

**МЕТОДИЧЕСКИЕ
РЕКОМЕНДАЦИИ**

**Безопасность школьников
в сети Интернет**

2017 год

**Е.А. Багрова, И.В. Лысакова, к.п.н., Э.Г. Счастливая, В.П. Малыш,
М.В. Салыгина.**

Методические рекомендации «Безопасность школьников в сети Интернет».
Методические рекомендации предназначены для обучающихся всех ступеней образования, для педагогических работников и социальных педагогов, классных руководителей, сотрудников служб сопровождения, родителей (законных представителей) школьников. Настоящие рекомендации могут быть использованы при проведении родительских собраний, внеклассных мероприятий, классных часов.

Содержание

- Аннотация
- Актуальность
- Цель разработки
- Цели и задачи рекомендаций
- Нормативно-правовое обеспечение
- Ресурсное обеспечение
- Основные принципы контр пропагандистской деятельности
 - Профилактическая работа с детьми, с родителями
- Информационный ресурс
- Этапы реализации мероприятий
- Ожидаемые результаты
- Перспективы работы
- Примерный план реализации направлений работы по обеспечению безопасности в сети Интернет

Приложения

- Приложение 1 Правила работы в сети Интернет и в мобильных сетях связи для детей и родителей
- Приложение 2 Правила использования сети Интернет
- Приложение 3 Регламент по работе учителей и школьников в сети Интернет
- Приложение 4 Основные рекомендации для родителей по обеспечению безопасности детей в Интернете
- Краткий словарь используемых терминов

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

«Безопасность школьников в сети Интернет»

Аннотация к содержанию

Развитие образования начала XXI века обусловлено, прежде всего, переходом к постиндустриальному информационно-правовому обществу, характеризующемуся изменением социально-культурных условий развития системы образования, ростом интенсивности информационных процессов, тенденцией расширения доли Интернета в информационном пространстве. Интернет - один из основных каналов массовой информации, способный воздействовать на подростков, не определившихся в своих идеологических приоритетах. Необходимо учитывать, что современные информационные технологии создают возможность манипулятивного воздействия на личность, что бросает вызов интересам общественной и государственной безопасности. Особому риску подвержены школьники, т.к. их сознание наиболее восприимчиво к любому влиянию. Образовательное учреждение – это территория для развития личности обучающихся, достаточных для интеграции в современное общество, обладающих необходимым набором компетенций в вопросах правового воспитания и безопасного поведения в сети Интернет. Школа – это стартовая площадка для вступления выпускников во взрослую жизнь и успешного становления личности в современном обществе. Методические рекомендации «Безопасность детей в Интернет» 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 опыт работы учителей информатики и классных руководителей, учителей-предметников, использующих на уроках и во внеклассной работе информационно-коммуникационные и Интернет-технологии, психологов работающих в образовательном учреждении. Настоящие рекомендации могут быть использованы при проведении родительских собраний, тематических и внеклассных мероприятий, классных часов, индивидуальных бесед.

Актуальность

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 много всего другого. 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» могут стать полезными в решении этой проблемы.

Цель разработки рекомендаций – показать актуальность данной проблемы.

Рекомендации призваны 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 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 рекомендаций

Целью разработки Методических рекомендаций является обеспечение информационной безопасности детей и подростков при обучении, организации внеурочной деятельности, в свободном использовании современных информационно-коммуникационных технологий (сети Интернет)

- Задачи:***
1. Организация технического и правового контроля безопасности.
 2. Формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков.
 3. Создание педагогических условий обеспечения информационной безопасности обучающихся, 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. - оказание помощи родителям и педагогам в психолого-педагогическом изучении детей; - организация коррекционной работы с детьми, входящими в группу риска; - рекомендации по организации досуга и др.
6. Повышение уровня правовой культуры всех субъектов образовательного процесса;
7. Выработка способов взаимодействия семьи и школы, способствующей социально-педагогическому образованию учителей родителей и учащихся.
8. Выявление детей, нуждающихся в незамедлительной помощи и защите, оказание первой экстренной помощи;
9. Обеспечение психологической безопасности подростка, снятие стрессового состояния;
10. Изучение особенностей психолого-педагогического статуса каждого обучающегося с целью своевременной профилактики и эффективного решения проблем, возникающих в психическом состоянии, общении, развитии и обучении; формирование позитивного образа «Я», уникальности и неповторимости не только собственной личности, но и других людей.

Участники и исполнители:

Обучающиеся 5-11 классов, учителя - предметники, классные руководители, администрация, специалисты службы сопровождения, родители.

Нормативно-правовое обеспечение

Научно-методические основы программы соответствуют основным нормативно-правовым документам в образовании Российской Федерации:

- Закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ, статья 28 и др.
- Государственная программа Российской Федерации «Развитие образования» на 2013-2020 годы, утвержденной распоряжением Правительства Российской Федерации № 792-р от 15.05.2013,
- Конвенция о правах ребенка;
- Закон «Об образовании в Тульской области»;
- Федеральный Государственный Образовательный Стандарт в основной и средней школе (ФГОС);
- Федеральный закон Российской Федерации от 29 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- Закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»;
- «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821 – 10

Нормативное обеспечение образовательного учреждения

- Локальный акт «Правила использования сети Интернет»
- Регламент работы учителей и школьников в сети Интернет
- Инструкция для сотрудников о порядке действий при осуществлении контроля за использованием учащимися общеобразовательного учреждения сети Интернет.
- Журнал учета работы в Интернет.
- Методические рекомендации «Безопасность детей в Интернете»

Ресурсное обеспечение:

- 1) совершенствование профессионализма кадровых ресурсов – учителей и специалистов службы сопровождения;
- 2) активная работа с классными руководителями, Советом ОУ, родительской общественностью
- 3) привлечение специалистов, сотрудников правоохранительных органов для реализации мероприятий
- 4) формирование методических ресурсов ОУ

Методические рекомендации должны отвечать требованиям реализации, обеспечивающим:

- Целостность;
- Преемственность
- Последовательность;
- Логичность;
- Направленность на позитивные изменения и результаты в вопросах правового воспитания;
- Мониторинг результатов педагогической деятельности;
- Ориентация на дальнейшее совершенствование образовательного процесса в вопросах безопасного поведения детей в сети Интернет.

Основные принципы контр пропагандистской деятельности:

- патриотизм

- гуманизм
- соблюдение прав человека
- учет особенностей национального менталитета
- социальная справедливость
- системность

Контр пропагандистская деятельность в Интернете может осуществляться по двум направлениям:

- 1) Ограничение доступа к определенным материалам
- 2) Создание многочисленных контролируемых специалистами сайтов в целях публикаций на страницах контр материалов или опровержение существующих. **Первое направление** может путем:

- запрета доступа конкретным лицам или конкретным компьютерам в Интернет;
- запрета доступа к веб-сайтам с известными адресами, где размещаются нежелательные материалы;
- усложнение доступа определенной информации через снижение скорости соединения для предотвращения скачивания и получения материалов.

Перечисленные меры могут реализовываться правоохранительными органами или специальными службами.

Профилактическая работа с детьми

Работа с обучающимися в образовательном учреждении должна быть организована с учетом возрастных особенностей, направлена на формирование антиэкстремистского мировоззрения. Формы и методы работы с детьми могут быть различными. В средней школе рекомендуется проводить мероприятия в виде бесед, ролевых игр, диспутов, тренингов. В старшей школе – в виде тематических проектов, выпуска стенгазет, плакатов; участия в акциях, конкурсах, мероприятий, направленных на повышение квалификации учителей, просвещение родителей, обучение детей правилам безопасного пользования Интернет.

Рекомендуются классные часы по теме «Безопасность в сети Интернет»;

выпуск листовок,

буклетов,

памяток,

показ презентаций для обучающихся «Безопасность в Интернете» и т.д.

Формирование у школьников позитивной адаптации к жизни, как процесса сознательного достижения человеком относительно устойчивых отношений между собой, другими

людьми и миром в целом. В отношении обучающихся и особенно подростков педагогам необходимо сформировать устойчивое понимание общественного неприятия идеологии экстремизма, с которой могут сталкиваться школьники в сети Интернет. С этой целью может быть эффективной проведение разъяснительной работы, основанной на применении аргументации и контр аргументации, позволяющие достигнуть убеждающего эффекта.

Рекомендуемые направления работы:

1) Разъяснительная работа, направленная на убеждающий эффект. Убеждение как эффективный способ воздействия через отбор наиболее ценной, объективной информации, противодействия идеологии терроризма и экстремизма, обращено к разуму с применением рациональных аргументов, логики, авторитетов, конкретных жизненных примеров.

2) Применение методов противодействия идеологии экстремизма: приемы, способы, техники по реализации методов противодействия идеологии экстремизма в сети Интернет. К ним могут относиться:

1) метод предоставления собеседнику фактов и цифр, подтверждающих доказываемые тезисы и положения

2) метод противоречия, основанный на выявлении противоречий в аргументации собеседника

3) метод видимой поддержки, демонстрирующий согласие с примененными доводами оппонента, а затем выдвижение контраргументов

4) метод поэтапного согласия, «да»/»но»

3) Приемы и способы воздействия на отдельных учеников, на целевые аудитории, позволяющие учитывать эмоциональную сферу собеседника, создать эмоциональное сопереживание, смысловой резонанс, альтернативное позиционирование и др.

Основной прием - выработка умения верифицировать информацию, т.е. устанавливать ее достоверность, применяя критический взгляд на предоставленные материалы

4) Приемы, направленные на нейтрализацию замечаний, к которым относятся желание проявить себя, сопротивление, стремление к получению информации, ироничные замечания, отговорки, объективные замечания, предубеждения и проч.

5) Приемы, направленные на нейтрализацию технологий информационного воздействия, таких как манипулирование с истинной информацией, с опросами общественного мнения, тенденциозное представление информации, анонимный авторитет, «забалтывание», эмоциональный резонанс, эффект бумеранга, эффект ореола, эффект первичности, информационная блокада. Профилактическая работа с родителями Родители должны понимать, что Интернет, по мере расширения сферы его использования в повседневной жизни, создает потенциальную угрозу манипулятивного воздействия на личность. Формы работы с родителями различны – это родительские собрания («Безопасный Интернет - детям»), индивидуальные беседы, лекции. Родители должны понимать, что никто так не

отвечает за безопасность детей в Интернете, как сами родители. Только они могут полностью контролировать своих детей во время досуга.

Информационный ресурс

Для достижения положительных результатов необходимо проводить комплексную работу семьи и школы. Учителя и родители смогут предостеречь детей от возможных опасностей и ошибок. Существует ряд сайтов, посвященных безопасности детей в Интернете: www.saferunet.ru, www.detionline.org, www.interneshka.net, ресурсы которые оказывают эффективную помощь, как взрослым, так и детям. Информация для родителей и детей по безопасной работе в Интернет размещена на официальном сайте образовательного учреждения, в школьных помещениях: предметных кабинетах, рекреациях; на обозримом месте в здании школы. Образовательное учреждение, выполняя воспитательную миссию, должно обеспечивать контроль за эффективностью профилактической работы с привлечением сотрудников правовых органов и администрации Суворовского района, специалистов. Рекомендуется в систему мониторинга школы включить мониторинг качества знаний и практических умений в вопросах правового воспитания школьников, качества реализации воспитательной работы по безопасности поведения в сети Интернет. Итогом всех мероприятий по результатам проведения системного мониторинга должно стать совершенствование управленческих решений. 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.

Этапы реализации мероприятий

1 этап – организационный

1. Разработка нормативно-правовой базы по обеспечению безопасного поведения обучающихся в сети Интернет.
2. Создание банка методических материалов (модули, программы обучения, презентации, виртуальные галереи творческих работ обучающихся и др.).
3. Анализ реальной ситуации по данной проблеме (первичный мониторинг).
4. Диагностика интересов и направлений занятости учащихся во внеурочное время (промежуточный мониторинг).
5. Составление плана реализации программы по безопасности в сети Интернет для обучающихся основной и средней ступени обучения.

2 этап – практический

1. Организация и проведение профилактических воспитательных мероприятий (информационно-профилактических, творческих, исследовательских, др.).

2. Разработка рекомендаций педагогам, родителям и ученикам по профилактике компьютерной зависимости.
3. Разработка памятки для учеников по использованию ресурсов сети Интернет.
4. Анкетирование обучающихся, родителей, педагогов.
5. Текущий контроль за эффективностью реализации программы.

3-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.

Ожидаемые результаты

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

1. Обеспечит потребность учителя в постоянном повышению 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.
4. Будут сформированы у выпускников устойчивые навыки безопасного поведения в сети Интернет

Перспективы 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 РЕАЛИЗАЦИИ НАПРАВЛЕНИЙ РАБОТЫ

Выявление и реабилитация несовершеннолетних и их семей, оказавшихся в сложной жизненной ситуации Исследования социального статуса семей обучающихся. Составление социального паспорта класса и школы Составление базы данных по социальнонеблагополучным семьям Проведение индивидуальных профилактических мероприятий с семьями социального риска Мини-тренинги («Учимся снимать усталость», «Как преодолеть тревогу», «Способы решения конфликтов», «Стресс в жизни человека – способы саморегулирования эмоционального состояния», «Как сказать НЕТ») Классные часы по профилактике суицидального поведения «Что может быть дороже жизни», «Мы выбираем жизнь», «Организация досуга и возможные последствия контакта в сети Интернет с экстремистскими сообществами в социальных сетях», «Основы безопасной работы в сети Интернет» Проведения развивающих занятий с подростками «Ценит настоящее», «Самопринятие, самоуважение. Самоодобрение». Занятия по профилактике киберпреступности среди несовершеннолетних, «Профилактика зависимого поведения» Конкурсы рисунков и плакатов «Счастье жить». «Безопасный интернет» Психолого-педагогическая поддержка обучающихся при подготовке и во время проведения экзаменов (ГИА) Тестирование и анкетирование подростков в целях оказания помощи в экстренных ситуациях Исследования в динамике Социального статуса, уровня адаптации, уровня тревожности Индивидуальные и групповые беседы с обучающимися, попавшими в трудную жизненную ситуацию Диагностика психоэмоционального состояния учащихся по проективным методикам (рисуночные тесты, цветовой тест Люшера и др) для выявления учащихся с высоким уровнем тревожности и депрессии. Составление программ реабилитации. Диагностика по выявлению наличия признаков компьютерной и игровой зависимости Выявление особенностей адаптации у вновь принятых учащихся. Анкетирование учащихся на предмет участия в социальных сетях, различных виртуальных группах Для учителей, классных руководителей, психологов Знакомство педагогов с нормативной базой и школьными локальными актами: приказы, регламент работы учителей и школьников в сети Интернет, Инструкция для сотрудников о порядке действий при осуществлении контроля за использованием обучающимися ОУ сети Интернет Тематические совещания, методические объединения, педсоветы на тему «Возрастные психолого-педагогические особенности подростков», «Причины подросткового суицида. Роль взрослых в оказании помощи подросткам в кризисных ситуациях». «Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях» Семинары-лекции «Профилактика семейного неблагополучия и суицидального поведения детей и подростков», «Как дружить в сети Интернет», «Интернет: плюсы, минусы, подводные камни», «Правила безопасной работы на компьютере», «Полезный и безопасный интернет» Индивидуальные консультации для классных руководителей «Создание благоприятного психологического климата в

классном коллективе» Создание странички сайта «Внимание! Компьютерная зависимость», линии помощи «Дети онлайн» Диагностика синдрома профессионального выгорания Мониторинг удовлетворенности образовательным процессом обучения Социометрия. Диагностические исследования учащихся по выявлению психологического климата в коллективе Для родителей Родительские собрания «Психологические особенности периода адаптации», «Формы родительской поддержки и помощи подросткам», «Роль взрослых в оказании помощи подростку в кризисной ситуации» Тестирование, анкетирование родителей по выявлению компетентности оказания помощи в кризисной ситуации подростка» Разработка методических рекомендаций по профилактике причин возникновения и форм проявления невротических расстройств у несовершеннолетних» Индивидуальные и групповые консультации для родителей Размещение и ознакомление родителей с Памятками по обеспечению информационной безопасности на сайте Мониторинг: Анкетирование родителей на предмет их удовлетворенности процессом обучения и психологической комфортностью детей на уроках Консультирование по результатам психологического обследования: «Подросток в вашей семье» 5- 11 кл. «Групповое консультирование на возрастных этапах» Тематическое консультирование: «Подросток в Вашей семье. Вопросы развития и воспитания» Особенности суицидального поведения подростков Работа с семьей подростка, имеющего риск суицидального поведения Психолого-педагогическое консультирование родителей для организации эффективного детскородительского общения Выступление психолога на родительских собраниях в выпускных классах «Предотвращение предэкзаменационного стресса», распространение тематических буклетов Мониторинг: Анкетирование родителей на предмет их удовлетворенности процессом обучения и психологической комфортностью детей на уроках Консультирование по результатам психологического обследования: «Подросток в вашей семье» 5- 11 кл. «Групповое консультирование на возрастных этапах»

ПРИЛОЖЕНИЯ

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 относятся 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 посещения 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 незащищен 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

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 вводятся 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 техническими 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 учреждения 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 учреждения 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.

Приложение 3

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 ЕГЭ; 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 (сетевое) общения; опубликование интересных авторских материалов педагогов и учащихся, обмен опытом; создание вебстраниц; 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 учебнообразовательном 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 4). 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 программными 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
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
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, ТВпрограмм, 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 № п / п Наименование тематической категории Содержание 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 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 Интернетресурсов Сайты, предлагающие услуги по отправке SMSсообщений 10 Интерактивные доски Содержащие несовместимую с задачами № п / п Наименование тематической категории Содержание объявлений (ресурсы данной категории, несовместимые с задачами образования) 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 Интернетпредставительства 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 категории, несовместимые с задачами образования) Содержащие несовместимую с задачами образования и воспитания информацию новостные ресурсы и сайты СМИ (радио, телевидения, печати) № п / п Наименование тематической категории Содержание 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 4 Основные рекомендации для родителей по безопасности в сети Интернет 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. Программное обеспечение от Microsoft для обеспечения безопасности в Интернете: Windows 7 с функцией родительского контроля (ввод ограничений по играм, программам и проводимому за компьютером время). Internet Explorer 8 – браузер с фильтром, предотвращающим мошенничество (помогает защититься от скрытой установки вредоносных программ, которые могут повредить, передать злоумышленникам или уничтожить ваши документы, использовать ваши персональные данные или просто нарушить работу ПК). Антивирус Microsoft Security Essentials – решение против шпионских программ (Решение Microsoft® Security Essentials обеспечивает БЕСПЛАТНУЮ защиту ПК от вирусов, шпионского и другого вредоносного ПО на основе передовой технологии) . Windows Live с функцией «Семейная безопасность» (С помощью данной службы можно защитить детей от просмотра нежелательного веб-содержимого, управлять списком пользователей, а также отслеживать посещаемые детьми веб-сайты). 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 пользовании 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 верования других людей. Используйте фильтры, блокирующие нежелательное содержание. Разъясните детям нежелательность использования ненормативной лексики, требуйте соблюдения определенного этикета и вежливости. Относитесь к программным средствам защиты как к дополнительным элементам контроля. Пусть дети всегда могут попросить Вас о помощи. Не разрешайте личных встреч с новыми знакомыми из Интернета без вашего одобрения. Запретите оставлять свою личную информацию в Интернете. Конечно же, никто так сильно не отвечает за безопасность детей в Интернете, как сами родители. Ведь только родители могут полностью контролировать своих детей.

Возрастные особенности детей и Интернет

Дети от 7 до 10 лет: 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 в этом возрасте пользоваться средствами мгновенного обмена сообщениями. Беседуйте с детьми об их друзьях в Интернет. Приучите детей сообщать Вам, если их что-то встревожило в сети.

Дети от 10 до 13 лет: Создайте ребенку собственную учетную запись с ограниченными правами. Используйте средства фильтрации нежелательного материала. Напоминайте детям о конфиденциальности личной информации. Приучите детей спрашивать разрешение при скачивании программ или файлов из Интернета. Поощряйте детей сообщать Вам, если их что-то тревожит или смущает в Интернете. Настаивайте на том, чтобы дети позволяли Вам знакомиться с их электронной почтой. Расскажите детям об ответственном и достойном поведении в Интернете.

Дети в возрасте 14-17 лет: Контролируйте, какими чатами и досками объявлений пользуются дети. Настаивайте, чтобы Ваши дети никогда не соглашались на личные встречи с друзьями из Интернета. Напоминайте детям о конфиденциальности информации. Помогите им защититься от спама. Предостерегите Ваших детей от использования Интернета для хулиганства. Убедитесь, что подростки советуются с Вами перед покупкой или продажей чего-либо через Интернет. Обсудите с подростками азартные игры и их возможный риск. Как

избежать проблем, связанных с игровыми сайтами? Не секрет, что дети обожают игры, а современные дети обожают играть в сети Интернет. Но блуждая по Интернету, они легко могут попасть и на сервер с азартными играми. Закон разрешает для несовершеннолетних большинство игр, но это не касается игр на деньги. Собственно, использование денег и является разницей между теми сайтами с азартными играми и сайтами, где просто играют. На последних в качестве развлечения предлагаются на выбор аркады, словесные игры, головоломки. Поощрительным моментом там является начисление очков или баллов. Нет траты денег. Существуют сайты, где вместо реальных денег используются игровые, но они не менее опасны, чем сайты с играми на деньги, так как вырабатывают привычку играть на деньги вообще и провоцируют азарт. Контроль игр. Как избежать проблем, связанных с игровыми сайтами? Контроль игр должны осуществлять родители, обсудить, какие жанры игр предпочтительны (например, стратегии или шахматы). Немаловажен такой фактор, как количество участников – не обязательно играть с кем-то, можно и одному. Регулярно не только напоминайте детям, что на деньги играть нельзя, но и постарайтесь обосновать этот запрет. Так как наилучшая защита ребенка от игр на деньги – это его собственное понимание всей опасности. Объясните детям, что выигрыш таких сайтов много больше, чем проигрыш, иначе они бы просто не существовали. Контроль игр может спасти вас от долгов. Использование номеров ваших кредитных карт без вашего разрешения должно стать для детей табу, а сами «кредитки» находиться в недоступном месте. Ведь некоторые виды карточек предполагают возможность кредитования, а это может спровоцировать появление долгов. К чему могут привести игры на деньги? Важно объяснить ребенку, что игры на деньги могут приводить к зависимости, которой очень трудно сопротивляться даже взрослым. Зависимость – как первое время бессимптомно, тяжело протекающая болезнь, которая часто становится хронической. Во избежание этого чаще обращайтесь внимание на круг интересов вашего ребенка. Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но в то же время, сеть таит в себе много опасностей. Обязательно нужно поговорить с детьми, объяснить, что могут возникать различные неприятные ситуации и то, как из них лучшим образом выходить. Помните, что безопасность ваших детей в Интернете, на 90% зависит от вас. Компьютерная зависимость Если вы заметили, что ребенок может часами просиживать перед голубым экраном за игрой в «Counter Strike», «Quake», днями не выходить из Интернета, заменяя живое общение чатами, форумами, сайтами знакомств - тогда есть о чем задуматься. Термин «компьютерная» или «киберзависимость» определяет патологическое пристрастие человека к проведению всего свободного времени за компьютером ради развлечения. Все интересы «компьютерных фанатов» или «геймеров» сводятся лишь к удовлетворению: игровой зависимости (стрелялки и стратегии или онлайн-азартные игры); киберсексуальной зависимости – непреодолимого влечения к просмотру порносайтов; непреодолимого пристрастия к виртуальному общению по веб-сети; навязчивого веб-серфинга – бесконечный поиск новой информации не ради самой информации, а ради праздного любопытства. Основные типы компьютерной зависимости: - Зависимость от Интернета (сетеголизм) Сетеголиками (зависимость от Интернета) проявляются бесконечным пребыванием человека в сети. Иногда они находятся в виртуальном мире по 12-14 часов в сутки, заводя виртуальные знакомства, скачивая музыку, общаясь в чатах. Это неряшливые, неуравновешенные люди, которые наплеватьски относятся к близким. - Зависимость от компьютерных игр (кибераддикция) Кибераддикция (зависимость от компьютерных игр) подразделяется на

группы в зависимости от характера той или иной игры: - Ролевые компьютерные игры (максимальный уход от реальности). - Не ролевые компьютерные игры (стремление к достижению цели – пройти игру, азарт от достижения цели, набора очков). Признаки компьютерной зависимости: Значительное улучшение настроения от работы за компьютером. Нежелание оторваться от работы или игры на компьютере. Если Вы отрываете больного от компьютера, он испытывает раздражение, даже проявляет некоторую агрессию по отношению к Вам. Неспособность спланировать окончание работы или игры на компьютере. Пренебрежение домашними делами в пользу компьютера. Пренебрежение личной гигиеной и сном в пользу компьютера. При общении с окружающими сведение любого разговора к компьютерной тематике. Отказ от общения с друзьями. Можно наблюдать и некоторые физические отклонения, страдающего компьютерной зависимостью: нарушение зрения, снижение иммунитета, головные боли, повышенная утомляемость, бессонница, боли в спине, туннельный синдром (боли в запястье). Лечение компьютерной зависимости – сложная проблема, которая требует согласованной работы специалистов различных областей медицины и родителей. Советы по предотвращению развития компьютерной зависимости у детей и подростков Так как первопричиной ухода ребенка из реального мира является неудовлетворенность существующей действительностью, необходимо в первую очередь выяснить, что же побудило ребенка уйти «в компьютер». Неправильно критиковать ребенка, проводящего слишком много времени за компьютером. Если вы видите у ребенка признаки компьютерной зависимости, не обостряйте ситуацию, отведите его к психотерапевту. Можно попытаться вникнуть в суть игры, разделив интересы ребенка, это сблизит ребенка с родителями, увеличит степень доверия к ним. Рекомендуется ограничивать доступ детей к играм и фильмам, основанным на насилии. Рекомендации по сохранению здоровья при работе детей за компьютером в школе и дома: Расстояние от глаз до экрана должно составлять 50-70 см. Нельзя работать за компьютером в темноте. Ребёнок школьного возраста может проводить за компьютером непрерывно не более 10-20 минут, после чего необходимо сделать перерыв и небольшую гимнастику для глаз (оптимальная продолжительность непрерывных занятий с компьютером для учащихся: начальной школы должна быть не более 15 минут; основной школы – 20 минут, старшей школы – 25-30 минут). Если есть проблемы со зрением, то садиться за монитор можно только в очках. Необходимо постоянно снижать количество пыли в помещении посредством влажной уборки. Психическая нагрузка и стресс при потере информации. Компьютер требует сосредоточенности. Однако психическую нагрузку можно уменьшить (в работе следует делать перерывы, необходимо следить за содержательной стороной работы за компьютером). Учитывая эти факторы вредоносного влияния компьютера на организм человека (нагрузка на зрение, стесненная поза, излучение и воздействие на психику), родители могут помочь организовать ребенку дома наиболее безопасную среду при взаимодействии с компьютером.

КРАТКИЙ СЛОВАРЬ ИСПОЛЬЗУЕМЫХ ТЕРМИНОВ

Интернет (от английского Internet) - это общедоступная всемирная компьютерная сеть, которая связывает между собой компьютеры и позволяет пользователям передавать и получать различную информацию. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть.

IP-адрес - (сокращение от английского Internet Protocol Address) - уникальный сетевой адрес устройства (компьютера, мобильного телефона, планшета, сервера и т. п.) в компьютерной сети. Статический IP адрес (постоянный, неизменяемый IP адрес) - это адрес (идентификатор), назначенный устройству в сети на постоянной основе. Данный тип адреса остается неизменным при каждом подключении к сети и всегда идентифицирует то же устройство, которому он был назначен изначально. Как правило, все сервера в Интернете имеют статические IP адреса. Это необходимо для того, чтобы при подключении к данному IP адресу в любой момент времени пользователь получал доступ к тому же самому серверу в сети. Динамический IP адрес (непостоянный, изменяемый IP адрес) - это адрес (идентификатор) который присваивается устройству автоматически при выходе в Интернет и используется до завершения сеанса соединения.

Веб-сайт или сайт (от английского website: web- «паутина, сеть» и site - «место», буквально «место, сегмент, часть в сети») - совокупность электронных документов (файлов) частного лица или организации, представленных в виде интернет-страниц, имеющих уникальный интернет-адрес.

Портал (portal от латинского porta - ворота) - сайт, который содержит большое число ссылок на другие сайты Интернета. Портал может предоставлять посетителям различные сервисы (почта, погода, новости, обсуждения, голосования и т. п.). Как правило, на портале есть возможность разместить объявление или статью, загружать фотографии, комментировать информацию, сохраненную на портале другими пользователями.

Блог (от английского blog - интернет-дневник) - веб-сайт, основное содержимое которого – регулярно добавляемые записи, содержащие текст, изображения или видео. Для блогов характерны длинные записи, актуальные к конкретному промежутку времени или событию. Как правило, блоги рассчитаны на широкий круг читателей и предполагают возможность публично комментировать записи автора. Блогер (от английского blogger) - лицо, ведущее блог. Блогосфера (от английского blogosphere) - совокупность всех блогов в Интернете.

Микроблог - аналог обычного блога, но с короткими постами (100-200 символов). Используется обычно для того, чтобы написать что-то очень интересное о том, что сейчас делает пользователь.

Твит (от английского tweet - чирикать, болтать, щебетать) - запись в сети микроблогов Твиттер. Ретвит - цитирование твита другого пользователя сети микроблогов Твиттер. Социальная сеть или соцсеть (от английского social networking service) - это объединение личных Интернет- страниц пользователей, объединенных по каким-то признакам. В первую очередь, социальные сети рассчитаны на поиск нужных контактов и общение. Характерными особенностями социальных сетей являются: -создание личных профилей (публичных или полупубличных), в которых зачастую требуется указать реальные персональные данные и другую информацию о себе (место учебы и работы, хобби, жизненные принципы и т. п.); - предоставление возможностей обмена информацией (размещение фотографий, видео, текстовых записей, организация тематических сообществ, обмен личными сообщениями и т. п.); - возможность задавать и поддерживать список других пользователей социальной сети, с которыми у пользователя имеются

некоторые отношения (например, дружба, родство, деловые и рабочие связи и т. п.); - имеется возможность организации личной переписки между пользователями с помощью мгновенных сообщений (чатов) .

Хэштег (или хештег; от английского hashtag от hash - символ # («решетка») + tag - метка, ярлык) - это слово или фраза, которым предшествует символ #. Хештег предназначен для объединения сообщений (или групп сообщений) по определенной теме или типу с помощью слов или фраз, начинающихся с символа #. Например, #Медиагвардия. Для объединения сообщений могут быть использованы как один, так и несколько хэштегов. Хэштеги дают возможность группировать подобные сообщения, таким образом можно найти хэштег и получить подборку сообщений, которые его содержат. Пост (от английского post) - отдельно взятое сообщение, размещенное в социальной сети или блоге. Репост (от английского repost) - размещение в блоге копии поста другого блогера, пользователя социальной сети или любого другого исходного материала, а также копирование самим автором материала, ранее размещенного в Интернете. Обычно репост содержит ссылку на оригинальный материал и делается с целью поддержать позицию автора исходного материала. Также репост может иметь целью распространение важной, по мнению совершающего репост, информации (иным методом реализации данного сообщения является написание краткого содержания поста своими словами и дача ссылки на исходный пост).

Анонимизация (от английского anonymization) - процесс удаления или сокрытия данных в сети с целью предотвращения установления личности пользователя, местонахождения устройства, с которого осуществлен выход в Интернет, места назначения отправляемой пользователем информации. Анонимайзер (от английского anonymizer) - средство для сокрытия информации об устройстве или пользователе в сети. Может быть программой, устанавливаемой на устройство, или специальным веб- сайтом. На сегодняшний день наиболее распространение. Основные сферы использования анонимайзеров: обеспечение конфиденциальности пользователя; предоставление доступа к запрещенным веб-сайтам и т. п..

Хостинг - (англ. hosting) - услуга по предоставлению вычислительных мощностей для размещения информации на сервере, постоянно находящемся в сети (обычно Интернет).

