

Муниципальное Казенное Общеобразовательное Учреждение

«Ново-Усурская СОШ»

ПРИНЯТО

на педагогическом совете

протокол согласования №1

от «28» августа 2020 г.

УТВЕРЖДАЮ

директор школы



Балабеков Ф. Н.

от «02» сентябрь 2020 г.

ПРОГРАММА
ПО СОЗДАНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ
СРЕДЫ В ШКОЛЕ

«Безопасность детей в
сети Интернет»

с. Новы Усур 2020 год

Безопасность детей в сети Интернет

Аннотация

Методические рекомендации «Безопасность детей в Интернете» посвящены решению проблемы защиты юных пользователей от различных опасностей, подстерегающих их во всемирной паутине.

Данные методические рекомендации предназначены для школьных учителей, классных руководителей, родителей и учащихся.

В основу рекомендаций положен многолетний опыт работы учителей информатики и классных руководителей, учителей-предметников, использующих на уроках и во внеклассной работе информационно-коммуникационные и интернет-технологии. Настоящие рекомендации могут быть использованы при проведении родительских собраний, внеклассных мероприятий, классных часов.

Пояснительная записка

Для гармоничного развития личности ребенку необходимо освоение новых технологий, а соответственно и знакомство с Интернетом, как с глобальным источником информации. Но реальность такова, что дети реже используют Интернет как библиотеку знаний, а делают упор на игры и общение в сети. Интернет стал неотъемлемой частью нашей жизни. С помощью всемирной паутины мы находим нужную информацию, общаемся с друзьями, узнаем последние новости, совершаем покупки и еще очень много всего. Но, как известно, в Интернете есть не только полезное. Интернет для детей таит в себе множество опасностей. Существует множество сайтов, пропагандирующих порнографию, проституцию, насилие, войны, межнациональную и религиозную рознь, употребление наркотиков и алкоголя. Такого рода информация может травмировать психику ребенка, вызвать страх, панику и внушить им ужас. Большинство взрослых, которые знакомы с Интернетом, понимают и осознают эту проблему. Но лишь немногие из них знают, как правильно защитить детей от такого рода информации. Методические рекомендации «Безопасность детей в Интернете» помогут им в решении этой проблемы.

Цель разработки данных рекомендаций – показать актуальность данной проблемы. Помочь учителям, родителям и учащимся усвоить правила пользования Интернетом, знать источники опасности, которые таит в себе всемирная паутина, и первоочередные шаги для обеспечения безопасности. От наших детей зависит наше с вами будущее, и с этим трудно поспорить. Ведь чем лучше мы сможем воспитать новое поколение, тем лучше будет мир, в котором мы живем. Именно поэтому мы должны защищать детей, учить, воспитывать и самое главное любить. Безопасность детей одна из главных задач цивилизованного общества, поэтому обеспечивать безопасность детей в Интернете должны все, кто причастен к этому обществу.

Методические рекомендации содержат перечень угроз, которые подстерегают детей в Интернете; советы родителям, как сделать прогулки ребенка в Интернете более безопасными; пособие для детей и родителей о правилах работы в сети, которые можно разместить на сайте школы, класса, личном сайте педагога. А также описание типов и признаков компьютерной зависимости, статистику компьютерной зависимости среди школьников 8-16 лет, советы по предотвращению развития компьютерной зависимости у детей и подростков, которые можно использовать на родительских собраниях по данной тематике. Приложения включают в себя тест на компьютерную зависимость, который могут провести педагоги, классные руководители и сами родители. Так же в приложениях есть две презентации «Этика сетевого общения» и «Как уберечь ребенка от опасностей, подстерегающих его в сети?». Первую можно использовать на уроках и внеклассных мероприятиях, вторую – на родительском собрании.

Использование данных методических материалов должно заставить задуматься о безопасности детей в сети и выяснить, что можно и нужно делать, чтобы всемирная сеть не становилась врагом юных пользователей. Как, правило, не выросло еще то поколение родителей, которые достаточно хорошо осведомлены о рисках и опасностях, которые подстерегают детей при работе в Интернете. Методические рекомендации «Безопасность детей в Интернете» должны помочь им в решении этой проблемы.

Цели и задачи программы

Цель: обеспечение информационной безопасности детей и подростков при обучении, организации внеучебной и внеурочной деятельности и свободном использовании современных информационно-коммуникационных технологий (в частности 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. Организации просветительской работы с учащимися и их родителями.

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.

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 и школы. Именно преподаватели и родители смогут предостеречь детей от возможных опасностей и ошибок. Существует ряд сайтов, посвященных безопасности детей в Интернете, 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.

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.

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.

Приложение 1.

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.

Приложение 2

Использование сети Интернет в образовательном учреждении

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

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.

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.

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-социалистической 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 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,	Несовместимая с задачами образования и воспитания информация о шейпинге, фигуре, похудении, медицине,

№ п / п	Наименование тематической категории	Содержание
	несовместимые с задачами образования)	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 онлайн-овые и оффлайн-овые 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 Интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
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	Сайты, содержащие несовместимую с задачами образования и

№ п / п	Наименование тематической категории	Содержание
	(ресурсы данной категории, несовместимые с задачами образования)	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 категории, несовместимые с задачами образования)	Содержащие несовместимую с задачами образования и воспитания информацию новостные ресурсы и сайты 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.

Приложение 3

1. Опасности Интернета.

На сегодняшний день Интернет предлагает несколько способов виртуального общения: социальные сети, форумы, ICQ, чаты, интернет-дневники или блоги. Источники проблем: Нежелательное содержание.

Азартные игры.

Вредоносные и нежелательные программы.

Мошенники, хакеры.

Интернет-зависимость (виртуальное замещение реальности)

Сексуальные домогательства.

Некорректность общения.

Интернет-хулиганы.

2. Защита детей – руководство к действию.

Существует большое количество программного обеспечения, с помощью которого можно осуществлять «Родительский контроль», многие антивирусы имеют эту функцию в своем арсенале. Родительский контроль так же представлен и в самой операционной системе Windows Vista и Windows 7, но это спасает лишь отчасти. Нельзя наивно думать, что если вы скачали программу из Интернета, проблема решена. Ваши дети умнее, чем вы думаете, они легко могут обойти все преграды и добиться своего. Поэтому, лучше быть на шаг впереди.

Первоочередные шаги для повышения безопасности:

Регулярно скачивайте обновления для программного обеспечения.

Установите антивирусное и антишпионское программное обеспечение.

Установите фильтр (например, Интернет-Цензор).

Установите спам-фильтр (например, в Outlook).

Не открывайте писем от пользователей, которых вы не знаете.

Лучший способ защиты детей – правильное воспитание.

Научите своего ребенка отличать хорошее от плохого.

Объясните ему, как следует вести себя в той или иной ситуации. Предупрежден - значит вооружен.

Помогайте ребенку решить его детские проблемы, даже если они вам кажутся пустяковыми. Он должен всегда чувствовать вашу поддержку.

Все то, чему вы учите своего ребенка, вы должны подкреплять собственным примером, иначе от обучения будет мало пользы.

Помните, что правильное воспитание - залог хорошего будущего ребенка.

Для лучшего взаимопонимания и устранения возможных недоразумений, лучше сразу расставить все точки над «и», установить некоторые ограничения для самостоятельного выхода в Интернет.

Обсудите это с детьми, чтобы они понимали необходимость подобных запретов, тогда вместе вы обязательно можете сделать прогулки ребенка в сети наиболее безопасными.

Составьте список правил работы детей в Интернете и помните, что лучше твердое «нет», чем неуверенное «да». Пусть ограничения будут минимальны, но зато действовать всегда и без ограничений.

Правила поведения при использовании детей Интернетом.

Приучите детей посещать только те сайты, которые Вы разрешили.

Используйте программные средства блокировки нежелательного материала.

Научите детей советоваться с Вами при раскрытии личной информации.

Требуйте от детей ничего не скачивать из Интернета без Вашего одобрения.

Не разрешайте пользоваться средствами мгновенного обмена сообщениями.

Беседуйте с детьми об их друзьях в Интернет.

Приучите детей сообщать Вам, если их что-то встревожило в сети.

Объясните детям, что в Интернете не вся информация правдива.

Научите детей проверять найденную информацию по другим источникам.

Научите детей различным способам поиска.

Поговорите с детьми о недопустимости вражды между людьми и о расизме, убедите их уважать вер