Программа безопасности школьников в сети Интернет

Пояснительная записка

В связи с глобальным процессом активного формирования и использования информационных ресурсов особое значение приобретает информационная безопасность детей.

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. Использование Интернета в работе с детьми достаточно обширно: это использование электронной почты; поиск в сети нужной информации; создание собственных школьных веб-страниц; рассылка; обмен опытом; ответы на типичные вопросы; совместные проекты школьников (и учителей) разных школ.

Использование Интернета в образовательной деятельности таит в себе много опасностей. Бесконтрольный доступ к Интернету может привести к:

- Инернет – зависимости
- знакомству с человеком с недобрыми намерениями.
- заражению вредоносными программами при скачивании файлов,
- неправильному формированию нравственных ценностей
- нарушению нормального развития ребенка

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

Очень важно, чтобы во всех школах был безопасный Интернет. По статистическим данным на сегодняшний день в России насчитывается от 9 до11 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.

Просвещение подрастающего поколения в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и нормальному развитию.

Медиаобразование выполняет важную функцию защиты от противоправного воздействия средств массовой коммуникации, а также способствует предупреждению криминальных посягательств на детей с использованием информационно - телекоммуникационных сетей.

Принятый 29 декабря 2010 года Федеральный закон Российской Федерации № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" устанавливает правила медиа-безопасности детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно телекоммуникационных сетях и сетях подвижной радиотелефонной связи. Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

В обеспечении мер по Интернет-безопасности образовательное учреждение должно играть ключевую роль, так как в современной школе обучение проводится с использованием технологий, отвечающих своему времени, имеются в виду информационно-коммуникационные технологии. Поэтому школа должна взять на себя главную ответственность за развитие у детей и их родителей цифровой грамотности и обучение их навыкам безопасности.

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 наименее привилегированных и самых младших детей.

1. Цели и задачи программы.

Цель: Обеспечение безопасной информационной образовательной среды школы при обучении, внеурочной деятельности, а также в свободном использовании сети Интернет.

Задачи:

1. Организация технического контроля безопасности;
2. Формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;
3. Создание педагогических условий обеспечения информационной безопасности учащихся, использующих Интернет в образовании.
4. Изучение нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
5. Организация разъяснительной работы среди обучающихся и их родителей;

Участники и исполнители: учащиеся начальной школы 1-4кл, средней школы 5-9 классы, учителя - предметники, классные руководители, администрация, родители.

2. **Нормативно-правое обеспечение**

Федеральный уровень

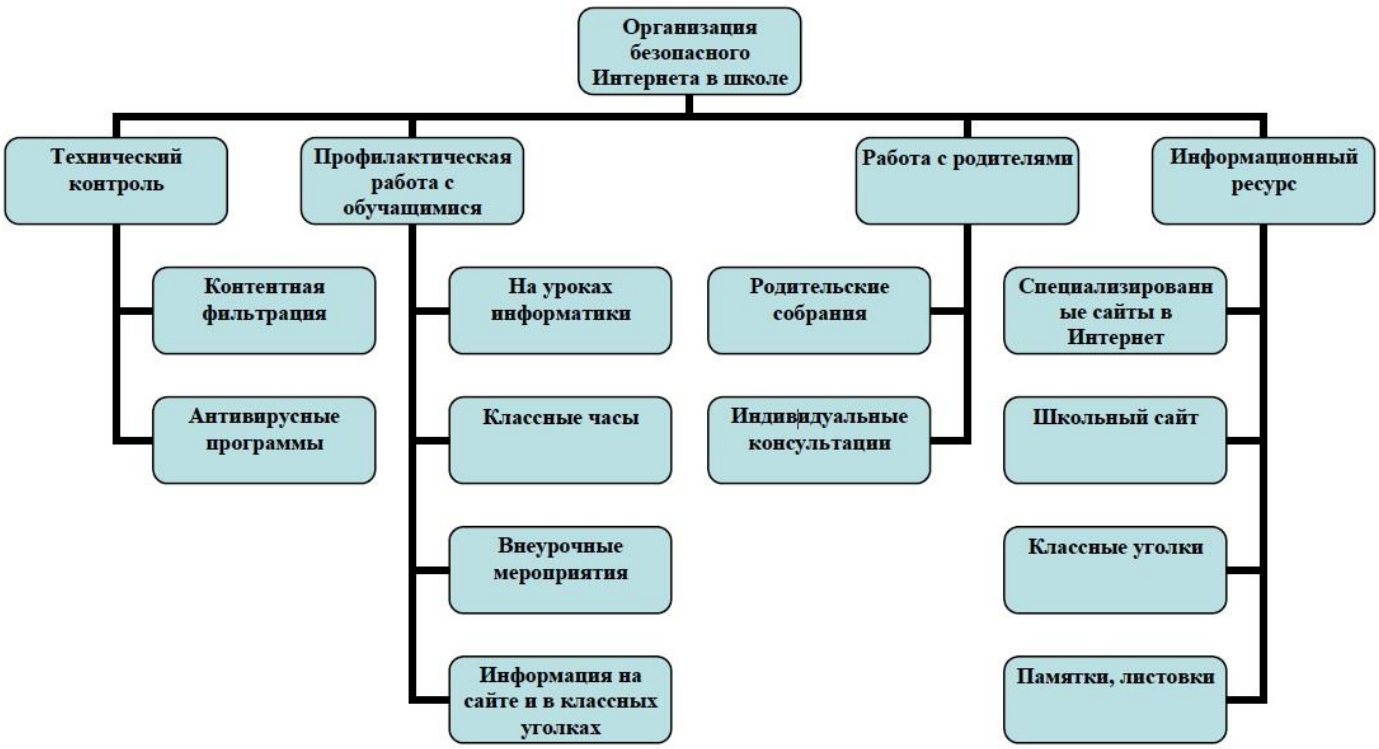
1. Закон «Об образовании» № 273 ФЗ от 29.12.2012
2. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
3. Постановление от 18 апреля 2012 г. N 343 «Об утверждении правил размещения в сети интернет и обновления информации об образовательном учреждении»
4. «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10;

Школьный уровень

1. Локальный акт «Правила использования сети Интернет»
2. РЕГЛАМЕНТ по работе учителей и школьников в сети Интернет
3. Инструкция для сотрудников о порядке действий при осуществлении контроля за использованием учащимися общеобразовательного учреждения сети Интернет.

3. Организация безопасного интернета в школе

Для решения вопросов безопасности Интернета в школе организован технический контроль, ведется профилактическая работа с обучающими и их родителями, доступны информационные ресурсы для всех участников образовательного процесса.



Технический контроль.

Чтобы ограничить доступ учащихся к информации, которая может оказать на них негативное воздействие, установлена специальная система фильтрации исключающая доступ к такой информации. Блокируется доступ к сайтам, содержащим материалы, которые определены как опасные. С помощью технологии фильтров и блокировки можно ограничить список собеседников, с которыми дети общаются через Интернет. Тем не менее, нет компьютерных программ, способных полностью защитить ребенка от доступа к нежелательной информации.

Антивирусная программа установлена на все компьютеры, также позволяет ограничить доступ юных пользователей Интернета к нежелательному контенту и обеспечить безопасность школьной компьютерной сети.

Профилактическая работа с детьми.

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. мероприятий, направленных на обучение учителей, родителей и детей правилам безопасного пользования Интернетом. Это классные часы по теме «Безопасность в сети Интернет»; листовки, буклеты, памятки для учащихся «Безопасность в Интернете» и т.д.

Профилактическая работа с родителями.

Формы работы с родителями различны – родительские собрания («Безопасный Интернет - детям»), 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.

Информационный ресурс.

Для достижения положительных результатов необходимо проводить комплексную работу семьи школы. Именно преподаватели и родители смогут предостеречь детей от возможных опасностей и ошибок. Существует ряд сайтов, посвященных безопасности детей в Интернете: www.detionline.org, www.interneshka.net, ресурсы которых оказывают огромную помощь, как взрослым, так и детям. Также информация для родителей и детей по безопасной работе в Интернет размещена на официальном сайте школы и в классных уголках.

Таким образом, в школе необходимо регулярно вести работу по формированию безопасной информационной образовательной среды школы, обеспечению информационной безопасности учащихся, использующих

Интернет в образовании, и пропаганде безопасного поведения в сети Интернет.

4. **Сроки реализации программы:** 2022-2026 уч.гг
5. **Этапы реализации программы**

1этап - организационный

1. разработка нормативно-правовой базы;
2. создание банка методических материалов;
3. разработка элективного курса;
4. анализ реальной ситуации по данной проблеме;
5. диагностика интересов и направлений занятости учащихся во внеурочное время;
6. составление плана реализации проекта;

2 этап – практический

1. организация и проведение воспитательных мероприятий (информационно-профилактических, творческих, исследовательских);
2. разработка рекомендаций педагогам, родителям и ученикам по профилактике компьютерной зависимости;
3. разработка памятки для учеников по использованию ресурсов сети Интернет;
4. текущий контроль за реализацией проекта.

4-й этап – обобщающий

1. обработка результатов мониторинга;
2. анализ результатов реализации проекта в соответствии с поставленными целью и задачами;
3. определение перспектив и путей дальнейшего развития.

6. Ожидаемые результаты

Системный подход в решении задач построения в школе безопасной среды для доступа к сети Интернет:

1. обеспечит потребность учителя в постоянном повышении уровня своей квалификации и профессионализма по данному вопросу;
2. поможет родителям грамотно организовать информационное пространство ребенка в семье;
3. совместные усилия педагогов и родителей создадут рабочую среду ребенка и в школе и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

7.Перспективы дальнейшей работы.

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. Задача взрослых (педагогов, родителей) - формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности.

План работы

№	Сроки проведения	Мероприятие	Ответственные
1	Сентябрь	1. Изучение нормативных документов по организации безопасного доступа к сети Интернет. Сбор документации.	Зам. директора по УВР
		2. Классный час по безопасной работы в сети Интернет для учащихся 1–9 классов	Классные руководители
2	Октябрь	1.Производственнос совещание. Знакомство педагогов с нормативными документами и школьными локальными актами: 1. Локальный акт «Правила использования сети Интернет» 2. РЕГЛАМЕНТ по работе учителей и школьников в сети Интернет 3. Инструкция для сотрудников о порядке действий при осуществлении контроля за использованием учащимися общеобразовательного учреждения сети Интернет.	Учитель информатики
		3. Диагностика по выявлению наличия признаков компьютерной и игровой зависимости.	Классные руководители Психолог школы
3	Ноябрь	всероссийский общественный проект- **Линия помощи "Дети онлайн".**	Классные руководители
		2.НШ Правила безопасного использования сети Интернет для школьников младших классов http://azbez.com/node/1284	Кл.рук
		3.Школьные дебаты «Безопасный интернет»	Классные руководители, учителя информатики
		4.Создание странички на школьном сайте «Компьютерная зависимость».	Учитель информатики
4	Декабрь	Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях	Кл.руководители
5	Январь	Родительский всеобуч «Положительные и отрицательные стороны Интернета»	Классные руководители
6	Февраль	1.Конкурс рисунков «Я выбираю ….»	Учитель ИЗО Шаповалова И.Н.
7	Март	НШ Флеш – игра «Необычайные приключения в интернете» http://detionline.com/mts/game	Родители
8	Апрель	Всероссийский чемпионат по онлайн-игре «Изучи Интернет — управляй им» Учащимся основной и старшей школы	Классные руководители, родители

		http://igra-internet.ru/	
9	Май	На уроках информатики провести беседы, диспуты: «Безопасность при работе в Интернете», «О личной безопасности в Интернет», «Сетевой этикет», «Этика сетевого общения » (7-8 классы), «Форумы и чаты в Интернет», «Информационная безопасность сетевой технологии работы» (9 классы).	Классные руководители,
10	В течение года	Индивидуальная работа с группой риска (интернет-зависимых и «игроманов»)	Классные руководители, психолог

Приложения

Правила работы в сети Интернет и мобильных сетях связи для детей и родителей

Компьютер в наше время стал для ребенка и другом и помощником и даже воспитателем, учителем. Между тем, существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, нарушение психики неустойчивых школьников, представляющих для детей угрозу.

Преодолеть нежелательное воздействие информационной среды можно 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.

Следует понимать, что подключаясь к сети Интернет, Ваш ребенок встречается и целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны, прежде всего, родители перед тем, как разрешить ему выход в сеть Интернет.

Наиболее частые угрозы в сети:

1. **Угроза заражения вредоносным Программным обеспечением (ПО)**. Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить почту, компакт-диски и прочие сменные носители информации или скачанные из сети Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня стало простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов.

2. **Доступ к нежелательному содержимому.** Сегодня любой ребенок, выходящий в сеть Интернет, может просматривать любые материалы. К таким материалам относится насилие, наркотики, порнография, страницы с националистической или откровенно фашистской идеологией и многое другое.

3. **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.

4. **Интернет-магазины**. Несмотря на то, что покупки через сеть Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Рекомендации по уменьшению опасности от посещений детьми Интернет.

1. Посещайте сеть Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения сети Интернет;

2. Объясните детям, что если в сети Интернет что–либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;

3. 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.;

4. Научите ваших детей уважать собеседников в сети Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково и в Интернет, и в реальной жизни;

5. Объясните детям, что далеко не все, что они могут прочесть или увидеть в сети Интернет - правда. Приучите их спрашивать о том, в чем они не уверены;

6. Не забывайте контролировать детей в сети Интернет с помощью специального программного

обеспечения. Это поможет вам отфильтровать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

Домашний контроль работы сети

Родителям необходимо постоянно вести разъяснительную работу, т.к. без понимания данной проблемы невозможно ее устранить силами только учителей. Очень часто родители не понимают или недооценивают те угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, тому, как вести себя с незнакомыми людьми, что можно говорить о себе, а что нет, между тем, «выпуская» его в сеть Интернет, не представляют себе, что точно так же нужно обучить его основам безопасности в сети Интернет.

Ребенок абсолютно беззащитен перед потоком информации. Дома необходимо выработать общие правила, которые бы сводились к следующему:

- Какие сайты могут посещать дети и что они могут там делать;
- Сколько времени дети могут проводить в сети Интернет;
- Как защитить личные данные;
- Как следить за безопасностью;
- Как вести себя вежливо;
- Как пользоваться чатами, группами новостей, службами мгновенных сообщений.

Следите за выполнением данных правил и рекомендаций!!!

Регулярно, по мере необходимости, вносите изменения в них!

г.

ПРАВИЛА
использования сети Интернет

1. Общие положения.

1.1. Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящие Правила регулируют условия и порядок использования сети Интернет в учреждении.

1.3. Настоящие Правила имеют статус локального нормативного акта учреждения.

2. Организация использования сети Интернет в учреждении.

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете школы. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводится в действие приказом директора школы.

2.2. Правила использования сети Интернет разрабатывается педагогическим советом школы на основе примерного регламента самостоятельно либо с привлечением внешних экспертов, в качестве которых могут выступать:

— преподаватели других образовательных учреждений, имеющие опыт использования Интернета в образовательном процессе;
— специалисты в области информационных технологий;
— представители органов управления образованием;
— родители обучающихся.

2.3. При разработке Правил использования сети Интернет педагогический совет руководствуется:

— законодательством Российской Федерации;
— опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;
— интересами обучающихся;
— целями образовательного процесса;
— рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети.

2.4. **Руководитель учреждения** отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в учреждении, а также за выполнение установленных правил. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с установленными в учреждении правилами директор школы назначает своим приказом ответственного за организацию работы Точки доступа к Интернету и ограничение доступа.

2.5. **Педагогический совет:**

— принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;
— определяет характер и объем информации, публикуемой на интернет-ресурсах учреждения;

— дает руководителю учреждения рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за работу Точки доступа к Интернету, за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети.

2.6. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий занятие.

Преподаватель:

— наблюдает за использованием компьютера и сети Интернет обучающимися;

— принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.7. Во время свободного доступа обучающихся и сотрудников к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляет ответственный за работу Точки доступа к Интернету.

Работник образовательного учреждения - ответственный за работу Точки доступа к Интернету:

— наблюдает за использованием компьютера и сети Интернет обучающимися и работниками учреждения;

— принимает меры по пресечению по пресечению обращений к ресурсам, не имеющих отношения к образовательному процессу;

— сообщает руководителю о преднамеренных попытках обучающегося или сотрудника осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу.

2.8. При использовании сети Интернет в учреждении обучающимся и сотрудникам предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в учреждении или предоставленного оператором услуг связи.

2.9. Пользователи сети Интернет в учреждении должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения пользователями ресурсов, не имеющих отношения к образовательному процессу и содержание которых противоречит законодательству Российской Федерации. Участникам использования сети Интернет в учреждении следует осознавать, что учреждение не несет ответственности за случайный доступ к подобной информации, размещенной не на интернет-ресурсах учреждения.

2.10. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в учреждении правилами обеспечивается работником учреждения, ответственным за работу Точки доступа к Интернету и назначенным его руководителем.

2.11. Принципы размещения информации на интернет-ресурсах учреждения призваны обеспечивать:

— соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;

— защиту персональных данных обучающихся, преподавателей и сотрудников;

— достоверность и корректность информации.

2.12. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах, создаваемых учреждении, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников учреждении размещаются на его интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.13. В информационных сообщениях о мероприятиях, размещенных на сайте учреждения без уведомления получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

2.14. При получении согласия на размещение персональных данных представитель учреждения обязан разъяснить возможные риски, последствия их опубликования. Учреждение не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в учреждении.

3.1. Использование сети Интернет в учреждении осуществляется, как правило, в целях образовательного процесса.

3.2. По разрешению лица, ответственного за организацию в учреждении работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе:

— размещать собственную информацию в сети Интернет на интернет-ресурсах учреждения;

— иметь учетную запись электронной почты на интернет-ресурсах учреждения.

3.3. Пользователям запрещается:

— обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

— осуществлять любые сделки через Интернет;

— осуществлять загрузки файлов на компьютер учреждении без специального разрешения;

— распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу локальной сети и ограничение доступа к информационным ресурсам.

Ответственный за работу Точки доступа к Интернету обязан:

— принять информацию от преподавателя;

— направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);
— в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

— доменный адрес ресурса;
— сообщение о тематике ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо его несовместимости с задачами образовательного процесса;
— дату и время обнаружения;
— информацию об установленных в учреждении технических средствах технического ограничения доступа к информации.

РЕГЛАМЕНТ

по работе учителей и школьников в сети Интернет

1. Общие положения

Настоящий регламент разработан в связи с широким применением информационных ресурсов сети Интернет в образовательном процессе.

Использование сети Интернет в образовательном учреждении (ОУ) должно быть направлено на решение задач учебно-воспитательного процесса. При организации доступа в сеть учителя сталкиваются с проблемами технического, организационного и педагогического характера. Регламент определяет порядок эффективного использования сети Интернет, ограничение доступа к ресурсам сети, не имеющим отношения к образовательному процессу, а также время работы в сети.

Выход в сеть должен быть обусловлен поставленной целью, так например: поиск информации; усиление мотивации в изучении учащимися образовательных дисциплин; подготовка к ОГЭ; тестирование; участие в Интернет-олимпиадах, конкурсах; подготовка к поступлению в учреждения профессионального образования; погружение в языковую среду; проведение исследовательской работы; дистанционное обучение и использование его элементов в образовательном процессе; повышение квалификации педагогов; отработка навыков, развитие коммуникационного (сетевого) общения; опубликование интересных авторских материалов педагогов и учащихся, обмен опытом; создание веб-страниц; создание мультимедиа презентаций; электронная отчетность; другое.

К работе в сети Интернет допускаются участники образовательного процесса, прошедшие предварительную регистрацию у лица, ответственного за доступ к сети по образовательному учреждению.

2. Организация использования сети Интернет в общеобразовательном учреждении

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете ОУ.

2.2. Регламентация доступа к информации сети Интернет определяется педагогическим советом на основании предложений педагогов о закрытии определенных сайтов. По решению педагогического совета может быть организован специальный совет ОУ по использованию сети Интернет.

2.3. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводятся в действие приказом руководителя ОУ.

Правила использования сети Интернет разрабатываются педагогическим или специализированным советом ОУ на основе настоящего регламента самостоятельно либо с привлечением внешних экспертов, в качестве которых могут выступать: преподаватели других образовательных учреждений, имеющие опыт использования Интернета в образовательном процессе; специалисты в области информационных технологий; представители органов управления образованием; родители обучающихся.

При разработке правил использования сети Интернет педагогический совет руководствуется:

- законодательством Российской Федерации;
- опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;

- интересами обучающихся;

- целями образовательного процесса;

- рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети.

2.4. Педагогический совет:

- принимает решение о блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;

- определяет характер и объем информации, публикуемой на Интернет-ресурсах ОУ;

- дает руководителю ОУ рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети.

2.5. Руководитель ОУ отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в ОУ, а также за выполнение установленных правил.

2.6. Для обеспечения доступа участников образовательного процесса к сети Интернет, в соответствии с установленным в ОУ правилами, руководитель ОУ назначает своим приказом ответственного за организацию работы с сетью Интернет и контроль безопасности работы в сети, а также вносит изменения в должностные инструкции работников, использующих ресурсы сети в образовательном процессе, в соответствии с рекомендациями (Приложение 1).

2.7. Во время уроков и других занятий в рамках образовательного процесса, а также во время свободного доступа обучающихся к сети Интернет вне учебных занятий контроль использования обучающимися информационной сети осуществляет преподаватель, ведущий занятие, или работники ОУ, определенные приказом его руководителя.

Преподаватель или работник ОУ:

- организует работу в сети;

- наблюдает за использованием компьютеров и сети Интернет обучающимися;

- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу;

- ведет записи в регистрационном журнале доступа к сети Интернет;

- сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу;

- в целях экономии трафика создает и ведет накопительную базу образовательных Интернет-ресурсов.

2.8. При использовании сети Интернет участникам образовательного процесса предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательному процессу. Ограничение доступа к ресурсам сети, несовместимым с задачами обучения и воспитания, осуществляется с помощью установки на компьютерах (сервере) специальных программ, запрещающих доступ к определенным сайтам, или использованием технических и программных средств контентной фильтрации, установленных в ОУ или предоставленных оператором услуг связи.

2.9. В связи с невозможностью техническими и программным средствами добиться полной фильтрации ресурсов сети Интернет вследствие их частого обновления, необходимо присутствие педагога или другого ответственного лица при работе

обучающихся в сети. ОУ не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах ОУ.

2.10. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в ОУ правилами обеспечивается работником ОУ, назначенным его руководителем.

В случае обнаружения ресурса, несовместимого с задачами обучения и воспитания несовершеннолетних, и/или нарушающего законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и розни, иные ресурсы схожей направленности), ответственный за организацию работы с сетью Интернет и контроль безопасности работы в сети должен незамедлительно, без согласования с педагогическим или специальным советом закрыть доступ к данному источнику.

2.11. Принципы размещения информации на Интернет-ресурсах ОУ призваны обеспечивать:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, преподавателей и сотрудников;
- достоверность и корректность информации.

2.11. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на Интернет-ресурсах, создаваемых ОУ, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников ОУ размещаются на его Интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.12. В информационных сообщениях о мероприятиях, размещенных на сайте ОУ без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

2.13. При получении согласия на размещение персональных данных представитель ОУ обязан разъяснить возможные риски и последствия их опубликования. ОУ не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в образовательном учреждении

3.1. Использование сети Интернет в ОУ осуществляется, как правило, в целях образовательного процесса.

3.2. По разрешению лица, ответственного за организацию в ОУ работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе размещать собственную информацию в сети Интернет на Интернет-ресурсах ОУ и иметь учетную запись электронной почты.

3.3. Работникам школы и обучающимся запрещается:

- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации;
- осуществлять любые сделки через Интернет;
- использовать сеть Интернет в коммерческих целях;

- осуществлять загрузки файлов на компьютер ОУ без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель должен зафиксировать доменный адрес ресурса и сообщить об этом лицу, ответственному за работу в сети Интернет.

Ответственный обязан:

- принять информацию от преподавателя и, в случае наличия технической возможности, внести указанный ресурс в число запрещенных, или направить информацию о некатегоризированном ресурсе оператору технических средств и программного и технического ограничения доступа к информации.

СИСТЕМА КЛАССИФИКАЦИИ ИНФОРМАЦИИ ЗАПРЕЩЕННОГО ДОСТУПА

1. Классификатор информации, запрещенной законодательством Российской Федерации

В соответствии с законодательством Российской Федерации общеобразовательное учреждение свободно в выборе и применении классификаторов информации, несовместимой с задачами образования и воспитания учащихся, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.

№ п / п	Наименование тематической категории	Содержание
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	- Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; - Информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение.
2	Злоупотребление свободой СМИ /экстремизм	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Злоупотребление свободой СМИ / наркотические средства	сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганду каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ / информация с ограниченным доступом	сведения о специальных средствах, технических приемах и тактике проведения контртеррористической операции
5	Злоупотребление свободой СМИ / скрытое воздействие	Информация содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	А) Экстремистские материалы, т.е. предназначенные для обнародования документы либо информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы; Б) экстремистская деятельность (экстремизм) включает в себя деятельность по распространению материалов

		(произведений), содержащих хотя бы один из следующих признаков: - насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; - подрыв безопасности Российской Федерации; захват или присвоение властных полномочий; создание незаконных вооруженных формирований; - осуществление террористической деятельности либо публичное оправдание терроризма; - возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; - унижение национального достоинства; осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; - пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; - воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, соединенное с насилием или угрозой его применения; - публичную клевету в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, соединенную с обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; - применение насилия в отношении представителя государственной власти либо на угрозу применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; - посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; - нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением.
7	Вредоносные программы	Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению

		работы ЭВМ, системы ЭВМ или их сети
8	Преступления	- Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); - Оскорбление (унижение чести и достоинства другого лица, выраженное в неприлично форме); - Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; - Склонение к потреблению наркотических средств и психотропных веществ; - незаконное распространение или рекламирование порнографических материалов; - публичные призывы к осуществлению экстремистской деятельности; - информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также пропаганду социального, расового, национального и религиозного неравенства; - публичные призывы к развязыванию агрессивной войны.
9	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную специально охраняемую законом тайну

2. Классификатор информации, несовместимой с задачами образования и воспитания

№ п / п	**Наименование тематической категории**	**Содержание**
1	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию.
2	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы.
3	Вождение и автомобили (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям.
4	Досуг и развлечения (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания информация в виде фотоальбомов и рейтингов фотографий, открыток, гороскопов, сонников, гаданий, магии, астрологии, ТВ-программ, прогнозов погоды, тестов, рейтингов, фотоконкурсов, конкурсов онлайн, несовместимая с задачами образования и воспитания

№ п / п	Наименование тематической категории	Содержание
		информация о туризме, путешествиях, тостах, поздравлениях, кроссвордах, сканвордах, ответов к ним, фэнтези и фантастике, кулинарии, рецептах, диетах, моде, одежде, обуви, модных аксессуарах, показах мод, текстах песен, кино, киноактерах, расписаниях концертов, спектаклей, кинофильмов, заказе билетов в театры, кино и т.п., дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними, рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании, службах знакомств, размещении объявлений онлайн, анекдотах, приколах, слухах, сайтах и журналы для женщин и для мужчин, желтая пресса, онлайн-ТВ, онлайн радио, знаменитости, косметика, парфюмерия, прически, ювелирные украшения.
5	Здоровье и медицина (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иных материалах по теме "Здоровье и медицина", которые, являясь академическими, по сути, могут быть также отнесены к другим категориям, например, порнография, трупы и т.п.
6	Компьютерные игры (ресурсы данной категории, несовместимые с задачами образования)	Несовместимая с задачами образования и воспитания компьютерные онлайновые и оффлайновые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты.
7	Корпоративные сайты, Интернет - представительства негосударственных учреждений (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания информацию сайты коммерческих фирм, компаний, предприятий, организаций.
8	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги.
9	Отправка SMS с использованием	Сайты, предлагающие услуги по отправке SMS-сообщений

№ п / п	Наименование тематической категории	Содержание
	Интернет-ресурсов	
10	Модерируемые доски объявлений (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания информацию модерируемые доски сообщений/объявлений, а также модерируемые чаты.
11	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и проч.
12	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека.
13	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники.
14	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам. Peer - to- Peer программы, сервисы бесплатных прокси - серверов, сервисы, дающие пользователю анонимность
15	Онлайн - казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и проч.
16	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц.
17	Поиск работы, резюме, вакансии (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания Интернет-представительства кадровых агентств, банки вакансий и резюме.
18	Поисковые системы (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания Интернет-каталоги, системы поиска и навигации в Интернете.
19	Религии и атеизм (ресурсы данной категории, несовместимые с задачами образования)	Сайты, содержащие несовместимую с задачами образования и воспитания информацию религиозной и антирелигиозной направленности
20	Системы поиска изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию.
21	СМИ (ресурсы данной	Содержащие несовместимую с задачами образования и воспитания информацию новостные ресурсы и сайты

№ п / п	Наименование тематической категории	Содержание
	категории, несовместимые с задачами образования)	СМИ (радио, телевидения, печати)
22	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака. Реклама табака и изделий из него.
23	Торговля и реклама (ресурсы данной категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания информацию сайты следующих категорий: аукционы, распродажи онлайн, Интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете.
24	Убийства, насилие	Сайты, содержащие описания или изображения убийств, мертвых тел, насилия и т. п.
25	Чаты (ресурсы данной категории, несовместимые с задачами образования)	Несовместимые с задачами образования и воспитания сайты для анонимного общения в режиме онлайн.

Инструкция

для сотрудников общеобразовательных учреждений

о порядке действий при осуществлении контроля за использованием учащимися сети Интернет

1. Настоящая Инструкция устанавливает порядок действий при обнаружении сотрудниками общеобразовательных учреждений и членами общественных советов учреждений:

1. возможности доступа учащихся к потенциально опасному контенту;
2. вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для учащихся, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, региональном уровне, муниципальном уровне, а также на уровне общеобразовательного учреждения.

2. Контроль за использованием учащимися сети Интернет осуществляют:

1. во время проведения занятий – учитель, проводящий занятие или специально уполномоченный руководителем учреждения на осуществление такого контроля;
2. во время использования сети Интернет для свободной работы учащихся - лицо, уполномоченное общеобразовательного учреждения по вопросам регламентации доступа к информации в Интернете или руководителем общеобразовательного учреждения в установленном советом порядке.

3. Лицо, осуществляющее контроль за использованием учащимися сети Интернет:

- определяет время и место работы учащихся в сети Интернет с учетом использования соответствующих технических возможностей в образовательном процессе, а также длительность сеанса работы одного учащегося;
- способствует осуществлению контроля за объемом трафика образовательного учреждения в сети Интернет;
- наблюдает за использованием компьютеров и сети Интернет учащимися;
- запрещает дальнейшую работу учащегося в сети Интернет в случае нарушения учащимся порядка использования сети Интернет и предъявляемых к учащимся требований при работе в сети Интернет;
- не допускает учащегося к работе в Интернете в предусмотренных Правилами использования сети Интернет случаях;
- принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсам, несовместимых с задачами образования.

4. При обнаружении информации, в отношении которой у лица, осуществляющего контроль за использованием учащимися сети Интернет, возникают основания предполагать, что такая информация относится к числу запрещенной для распространения в соответствии с законодательством РФ или иному потенциально опасному для учащихся

контенту, ответственное лицо направляет соответствующую информацию руководителю общеобразовательного учреждения и в общественный совет учреждения, которые принимают необходимые решения.

5. При обнаружении вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для учащихся, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, региональном уровне, муниципальном уровне, а также на уровне общеобразовательного учреждения, ответственное лицо направляет соответствующую информацию по специальной «горячей линии» для принятия соответствующих мер по восстановлению доступа к разрешенному контенту.

Линия помощи "Дети онлайн"

1 февраля 2010 года в рамках Года Безопасного Интернета в России запущен всероссийский общественный проект- Линия помощи "Дети онлайн".

Телефон Линии помощи: 8-800-25-000-15.

Организаторы проекта - Фонд "Дружественный Рунет" и Фонд Развития Интернет. Интерактивная Линия помощи "Дети онлайн" начала работу в тестовом режиме **15 декабря 2009 года**.
На Линии помощи "Дети онлайн" работают профессиональные эксперты - психологи Фонда Развития Интернет и технические специалисты. Работа ведется при методической поддержке Московского Государственного Университета имени М.В. Ломоносова, Федерального института развития образования МОН РФ и Московского Государственного Технического Университета им. Баумана.

Основные функции Линии помощи:

• Оказание психологической и практической помощи детям и подросткам, которые столкнулись с опасностью или негативной ситуацией во время пользования интернетом или мобильной связью (виртуальное преследование, домогательство, грубость, шантаж, мошенничество, несанкционированный доступ к ПК, нежелательный контент и т.д.).

• Консультирование родителей и педагогов по теме безопасного использования интернета и мобильной связи детьми.

Линия "Дети онлайн" будет способствовать развитию навыков безопасного использования Интернета у детей, родителей и педагогов и станет каналом получения информации о распространенности, динамике современных инфокоммуникационных угроз и эффективности мероприятий в области безопасного использования информационных коммуникаций.

Линия помощи "Дети онлайн" адресована трем целевым группам на территории России:

• несовершеннолетним пользователям (до 18 лет) Интернет и мобильной связи;

• их родителям;

• педагогам и работникам образовательных и воспитательных учреждений.

Прием звонков осуществляется по телефону: **8-800-25-000-15** (звонок по России бесплатный) по рабочим дням , прием электронных сообщений - по адресу: helpline@detionline.org
Официальный сайт Линии помощи "Дети онлайн": www.detionline.org.

7 советов по компьютерной безопасности для учащихся

Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, программ-шпионов и других возможных атак.

1. Соблюдайте основные меры компьютерной безопасности

Перед тем, как отправиться в путешествие по интернету, необходимо выполнить три важных действия для усиления компьютерной защиты.

1. **Активизации брандмауэра**
2. **Обновления антивирусных программ**
3. **Обновления программного обеспечения**

2. Не открывайте файлы, полученные от неизвестных корреспондентов

Электронная почта и мгновенные сообщения позволяют быстро обменяться информацией с друзьями, родственниками и одноклассниками. Но если не проявить необходимой осторожности, электронная почта и мгновенные сообщения могут распространить вирусы и черви. Основная масса вредоносных программ попадает в компьютер через электронную почту теми, кто нечаянно попытался открыть зараженный файл. Не дайте себя одурачить! Ни в коем случае нельзя открывать файл, вложенный в письмо электронной почты или мгновенное сообщение, если его отправитель неизвестен и вы не ожидаете получения файла. Дополнительные сведения, которые помогут защититься от вирусов и червей, можно найти в разделе Как защититься от вирусов. Советы по безопасному использованию служб мгновенных сообщений можно получить в разделе Советы по безопасности мгновенного обмена сообщениями и защите личной информации.

3. Как бороться со спамом и сетевыми мошенниками

Нужно также освоить способы борьбы со спамом и сетевым мошенничеством. Чтобы узнать, как освободить время для школьных дел и развлечений, избавившись от необходимости удалять спам, прочитайте разделы Как предотвратить получение спама по электронной почте и Пять запрещенных и три необходимых действия, позволяющих справиться со спамом в электронной почте.

Мошенничество phishing представляет собой еще одну угрозу конфиденциальности ваших данных. У вас могут украсть номер кредитной карты, пароли, учетную информацию или другие личные данные. Для ознакомления со способами защиты обратитесь к разделу Мошеннические письма: пять способов защиты личных данных.

4. Как защититься от программ-шпионов

Ваш браузер погряз во всплывающих окнах? На экране компьютера появились панели, которые вы не загружали? Возможно, вы стали жертвой программы-шпиона. Она занимается сбором вашей личной информации, не предупреждая об этом и не спрашивая на то разрешения. Получить эту вредоносную программу можно при скачивании музыки или программ обмена файлами; загрузки бесплатных игр с подозрительных сайтов или других программ. Чтобы ознакомиться с признаками программ-шпионов и узнать, как избежать заражения компьютера, прочитайте раздел Что из себя представляет программа-шпион?

5. Принимайте необходимые меры предосторожности, пользуясь беспроводной связью

В настоящее время многие высшие учебные заведения и колледжи оснащены беспроводными сетями. Это дает возможность путешествовать по интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях или даже общественных парках. Такие сети очень удобны, но их использование сопряжено со снижением уровня

безопасности. Если вы устанавливаете беспроводную сеть дома, прочитайте раздел Защита домашней сети и обратите особое внимание на информацию о безопасности. Прочитайте также раздел Безопасное использование беспроводных сетей общего пользования, чтобы получить три дополнительных совета по безопасности WiFi-соединений.

6. Пароль защищает ваш компьютер и блокирует возможность его использования

Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате. Если вы не пользуетесь паролем для входа в компьютер, кто угодно может получить доступ. Прямо сейчас, не откладывая в долгий ящик, воспользуйтесь нашими рекомендациями по созданию надежных паролей и всегда блокируйте доступ к компьютерной системе на то время, когда вы с ней не работаете. (Чтобы «запереть» компьютер с операционной системой Windows, удерживайте нажатыми клавиши «Windows + L». Когда понадобится возобновить работу, следуйте инструкциям на экране)

7. Делайте резервные копии результатов работы (а также игр и других развлекательных программ)

Образ студента, оставшегося без своей курсовой работы из-за того, что он забыл сделать резервную копию, стал уже почти штампом. Тем не менее многие до сих пор не находят времени на копирование. Пользователи Windows XP, могут воспользоваться программой Архивация данных, которая выполнит за вас эту работу. О том, как ею пользоваться, читайте в разделе удобное копирование с помощью Архивации данных Windows XP.

Как выбрать файлы для резервного копирования и найти место для их хранения, читайте в разделе Основы архивации данных: Приступая к работе.

Источник: http://www.microsoft.com/

Шкала Интернет-зависимости Анастасии Жичкиной

Инструкция: Выберите, пожалуйста, один из двух вариантов ответов (А или Б) тот, который лучше всего подходит для описания вашего поведения в Интернете и отметьте его галочкой. В этой анкете нет правильных или неправильных ответов, нам важно знать именно Ваше мнение.

1. А. Когда мне грустно или одиноко, я обычно выхожу в Интернет.
1. Б. Я не чувствую необходимости выйти в Интернет тогда, когда у меня плохое настроение.

2. А. Когда я провожу в Интернете меньше времени, чем обычно, я чувствую себя подавленно.
2. Б. Мое эмоциональное состояние не зависит от того, сколько времени я провожу в Интернете.

3. А. Я чувствую, что мое увлечение Интернетом мешает моей учебе, работе или отношениям с людьми вне Интернета.
3. Б. Использование Интернета не мешает моим отношениям с людьми, учебе или работе.

4. А. Многие мои знакомые не знают, сколько времени я на самом деле провожу в Интернете.
4. Б. Большинство моих знакомых знает, сколько времени я провожу в Интернете.

5. А. Я часто пытаюсь уменьшить количество времени, которое я провожу в Интернете.
5. Б. Я не пытаюсь уменьшить количество времени, которое я провожу в Интернете.

6. А. Когда я не в Интернете, я часто думаю о том, что там происходит.
6. Б. Когда я не в Интернете, я редко думаю о нем.

7. А. Я предпочитаю общаться с людьми или искать информацию через Интернет, а не в реальной жизни.
7. Б. Я далеко не всегда прибегаю к помощи Интернета, когда мне нужно найти информацию или пообщаться.

Ключи
Интернет-зависимость – один из видов поведенческих зависимостей, который проявляется в навязчивом постоянном стремлении войти в Интернет и потере субъективного контроля за его использованием.
Выбор варианта «А» оценивается в 1 балл, выбор варианта «Б» – 0 баллов.
Склонными к Интернет-зависимости считаются испытуемые с баллами по шкале Интернет-зависимости 3 и выше, не склонными к Интернет-зависимости – с баллом 0 по этой шкале. Интернет-зависимыми в строгом смысле слова считаются те, кто набирает 6-7 баллов по этой шкале.

Тест на детскую Интернет-зависимость (С.А. Кулаков)

Ответы даются по пятибалльной шкале: 1 – очень редко, 2 – иногда, 3 – часто, 4 – очень часто, 5 - всегда

1. Как часто Ваш ребенок нарушает временные рамки, установленные вами для пользования сетью?
2. Как часто Ваш ребенок запускает свои обязанности по дому для того, чтобы провести больше времени в сети?
3. Как часто Ваш ребенок предпочитает проводить время в сети вместо того, чтобы провести его в кругу семьи?
4. Как часто Ваш ребенок формирует новые отношения с друзьями по сети?
5. Как часто Вы жалуетесь на количество времени, проводимые Вашим ребенком в сети?
6. Как часто учеба Вашего ребенка страдает из-за количества времени, проведенном Вашим ребенком в сети?
7. Как часто Ваш ребенок проверяет электронную почту, прежде чем заняться чем-то другим?
8. Как часто Ваш ребенок предпочитает общение в сети общению с окружающими?
9. Как часто Ваш ребенок сопротивляется или секретничает при вопросе о том, что он делает в Интернете?
10. Как часто Вы заставали своего ребенка пробивающимся в сеть против Вашей воли?
11. Как часто Ваш ребенок проводит время в своей комнате, играя за компьютером?
12. Как часто Ваш ребенок получает странные звонки от его новых сетевых «друзей»?
13. Как часто Ваш ребенок огрызается, кричит или действует раздраженно, если его побеспокоили по поводу пребывания в сети?
14. Как часто Ваш ребенок выглядит более уставшим и утомленным, чем в то время, когда у Вас не было Интернета?
15. Как часто Ваш ребенок выглядит погруженным в мысли о возвращении в сеть, когда он находится вне сети?
16. Как часто Ваш ребенок ругается и гневается, когда Вы сердитесь по поводу времени, проведенного им в сети?
17. Как часто Ваш ребенок предпочитает своим прежним любимым занятиям, хобби, интересам других нахождение в сети?
18. Как часто Ваш ребенок злится и становится агрессивным, когда Вы накладываете ограничение на время, которое он проводит в сети?
19. Как часто Ваш ребенок предпочитает вместо прогулок с друзьями проводить время в сети?
20. Как часто Вы чувствуете подавленность, упадок настроения, нервничает, когда находится вне сети, а по возвращении в сеть все это исчезает?

При сумме баллов 50-79 родителям необходимо учитывать серьезное влияние Интернета на жизнь вашего ребенка и всей семьи.
При сумме баллов 80 и выше, у ребенка с высокой долей вероятности Интернет-зависимость и ему необходима помощь специалиста.

Родительское собрание на тему "Безопасность детей в сети Интернет"

Цель: просвещение родителей по теме “Безопасность детей в сети Интернет”.

Подготовительные мероприятия:
- анкетирование учащихся по теме собрания;
- подготовка буклета для родителей по теме собрания.

Ход родительского собрания

I. Мотивация к деятельности. Тренинг.

Родители рассаживаются по кругу лицом друг к другу, передавая из рук в руки приятный на ощупь мягкий мячик, высказывают свою точку зрения и аргументы по предлагаемому вопросу. Первый вопрос – мячик передают по часовой стрелке, второй вопрос - мячик передают против часовой стрелки и т.д.

Вопросы.

1. Чем является компьютер в вашей семье? Приведите примеры ситуаций из вашей жизни, связанных с положительными и отрицательными эмоциями по поводу ис-пользования компьютера.
2. Что сделаем, чтобы не повторять ежедневно: “Ты опять весь день просидел (а) за компьютером”?
3. Какую пользу извлекает Ваш ребенок при использовании сети Интернет?
4. Какие опасности ждут Вашего ребенка в сети Интернет?

II. Анализ, обсуждение ситуаций и разработка рекомендаций.

Еще недавно компьютеры были скорее роскошью, но уже сейчас являются чуть ли не “предметом первой необходимости”.

Результаты анкетирования детей класса показали, что:

• 100 % детей имеют дома компьютер

• В среднем ежедневно дети проводят за ним по 4 часа в день

• Из видов деятельности, преобладающих в общении с компьютером, дети на первое место поставили – компьютерные игры. 96% из них каждый день играют в компьютерные игры, причем 51% может начать играть, даже не пообедав.

• На втором месте – общение в Сети. 70% пользуются Интернетом – из них 100% общаются в социальных сетях, 63% - играют в сетевые онлайн игры.

• Далее дети выбирают прослушивание музыки, рисование, печать документов соответственно 46%, 135 и 1%

• 38% -при определении рейтинга использования свободного времени на I место поставили компьютер, исключив при этом занятия спортом, прогулки на воздухе, общение с семьёй.

Сегодня мы с вами остановимся на особенно важной проблеме современных школьников – зависимости от сети Интернет.

Зависимость в медицинском смысле определяется как навязчивая потребность в приеме привычного вещества, сопровождающаяся ростом толерантности и выраженными симптомами. Рост толерантности означает привыкание ко всё большим и большим дозам.

Интернет-зависимость – это навязчивая потребность в использовании Интернета.

Существует 5 типов Интернет-зависимости:
• бесконечный веб-серфинг — постоянные «путешествия» по Интернету с целью по-иска информации.
• пристрастие к виртуальному общению и виртуальным знакомствам, характе-ризуется большими объёмами переписки, постоянным участием в ча-тах, форумах, избыточностью знакомых и друзей из Интернета.
• игровая зависимость — навязчивое увлечение сетевыми играми.
• навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах.
• киберсексуальная зависимость — навязчивое влечение к посеще-нию порносайтов.

Интернет-зависимость характеризуется сильным желанием ребенка быть в сети, что приводит к нежеланию проводить время с семьей и друзьями, спать, посещать и делать уроки. Ребенок может перестать следить за своим внешним видом, начинает болезненно реагировать на просьбы отвлечься от компьютера, терять контроль за своим временем, лгать, причем уход от реальности может усиливаться день ото дня.

Родители должны уметь распознать признаки надвигающейся зависимости, прежде чем она станет реальной проблемой. Но это легче сказать, чем сделать.
Зависимость от Интернета все чаще называют чумой XXI века. В отличие от сигарет или наркотиков запретить Интернет нельзя – глобальная Сеть прочно вошла в нашу жизнь. Интернет – необходимый инструмент, которым ребенку в новом тысячелетии предстоит пользоваться постоянно.

Младший подростковый возраст — время быстрых изменений в жизни. Хотя дети все еще сильно зависят от своих родителей, они уже хотят некоторой свободы. Ребята начинают интересоваться окружающим миром, и отношения с друзьями становятся для них по-настоящему важными.
Дети этого возраста используют Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайновые игры и заходят на фанатские сайты своих кумиров. Их любимый способ общения — мгновен-ный обмен сообщениями.

Данные, показывают, что дети начинают пользоваться Интернетом в самом раннем возрасте, и роль, которую Глобальная сеть играет в жизнях подростков, значительна.
• Дети опережают взрослых по количеству времени, которое они проводят в Интернете. В возрасте между 8 и 13 годами дети составляют половину общего числа пользователей Интернета
• Более 90% подростков 8-16 лет сталкивались с порнографией в сети
• 44 % детей, регулярно использующих Интернет, хоть один раз подвергались сексуальным домогательствам при виртуальном общении, 11 % подверглись этому несколько раз.
• 14.5 % детей назначали встречи с незнакомцами через Интернет. 10 % из них ходили на встречи в одиночку, а 7 % никому не сообщили, что с кем-то встречают-ся.
• 38% детей просматривают страницы о насилии
• 16% детей просматривают страницы с расистским содержимым
• Согласно исследованию, проведенному в 2006 году в Польше, почти 1/3 родителей (28,4%) не осознает опасностей, с которыми могут встретиться их дети в Интер-нете
Сегодня мы с вами вместе попробуем разобраться в том, какие опасности ждут ребенка в сети и как его от них оградить.

Основные угрозы для детей в сети Интернет

1. Системы мгновенного обмена сообщениями

Системы обмена мгновенными сообщениями (например, MSN Messenger, Yahoo! Messsenger, Google Talk, ICQ…) стали широко используемым каналом общения для молодых людей. Это не могло остаться незамеченным со стороны кибер-преступников, которые быстро сделали его основным каналом для своей деятельности.
Одна из самых опасных угроз заключается в том, что преступники, используя данные программы, обманывают детей и подростков и представляются им другим человеком, чем они есть на самом деле.
В этих программах пользователи авторизуются с использованием адреса электронной почты и пароля. Например, если кто-то узнает данные другого пользователя и подключится к программе от его лица, то остальные люди, с которыми этот пользователь общается, будут думать, что они общаются именно с данным пользователем, хотя это не так. Если Вы обмениваетесь информацией или файлами с этим псевдо-пользователем, то преступник сможет легко ими завладеть. Именно по этой причине очень важно не распространять любую конфиденциальную информацию (персональные данные, фактический адрес проживания, банковские реквизиты и пр.) через подобные небезопасные каналы связи, как системы обмена мгновенными сообщениями.
Другая опасность состоит еще в том, что к подобным преступлениям часто прибегают педофилы. Их задача – собрать сведения о детях и подростках, а затем договориться с ними о реальной встрече или заставить их пойти на встречу. Педофилы зачастую представляются другими молодыми людьми, профессиональными фотографами или т.п.
Образование – это самый лучший способ защитить детей от подобного рода угроз. Посоветуйте им не общаться с незнакомцами, причем не только в онлайне, но и в обычном мире. Дети должны обладать достаточной уверенностью, чтобы быть способными открыто обсуждать с родителями или учителями свои проблемы.
Другой потенциальный риск в обмене мгновенными сообщениями – это инфицирование вирусами и вредоносными кодами. Почти 60% червей (вредоносные коды, которые распространяют сами себя), обнаруженных антивирусной лабораторией PandaLabs на протяжении первого полугодия, были созданы для распространения через системы обмена мгновенными сообщениями. Некоторые из них созданы для кражи паролей к онлайн-банкам. В этом случае в большей степени рискуют сами родители, потому что будут украдены их банковские данные, и, следовательно, могут пропасть их деньги.
Существуют простые способы, которые могут быть полезны для предотвращения случаев проникновения вредоносных кодов на компьютеры через системы обмена мгновенными сообщениями: не открывайте файлы и не нажимайте на ссылки, которые Вы получили через эти системы. По крайней мере, не делайте этого, пока точно не убедитесь, что человек, который их Вам прислал, является именно тем, кем он себя называет.

2. Электронная почта

Электронная почта – это другой источник опасности для молодых ребят. В этом случае также существует несколько угроз:
• Во-первых, это спам. Очень часто данный тип нежелательной почты используется для рекламы различных предложений: от казино до лекарств. Дети более подвер-жены доверять сообщениям, которые представлены в данных письмах, со всеми вытекающими отсюда последствиями. Они могут получить доступ к онлайн-казино и проиграть большую сумму денег, или они могут купить лекарства или даже нар-котики с большим риском для своего здоровья.
• Далее, существуют ложные предложения работы. Это не представляет серьезную

опасность для детей, но может являться таковой для подростков. Обычно эти со-общения содержат фантастические условия работы. Они обещают большие зарпла-ты без каких-либо усилий. Все, что в таких случаях необходимо, - это номер бан-ковского счета, куда будут перечисляться деньги, а затем, в обмен на комиссию, получателя попросят перевести эти средства на другой банковский счет. Это вы-глядит слишком хорошо, чтобы быть правдой, и любой здравомыслящий взрослый человек насторожиться от такого предложения. Однако молодые люди ищут легких денег. В результате этого они непроизвольно становятся соучастником преступле-ния, т.к. целью подобных финансовых переводов является «отмывание» преступ-ных денег.

• Другой риск связан с вирусами и вредоносными программами, которые могут по-пасть на компьютер. Как правило, они распространяются через сообщения в элек-тронной почте, которые имеют определенную тематику (реклама новых фильмов, эротические фотографии, скачивание игр и т.д.) и предлагают пользователям на-жать на ссылку или скачать файл, являющиеся причиной инфекции. Данная техни-ка известна как «социальная инженерия». Многие взрослые люди становятся жерт-вами данной техники, что уж говорить про детей, которые очень легко могут стать жертвами.

Лучший способ защитить детей и подростков от этих угроз – это научить их быть бди-тельными по отношению к письмам из неизвестных источников. Они должны знать, что большинство из написанного в этих письмах является ложью, и что они никогда не должны открывать файлы или нажимать на ссылки в письмах подобного рода.

3. Программы обмена файлами

Обмен файлами в P2P-сетях является еще одним из основных источников распростране-ния инфекций. Большинство вредоносных кодов (преимущественно, черви) копируются в папки с этими программами под заманчивыми именами (названия фильмов, программ и т.д.) для того, чтобы привлечь внимание других пользователей, которые захотят скачать эти файлы и запустить их на своих компьютерах.

По сути дела, это еще один вариант социальной инженерии: названия файлов могут быть умышленно созданы таким образом, чтобы привлечь именно детей и подростков, которые по незнанию скачают вредоносные программы на свои компьютеры.

Именно по этой причине детям следует знать, какие файлы они могут скачивать, а какие скачивать нельзя. Более того, очень хорошая идея – это проверять каждый скаченный файл с помощью решения безопасности до момента их первого открытия / запуска.

Если при запуске файла возникает ошибка или открывается диалоговое окно с вопросом о лицензии или предложением скачать дополнительный кодек, то подобные действия долж-ны сразу же Вас заставить быть бдительным, потому что, скорее всего, данный файл со-держит в себе вирусы или другое вредоносное программное обеспечение.

4. Социальные сети и блоги

Сайты социальных сетей (например, Facebook, MySpace, одноклассники, Вконтакте) широ-ко используются для распространения фотографий и видео, общения с людьми и пр., так же как и блоги. В обоих случаях необходимо создавать персональный профиль для то-го, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденци-альную информацию как имя, возраст и т.д.

Детям следует постоянно напоминать, что необязательно предоставлять эту информацию, а достаточно только указать адрес электронной почты и имя, которое может быть псевдо-нимом. Нельзя распространять такую информацию, как возраст, адрес проживания, а так-же свои фотографии и видео.

Многие подростки используют блоги в качестве своих персональных дневников. Как пра-вило, такие онлайн-журналы содержат значительно более широкую информацию, чем

следовало бы публиковать. Крайне важно предотвратить публикацию любых данных, которые могли бы идентифицировать пользователя как ребенка или подростка, а также содержать информацию о месте проживания, учебы и другую персональную конфиденциальную информацию.
Аналогично, в некоторых социальных сетях, например в MySpace, есть возможность обмениваться файлами с другими пользователями. Необходимо отдельно обратить внимание ребенка на то, какими файлами он может обмениваться с другими пользователями и кому он может разрешить просматривать эту информацию. Совсем не сложно, например, разместить свои фотографии, но защитить их паролем, который будет доступен только своим друзьям и семье.
Родителям следует знать об этих новых сервисах, а также о том, как они работают и какие риски они представляют для пользователей. Родители также должны быть способны проинструктировать своих детей о том, как использовать эти сервисы правильно и безопасно.

5. Мобильные телефоны с выходом в Интернет

Стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибер-атак за последние несколько лет. Исследование показало, что такие технологии как Bluetooth (позволяет обмениваться файлами между устройствами по беспроводному каналу) и высокоскоростной доступ в Интернет сделали сотовые телефоны очень уязвимыми для атак.
В настоящее время сотовые телефоны широко используются детьми и подростками. Соответственно, они сталкиваются с точно такими же рисками, как и при использовании ПК, подключенного к Интернету.
Во-первых, сейчас широко распространены системы обмена мгновенными сообщениями для сотовых телефонов. Дети могут войти в чаты в любой момент, при этом не важно, где они находятся физически, и столкнуться с теми рисками, о которых мы подробно говорили выше: кража персональных данных, педофилы, распространение вирусов и вредоносных программ и т.д.
Спам также начинает одолевать сотовые телефоны. За последние несколько лет SMS-сообщения с рекламой всех типов продуктов и сервисов наводнили сотовые телефоны во всем мире. Большая часть подобной рекламы – это реклама порнографии. Это означает, что дети могут столкнуться с подобной информацией не только при выходе в Интернет со своего компьютера, но и при использовании собственного мобильного телефона.
В результате, родители также должны контролировать то, как дети пользуются своими сотовыми телефонами. Поэтому мы рекомендуем родителям покупать своим детям сотовые телефоны без встроенных функций, которые могли бы подвергать их такому риску (подключение к Интернету, SMS, наличие Bluetooth и т.д.), а подросткам необходимо объяснять, как следует безопасно использовать свой сотовый телефон. Постоянно напоминайте им, чтобы они не отвечали на сообщения из подозрительных и неизвестных источников и не соглашались на встречу с незнакомцами.

Итак. вот **несколько рекомендаций общих психологов для профилактики Интернет-зависимости у детей:**
1. Ограничьте количество времени, которое дети могут проводить в Интернете. Убедитесь, что ребенок пользуется Сетью во время, отведенное домашнему заданию, для учебы, а не для развлечений. Вместе с ребенком составьте подробный план с указанием, на что тратится время, проводимое за компьютером. Это поможет со-кратить время на бездумное обновление странички одноклассников в ожидании нового сообщения, чтение новостей ради самого процесса чтения и т.д.
2. Не ставьте компьютер в комнате ребенка. Установите компьютер в гостиной или в своей комнате – там, где вы сможете легко контролировать то, что ваш ребенок де-лает в

Интернете. С помощью современных мобильных телефонов можно подклю-читься к Сети для общения, игр и просмотра сайтов. Неважно, с помощью какого устройства ребенок будет уходить в виртуальный мир. Важно не допустить, чтобы виртуальная реальность не стала для него домом.
3. Выясните, что ваш ребенок любит делать в Интернете. Некоторые онлайн-игры, в которых действие происходит в фантастических мирах с тысячами игроков по все-му миру, например, World of Warcraft, действительно увлекают. Известны случаи, когда взрослые люди достигали крайней степени истощения, не в силах оторваться от любимой игры, не говоря уже о таких «мелочах», как разводы, потеря работы и т.д. Кроме того, во многих играх, чтобы добиться успеха, нужно не только прово-дить в игре много часов в день, необходимо также вкладывать в своего персонажа реальные деньги, обменивая их на игровую валюту. Не получив денег на игру от родителей, ребенок может пойти на обман или воровство.
4. Не подавайте детям плохой пример. Не проводите слишком много времени у ком-пьютера, не берите с собой за город ноутбук или планшет. Активный отдых всей семьей поможет ребенку переключиться на реальную жизнь. Займите ребенка дру-гими вещами, настольными или спортивными играми. Найдите ему занятие по ду-ше. Тогда Интернет станет подспорьем в учебе, вспомогательным средством поис-ка информации и общения, а не способом ухода от реальности и бегства от про-блем.

Советы по безопасности, или Как Вы можете защитить своих детей
1. Создайте список домашних правил Интернета при участии детей.
2. Используйте программы по защите детей в сети.
Существует ряд программ, позволяющих защитить собственного ребенка от посещения, нежелательных сайтов.
Программа «Интернет-Цензор» – Интернет—фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов.
Хотите оградить ребенка от опасных и вредных сайтов? Используйте бесплатное про-граммное обеспечение «Интернет Цензор» - это быстро и очень просто!
Лучшее решение для защиты ребенка в Интернете! В основе работы Интернет Цензора лежит технология "белых списков", гарантирующая 100% защиту от опасных и нежела-тельных материалов. Программа содержит уникальные вручную проверенные "белые спи-ски", включающие все безопасные сайты Рунета и основные иностранные ресурсы. Про-грамма надежно защищена от взлома и обхода фильтрации.
Более подробную информацию о программе, возможность бесплатно скачать программу вы можете на странице http://www.icensor.ru/soft/
Родителям демонстрируется работа с данной программой, показывается, как можно добавить сайт в «белый» или «черный» список.
3. Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы вы говорили о чем-то другом.
4. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
5. Позволяйте детям заходить на детские сайты только с хорошей репутацией.
6. Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете.
7. Научите детей не загружать программы без вашего разрешения — они могут нена-рочно загрузить вирус или шпионскую программу.
8. Чтобы ребенок не мог заниматься чем-то посторонним без вашего ведома, создай-те для него учетную запись с ограниченными правами.
9. Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если

рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай повторится.
10. Расскажите детям о порнографии в Интернете и направьте их на хорошие сайты о здоровье и половой жизни.
11. Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами.
12. Расскажите детям об ответственном поведении в Интернете. Ребята ни в коем слу-чае не должны использовать Сеть для хулиганства, сплетен или угроз другим.

Если вы обеспокоены безопасностью ребенка при его работе в Интернете или при использовании мобильной связи;
Если ребенок подвергся опасности или стал жертвой сетевых преследователей и мошенников;
Обратитесь на линию помощи «Дети онлайн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и Интернет;
Позвоните по телефону 8−800−25−000−15 (звонок по России бесплатный, прием звонков осуществляется по рабочим дням с 9−00 до 18−00 мск).
Или направьте Ваше письмо по адресу: helpline@detionline.com
Подробнее о Линии помощи вы можете узнать на сайте http://detionline.com

И последний мой совет Вам – будьте внимательны к своим детям!

III. Рефлексия.
Предлагается обвести свою ладошку и на каждом пальце написать следующее:
• Большой палец – над эти я еще хотел (а) бы поработать
• Указательный палец – здесь мне были даны конкретные указания
• Средний палец – мне совсем не понравилось
• Безымянный палец – психологическая атмосфера
• Мизинец – мне здесь не хватило
Благодарю за внимание!

Список использованных ресурсов
1. Азбука безопасности. В Интернете http://azbez.com/safety/internet
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" http://www.fid.su/projects/saferinternet/year/actions/tvidi/
3. Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html
4. Безопасность детей в Интернете http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html
5. Копилочка активных методов обучения http://www.moi-universitet.ru/ebooks/kamo/kamo/
6. Материалы сайта «Интернешка» http://interneshka.net/

Источник: http://mm-festival.letitbit.net/download/51d17a051c92d018c4d07b6e888c62069/VVPyryeva_6.rar.html

Правила безопасного использования сети Интернет для школьников младших классов

Вы должны это знать:

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

Источник:http://www.friendlyrunet.ru/

АДРЕС

http://interneshka.net/

Памятка для обучающихся начальной школы

1. Всегда помни своѐ Интернет-королевское имя (e-mail, логин, пароли) и не кланяйся всем подряд (не регистрируйся везде без надобности)!

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

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

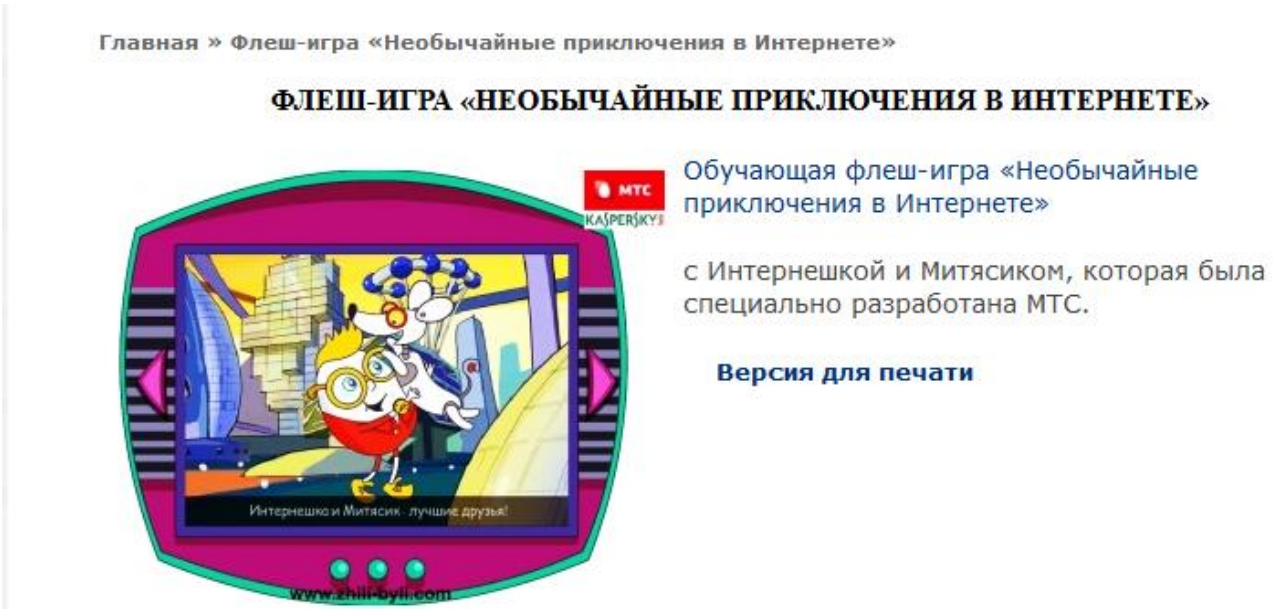
4. Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)!

5. Если хочешь дружить с другими царствами-государствами, изучай полезные социальные сервисы Web2.0: они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных – друзей званных!

6. Не забывай обновлять антивирусную программу – иначе вирус Серый Волк съест весь твой компьютер!

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

Адрес игры http://detionline.com/mts/game



Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях

Проблема сохранения персональных данных в Интернете встала особенно остро после увеличения случаев мошенничества, киберпреследования и запугивания пользователей. Получив личную информацию о жертве, злоумышленник с легкостью может испортить ей жизнь или даже подорвать материальное благосостояние. Поэтому крайне важно держать свои персональные данные в секрете, скрываясь под многочисленными никами, номерами и нейтральными учетными записями, чтобы избежать неприятностей. Однако в связи с желанием многих пользователей пользоваться социальными сетями и сайтами знакомств, скрывать всю информацию о себе не представляется возможным. Как иначе зарегистрироваться на «Одноклассниках», если не указывать имя, фамилию и учебные заведения? Как завести знакомство с девушкой/парнем на сайте, не опубликовав фотографию и способы связи? Никак.

К сожалению, приходится признать, что пользование социальными сетями вроде «одноклассников» и «вконтакте» является небезопасным – именно из-за этих самых «персональных данных». По ним, помимо старых друзей и знакомых, вас могут найти люди, знаться с которыми вы вовсе не жаждете. Избежать этого нельзя – выкладывая в Интернет информацию о себе, вы делаете ее доступной всем, а не только тем, для кого она предназначалась. Поэтому, регистрируясь на подобных ресурсах, нужно быть морально готовым к неприятным контактам, а не только поиску друзей детства. К числу «неприятных» относятся контакты с теми, кто навязчиво предлагает свое общество в киберпространстве (или наяву, найдя Вас по данным из соцсети) вопреки Вашему четко высказанному желанию.

И все-таки «утечки» личной информации можно избежать, даже пользуясь ресурсами, где указывать ее обязательно. Например, на сайтах, не являющихся социальными сетями и магазинами, вполне можно указать вместо настоящего имени-фамилии псевдоним, или, если это позволит интерфейс, вовсе оставить эти пункты анкеты пустыми. На сайтах знакомств можно указывать лишь электронные способы связи, например, специально выделенный для подобных контактов e-mail или номер аськи. Если же разговор по ним окажется удачным, ничто не мешает поделиться потом с собеседником «более реальными» электронными координатами, а то и телефоном или адресом. «Специальный» ящик нужен не только для защиты от возможного киберпреследования. Указывая адрес электронной почты в открытом доступе, вы рискуете попасть в базу данных спамеров и ежедневно получить массу ненужных и «завешивающих» ящик рассылок. Поэтому указывайте адрес, заранее зарегистрированный для общения на сайте, который не жалко потерять из-за потока спама. Иначе придется регистрировать новый личный ящик и сообщать его адрес всем старым контактам.
При пользовании популярной социальной сетью необходимо загружать личные фотографии и файлы только в доступ «для друзей». Таким образом, увидеть их смогут лишь те люди, кого вы лично одобрите. При этом важно осторожно подходить к выбору друзей, не принимать все заявки подряд для количества. Радость от большого числа «друзей» быстро омрачится неприятностями. Какими? Например, вы можете стать жертвой злого шутника, который использует ваши данные для организации киберпреследования. Ваши враги могут воспользоваться вашими фотографиями и контактами для размещения на других ресурсах, где бы вы совсем не хотели их видеть. Мошенники, спамеры, фишеры, получив информацию о вас, непременно включат ее «в свой оборот». Всегда старайтесь оставить о себе минимум информации, не сообщайте ничего лишнего, не открывайте доступ к своим личным страничкам незнакомым людям и общение в социальных сетях принесет максимум удовольствия и минимум проблем.
Источник: http://www.saferunet.ru/teenager/news/569/