

Муниципальное бюджетное общеобразовательное учреждение
начальная общеобразовательная школа д. Соколовка
муниципального района Давлекановский район Республики Башкортостан



УТВЕРЖДАЮ

Директор МБОУ «НОШ д. Соколовка»

А.М. Минибаев

Программа обучения правилам безопасного поведения в Интернет – пространстве на 2017-2020 годы.

Пояснительная записка

В наше время невозможно переоценить роль ИКТ в жизни как взрослых, так и детей. Они прочно вошли в нашу жизнь, неся не только доброе и вечное, но и определённый процент негатива, так как первая часть аббревиатуры ИКТ, а именно «информационно», непосредственно связана с поиском необходимых данных, наглядности в сети Интернет. По результатам проведенного «Лабораторией Касперского» опроса 47% родителей отмечают, что их дети сталкиваются с нежелательным контентом в Интернете. Остальные респонденты (53%) не знают, какой опасности подвергаются несовершеннолетние в Сети. Чаще всего родители хотят оградить своих детей от сайтов для «взрослых» (49%). Реже это компьютерные вирусы и шпионские программы (23%), а также недоброжелательно настроенные пользователи (15%).

Угрозы, от которых родители хотят оградить детей

Большинство опрошенных родителей ограничивают время пребывания детей в Интернете (86%), а также запрещают своему ребенку публикацию каких-либо личных данных в Сети (83%). «Результаты проведенного опроса свидетельствуют об актуальности проблемы защиты детей от нежелательного контента в Интернете. Каждый день появляется более 70 000 новых вредоносных программ, киберпреступники продолжают оттачивать мастерство социальной инженерии, и простого запрета со стороны родителей нередко недостаточно для того, чтобы оградить ребенка от опасных ресурсов.

Показатель времени пребывания детей в Интернете слишком высок, он и помог раскрыть тёмную сторону мировой сети. Анонимность Интернета и лёгкость в создании вымышленных личностей открыли широкую дорогу для сетевых хищников, воров личных данных, хакеров и других мошенников. Так как дети и подростки обычно не осведомлены о хитростях и техниках, которые эти "хищники" применяют, чтобы обмануть свои жертвы, и так как большинство используют интернет в повседневной жизни, то молодые люди рискуют в большей степени, чем другие пользователи Интернета.

Использование Интернета детьми без присмотра может привести к таким последствиям:

- В последнее время значительно участились случаи, когда программы - «дозвонщики» самостоятельно набирают дорогостоящие телефонные номера, создавая новое модемное подключение. Вы узнаете об этом только тогда, когда Вам приходит крупный телефонный счет.
- Дети очень любят общение в чатах. Однако при таком общении ребенку сложно увидеть истинное лицо человека, с которым они общаются. Если же такая виртуальная беседа приводит к личной встрече, последствия могут оказаться печальными.
- Дети рискуют, в одиночку посещая игровые страницы, так как множество из них являются пиратскими сайтами с большим количеством порнографической рекламы в виде всплывающих окон. Такие окна автоматически появляются на экране и часто содержат изображения, которые абсолютно не рекомендуются к детскому просмотру.

По имеющимся данным, в России более 9 млн пользователей Интернета ещё не достигли возраста 14 лет. Из них 25% детей ходят в Интернет под присмотром родителей, 75% бороздят его просторы в свободном плавании. Причем оказалось, что 48% детской аудитории Рунета не сталкиваются с ресурсами нежелательного содержания. В то же время 39% детей просматривали порносайты, 19% - наблюдали сцены насилия, 16%- интересовались азартными играми, 14%- наркотическими веществами, 11%-экстремизмом или национализмом. Поэтому необходимо научить ребенка пользоваться Интернетом, уберечь его от виртуальных недоброжелателей и вполне реальных неприятностей.

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 учащихся.

Данная программа рассчитана на период с 2017 по 2020 год.

Для организации безопасного доступа к сети Интернет в школе созданы следующие условия:

1. В МБОУ НОШ д. Соколовка разработаны и утверждены:

- ПРАВИЛА использования сети Интернет
- ИНСТРУКЦИЯ пользователя по безопасной работе в сети Интернет.
- ИНСТРУКЦИЯ о порядке действий при осуществлении контроля за использованием учащимися ОУ сети Интернет.
- **Классификаторы** информации, доступ к которой учащихся ОУ запрещен и разрешен.

2. Контроль использования учащимися сети Интернет осуществляется с помощью программно-технических средств и визуального контроля.

1. Нормативно-правовая база

Программа разработана с учетом требований законов РФ:

- «Об образовании в Российской Федерации», Закон РФ от 29.12.2012г. № 273-ФЗ;
- Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10;

2. Цели, задачи, основные мероприятия реализации программы

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

Задачи:

- формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;
- формирования информационной культуры как фактора обеспечения информационной безопасности;
- изучение с нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
- формирование знаний в области безопасности детей использующих Интернет;
- организации просветительской работы с родителями и общественностью.

Содержание программы

Одной из важных задач является создание и функционирование качественных интернет-ресурсов для детей. Сегодня крайне необходимо инициирование и создание новых «детских» ресурсов интернета в сфере образования и культуры. Чтобы интернет стал более безопасным для подрастающего поколения, сегодня необходима новая стратегия создания гуманного «детского» киберпространства.

Выработка единой стратегии безопасности возможна только совместными усилиями всех участников образовательного процесса: прежде всего педагогических работников (классных руководителей – без их помощи невозможно обучение двух других категорий пользователей сети Интернет), родителей и учащихся, поэтому программа предполагает работу по трём направлениям. Ни для кого не секрет, что для того, чтобы обучить детей, нужно чтобы правила безопасного поведения в сети Интернет усвоили взрослые (учителя и родители).

Работа с педагогическим коллективом

Обучение педагогических работников может проводиться в форме мастер-классов, семинаров, круглых столов, в рамках которых должны рассматриваться проблемы информационной безопасности личности в сети Интернет, нежелательный контент и меры борьбы с ним, виды и формы информационно-психологического воздействия и методы защиты от него, правила и нормы речевого этикета, причины возникновения девиантного поведения детей и методы работы по их профилактике и устранению. Прежде чем начать работу по предлагаемому плану необходимо ознакомить педагогов с планом обучения родителей и учащихся.

№ п/п	Наименование мероприятия	Сроки	Ответственные
1.	Ознакомление с рекомендациями по Интернет-безопасности для родителей и детей	Ежегодно август	Классные руководители
2.	Беседы со специалистом в области ИКТ: «Защита компьютера, репутации и секретной личной информации»; «Надежные пароли, безопасные веб-сайты, фишинговые сообщения электронной почты, ссылки или телефонные звонки»; «Защита финансовой информации в Интернете. Полезные Интернет-ресурсы» «Безопасное использование социальных сетей» «Защита от вредоносного ПО»	В течение года	Классные руководители
3.	Самообразование учителей по данной теме с использованием полезных Интернет-ресурсов	В течение года	Классные руководители
4.	Индивидуальные беседы	По мере необходимости	Классные руководители

Необходимую информацию можно найти на сайтах: «Школьный сектор. Права и дети в Интернете» (schoolsectorp.wordpress.com), «Безопасность» (sos-ru.info), «Безопасный Интернет» (saferinternet.ru).

Работа с родителями

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергаются их дети, находящиеся в сети Интернет. Некоторые из них считают, что это лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребёнка основам безопасности дома и на улице, не оттают себе отчёта в том, что он абсолютно незащищён перед потоком информации из Интернета. Наша задача – выработать в нём критическое мышление.

С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно её устранить силами только образовательного учреждения. Формы работы с родителями разнообразны: выступления на родительских собраниях, индивидуальные беседы, информация на сайте гимназии, встречи со специалистами-информатиками, психологами, семинарские занятия.

№ п/п	Наименование мероприятия	Сроки	Ответственные
1.	Ознакомление с рекомендациями для родителей различных возрастных категорий детей	Ежегодно сентябрь-октябрь	Классные руководители
2.	Обще школьное родительское собрание на тему: «Быть или не быть Интернету в компьютере вашего ребенка?»	Декабрь 2018	Директор, учителя
3.	Анкетирование «Знают ли родители, с кем общается их ребенок в сети?»	Ежегодно	Классные руководители
4.	Индивидуальные беседы	По мере необходимости	Классные руководители
5.	Обновление информация на сайте школы	По мере необходимости	Ответственный за обновление информации на сайте
6.	Беседы со специалистом в области ИКТ: «Защита компьютера, репутации и секретной личной информации»; «Надежные пароли, безопасные веб-сайты, фишинговые сообщения электронной почты, ссылки или телефонные звонки »; « Защита финансовой информации в Интернете . Полезные Интернет-ресурсы» «Безопасное использование социальных сетей» «Защита от вредоносного ПО»	В течение года	Директор, учителя
7.	Беседы с психологом об Интернет -зависимости	По мере необходимости	классные руководители
8.	Родительское собрание: «Интернет: плюсы и минусы»	Январь 2018	Директор, учителя

Одной из задач обеспечения защиты детей в интернете является решение проблемы контентной фильтрации. Многие российские фирмы предоставляют специальные программы по фильтрации информации. Так, например, известная фирма А. Касперского представляет целый ряд программ для родительского контроля детей в Интернете. Только каждый десятый (11%) использует специальные программы с

функцией [Родительского контроля](#) для ограничения определенного содержания в Интернете. Поэтому рекомендуется всем родителям ознакомиться с функцией [«Родительского контроля»](#), которая входит в состав некоторых программ, в том числе и *Kaspersky Internet Security 2012*. Функция [«Родительский контроль»](#) позволяет контролировать время использования компьютера и Интернета ребенком, запуск определенных программ, ограничивать загрузку файлов из Интернета, а также контролировать общение в социальных сетях. Кроме того, Родительский контроль позволяет просматривать статистические отчеты о действиях, совершенных ребенком на компьютере.

Работа с учащимися

Работа в этом направлении должна вестись в зависимости от возрастных особенностей: начальное звено (2-4 класс) На каждом этапе необходимы специальные формы и методы обучения в соответствии с возрастными особенностями. Формирование навыков информационной безопасности и культуры должно проводиться не только на уроках, а также и во внеурочной деятельности.

№ п/п	Наименование мероприятия	Возрастная категория	Сроки	Ответственные
1.	Тематическое анкетирование учащихся	1-4 классы	ежегодно	классные руководители
2.	Ознакомление с памятками для учащихся начальной школы	1-4 классы	ежегодно	классные руководители
3.	Уроки безопасности работы в Интернет для учащихся 1–4, 5–9, 10– 11 классов.	1-4 классы	ежегодно сентябрь	классные руководители
4.	Классные часы, задачей которых является ознакомление учащихся с опасностями, которые подстерегают их в Интернете: «Безопасность в сети Интернет» «Развлечения и безопасность в Интернете», «Темная сторона Интернета» «Опасности в Интернете» «Как обнаружить ложь и остаться правдивым в Интернете», «Остерегайся мошенничества в Интернете»	(1-4) классы	в течение года	классные руководители

Классными руководителями может быть проведено он-лайн-знакомство со следующими сайтами.

«Школьный сектор. Права и дети в Интернете» (schoolsectorp.wordpress.com). Данный детский правовой сайт состоит из двух основных частей: игровой и информационной. В игровой — ситуации, иллюстрирующие юридические проблемы, с которыми мы сталкиваемся в жизни. Помощники — забавные персонажи, которые могут стать друзьями.

«Безопасность. Правила безопасности в повседневной жизни» (sos-ru.info). На сайте систематизировано и выложено много собранной из различных источников полезной и практичной информации по безопасности жизнедеятельности.

«Безопасный Интернет» (saferinternet.ru). Портал Российского Оргкомитета по проведению Года Безопасного Интернета.

Одним из наиболее значимых пунктов данной программы является создание «Совета по Интернет-безопасности», в рамках которого учащиеся будут изучать и создавать проекты по данной тематике, проводить заседания, выступать с докладами, что позволит воспитать не только культуру общения в сети, но и привить нравственность, ответственность за использование и передачу информации.

Неделя безопасного Интернета проводится в целях привлечения внимания к проблеме детей и взрослых в сети Интернет. Предметная неделя как форма методической, учебной и внеклассной работы представляет собой комплекс взаимосвязанных мероприятий, предлагает разнообразные формы деятельности, способствует личностному развитию учащихся. Сценариями предлагаемых внеклассных мероприятий, классных часов, бесед изобилуют учительские и школьные сайты, а также сайты педагогических сообществ.

Методические рекомендации «Безопасный Интернет»

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

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

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

Анкетирование учащихся.

Для изучения безопасности в сети Интернет и отношения к ней подростков разрабатываются анкеты, позволяющие проанализировать современную ситуацию в образовательной среде.

Анкетирование предполагается проводить в форме анонимного опроса как на бумажных носителях, так и в электронном виде. Примерные формы анкет представлены в Приложении 1 и Приложении 2.

Проведение круглого стола

«Основы безопасности в сети Интернет»

Цель: формирование устойчивых жизненных навыков при работе в сети Интернет. Работе круглого стола предшествует предварительная подготовка учащихся по предложенной тематике. Перечень вопросов для обсуждения выявляется в результате анкетирования учащихся.

Примерные вопросы для обсуждения:

1. Для чего нужен Интернет?
2. Какие существуют риски при пользовании интернетом, и как их можно снизить?
3. Какие виды мошенничества существуют в сети Интернет?
4. Как защититься от мошенничества в сети Интернет?
5. Что такое безопасный чат?
6. Виртуальный собеседник предлагает встретиться, как следует поступить?
7. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений.

При подведении итогов круглого стола обучающимся можно предложить правила поведения в сети Интернет.

(Приложение 3).

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

Конкурс буклетов "Правила поведения в сети Интернет"

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

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

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

Очный этап конкурса предполагает публичную защиту буклета и ответы на вопросы одноклассников. По результатам данного этапа определяется победитель.

Проведение тематического классного часа

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

Задачи:

- 1) информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;
- 2) информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);
- 3) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

- 4) профилактика формирования у учащихся интернет-зависимости и игровой зависимости (игромании, гэмблинга);
5) предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий.

Ожидаемые результаты:

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

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

При организации классного часа важно исходить из возрастных особенностей учащихся, учесть уровень их знакомства с Интернетом. Организовать проведение классного часа необходимо таким образом, чтобы несовершеннолетние не только получили необходимый минимум знаний об информационной безопасности, но смогли *высказать свою точку зрения на указанную проблему*.

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

- необходимость деятельностного подхода в учебной работе учащихся в активном и интерактивном режиме;
- целесообразность использования методик учебного сотрудничества, различных вариантов работы в группах, кооперации, моделирования жизненных ситуаций.

Образовательные технологии № п/п
1

Виды учебной работы
Лекция

Образовательные технологии
Проблемное обучение,

2	Практические занятия	<i>визуализация Деловая игра, разбор конкретных ситуаций, практическая работа, технология развития критического мышления, технология Дебаты, авторская мастерская</i>
3	Реферат, проектирование	<i>Проектная деятельность, исследова тельская работа.</i>

Список используемой литературы Г.У.Солдатов, Е.И.Рассказова. Из-за интернета я не ел и не спал». Зависимость или новый образ жизни?

//Журнал «дети в информационном пространстве - М., 2011, №9 – СС. 22-29

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

3. Интернет-ресурсы:

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

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

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

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

<http://www.interneshka.net>

<http://www.saferinternet.ru>

<http://content-filtering.ru>

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

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

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

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

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

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

Приложение 1.

Анкета №1 Осторожно, вирус!

Что является основным каналом распространения компьютерных вирусов?

1. Веб-страницы
2. Электронная почта
3. Флеш-накопители (флешки)

Для предотвращения заражения компьютера вирусами следует:

1. Не пользоваться Интернетом
2. Устанавливать и обновлять антивирусные средства
3. Не чихать и не кашлять рядом с компьютером

Если вирус обнаружен, следует:

1. Удалить его и предотвратить дальнейшее заражение
2. Установить какую разновидность имеет вирус
3. Выяснить как он попал на компьютер

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

1. Применение брандмауэра

2. Обновления операционной системы
3. Антивирусная программа

Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?

1. Уничтожение компьютерных вирусов
2. Создание и распространение компьютерных вирусов и вредоносных программ.
3. Установка программного обеспечения для защиты компьютера.

Приложение 2.

Анкета №2 Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?

1. Свои увлечения
2. Свой псевдоним
3. Домашний адрес

2. Чем опасны социальные сети?

1. Личная информация может быть использована кем угодно в разных целях
2. При просмотре неопознанных ссылок компьютер может быть взломан
3. Все вышеперечисленное верно

3. Виртуальный собеседник предлагает встретиться, как следует поступить?

1. Посоветоваться с родителями и ничего не предпринимать без их согласия.
2. Пойти на встречу одному
3. Пригласить с собой друга

4. Что в Интернете запрещено законом?

1. Размещать информацию о себе
2. Размещать информацию других без их согласия
3. Копировать файлы для личного использования

5. Действуют ли правила этикета в Интернете?

1. Интернет - пространство свободное от правил
2. В особых случаях
3. Да, как и в реальной жизни.

Приложение 3.

Круглый стол Основы безопасности в сети Интернет

Правила работы в сети Интернет

1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. При общении в Интернет не указывать свои личные данные, а использовать псевдоним (ник).
7. Без контроля взрослых ни в коем случае не встречаться с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
9. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.
10. Не всей той информации, которая размещена в Интернете, можно верить.
11. Не оставляйте без присмотра компьютер с важными сведениям на экране.
12. Опасайтесь подглядывания через плечо.
13. Не сохраняйте важные сведения на общедоступном компьютере.

Приложение 4.

Материалы для проведения родительского собрания.

Анкета для родителей.

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

1. В каком классе учится Ваш ребенок? _____

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

3. Использование информационных технологии в школе

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

- урок, с применением новых информационных технологий более популярен у моего ребенка (более интересен, понятен и т.п. - со слов ребенка)

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

- ребенок готовится к уроку, используя компьютер (Интернет, полезные ссылки на сайте школы, рекомендуемые учителем сайты и т.п.)
- классный руководитель проводит родительские собрания с использованием компьютера

Другое: _____

4. Работа "Электронного журнала".

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

- в нашем классе есть "Электронный журнал", его работа очень важна для нас
- в нашем классе есть "Электронный журнал", но в его работе нет необходимости
- возможности "Электронного журнала" очень важные, но в нашем классе он не работает
- в нашем классе он не работает и думаю, что нет в нем необходимости.

Другое: _____

5. Посещение Школьного сайта

- часто посещаем (в том числе раздел Новости)
- очень редко посещаем
- не посещаем

Другое: _____

6. Школьный сайт.

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

7. Есть ли у Вас дома компьютер?

- да (один)
- да (несколько)
- нет

Другое: _____

8. Кто пользуется компьютером у Вас дома?

- только родители
- только ребенок
- все члены семьи (родители и дети)

Примерный список вопросов, которые планируется обсудить на родительском собрании

1. В каком возрасте следует разрешить детям посещение интернета?
2. Следует ли разрешать детям иметь собственные учетные записи электронной почты?
3. Какими внутрисемейными правилами следует руководствоваться при использовании интернета?
4. Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?
5. Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, Mail Agent)?
6. Могут ли дети стать интернет-зависимыми?
7. Что должны знать дети о компьютерных вирусах?
8. Как проследить какие сайты посещают дети в интернете?
9. Что следует предпринять, если моего ребенка преследуют в интернете?
10. Помогает ли фильтрующее программное обеспечение?

11. На какие положения политики конфиденциальности детского сайта нужно обращать внимание?
12. Какие угрозы встречаются наиболее часто?
13. Как научить детей отличать правду от лжи в Интернет?

Приложение 5.

Рекомендации для родителей (законных представителей) детей различных возрастных категорий.

Возраст от 7 до 8 лет

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

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

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

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

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

Советы по безопасности в сети Интернет

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

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

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

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

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

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

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

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

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

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

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

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

Подробнее о таких фильтрах

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

Не разрешайте детям использовать службы мгновенного обмена сообщениями.

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

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

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

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

Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст от 9 до 12 лет

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

Советы по безопасности в этом возрасте

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

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

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

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

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

Не забывайте беседовать с детьми об их друзьях в Интернет.

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

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

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

Приучите детей не загружать программы без вашего разрешения.

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

Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

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

Расскажите детям о порнографии в Интернет.

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

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

Приложение 8.

Примерные материалы итогового анкетирования обучающихся по теме "Безопасный Интернет"

1. Укажите свой возраст _____

2. Что такое Интернет? _____

3. Какие опасности существуют в Интернете? _____

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

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

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

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

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

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

б) стараться давать как можно меньше информации о себе

в) размещать фотографии свои, друзей и родственников

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

а) выключить и спрятать в шкаф

б) установить антивирусную программу

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

а) лучше не иметь антивирусную программу

б) обновлять антивирусную базу

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

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

а) чёрный властелин

б) хакеры

в) шпионы

г) пожиратели смерти

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

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

Приложение 9 Памятка для учащихся начальной школы *Контентные риски*

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

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

Электронные риски

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

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

Коммуникационные риски

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

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

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

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

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

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

Потребительские риски

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

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