**УРОКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Использование Интернета в образовательных учреждениях и дома расширяет информационное образовательное пространство обучающего и позволяет повысить эффективность обучения. Доступ учащихся к информационным ресурсам сети Интернет дает возможность школьникам пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельного обучаться. Благодаря таким ресурсам у школьников появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие. Использования Интернета в работе с детьми и собственно в работе школы достаточно обширно: это использование электронной почты; поиск в сети нужной информации; создание собственных школьных веб-страниц; рассылка и/или съем материалов (нормативных документов, информации о семинарах и конкурсах и т.п.); обмен опытом; ответы на типичные вопросы; получение ("скачивание") небольших обучающих программ по разным предметам; совместные проекты школьников (и учителей) разных школ.

Однако использование Интернета в образовательной деятельности таит в себе много опасностей. Очень важно, чтобы во всех школах был безопасный Интернет. По статистическим данным на сегодняшний день в России насчитывается от 8 до 10 млн. интернет-пользователей в возрасте до 14 лет. Две трети детей выходят в глобальную сеть самостоятельно, без присмотра родителей и педагогов. Примерно 40% школьников посещают веб-страницы нежелательного и запрещенного содержания. Не секрет, что у многих развивается интернет-зависимость и игромания.

Отказываться от информационных технологий бессмысленно, но бесконтрольный доступ к Интернету может привести к негативным последствиям:

¨     киберзависимости,

¨      заражению вредоносными программами при скачивании файлов,

¨      нарушению нормального развития ребенка,

¨     неправильному формированию нравственных ценностей,

¨     знакомству с человеком с недобрыми намерениями.

         Сегодня проблема информационной безопасности школьников стала актуальной. Надо с первого знакомства с информационными технологиями разъяснять ребенку, как ему вести себя в информационном пространстве. Важно, чтобы взрослые, и дети понимали, что в информационном пространстве есть свои плюсы и минусы, есть плохое и хорошее. Необходимо научить детей извлекать из ресурсов только лучшее и безопасное, делать осознанный и грамотный выбор. Необходимо обсуждать с детьми все вопросы, которые возникают у них при использовании Интернет. Чем больше взрослые будут знать о том, как дети используют Интернет, тем проще определить и объяснить, что является приемлемым и безопасным.

Для преодоления негативного воздействия сети Интернет школа должна проводить целенаправленную воспитательную работу с педагогическим коллективом, учащимися, родителями.

Безопасность детей одна из главных задач цивилизованного общества, поэтому обеспечивать безопасность детей в Интернете должны все, кто причастен к этому обществу.

С подключением доступа к сети Интернет в школе проведены следующие организационные мероприятия:

¨      Назначен ответственный за работу «точки доступа к сети Интернет» в школе.

¨      Утверждена инструкция ответственного за работу «точки доступа к сети Интернет».

¨      Координация и информационно – методическое обеспечение осуществляется заместителем директора по УВР.

Профилактическая работа с обучающимися. Работа с учащимися с учетом их возрастных особенностей.

В начальной школе – в виде сказок, игр. В средней школе – в виде бесед, ролевых игр, диспутов, тренингов. В старшей школе – в виде проектов, выпуска стенгазет, участия в акциях, конкурсах.

Ежегодно в нашей школе проходит традиционная неделя естественно-математических наук, в рамках которой проводится День безопасного Интернета. Программа, посвященная этому дню, включает в себя ряд мероприятий, направленных на обучение учителей, родителей и детей правилам безопасного пользования Интернетом. Это классные часы по теме «Безопасность в сети Интернет»; выпускаются листовки с памятками для учащихся «Безопасность в Интернете» и т.д.

**Профилактическая работа с родителями**.

Формы работы с родителями различны – родительские собрания, индивидуальные беседы, лекции. Родители должны понимать, что никто так сильно не отвечает за безопасность детей в Интернете, как сами родители. Только они могут полностью контролировать своих детей.

Вот выдержка из аннотации к книге Заряны и Нины Некрасовых «Как оттащить ребенка от компьютера и что с ним делать», вышедшей в издательстве «София»: «Дети и подростки прирастают к розетке тогда, когда реальный мир не может предложить им других полноценных занятий. Не надо бороться с компьютером, борьба не укрепляет семьи. Надо просто понять истинные потребности своих детей - и найти в себе силы и время общаться, играть, слушать их. Просто посмотреть на все (в том числе и на компьютеры, ТВ, мобильник, плеер и прочие розеточные изобретения) глазами детей и подростков. И тогда виртуальный мир станет помощником вашей семье, для чего он, собственно, и предназначен».

Для разъяснения родителям опасностей Интернета проводятся родительские собрания «Безопасный Интернет - детям».

Формирование информационной культуры и безопасности - процесс длительный и сложный, но важный и необходимый. Интернет может быть и всемирной энциклопедией, объединяющей информационные ресурсы во всем мире. Задача взрослых (педагогов, родителей) - формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности. А для этого необходимо повышать квалификацию педагогов по вопросам информационной безопасности, чтобы уметь оперативно ориентироваться и ориентировать детей по безопасному поведению в Интернете. Регулярно проводить родительский всеобуч по вопросам кибербезопасности и работать не вдогонку, а на опережение.

Решение задачи по обеспечению безопасности при использовании компьютера и интернета детьми требует  комплексного подхода, решения множества психолого-педагогических вопросов. Эти направления должны стать основой для решения проблем медиабезопасности в образовательных учреждениях.

Стимулируя детей к более широкому разнообразию онлайн-деятельности и одновременно с этим обучая их критически оценивать ресурсы, развивая навыки безопасного поведения в сети, педагоги приумножают те преимущества, которые дает обучение в онлайне, усиливает защиту наших детей и повышают компетентность всех участников образовательного процесса. Особые усилия необходимы в отношении самых младших детей.

**Нормативно-правое обеспечение** является основой деятельности образовательного учреждения по всем направлениям. В образовательном учреждении должен быть сформирован пакет нормативно-правовой документации федерального, регионального и муниципального и учрежденческого уровней по вопросам информационной безопасности. К таким документам относятся документы по контентной фильтрации, по обработке персональной информации, положения и регламенты по работе в сети Интернет как педагогических работников, так и школьников, различные положения об организации профилактической работы по медиабезопасности, о формах профилактической работы с детьми и родителями по Интернет-безопасности, правила безопасного поведения в сети Интернет. В образовательном учреждении приказами должны быть назначены лица, ответственные за контентную фильтрацию, за работу с персональными данными, за организацией работы школьников в сети Интернет и т.д.

В **организационном плане** по обеспечению информационной и медиабезопасности в образовательном учреждении должен выполняться ряд мер технико-технологической направленности:

- установка только лицензионного программного обеспечения,

- подключение к системе контентной фильтрации;

- установка антивирусных программ,

-установка и настройка программ-фильтров, брандмауэров.

К организационным внутришкольным мероприятиям относятся:

¨     разработка и реализация правил Интернет-безопасности, с привлечением заинтересованных лиц: директора школы, классных руководителей, преподавателей информационных технологий, самих учащихся и их родителей, поставщиков услуг интернета,

¨     организация работы детей в Интернет по расписанию с ограничением по времени под наблюдением педагогических работников,

¨     регулярная проверка принимаемых мер в области Интернет безопасности в образовательном учреждении.

Для организации **профилактической работы** по медиабезопасности с детьми и родителями педагогический работник должен знать проблемы и опасности, которые подстерегают пользователя в сети Интернет, и быть готов дать рекомендации по решению данных проблем.

    Для организации профилактических мер в образовательном учреждении необходимо периодически проводить мониторинг, диагностику проблем по Интернет-безопасности среди детей и родителей. Данный мониторинг и разъяснительную работу можно проводить в Интернет-проекте «Дневник.ру». В этом проекте реализованы функции школьного модератора, в обязанности которого входит модерация нежелательного содержания в сети проекта и есть возможность применять действенные санкции к нарушителям правил пользования интернетом. В Интернет-проекте «Дневник.ру» можно организовать виртуальные мероприятия с родителями по вопросам Интернет-безопасности, разместить рекомендации в электронном виде.

В аспекте **программно-методического обеспечения** в образовательном учреждении должна быть разработана программа (раздел, модуль комплексной программы по профилактике девиантного поведения детей), в которую должны быть включены темы по медиабезопасности, о безопасном поведении в сети Интернет. Такие же темы и проблемы должны включаться в программы воспитательной деятельности.

Рекомендуемая тематика для организации профилактической деятельности:

- нежелательная информация в Интернете, как ее избежать,

- проблемы достоверности информации в Интернете, как проверить достоверность информации,

- социальные сети: опасности и правила поведения в социальных сетях,

- кибермошенничества, как избежать кибермошенников,

- киберхулиганство, киберзапугивание, правила поведения в опасной виртуальной ситуации,

- вредоносные программы, методы борьбы с ними,

- полезные ссылки, ресурсы, сервисы в Интернете.

Во время мероприятий по медиабезопасности следует ознакомить обучающихся:

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

- с информацией о необходимости критического отношения к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи,

признаках отличия достоверных сведений от недостоверных, способах нейтрализации вредной и опасной для детей информации, распознавания признаков злоупотребления доверчивостью;

- с правилами общения в социальных сетях (сетевой этикет);

- ознакомить обучающихся с адресами помощи в случае интернет-угрозы, номером всероссийского детского телефона доверия.

Тематика проведения различных школьных мероприятий по медиабезопасности может быть самой разнообразной, например:

- противозаконная, неэтичная и вредоносная информация в Интернете: как ее избежать,

- достоверность информации в интернете, проблемы и способы проверки информации на достоверность и полноту,

- этика сетевого общения,

- личная информация: нужна ли она в интернете, как защитить личную информацию в блогах, социальных сетях и пр.

- социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников,

- что такое хакерство: этика и основы,

- интернет- зависимость: угрозы, реальность, проблемы, решения,

- Web -серфинг: как не потерять себя и свое время в Интернете,

- как распознать кибермошенничество и не стать жертвой,

- нигерийские письма: предложения в письмах и как не попасться на удочку мошенников,

- что такое киберхулиганство: как не стать жертвой и киберхулиганом;

- как защитить свою почту от спама и не стать спамером,

- компьютерные вирусы и методы борьбы с ними,

- киберпреступления в законодательстве России,

- безопасность в коммерческих Интернет-сервисах: Интернет-магазины, услуги различных фирм и др.,

- компьютерные игры, как не стать игроманом,

- азартные игры в Интернете – поле чудес для….?

- мобильные угрозы в современном мире,

- как правильно вести себя с киберхулиганами и защититься от нежелательного общения,

- твоя жизнь не игрушка.

**Методические рекомендации по организации урока**

**информационной безопасности в основной школе**

Анализ УМК по информатике и ИКТ для основной школы на предмет изучения информационной безопасности позволяет сделать вывод о том, что на уровне основного общего образования в рамках предмета «Информатика» акцент в соответствии с требованиями ФГОС делается на формировании навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

***УМК «Информатика» 7 - 9 класс (ФГОС), автор Угринович Н. Д.***

Тема «Информационное общество и информационная безопасность». Всего 3 часа: 1 час в 7 кл. и 2 часа в 9 кл. Содержание темы: Информационное общество. Информационная культура. Перспективы развития информационных и коммуникационных технологий. Правовая охрана программ и данных. Защита информации. Правовая охрана

информации. Лицензионные, условно бесплатные и свободно распространяемые программы.

***УМК «Информатика» 7 - 9 класс (ФГОС), авторы Семакин И.Г. и др.***

Аспекты информационной безопасности рассматриваются в 7 и 9 классах в рамках тем «Компьютер: устройство и программное обеспечение» (содержание темы: правила техники безопасности и эргономики при работе

за компьютером, использование антивирусных программ) и «Информационные технологии и общество» (содержание темы: проблемы безопасности информации, этические и правовые нормы в информационной сфере).

***УМК «Информатика» 5-9 класс (ФГОС), автор Босова Л.Л.*** Предметные результаты «Формирование навыков и умений безопасного

* целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права» формируются в 5 классе при изучении темы «Передача информации», в 7 классе при изучении тем «Всемирная паутина» и «Программное обеспечение компьютера», в 9 классе при изучении темы «Информационные ресурсы и сервисы Интернета».

***УМК «Информатика» 7-9 класс, (ФГОС), авторы Горячев А.В.***

Некоторые аспекты информационной безопасности рассматриваются в 7 классе при изучении темы «Общение в сети Интернет». Содержание темы: Как вести себя и чего опасаться в сети Интернет. Ваша личная территория в

сети Интернет. Личное и публичное общение в Интернете. Как правильно спорить в Интернете.

***УМК «Информатика» 7-9 класс, (ФГОС), авторы Гейн А.Г, Юнерман Н.А. и др***.

* + 9 классе в рамках темы «Правовые вопросы Интернета. Безопасность
* этика Интернета. Защита информации» рассматриваются вопросы информационной безопасности в сети Интернет.

Таким образом, все авторские коллективы уделяют внимание вопросам информационной безопасности, в основном аспектам безопасного поведения

* Интернете и защите от компьютерных вирусов. В основном такие уроки запланированы авторами в начале 7 класса и в конце 9 класса. При этом, с учетом потери уроков в праздничные дни и подготовкой к ОГЭ в конце 9 класса, учителя информатики часто предлагают данные темы на самостоятельное изучение обучающимся. А в 5, 6, 8 классах эта тема в явном виде вообще отсутствует. Однако именно в подростковом возрасте дети становятся участниками сетевых сообществ, ведут активную деятельность в Интернете. Конечно же, на этом этапе необходимо рассказать им о защите персональных данных, о признаках компьютерной зависимости и синдрома информационной усталости, о мошенничестве, связанном с использованием мобильных устройств. Поэтому совершенно необходимо дополнительное проведение занятий информационной безопасности. Это могут быть классные часы или внеурочные занятия, проектная деятельность.

Вместе с переходом в возрастную категорию «подросток» проблемы, связанные с Интернетом, становятся действительно острыми и глобальными. Дополнительная психологическая и социальная проблема детей подросткового возраста заключается в возрастном становлении характера и скептическом и недоверчивом отношении к замечаниям и рекомендациям родителей и учителей. А техническая подготовленность к использованию возможностей сети Интернет уже достаточна высока на фоне несформировавшейся психики и неустойчивого социального поведения школьников средней школы.

Учителю, чтобы усилить воспитательные меры работы с учениками важно показать, что вы такой же регулярный пользователь в сети, и сетевых сервисов: социальных сетей, чатов, форумов профессиональной направленности или связанных с личными увлечениями. Можно наладить с ними виртуальное общение по электронной почте, по skype, задавать задания, связанные с необходимостью налаживания такого рода общения.

Например, преподаватель биологии может попросить своих учеников, посадивших семена огородных растений дома для домашнего наблюдения за их ростом, присылать фотографии стадий роста растений по электронной почте. Таким образом, отрабатываются не только домашние задания непосредственно по программе курса и имеет место внедрение ИКТ в

образовательный процесс, но и формируется элемент электронной учебной коммуникации с преподавателем, повышающий авторитет учителя и заставляющий ученика осознанно работать с образовательными возможностями [11].

Как включить в образовательный процесс мероприятия, повышающие информационную культуру школьника основной школы? Какие методы, формы при этом использовать?

Информационная безопасность в Интернете может обсуждаться во время уроков информатики, социологии, ОБЖ, гражданского права и др. В образовательном учреждении рекомендуется проводить неделю, день, уроки Интернет-безопасности, внеклассные мероприятия.

Мероприятия можно приурочит к профессиональным праздникам:

*Международный день защиты информации* – 30ноября.Праздникначал существовать в 1998 году (с праздника есть даже сайт) т.к. в 1988 г. была зафиксирована первая массовая эпидемия червя, получившего название по имени своего «творца» – Морриса. Праздник существует и признан международным благодаря американской Ассоциация компьютерного оборудования. Цель этого Дня — напомнить всем о необходимости защиты компьютерной информации, а также обратить внимание производителей и пользователей аппаратных и программных средств на проблемы безопасности.

*Международный день безопасного Интернета* –второй вторникфевраля (введен в 2004 году). Сайт международного дня безопасности Интернета www.saferinternetday.org

Во время мероприятий по медиабезопасности следует ознакомить обучающихся:

* с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;
* с информацией о необходимости критического отношения к сообщениям
  + СМИ (в т.ч. электронных), мобильной (сотовой) связи, признаках отличия достоверных сведений от недостоверных, способах нейтрализации вредной и опасной для детей информации, распознавания признаков злоупотребления доверчивостью;
* с правилами общения в социальных сетях (сетевой этикет).
  + - рекомендациях «Безопасный Интернет» [14] предлагается следующая тематика проведения школьных мероприятий по медиабезопасности:
* Противозаконная, неэтичная и вредоносная информация в Интернете: как ее избежать.
* Достоверность информации в Интернете, проблемы и способы проверки информации на достоверность и полноту.
* Этика сетевого общения.
* Личная информация: нужна ли она в Интернете, как защитить личную информацию в блогах, социальных сетях и пр.
* Социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников.
* Что такое хакерство? Почему хакеров считают преступниками.
* Интернет- зависимость: угрозы, реальность, проблемы, решения.
* Web -серфинг: как не потерять себя и свое время в Интернете.
* Как распознать кибермошенничество и не стать жертвой.
* Нигерийские письма: предложения в письмах и как не попасться на удочку мошенников.
* Что такое киберхулиганство: как не стать жертвой и киберхулиганом.
* Как защитить свою почту от спама и не стать спамером.
* Компьютерные вирусы и методы борьбы с ними.
* Законодательство России о киберпреступлениях.
* Безопасность в коммерческих Интернет-сервисах: Интернет-магазины, услуги различных фирм и др.,
* Компьютерные игры, как не стать игроманом.
* Азартные игры в Интернете – поле чудес для….?
* Мобильные угрозы в современном мире.
* Как правильно вести себя с киберхулиганами и защититься от нежелательного общения.

Одним из эффективных способов изучения любого учебного материала

* в частности вопросов по информационной безопасности является метод высокотехнологичных учебных проектов. Учителю любой дисциплины важно инициировать большие и малые телекоммуникационные учебные проекты.
  + методических рекомендации по проведению уроков «Безопасность в

Интернете» в начальной и средней школе [11] *учебный* *телекоммуникационный проект* рассматривается как совместная учебно-познавательная, творческая или игровая деятельность учащихся-партнеров, организованная на основе компьютерной телекоммуникации, имеющая общую цель, согласованные способы деятельности, направленная на достижение общего результата деятельности.

Так, например, можно участвовать в сетевых проектах для школьников организованных дистанционно или организовать собственный учебный проект.

Школьной проектной деятельностью учитель решает сразу несколько проблем [11]: во-первых, учащиеся приобретают навык практического применения полученных теоретических знаний по использованию компьютеров, компьютерных технологий и Интернета и связанные с этим вопросы безопасности; во-вторых, и это самое главное, школьник начинает видеть в компьютере и Интернете не только игрушку и поток непотребных

ресурсов, но инструмент создания нового, интересного и нужного не только ему, но и окружающим его в школе и дома людям, пространства. И в этом пространстве ребёнок подобен творцу: каким он его создаст, таким его мир и будет.

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

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

б) очень высокотехнологичным, чтобы для его реализации школьнику

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

в) долгосрочным и предусматривающим дальнейшее коммуникативное дополнение. После размещения его в сети у детей, гордящихся проделанной работой, должен быть стимул общаться в Интернете на тему своего проекта и постоянно дополнять и дорабатывать его. Для этого необходимо устраивать публичные показы проектов школьников на классных часах, на предметных уроках, в рамках программы которых сделаны эти проекты.

Если ребенок с социально-значимым результатом побывал в сети, узнал, что в сети можно оформлять фото и видео материалы, создавать презентации, инструменты для проверки знаний, организовать личное сетевое пространство, проводить информационные исследования, то вряд ли него появится в дальнейшем желание вновь перейти к праздному лицезрению сетевых ресурсов.

Конкретным примером реализации проектной деятельности может стать WEB-квест. Для примера можно рассмотреть WEB-квест «Безопасный Интернет» http://www.web-kvest.pldetstva.edusite.ru/p1aa1.html

*Веб-квест* -это игра,реализованная на сетевом ресурсе с заданиями надкоторыми работают учащиеся, выполняя ту или иную возложенную на них миссию – выбрав одну из ролей, предложенных учителем.

*Особенностью* образовательных веб-квестов является то,что часть илився информация для самостоятельной или групповой работы учащихся с ним находится на различных веб-сайтах, ссылки на которые может предложить педагог, предварительно выбрав самые интересные и информативные по изучаемому вопросу. Кроме того, результатом работы с веб-квестом является публикация работ учащихся в виде веб-страниц и веб-сайтов (локально или в Интернет).

При продумывании методов организации урока и внеурочной деятельности важно помнить об особенностях мышления современной молодежи - «клиповом», которое не отличается глубиной проникновения в информацию, но зато отличается большими скоростями пропускания через себя информации. Дети сегодня не умеют анализировать текстовую информацию, не обладают навыками функциональной грамотности чтения. Для формирования данной грамотности, важно учить детей сворачивать и разворачивать информацию, представлять ее в различных формах. Решением проблемы может стать задания по преобразованию одного вида информации

* другой вид. Например, можно предложить информацию из видео или текст перевести в графику – плакат, комикс, инфографику или, наоборот, по картинке, плакату, комиксу, инфографике составить рассказ, объясняющий

вопросы безопасности информации. Результаты деятельности важно предоставить общественности – опубликовать в Интернете, повесить в тематических уголок школы, выпустить газету для школы с результатами деятельности, выступить перед младшими школьниками.

На уроке ребятам предлагается посмотреть ролики

* Развлечения и безопасность в Интернете
* Как обнаружить ложь и остаться правдивым в Интернете
* Остерегайся мошенничества в Интернете
* Как оставаться в безопасности на YouTube

По материалам видеороликов создать в группах тематические листовки, используя сетевые технологии совместного редактирования Google.

Лучшие листовки повесить в *уголок безопасности*, который должен быть в каждой школе.

*Итак, резюмируем, на что нужно обратить особое внимание при рассмотрении вопроса об Интернет безопасности детей основной школы:*

1. Относись к информации осторожно. То, что веб-сайт эффектно выглядит, еще ни о чем не говорит. Спроси себя: для чего этот сайт сделан? 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. Часто в Сети можно столкнуться с подделками под известные сайты социальных сетей или почтовых сервисов, так называемым «фишингом». После неосторожного ввода имени пользователя и пароля на страницах не настоящих, поддельных сайтов, злоумышленники используют пароли в своих целях на реальных сайтах. Например, для рассылки спама от имени владельца почтового ящика или злоумышленного обращения в социальных сетях от имени владельца аккаунта. Каждый сайт в Интернете имеет свой уникальный адрес. Необходимо проверять именно адрес страницы, не доверяя внешнему оформлению, которое может быть скопировано с оригинального.
3. Используя информацию из Интернета в своей работе, следуй правилу трех источников. Организуй поиск и сравни три разных источника

информации, прежде чем решить, каким источникам можно доверять. Не забывай, что факты, о которых ты узнаешь в Интернете, нужно очень хорошо проверить, если ты будешь использовать их в своей работе.

Хотя Интернет – специфическая среда для общения, в ней существуют определенные правила вежливости, которые широко обсуждаются в Интернете, но, к сожалению, культура общения остается на низком уровне. В сети нередко можно наблюдать грубость, речевую агрессию, нетерпимость к чужим мнениям. Важно сохранять правила человеческого общения даже в случае анонимной коммуникации. На эмоциональное послание лучше отвечать не мгновенно, а через некоторое время, дабы не плодить излишний негатив в общении. Основные правила общения в сети описаны в приложении «*Сетевой этикет»*.

**Единый урок «Безопасный Интернет»**

**Цель урока:**

Познакомить учащихся с преимуществами сети Интернет, скрытыми и открытыми угрозами Интернета, классификации интернет угроз;

Сформировать понятия Интернета; Научить учащихся критически относиться к информационной продукции, распространяемой в сети Интернет; Уметь отличать достоверные сведения от недостоверных, вредную информацию от безопасной; Распознавать признаки злоупотребления неопытностью и доверчивостью учащихся, попытки вовлечения их в противоправную деятельность.

**Оборудование:** интерактивная доска с ноутбуком, презентация, видео ролик, буклеты, смайлики.

**Ход урока**

**1. Организационный момент (приветствие учащихся начальной школы, основной и средней школы).**

**2. Мотивационное начало урока**

Тема нашего урока “Безопасность в Интернете”.

**Безусловные преимущества использования Интернет**

В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а так же получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам.

**Скрытые и открытые угрозы Интернет**

Однако бурное развитие Интернета несет также существенные издержки. Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов. Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются ресурсами, содержащими неэтичный и агрессивный контент. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки. Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

1. ***Установите комплексную систему защиты.***

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

1. ***Будьте осторожны с электронной почтой***

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

1. ***Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.***Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.
2. ***Обновляйте операционную систему Windows.***

Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

1. ***Не отправляйте SMS-сообщения.***

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.

При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

1. ***Пользуйтесь лицензионным ПО.***

Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.

Лицензионные программы избавят Вас от подобной угрозы!

1. ***Используйте брандмауэр.***

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

1. ***Используйте сложные пароли.***

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

1. ***Делайте резервные копии.***

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.

1. ***Функция «Родительский контроль» обезопасит вас.***

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз.

***Школьникам младших классов***

**Если ты любишь сидеть в Интернете, запомни эти правила безопасности!**

Если что-то непонятно

страшно или неприятно,  
Быстро к взрослым поспеши,  
Расскажи и покажи.

Как и всюду на планете,  
Есть опасность в интернете.  
Мы опасность исключаем,  
Если фильтры подключаем.

Как и всюду на планете,  
Есть опасность в интернете.  
Мы опасность исключаем,  
Если фильтры подключаем.

Злые люди в Интернете  
Расставляют свои сети.  
С незнакомыми людьми  
Ты на встречу не иди!

С грубиянами в сети  
Разговор не заводи.  
Ну и сам не оплошай -  
Никого не обижай.

Чтобы вор к нам не пришёл,  
И чужой нас не нашёл,  
Телефон свой, адрес, фото  
В интернет не помещай  
И другим не сообщай.

***Школьникам средних классов***

**Вы должны это знать:**

* При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
* Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
* Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылась вам спам.
* Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
* Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.
* Если вас кто-то расстроил или обидел, расскажите все взрослому.

**Физкультминутка (1 мин)**

Но сначала, мы немножко отдохнем и проведем физкультминутку.

Мы все вместе улыбнемся,

Подмигнем слегка друг другу,

Вправо, влево повернемся

И кивнем затем по кругу.

Все идеи победили,

Вверх взметнулись наши руки.

Груз забот с себя стряхнули

И продолжим путь науки.

Итак, как же бороться с сетевыми угрозами?

***Школьникам старших классов***

**Вы должны это знать:**

* Не желательно размещать персональную информацию в Интернете.

Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

* Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
* Не отвечайте на Спам (нежелательную электронную почту).
* Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
* Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
* Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
* Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
* Никогда не поздно рассказать взрослым, если вас кто-то обидел.

**Учителям и преподавателям**

***Чтобы помочь учащимся, Вы должны это знать:***

* Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет—угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а так же какое программное обеспечение на них установлено.
* Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях.
* Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.
* Выберите интересные ресурсы и предложите детям изучить их вместе.
* Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

***Использование Интернета является безопасным, если выполняются три основные правила.***

***1. Защитите свой компьютер***

Регулярно обновляйте операционную систему.

Используйте антивирусную программу.

Применяйте брандмауэр.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке содержимого.

***2. Защитите себя в Интернете***

С осторожностью 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.

**Урок Интернет-безопасности**

В настоящее время, в связи с переходом на новые стандарты образования, и теми требованиями, которые выдвигает общество образованию в целом, и организации образовательного процесса в частности, невозможно представить работу современного учителя без применения компьютерных технологий.

Всемирная сеть Интернет, а также использование различных текстовых программ и графических редакторов дают учителю почти неограниченные возможности к творчеству, самореализации и наиболее эффективной организации учебного процесса.

В информационном обществе сознание обучающимися значимости проблемы безопасности детей в Интернете и ее решения для будущего общества и образования необходимо формировать в урочной деятельности школьных курсов, включая курс “Информатика и ИКТ” с использованием всех педагогических технологий. Акцент в курсе необходимо делать на актуальности данной темы и постоянный самоконтроль учащихся в их дальнейшей самостоятельной деятельности

**Целиурока:**

* *Методическая:*показать актуальность данной темы
* *Учебная:*обучение информационной безопасности в Интернете
* *Воспитательная:*развитие самоконтроля учащихся и воспитание внимательного отношения к информационным ресурсам

**Задачиурока:**

* Ознакомить уч-ся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет и научить избегать их;
* Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности и освоить практические навыки работы в сети Интернет
* Отработка навыков и умений: сравнения информации, критического анализа; выделения главных мыслей и грамотного их изложение; восприятия и усвоения услышанного;
* Расширение кругозора учащихся
* Формирование информационной культуры

**Оснащение и методическое обеспечение урока:**

* Компьютерный класс, подключенный к Internet;
* АРМ учителя,
* Доска.

**Ход урока**

**1. Организационный момент. Постановка задачи.**

**2. Значение Интернет.**

**Учитель**: Ребята, в Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями.

Но сеть Интернет скрывает и угрозы.

**3. Наиболее часто встречающиеся угрозы при работе в Интернет:**

**Учитель**: Давайте разобьёмся на группы и каждая группа подумает и назовет опасности, которые нас поджидают в Интернете

(дети подумав, называют угрозы. Вся информация открывается в презентации)

Угроза заражения вредоносным программным обеспечением (ПО). Для распространения вредоносного ПО и проникновения в компьютеры используется почта, компакт-диски, дискеты и прочие сменные носители, или скачанные из сети Интернет файлы. Эти методы довольно часто используется хакерами для распространения троянских вирусов;

Доступ к нежелательному содержимому. Это насилие, наркотики, страницы подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией. Независимо от желания пользователя, на многих сайтах отображаются всплывающие окна, содержащие подобную информацию;

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. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи;

Поиск развлечений (например, игр) в Интернете. Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег.

Неконтролируемые покупки.

**Учитель**: А сейчас мы посетим сайт, который помогает вас защитить от ненужной информации http://icensor.ru/

**4. Составление правил поведения в сети Интернет**

**Учитель**: Очередное задание для каждой команды. Мы знаем, что для плодотворной работы в Интернете, защиты от ненужной информации, нам необходимо соблюдать правила пользования Интернет-ресурсами. Сейчас вам в группах необходимо обсудить и сформулировать не более 5 самых важных правил безопасности поведения детей и подростков в сети Интернет. Одно правило может ссылаться сразу на несколько сайтов. (Работа проводится с использованием компьютеров, подключенных к сети Интернет)

Когда ребята готовы, на доске составляется сводная таблица правил поведения в сети Интернет.

|  |  |
| --- | --- |
| Никогда | Всегда |
| Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или номер школы без разрешения родителей | Всегда будь внимательным, посещая чаты. Даже если в чате написано, что он только для детей, нельзя точно сказать, что все посетители действительно являются твоими ровесниками. В чатах могут сидеть взрослые, пытающиеся тебя обмануть |
| Никогда не отправляй никому свою фотографию, не посоветовавшись с родителями | Всегда спрашивай у родителей разрешения посидеть в чате |
| Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах | Всегда покидай чат, если чье-то сообщение вызовет у тебя чувство беспокойства или волнение. Не забудь обсудить это с родителями |
| Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера | Всегда держи информацию о пароле при себе, никому его не говори |
|  | Если ты услышишь или увидишь, что твои друзья заходят в “небезопасные зоны”, напомни им о возможных опасностях и посоветуй, как им правильно поступить. |
|  | Будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в “небезопасную зону” или загрузить на свой компьютер вирус или программу - шпион. |
|  | Если вы получили оскорбляющие сообщения, расскажите об этом родителям |
|  | Всегда принимайте помощь от взрослых или друзей, разбирающихся в вопросах безопасного Интернета. Мама и папа могут не знать ответов на все интересующие вас вопросы. |
| Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые | Всегда помни, что если кто-то сделает тебе предложение, слишком хорошее, чтобы быть правдой, то это, скорее всего, обман |
|  | Всегда держись подальше от сайтов "только для тех, кому уже есть 18". Такие предупреждения на сайтах созданы специально для твоей же защиты. Сайты для взрослых также могут увеличить твой счет за Интернет |

**Учитель**: Вы, ребята, хорошо поработали и за это я хочу показать и рассказать вам сказку:

**5. 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 её 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 всё-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 трёхуровнего, 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 “Лохотрон-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.

**6. Практическая часть.**

Зайдитевдетскийчат [http://prikol.interchat.ru/](http://prikol.interchat.ru/_blank),зарегистрируйтесьтам,ипообщайтесь,используяправилабезопасности,скоторымимысегодняознакомились.

**7. Подведение итогов урока.**

**8. Домашнее задание.**Найти в Интернете сайты, защищающие вас от “опасной” информации.