

Межрегиональный телекоммуникационный проект
для педагогов, специалистов и руководителей образовательных учреждений
"Методическая поддержка обеспечения информационной безопасности детей"
(Координатор проекта - ГАОУДПО ВИПКРО имени Л.И. Новиковой)



МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по информационной безопасности в сетевой проектной деятельности

"Тот, кто не смотрит вперед, оказывается позади"

Дж. Герберт

Авторы-составители:

Дроздова Динара Николаевна,

учитель начальных классов, МКОУ Нечаевская ООШ,
Гусь-Хрустальный район, Владимирской области

Мелещенко Ирина Геннадьевна,

учитель английского языка, МБОУ СОШ №8 г.Новокузнецка Кемеровской области

Плужникова Анна Евгеньевна,

учитель русского языка и литературы, МБОУ СОШ № 14,
г.Апатиты Мурманской области

Денисова Инна Петровна,

зам.директора по УВР, МБОУ СОШ №5 г.Киржача Владимирской области

Панкратова Марина Магомедхабибовна,

учитель химии МБОУ СОШ № 3 г.Вязники Владимирской области

Чернова Светлана Александровна

учитель начальных классов, ГКОУ ВО "Областная санаторная школа-интернат"
г. Вязники Владимирской области

2013 год

ОГЛАВЛЕНИЕ

Пояснительная записка.....	3
Основные термины и понятия.....	5
Список сокращений.....	7
Нормативно-правовые основы информационной безопасности детей.....	8
Содержание.....	9
Телекоммуникационный проект.....	9
Понятие безопасной работы в Интернете.....	10
Обзор требований безопасности в школе.....	11
Защита личной информации учеников.....	12
Безопасное поведение в Интернете.....	13
Список рекомендуемой литературы.....	15
Приложения.....	16
1. Требования к участникам телекоммуникационного проекта.....	16
2. Образец согласия родителей о персональных данных детей, участвующих в сетевых проектах.....	17
3. Советы родителям о правилах поведения детей в Интернете.....	19
4. Советы педагогам при организации сетевой проектной деятельности с учащимся	22
5. Рекомендации по составлению мероприятий с обучающимися и родителями по информационной безопасности в сети Интернет.....	23
6. Анкета для опроса родителей участников сетевого проекта.....	24
7. Памятка для родителей “Если Ваш ребенок участвует в создании проекта, какова Ваша роль?”	27
8. Перечень интернет-ресурсов для работы педагога с учащимися и их родителями по информационной безопасности.....	29
9. Перечень Интернет-сервисов, рекомендуемых для организации сетевых проектов.....	29

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Проблема информационной безопасности в сетевой проектной деятельности необычайно актуальна в наше время.

Современное образование сопровождается повсеместным использованием информационных ресурсов. Это находит отражение в последних государственных документах, регулирующих отношения в сфере образования – Федеральный Закон РФ «Об образовании», президентская программа «Наша Новая школа», ФГОС НОО, Стратегия инновационного развития Российской Федерации на период до 2020 года.

Главным ориентиром отечественной школы является «воспитание и развитие качеств личности, отвечающих требованиям информационного общества». В условиях современной модернизации российского образования особое значение приобретает проблема медиабезопасности учащихся, то есть – состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»). С активизацией роли Интернета в образовании учащиеся получили доступ ко многим образовательным ресурсам. Однако сознание современного школьника подвергается давлению хаотичного потока информации из Интернета. Она перекрывает знания ребенка, получаемые от родителей, воспитателей, учителей.

Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете, Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочной плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда

их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию").

Преодолеть нежелательное воздействие компьютера возможно только совместными усилиями учителей, родителей и самих школьников.

Поэтому ЦЕЛЬ нашей работы:

- Повышение уровня сетевой культуры юных пользователей,
- оказание методической помощи педагогам, родителям и всем заинтересованным в информационной безопасности детей и подростков в сети.

Ожидаемые результаты :

методические рекомендации при работе над телекоммуникационными проектами, могут послужить основой для проведения классных часов, бесед по информационной безопасности, уроков безопасной работы в Интернете, а также наши рекомендации помогут родителям правильно организовать, проконтролировать работу собственных детей в Интернете, ученики узнают о рисках, которые подстерегают их в Интернете, научатся правильно реагировать на различные неприятные ситуации, которые могут случиться с ними в виртуальной реальности.

Новизна данной работы заключается как в самом названии, так и в полноте охвата темы, широком историко-методическом материале, использованном при составлении рекомендаций.

ОСНОВНЫЕ ТЕРМИНЫ И ПОНЯТИЯ

[Ссылка на словарь компьютерных терминов](#)

[Ссылка на словарь терминов по информационной безопасности](#)

Аватара - маленькая картинка - фотография, рисунок, графика, вставляемая пользователем в качестве своего виртуального изображения на форумах, в социальных сетях и др. местах общего пользования в Интернете.

Аккаунт- запись, содержание сведения о пользователе компьютерной сети.

Атака - нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой.

Блог- (от англ.blog- журнал или дневник событий) - это веб-сайт, в качестве наполнения которого выступают регулярно обновляемые записи, добавляемые изображения или размещённые мультимедийные объекты, выражающие какую-либо мысль автора.

Безопасность информации - состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Брандмауэр – это специальная программа или устройство, которое позволяет блокировать попытки хакеров, вирусов и червей получить доступ к вашему компьютеру через Интернет.

Браузер- программа для просмотра интернет - сайтов и перехода от одной странице к другой.

Веб-форум - класс веб-приложений для организации общения посетителей веб-сайта.

Виртуальная агрессия - это действия, имитирующие применение силы и совершаемые с целью нарушить изначально заданную целостность объекта игры, в чувственном аспекте весьма приближенный к наглядному его образу.

Веб-сайт - wiki сайт - структуру и содержимое которого пользователи могут сообщать изменять с помощью инструментов, предоставляемых самим сайтом.

Гиперссылка - это какой-либо элемент веб-страницы сайта (текст, изображение, блок), с помощью которого при нажатии можно перейти на другую страницу или сайт, а также скачать другой объект, например, файл.

Груминг – это тактический подход взрослого человека к несовершеннолетнему, как

правило, с сексуальными целями.

Интернет - всемирная система объединённых компьютерных сетей, построенная на базе протокола IP и маршрутизации IP-пакетов. Интернет образует глобальное информационное пространство.

Информационный ресурс - в широком смысле - совокупность данных, организованных для эффективного получения достоверной информации. Информационные ресурсы - по законодательству РФ - отдельные документы и отдельные массивы документов, в информационных системах: библиотеках, архивах, фондах, банках данных, других видах информационных систем.

Информационная безопасность системы - состояние защищенности информационной среды (информации, информационных ресурсов, фондов и информационных систем, баз данных), при которой её формирование, использование, развитие и информационный обмен обеспечивается защитой информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования.

Кибер-буллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи.

Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительным признаком которых является способность к размножению (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру.

Контент- означает “содержание, содержимое”, это собирательный термин в информационном ресурсе.

Программа фильтрации - программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определённым сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра.

Рефер - человек привлёкший в Интернет проект других участников.

Сетевой этикет- правила поведения, общения в сети, традиции и культура интернет-сообщества.

Фишинг — это вид хищения персональных данных через Интернет.

Чат, чаттер — средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее

организовывать такое общение.

Хостинг - услуга по предоставлению дискового пространства для физического размещения информации (файлов сайта) на сервере находящемся в сети Интернет.

Электронные ресурсы - учебные материалы, для воспроизведения которых используются электронные устройства.

Электронное сообщение- информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Список сокращений

[Ссылка на Интернет-издание](#)

CHPPT - защищенный гипертекстовый транспортный протокол.

CMS (англ. Content Management System) – "система управления содержанием" сайта.

CSS - Cascading Style Sheets (Каскадные таблицы стилей) — технология описания внешнего вида Интернет-сайта, написанного языком разметки. Преимущественно используется как средство оформления веб-страниц в формате HTML.

DDoS-атака - сокращение от англ. Distributed Denial Of Service Attack (атака типа "отказ в обслуживании"). Компьютерное преступление, особенностью которого является то, что злоумышленники не ставят своей целью незаконное проникновение в защищенную компьютерную систему с целью кражи или уничтожения информации. Цель данной атаки - парализовать работу атакуемого веб-узла.

DRM — защита произведений от копирования и других действий, запрещаемых авторами или иными правообладателями на основании авторского или смежных прав.

ICQ - одна из самых популярных программ общения через Интернет.

IP-адрес - сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

НСД - несанкционированный доступ.

HTTP-протокол передачи гипертекста.

HTML- язык разметки гипертекста. Это базовый язык создания документов в сети Интернет.

PCT - Шифровальное средство для закрытой передачи данных в WWW.

SSL - это технология, обеспечивающая безопасное соединение между веб-сервером

и программным обеспечением клиента (Safe Server Link).

SkyDNS — бесплатный интернет-сервис на основе службы DNS для блокировки доступа к опасным, вредоносным сайтам и сайтам не подходящим для просмотра несовершеннолетними.

UAC (англ.) - контроль учётных записей пользователей. UAC - это компонент операционных систем Microsoft Windows, впервые появившийся в Windows Vista, запрашивающий подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера вредоносными программами, проще говоря - вирусами.

URL - адрес страницы в Интернете.

Нормативно-правовые основы информационной безопасности детей

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
2. Закон РФ "Об авторском праве и смежных правах"
3. Указ Президента Российской Федерации от 17.03.2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"
4. Федеральный закон Российской Федерации от 28 декабря 2010 г. N 390-ФЗ "О безопасности"
5. Федеральный закон Российской Федерации от 25 июля 2011 г. N 261-ФЗ г. Москва "О внесении изменений в Федеральный закон "О персональных данных"
6. Постановление Правительства Российской Федерации от 18 апреля 2012 г. N 343 г. Москва "Об утверждении Правил размещения в сети Интернет и обновления информации об образовательном учреждении"
7. Письмо Минобразования РФ от 13.08.2002г №01-51-088ин "Об организации использования информационных и коммуникационных ресурсов общеобразовательных учреждений"

Содержание

В настоящее время в России идёт становление новой системы образования, ориентированной на вхождение в мировое образовательное пространство. Целью реализации ФГОС второго поколения является не предметный, а личностный результат. Важна прежде всего личность самого ребенка и происходящие с ней в процессе обучения изменения. Стандарт включает в себя не только требования к знаниям, но и к уровню воспитанности, развития личности, а также к условиям образования.

Акцент переносится с "усвоения знаний" на формирование "компетентности", происходит переориентация на личностно-ориентированный (гуманистический) подход, противоположный знаниево-ориентированной, безличностной педагогике; школы обеспечиваются современными компьютерами, электронными ресурсами, доступом к Интернету. Это способствует внедрению новых педагогических технологий в учебно-воспитательный процесс отечественной школы. В соответствии с новыми ФГОС образовательное учреждение должно предоставлять ученикам возможность формирования индивидуальных учебных планов, включающих обязательное выполнение индивидуального проекта.

В основе проектной деятельности лежит развитие познавательных навыков учащихся, умений самостоятельно конструировать свои знания, ориентироваться в информационном пространстве, развитие их критического и творческого мышления, умение увидеть, сформулировать и решить проблему. Навыки информационной грамотности – навыки 21 века, которые подразумевают способности определить необходимую информацию и затем найти ее, собрать, организовать, оценить и использовать для создания новых идей или решения задач.

Разновидностью метода проектов является метод телекоммуникационных проектов. Под учебным телекоммуникационным проектом понимается совместная учебно-познавательная, творческая или игровая деятельность учащихся-партнеров, организованная на основе компьютерной телекоммуникации, имеющая общую цель, согласованные методы, способы деятельности, направленную на достижение общего результата деятельности.

Однако подключенные к Интернету компьютеры представляют собой серьезную проблему для школы. Учителя ратуют за то, чтобы их ученики имели доступ к материалам обучения, сотрудничали с экспертами и обменивались знаниями и

идеями. Однако, помимо этого Интернет – это еще и значительный риск для безопасности в виду незаконного использования. Каким же образом школа может защитить учеников, оборудование и информацию.

В мировой практике **понятие безопасной работы в Интернете** включает в себя довольно широкий спектр рисков. Вот только некоторые из них:

- опасность размещения в сети личных данных (имен, фамилий, адресов, фотографий, электронных адресов и т. п.);
- опасность предоставления данных о финансовом положении своей семьи;
- опасность несанкционированного использования детьми кредитных карточек;
- опасность неподконтрольного взрослым объединения детей в сомнительные организации;
- опасность получения детьми непристойных материалов различного характера (порнография, жестокость и т. п.);

В России под безопасным использованием Интернета чаще понимается:

- антивирусная безопасность;
- борьба с несанкционированным подключением к вашей сети;
- ограничение доступа к сайтам с непристойной информацией.

Однако с учащимися желательно обсудить и мировой опыт, и проблемы безопасности внутри страны. Инструкции по безопасному использованию Интернета должны быть разъяснены учащимся до того, как они получают доступ к Интернету или им предоставят индивидуальные адреса электронной почты.

Как удерживать учащихся от доступа к веб-сайтам, содержащим неприличные материалы, и контакта с лицами, представляющими угрозу? Чтобы защитить учащихся и убедить в необходимости этого их родителей, необходимо принять меры, направленные на предотвращение любых несанкционированных вторжений в информационное пространство школы.

В соответствии с мировым опытом, одним из способов обеспечения безопасной работы учащихся в Интернете является разработка и применение внутри учебного заведения Правила Безопасного Использования Технологий (ПБИТ). ПБИТ представляет собой подписанное учащимися, их родителями и учителями письменное соглашение, которое определяет порядок использования Интернета.

ПБИТ должна включать инструкцию по публикации в Интернете личных данных учащихся, их фотографий, аудио- и видеоматериалов и т. п.

Если Ваши дети пользуются Интернетом, Вы, без сомнения, беспокоитесь о том, как уберечь их от неприятностей, которые могут подстерегать их в путешествии по этому океану информации. Хотя значительная часть ресурсов Интернета не может нанести детям вреда, распространение материалов, предназначенных только для взрослых или неприемлемых по какой-либо другой причине, может легко привести к неприятным последствиям. Обсудите с группой вопросы безопасности учащихся, связанные с их деятельностью в Интернете в Вашем проекте. Что Вы готовы предпринять для ограждения их от доступа к веб-сайтам, содержащим непристойные материалы, и для ограничения от контактов с лицами, представляющими угрозу?

Обзор требований безопасности в школе

1. Административные настройки безопасности – предназначены для того, чтобы предотвратить доступ неавторизованных пользователей к школьным компьютерам и обеспечивать уверенность в том, что приватная информация (например, данные учеников) не выходит за пределы школьной сети.
2. Программное обеспечение системы безопасности, хотя и не является совершенным, помогает защитить оборудование и программы от:
 - Вирусов – компьютерных программ, которые многократно копируют сами себя, повреждают файлы или удаляют данные
 - Программы автоматической демонстрации или загрузки рекламы
 - Шпионских программ, которые секретно собирают информацию о пользователях компьютера
 - Других хакерских программ, таких как спам, программы перехвата информации, фишинг и др.
3. Программы фильтрации – предназначены для того, чтобы блокировать доступ учеников к запрещенным сайтам, например:
 - Сайтам социальных сетей и персональным почтовым ящикам, чтобы ученики не отвлекались от учебных заданий и не проявляли виртуальную агрессию
 - Фото- и видеохостингам, чтобы ученики не имели доступа к ненадлежащим

материалам

- Сайтам-файлообменникам, которые продвигают ненадлежащее использование информации, защищенной авторским правом, для предотвращения обмена пиратскими аудиофайлами
- Сайтам мгновенной передачи сообщений и микроблогам для профилактики жульничества, бездельничанья и злоупотребления общением со сверстниками.

4. Правила безопасного использования технологий – ученики и их родители обычно получают доступ к работе на компьютерах после того, как подписывают Правила безопасного использования технологий. В этих правилах описывается, как ученики должны работать на компьютере, защищать персональную информацию и действовать осторожно.

5. Памятки по безопасности – учителя часто развешивают памятки по безопасности в учебных классах и компьютерных лабораториях и распространяют их среди учеников и их родителей, чтобы регулярно напоминать им о правилах безопасного поведения в Интернете.

Защита личной информации учеников

Администрация образовательного учреждения должна заботиться о том, чтобы в соответствии с законом и этикой заботиться об информационной безопасности учащихся. Для защиты личной информации учеников можно использовать индивидуальные учетные записи и систему паролей, которые будут защищать данные от несанкционированного просмотра. Для ограничения доступа к информации пароли предоставляются только участникам совместной работы, школьным администраторам и родителям учеников.

Создайте индивидуальную учетную запись ученика (содержащую ограниченное количество информации) для пользования онлайн инструментами. Многие инструменты, применяемые в образовательных целях, требуют только регистрации учителя, а некоторые из них не требуют регистрации вовсе. Подбирайте инструменты, которые защищают личную информацию учеников.

Сообщение своего имени (без фамилии) при общении в Интернете не сопряжено ни с какими, если ученик не предоставляет никакой дополнительной информации. Использование реальных имен поможет вам выявлять отлично успевающих

учеников и тех, кто нарушает правила поведения. Для совместной работы в блогах и сайтах групп ученики могут использовать свое имя в сочетании с первой буквой фамилии. Внимательно изучите Правила использования ИКТ на предмет возможности сообщения имен.

Предупредите учеников об осторожности при предоставлении информации о себе или сверстниках в различных формах, опросах, исследованиях и электронных письмах. Если ученик сомневается в каком-то вопросе, ему следует спросить учителя.

Помимо мер безопасности, которые принимаются школой, ученики также должны четко знать, как вести себя в Интернете, чтобы избежать неприятностей. Каждый новый источник – это потенциальная угроза, а они появляются постоянно, и поэтому никакие меры безопасности не могут защитить учеников на 100%.

Безопасное поведение в Интернете

1. Знать, что делать – в процессе использования интернет вы должны:

- Иметь конкретный план работы и понимание того, что вы делаете
- Использовать эффективные стратегии поиска
- Использовать подходящие сайты для поиска изображений, звукозаписей, видео
- Защищать вашу персональную информацию (полное имя, место жительства, номер телефона и тому подобное)

2. Знать, кому можно доверять – все контакты через Интернет за пределами школы должны осуществляться с разрешения или при непосредственном участии учителя. Если у вас возникают какие-либо трудности в процессе общения, обсудите это с учителем

3. Знать, чего следует избегать – не рекомендуемые действия в Интернете:

- Переход на рекламные сайты
- Ответ на электронные письма или сообщения незнакомых людей
- Переход на ненадлежащие сайты
- Создание социальных закладок или обмен адресами ненадлежащих сайтов

4. Знать, как реагировать – если вы случайно перешли на ненадлежащий сайт, сообщите об этом своему учителю и выполните одно из следующих действий:

- Выключите монитор
- Закройте окно браузера
- Нажмите кнопку «Перейти на домашнюю страницу»

5. Осознавать последствия – если вы нарушаете правила безопасного поведения в Интернете, вы можете:

- Потерять права использования компьютера
- Повредить вирусами данные, хранящиеся на компьютере
- Потерять права совместной работы над проектом
- Получить выговор от руководства школы

Составлено на основе [материалов курса Intel «Методы сотрудничества в классе 21 века»](#)

Список рекомендуемой литературы

1. Журнал "Дети в информационном обществе" - новый издательский проект, осуществляемый с 2009 года Фондом Развития Интернет при научной поддержке факультета психологии МГУ имени М.В. Ломоносова и Федерального института развития образования Министерства образования и науки РФ. Периодичность - 4 раза в год. Выпуски №1-№7. [Ссылка](#).
2. Интерактивный курс "Основы безопасности детей и молодежи в интернете". ([Электронный ресурс](#))
3. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет. ([Электронный ресурс](#))
4. Роман Кравченко.Осторожно, интернет! IT - помощник.(Электронный ресурс). Режим доступа: <http://helpsnet.ru/ostorozhno-internet/>
5. Мошеннические сайты: как отличить сайт мошенников. [[Электронный ресурс](#)].
6. Детская безопасность в Интернете. [[Электронный ресурс](#)].
7. Интернет-угрозы: троллинг и кибербуллинг. [[Электронный ресурс](#)].
8. Смагулова Ш., Байтугелова Н., Наурызбаев Т. Информационная безопасность детей: Проблемы и пути решения./ Пособие для педагогов, психологов, родителей и всех заинтересованных сторон. - Астана, 2010. ([Ссылка](#)).
9. Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт. [[Электронный ресурс](#)].
- 10.Использование систем контентной фильтрации в школах. Методические и справочные материалы.([Ссылка](#))
- 11.Образовательно-выставочный проект "Дети в интернете". [[Электронный ресурс](#)].
- 12."Интернет: реальные и мнимые угрозы" (под научной редакцией и с комментариями Антона Серго, [электронный ресурс](#)).

ПРИЛОЖЕНИЯ

Приложение 1.

Требования к участникам телекоммуникационного проекта.

Под **учебным телекоммуникационным проектом** мы понимаем совместную учебно-познавательную, творческую или игровую деятельность учащихся-партнеров, организованную на основе компьютерной телекоммуникации, имеющую общую цель, согласованные методы, способы деятельности, направленную на достижение общего результата деятельности.

Специфика телекоммуникационных проектов заключается прежде всего в том, что они по самой своей сути всегда межпредметны. Организация телекоммуникационных проектов требует специальной и достаточно тщательной подготовки как учителей, так и учащихся.

От учителя требуется:

- умение увидеть и отобрать наиболее интересные и практически значимые темы проектов;
- владение всем арсеналом исследовательских, поисковых методов, умение организовать исследовательскую самостоятельную работу учащихся;
- переориентация всей учебно-воспитательной работы учащихся по своему предмету на приоритет разнообразных видов самостоятельной деятельности учащихся, на приоритет индивидуальных, парных, групповых видов самостоятельной деятельности исследовательского, поискового, творческого плана.

От учащихся требуется:

- знание и владение основными исследовательскими методами (анализ литературы, поиск источников информации, сбор и обработка данных, научное объяснение полученных результатов, видение и выдвижение новых проблем, выдвижение гипотез, методов их решения);
- владение компьютерной грамотностью, что предполагает: умение вводить и редактировать информацию (текстовую, графическую), пользование компьютерной телекоммуникационной технологией, обработку получаемых количественных данных с помощью программ электронных таблиц, пользование базами данных, распечатку информации на принтере;
- владение коммуникативными навыками;

- умение самостоятельно интегрировать ранее полученные знания по разным учебным предметам для решения познавательных задач, содержащихся в телекоммуникационном проекте;

**Что должен уметь ученик в области компьютерной
телекоммуникационной технологии:**

- умение войти в сеть;
- умение составить и отправить по сети письмо;
- умение "перекачать" информацию из сети на жесткий или гибкий диск и наоборот, с жесткого или гибкого диска - в сеть;
- структурировать полученные письма в специальной директории;
- входить в электронные конференции, размещать там собственную информацию и читать, "перекачивать" имеющуюся в различных конференциях информацию;
- пользоваться удаленными базами данных;
- входить в сеть Интернет и пользоваться ее услугами .

Таким образом, требования к участникам совместного проекта достаточно высоки.

Необходимо также определить **правила для групповой работы** и работы с партнерами, находящимися на расстоянии:

- доброжелательность при всех обстоятельствах;
- обязательность в выполнении всех заданий в оговоренные сроки;
- взаимопомощь в работе;
- тщательность и добросовестность в выполнении работы;
- полнейшее равноправие и свобода в выражении мыслей, идей.

Использованы материалы [сайта](#).

Приложение 2.

Образец согласия родителей для участия учащихся в сетевых проектах.

Уважаемые родители!

Как часть образовательной программы у Вашего сына или дочери будет

возможность публиковать документы и проекты в Интернете. Это может быть личная домашняя страница, сочинение, творческая работа, изображение, отчеты по исследовательской работе, фотографии учащихся класса (школы) или описания совместных проектов в местном масштабе или на международном уровне. Люди во всем мире с доступом в Интернет будут в состоянии рассмотреть и, возможно, ответить на работу Вашего ребенка по электронной почте. Мы считаем, что это — возможность дополнительного образования и успешного развития наших учеников.

Мы будем публиковать эти документы только с Вашего письменного разрешения.

Пожалуйста, ознакомьтесь с правилами размещения материалов учащихся в Интернете и отметьте публикацию каких документов нежелательно осуществлять с Вашей точки зрения. Спасибо за Ваше сотрудничество.

Размещая материалы учащихся, мы будем руководствоваться следующими правилами:

- Не разрешается издавать материалы с номером телефона Вашего ребенка, адресом или фамилией;
- Не разрешается издавать материалы, содержащие любую информацию, указывающую на местоположение ученика в точный час, кроме нахождения его в школе или участия в школьной деятельности;
- Не разрешается публикация материалов, содержащих нежелательный материал или содержащих прямые или косвенные ссылки на такой материал;
- Перед публикацией материалы должны быть рассмотрены и одобрены учителем (или родителем) ученика, осуществляющим работу над проектом.

Поставьте отметку в строке с материалами, которые нежелательны для публикации:

- _____ Имя учащегося
- _____ Личные фотографии учащегося
- _____ Школьные фотографии учащегося (с уроков и школьных мероприятий)
- _____ Групповые школьные фотографии

Разрешение родителя:

Я, _____ предоставляю разрешение
публиковать материалы моего сына/дочери/ _____ учени _____
_____ класса школы _____ г. _____ в Интернете в соответствии с
правилами, описанными выше.

Подпись родителя/опекуна: _____ Дата: _____

Это разрешение будет действительно до тех пор, пока Вы сами не захотите изменить эту форму и подписать новое разрешение. В случае возникновения проблем, связанных с публикацией материалов в Интернете, Вы можете связаться с классным руководителем своего ребенка _____.

Приложение 3.

Советы для родителей о работе детей в Интернете.

Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение по использованию Интернет.

Что могут делать дети в возрасте 5-6 лет?

Для детей такого возраста характерен положительный взгляд на мир. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

- В таком возрасте желательно работать в Интернет только в присутствии родителей;
- Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра;
- Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети;

- Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Ваши дети растут, а, следовательно, меняются их интересы.

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.

Что можно посоветовать в плане безопасности в таком возрасте?

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;
- Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса;
- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей;
- Научите детей не загружать файлы, программы или музыку без вашего согласия;
- Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

9-12 лет

В данном возрасте дети, как правило, уже слышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть,

прочитать, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;
- Не забывайте беседовать с детьми об их друзьях в Интернет;
- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет;
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.
- Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами;
- Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

13-17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются

электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

- Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения;
- Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни;
- Необходимо знать, какими чатами пользуются ваши дети;
- Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет;
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;
- Приучите детей не загружать программы без вашего разрешения;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.
- Расскажите детям о порнографии в Интернет;
- Приучите себя знакомиться с сайтами, которые посещают подростки;
- Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям;
- Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните что дети не могут играть в эти игры согласно закона.

Использованы материалы [сайта](#).

Приложение 4.

Советы педагогам при организации сетевой проектной деятельности с учащимся

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

Приложение 5.

Рекомендации по составлению мероприятий с обучающимися и родителями по основам культуры работы и информационной безопасности в сети Интернет.

№	Мероприятие	Ответственный	Помощник
1	Проводить с обучающимися занятия по повышению уровня их безопасности при работе в сети Интернет.	Ответственный за информационную безопасность в школе	Заместитель директора по воспитательной работе
2	Организовать проведение классных часов по тематике, раскрывающей правила безопасного поведения детей в сети Интернет.	Заместитель директора по воспитательной работе	Классные руководители
3	Организовать формирование и	Заместитель	Учащиеся-

	ведение специального школьного каталога «Мой безопасный интересный Интернет».	директора по воспитательной работе	тьютеры
4	Разработать подборку веб-ссылок на сайты сети Интернет (например, сайты профильных ВУЗов).	Учителя-предметники	
5	Составить и разместить на сайте ОУ памятку по вопросам культуры работы и информационной безопасности обучающихся в сети Интернет, которой смогут пользоваться учащиеся и их родители.	Ответственный за информационную безопасность в школе	Заместитель директора по воспитательной работе
6	Проводить разъяснительную работу по информационной безопасности детей в сети Интернет с привлечением специалистов.	Ответственный за информационную безопасность в школе	Представители МВД, прокуратуры, специалисты в области компьютерной коммуникации
7	На ежегодных родительских конференциях обсуждать вопросы информационной безопасности детей в сети Интернет. Организовывать обмен опытом между родителями по данному вопросу.	Заместитель директора по воспитательной работе	Классные руководители

Анкета для опроса родителей участников сетевого проекта

Уважаемые родители! Просим Вас принять участие в исследовании, связанном с реализацией проекта "НАЗВАНИЕ..." в Вашем образовательном учреждении. Опрос является анонимным, результаты исследования будут использованы только исследователями и только в обобщенном виде. Спасибо за участие в исследовании!

1. Впишите наименование ОУ, в котором учится Ваш ребенок.

2. Имеете ли Вы дома персональный компьютер?
 - да
 - нет
3. Подключен ли Ваш домашний персональный компьютер к сети Интернет?
 - да
 - нет
4. Как Вы считаете, позволяют ли Вашему ребенку полноценно дистанционно обучаться технические условия, создаваемые школой?
 - да
 - нет
 - затрудняюсь ответить
5. Я считаю, что участие моего ребенка в проекте «НАЗВАНИЕ...»... Продолжите предложение, выбрав несколько вариантов ответа
 - расширяет его знания по предмету
 - дает ему возможность пользоваться дополнительными образовательными ресурсами
 - способствует развитию большего интереса к предмету
 - дает возможность моему ребенку заниматься в соответствии с личностным особенностям (по индивидуальному плану)
 - не имеет отличий от обычных занятий в школе
 - вызывает дополнительные трудности в учебе
 - затрудняюсь ответить

6. Согласны ли Вы с утверждением, что дистанционное обучение позволяет учителю осуществлять индивидуальный подход к Вашему ребенку.
- да
 - нет
 - затрудняюсь ответить
7. Испытывает ли Ваш ребенок какие-либо трудности при дистанционном обучении? Если испытывает то, какие? Выберите не более трех вариантов ответа
- недостаточный уровень владения компьютером
 - не всегда понимает объяснение учителя
 - неумение быстро организовать свою деятельность
 - проблемы технического характера
 - затрудняюсь ответить
 - трудностей не испытывает
8. Изменилось ли эмоциональное состояние Вашего ребенка в условиях обучения с использованием дистанционного обучения?
- стал более спокоен, не переживает по поводу уроков
 - повысилось чувство тревожности из-за невыполненных уроков в дистанционном обучении
 - изменений нет
9. Хотите ли Вы, чтобы Ваш ребенок продолжил дистанционное обучение?
- да
 - нет
 - затрудняюсь ответить
10. Когда Ваш ребенок использует дистанционные образовательные технологии? Выберите несколько из списка.
- дома при подготовке домашнего задания
 - из дома на занятиях по школьному предмету под наблюдением учителя
 - только на занятиях в школе
 - затрудняюсь ответить
11. Приходится ли Вам помогать ребенку когда он готовит дистанционные задания?
- да

- нет

12. Мне нравится, что мой ребенок участвует в проекте «НАЗВАНИЕ...»

- да
- скорее да, чем нет
- скорее нет, чем да
- нет

Приложение 7.

Памятка для родителей

«Если Ваш ребенок участвует в создании проекта, какова Ваша роль?»

№	Этапы и под этапы проектной деятельности	Возможные воздействия родителей
1	Выдвигаются первоначальные идеи, и выбирается лучшая идея	Помогите ребенку выдвинуть как можно больше идей, записывайте их на листе бумаги вразброс, чтобы не выделять идеи порядком записи в столбце. Пусть идеи будут самыми разнообразными и дерзкими. Чем больше идей, тем больше выбор
2	Выбирается и формулируется тема проектной работы	Помогите выбрать лучшую идею и обосновать выбор
3	Формулируется задача проекта	Может потребоваться помощь в правильной формулировке
4	Разрабатываются планы и структура выполнения проекта	Помогите спланировать работу с учетом занятости вашего ребенка
5	Определяются сроки представления результатов (конечные и промежуточные), дорабатывается сама идея с учетом ее актуальности	Возможно, потребуется корректировка плана проектной работы с учетом особенностей личного расписания ребенка

6	Обсуждаются возможные результаты работы по теме проекта	Предположите, что у вас получится
7	Определяются и распределяются учебные задачи и устанавливаются сроки их	Разбейте объем работ на небольшие части и определите срок выполнения каждой
8	Составляются программа и календарный план выполнения работ	Скорректируйте план с учетом личной занятости ребенка. Содействуйте выполнению этого плана
9	Распределяются конкретные задания и обязанности между участниками проектной группы	Может потребоваться разъяснение обязанностей
10	Изучаются источники и литература по теме проекта	Посодействуйте ребенку в передвижении до библиотеки, обращайтесь его внимание в книжных магазинах на книги по теме проекта
11	Собирается и обрабатывается информация по проблеме	Посодействуйте в нахождении разнообразных источников информации. Источниками информации могут быть опрос, наблюдение, эксперимент, интервью, а также книги и периодические издания, Интернет. Если ребенок выбрал Интернет, не забудьте рассказать ему о правилах безопасного использования интернета
12	Готовятся выводы, которые сопоставляются с задачами проектной работы	Может потребоваться помощь в подготовке выводов, грамматический и стилистический контроль
13	Оформляются результаты работы, и готовится отчет	Подскажите основные правила оформления документов
14	Проект готовится к презентации	Помогите провести последнюю проверку перед презентацией,

		прорепетировать выступление, снять стресс перед выступлением
14	Проводится публичная презентация проектной работы	Присутствуйте на защите. Поддержите ребенка, у вас есть повод гордиться им
16	Анализируется работа, проделанная в течение проектного периода	Обсудите вашу совместную работу, подумайте, что можно было сделать по-другому
17	Оценивается работа проектной группы в целом и каждого участника в частности	Воспользуйтесь памяткой оценки проектной деятельности

Приложение 8.

Перечень интернет-ресурсов для работы педагога с учащимися и их родителями по информационной безопасности и организации сетевых проектов

1. Презентация “Правовое регулирование охраны и защиты прав несовершеннолетних. [Ссылка для скачивания](#).”
2. Презентация “Защита детей от информации, причиняющей вред их здоровью и развитию”. [Ссылка для скачивания](#)
3. Интерактивная игра для детей 7 - 10 лет “Джунгли Интернета”. [Ссылка](#).
4. Сказка о золотых правилах безопасности в Интернете. [Ссылка](#).
5. Презентация “Безопасность детей в интернете”. [Ссылка для скачивания](#).
6. Презентация: “Правила безопасности в Интернете”. [Ссылка для скачивания](#).
7. Разработка сетевого учебного проекта. [Ссылка для скачивания](#).
8. Методические рекомендации по организации и проведению сетевых игр по русскому языку и литературе. [Ссылка для скачивания](#).
9. Игра для учеников “День безопасности”. [Ссылка для скачивания](#).
10. Простые правила для детей об информационной безопасности (в стихах). Можно скачать брошюру. [Ссылка для скачивания](#).
11. Фильм “Интернет для начинающих пользователей. [Ссылка для скачивания](#).”

Приложение 9.

Перечень Интернет-сервисов, рекомендуемых для организации сетевых проектов

1. Сервис DocMe.ru - это бесплатный интернет-сервис для публикации, хранения и чтения документов различных форматов.
 - [Справка по освоению сервиса Docme.ru](http://DocMe.ru)
 - [Руководство новичка](http://DocMe.ru)
2. Сервис [ФОТОФИЛЬМ](http://Fotofilmi.ru) - онлайн сервис для создания красивых бесплатных слайд-шоу из Ваших фотографий
 - [Справка по освоению сервиса Fotofilmi.ru](http://Fotofilmi.ru)
3. [Сервис Imagechef](http://Imagechef.com) - создание мозаики из слов.
 - [Осваиваем Сервис Imagechef](http://Imagechef.com)
4. [Сервис Photovisi.com](http://Photovisi.com) - это бесплатный и легкий в использовании онлайн-инструмент создания фотоколлажей.
5. [Сервис Photo Peach](http://PhotoPeach.com) - потрясающие возможности для творческого представления своих работ.
 - [Справка по освоению сервиса Photo Peach.com](http://PhotoPeach.com)
6. [Сервис ПИКАСА](http://Picasa.com) - возможность загружать свои фотографии, публиковать их в Интернете без особого труда, создавать потрясающие веб-альбомы для друзей и родных или общедоступные альбомы, в которые может заглянуть каждый.
 - [Все функции Веб-альбомов Picasa](http://Picasa.com)
7. Интересный сервис [Photosnack](http://Photosnack.com) - позволяет «выйти» за рамки обычной открытки и устроить целое шоу с весёлой музыкой.
8. Сервис [TimeRime](http://TimeRime.com) позволяет расположить события, связанные с каким-либо событием в правильной последовательности и представить их в виде «ленты времени».
9. Сервис [MyPlick](http://MyPlick.com) позволит создать сборник стихов, украсить его иллюстрациями, вставить подходящую музыку.
10. [Яндекс.Видео](http://Yandex.Video) - сервис, позволяющий загружать и хранить собственные ролики (объем фильма не ограничен) - нужна регистрация в почте Яндекс.ру
11. [Графинг](http://Graphing.ru) - это бесплатный сервис создания и редактирования векторных и растровых изображений. С помощью онлайн-редактора вы можете прямо в окне браузера создать картинку и сохранить её копию на сервере в форматах: GIF, PNG, JPEG.
 - [Справка по освоению сервиса Graphing.ru](http://Graphing.ru)
12. [Сервис Muebook.com](http://Muebook.com) - отличный сервис для создания своеобразных мультимедийных «книг».

- [Справка по освоению сервиса Myebook.com](#)
- 13. [Сервис vuvoh.com для школ, позволяющий создавать интересные слайд-шоу](#)
 - [Инструкция по работе с сайтом vuvoh.com](#)
- 14. [doPDF](#) - это бесплатный PDF конвертер для использования в коммерческих и личных целях. Используя doPDF можно создавать PDF файлы, выбрав команду "Печать" из практически любого приложения. С помощью одного клика мышки можно создавать PDF файлы из документов формата Microsoft Excel, Word или PowerPoint, а также из электронной почты и ваших любимых веб-сайтов.