родителей выдается на каждого родителя Приложение 5)*

- 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.

Как проводить Родительский контроль над поведением детей в Интернет?

Обеспечивать родительский контроль в Интернет можно с помощью различного программного обеспечения. В данной статье мы рассмотрим только некоторое ПО, в частности, Родительский контроль в Windows Vista, средства Родительского контроля, встроенные в Kaspersky Internet Security. Рассмотрим их подробнее.

Родительский контроль в Windows Vista

До выхода Windows Vista средства родительского контроля можно было обеспечить с помощью операционной системы и программного обеспечения сторонних производителей. Однако с выходом новой операционной системы Windows Vista положение коренным образом изменилось. В состав ОС были включены средства Parental Control (Родительский контроль). Это позволит родителям намного проще решать вопросы контроля за поведением своих детей и их безопасностью при работе на компьютере.

Для задания Родительского контроля вам потребуется создать ограниченную учетную запись, под которой ваш ребенок будет работать за компьютером. Кроме того, не забудьте установить устойчивый (строгий) пароль на вашу учетную запись Администратора (рис. 1).

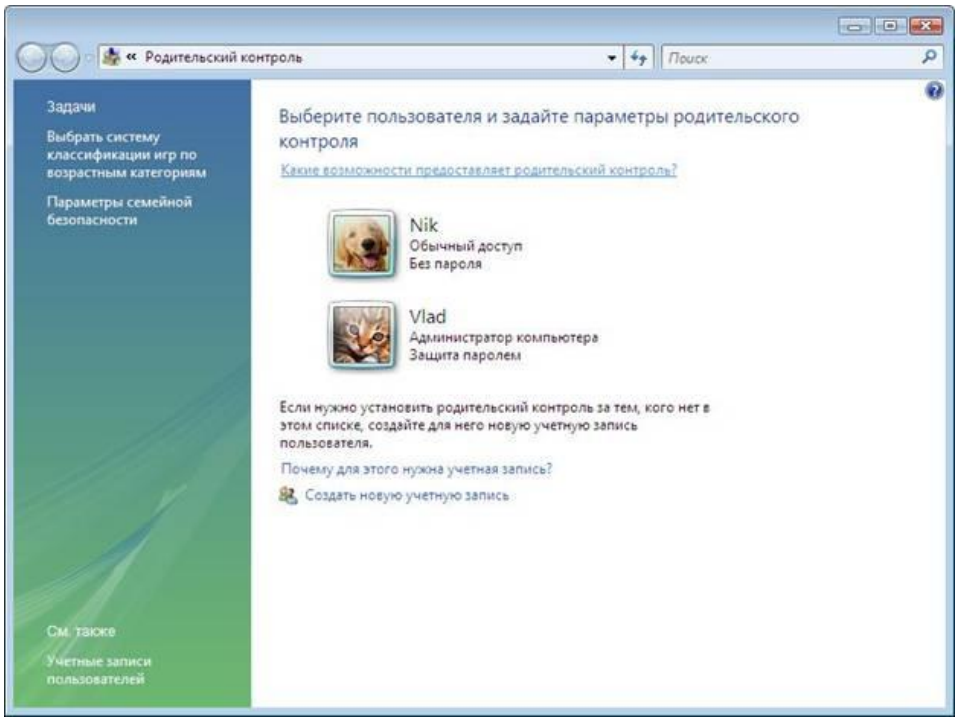


Рисунок 1 - Родительский контроль

Рассмотрим функции, решаемые с помощью родительского контроля (рис. 2):

- **Ограничение времени, проводимого ребенком за компьютером.** Можно определить время, в течение которого детям разрешен вход в систему. В частности, определить дни недели и разрешенные часы доступа в соответствующий день недели. Это не позволит детям входить в систему в течение определенного периода времени. Если в момент окончания разрешенного периода времени ребенок работает за компьютером, происходит автоматический выход из системы.
- **Установка запрета на доступ детей к отдельным играм.** Запрет можно устанавливать исходя из допустимой возрастной оценки, выбора типа содержимого или запрещая доступ к определенным играм.
- **Ограничение активности детей в Интернете.** Ограничить детей можно с помощью установки круга допустимых веб-узлов, исходя из возрастной оценки, запрета или разрешения загрузки файлов, определения условий фильтрования содержимого (т.е. вы должны определить, какое содержимое фильтры должны разрешать или блокировать). Вместе с тем можно разрешить или блокировать доступ к определенным веб-узлам.
- **Установка запретов на использование детьми отдельных программ.** Можно запретить детям доступ к определенным программам.
- **Ведение отчетов о работе ребенка за компьютером.**

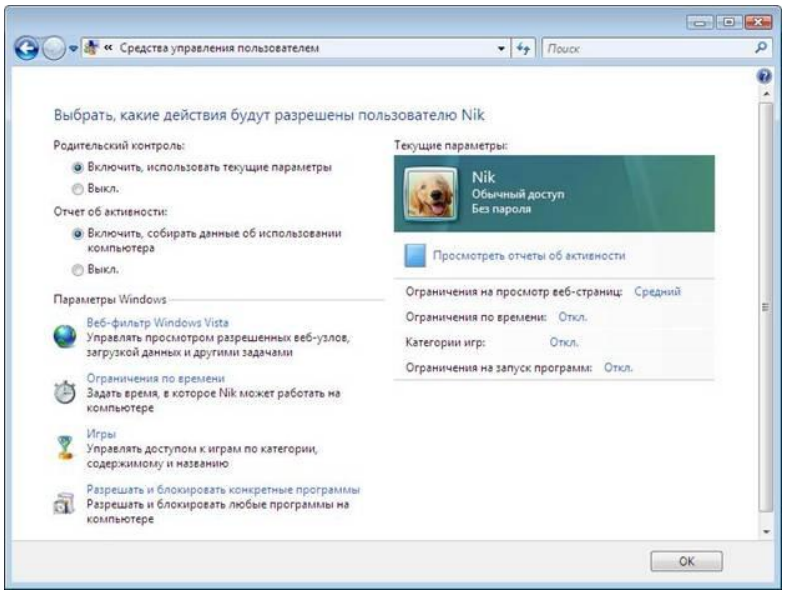


Рисунок 2 - Средства управления пользователем

Ограничение времени использования компьютера

Разрешенное время доступа можно определить для каждого дня недели и заблокировать при этом доступ в любое другое время (рис.3). Для этого:

- Откройте папку «Родительский контроль».
- При появлении соответствующего запроса введите пароль администратора или подтверждение пароля.
- Выберите учетную запись, для которой вы хотите задать ограничение времени.
- В группе «Родительский контроль» выберите «Вкл».

- Щелкните «Ограничение по времени».
- В появившейся сетке выберите разрешенные часы[2].

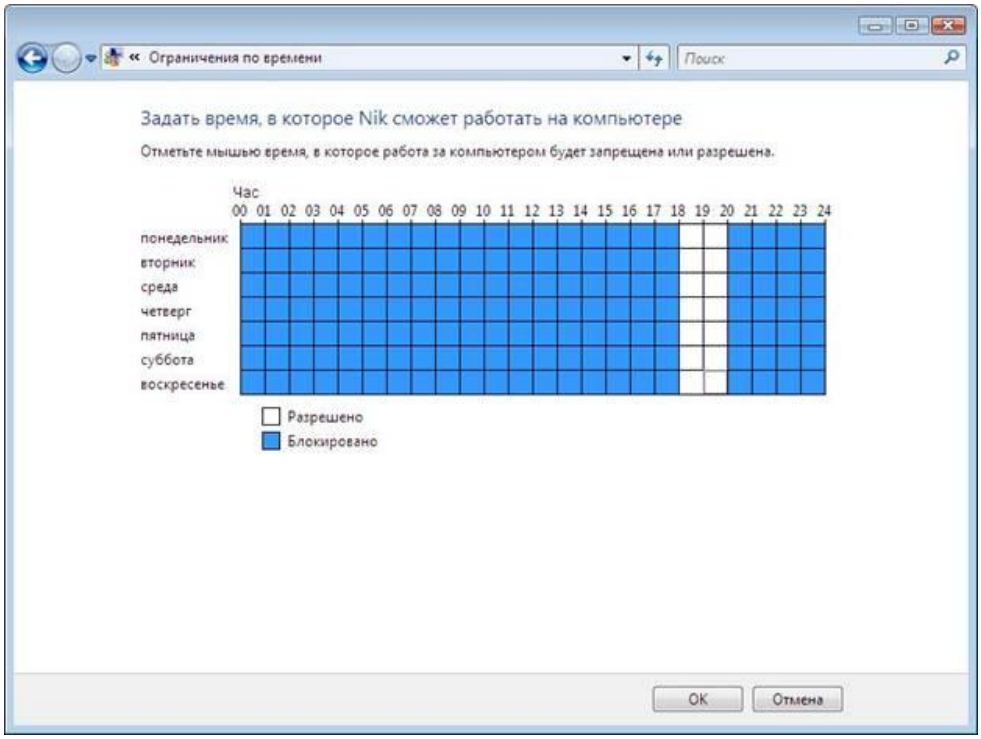


Рисунок 3 - Ограничение времени доступности компьютера для данного пользователя

В данной статье мы не будем подробно рассматривать Установку запрета на доступ детей к отдельным играм и Установку запретов на использование детьми отдельных программ.

Как работает веб-фильтр родительского контроля?

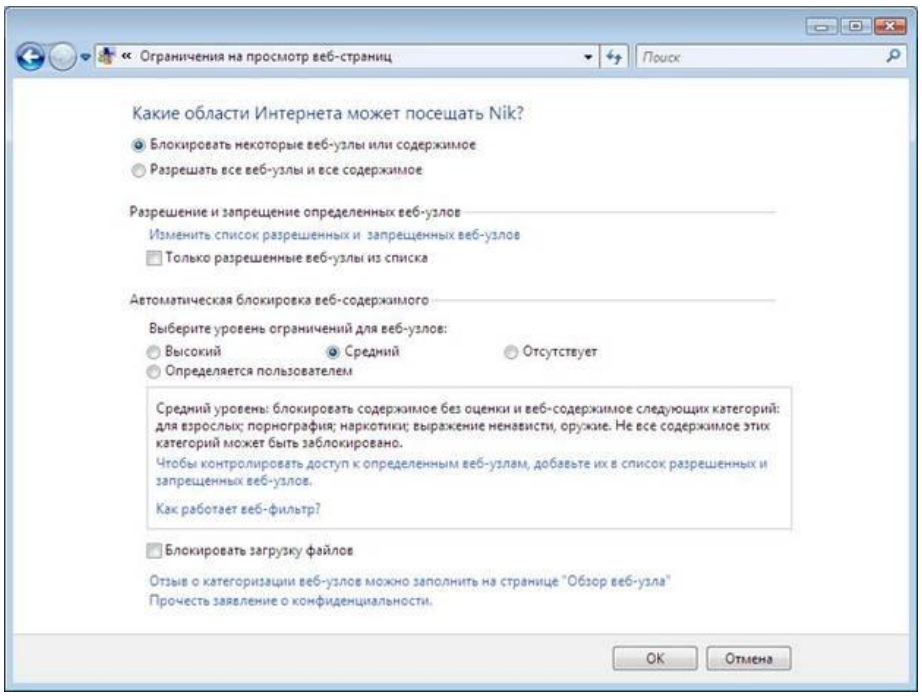


Рисунок 4 - Ограничение на просмотр веб-узлов

Веб-фильтр родительского контроля оценивает содержимое веб-узлов и может блокировать те из них, содержимое которых определено как нежелательное. Включение веб-фильтра позволит значительно уменьшить число нежелательных узлов, которые смогли бы просматривать дети, но, естественно, не гарантирует стопроцентной защиты. Так как нежелательность содержимого является субъективным критерием, следовательно, фильтры смогут блокировать далеко не все содержимое, которое вы считаете нежелательным.

Выбор уровня ограничений для автоматической блокировки содержимого

Существует четыре уровня ограничений для обозначения содержимого, которое следует блокировать:

- **Высокий**. Веб-узлы для детей с понятным и подходящим для них содержимым. На таких узлах используется стиль изложения, понятный детям от 8 до 12 лет, а его содержимое доступно для детского понимания. Если выбран этот уровень, детям разрешается просматривать веб-узлы для детей, а также другие веб-узлы, внесенные в список разрешенных веб-узлов.
- **Средний.** Производится фильтрация веб-узлов на основании типа содержимого. В этом случае ребенок получит доступ к различной информации в Интернете, за исключением нежелательного содержимого. Чтобы узнать, какие веб-узлы ребенок посещал или пытался открыть, следует просмотреть отчет об активности в Интернете.
- **Низкий**. Содержимое веб-узлов не блокируется.
- **Особый**. Данный уровень также предусматривает блокирование веб-узлов на основании типов содержимого, но позволяет производить фильтрацию по дополнительным критериям.

Вместе с тем стоит отметить, что можно разрешить или заблокировать отдельные узлы, добавив их в список разрешенных и блокируемых веб-узлов, независимо от выбранного уровня фильтрации.

Выбор типов содержимого для блокировки

Типы содержимого, на основании которых может производиться блокировка веб-узлов.

- **Порнография**. Веб-узел имеет содержимое откровенно сексуального характера, направленное на возбуждение полового влечения.
- **Для взрослых.** Веб-узел содержит информацию откровенно сексуального характера, не носящую медицинский или научный характер.
- **Половое воспитание.** Веб-узел содержит информацию о репродуктивной функции человека и половом развитии, заболеваниях, передающихся половым путем, контрацепции, безопасном сексе, сексуальности или сексуальной ориентации.
- **Агрессивные высказывания.** Веб-узел пропагандирует враждебность или агрессию по отношению к человеку или группе людей на основании принадлежности к определенной расе, религии, полу, национальности, этнического происхождения или иных характеристик; порочит других или оправдывает

неравенство на основании вышеперечисленных характеристик либо научным или иным общепринятым методом оправдывает агрессию, враждебность или клевету.

- **Изготовление бомб.** Веб-узел пропагандирует или содержит инструкции по нанесению физического вреда людям или частной собственности при помощи оружия, взрывчатых веществ, розыгрышей или иных видов насилия.
- **Оружие.** Веб-узел продает, освещает или описывает огнестрельное или холодное оружие, а также предметы боевых искусств, либо содержит информацию об их использовании, аксессуарах или модификациях.
- **Наркотики.** Веб-узел рекламирует, предлагает, продает, поставляет, поощряет или иными способами пропагандирует незаконное использование, выращивание, производство или распространение наркотиков, медицинских препаратов, химических веществ и растений, вызывающих наркотическое опьянение, или атрибутов, связанных с употреблением наркотиков.
- **Алкоголь**. Веб-узел рекламирует или содержит предложения о продаже алкогольных напитков или средств для их производства, содержит рецепты или информацию о сопутствующих принадлежностях либо пропагандирует употребление и опьянение алкоголем.
- **Табак**. Веб-узел содержит рекламу, предложения о продаже или иными способами пропагандирует табакокурение.
- **Азартные игры.** Веб-узел позволяет пользователям делать ставки и играть на тотализаторах (в том числе лотереи) в Интернете, получать информацию, содействие или рекомендации по заключению пари, а также дает инструкции, оказывает содействие или обучает азартным играм.
- **Содержимое без оценки.** Содержимое, которое не оценивается веб-фильтром.

Ограничение доступа детей к некоторым типам содержимого в Интернете

При помощи родительского контроля можно разрешить или запретить доступ детей к отдельным веб-узлам. Также можно заблокировать некоторые веб-узлы на основании их содержимого.

Разрешение или запрещение доступа к отдельным веб-узлам

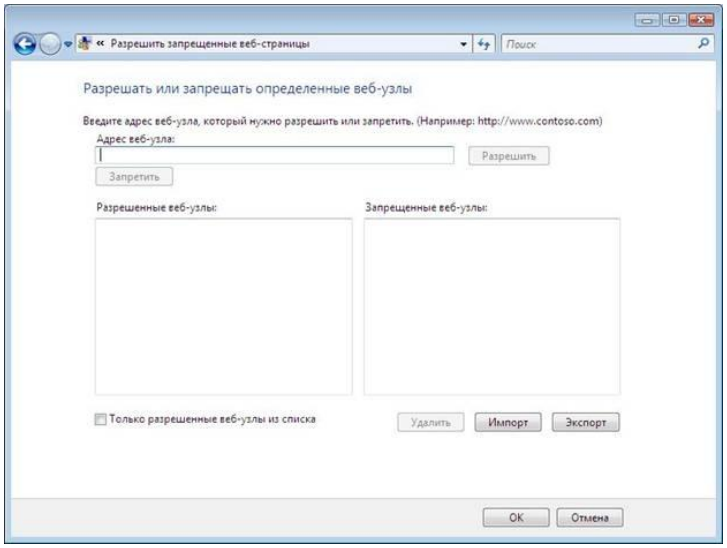


Рисунок 5 - Разрешать или запрещать определенные веб-узлы

1. Откройте «Родительский контроль».
2. Введите пароль администратора или подтверждение пароля, если появится соответствующий запрос.
3. Щелкните имя пользователя, которому нужно установить веб-фильтр.
4. В группе Родительский контроль выберите Вкл.
5. Щелкните Веб-фильтр Windows Vista.
6. Щелкните Блокировать некоторые веб-узлы или содержимое.
7. Щелкните Изменить список разрешенных и запрещенных веб-узлов.
8. В поле Адрес веб-узла введите адрес веб-узла, доступ к которому требуется разрешить или запретить, и нажмите кнопку Разрешить или Блокировка.

Автоматическая блокировка некоторых типов содержимого в Интернете

Включение веб-фильтра должно значительно уменьшить число нежелательных веб-узлов, которые смогли бы просматривать дети. Однако нежелательность содержимого является субъективным критерием, и фильтр может блокировать не все содержимое, которое вы считаете нежелательным. Также в связи с постоянным появлением новых веб-узлов фильтру требуется время на анализ и оценку их содержимого.

1. Откройте «Родительский контроль».
2. Введите пароль администратора или подтверждение пароля, если появится соответствующий запрос.
3. Щелкните имя пользователя, которому нужно установить веб-фильтр.
4. В группе Родительский контроль выберите Вкл.
5. Щелкните Веб-фильтр Windows Vista .
6. Щелкните Блокировать некоторые веб-узлы или содержимое.
7. В группе Автоматическая блокировка веб-содержимого выберите необходимый уровень содержимого.

Примечание

Можно запретить загрузки, установив флажок Блокировать загрузку файлов.

Родительский контроль в Kaspersky Internet Security 7.0

Следует отметить, что в случае использования Windows XP единственным действенным средством использования родительского контроля остаются средства сторонних производителей. Вместе с тем нельзя не признать того, что некоторые параметры родительского контроля в KIS 7.0 могут помочь и в случае использования Windows Vista.

Для настройки Родительского контроля в KIS 7.0 вам необходимо на главной странице приложения выбрать Родительский контроль (рис. 6).

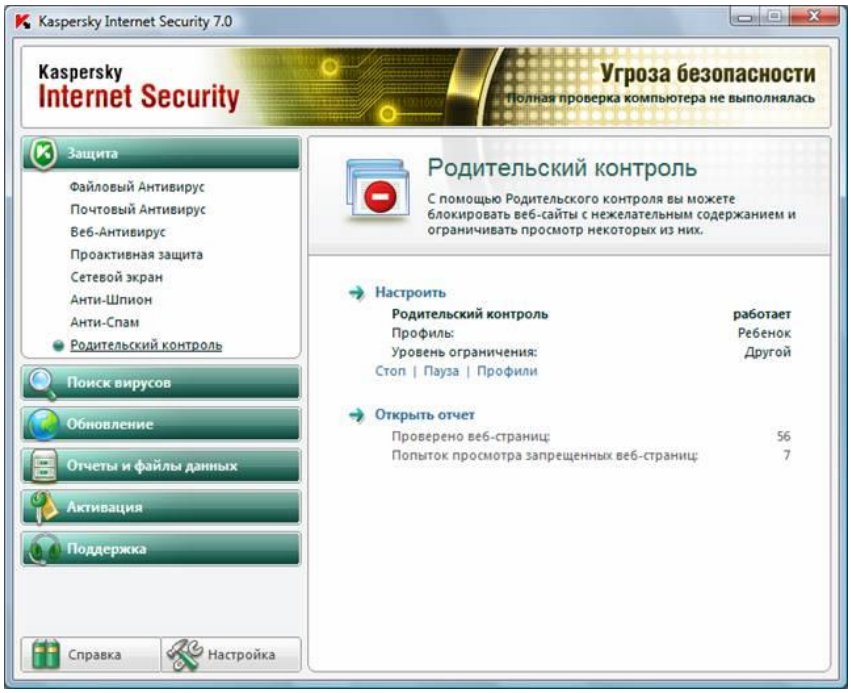


Рисунок 6 - Настройка Родительского контроля в KIS 7.0

Далее необходимо настроить соответствующий профиль как для родителей так и для ребенка (рис. 6). Следует учесть, что по умолчанию Родительский контроль выключен.

После включения всем учетным записям компьютера будет присвоен профиль «Ребенок».

Профиль – это набор правил, регламентирующих доступ пользователя к определенным интернет-ресурсам. По умолчанию созданы три предустановленных профиля:

- **Ребенок** (данный профиль используется по умолчанию).
- **Подросток.**
- **Родитель.**

Для каждого из предустановленных профилей разработан оптимальный набор правил с учетом возраста, опыта и других характеристик каждой группы. Так, например, профиль **Ребенок** обладает максимальным набором ограничений, а в профиле **Родитель** ограничений нет. Удалять предустановленные профили нельзя, но вы можете изменять параметры профилей **Ребенок** и **Подросток** по своему усмотрению.

После установки приложения профиль **Ребенок** является профилем, который используется по умолчанию для всех пользователей, с учетной записью которых не связан ни один профиль.

Для того чтобы использовать предустановленные профили **Подросток** и **Родитель,** установите флажок **Использовать профиль** в окне **Настройка профилей**. В результате выбранные профили будут отображены в раскрывающемся списке блока **Профили** в окне настройки компонента **Родительский контроль.**

В блоке **Пароль** вы можете задать пароль, ограничивающий доступ пользователей к веб-ресурсам под данным профилем. Дальнейшее переключение пользователей на данный профиль будет возможно только после указания заданного пароля. Если поле **Пароль** оставлено пустым, на этот профиль сможет переключиться каждый пользователь компьютера. Для профиля **Ребенок** пароль не задается.

В блоке **Пользователи** вы можете прикрепить определенную учетную запись Microsoft Windows к выбранному профилю Родительского контроля.

Для того чтобы выбрать учетную запись, которую вы планируете связать с профилем, нажмите на кнопку **Добавить** и в стандартном окне Microsoft Windows укажите необходимую учетную запись.

Для того чтобы настраиваемый профиль не применялся к учетной записи пользователя, выберите этого пользователя в списке и нажмите на кнопку **Удалить.**

Чтобы отредактировать настройки параметров профиля:

- Откройте окно настройки приложения и выберите компонент Родительский контроль в разделе **Защита.**

- Выберите предустановленный профиль, параметры которого вы хотите изменить, из раскрывающегося списка в блоке **Профили** и нажмите на кнопку **Настройка.**

Настройка фильтрации

Ограничения, применяемые к профилям Родительского контроля, основаны на применении фильтров. *Фильтр* – это ряд критериев, по которым Родительский контроль принимает решение о возможности загрузки того или иного веб-сайта.

Чтобы изменить параметры фильтрации для текущего уровня ограничений:

1. Откройте окно настройки приложения и выберите компонент **Родительский контроль** в разделе **Защита.**
2. Выберите профиль из раскрывающегося списка в блоке **Профили** и нажмите на кнопку **Настройка** в блоке **Уровень ограничения.**
3. Отредактируйте параметры фильтрации на соответствующих закладках окна **Настройка профиля: <название профиля>.**

Ограничение времени доступа к интернет-ресурсам

В дополнение к средствам Родительского контроля, созданным в Windows Vista, KIS 7.0 позволяет установить ограничение времени доступа к Интернет (рис. 7).

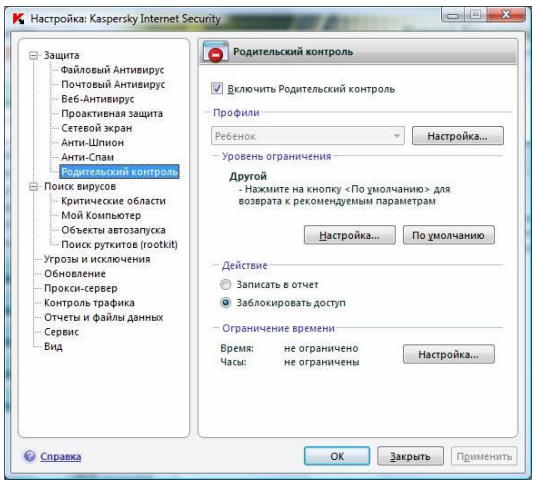


Рисунок 7 - Настройка Родительского контроля

Чтобы установить ограничение на работу в интернете по суммарному количеству времени в течение суток, установите флажок **Ограничить суточное время работы в интернете** и задайте условие ограничения.

Чтобы ограничить доступ к интернету определенными часами в течение суток, установите флажок **Разрешить доступ к интернету в указанное время** и задайте временные интервалы, когда работа в интернете разрешена. Для этого воспользуйтесь кнопкой **Добавить** и в открывшемся окне укажите временные рамки. Для редактирования списка разрешенных интервалов работы используйте соответствующие кнопки (рис. 8).

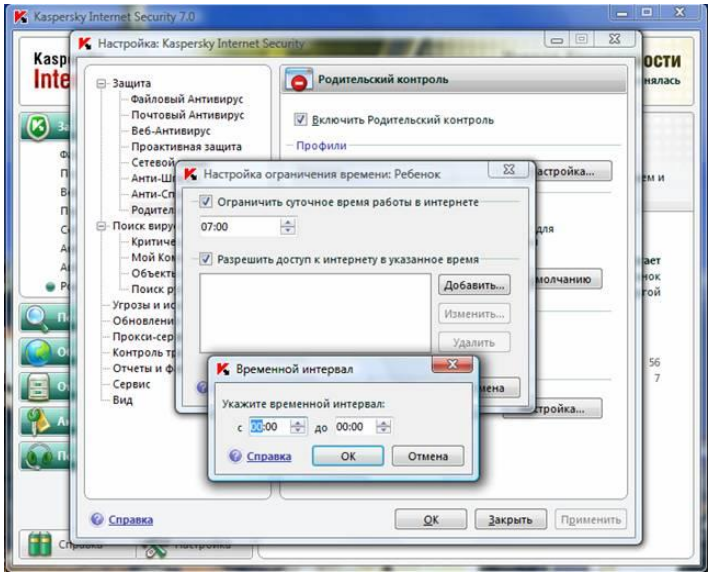


Рисунок 8 - Настройка временного интервала доступа в Интернет

Если вы задали оба временных ограничения, причем значение одного из них превышает другое по количеству отведенного времени, то будет выбрано наименьшее значение из заданных.

Пример: для профиля Ребенок вы ограничили суммарное суточное время работы в интернете тремя часами и дополнительно разрешили доступ в интернет только с 14:00

до 15:00. В итоге доступ к веб-сайтам будет разрешен только в течение этого временного интервала, несмотря на общее разрешенное количество часов. Вы можете задавать несколько временных интервалов в рамках одних суток.

Таким образом, вы сможете указать временной интервал в то время, когда вы сможете контролировать своего ребенка.

Так же вы можете использовать детские интернет браузеры например: (слайд 28, приложения 6). Сайт http://myttk.ru/kids/

4. **Заключение.** Собрать ответы на опросник Приложение 4. Мы продолжим наши беседы, если вам это интересно. До свидание, до следующей встречи.

Уроки интернет-безопасность в начальной школе.

Урок № 1

Тема: Безопасное поведение в сети интернет.

Класс: 4

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

Задачи урока:

- Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности
- Разработка норм и правил поведения детей в сети Интернет
- Отработка навыков и умений: сравнения информации, критического анализа; выделения главных мыслей и грамотного их изложение; восприятия и усвоения услышанного;
- Ознакомление с технологиями Web 2.0
- Расширение кругозора учащихся

Знания, умения:

- научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях,
- 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.

Форма проведения: беседа

Оборудование: компьютер; мультимедийный проектор

Дидактический материал: презентация (Приложение 3)

План урока:

№	Этапы урока	Виды и формы работы	Время
1	Организационный момент	Проверка готовности класса к уроку, приветствие	1 мин.
2	Актуализация и мотивация	Вступительное слово. Постановка цели урока	1 мин.
3	Объяснение нового материала	Беседа с использованием слайдов презентации.	22 мин.
4	Физкультминутка		3 мин.
5	Домашнее задание	Объяснение домашней работы	2 мин.
6	Подведение итогов урока	Работа по вопросам учителя	8 мин.
7	Рефлексия	Работа со смайликами.	3 мин.

Ход урока:

1. Организационный момент.

Проверка готовности класса к уроку, приветствие

2. Актуализация и мотивация.

Сегодня все больше и больше компьютеров подключаются к работе в сети Интернет. При этом все большее распространение получает подключение по высокоскоростным каналам, как на работе, так и дома. Практически каждый из вас проводит по несколько часов в день в интернете. Так как изначально Интернет развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. А вы знаете правила безопасной работы в интернете?

3. Объяснение нового материала.

Использование интернета станет безопасным, если выполнять три основных правила:

1. Защитите свой компьютер: регулярно обновляйте операционную систему, используйте антивирусную программу, применяйте брандмауэр, создавайте резервные копии важных файлов, будьте осторожны при загрузке содержимого.

- ✓ ***Брандмауэр***

Программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельной компьютерной системой. Например, брандмауэр позволяет ограничивать трафик на основе предварительно

заданных правил, которые разрешают обмен данными только между указанными адресами.

2. Защитите себя в Интернете: Не разглашайте личную информацию, думайте о том, с кем разговариваете, помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3. Соблюдайте правила: Закону необходимо подчиняться даже в Интернете, при работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Опасности которые могут вас подстерегать:

1. **Вирусы, черви и Трояны**

Вирусы и черви представляют собой опасные программы, которые могут распространяться через электронную почту или веб - страницы. Вирусы могут повредить файлы или программное обеспечение, хранящиеся на компьютере.

Черви распространяются быстрее вирусов — напрямую с одного компьютера на другой. Например, червь электронной почты может осуществлять самостоятельную рассылку по адресам электронной почты из адресной книги пользователя. Интернет - червями осуществляется поиск компьютеров, которые подключены к Интернету и не содержат последние обновления системы безопасности.

«Троянские кони» (Трояны) являются опасными программами, которые выглядят безопасными, например, играми, но после активации могут повредить файлы; при этом пользователь не будет об этом знать.

2. **Хакеры и взломщики**

Хакерами и взломщиками называют людей, которые взламывают защиту систем данных. Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности.

Лучшим способом защиты компьютера от вторжения является применение брандмауэра и регулярное обновление операционной системы.

Хакерами называют людей, которые знают о компьютерах и вычислительных системах больше, чем средний пользователь. Они имеют обширные знания о технологии, но они не используют эти знания для совершения преступления. Хакеры, как правило, не преследуют в своей деятельности корыстных целей, а желают углубиться в суть системы для собственного образования.

Взломщики также являются компьютерными специалистами высокого уровня, но, в отличие от хакеров, они используют свои знания для запрещенной деятельности: они вламываются в чужие компьютеры с корыстными намерениями и используют их в преступных целях. Наилучшей защитой от взлома компьютера является защита с помощью использования сервиса безопасности и противовирусной защиты (например, Live OneCare) и надлежащее поддержание операционной системы в порядке.

3. Спам в Интернете

Массовая рассылка нежелательных сообщений электронной почты известна как спам. Он приводит к перегрузке систем электронной почты и может заблокировать почтовые ящики. В качестве средства для рассылки спама его отправители иногда используют червей электронной почты.

Правила для работы с электронной почтой:

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
2. Никогда не отвечайте на спам.
3. Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).
4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.
5. Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.
6. Закрывайте сомнительные всплывающие окна
7. Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке. При отображении такого окна самым безопасным способом его закрытия является нажатие значка X (обычно располагается в правом верхнем углу). Невозможно знать наверняка, какое действие последует после нажатия кнопки «Нет».
8. Остерегайтесь мошенничества

В Интернете легко скрыть свою личность. Рекомендуется проверять личность человека, с которым происходит общение (например, в дискуссионных группах). Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам.

Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних. Обсудите с детьми, как правильно и безопасно использовать Интернет.

Законы применяемые к Интернету

Интернет является общественным ресурсом. В Интернете необходимо следовать основным правилам так же, как правилам дорожного движения при вождении.

Несмотря на то, что большая часть законов была создана до широкого распространения Интернета, закон также распространяется и на него. Все, что незаконно в обычной жизни, незаконно и в Интернете.

Интернет предоставляет беспрецедентные возможности свободного общения, но они также подразумевают ответственность. Например, владелец веб-сайта всегда несет ответственность за его содержимое и законность самого сайта и места его публикации.

Авторское право

Авторским правом защищается способ реализации идеи, но не сама идея. Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено. Например, при использовании материала в собственной презентации необходимо указать источник.

Передача и использование незаконных материалов (например, пиратские копии фильмов или музыкальных произведений, программное обеспечение с надорванными защитными кодами и т.д.) является противозаконным.

Копирование программного обеспечения или баз данных, для которых требуется лицензия, запрещено даже в целях личного использования.

Неразрешенное использование материала может привести к административному взысканию в судебном порядке, а также иметь прочие правовые последствия.

5. **Физкультминутка.**

Раз и два, раз и два!
Прямо спину вы держите,
Раз и два! Раз и два!
И под ноги не смотрите,
Раз и два! Раз и два!
Раз – присели, два – привстали.
Руки кверху все подняли.
Сели-встали, сели-встали.
Ванькой - встанькой словно стали.
Раз-два, раз-два,
Заниматься нам пора!

6. **Домашнее задание:** Нарисовать рисунок иллюстрацию к правилам полезного и безопасного использования Интернета.

7. **Подведение итогов урока.**

Помните

После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.

Проверяйте

Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.

Думайте

Благоразумно ли размещать личную информацию на собственном веб - сайте, если невозможно быть уверенным в целях ее использования?

Обращайте внимание

Имена учеников, их фотографии и другая личная информация из школьного журнала может публиковаться на веб-сайте школы только с согласия учеников и их родителей.

Вы должны это знать и выполнять:

1. Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
2. Прежде чем начать дружить с кем-то в Интернете, спросите у родителей как безопасно общаться.
3. Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.
4. Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели фотографии Вас, Ваших друзей или Вашей семьи.
5. Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.
6. Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
7. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

7. Рефлексия. Выберите смайлик соответствующий вашему настроению.

Урок № 2

Тема: Безопасное поведение в сети интернет.

Класс: 4

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

Задачи урока:

- Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности
- Разработка норм и правил поведения детей в сети Интернет
- Отработка навыков и умений: сравнения информации, критического анализа; выделения главных мыслей и грамотного их изложение; восприятия и усвоения услышанного;
- Ознакомление с технологиями Web 2.0
- Расширение кругозора учащихся
- Закрепление полученных знаний на предыдущем уроке.

Знания, умения:

- научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях,
- 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.

Форма проведения: беседа

Оборудование: компьютер; мультимедийный проектор

Дидактический материал: презентация (Приложение7), карточки № 1, 2 (приложение 8)

План урока:

№	Этапы урока	Виды и формы работы	Время
1	Организационный момент	Проверка готовности класса к уроку, приветствие	1 мин.
2	Актуализация и мотивация	Вступительное слово. Постановка цели урока	1 мин.
3	Проверка домашнего задания	Ребята сдают рисунки.	2 мин.
4	Игра за и против	Работа в группах	15 мин.
5	Физкультминутка	Участникам предлагается в течении 10 секунд пожать руки как можно большего числа других людей.	2 мин.
6	Практическая работа	Работа в группах	7 мин.
7	Тестирование	Тест (слайды № 7-14)	7 мин.
8	Подведение итогов урока	Работа по вопросам учителя	3 мин.
9	Домашнее задание	Объяснение домашней работы	2 мин.

Ход урока:

1. **Организационный момент**
   Проверка готовности класса к уроку, приветствие

2. **Актуализация и мотивация.**
   Здравствуйте ребята мы с вами продолжаем изучать тему – «Безопасное поведение в сети интернет».
3. **Проверка домашней работы.**
4. **Игра за или против.**

Для начала, предлагаю разделиться на три группы и поиграть в игру «За или против». Вы увидите несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения, даю на подготовку 10 мин.

(*каждой группе раздаются карточка № 1, Приложение 8)*

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 магазины – это плохо, потому что это наиболее популярный вид жульничества в Интернете.
5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Обсуждение результатов.

5. Физкультминутка. «Собери рукопожатия» (2 мин.).

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

Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Чем он был вызван?

Аналогия с работой в Интернет.

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?

6. Практическая работа (7 мин.).

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

Давайте посмотрим, что об этом можно прочитать на web-страницах и попробуем сформулировать правила безопасной работы.

- У вас на столах лежат карточки с адресами web-страниц, которые я предлагаю вам сегодня посетить *(Карточка №2, приложение 8)*. Данный ресурс добавлен в закладки браузера Opera в папку «Безопасный Интернет». Познакомьтесь с информацией ресурса и сформулируйте правила безопасной работы в сети.

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

(Каждой группе на высказывание 1 мин.)

7. Тестирование (7 мин.).

Проведем небольшое тестирование. Какие действия вы предпримите в предложенных ситуациях.

Работа с тестом *(на каждый вопрос дается 1мин).*

8. Подведение итогов урока (5 мин.).

Я рада, что вы не остались равнодушны к теме безопасного интернета. Спасибо за активное участие (оценка работы группы).

9. Домашнее задание 1. Дать определение понятию «информационная безопасность». 2. Составить информационный лист «Моя безопасная сеть».

Приложение 1

Анкета для обучающихся:

1. Есть ли у вас дома интернет? (да/нет)
2. Какие сайты вы чаще всего посещаете?
3. Знаете ли вы о тех опасностях, которые подстерегают вас в интернете? (да/нет)

Анкета для родителей:

1. Знаете ли вы, чем опасен Интернет для ваших детей? (да/нет)
2. Интересуетесь ли вы тем, что делает ваш ребенок в Интернете? (да/нет)
3. Знаете ли вы, как уберечь своего ребенка от опасности работы в Интернете? (да/нет)

Приложение 4

Вопросы:

1. Как вам помогло предыдущее собрание, тема которого была «Безопасность детей в интернете?

2. Что бы вы еще хотели узнать о том как обеспечить безопасность детей при работе в интернете?

Приложение 5

Приложение 8

Карточка № 1

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 магазины – это плохо, потому что это наиболее популярный вид жульничества в Интернете.
5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Карточка № 2

http://www.rgdb.ru
Российская государственная детская библиотека
http://ant.pc777.ru
Компьютерная служба
http://www.interneshka.net
Детский онлайн конкурс «Интернешка» по безопасному использованию Интернета
http://inetetiq.pp.ru
Правила этикета в Интернете
http://www.onlandia.org.ua/rus/
Онляндия – безопасная веб-страна
http://www.securelist.com/ru/safeonline/rules/
Все об интернет-безопасности
http://www.friendlyrunet.ru/safety/72/index.phtml
Дружественный Рунет

Список используемой литературы:

1. «Школьный сектор. Права и дети в Интернете» (schoolsectorp.wordpress.com),
2. «Безопасность» (http://sos-ru.info),
3. «Безопасный Интернет» (http://www.saferinternet.ru)
4. «Интернешка» http://interneshka.net/presscenter/index.phtml
5. Челышева И.В. «Медиаобразование для родителей: освоение семейной медиаграмотности». Научно-популярное издание. Таганрог: Изд-во ТТИ ЮФУ, 2008. 184 с. ISBN 978-5-8327-0258-2.
6. Методические рекомендации по проведению уроков «Безопасность в интернете» в начальной и средней школе Автор: Комарова Наталия Ивановна — кандидат социологических наук, ведущий научный сотрудник НИИСО МГПУ Технический консультант: Гончаров Дмитрий Константинович - старший научный сотрудник НИИСО МГПУ.
7. Методические рекомендации: Методика организации недели «Безопасность Интернет»./Авторы составители: Селиванова О. В., Иванова И. Ю., Примакова Е. А., Кривопалова И. В. - Тамбов, ИПКРО 2012.
8. Прогулка через дикий Интернет Лес (Through the Wild Web Woods). Игра для детей, посвященная вопросам обеспечения безопасности в интернете. Пособие для учителей. «***Строим Европу для детей и вместе с детьми»***. http://www.coe.ru/drive/children/Teachers%20aids/WildWebWoods_RUS.pdf
9. Игра http://www.wildwebwoods.org/popup.php?lang=ru