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 работе с родителями старших подростков
по вопросам информационной безопасности детей

Авторы-составители
команда “Созвездие “14”:

1. ***Сорокина Татьяна Владимировна*** **, воспитатель МБДОУ детский сад № 17 “Рябинушка” Ковровского района**
2. ***Павлова Надежда Вячеславовна,*** **заместитель директора по УВР, учитель физики МОУ ООШ №3 г. Камешково**
3. ***Кузицына Елена Васильевна,*** **учитель информатики МБОУ “Никологорская сош Вязниковского района”**
4. ***Федосеева Наталья Сергеевна,*** **учитель математки МБОУ “СОШ № 28” г. Владимир**
5. ***Байрамова Ольга Михайловна,*** **учитель русского языка и литературы МБОУ СОШ №19 г. Владимира**
6. ***Барабанова Наталья Евгеньевна*****, учитель математики и информатики МКОУ Курловской СОШ №2 Гусь-Хрустального района**
7. ***Зайцева Елена Михайловна*****, педагог-психолог и учитель технологии МОУ “Мошокская средняя общеобразовательная школа” Судогодского района**
8. ***Кузнецова Наталья Павловна*****, учитель математики МОУ СОШ № 4, г. Муром**
9. ***Лебедева Ольга Александровна*****, учитель биологии МБОУ “Головинская средняя общеобразовательная школа” Судогодского района**

2013 год

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Актуальность разработки данных методических рекомендаций

«Проблема обеспечения безопасности пользователей сети Интернет, защиты их от противоправного и агрессивного контента на сегодняшний день является весьма актуальной. К сожалению, в современном мире новые информационно-коммуникационные технологии помимо прогрессивного и инновационного начала несут в себе риск негативных воздействий. Тем важнее сейчас объединить усилия всех участников процесса информационного обмена – государства, бизнеса и гражданского общества – с целью построения безопасной интернет-среды, формирования позитивного контента, пропаганды «здорового» Интернета….»

Министр связи и массовых коммуникаций Российской Федерации

И.О. Щёголев, 23.03.2009

Стремительное развитие электронных средств информации и коммуникации заставляет задуматься над тем, как они влияют на образ жизни, воспитание и личностное становление подрастающего поколения.

Сегодня все больше и больше компьютеров подключаются к работе в сети Интернет. При этом все большее распространение получает подключение по высокоскоростным каналам как на работе, так и дома. Все большее количество детей получает возможность работать в сети Интернет.

Как правило, ребенка в сети Интернет привлекает возможность общения и игры. Виртуальная среда так же, как и реальный мир, имеет свои законы и правила поведения. Основную опасность представляет её глобальность и, как следствие, возможность общения ребенка не только со сверстниками, но и с личностями – потенциальными источниками разрушающего социального и психологического поведения. Одновременно опасность представляет анонимность собеседника. Поэтому, прежде чем отпускать ребенка в самостоятельное путешествие по бескрайним просторам Интернета, следует научить его основам безопасного и грамотного пользования сетью.

Цель методических рекомендаций: оказать методическую помощь педагогам, классным руководителям, педагогам дополнительного образования при организации работы с родителями старших подростков по информационной безопасности детей в части использования сети Интернет, которая сможет предупредить угрозы и сделать работу детей в Интернете полезной и безопасной.

Результатом использования данных методических рекомендаций должно стать овладение родителями опытом контроля деятельности детей в сети Интернет.

Решающим фактором безопасного поведения ребенка в Интернете является внимание со стороны родителей к проблеме взаимодействия ребенка с компьютерным миром вообще и сетью Интернет в

частности.

Педагогам необходимо обратить внимание родителей на эту специфическую проблему киберопасности, подчеркнуть важность участия родителей в безопасной коммуникации ребенка в сети и организовать периодические встречи, посвященные теме взаимодействия ребенка с сетью Интернет.

В старшем подростковом возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернете старшеклассники уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в сети Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей. Данные рекомендации научат производить соответствующие действия.

Новизна данных методических рекомендаций по сравнению с подобными разработками заключается в их доступном использовании всеми категориями родителей вне зависимости от уровня владения ИКТ. Они позволяют повысить компьютерную грамотность родителей по обеспечению информационной безопасности подростков в сети Интернет.

Данные методические рекомендации по вопросам информационной безопасности детей составлены для работы с родителями старших подростков и разработаны в рамках регионального телекоммуникационного проекта для педагогов, специалистов и руководителей всех видов ОУ "Методическая поддержка обеспечения информационной безопасности детей", проходившим в январе 2013 года на сайте "ВикиВладимир".

ОСНОВНЫЕ ТЕРМИНЫ И ПОНЯТИЯ

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

Аккаунт — запись, содержащая сведения о пользователе компьютерной сети.

Активная угроза — преднамеренное несанкционированное изменение состояния системы.

Антивирусная программа — программа, предназначенная для предотвращения доступа к персональному компьютеру вредоносных программ. Программа обнаруживает зараженные компьютерным вирусом файлы и удаляет их.

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

Баннер (англ. *banner* — флаг, транспарант) — графическое изображение рекламного характера, аналогичное рекламному модулю в прессе. Может быть как статичным изображением или даже текстом так и содержать анимированные элементы (вплоть до видео и интерактивных объектов). Как правило содержит гиперссылку на сайт рекламодателя или страницу с дополнительной информацией.

Блог (англ. blog, от web log — интернет-журнал событий, интернет-дневник, онлайн-дневник) — веб-сайт, основное содержимое которого — регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа.

Веб-образователь, браузер, (от англ. Web browser) — программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц (преимущественно из Сети), их обработки, вывода и перехода от одной страницы к другой.

Веб-портал (от англ. *Web portal* или англ. *Portal* , «главный вход») — это совокупность взаимосвязанных непосредственно и через сеть «Интернет» аппаратных средств, включающих компьютеры и машиночитаемые электронные носители информации с заранее записанной на них информацией и/или выполненные с возможностью записи и считывания информации в виде компьютерных программ, баз данных и т. п., выполненная с возможностью обработки указанной информации и команд пользователя веб-портала и предоставления ему Интернет-сервисов как результатов обработки указанных информации и команд.

Видиохостинг — сайт, позволяющий загружать и просматривать видео в браузере, например через специальный проигрыватель.

Вирус — вредоносная программа, которая распространяется, копируя себя в другие программы. Вирус может распространяться через файлы, сообщения электронной почты или веб-страницы. Компьютер может заразиться вирусом во время работы пользователя в Интернете или при открытии вложений электронной почты. Вирусы могут снизить работоспособность компьютера или системы.
http://laste.arvutikaitse.ee/rus/html/ope_sanasto.htm

Вишинг — разновидность фишинга, распространенным сетевым мошенничеством, когда клиенты

какой-либо платежной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п. При этом ссылка в сообщении ведет на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в Интернете достаточно сложно

Вредоносное ПО (malware – сокращение от malicious software) – это различные программы, которые могут наносить вред. Вредоносное ПО – это любая нежелательная программа, которая устанавливается на компьютере без вашего ведома. вирусы, черви и троянские кони – это примеры вредоносных программ, которые часто совокупно называются вредоносным ПО.

http://www.microsoft.com/ru-ru/security/resources/malware-whatis.aspx

Всплывающее окно — новое окно, которое открывается поверх активного окна обозревателя Интернета. Как правило, такое окно не содержит видимого веб-адреса. Во всплывающих окнах, которые открываются без запроса пользователя, обычно содержится реклама.

Гейминг (gaming) — означает занятие какой-то игрой с помощью видеоприставки, в Интернете или на компьютере.

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. http://exerising.ru/glossarij

Интернет-мошенничество или кибермошенничество — это один из видов киберпреступления, целью которого является обман пользователей.

Кибербуллинг (cyber-bullying) — это виртуальный террор, чаще всего подростковый.

Контент — (от английского content - содержание) – это абсолютно любое информационно значимое, содержательное наполнение информационного ресурса или веб-сайта. Контентом называются тексты, мультимедиа, графика.

Социальная сеть (от англ. social networking service) — платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений.

Нигерийские письма — распространенный вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама).

Загрузка — сохранение файлов из Интернета на собственном компьютере.

Защита данных — набор правил, которые обеспечивают сохранение конфиденциальности информации. Безопасность данных распространяется на конфиденциальную информацию, например, личную информацию, и поддерживается политикой информационной безопасности или заявлением о конфиденциальной информации.

«Защитник», «защитная» программа, фаервол, брандмауэр — программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельным компьютером. Например, с помощью настройки фаервола по правилам можно запретить некоторым или всем программам выходить в Интернет. Можно настроить фаервол на запрет запуска скриптов при просмотре страниц в Интернете.

Злоумышленник — лицо, осуществляющее осознанные действия по нарушению информационной безопасности объекта защиты. http://www.z-it.ru/usefull-information/glossary

Интернет цензура — контроль и пресечение публикации или доступа к информации в сети Интернета.

Информационная безопасность — политика мер, реализуемая для обеспечения контроля над рисками информационной стабильности и безопасности.

Интерне́т-зави́симость (или Интернет-адди́кция) — навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета.

Интернет-цензура — контроль и пресечение публикации или доступа к информации в сети Интернета. http://ru.wikipedia.org/wiki/Интернет-цензура

Информационная безопасность информационной 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.

Информационный ресурс — в широком смысле - совокупность данных, организованных для эффективного получения достоверной информации.

Кибербуллинг — агресивное, умышленное действие,совершаемое группой лиц или одним лицом с использованием электронных форм контакта, повторяющееся неоднократно и продолжительное во времени в отношении жертвы, которой трудно защитить себя.

Логин — имя (идентификатор) учётной записи пользователя в компьютерной системе или процедура входа (идентификации и затем аутентификации) пользователя в компьютерную систему, как правило, путём указания имени учётной записи и пароля.

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа.
http://ru.wikipedia.org/wiki/%CC%E5%E6%F1%E5%F2%E5%E2%EE%E9_%FD%EA%F0%E0%ED

Опасные программы: вирусы, черви и трояны — программа или часть программы, которая предназначена для распространения нежелательных событий в компьютерной или информационной системе, например, подбор паролей, уничтожение компьютерных данных. Обладают возможностями по самостоятельному распространению себя в Сети путем копирования.

Операционная система — главная программа, которая работает «между» компьютером и прикладным программным обеспечением. С помощью операционной системы компьютер управляет установленным программным обеспечением, а также контролирует и использует его. К распространенным операционным системам относятся семейства программ Microsoft® Windows®, Apple® Mac OS и Linux®. Под словом «семейство» подразумевается выпуск новых версий программ.

Пароль — это секретное слово или набор символов, предназначенный для подтверждения личности или

полномочий. Пароли часто используются для защиты информации от несанкционированного доступа. В большинстве вычислительных систем комбинация «имя пользователя — пароль» используется для удостоверения пользователя.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе:

- его фамилия, имя, отчество,
- год, месяц, дата и место рождения,
- адрес, семейное, социальное, имущественное положение, образование, профессия, доходы,
- *другая* информация

Почта; электронная почта; сообщение электронной почты — электронная передача текста или мультимедийной информации между компьютерами.

Провайдер – фирма, предоставляющая услуги по подсоединению к некоторой глобальной компьютерной сети, в частности к Интернет

Риск — это вероятность того, что источник угрозы воспользуется уязвимостью, что приведет к негативному воздействию. Например, риск потери доступности информационной системы; риск потери конфиденциальности данных.

Резервное копирование (англ. *backup*) — процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

http://ru.wikipedia.org/wiki/%D0%E5%E7%E5%F0%E2%ED%EE%E5_%EA%EE%EF%E8%F0%EE%E2%E0%ED%E8%E5

Родительский контроль — это программы и службы, которые позволяют родителям и опекунам отслеживать, как ребенок использует компьютер: от фильтрации веб-содержимого и управления контактами электронной почты до ограничений на общение через Интернет. Цель таких средств – обеспечить безопасность ребенка в Интернете, и эти инструменты иногда называют семейными настройками и настройками семейной безопасности.

Сайт – специальным образом оформленные данные о каком-либо предмете или явлении и хранящиеся на WWW-сервере, т. е. это программа, которая интерпретируется как текст, графика, анимация, звук,…

Санкционированный доступ – доступ к данным или к элементам сети, разрешенный уполномоченным лицом

Сервер — программа, которая распределяет файлы по компьютерам в сети на основе предварительно заданных правил. Например, в Интернете пользователи получают сообщения электронной почты от сервера электронной почты сети. Сервером часто называют компьютер, на котором установлена серверная программа.

Серфинг — просмотр содержания интернет-страниц.

Сетевой дневник или блог — общественный интерактивный дневник, расположенный в сети Интернет, имеющий возможность открытого и ограниченного доступа.

Сетевой этике́т (нетикет) — правила поведения, общения в Сети традиции и культура интернет-сообщества, которых придерживается большинство. http://ru.wikipedia.org/wiki/Сетевой_этикет

Скайп — специальная программа, наиболее часто используемая в Интернете для организации голосовой связи. Имеет дополнительные возможности текстового и видео общения, посылки файлов.

Социальная сеть (от англ. social networking service) — платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений.

Спам — нежелательная электронная почта, которая, как правило, рассылается в целях прямой почтовой рекламы и других предложений коммерческого характера. Спам почти всегда единовременно рассылается большому кругу получателей.

Трафик - объем данных в байтах, проходящий через сервер за определенный период времени.http://book.majordomo.ru/article/4/

Учётная запись — запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе. Как синонимы в обиходе могут использоваться разг. *учётка* и сленговые варваризмы *акк*, *акка́унт* и *экка́унт*, от англ. *account* — учётная запись, личный счёт.

Файлообменник, файлхостинг или файловый хостинг — сервис, предоставляющий пользователю место под его файлы и круглосуточный доступ к ним через web, как правило по протоколу http. Такой сервис позволяет удобно «обмениваться» файлами.
http://ru.wikipedia.org/wiki/%D4%E0%E9%EB%EE%EE%E1%EC%E5%ED%ED%E8%EA

Фильтр — специальный алгоритм поисковых систем, позволяющий исключить из выдачи результатов сайты, уровень ранжирования которых был поднят искусственными методами.

Фишинг – это вид хищения персональных данных через Интернет. При этом используются сообщения электронной почты и мошеннические веб-сайты, цель которых – украсть ваши личные данные или информацию, такую как номера кредитных карт, пароли, данные учетной записи и другую информацию.
http://www.microsoft.com/ru-ru/security/online-privacy/phishing-scams.aspx

Форум — место обсуждения в Интернете, часто посвященное определенной теме. Здесь люди могут оставлять сообщения в интерактивном режиме, отвечать на чужие сообщения, используя форматы, указанные поставщиком данной услуги. Для некоторых дискуссионных форумов требуется регистрация. В некоторых форумах имеется архив, который можно использовать для поиска определенной темы. Некоторые форумы контролируются администратором,который имеет право удалять и редактировать любые размещенные сообщения или запрещать доступ для пользователей, которые оскорбляют своих собеседников.

Френд — дословный перевод с английского – друг. В социальных сетях – участник этой же сети, которому можно присвоить статус «френд», после чего у него появляются дополнительные возможности для чтения закрытых для других сообщений и другие возможности.

Хакер, взломщик — человек, взламывающий информационные сети или системы организации, либо использующий их без разрешения. В последнее время основное распространение получили не физические персонажи, взламывающие компьютерные программы и сети, а написанные этими хакерами программы,

которые автоматически, без непосредственного участия человека, осуществляют взлом, подбор паролей, уничтожение или порчу компьютерной информации и другую нежелательную и несанкционированную деятельность.

Чат, чаттер (англ. *chatter* — болтать) — средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение. http://ru.wikipedia.org/wiki/%D0%A7%D0%B0%D1%82

Электронное сообщение — информация, переданная или полученная пользователем инфрмационно-телекоммуникационной сети http://4systems.ru/topics/Dictionary

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

1. **Acc - "Account"** - учетная запись.
2. **IP-адрес** (*айпи-адрес*, сокращение от англ. *Internet Protocol Address*) — сетевой адрес узла в компьютерной сети, построенной по протоколу IP. В сети Интернет требуется глобальная уникальность адреса; в случае работы в локальной сети требуется уникальность адреса в пределах сети. В версии протокола IPv4 IP-адрес имеет длину 4 байта.
3. **USB** (*ю-эс-би,* англ. *Universal Serial Bus* — «универсальная последовательная шина») — последовательный интерфейс передачи данных для среднескоростных и низкоскоростных периферийных устройств в вычислительной технике.
4. **FAQ** - „Frequently Asked Questions" - Часто задаваемые вопросы, в рунете вариант: "ЧАВО"
5. **FTP** (англ. *File Transfer Protocol* — протокол передачи файлов) — стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). FTP часто используется для загрузки сетевых страниц и других документов с частного устройства разработки на открытые сервера хостинга.
6. **HTTP** (англ. *HyperText Transfer Protocol* — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов).
7. **URL** — единый указатель ресурсов (англ. *URL — Uniform Resource Locator*) — единообразный локатор (определитель местонахождения) ресурса.
8. **HTML** (от англ. *HyperText Markup Language* — «язык разметки гипертекста») — стандартный язык разметки документов во Всемирной паутине. Большинство веб-страниц создаются при помощи языка HTML (или XHTML). Язык HTML интерпретируется браузерами и отображается в виде документа в удобной для человека форме.
9. **ICQ** (англ. *I seek You* — «я ищу тебя») — централизованная служба мгновенного обмена сообщениями сети Интернет, в настоящее время принадлежащая инвестиционному фонду Mail.ru Group (Россия).
10. **SEO** (сокр. Search engines optimization) - поисковая оптимизация сайта с целью получения высоких мест в результатах поиска по заданным запросам.
11. **WWW** (англ. *World Wide Web*) — распределенная система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к Интернету.
12. **НСД -** несанкционированный доступ.
13. QIP (Quiet Internet Pager) — бесплатная программа мгновенного обмена **с**ообщениями по протоколу OSCAR, во многом аналогичная программе ICQ.
14. **ПД** — передача данных
15. **ПК** (англ. *personal computer, PC*) персональный компьютер, — компьютер, предназначенный для эксплуатации одним пользователем, то есть для личного использования. К ПК условно можно отнести также и любой другой компьютер, используемый конкретным человеком в качестве своего личного компьютера.

16. **DRM** — защита произведений от копирования и других действий, запрещаемых авторами или иными правообладателями на основании авторского или смежных прав. Термин «технические средства защиты авторских прав» используется в законодательстве Российской Федерации, запрещающем обход таких средств. «DRM» — аббревиатура от английского выражения «digital rights management», слова которого по отдельности переводятся как «цифровой», «права́», «управление».
17. **ПО -** программное обеспечение
18. **CMS** - (Content Management System система управления содержимым) — информационная система или компьютерная программа для обеспечения и организации совместного процесса создания, редактирования и управления контентом.
19. **CSS** (англ. *Cascading Style Sheets* — каскадные таблицы стилей) — формальный язык описания внешнего вида документа, написанного с использованием языка разметки. Преимущественно используется как средство описания, оформления внешнего вида веб-страниц, написанных с помощью языков разметки HTML и XHTML, но может также применяться к любым XML-документам, например, к SVG или XUL.
20. **URI** (англ. *Uniform Resource Identifier*) — унифицированный (единообразный) идентификатор ресурса. На английский манер произносится как [*ю-ар-а́й*], по-русски чаще говорят [*у́ри*]. URI — это последовательность символов, идентифицирующая абстрактный или физический ресурс. Ранее назывался Universal Resource Identifier — универсальный идентификатор ресурса.
21. **Akey** - это новая и очень полезная программа, при использовании которой Вы совершенно забудете о том, как рыскали в поисках ключей для вашего антивируса или любой другой программы.
22. **TBB** - Tor Browser Bundle - программа помогает вам защититься от различного рода сетевой слежки, угрожающей личной свободе и частной жизни, конфиденциальной профессиональной деятельности и отношениям, а так же обезопаситься от деятельности органов государственной безопасности, известной под названием анализ трафика. Сервис Tor защищает вас путем переадресации ваших коммуникаций через распределенную сеть ретрансляторов, предоставляемых волонтерами по всему миру: это не оставляет отслеживающему ваше Интернет соединение возможности, узнать какие сайты вы посещали, а посещаемым вами сайтам - узнать ваше физическое местоположение.

Нормативно-правовые основы информационной безопасности детей

МЕЖДУНАРОДНЫЙ УРОВЕНЬ

1. "ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В МЕЖДУНАРОДНОМ ЗАКОНОДАТЕЛЬСТВЕ" (С.А. Буданов) ("Общество и право", 2008, № 1) http://www.recoveryfiles.ru/laws.php?ds=3062

ФЕДЕРАЛЬНЫЙ УРОВЕНЬ

1. Письмо Минобразования РФ от 13.08.2002г №01-51-088ин "Об организации использования информационных и коммуникационных ресурсов общеобразовательных учреждений" http://www.zakonprost.ru/content/base/7095/
2. Федеральный закон от 13.03.2006 N 38-ФЗ (ред. от 18.07.2011) "О РЕКЛАМЕ" http://zakonprost.ru/zakony/o-reklame/
3. Федеральный закон Российской Федерации о защите персональных данных от 27 июля 2006 года №152-ФЗhttp://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html
4. Федеральный закон российской Федерации от № 63-ФЗ "Об электронной подписи" http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=132463
5. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
6. Закон о мерах по защите нравственности и здоровья детей во Владимирской области. Принят постановлением Законодательного Собрания Владимирской области от 20 декабря 2006 года N 761 (в ред. Законов Владимирской области от 10.08.2009 N 107-ОЗ, от 30.12.2009 N 192-ОЗ) http://pravarebenka33.ru/company/law_quot_on_measures_to_protect_children_39_s_health_and_morality_in_e_vladimir_region_quot.php
7. Федеральный закон от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (с изменениями и дополнениями) http://base.garant.ru/12181695/
8. Федеральный закон Российской Федерации от 28 декабря 2010 г. N 390-ФЗ "О безопасности"
9. Федеральный закон Российской Федерации 21.12.2010г. № 436 - ФЗ г.Москва "О защите детей от информации, причиняющий вред их здоровью и развитию" (принят ГД РФ 21.12.2010г //Парламентская газета 2011.3 января) http://www.rg.ru/2010/12/31/deti-inform-dok.htm
10. Федеральный закон Российской Федерации от 25 июля 2011 г. N 261-ФЗ г. Москва "О внесении изменений в Федеральный закон "О персональных данных"
11. Закон РФ "Об образовании" № 273- ФЗ http://www.eduhelp.info/page/federalnyj-zakon-ob-obrazovanii-v-rossijskoj-federacii-podpisal-putin

12. Федеральный закон о защите детей от информации, причиняющей вред их здоровью и развитию (в ред. Федерального закона от 28.07.2012 N 139-ФЗ)
    http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=133372;fld=134;dst=4294967295;rnd=0.3
    871055679395795;from=108808-0
13. Указ Президента Российской Федерации от 1 июня 2012 года “О национальной стратегии действий в интересах детей на 2012-2017 годы” http://base.garant.ru/70183566/
14. Федеральный закон (проект) о внесении изменений в отдельные законодательные акты Российской Федерации по вопросам регулирования отношений при использовании информационно-телекоммуникационной сети Интернет.
    http://i-deti.org/upload/iblock/3de/lbi-110921133142-phpapp02.pdf
15. Федеральный закон «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию»
    http://clck.ru/4b47M

РЕГИОНАЛЬНЫЙ УРОВЕНЬ

1. Постановление Губернатора Владимирской области от 9 августа 2012 г. N 888 "Об утверждении долгосрочной целевой программы "Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2013 - 2015 годы" http://www.garant.ru/hotlaw/vladimir/416211/

ШКОЛЬНЫЙ УРОВЕНЬ

1. Локальные акты:
   Положение об электронной почте http://kurasovka.narod.ru/document/ob_elektronnoi_poshte.pdf“
   Положение о сайте ОУ” http://www.maaam.ru/stati-polzovatelei/polozhenie-o-saite-dou.html
2. Типовые правила использования сети Интернет в общеобразовательном учреждении
   http://do.gendocs.ru/docs/index-303579.html?page=8#900859

Теоретические основы

Для реализации своего социального поведения в обществе ребенок нуждается в постоянном притоке информации. Постоянная информационная связь с окружающим миром, социальной средой, в которой он действует как активный социальный субъект, является одним из важнейших условий нормальной жизнедеятельности.

Но на ребенка оказывают огромное влияние не только постоянный информационный контакт с окружающей социальной средой или его отсутствие, но и количество, объем, содержание и структура поступающей и перерабатываемой информации. **Информационно-коммуникативные процессы могут таить в себе опасности,** представляющие реальную угрозу для развития личности и общества в целом. Условия кардинального реформирования российского общества качественно изменили взаимоотношения между людьми, выдвинув отношения соревновательности, конкуренции и борьбы на ведущее место в системе социальных отношений. Причем это отразилось на всех уровнях социального взаимодействия - от межличностного общения, до массовой коммуникации. Отношения конкуренции наряду с позитивным их влиянием на повышение инициативы и активности значительной части населения привели также к массовому использованию способов и приемов информационно-психологического воздействия. Манипулирование людьми, использование различных средств и технологий информационно-психологического воздействия стало достаточно обычным явлением в повседневной жизни, экономической конкуренции и политической борьбе. Таким образом, понимание угроз информационно-психологической безопасности личности, механизмов их действия и возможностей психологической защиты становится не только теоретической проблемой, но и насущной потребностью социальной практики и повседневной жизни человека.

Личность ребенка, включенная в процесс познания, оказывается незащищенной от потоков информации, в связи с чем возникает острая необходимость расширения содержания общего среднего образования, введения в него новых компонентов, связанных с обучением информационной безопасности.

Многочисленными исследованиями доказано, что из многообразных факторов риска к наиболее ***распространенным и разрушительным для физического, психического и нравственного здоровья школьников*** относятся некоторые разновидности **компьютерных игр** и **непродуктивное использование**

ресурсов Интернет. К объективным предпосылкам причинения такого рода ущерба детям и молодежи являются расширение доступа к ресурсам Интернет, наличие на рынке компьютерных программ дешевых компакт-дисков с играми разнообразного содержания.

Угроза компьютерных игр весьма реальна. Многие современные компьютерные игры, предназначенные для детей и молодежи, наводнены монстрами, палачами, скелетами, приведениями, чудовищами, людоедами и т.д. При помощи компьютера натуралистично воспроизводятся лужи крови и мозги на стенах, жуткие вопли и скрежет ломаемых костей, оторванные головы и летящие куски окровавленной плоти. Движущиеся под музыку образы на цветном экране оказывают на игроков гипнотический эффект. В ходе игр подростки имитируют действия убийц, преступников: убивают десятками, калечат, расчленяют тела персонажей игр. Под предлогом борьбы со злом дети программируются на жестокость и садизм. Смысл многих игр сводится к убийству, совершению преступлений разного рода. Ребенок приобщается к реалиям криминального мира. Иные игры фактически предполагают многократную имитацию самоубийства в сюжетах со смертельными трюками на гоночных автомобилях, мотоциклах, самолетах. Под влиянием страшных образов дети начинают пугаться темноты, жалуются на кошмарные сны, боятся оставаться в комнате без взрослых. Игроки находятся в состоянии «пассивного возбуждения», при котором удовольствие достигается без усилий, что оказывает расслабляющее влияние на личность, действует как наркотик. У детей создается ощущение собственного всемогущества.

Увеличивается время, затрачиваемое на компьютерные игры. Реальные дела забываются, жизненные проблемы не решаются. У некоторых подростков появляются признаки компьютерной наркомании. Нарушается общение со сверстниками, утрачиваются контакты с близкими. При отсутствии возможности играть на компьютере у заядлых игроков начинается типичная «ломка».

Постепенно меняется поведение компьютерных игроков в реальной жизни. Учеба, общение, спорт, искусство занимают в их жизни все меньшее место. Притязания детей возрастают, а готовность к преодолению трудностей не совершенствуется. Формируется аддиктивное поведение, для которого характерно стремление к уходу от реальности путем изменения своего психического состояния посредством определенных видов деятельности или приема некоторых веществ. Многообразные формы аддиктивного поведения объединяет общее аддиктивное звено – стремление к искусственному изменению психического состояния, вызыванию субъективно приятных эмоций. Причем аддикты могут легко переходить от одной формы аддикции к другой, например от Интернет-зависимости к зависимости от алкоголя или наркотиков.

Дети не видят угрозы, которую несет в себе глобальная сеть. Согласно статистике 9 из 10 детей в возрасте от 8 до 15 лет сталкивались с порнографией в сети, около 17% регулярно подключаются к запретным ресурсам, 5,5% готовы претворить увиденное там в жизнь.

Дети уже привыкли использовать всемирную сеть как основной источник общения. Характерно, что в большинстве случаев **интернет-общение захватывает именно те личности, которые испытывают дефицит общения в реальной жизни** и не имеют сложившихся ярко выраженных стереотипов общения.

Взгляды на межличностное взаимодействие у такого человека будут формироваться на основе сетевого, а не реального опыта. И, следовательно, неизбежен неосознанный перенос этого опыта на общение в повседневной жизни.

В среде подростков со скоростью пожара распространяется увлечение веб-журналами (или, иначе говоря, блогами), которые порой ведут Интернет-дневники без ведома взрослых. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

При этом все больше молодых пользователей создают собственные дневники, и каждый стремится привлечь как можно больше внимания аудитории. Иногда это приводит к тому, что дети размещают в блогах такой неуместный материал, как провокационные фотографии и видеоролики – свои или друзей.

Также одним из распространенных факторов риска является ***мошенничество и преступления в Интернете.*** В России мошенничество с помощью Интернета или хищения данных кредитной карты еще не стали очень широко распространены. Однако мы можем стоять на пороге этого явления, и нужно сделать так, чтобы оно не застало нас врасплох.

Среди Интернет-мошенничества широкое распространение получила применяемая хакерами техника «phishing», состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

Кроме того, если вы сами или ваши дети пользуетесь кредитной картой для оплаты товаров и услуг через Интернет, по телефону или даже лично в соседнем магазине, вы уязвимы для мошенников.

При любой операции оплаты с использованием кредитной карты компании должны проверить информацию о счете, прежде чем предоставить товары или услуги. Данные о кредитных картах хранятся на крупных серверах. К сожалению, хакеры могут взломать такую систему и завладеть информацией, чтобы воспользоваться ею в корыстных целях, например, оплачивать свои счета, используя деньги с вашей карты.

Преступления в Интернете заключаются в том, что преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут

действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

С умыслом или без умысла дети могут заняться онлайновым пиратством –незаконным копированием и распространением (как для деловых, так и для личных целей) материалов, защищенных авторским правом (например, музыки, фильмов, игр или программ) без разрешения правообладателя.

Перечисленное многообразие рисков при отсутствии условий информационной безопасности не позволит ребенку полноценно развиваться, своевременно адаптироваться к меняющимся социальным условиям и организовывать свое поведение (жизнедеятельность), позволяющее удовлетворять основные потребности в обществе в социально приемлемых формах с учетом интересов других людей и действующих социальных институтов.

Логично предположить, что отследить всю информацию, попадающую в интернет, невозможно, как невозможно предвидеть может ли ребенок случайно зайти на сайт, где ему рекомендуют употребление наркотиков, алкоголя, изготовление взрывчатки. Ребенок, находясь в сетевых ресурсах, вынужден во всплывающем рекламном окне видеть фотографию обнаженного тела. Согласно нашим исследованиям, педагоги и родители не понимают и не предвидят всей опасности, исходящей от интернета. Между тем, ребенок может войти в сатанинские культы, сетевые «оргии», причем принимать участие в их собраниях, сидя дома за компьютером, намного легче.

Поэтому, информационную безопасность личности школьника целесообразно рассматривать как состояние защищенности от действия многообразных информационных факторов, препятствующих или затрудняющих формирование и функционирование адекватной информационно-ориентировочной основы социального поведения человека и в целом жизнедеятельности в современном обществе.

Информационная безопасность - проблема не только социальная (конкуренция СМИ, возрастающая роль интернета, отсутствие цензуры и т.д.), но и педагогическая, потому что ее решение напрямую зависит от уровня и качества образованности подрастающего поколения, от степени зрелости личности и ее готовности к самореализации в обществе. **Один из возможных путей решения проблемы информационной безопасности - обучение ребенка адекватному восприятию и оценке информации, ее критическому осмыслению на основе нравственных и культурных ценностей.**

В условиях современной школы возможно создать условия для овладения детьми навыками информационной безопасности. Однако, реально использовать свои навыки ребенок будет только в том случае, если у него есть для этого положительный пример - родитель. Поэтому нераздельно с обучением детей навыкам информационной безопасности, необходимо проводить и просвещение родительской общественности в этом вопросе. Школьникам и их родителям необходимо знать о том, что в виртуальном мире существует целый свод правил, которыми нужно руководствоваться при работе и общении в сети. Незнание, неумение использовать основные нормы поведения (в принципе, похожие на те, которыми мы руководствуемся в обычной жизни), приводит к тому, что подростки демонстрируют в виртуальном пространстве асоциальное поведение, а то и совершают правонарушения в сфере ИКТ. Кажущаяся безнаказанность, анонимность, доступность приводит к таким поступкам, на которые в реальном мире

большинство детей не способны. Причем многие из них даже не задумываются о том, что данные действия могут нанести реальный моральный, экономический, или даже физический вред тому, против кого они направлены. Только совместными усилиями возможно создать безопасную Интернет - среду для наших детей.

Содержание

Стремительное развитие компьютерных технологий качественно меняет окружающую жизнь и порождает множество проблем, в частности, проблему формирования информационной культуры и безопасности среди старших подростков.

Существуют различные мнения о том, когда нужно давать детям доступ в Интернет. Зарубежные специалисты сходятся в том, что запрет на Интернет может быть действенным только до тех пор, пока это не ограничивает потребности ребенка в сфере образования. Современные школы уже подключены к Интернет, и преподавание информатики начинается со второго класса. Почти каждый подросток имеет доступ к Интернет либо с домашнего компьютера, либо с сотового телефона. Компьютер и Интернет, как всякие сложные технологические продукты, наряду с неоспоримыми преимуществами могут нанести серьезный вред подростку. Одним из главных вопросов, связанных с компьютеризацией, является изучение влияния компьютера на организм, психическое состояние и развитие ребенка..

При современном уровне развития техники вредными для детей и, вообще, пользователей любых возрастов, являются скорее не излучения, а умственное и нервное переутомление.

Вот выдержка из аннотации к книге Заряны и Нины Некрасовых «***Как оттащить ребенка от компьютера и что с ним делать***», вышедшей в издательстве «София»:

«*Дети и подростки прирастают к розетке тогда, когда реальный мир не может предложить им других полноценных занятий. Не надо бороться с компьютером, борьба не укрепляет семьи. Надо просто понять истинные потребности своих детей - и найти в себе силы и время общаться, играть, слушать их. Просто посмотреть на все (в том числе и на компьютеры, ТВ, мобильник, плеер и прочие розеточные изобретения) глазами детей и подростков. И тогда виртуальный мир станет помощником вашей семье, для чего он, собственно, и предназначен».*

Родители должны помнить, что ребенок проходит в своем психологическом развитии определенные стадии, которые достаточно сильно отличаются друг от друга. Это также отражается и на интересах детей при работе в Интернете. Родителям важно знать, какие особенности имеют дети в том или ином возрасте, для того чтобы правильно расставлять акценты внимания при своих беседах с детьми о правилах безопасности в Интернете.

Кроме того, нужно учитывать, что наши дети начинают осваивать Интернет в разном возрасте: кто-то в возрасте 14 – 17 лет, находясь в старших классах, кто-то в 10 – 13 лет, а кто-то еще в дошкольном возрасте получает первый опыт взаимодействия с Интернетом.

Подростки, как правило, проходят через период низкой самооценки; ищут поддержку у друзей и не охотно слушаются родителей. Более старшие ищут свое место в мире и пытаются обрести собственную независимость; в то же время они охотно приобщаются к семейным ценностям. В этом возрасте подростки уже полноценно общаются с окружающим миром. Они бурлят новыми мыслями и идеями, но испытывают недостаток жизненного опыта. Родителям важно продолжать следить, как используют Интернет их дети в этом возрасте.

В этом возрасте дети уже наслышаны о том, какая информация существует в Интернете. И совершенно нормально, что они хотят все это сами увидеть, услышать, прочесть. Доступ к нежелательным материалам (например, порнографическим картинкам или инструкциям по изготовлению взрывчатки) можно легко заблокировать при помощи программных фильтров.

Они скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Кроме того, подростки активно используют поисковые машины. Большинство пользовалось чатами, и многие общались в приватном режиме. Мальчики в этом возрасте склонны сметать все ограничения и жаждут грубого юмора, крови, азартных игр и картинок для взрослых. Девочкам больше нравится общаться в чатах; и юные дамы более чувствительны к сексуальным домогательствам в Интернете.

Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее участие взрослых тоже необходимо. Особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и ребенком. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Родители должны также помнить о необходимости хранить свои пароли в секрете, чтобы подростки не смогли

зарегистрироваться под именем старших.

Взрослым важно помнить, что даже самые искушенные дети не видят опасностей Интернета и не осознают рисков его использования. Проблема заключается в том, что у детей еще не сформированы критерии различия. Ребенку, в силу особенностей его психологического развития, интересно все. Оставить ребенка один на один с компьютером в Интернете, это все равно, что бросить его одного на улице большого и незнакомого города. Когда ребенок часами сидит один за компьютером, происходит почти тоже самое - скорее всего, он слоняется по виртуальным улицам и подворотням. Поэтому родители и педагоги, сначала сами должны научиться азам компьютерной безопасности, а потом научить этому своих детей.

Для этого нужна хорошо продуманная методика обучения основам информационной безопасности.

Организация режима доступа к *образовательным ресурсам* Интернет:

- проведение инструктажей по доступу к образовательным ресурсам Интернет;
- установка программ-фильтров на школьные компьютеры (смотри приложение 5);
- проведение лектория для родителей учащихся по режиму доступа детей к образовательным ресурсам (смотри приложение 7);
- тесты и анкеты для родителей по изучению ИКТ компетенций школьников, а также для диагностики определения степени компьютерной зависимости подростков (смотри приложение 2);
- памятки родителям (смотри приложение 4);
    1) Десять фактов, которые нужно сообщить детям ради безопасности в Интернет.
    2) Памятка для родителей по безопасному использованию сети Интернет.
    3) Рекомендации родителям по предупреждению компьютерной зависимости у ребенка.
    4) Основные правила безопасности в сети Интернет для родителей.
    5) Что делать, если ребенок столкнулся с какой-либо интернет угрозой?
    6) Рекомендации родителям, с помощью которых можно всегда достойно выйти из ситуации, пользователя пытается донимать сетевой грубиян.
    7) Цензура компьютерных игр.
    8) Советы родителям по предупреждению развития компьютерной зависимости у детей.
    9) Что делать, если Ваш ребенок стал потенциальной целью преступника?
    10) Преступники в интернете: что можно сделать для снижения опасности?
    11) Как сделать общение в интернете комфортным?
    12) Советы по повышению безопасности участия Ваших детей в он-лайновых играх
    13) Как предостеречь детей от игр на деньги?
    14) Как поступать, если дети столкнулись с грфферами?
- профилактика основных интернет-рисков (смотри приложение 5)

Организация контроля использования ресурсов Интернета подростком в *домашних условиях*, с помощью программ Родительского контроля:

- ограничивать время, которое он проводит за экраном монитора,

- блокировать доступ к некоторым сайтам,
- блокировать доступ к другим интернет-сервисам,
- запрещать запуск некоторых игр и программ.

При среднем уровне защиты работает фильтр на сайты, посвященные оружию, наркотикам, разного рода непристойностям и содержащим нецензурную лексику.

Видеть в современной технике только добро или только зло - это крайности, которых следует избегать. Техника всего лишь инструмент в человеческих руках, предназначенный для достижения тех или иных целей. И как при использовании любого инструмента, работа в Интернет требует определенной техники, а точнее - культуры безопасности.

При всей важности технических средств, понятно, что они являются всего лишь частью осуществления политики информационной безопасности. Она включает воспитательные и образовательные мероприятия.

В проведении политики информационной безопасности школы принимают участие все заинтересованные в этом лица: педагоги, учащиеся, их родители. Документально политика использования ресурсов сети Интернет зафиксирована в «Правилах использования сети Интернет в муниципальном общеобразовательном учреждении»..

В *помощь классным руководителям* для проведения классных часов и родительского лектория могут быть использованы:

- разработки классных часов по информационной безопасности (приложение 1), (приложение 7)
    1. Родителям о безопасности детей во Всемирной паутине.
    2. Правила безопасности и этикета в Интернете для подростка.
    3. Информационные технологии как основа единого информационного пространства школы
    4. Компьютер в жизни школьника.
    5. Механизм обеспечения информационной безопасности учащихся в школе при использовании Интернета.
    6. Информационная безопасность.
    7. Безопасность в сети интернет.
    8. Обеспечение информационной безопасности при работе с Интернет.
    9. Информационная безопасность семьи и ребенка.
    10. Актуальные проблемы безопасности образовательной среды: мониторинг как инструмент выявления проблемных зон.
    11. Правила безопасности и этикета в Интернете для подростка.
- Наглядный материал (смотри приложение 6).

Формирование информационной культуры и безопасности - процесс длительный и сложный, но важный и необходимый. Интернет может быть и всемирной энциклопедией, объединяющей информационные ресурсы во всем мире. Но он может превратиться и в зловещую паутину, губящую людей, если люди будут искать в ней нечистоты и превращать ее во всемирную помойку. Задача взрослых

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

Возникает проблема: "Каким же образом решать задачу просвещения родителей в вопросах информационной безопасности?" Очень просто.

Во-первых, необходимы беседы о работе детей в сети Интернет, которые проводятся проводятся на заседаниях школьного «Родительского лектория», на классных и общешкольных родительских собраниях.

Мы понимаем, что родителям часто бывает сложно контролировать своих детей, т.к. дети уже знают гораздо больше их, поэтому советуем начинать воспитание информационной культуры с раннего возраста.

Во-вторых, в каждой школе создан школьный сайт или блог, где открыта страничка для родителей с размещенными рекомендациями, сводящимися к простым и очевидным правилам, советам, рекомендациям. На страницах сайта, родительских собраниях необходимо организовать "ликбез" с целью повышения компьютерной грамотности родителей, познакомить с проблемами, которые могут возникнуть при работе на компьютере. Тематика вопросов может быть такова:

1. Что дети должны знать о вредоносных и нежелательных программах в интернете?
2. Что такое вирус?
3. Что такое нежелательное программное обеспечение? Как можно определить, что ваш компьютер заражен? Как снизить риск заражения?
4. Повышение уровня безопасности компьютера.

Кто как не родители смогут обеспечить и проконтролировать безопасность информационной среды у своих детей, которые владеют компьютером значительно лучше их самих?

Поэтому вторым направлением работы с родителями является их знакомство с возможными интернет-рисками и их профилактикой (смотри приложение 5).

Сюда можно отнести вопросы:

1. Онлайновое пиратство у себя дома и как его предотвратить.
2. Безопасное общение детей в интернете.
3. В чем состоит общение детей в чатах и системах обмена мгновенными сообщениями
4. Кибермошенничество. Как его предупредить?
5. Кибербуллинг. Как справиться с кибербуллингом?
6. Предупреждение встреч с незнакомцами и грумингом.
7. Рекомендации по предупреждению.

При этом мы рекомендуем соблюдать родителям ряд правил:

Первое правило – это внимательное отношение к действиям своих детей в Интернете. Мы советуем родителям активно участвовать в общении ребёнка с Интернетом, особенно на этапе освоения, и не отправлять его в «свободное плавание» по Интернету. Родители должны обязательно следить за контактами детей в Сети и знакомиться с сайтами, которые они посещают.

Второе важное правило - постоянное напоминание подросткам о возможностях и опасностях работы с ресурсами Интернет. Родителям необходимо объяснять своему ребёнку, что если он столкнулся с

негативом или насилием со стороны другого пользователя, то обязательно должен сообщить об этом близким людям. Важно контрольровать трату денежных средств при скачивании платной информации и получению платных услуг, особенно путём отправки денег.Мы рекомендуем родителям сформировать список полезных, интересных и безопасных ресурсов, которыми могут пользоваться подростки

Третье правило для родителей – контроль за работой детей в Интернете.Эффективной мерой является установка на компьютер программного обеспечения с функциями «родительского контроля».

Повышение своего уровня компьютерной грамотности – **одно из главных правил** для родителей, которым небезразлична информационная безопасность их детей.

Соблюдение этих простых и в то же время эффективных правил позволит родителям защитить своих детей от сетевых угроз и сделать пользование Интернет-ресурсами максимально полезным. Единство родительских и педагогических усилий поможет нам оптимально использовать «плюсы» и нейтрализовать «минусы» работы с ресурсами всемирной Сети.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Безмалый В.Ф. Обеспечение безопасности детей при работе в Интернет.[Электронный ресурс] - URL:http://www.ifap.ru/library/book331.pdf
2. Безопасность детей в Интернете - URL:http://www.microsoft.com/rus/childsafety
3. Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт. [Электронный ресурс]. - URL:http://i-deti.org/
4. Безопасный интернет: для кого и от кого?-URL: http://www.mobile-review.com/articles/2012/kid-safe-inet.shtm
5. Безопасный 3G-интернет для учебы.
URL:http://www.chip.ua/novosti/internet-i-seti/2012/08/bezopasnyi-3g-internet-dlya-ucheby
6. Борьба с вредоносными программами http://support.kaspersky.ru/viruses
7. Горбачева Е. В. Административно-правовое обеспечение информационной безопасности несовершеннолетних. [Электронный ресурс] - URL:
http://www.dissercat.com/content/administrativno-pravovoe-obespechenie-informatsionnoi-bezopasnosti-nesovershenn
nikh#ixzz2IZYiXTYN
8. Грег Шипли. Основы безопасности ИТ. [Электронный ресурс] - URL:
http://www.ccc.ru/magazine/depot/03_04/read.html?0501.htm
9. Дети и интернет, какие опасности скрывает всемирная паутина. / Методическое пособие для родителей. - URL: http://www.pandia.ru/text/77/115/462.php
10. Детская безопасность в Интернете. [Электронный ресурс]. - URL:
http://www.debotaniki.ru/2012/09/detskaya-bezopasnost-v-internete/
11. Дети в Интернете: кто предупрежден, тот вооружен. - URL: http://do.znate.ru/docs/index-26385.html
12. Десять фактов, которые нужно сообщить детям ради безопасности в Интернете
http://do.znate.ru/docs/index-32759.html
13. Ежеквартальный журнал для педагогов, психологов и родителей “Дети в информационном обществе” издаётся Фондом Развития Интернет с 2009года. Научная поддержка: факультет психологии МГУ имени М.В.Ломоносова и Федеральный институт развития образования МОНРФ. Информационная поддержка: Министерство образования и науки Российской Федерации. Выпуски №1 - 11- URL:
http://detionline.com/journal/numbers/11
14. 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- URL:Режим доступа: http://www.fid.su/projects/journal/
15. Интерактивный курс “Основы безопасности детей и молодежи в интернете”. [Электронный ресурс] -URL: http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/html/etusivu.htm
16. "Интернет: реальные и мнимые угрозы" (под научной редакцией и с комментариями Антона

Серго).[Электронный ресурс]. - URL: http://www.internet-law.ru/book/index2.htm
17. Интернет-угрозы: троллинг и кибербуллинг. [Электронный ресурс]. - URL: http://internetua.com/internet-ugrozi--trolling-i-kiberbulling
18.Информационная безопасность детей в мире компьютерных технологий, ИНТЕРНЕТ Орел Инна Юрьевна Муниципальное образовательное учреждение «Ягринская гимназия» (МОУ «Ягринская гимназия»), г. Северодвинск [Электронный ресурс] - URL: http://ito.edu.ru/2010/Arkhangelsk/IV/IV-0-2.html
19. Конотопов А. Обучающий курс"Гений Интернета" - URL:http://konotopov.com/internet/
20. Линии помощи «Дети онлайн». http://www.detionline.com/
21.Интернет-угрозы и эффективное противодействием им в отношении пользователей. http://www.saferunet.ru/
22. Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным.
http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html
23.Мельников В.П. Информационная безопасность и защита информации. [Электронный ресурс]. - URL:http://www.books.demetri.ws/inf_books_25
24. ОБЩИЕ РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА И МОБИЛЬНОЙ СВЯЗИ- URL: http://do.znate.ru/docs/index-30424.html
25. О ЛИНИИ ПОМОЩИ «ДЕТИ ОНЛАЙН» http://do.znate.ru/docs/index-30424.html
26. Ольхова Н.Е. Беседа с родителями "Интернет - зависимость". [Электронный ресурс]. //Электронно - педагогический журнал Большая перемена. -URL :
http://www.pomochnik-vsem.ru/load/publikacii_pedagogov/klassnoe_rukovodstvo/beseda_s_roditeljami_internet_zavost/37-1-0-2567
27.OS.zone.net - Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль».
http://www.oszone.net/6213/
28. Презентация "Правовое регулирование охраны и защиты прав несовершеннолетних. "Защита детей от информации, причиняющей вред их здоровью и развитию" - URL: http://www.myshared.ru/slide/193722/
29. Проблема информационной безопасности в содержании школьного образования Мошкин В. Н., Чередниченко А. И.[Электронный документ]//- URL:http://www.uni-altai.ru/engine/download.php?id=502
30. Пырьева В.В. Методическая разработка родительского собрания на тему "Безопасность детей в сети Интернет"- URL:http://www.proshkolu.ru/user/VeraPyryeva/blog/243888/
31. РЕКОМЕНДАЦИИ ПО ПОЛЬЗОВАНИЮ СОЦИАЛЬНЫМИ СЕТЯМИ И ОНЛАЙН-ИГРАМИ - URL:http://do.znate.ru/docs/index-30424.html
32. Родителям о безопасном интернете. - URL:http://74322s004.edusite.ru/p67aa1.html
33. Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети. -

URL:http://www.rgdbы.ru/innocuous-internet
34.Руководящие указания для детей и молодых людей по защите в онлайновой среде. - URL: http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/children/gl-child-2009-r.pdf
35. Смагулова Ш., Байтугелова Н., Наурызбаев Т.Информационная безопасность детей: Проблемы и пути решения./ Пособие для педагогов, психологов,родителей и всех заинтересованных сторон. - Астана, 2010 - URL:http://www.bala-kkk.kz/fileadmin/user_upload/images/Informacija_bezopasnost_rus..pdf
36.Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля.- URL:http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids
37. Тест на выявление Интернет-зависимости. -URL: http://www.psyhelp.ru/internet/test.php
38.Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета. - URL:http://www.fid.su/
39.Энциклопедия информационной безопасности. [Электронный ресурс] - URL: http://www.securelist.com/ru/encycloped

ПРИЛОЖЕНИЯ

Приложения включают материалы, необходимые для организации рекомендуемого вида деятельноси. Данные приложения помогут

- *педагогам грамотно организовать мероприятия направленные на формирование у родителей ответственного отношения к информационной безопасности детей;*
- *оформить стенды в образовательном учреждении по информационной безопасности для различных возрастных категорий (родители, старшие подростки);*
- *родителям оценить степень компьютерной зависимости своего ребенка, уровень своих знаний по информационнотй безопасности, овладеть опытом контроля деятельности детей в Интернете, правильно реагировать на возникшие проблемы и грамотно предупреждать их появление в дальнейшем.*

Приложение 1. Разработки родительских собраний

Приложение 2. Тестовые задания, анкеты для родителей

Приложение 3. Методики создания практических заданий, адресованных родителям

Приложение 4. Памятки и советы родителям

Приложение 5. Профилактика основных интернет-рисков и борьба с ними

Приложение 6. Схемы, диаграммы, фотографии, карты, ксерокопии архивных материалов

Приложение 7. Примерная тематика открытых мероприятий, экскурсий и т.д.

Для педагогов.

- Мероприятия с родителями по основам информационной безопасности детей в сети Интернет

  1) С периодичностью не реже 1 раз в учебный год необходимо проводить общешкольное и/или классные тематические родительские собрания, посвящённые вопросам информационной безопасности детей в сети Интернет (по возможности с участием специалистов в области компьютерной коммуникации).

  2) Классным руководителям необходимо проводить в рамках родительских собраний семинары по обмену опытом обеспечения безопасности ребенка в информационном обществе.

Формы проведения родительского всеобуча на тему детской безопасности в Интернет могут включать:

- общешкольные и классные родительские собрания на тему «Возможности и опасности ребенка в Интернете»;
- практические занятия по повышению уровня безопасности детей в Интернете при помощи технических и технологических средств;
- информирование по данной проблеме на страницах сайтов образовательного учреждения;
- выпуск и распространение информационных буклетов по проблеме безопасности детей в Интернете;
- семинары для родителей по обмену опытом обеспечения безопасности ребенка в информационном обществе
- участие родителей в Неделе безопасности в Интернете (http://ipk.68edu.ru/docs/bezopasnostdeti/nedelya-internet.pdf).

Приложение 1. Разработки родительских собраний

Родительское собрание № 1

«Родителям о безопасности детей во Всемирной паутине».

(**http://nsportal.ru/shkola/materialy-dlya-roditelei/library/roditelskoe-sobranie-roditelyam-o-bezopasnosti-detey-vo**)

Цель:Формирование ответственного отношения по обеспечению безопасности детей при работе в сети Интернет.

Задачи:

1. Создать условия для знакомство с возможностями, открываемыми компьютерными технологиями и глобальной сетью Интернет по обеспечению безопасного использования детьми ресурсов Интернета.

3. Расширение информационного поля родителей о влиянии интернета на здоровье и безопасность ребёнка.

Литература:

http://www.dinkypage.com/ita42
http://www.oszone.net/6213/
http://www.microsoft.com/ru-ru/security/family-safety/childsafety-internet.aspx
http://sch730.edusite.ru/p158aa1.html
http://wiki.pippkro.ru
http://lavandamd.ru
http://rovit.rxfly.net/stati/seti/69-bezopasnyj-internet-dlja-detej-i-ih-roditelej.html
www.cursed-games.com
vkus-zdorovya.ru
www.consumer-club.com.ua

demanrus.ru
www.cifrovik.ru
www.azbykamam.ru
ru.photaki.com

Приёмы технологии критического мышления:

- верные и неверные утверждения;
- таблицы ПМИ;
- резюме.

Предварительная работа:

- поиск материала об использование ресурсов сети Интернет детьми;
- анкетирование учащихся.

Организация:

1) родители сидят за столами, перед ними лежит бумага, ручки;
2) объявляется тема родительского собрания;
3) учитель предлагает заполнить анкету.

Стадия вызова

Перед каждым из родителей лежит лист с таблицей «Верные-неверные утверждения», в котором предлагается заполнить вторую колонку.

№	Верные-неверные утверждения	До про-смотра	После просм отра
1.	0% российских детей, пользуются детскими социальными сетями: «Мир Бибигона», Tvidi и др.		
2.	Дети пользуются теми же социальными сетями, что и взрослые: «ВКонтакте», «Одноклассники» и др.		
3.	75% «пятиклашек» и 99% «шестиклашек» зарегистрированы «ВКонтакте» потому, что «это круто», «там все наши», «там прикольно».		
4.	Если дома есть компьютер с выходом в Интернет, то каждый школьник 7-11 класса в обязательном порядке каждый день зависает «ВКонтакте».		
5.	Ученики «ВКонтакте»: -пишут короткие сообщения; - смотрит мультики, видео; - слушает музыку;		

	- размещает фотографии, видео; -знакомится, дружит, гламурничает (ведь в реальной жизни не всегда получается).		
6.	75% юных Интернет-пользователей выходят в сеть самостоятельно; 88% четырёхлетних выходят в сеть вместе с родителями, а к 14 годам совместное использование сетью сохраняется лишь для 7% ребят.		
7.	100% родителей разрешают своим детям путешествовать по Всемирной паутине.		
8.	Путешествия по сети Интернет оказывают положительное влияние на успехи ребёнка.		
9.	Путешествия по сети Интернет оказывают положительное влияние на здоровье ребёнка.		
10.	93% родителей не применяют никаких мер для повышения безопасности при посещении детьми сети Интернет.		
11.	Основная часть родителей не знает какие угрозы подстерегают детей наиболее часто при посещении Интернета.		
12.	Большинство родителей считают, что наиболее эффективным способом защиты детей от Интернет-угроз являются специализированные системы фильтрации контента и наблюдение взрослых.		

Стадия содержания.

1. Классный руководитель демонстрирует презентацию «Результаты школьных исследований «Дети в Интернете и родители»», «Обеспечение безопасности детей при работе в Интернет» (Приложение 2 см блок). В ходе просмотра родители заполняют вторую колонку таблицы и сверяют её с первой.

2. Родителями заполняется таблица ПМИ: что хорошего, негативного в использовании детьми сети Интернет и что показалось интересным.

Плюсы	Минусы	Интересно

Родителям предлагается высказаться, затем раздаются результаты детских анкет (Приложение 1). Родители сверяют свои результаты и ответы своего ребёнка.

Стадия рефлексии.

В конце родительского собрания предлагается написать родителям краткий вывод (приём резюме).

Я понял, что …

Меня удивило, что …

Меня заинтересовало, что …

Все выводы проговариваются вслух. Затем родителям раздаются буклеты (приложения 3) которые предлагается прочитать и обсудить вместе с детьми, поместить рядом с компьютером ребёнка.

Приложение род собр №1

Почитайте, посмотрите, поиграйте вместе с детьми

НЕвредные и "Вредные советы"

Папы, мамы — в Интернете...
Дети где?.. Так где же дети?!
Дети тоже в Интернете?
В Интернете тоже дети...
Мы предложим вам и детям,
В стиле Остера советы,
Пусть и «вредные» советы,
Вы спешите почитать!
Если пишешь реферат ты,
То смелей качай с Ин-ета,
Ставь свои инициалы,
И фамилию пиши
Плагиата ты не бойся,
Мало кто об этом знает,
Ну, а если кто узнает -
Не докажет никогда
Если ты остался дома,
Без родителей, один,
Смело ты гуляй в Ин-ете,
Torrent смело запускай!
И пускай себе качает:
Фильмы, музыку, программы.
Что получится, узнаешь,
Прокурор придёт когда!
Если вы с утра решили

Хорошо себя вести,
Смело в Интернет ныряйте,
И играйте там, играйте
Он-лайн игры — это классно!
Деньги быстро убегут
Пароль, логин, адрес почты,
Помни твердо, наизусть!
И когда тебе случится,
Повстречаться с диверсантом,
Не теряя ни минуты,
Все ты точно сообщи
Если ты нашел в Ин-ете
Информацию крутую,
Верь и факты эти смело
Ты нигде не проверяй!
Даже если вдруг случится,
Что ты домыслы нашёл,
То тверди ты людям смело,
Что Интернет никогда не врёт
Если надо очень быстро
Информацию найти,
Ты скорей пиши в Ин-ете
Быстро, быстро ты запрос.
Если надо очень быстро,
То пиши запрос ты сложный,
И тогда ты точно скоро
Информацию найдёшь
Перед тем как выйти в сеть,
Ты родителям поведай то,
Что фильтры надо срочно,
На комп-е настроить точно.
И тогда систему вашу,
Не придется обновлять,
Будь вежлив ты в сети всегда,
И слов сердитых не пиши,
По пустякам не спорь ты никогда,
И этику сети учи!

Родительское собрание № 2

Правила безопасности и этикета в Интернете для подростка.

Антонова Елена Анатольевна, методист МОУ ДПО УМЦ г. Челябинска

Задачи: Показать родителям важность и значимость проблемы формирования сетевого этикета у подростка. Рассказать родителям о правилах общения в Интернете.Ознакомить родителей с источниками информации по проблеме безопасности ребенка в Интернете.

Вопросы обсуждения: статистика и цифры о роли Интернета в жизни школьников. Влияние Интернет общения на формирование личности ребенка.

Подготовительная работа:

Анкетирование учащихся, подготовка статистики. Подготовка шаблонов.

Оформление на доске.

Ход собрания:

Вступительное слово

Интернет общение в жизни ребенка — это хорошо или плохо? Сколько и как должен общаться ребенок в Интернете? Нужно ли ограничивать общение детей в сети? Важно ли прививать этические понятия ребенку по отношения к общению в Интернете? На эти и другие вопросы мы постараемся ответить. Обратимся к статистике. Результат анкеты учащихся и родителей класса.

Учитель знакомит с результатами анкетирования родителей и учеников.

Анкета для родителей.

ФИО родителя.	
Класс в котором учится ребенок.	
Класс в котором учится ребенок.	
1.Есть ли у вас дома компьютера?	Да. Нет
2.Есть ли Интернете.	Да. Нет
Сколько времени ребенок проводит за компьютером?	

4.Какие средства для общения в Интернете Вы знаете.	
5.Общается ли ли в Интернете ваш ребенок с друзьями?	Да. Нет
6.Какими средствами общения в Интернете пользуется ребенок.	
7.Есть ли у ребенка электронный ящик?	
8.Есть ли у ребенка блог или живой журнал?	Да. Нет.
9.Посылает ли ребенок электронные открытки?	Да. нет.
10.Говорите ли вы с ребенком о правилах сетевого этикета.	Да. Нет.
11. Говорите ли вы с ребенком об опасностях в Интернете?	Да. Нет.

Анкета учащегося. (проводится и анализируется до собрания)

Фамилия Имя_____

Класс_____

1.Есть ли дома компьютер?

2.Есть ли дома Интернет?

3.Сколько времени проводишь за компьютером?

4. Какие средства для общения в Интернете ты знаешь?

5.Общаешься ли в Интернете с друзьями?

6. Какими средствами общения в Интернете ты пользуешься?

7.Пользуешься ли электронным ящиком?

8.Есть ли утебя блог или живой журнал?

9.Посылаешь ли электронные открытки?

10 Знаешь ли ты правила сетевого этикета?

11. Какие опасности могут подстерегать тебя в Интернете?

12. Разговаривал ли ты с родителями о Сетевом этикете, о правилах поведения в сети?

Анализ анкет. Постановка проблемы.

Анализ анкеты детей и родителей показал результаты.....

В связи с тем, что дети.....

В связи ч тем, что родители.....

Необходимо.....

Поговорить об опасностях в Интернете, которые подстерегают ребенка.

По материалам Компьютерной газеты мы можем узнать о проблеме безопасности детей в сети.

«Безопасность детей в сети Интернет» http://www.nestor.minsk.by/kg/2006/33/kg63308.html

«Уже давно для многих Интернет стал жизненно необходимой вещью, без которой Homo Sapiens уже не Homo Sapiens. Было бы достаточно банально перечислять все блага вездесущего потомка Arpanet, тем не

менее факт остается фактом — мы глубоко "погрязли" в паутине и отказаться от этого изобретения человечества многим просто не под силу, особенно если эти многие — дети. Специфика человеческой психики такова, что мы быстро привыкаем к новой среде в которой комфортно себя чувствуем, изоляция же нас из этой среды равносильна насилию.

Проблема защиты детей в Сети находит самый широкий резонанс и это не случайно. Согласно последней СТАТИСТИКЕ (сайт) :

- около 50% детей выходят в Сеть без контроля взрослых:
- 28% из вышедших в Интернет детей "серфят" в поисках "клубнички":
- 19% детей иногда посещают порносайты, еще 9% делают это регулярно. 38% детей, просматривают страницы о насилии, 16% детей просматривают страницы с расистским содержимым, 26% детей участвуют в чатах о сексе.
- 25% пятилетних детей активно используют Интернет. Уже в 2001 году 25% пятилетних детей в США пользовались Интернетом. Эта цифра достигает 75% среди детей возраста 15–17 лет. Данные, собранные в результате опроса "Использование компьютера и Интернета детьми и подростками в 2001 году", проведенного департаментом образования США показывают, что дети начинают пользоваться Интернетом в самом раннем возрасте.
- Дети опережают взрослых по количеству времени, которое они проводят в Интернете.
- Дети в возрасте между 8 и 13 годами дети составляют половину общего числа пользователей Интернета. Большинство из них выходит в Сеть из дома и самыми частыми их занятиями являются браузинг, чаты и онлайновые игры.
- 44% детей один раз подвергались сексуальным домогательствам в Интернете. 11% подверглись им несколько раз.
- 14.5% детей, принявших участие в опросе, назначали встречи с незнакомцами через Интернет, 10% из них ходили на встречи в одиночку, а 7% никому не сообщили, что с кем–то встречаются.

Как воспитывать своего ребенка в контексте интернет–безопасности — дело каждого, иногда достаточно просто строгого слова родителя. Тем не менее, сам факт существования руководств, говорит об актуальности темы и ее крайней значимости. (памятки для родителей о информационной безопасности)

Одной из проблем современных пользователей является соблюдение этикета, или сетикета.

Давайте остановимся на понятиях: **этикет, сетикет (сетевой этикет)**

Этике́т (от франц. Etiquette -этикетка, надпись, впервые появившаяся при дворе Людовика 14) - этикет - (не писанные), общепринятые правила поведения в обществе.

Сетике́т, нетике́т (неологизм, является слиянием слов «сеть» (англ. *net*) и «этикет») — правила поведения, общения в Сети, традиции и культура интернет-сообщества, которых придерживаются большинство. Это

понятие появилось в середине 80-х годов XX века в эхоконференциях сети FIDO.

(Материал из Википедии — свободной энциклопедии)

Для того чтобы разработать свои практические рекомендации для родителей и детей необходимо объединиться в творческие группы.

Работа в творческих группах.

Первая группа

Цель:Разработка принципов ведения диалога в сети.

Родителям выдается шаблон таблицы и отдельные модули - карточки. Родители распределяют по теме все модули и карточки с народной мудростью. Получают готовую карту «Принципов ведения диалога в сети»

Сетевой этикет.

Сетевой этикет – новое понятие. Интернет развивается и расширяется, все больше людей общается в сети. Начиная общаться в блогах друг с другом, они допускают множество незаметных на первый взгляд ошибок. Эти ошибки могут доставить неприятности собеседникам в сети. Избежать этих ошибок помогут несколько советов. С принципами необходимо познакомить детей.

Перед началом ведения дискуссии в сети следует усвоить некоторые принципы ведения диалога в блоге, форуме, чате...

Принцип вежливого тона. “Вежливость ничего не стоит, но приносит многое”	В ходе общения в сети очень важно обратиться к партнёру по имени как можно непринуждённее, давая понять, что его имя для вас много значит.
Принцип внимания «Понимай самого себя и уважай другого»	Важное условие успешного ведения беседы в сети - исключительное внимание к собеседнику. Ещё лучше сопровождать диалог в сети фразами: "Да!", "Понимаю тебя...", "Это интересно...", "Приятно это читать..." и т.д. Такая реакция является приглашением высказаться свободно и непринуждённо. Она помогает выразить одобрение, интерес, понимание. Можно проявить стремление получить дополнительные факты и прояснить позицию человека: "Пожалуйста, уточните это...", "Не можете ли ещё раз подробнее, укажите источники?", "Не объясните ли вы это?". Помогают сближению следующие фразы: "Как я понял тебя...", «Ты можешь поправить меня, если я ошибаюсь...", "Другими словами..." и т.д.
Принцип рациональности.	Необходимо в ходе диалога в сети вести себя

«Лучше одно слово, чем девять»	сдержанно, если даже собеседник проявляет эмоции. Неконтролируемые эмоции отрицательно сказываются на процессе общения в сети.
Принцип понимания. «Мир силен не оружием, а людьми доброй воли.»	Постарайтесь понять собеседника в сети. Невнимание к его точки зрения ограничивает возможность выработки различных точек зрения на один вопрос.
Принцип общения. «Обдумывай хоть неделю, но скажи ясно.»	Если постоянные читатели не вступает в дискуссию в сети, привлеките его внимание интересной темой.
Принцип отказа от поучительного тона. «Доброе слово железные ворота отопрет.»	Не старайтесь поучать. Будьте открыты для аргументов и постарайтесь убедить собеседника в необходимости информации.
Принцип разграничения между собеседником и предметом разговора. «Зла за зло не воздавай.»	Необходимо разбираться с проблемой, а не друг с другом.

Вторая группа

Цель: Знакомство с Правилами этикета при общении по электронной почте. Подготовка рекомендаций для родителей и детей по источнику сайт: «Этикет от А до Я» http://www.etiket.ru/contact/email.html В этом документе описываются простые правила этикета при общении пользователей по электронной почте.

Адреса и персональные имена

Персональное имя (не то же самое, что подпись)- произвольная строка, которую многие мэйлеры (программы электронной почты) позволяют присоединять к вашим сообщениям в качестве текстового комментария.

- Если ваша система позволяет, всегда пишите персональное имя: оно является для вас лучшей "визитной карточкой", чем адрес e-mail
- Используйте осмысленные имена. Выражения типа "догадайся сам" не только мешают определить автора письма, но и оскорбляют интеллект адресата
- Если ваша почтовая система позволяет отправлять письма вместе с именами адресатов, используйте эту возможность. Таким образом, администратору сети будет легче найти адресата по имени, если сам адрес окажется ошибочным.

Пример: адрес 344188@foo.chaos.com содержит меньше информации, чем 344188@foo.chaos.com (Ford Prefect).

Тема письма (Subject)

- Длина, содержание и формат письма

Не забывайте давать названия своим письмам. Практически все мэйлеры позволяют присваивать почтовым сообщениям названия, и часто пользователь ориентируется именно по названиям, когда просматривает свою почту.

- Избегайте бессмысленных названий. Например, отправляя письмо службе технической поддержки WordPerfect, не следует называть его *WordPerfec*- с тем же успехом вы могли бы вообще ничего не писать.
- Если вы при ответе на письмо меняете тему разговора, не забудьте изменить и название
- Точный заголовок- самый простой способ определить тему беседы, и если вы измените тему, оставив заголовок прежним, адресат может прийти в замешательство.
- Старайтесь, чтобы длина вашего письма отвечала стилю беседы: если вы просто отвечаете на вопрос, делайте это кратко и по существу.
- Держитесь как можно ближе к теме. Если вы хотите поговорить о чем-то новом, лучше послать отдельное письмо. Тогда ваш адресат сможет хранить его отдельно.

Ответы

- Не пишите весь текст заглавными буквами- его становится тяжело читать (хотя краткое выделение может использоваться как усиление). Старайтесь разбивать ваше письмо на логические абзацы и избегайте чрезмерно длинных предложений.
- Старайтесь не допускать грамматических ошибок. Полное ошибок и опечаток письмо трудно читать. То, что электронная почта- быстрый способ связи, вовсе не означает, что можно расслабиться и забыть о правописании (по моему опыту, самое безграмотное сообщение- электронное). Если вы считаете свои мысли достойными изложения в письме, позаботьтесь, чтобы они были изложены правильно
- Избегайте публичных флэймов- писем, составленных под влиянием эмоций. Послания, отправленные в момент душевных переживаний, чаще всего только ухудшают ситуацию. Возможно, позже вы будете раскаиваться в своих словах, поэтому перед тем как начать "флэймовую войну", спокойно обдумайте положение. (Попробуйте сварить себе кофе- удивительно, как быстро улягутся ваши эмоции с помощью чашечки хорошего кофе.)
- Если ваш мэйлер поддерживает различные параметры оформления текста (жирный шрифт, курсив ит.д.), убедитесь, что мэйлер адресата обладает такими же возможностями. К тому времени, как был составлен этот документ, большинство программ электронной почты в Internet могли работать только с текстом, хотя ситуация, конечно, изменяется.
- Трижды подумайте перед тем, как включать номер вашей кредитной карточки в свои электронный письма. Электронную почту могут перехватить, и ваш счет в банке подвергнется опасности

- Включайте в ваше послание отрывки письма, на которое отвечаете. Помните, электронная почта- не разговор по телефону в реальном времени, и ваш адресат может забыть содержание предыдущего письма (особенно, если он ведет активную переписку). Включайте отрывки оригинального текста в ваш ответ, и адресат легче поймет, о чем идет речь
- Не переусердствуйте в цитировании предыдущих посланий. Очень неприятно получать обратно собственное письмо на пяти страницах (в качестве комментария) с маленькой припиской типа "я согласен" в конце. Отделяйте каким-то образом текст вашего послания от текста цитируемых писем, тогда ваш ответ будет легче читаться. Обычно используется для этих целей знак >, хотя это и не единственный вариант.
- Старайтесь не смешивать в своем послании информацию общего и личного характера
- Спросите себя: так ли уж необходим ваш ответ. Например, если вы получили письмо в результате веерной рассылки, вряд ли стоит извещать каждого из адресатов о своем отношении к нему- лучше послать письмо непосредственно автору.

Подписи

Подпись- небольшой текстовый отрывок в конце сообщения, обычно содержит информацию о **контактах.** Большинство мэйлеров могут автоматически "приклеивать" подпись к исходящим сообщениям.

- Если можете, используйте подпись. Она должна идентифицировать вас и содержать данные об альтернативных каналах связи (обычный телефон, факс). На многих системах, в частности, тех, где почта проходит через шлюзы, ваша подпись может быть единственным идентификатором.
- Делайте свою подпись покороче- 4-7 строчек вполне достаточно. Неоправданно длинные подписи загружают каналы связи
- Некоторые мэйлеры позволяют добавлять случайные строки к вашей подписи: будьте с этим аккуратнее. В любом случае помните
- *Краткость- сестра таланта.* Цитата на сотни слов из "Критики чистого разума" Канта в качестве подписи вряд ли порадует ваших адресатов
- консультант вряд ли сможет вам помочь - ему для этого просто не хватит для этого информации
- *Изменяющиеся подписи* лучше всего смотрятся, если носят шутливый характер. Высказывания на политическую тему, например, могут расстроить некоторых людей, в то время как короткая шутка только поднимает настроение.

Простые правила вежливости

Электронная почта- средство связи между людьми, и без правил вежливости здесь не обойтись.

- Если вы обращаетесь к кому-либо с просьбой, не забудьте сказать "пожалуйста". В то же время, если кто-то помогает вам, никогда не вредно сказать "спасибо". Хотя это может показаться банальным, вы будете удивлены тем, какое количество людей являются образцами вежливости в реальной жизни и словно забывают о своих манерах в переписке по e-mail.
- Не ждите, что вам ответят немедленно. Тот факт, что вы в течение десяти минут не получили ответа

на свой вопрос, вовсе не означает, что адресат вас игнорирует

- Помните, что не существует надежной почтовой системы. Неразумно помещать очень личную информацию в электронное письмо, если только вы не собираетесь его зашифровать с помощью надежной программы шифрования. Помните об адресате. Вы не единственный человек, который пострадает в случае, если деликатное сообщение попадет в плохие руки
- Включайте в свое письмо полную информацию по теме, особенно, если рассчитываете на квалифицированный ответ. Например, если вы посылаете сообщение "Программа электронных таблиц не работает" в службу технической поддержки компании "Lotus",

Хотя электронная почта похожа на разговор в реальном времени, она лишена возможности жестикуляции. Для решения этой проблемы в Internet используются "смайлики" - последовательности ASCII-символов, которые напоминают лицо, если смотреть на них, повернув голову набок.

Чаще всего применяют такие "смайлики":

:-) или :)- улыбка; обычно используется для выражения радости, удовольствия (иногда встречается \ или \- "усмешка").

:-(или :(- несчастное лицо; выражает сожаление или разочарование.

;-) или ;)- подмигивающее лицо; обычно выражает иронию и означает, что слова не следует понимать слишком буквально.

Существуют сотни различных "смайликов", одни используются чаще, другие - реже.

Правильное использование "смайликов" способно придать вашему письму живой характер и даже заменить жестикуляцию. Однако, не переусердствуйте.

И наконец...

Помните, что e-mail- средство связи с живыми людьми. Перед тем, как послать письмо, прочтите его внимательно еще раз и поставьте себя на место получателя.

Источник: сайт: «Этикет от А до Я» http://www.etiket.ru/contact/email.html

Третья группа

Цель: Разработать Соглашение о кодексе поведения в Интернете.

Примерный шаблон (по материалам сайта:Microsoft http://www.microsoft.com/rus/protect/athome/children/famwebrules.mspx)

Соглашение

Я ФИО_____

обязуюсь:

Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в интернете (___ минут или ___ часов).

Никогда не выдавать...

Всегда немедленно сообщать родителям...

Никогда не соглашаться...
Никогда никому, кроме своих родителей, не выдавать...
Вести себя в интернете правильно и не делать...
Никогда не загружать, не устанавливать и не...
Никогда не делать без разрешения родителей...
Сообщить моим родителям мое....

Образец соглашения

(по материалам сайта:Microsoft **http://www.microsoft.com/rus/protect/athome/children/famwebrules.mspx)**
Я ФИО_____

обязуюсь:

Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в интернете (___ минут или ___ часов).

Никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы.

Всегда немедленно сообщать родителям, если я увижу или получу в интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в интернете.

Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в Интернете, без разрешения родителей

Никогда никому, кроме своих родителей, не выдавать пароли интернета (даже лучшим друзьям).

Вести себя в интернете правильно и не делать ничего, что может обидеть или разозлить других людей или противоречит закону.

Никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без должного разрешения.

Никогда не делать без разрешения родителей в интернете ничего, требующего платы.

Сообщить моим родителям мое регистрационное имя в Интернете и имена в чате, перечисленные ниже:

Имя (ребенок) _____ Дата _____

Родитель или опекун _____ Дата _____

Представление группами результата.

l . Принципы ведения диалога в сети.

2. Правила этикета при общении по электронной почте.

3. Соглашение о кодексе поведения в Интернете.

Подведение итогов. Собрание заканчивается высказываниями детей на тему: «Интернет для меня -это....» и выводами родителей: «Мы должны с детьми говорить на тему безопасности и этикета в Интернете...»

Источники:

Журнал для пап «Батя» http://rusbatya.ru/index.php?option=com_content&task=view&id=220

ИД «Собеседник» http://www.sobesednik.ru/archive/sb/39_2008/children_nongrata/

Компьютерная газета http://www.nestor.minsk.by/kg/2006/33/kg63308.html

Сайт Microsoft http://www.microsoft.com/rus/protect/family/guidelines/rules.mspx

Сайт «Ребенок в сети» http://www.detionline.ru/index.html

Сайт пословиц http://allproverbs.ru/

Родительское собрание № 3.

Материалы для проведения родительского собрания "Информационные технологии как основа единого информационного пространства школы"

Анкета для родителей № 1

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

1. В каком классе учится Ваш ребенок?_____

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

- скорее положительно
- скорее отрицательно (не вижу необходимости)

Другое:_____

3. **Информационные технологии и обучение**

- в школе проводятся различные мероприятия с применением информационных технологий (проектная деятельность, уроки, классные часы и родительские собрания).
- урок, с применением новых информационных технологий более популярен у моего ребенка (более интересен, понятен и т.п. - со слов ребенка)
- ребенок с интересом и удовольствием выполняет проекты (рефераты, доклады), используя компьютер
- ребенок готовится к уроку, используя компьютер (Интернет, полезные ссылки на сайте школы, рекомендуемые учителем сайты и т.п.)
- классный руководитель проводит родительские собрания с использованием компьютера

Другое:_____

4. **Работа "Электронного журнала". (**Одной из возможностей ресурса является просмотр на страницах этого ресурса в Интернете оценок учащегося, которые выставляют учителя на уроках и их комментарии, домашнее задание... (пароль доступа индивидуален для каждого пользователя))

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

в нашем классе он не работает и думаю, что нет в нем необходимости

Другое:_____

5. Посещение Школьного сайта

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

Другое:_____

6. **Школьный сайт. Напишите, пожалуйста, что бы Вы хотели бы изменить в работе сайта.**

7**. Есть ли у Вас дома компьютер?**

- да (один)
- да (несколько)
- нет

Другое:_____

8. Кто пользуется компьютером у Вас дома?

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

Примерный список вопросов, которые планируется обсудить на родительском собрании

1. В каком возрасте следует разрешить детям посещение интернета?
2. Следует ли разрешать детям иметь собственные учетные записи электронной почты?

3. Какими внутрисемейными правилами следует руководствоваться при использовании интернета?

4. Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?

5. Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, Mail Agent)?25

6. Могут ли дети стать интернет-зависимыми?

7. Что должны знать дети о компьютерных вирусах?

8. Как проследить какие сайты посещают дети в интернете?

9. Что следует предпринять, если моего ребенка преследуют в интернете?

10.Помогает ли фильтрующее программное обеспечение?

11.На какие положения политики конфиденциальности детского сайта
нужно обращать внимание?

12.Какие угрозы встречаются наиболее часто?

13.Как научить детей отличать правду ото лжи в Интернет?

Анкета для родителей №2

1. Имеете ли вы компьютер?
2. Сколько времени проводит ваш ребенок за компьютером?
3. С какой целью он использует компьютер?
    1) подготовка к урокам
    2) поиск внеучебной информации (музыка, фильмы ...)
    3) общение
    4) чтение книг
    5) компьютерные игры
4. В какие игры играет Ваш ребенок?
5. Какие сайты посещает Ваш ребенок?
4. Боитесь ли Вы общения вашего ребенка с компьютером?
5. Изменилось ли поведение вашего ребенка после того, как он стал активно общаться с компьютером?
6. Как вы относитесь к увлечению детей компьютерными играми?
7. Посещает ли ваш ребенок компьютерный клуб?
8. Вызывает ли у вас это тревогу?
9. Считаете ли вы необходимым использование компьютера на школьных уроках по различным предметам?
10. Как Вы считаете: КОМПЬЮТЕР - ЭТО:
    1) друг
    2) враг
    3) свой вариант ответа

Приложение 2. Тестовые задания, анкеты для родителей

Тест №1. “ Определение зависимости подростков от компьютерных игр”

(А.В. Котлярова)

Отметьте утверждение, которое соответствует поведению Вашего ребенка

Утверждение	да	нет
1.Ребенок испытывает затруднения, грустит, раздражается при необходимости закончить игру		
2. Ради компьютерной игры ребенок жертвует времяпровождением с семьей, друзьями		
3. Ребенок преимущественно находится в хорошем настроении, занимаясь компьютерными играми		
4. Из-за компьютерной игры ребенок пренебрегает сном		
5. Игра за компьютером - главное средство для снятия стресса ребенка		
6. После игры за компьютером у ребенка возникают головные боли		
7. В обычной жизни ребенок испытывает пустоту, раздраженность, подавленность, которые исчезают при игре за компьютером		
8. При помощи игры на компьютере ребенок решает жизненные проблемы, достигает жизненных целей		
9. После компьютерной игры у ребенка возникает нарушение аппетита, стула		
10. Из-за компьютерной игры у ребенка возникают проблемы с учебой, но он продолжает в нее играть		
11. Из-за компьютерной игры ребенок пренебрегает питанием		
12. Ребенок испытывает потребность проводить за игрой все больше времени		
13. Из-за компьютерной игры ребенок пренебрегает гигиеной		

14. Во время игры ребенок полностью отрешается от действительности, целиком переносясь в мир игры		
15.После компьютерной игры у ребенка возникает сухость слизистой оболочки глаз		
16. Из-за компьютерной игры у ребенка появляются проблемы в семье, отношениях с людьми, но он продолжает играть		
17. Игра за компьютером служит ведущим средством для достижения комфортного состояния ребенка		

Анализ обработки анкеты: За каждый ответ “да” начисляется 1 балл. Если сумма выбранных ответов составляет более трех баллов, то велика вероятность того, что увлечение вашего ребенка компьютерными играми может перерасти в зависимость.

Тест №2 для родителей на наличие игровой интернет-зависимости их ребёнка

Поставьте в соответствующую графу один балл за каждый вопрос, на который вы ответили положительно.

Вопросы	Балл
1. Много ли времени ребенок проводит за компьютером, игровой панелью, планшетом, карманным персональным компьютером, смартфоном, играя в компьютерные игры? 2. Легко ли он прекращает игру по вашему требованию? 3. Часто ли бывают ситуации, когда ребенок прячется от вас и играет в компьютерные игры? 4. Часто ли он рассказывает вам о персонажах из компьютерных игр и игровых ситуациях? 5. Часто ли ребенок с друзьями обсуждает игровые ситуации? 6. Изменился ли резко его внешний вид, одежда? 7. Появились ли у него странные и нетипичные предметы: меч, плащ, необычные аксессуары, обувь? 8. Просит ли он у вас обновить компьютер? Сделать его мощнее, быстрее? 9. Просит ли ребенок деньги на игры или на непонятные вам цели? 10.. Изменились ли резко его привычки?	

Если сумма баллов дает больше 5, то вам надо обратить внимание на возможную игровую зависимость вашего ребенка.

Тест №3 “ Проверка степени компьютерной зависимости ребенка”

К ребенку, увлеченному игрой, обращается родитель с просьбой о помощи. И для ориентировки в степени

“застревания” ребенка в компьютере необходимо пройти уровни обращения:
1-й уровень-просьба формулируется просто, например “Сынок, помоги, пожалуйста, подвинуть кресло”.

Способы реагирования:

А.Ребенок легко откликается на просьбу, помогает, может увлечься этой помощью, переключиться на другое дело, отвлечься, забыть о компьютере- такое поведение полную свободу от компьютера на момент тестирования.

Б.Ребенок откликается со второго-третьего раза, демонстрирует недовольство, огрызается-такая реакция может быть при 1-й степени зависимости в пределах первого месяца овладения компьютером или на начальном этапе 2-й степени.

В.Ребенок не откликается на просьбу, явно не слышит, игру не прерывает- такое поведение свойственно зависимости 2-3 степени.

2-й уровень- в случае, если ребенок вел себя по схеме Б или В,необходимо, через какой-то промежуток времени, например, на следующий день, оьратиться к ребенку с развернутой, аргументированной просьбой, например: “Сынок,помоги мне, пожалуйста, подвинуть кресло. Я одна справиться не могу. Мне нужна твоя помощь. Пожалуйста, прерви свое занятие и помоги мне”. Если реакция на просьбу будет аналогичной,то можно делать вывод о наличии зависимости у ребенка и необходимости предоставить ему помощь.

Приложение 1.

Анкета для родителей (приложение 1 к родительскому собрание №1)

1. ….. минут, часов в течение дня я провожу за компьютером.
2. Для учёбы я использую Интернет ….. минут, часов в день.
3. В Интернете я люблю ……
4. В социальных сетях «ВКонтакте», «Одноклассники» я «сижу» ….. минут, часов.
5. В социальных сетях мне нравится…….
6. Я посещаю такие детские социальные сети как ….
7. Мои родители контролируют время моей работы, посещения социальных сетей ……..(да / нет др.)
8. Подключаясь к Интернет, появляются такие угрозы, как …….

Существуют определенные сайты, которые вы можете посоветовать родителям, для определения Интернет-зависимости, зависимости от компьютерных игр в режиме реального времени. Родитель, придя домой, в спокойной обстановке более правдиво ответит на вопросы, возможно, осознает уровень опасности.

Ресурсы:

Определение Интернет-зависимости

http://psyhelp.ru/internet/test.php
http://psychology.net.ru/tests/start.html?test_id=6
http://shkolazhizni.ru/test/27/

Тесты на определение зависимости от компьютерных игр
http://www.vrc-alternativa.ru/articles/igromania-test.php

Приложение 3. Методики создания практических заданий, адресованных родителям

1. Мероприятия с родителями по основам информационной безопасности детей в сети Интернет

1) С периодичностью не реже 1 раз в учебный год необходимо проводить общешкольное и/или классные тематические родительские собрания, посвящённые вопросам информационной безопасности детей в сети Интернет (по возможности с участием специалистов в области компьютерной коммуникации).

2) Рекомендовать классным руководителям проводить в рамках родительских собраний семинары по обмену опытом обеспечения безопасности ребенка в информационном обществе.

3) **Работа с родителями включает в себя следующие формы:**

1. Отправной точкой каждого учебного года является оформление Советом Старшеклассников стенда "Опасности Интернета", где собрана информация о запрещённых и полезных сайтах, статистические данные, об ответственности родителей за здоровье своих детей.

2. Педагогом-психологом школы разрабатываются и проводятся родительские собрания, на которых рассказывается о том, какие правила должны соблюдать родители, чтобы их дети избежали участи стать компьютерными "наркоманами".

3. Психологическим клубом "Доверие", где занимаются наравне с другими учащимися "дети группы риска" разрабатываются памятки-буклеты для родителей.

4. Совместные родительские собрания с детьми, на которых в форме игры рассказывается о истории появления компьютера, о правилах пользования Интернетом, как быть взаимно вежливым в Интернете, как необходимо фильтровать нужную информацию.

5. Выступление на родительском собрании медицинского работника на тему: "Компьютер и здоровье"

Предлагаемые темы родительских собраний:

" Компьютер в жизни подростка
" Поколение КОМП
" Внимание: дети в Интернете
" Виртуальная агрессия

" Компьютер без вреда.

Приложение 4. Памятки и советы родителям

Информация для родителей:

Приложение 2 к родительскому собранию №1 .

Результаты школьных исследований «Дети в Интернете и родители»

-0% российских детей регулярно пользуются детскими социальными сетями, предпочитая те же сервисы, что и взрослые;

-Около 86% российских детей из общего числа зарегистрированных в соцсетях пользуются "ВКонтакте";

-Лишь 5% опрошенных что-то знают о «Мире Бибигона», около 1% школьников вроде слышали о Tvidi;

-Опрос учащихся 5 классов показал, что 75% уже зарегистрированы «ВКонтакте», готовы зарегистрироваться хоть сейчас и все оставшиеся, потому что «это круто», «там все наши», «там прикольно».

-В 6 классах ситуация меняется: 99% опрошенных шестиклассников «уже давно» зарегистрированы «ВКонтакте»;

Опрос учащихся 7-11 классов показал, что если дома есть компьютер с выходом в Интернет, то школьник в обязательном порядке каждый день зависает «ВКонтакте». Что он там делает? Да, то же, что и все остальные: пишет короткие сообщения; смотрит мультики (младшие); слушает музыку; размещает фотографии, видео; знакомится, дружится, гламурничает (ведь в реальной жизни не всегда получается) и так далее;

-60% детей имеют доступ к сети Интернет дома, 28% - в школе, 10% - у друзей и лишь 2% - в Интернет-кафе. Причем 100% опрошенных родителей указали, что разрешают своим детям путешествовать по Всемирной сети.

-На вопрос «Оказывают ли путешествия по сети на школьные успехи Вашего ребенка?» 64% родителей ответили положительно, а 36% родителей указали, что путешествия по Интернету не влияют на успеваемость их ребенка.

- На вопрос «Оказывают ли путешествия по сети на здоровье Вашего ребенка?» лишь 43% родителей ответили положительно. 57% считают, что путешествия по сети не влияют на здоровье детей.

- На вопрос «Что Вас больше всего настораживает при использовании Вашим ребенком сети Интернет?» около 32% родителей указали вредоносные сайты, 28% - сайты с негативным и противоправным контентом.

Большинство родителей считают, что наиболее эффективным способом защиты детей от Интернет-угроз являются специализированные системы фильтрации контента и наблюдение взрослых.

Все большее количество детей получает возможность работать в Интернет. Но вместе с тем все острее встает проблема обеспечения безопасности наших детей в Интернет. Так как изначально Интернет

развивался вне какого-либо контроля, то теперь он представляет собой огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и взрослые?

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

ОБЩИЕ СОВЕТЫ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ В ВОЗРАСТЕ 14 – 17 ЛЕТ ПРИ РАБОТЕ В ИНТЕРНЕТЕ.

1. Измените в соответствии с интересами и запросами подростка список домашних правил использования подростком Интернета, требуйте его соблюдения.
2. Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются.
3. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.
4. Интересуйтесь, какими чатами и досками объявлений пользуются подростки и с кем они общаются.
5. Поощряйте использование модерируемых чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.
6. Возьмите за правило знакомиться с сайтами, которые посещают ваши дети. Убедитесь, что они не посещают сайты с оскорбительным содержанием, не публикуют личную информацию или свои фотографии.
7. Настаивайте, чтобы подростки никогда не соглашались на личные встречи с друзьями из Интернета без вашего участия. Напоминайте, какие опасности это может за собой повлечь.
8. Требуйте от подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.
9. Требуйте от подростков не загружать программы, музыку или файлы без консультаций с вами.
10. Объясните, что иначе подростки могут нарушить авторские права и тем самым закон.
11. Настаивайте на том, чтобы подростки ставили вас в известность, если что-либо или кто-либо в Сети тревожит или угрожает им. Объясните, что угрозы им – это также и угроза всей семье. Оставайтесь в случае чего спокойными и напомните детям, что они в безопасности, если рассказали вам. Помогайте им решить возникшие проблемы.
12. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
13. Постоянно напоминайте, что ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
14. Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете.

15. Обсудите с подростками азартные сетевые игры и связанный с ними риск. Напомните, что детям нельзя в них играть.
16. Поддерживайте уровень безопасности вашего компьютера на должном уровне. Если ваш ребенок лучше вас разбирается в программном обеспечении, то почему бы не поручить ему заботу о безопасности ваших семейных компьютеров?

Риски, с которыми подростки сталкиваются в сети и советы по профилактике и правильной реакции при возникновении угрозы.

Большинство старших подростков используют Интернет для получения информации. Однако, информация, выдаваемая Интернетом, может оказаться нежелательной и вредной для здоровья ребенка (страдает эмоциональная сфера подростка, также может быть нанесен прямой вред физическому здоровью ребенка.).
Примеры противозаконной, неэтичной и вредоносной информации:

- информация о насилии, жестокости и агрессии,
- информация, разжигающая расовую ненависть, нетерпимость по отношению к другим людям по национальным, социальным, групповым признакам,
- пропаганда суицида,
- пропаганда азартных игр,
- пропаганда и распространение наркотических веществ, отравляющих веществ,
- пропаганда анорексии (отказ от приема пищи) и булимии (чрезмерное потребление пищи),
- пропаганда деятельности различных сект, неформальных молодежных движений,
- эротика и порнография,
- нецензурная лексика

Распространение противозаконной информации преследуется по закону, например, распространение наркотических веществ через Интернет, порнографических материалов с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям

Что делать.

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. РОДИТЕЛЬСКИЙ контроль возможен и нужен в Интернете. Родители могут решить какое содержимое в Интернете могут просматривать их дети, отследить, какие сайты посещал ребенок, ограничить время пользования Интернетом

Ресурсы в помощь родителю:

http://icensor.ru/
http://www.oszone.net/6213/

2. Используйте опцию «Безопасный поиск», которую предоставляют популярные поисковых систем и почтовых служб. Опция легко настраивается самостоятельно.

3. Каждому пользователю домашнего ПК – свой пароль и логин. Учетная запись администратора должна быть у родителя, тогда только родитель сможет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера.
4. Самое важное: ДОВЕРИТЕЛЬНЫЕ ОТНОШЕНИЯ. Чем больше Вы общаетесь с ребенком на интересующие его темы, тем меньше тайн от Вас будет у него.

Интернет для старшего подростка – среда общения. Общение также может стать угрозой для Вашего ребенка, если он :

Подвергся **кибербуллингу** (буллинг - запугивание, унижение, травля, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе)

Как распознать опасность:

Обратите внимание на психологические особенности вашего ребенка. Признаки того, что ребёнок подвергается кибербуллингу, различны, но есть несколько общих моментов:

- признаки эмоционального дистресса на протяжении и после использования Интернета,
- прекращение общения с друзьями,
- избегание школы или школьных компаний,
- нестабильные оценки и отыгрывание злости в домашней обстановке,
- перемены в настроении, поведении, сне и аппетите
- не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками,
- склонны к депрессии и чаще своих ровесников думают о самоубийстве.

Что делать:

1. Научите

А) правильной реакции. Оскорбляют – либо покинь данный ресурс, либо игнорируй хулигана

Б) правильному поведению. Никогда никого не оскорбляй сам

2. Объясните: личная информация, выложенная в Интернет, может быть использована против тебя

3. Воспользуйтесь опцией: "заблокировать пользователя" или "занести в чёрный список".

При серьезных проблемах (угрозы перешли в реальную жизнь, касаются жизни или здоровья ребенка, а также членов вашей семьи, потрачены деньги ит.д)

1. Скопируйте и сохраните информацию со страницы сайта
2. Обратитесь в правоохранительные органы

Подвергся **Грумингу**- установление дружеских отношений с ребенком с целью личной встречи,вступления с ним в сексуальные отношения, шантажа и эксплуатации

Как распознать опасность

1. В компьютере появились материалы откровенного содержания

2. Ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый.

3. ребенок стал замкнутым и подавленным.

4. звонит по незнакомым вам номерам (либо звонят ему), при звонках старается уйти, в содержание разговора не посвящает

Как предупредить опасность:

1. объяснить, что нельзя:

- помещать личные данные в Интернет –сетях (домашний адрес, телефон и т.д)
- пересылать виртуальным знакомым свои фотографии или видео
- ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи
- использовать реальное имя при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх)

2. в доверительной беседе постарайтесь предупредить об опасности встречи с незнакомыми людьми из Интернета. Договоритесь, что если ребенок пойдет на такую встречу, то только с вами

3. создайте условия, чтобы ваш ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время.

4. Поговорите с ребенком на тему взаимоотношений мужчины и женщины (каким бы взрослым вы не считали бы своего ребенка). Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в Интернете тема любви часто представляется в неправильной, вульгарной форме.

Что делать:

1. сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов

2. обратитесь к представителям власти

Памятка №1

Памятка для родителей по безопасному использованию сети Интернет

Если ваши дети пользуются Интернетом дома, вы уже знаете, насколько важно защитить их от неподобающего содержимого и нежелательных контактов.

Подростки должны иметь практически неограниченный доступ к содержимому, сайтам или действиям. Они хорошо разбираются с тем, как использовать Интернет, однако родителям все равно следует напоминать им о соответствующих правилах безопасности. Родители всегда должны быть готовы помочь своим детям-подросткам разобраться, какие сообщения являются непристойными, а также избегать опасных ситуаций. Родителям рекомендуется напоминать детям-подросткам о том, какую личную информацию не следует предоставлять через Интернет.

Советы по безопасности, которые рекомендуется выполнять, когда ваши дети-подростки используют

Интернет:

1. Старайтесь по-прежнему поддерживать как можно более открытое общение внутри семьи и позитивное отношение к компьютерам. Обсуждайте с детьми их общение, друзей и действия в Интернете точно так же, как другие действия и друзей.

   Просите детей-подростков рассказывать вам, если что-то или кто-то в Интернете доставляет им чувство неудобства или страха. Если вы подросток и вам не нравится что-то или кто-то в Интернете, расскажите об этом.

1. Создайте список семейных правил использования Интернете дома. Укажите виды сайтов, которые можно посещать без ограничений, время подключения к Интернету, расскажите, какую информацию не следует разглашать в Интернете, а также предоставьте инструкции по общению с другими в Интернете, включая общение в социальных сетях.
2. Компьютеры, подключенные к Интернету, должны находиться в открытом месте, а не в спальне ребенка-подростка.
3. Изучите средства фильтрации Интернет-содержимого (такие как Windows Vista, средства родительского контроля Windows 7иФункции семейной безопасности Windows Live) и используйте их в качестве дополнения к контролю со стороны родителей.
4. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер. Internet Explorer..
5. Следите за тем, какие сайты посещает ваш ребенок-подросток и с кем он общается. Просите их пользоваться контролируемыми чатами, настаивайте на том, чтобы они использовали только общедоступные чаты.
6. Настаивайте на том, чтобы они никогда не соглашались на встречу с друзьями, с которыми они познакомились в Сети.
7. Научите детей не загружать программы, музыку или файлы без вашего разрешения. Обмен файлами и использование текста, изображений или рисунков с веб-сайтов может привести к нарушению авторских прав и может быть незаконным.
8. Поговорите со своими детьми-подростками о содержимом в Интернете, предназначенном для взрослых, и порнографии, а также укажите им позитивные сайты, посвященные вопросам здоровья и сексуальности.
9. Помогите им защитить себя от спама. Проинструктируйте своих детей-подростков никогда не давать свой адрес электронной почты при общении в Интернете, не отвечать на нежелательные почтовые сообщения и пользоваться фильтром электронной почты.
10. Знайте, какие сайты ваши дети-подростки посещают чаще всего. Убедитесь, что ваши дети не посещают сайты, содержащие оскорбительные материалы, и не публикуют свою личную информацию. Следите за тем, какие фотографии публикуют ваши дети-подростки и их друзья.
11. Учите своих детей отзывчивости, этике и правильному поведению в Интернете. Они не должны использовать Интернет для распространения сплетен, клеветы или запугивания других.

12. Проследите за тем, чтобы дети спрашивали у вас, прежде чем совершать финансовые операции в Интернете, включая заказ, покупку или продажу товаров.
13. Обсудите со своими детьми-подростками азартные игры в Интернете, а также потенциальные риски, связанные с ними. Напомните им о том, что азартные игры в Интернете являются незаконными.Ес

Памятка №2

Рекомендации родителям по предупреждению компьютерной зависимости у ребёнка

Для профилактики компьютерной зависимости психологи советуют следующее:

1. Показывать личный положительный пример. Важно, чтобы слова не расходились с делом и, если отец разрешает играть сыну не более часа в день, то сам не должен играть по три-четыре.
2. Ограничьте время работы с компьютером, объяснив, что компьютер – не право, а привилегия, поэтому общение с ним подлежит контролю со стороны родителей. Резко запрещать работать на компьютере нельзя. Если ребёнок уже склонен к компьютерной зависимости, он может проводить за компьютером два часа в будний день и три – в выходной, но обязательно с перерывами.
3. Предложить другие возможности времяпрепровождения. Можно составить список дел, которыми можно заняться в свободное время. Желательно, чтобы в списке были совместные занятия (походы в кино, на природу, игра в шахматы и т.д.)
4. Использовать компьютер как элемент эффективного воспитания, в качестве поощрения (например, за правильно и вовремя сделанное домашнее задание, уборку квартиры).
5. Обращать внимание на игры, в которые играют дети, т.к. некоторые из них могут стать причиной бессонницы, раздражительности, агрессивности, специфических страхов.
6. Обсуждать игры вместе с ребёнком. Отдавать предпочтение развивающим играм. Крайне важно научить ребёнка критически относиться к компьютерным играм, показывать, что это очень малая часть доступных развлечений, что жизнь гораздо разнообразней, что игра не заменит общения.
7. Если родители самостоятельно не могут справиться с проблемой, необходимо обращаться к психологам.

Памятка №3

Основные правила безопасности для родителей

1. Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.
2. Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
3. Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
4. Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
5. Спрашивайте ребенка о том, что он видел и делал в Интернтете

6. Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.
7. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.
8. Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чем он не уверен.
9. Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
10. Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.
11. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека.
12. Постараться регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;
13. Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости также неприятно, как и слышать;
14. Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

Памятка №4

Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.

2. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.
3. Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.

4. Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.
5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Вы можете скачать эти рекомендации.

Памятка №5.

Рекомендации родителям, с помощью которых можно всегда достойно выйти из ситуации, когда пользователя пытается донимать сетевой грубиян

1. Чат.

Если при общении в тематическом чате к вам пристает пользователь с оскорблениями, злыми шутками или издевательствами, отправьте его в игнор-лист (персональный «черный список») или сообщите администратору чата о его неприемлемом поведении. Скорее всего, грубиян будет забанен, то есть исключен из числа пользователей. Грубить хаму в ответ чревато получением такого же бана.

2***. Аська и прочие онлайн-месседжеры.***

Отвязаться от нежелательного собеседника в аське проще всего. Добавив разбушевавшегося грубияна в «черный список», вы больше никогда не увидите и не услышите его. Чтобы предотвратить дальнейшие беседы с «клонами» хама (то есть его «реинкарнациями» под другими номерами ICQ), необходимо поставить в настройка х клиента запрет на получение сообщений от неавторизованных пользователей. Тогда вы будете получать сообщения только от тех контактов, которые одобрите сами.

3***. Социальные сети.***

Решить проблему хамства в социальных сетях обычно помогают модераторы ресурса, которые обязаны внимательно следить за публичными сообщениями пользователей. В случае добросовестной работы модераторов Вы даже не успеете прочитать оскорбительное послание. Если же сетевой грубиян донимает вас по личной почте, вы всегда можете пожаловаться тому же модератору в индивидуальном порядке.

4. ***Сайты знакомств.***

К сожалению, приличная часть посетителей сайтов знакомств приходят туда вовсе не для того, чтобы найти себе друзей и любимых. Сайты знакомств являются излюбленным местом обитания сетевых хамов, любителей онлайновых издевательств и розыгрышей. Поэтому, пользуясь подобными ресурсами, нужно быть предельно внимательным и быть морально готовым к неадекватным сообщениям. Отвечать на провокации и грубости вовсе не обязательно, а кнопка жалобы администрации всегда под рукой.

5. ***Форумы.***

Свои местные хамы и так называемые тролли (провокаторы) есть на каждом популярном форуме. От

обычных собеседников, не согласных с Вашим мнением, их отличает провокационный тон сообщений, открытые издевательства или откровенная глупость аргументов. Пытаться доказать таким людям совершенно бесполезно, так как они преследуют единственную цель – позлить вас. Лучше представьте, что этого пользователя вовсе не существует на форуме и его сообщений тоже. Продолжайте беседу в привычной манере, не реагируя на попытки тролля вывести вас из себя. Вероятно, вскоре ему надоест тратить время зря и он оставит вас в покое.

Если же Вы сами не прочь сорвать злость и плохое настроение в Интернете, можете рискнуть пообщаться с сетевым хамом на его языке. В конце концов, он первый начал и вы не обязаны быть вежливым. Однако опускание до уровня банального грубияна занятие не делающее чести никому, поэтому куда лучше будет не обращать на него внимания.

Памятка №6

Цензура компьютерных игр

Цензура взрослыми компьютерных игр-вещь, совершенно необходимая, причем не надейтесь, что за вас это кто-то сделает. Каждая игра, попадающая в руки ребенка, вначале должна быть просмотрена кем-то из взрослых. Вникните в ее содержание, задайтесь вопросами: что даст эта игра вашему ребенку, какие качества личности будет развивать в нем, не будет ли формировать агрессивный стиль поведения, не даст ли какую-то опасную информацию?

Игра должна:

- развивать;
- не содержать бранных слов и выражений;
- не формировать циничное отношение к происходящему;
- не содержать агрессивной информации;
- не вызывать привыкания к боли, драматичным ситуациям;
- не учить противозаконным вещам;
- не содержать сексуальной тематики.

Аналогичной цензуре должны подвергаться и фильмы, которые смотрят дети, так как агрессия, негативная информация, чувство страха от просмотра фильмов также вредны для детской психики

Памятка №7

Ваш ребенок - жертва преступника

Уважаемые родители!. Обратите внимание на следующие признаки, позволяющие определить, что ребенок подвергся атаке злоумышленников в сети.

- ***Ваш ребенок проводит много времени в Интернете.*** Большинство детей, преследуемых Интернет-преступниками, проводят большое количество времени в Сети, особенно в чатах; подчас закрывают дверь в свою комнату и скрывают, чем они занимаются, сидя за компьютером.
- ***В семейном компьютере появились материалы откровенного содержания.*** В качестве предлога

для начала сексуальных обсуждений злоумышленники могут снабжать детей фотографиями, ссылками на соответствующие сайты и присылать сообщения эротической окраски. Для того чтобы внушить ребенку мысль о естественности сексуальных отношений между взрослыми и детьми, преступники могут использовать фотографии с изображением детской порнографии. Имейте в виду, что ваш ребенок может прятать порнографические файлы на дисках, особенно если другие члены семьи пользуются тем же компьютером.

- ***Вашему ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам незнакомы.*** Установив в Интернете контакт с вашим ребенком, некоторые злоумышленники могут попытаться вовлечь детей в секс по телефону или попытаться встретиться в реальной жизни. Если дети не решаются дать номер телефона, злоумышленник может сообщить им свой. Не разрешайте своему ребенку лично встречаться с незнакомцем без контроля с вашей стороны.
- ***Ваш ребенок получает письма, подарки или посылки от неизвестного вам лица.*** Обычно преследователи посылают своим потенциальным жертвам письма, фотографии и подарки. В других странах они порой даже отправляют билеты на самолет, чтобы соблазнить ребенка личной встречей. Ваш ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый. Интернет-преступники усердно вбивают клин между детьми и их семьями и часто преувеличивают небольшие неприятности в отношениях ребенка с близкими. Кроме того, дети, подвергающиеся сексуальному преследованию, становятся замкнутыми и подавленными.
- ***Ваш ребенок использует чью-то чужую учетную запись для выхода в Интернет.*** Даже дети, не имеющие доступа в Сеть дома, могут встретить преследователя, выйдя в Интернет у друзей или в каком-нибудь общественном месте, например библиотеке. Иногда преступники предоставляют своим жертвам учетную запись, чтобы иметь возможность с ними общаться.

Советы родителям по предотвращению развития компьютерной зависимости у детей

• Часто причиной возникновения компьютерной зависимости у детей и подростков становятся неуверенность в себе и отсутствие возможности самовыражения. В таких случаях родители должны поддержать ребенка и помочь ему разобраться с возникшими проблемами.

• Абсолютно неправильно критиковать ребенка, проводящего слишком много времени за компьютером. Это может только углубить проблему и отдалить ребенка от родителей.

• Если ребенок страдает игровой завистью, нужно постараться понять его и в какой-то мере разделить его интерес к компьютерным играм. Это не только сблизит ребенка с родителями, но и увеличит его доверие к ним, а значит, ребенок с большей уверенностью будет следовать советам родителей и с большим доверием делиться с ними своими проблемами.

• Критика воспринимается ребенком, как отказ родителей понять его интересы и потому вызывает замкнутость и в некоторых случаях агрессию.

• Основной мерой предотвращения возникновения зависимости любого типа у детей является правильное воспитание ребенка. При этом важно не ограничивать детей в их действиях (например, запрещать те или иные игры), а объяснять, почему то или иное занятие или увлечение для него не желательно.
• Рекомендуется ограничивать доступ детей к играм и фильмам, основанным на насилии. В то же время если ребенок все же встретился с такой информацией нужно в доступной форме объяснить ему почему такая информация для него опасна и почему он не должен стремиться узнать ее.
• Категорический запрет того или иного вида информации безо всяких объяснений только увеличит интерес ребенка к этой информации, а существование запрета сделает невозможным обсуждение проблемы между родителями и ребенком.

Дети и подростки нуждаются в самовыражении. За не имением других средств выражения своих мыслей и энергии они обращаются к компьютеру и компьютерным играм, которые создают иллюзию реальности безграничных возможностей, лишенной ответственности. Такая иллюзия оказывает разрушительное действие на психику.

Опасности	Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций.
Компьютер	Повысьте уровень общей безопасности Вашего компьютера.
Время	Следите за достижением равновесия у вашего ребенка между временем, проводимым в Интернете и вне его.
Правила	Обсудите внутрисемейные правила пользования Интернетом.
Этикет	Научите детей уважать других в Интернете.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАШ РЕБЕНОК СТАЛ ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

Регулярно проверяйте компьютер на наличие материалов откровенного характера или каких-либосвидетельств об общении с сексуальной окраской – это настораживающие признаки.

Контролируйте доступ вашего ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений.

Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.

Если ваш ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.

ПРЕСТУПНИКИ В ИНТЕРНЕТЕ: ЧТО МОЖНО СДЕЛАТЬ ДЛЯ СНИЖЕНИЯ ОПАСНОСТИ?

Пользуясь возможностями Интернета, дети подвергаются опасности вступить в контакт со злоумышленниками. Анонимность общения в Интернете способствует быстрому возникновению доверительных и дружеских отношений. Преступники используют преимущества этой анонимности для завязывания отношений с неопытными молодыми людьми. Вы сможете защитить своих детей, если поймете возможную опасность общения через Интернет и будете в курсе того, чем они занимаются в Сети.

КАК СДЕЛАТЬ ОБЩЕНИЕ В ИНТЕРНЕТЕ КОМФОРТНЫМ?

Контролируйте использование чата вашим ребенком. Помните о том, что дети могут участвовать в чатах, расположенных на сайтах, при помощи программ поддержки чатов, сотовых телефонов и даже некоторых онлайновых игр.

Добейтесь того, чтобы дети никогда не сообщали в чатах свои личные данные. Так, при выборе псевдонима необходимо выбирать имя, не выдающее личные данные детей. Например, вместо псевдонима DetroitSue можно использовать SassySue. Следует настоять на том, чтобы дети не посылали своих фотографий тем, с кем они познакомились в чате.

Дети должны знать, что они всегда могут обратиться к вам за советом или помощью. Предупредите ребенка о том, что, если что-либо в чате вызовет у него чувство дискомфорта, необходимо немедленно его покинуть и сообщить о происшедшем кому-нибудь из взрослых. Пусть дети всегда сообщают вам об участниках чата, которые предлагают им встретиться в приватных комнатах чата.

У детей должно быть настороженное отношение к попыткам собеседников перевести общение из виртуальной плоскости в реальную. Им никогда нельзя соглашаться на личную встречу с незнакомыми людьми, с которыми они познакомились в Интернете.

Скажите детям, чтобы они посещали только модерируемые чаты. Перед тем как вступить в беседу, пусть ознакомятся с положениями и условиями участия в чате, правилах поведения и положением о конфиденциальности.

СОВЕТЫ ПО ПОВЫШЕНИЮ БЕЗОПАСНОСТИ УЧАСТИЯ ВАШИХ ДЕТЕЙ В ОНЛАЙНОВЫХ ИГРАХ ПО СЕТИ.

Получите информацию. Ознакомьтесь с классификацией игр и условиями конфиденциальности, а также прочтите правила на сайте игры. В качестве примера можно познакомиться с кодексом поведения Xbox® Live.

Будьте в курсе, в какие игры и с кем играют ваши дети. Поместите компьютер или игровую консоль (например, Xbox) туда, где экран хорошо просматривается; искренне интересуйтесь, во что дети играют. Установите правила. Это следует сделать до выхода детей в Интернет; кроме того, убедитесь, что ребенок их понимает. С примером такого рода домашних правил можно ознакомиться, прочитав «Внутрисемейные правила пользования Интернетом**».**

Контролируйте чат и сообщения во время игр. Попросите детей сообщать вам, если другой игрок употребляет нецензурные слова; в этом случае можно выделить обидчика в списке и отключить или заблокировать его сообщения. Другой вариант – сообщить о некорректно ведущем себя игроке администраторам игры по электронной почте, в чате или другим способом. Для дополнительной информации о возможных мерах воздействия на таких игроков можно обратиться на официальный сайт игры. Обучите детей навыкам безопасности. Скажите детям, что, если кто-либо из игроков будет вести себя оскорбительно, игру следует остановить и немедленно сообщить вам. При необходимости – связаться с администратором.

Убедитесь в конфиденциальности. Требуйте от детей никогда не выдавать в игровом чате личную информацию (например, имя, пол или домашний адрес), фотографии и не соглашаться на встречи. Убедитесь, что дети знают о необходимости обратиться к вам за помощью в случае чего. Выбирайте соответствующие имена. Заставьте ребенка использовать подходящие имена героев, соответствующие игровым правилам. Эти имена не должны раскрывать никакую личную информацию или провоцировать домогательство.

Примечание: Для компьютеров и игровых консолей типа Xbox есть технология маскировки или скрытия голоса, позволяющая изменить настоящий голос ребенка. Имейте в виду, что взрослые также могут пользоваться этой программой и выдавать себя не за того, кто они есть на самом деле.

Берегитесь хулиганов**.**

Играйте вместе. Безопаснее всего для детей играть через Интернет вместе с вами. Возможно, им этого хочется меньше всего на свете (особенно тем, кто постарше), но это очень хороший способ научиться общению в Сети.

КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ ОТ ИГР НА ДЕНЬГИ?

Родители должны решить, во что можно играть их детям. Обсудите жанр игр (скажем, только бильярд, стратегии и шахматы) и количество участников (можно ведь играть и одному).

Напоминайте детям, что им нельзя играть на деньги. Предложите им играть в не менее увлекательные

игры, но которые не предполагают использование наличных или безналичных проигрышей,выигрышей.

Помогите детям понять механизм таких игр. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают.

Не позволяйте детям использовать номера ваших кредитных карт в Интернете. Держите их в недоступном для детей месте. В сетевых играх на деньги они обычно требуются. Дети могут ненароком влезть в долги.

Объясните, что к играм на деньги можно пристраститься. Всегда есть опасность приобретения зависимости. Это как болезнь. Особенно если есть кредитная карта и положительный баланс на ней; человек может играть, пока не истратит все до конца.

Контролируйте поведение своих детей в Интернете.

Следите за тем, какие сайты посещают ваши дети и что они делают в Интернете.

КАК ПОСТУПАТЬ, ЕСЛИ ДЕТИ СТОЛКНУЛИСЬ С ГРИФЕРАМИ?

Пусть ваши дети их игнорируют. Если ребенок не будет реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

Посоветуйте детям изменить параметры игры. Добейтесь, чтобы ребенок играл в игры, правила или режимы которых можно изменить, например, невозможность убить товарищей по команде. Таким образом, тактика гриферов становится бессмысленной.

Порекомендуйте создать частную игру. Большинство многопользовательских игр позволяет создавать закрытые комнаты, куда можно пускать только друзей.

Пусть дети играют на сайтах со строгими правилами.

Там, где установлены строгие правила, администратор сможет немедленно заблокировать хулиганов.

Пусть играют в игры, где от гриферов можно легко избавиться. Предложите ребенку играть в те игры, где сообщения хулиганов можно отключить или проголосовать за их исключение из игры.

Придумайте еще что-нибудь. Если обидчик продолжает беспокоить вашего ребенка, добейтесь, чтобы он сменил игру или сделал перерыв и вернулся позже.

Сообщайте о «дырах» в игре. Поищите вместе с ребенком уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору.

Пусть ваши дети воздерживаются отвечать огнем на огонь. Убедитесь, что ребенок не использует против обидчиков их же тактику; скорее всего, это спровоцирует гриферов на еще более озлобленное поведение. Или, что еще хуже, создаст о ребенке впечатление как об обидчике.

Рекомендуйте детям избегать провокаций с именами. Ребенок избежит многих проблем, если не станет использовать псевдоним, который может спровоцировать обидчика.

Пусть дети не выдают личную информацию. Хулиганы (да и вообще кто угодно) могут использовать настоящие имена, номера телефонов, а также домашние или электронные адреса, чтобы причинить ребенку неприятности.

СНИЖЕНИЕ РИСКА ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ.

Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации. При немедленном обращении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.

ЧТО ДЕЛАТЬ В СЛУЧАЕ ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ?

Если вы подозреваете, что ваши личные данные украдены, немедленно принимайте меры:

- Измените пароли.
- Поставьте в известность отдел обслуживания клиентов соответствующих организаций.
- Поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета.
- Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.
- Записывайте и сохраняйте абсолютно все.
- После выполнения всех действий всегда делайте копии документов.

В виртуальном мире есть свои правила Интернет-гигиены.

КАК МОЖНО ОПРЕДЕЛИТЬ, ЧТО ВАШ КОМПЬЮТЕР ЗАРАЖЕН?

Ваш компьютер может начать работать медленнее или прекращать работать и перезагружаться каждые несколько минут. Иногда вирус атакует файлы, необходимые для запуска компьютера. В подобном случае вы можете, нажав кнопку запуска, обнаружить, что смотрите на пустой экран.

Все эти симптомы являются типичными признаками заражения компьютера вирусом, хотя они могут вызываться также проблемами в аппаратной части или программном обеспечении, не имеющими ничего общего с вирусным заражением.

Совет: Помните, что, открыв и запустив зараженный файл, вы можете не сразу узнать, что получили вредоносную программу, так как вирусы часто начинают свою разрушительную работу не сразу. Пусть дети будут внимательны к сообщениям о том, что они отправили электронное письмо, содержащее вирус. Это может значить, что вирус указал ваш электронный адрес в качестве отправителя зараженного письма. Это необязательно означает, что на вашем компьютере есть вирус. Некоторые вирусы умеют

фальсифицировать электронные адреса.

Если компьютер внезапно начал медленно работать или вы видите всплывающие окна, даже еслине подключены к Интернету, то, возможно, вы стали жертвой программ-шпионов и других нежелательных программ. Они автоматически загружаются в систему без всякого уведомления. Часто они бывают прикреплены к другому файлу, который вы скачали или установили. Программа-шпион может загрузиться на ваш компьютер, даже если вы просто щелкнули по баннеру.

Памятка № 8

Онлайновое пиратство.

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя

Уважаемые родители!

1. Предупредите детей, что:
   - **Пиратство – это обычное воровство.**
2. Объясните вашим детям, что
   - если они незаконноскачивают файлы, то ваш компьютер рискует стать уязвимым для вирусов или программ-шпионов.
   - подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции.
   - официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией
   - распространители пиратских продуктов, преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя
3. Обсудите с детьми допустимые траты на музыкальные записи или игры, чтобы у молодого поколения не было соблазна для незаконного скачивания.
4. Научите детей законным методам скачиванияВ Интернете существует множество мест, где вы и ваши дети можете скачать программы, фильмы, игры и музыку бесплатно или за небольшую цену. Например, сайт MSN Music предлагает более миллиона записей от разных студий
5. Сами будьте примером.

Памятка № 9

ОСНОВЫ БЕЗОПАСНОГО ВЕДЕНИЯ ИНТЕРНЕТ- ДНЕВНИКА.

Уважаемые родители!

Правильное ведение дневника может дать детям и их родителям возможность общаться и поделиться друг

с другом опытом; дети могут поведать родителям о новых технологиях, а родители могут дать ряд ценных жизненных советов

Другое преимущество – привитие ответственности и дисциплины ведения дневника; возможность творческого самовыражения; новые возможности общения с друзьями и родственниками, обучение компьютерным и Интернет-технологиям, а также развитие навыков набора на клавиатуре, правописания, письменной речи и редактирования

Чтобы Интернет-дневник не стал источником опасности:

1.Требуйте от ваших детей

- никогда не публиковать в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения.
- никогда не помещать в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверять, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

2. Объясните, что публикуемая в Интернете информация остается там надолго и кто угодно может легко распечатать веб-журнал или сохранить его на своем компьютере.

3. Рекомендуйте детям

- пользоваться веб-журналами только с ясно сформулированными условиями использования и проверять, можно ли защитить с помощью пароля сами веб-журналы, а не только учетные записи пользователя (даже если это так, лучше держать в уме, что любой человек может получить доступ к Интернет-дневнику).
- не стремиться соревноваться с другими детьми, ведущими веб-журналы. Пусть дети стараются вести свой блог в положительном ключе и не использовать его для злословия или нападок в адрес других детей.разрешения правообладателя

Памятка № 10

Безопасный интернет вне дома

Уважаемые родители! Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями.Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в Интернет самостоятельно, им следует уяснить некоторые моменты.

Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций. В заключение беседы установите определенные ограничения на использование Интернета и обсудите их с детьми. Сообща вы сможете создать для ребят уют и безопасность в Интернете.

Если вы не уверены, с чего начать, вот несколько мыслей о том, как сделать посещение Интернета для детей полностью безопасным.

- Установите правила работы в Интернете для детей и будьте непреклонны.

• Научите детей предпринимать следующие меры предосторожности по сохранению конфиденциальности личной информации:

– Представляясь, следует использовать только имя или псевдоним.

– Никогда нельзя сообщать номер телефона или адрес проживания или учебы.

– Никогда не посылать свои фотографии.

– Никогда не разрешайте детям встречаться со знакомыми по Интернету без контроля со стороны взрослых.

• Объясните детям, что разница между правильным и неправильным одинакова как в Интернете, так и в реальной жизни.

• Научите детей доверять интуиции. Если их в Интернете что-либо беспокоит, им следует сообщить об этом вам.

• Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

• Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

• Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ – является кражей.

• Скажите детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

• Скажите детям, что не все, что они читают или видят в Интернете, – правда. Приучите их спрашивать вас, если они не уверены.

• Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

• Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Регулярно посещайте Интернет-дневник своего ребенка, если он его ведет, для проверки.

• Будьте внимательны к вашим детям!

Приложение 5. *Профилактика основных интернет-рисков и борьба с ними*

Вредоносные программы — *различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля*

какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Предупреждение столкновения с вредоносными программами

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
5. Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п).
7. Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
8. Расскажите ребенку, что если он пользуется интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки — по этой информации злоумышленники могут многое узнать о вашем ребенке.

Как избавиться от вредоносных программ

1. Загрузите компьютер в безопасном режиме (включите компьютер, нажмите и, удерживая клавишу F8, выберите Безопасный режим (Safe Mode) в открывшемся меню).
2. Проведите полную антивирусную проверку компьютера.
3. Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.
4. При невозможности самостоятельно решить проблему обратитесь за помощью в службу технической поддержки производителя установленного на вашем компьютере антивирусного ПО или в технический сервис.

Повысьте уровень безопасности вашего компьютора

Если на вашем компьютере установлена операционная система Microsoft® Windows® XP Service Pack 2, то можно использовать Windows Security Center. Эта программа позволяет просматривать информацию о состоянии защиты компьютера и изменять настройки, а также получать дополнительные сведения по вопросам безопасности.

Security Center показывает состояние трех важных компонентов безопасности: брандмауэра Интернета, антивирусных программ и службы автоматического обновления. Кроме того, он служит для перехода к другим разделам безопасности, а также поиска технической поддержки и ресурсов, имеющих отношение к защите компьютера.

Security Center работает в фоновом режиме, постоянно проверяя состояние трех наиболее важных компонентов.

Для того чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Центр обеспечения безопасности/Security Center;
- убедитесь, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).

Включить или отключить брандмауэр и автоматическое обновление вы можете непосредственно в Центре обеспечения безопасности.

Для управления защитой от вирусов обратитесь к настройкам установленного антивирусного программного обеспечения.

Установите на вашем компьюторе антишпионские настройки или дополнительное антишпионское программное обеспечение

Шпионскими называются программы, выполняющие определенные действия (например, сбор личной информации или изменение настроек) без согласия и контроля пользователя. Они могут существенно замедлить работу системы и привести к нежелательным изменениям в важных настройках.

Такие программы трудно удалить. Антишпионское программное обеспечение поможет избавиться от шпионских и других нежелательных программ. Проверка компьютера может выполняться по расписанию в удобное для вас время.

Для того чтобы предотвратить появление шпионского программного обеспечения на вашем компьютере,необходимо убедиться в том, что включены основные средства Центра обеспечения безопасности вашей операционной системы.

Рекомендуется также для повседневной работы использовать учетную запись с ограниченными правами.

Для удаления шпионского программного обеспечения, попавшего на ваш компьютер, следует воспользоваться специальным антишпионским программным обеспечением, в частности, следующими программами: Windows Defender; Malicious Software Removal Tool.

Эти бесплатные программы вы можете загрузить с сайта http://www.microsoft.com/downloads

Для этого в строке Search в выпадающем списке выберите All Downloads, в строке справа введите название

одного из указанных выше продуктов и нажмите кнопку Go.

Блокируйте доступ к неподходящим материалам

Один из наилучших способов защиты от нежелательной информации – это блокирование доступа еще до того, как она может быть получена.

Microsoft предлагает несколько таких способов.

Для того чтобы блокировать доступ к нежелательной информации в Internet Explorer® и MSN Explorer, нужно выполнить следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/ Control Panel;
- в панели управления откройте Свойства обозревателя/Internet Options;
- в появившемся окне перейдите на вкладку Содержание/Content;
- в разделе Ограничение доступа/Content Advisor нажмите кнопку Включить/Enable;
- в появившемся окне введите пароль, который будет защищать вводимые вами ограничения от изменения детьми;
- в окне Ограничение доступа/Content Advisor вы можете блокировать доступ к нежелательной информации.

Повысьте уровень безопасности ребенка с электронной почтой OUTLOOK® EXPRESS.

Для повышения уровня безопасности при работе ребенка с электронной почтой в меню программы Outlook® Express в разделе Сервис/Tools выберите команду Параметры/Options.

Перейдите на вкладку Безопасность/Security.

При помощи переключателя выберите зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use вы можете уменьшить вероятность появления вирусов на вашем компьютере. Для этих же целей служит переключатель Не разрешать сохранение или открытие вложений, которые могут содержать вирусы/Do not allow attachments to be saved or opened that could potentially be a virus. Если же виру все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочку Предупреждать, если приложения пытаются отправить почту от моего имени/Warn me when other applications try to send mail as me.

Для защиты пересылаемых писем от подделки и от возможности перехвата и прочтения кем-либо, кроме указанного получателя, есть возможность Шифровать содержимое и вложения всех исходящих сообщений/Encrypt content and attachments for all outgoing messages и Подписывать все отправляемые сообщения/Digitally sign all outgoing messages.

Заблокируйте поступление спама

Чтобы блокировать поступление спама (нежелательной почты), необходимо воспользоваться почтовым сервером, имеющим защиту от спама (например, hotmail.com), или почтовым клиентом, имеющим спам-фильтр (например, Microsoft Outlook).

Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере hotmail.com, необходимо зайти в этот почтовый ящик и перейти по ссылке Options и в вертикальном меню выбрать вкладку Mail.
Перейдя по ссылке Junk E-mail Filter, вы можете изменить настройки фильтра нежелательной почты.
При помощи ссылки Block Senders, находящейся на вкладке Mail, вы можете добавить любого отправителя в список заблокированных, при этом почта от этого отправителя не будет поступать в ваш почтовый ящик.
В случае, если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.
Для настройки этого фильтра в меню Microsoft Outlook выберите Сервис/Tools, в открывшемся меню выберите команду Параметры/Options. В открывшемся диалоговом окне перейдите на вкладку Настройки/Preferences и нажмите кнопку Нежелательная почта/Junk E-mail.
В появившемся диалоговом окне вы можете внести изменения в настройки фильтра нежелательной почты.
Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

Создайте отдельные учетные записи для разных пользователей

Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой «Мои документы». Родитель может создать себе учетную запись администратора, дающую полный контроль над компьютером, а детям – ограниченные учетные записи. Пользователи с ограниченными учетными записями не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение, включая большинство игр, медиаплееров и программ поддержки чатов.
Для того чтобы создать отдельную учетную запись для ребенка с ограниченными правами доступа для работы в Интернете, необходимо выполнить следующие действия:

- нажмите кнопкуПуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Учетные записи пользователей/User Accounts;
- в открывшемся окне выберите Создание учетной записи/Create a new account, введите ее имя;
- на этапе выбора типа учетной записи установите переключатель в положение Ограниченная запись/Limited;
- после нажатия кнопки Создать учетную запись/Create Account процесс создания учетной записи с ограниченными правами будет завершени ваш ребенок сможет выбрать ее при следующем входе в систему.

Повысьте уровень конфиденциальности при общении вашего ребенка в интернете с помощью INTERNET EXPLORER.

Сохранение конфиденциальности личной информации вашего ребенка при его работе в Интернете является важным механизмом безопасности.
Для того чтобы повысить уровень конфиденциальности при общении вашего ребенка в Интернете, выполните следующие действия:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;

- в панели управления откройте Свойства обозревателя/Internet Options;
- в появившемся окне перейдите на вкладку Конфиденциальность/Privacy;
- при помощи ползунка выберите необходимый уровень конфиденциальности.

Создавайте надежные пароли

Пароли – это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета кредитных карт, обратиться за ипотекой или даже общаться через Интернет от вашего имени. Вы можете не подозревать о таких действиях до тех пор, пока не станет слишком поздно. Создавать надежные пароли несложно. Для укрепления безопасности компьютера достаточно приложить незначительные усилия, с которыми можно познакомиться на сайте Microsoft по адресу http://www.microsoft.com/rus/athome/security/privacy/password.ms
Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, программ-шпионов и других возможных атак.

В настоящее время все большее распространение получают беспроводные сети. Это дает возможность путешествовать по Интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности. Если вы устанавливаете беспроводную сеть дома или собираетесь активно использовать беспроводными сетями общего назначения, прочитайте соответствующие разделы брошюры и обратите особое внимание на информацию по безопасности.
Принимайте необходимые меры предосторожности, пользуясь беспроводной связью!

Кибермошенничество — *один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.*

Предупреждение кибермошенничества

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.
2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.

3. Не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.
4. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.
5. Убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку:
    - Ознакомьтесь с отзывами покупателей.
    - Избегайте предоплаты.
    - Проверьте реквизиты и название юридического лица – владельца магазина.
    - Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois).
    - Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
    - Сравните цены в различных интернет-магазинах.
    - Позвоните в справочную магазина.
    - Обратите внимание на правила интернет-магазина.
    - Выясните, сколько точно вам придется заплатить.

Как справляться с кибермошенничеством

1. Проговорите с ребенком всю ситуацию. Он должен рассказать, какой сайт он посещал, на какие баннеры нажимал, какими услугами сети пользовался, что видел и т.д. Сохраните все электронные свидетельства совершенных действий и операций, скриншоты экранов – они могут служить доказательствами в дальнейшем.
2. Фишинг и вишинг: В случае хищения данных, поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета. Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.

Кибербуллинг — *преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully — драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Исследования буллинга начались еще в 70-х годов. прошлого века. Это поведение всегда присутствует в подростковой среде. В современном информационном обществе для буллинга все чаще используются инфокоммуникационные технологии. Буллинг, осуществляемый в*

виртуальной среде с помощью интернета и мобильного телефона, называют кибербуллингом. Многие исследования показывают, что кибербуллинг часто сопровождает традиционный буллинг.
Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

Предотвращение кибербуллинга

1. Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.
2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором, и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.
3. Обратите внимание на психологические особенности вашего ребенка. Специалисты выделяют характерные черты, типичные для жертв буллинга, они часто бывают: пугливы, чувствительны, замкнуты и застенчивы;тревожны, неуверены в себе, несчастны;склонны к депрессии и чаще своих ровесников думают о самоубийстве;не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками; мальчики могут быть физически слабее своих ровесников.
4. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.
5. Объясните детям, что личная информация, которую они выкладывают в интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.
6. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.
7. Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в интернете.
8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под статьи действия уголовного и административного кодексов о правонарушениях.

Как справляться с кибербуллингом

1. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.
2. Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).
3. Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он вам рассказал и показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ему уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
4. Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению кибер-буллинга.

Встречи с незнакомцами и груминг

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

Предупреждение встреч с незнакомцами и груминга

1. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети — с ровесниками или людьми старше себя.
2. Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии или видео.
3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также нехорошо ставить на аватарку фотографии других людей без их разрешения.
4. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя.

Помогите ему выбрать ник, не содержащий никакой личной информации.

5. Объясните ребенку опасность встречи с незнакомыми людьми из интернета. В сети человек может представиться кем угодно, поэтому на реальную встречу с интернет-другом надо обязательно ходить в сопровождении взрослых.
6. Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Постарайтесь сами поговорить с ребенком на эту тему. Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в интернете тема любви часто представляется в неправильной, вульгарной форме. Важно, чтобы ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время.

Как противостоять грумингу

1. Если ребенок желает познакомиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу
2. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию
3. Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он рассказал или показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ребенку уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
4. Сохраните все свидетельства переписки и контактов незнакомца с ребенком (скриншоты экрана, электронные письма, фотографии и т.п.).
5. При обнаружении признаков совращения следует немеделенно сообщить об этом в правоохранительные органы.
6. Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению груминга.

Контентные риски

К контентным рискам относятся материалы (тексты, картинки,аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска.

Противозаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.

Вредоносный (опасный) контент - контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков. Неэтичный контент - контент, который не запрещен к

распространению, но может содержать информацию,способную оскорбить пользователей.Подобное содержимое может распространяться ограниченно (например, "только для взрослых").

Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения,способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти сообещния, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы,психологического развития, социализации, а также физического здоровья детей и подростков.

Рекомендации по предупреждению контентных рисков

1. Используйте специальные технические средства, чтобы ограничивать доступ ребенка к негативной информации – программы родительского контроля и контентной фильтрации, настройки безопасного поиска. Часто пакет функций родительского контроля уже есть в вашей антивирусной программе. Программы родительского контроля позволяют: установить запрет на посещения сайтов различного негативного содержания, сайтов онлайн-знакомств, сайтов с вредоносным содержимым; ограничить время доступа ребенка к интернету; производить мониторинг переписки в социальных сетях и онлайн мессенджерах (чатах); блокировать сомнительные поисковые запросы в поисковых системах; блокировать баннеры; а также отслеживать все действия ребенка в сети.
2. Если ребенок пользуется общим компьютером, для каждого члена семьи создайте свою учетную запись на компьютере. Ваша учетная запись должна иметь надежный пароль и обладать правами администратора, чтобы ребенок не мог менять установленные вами настройки и программы.
3. Регулярно следите за активностью вашего ребенка в сети. Просматривайте историю посещений сайтов, чтобы быть уверенным, что среди них нет опасных. При необходимости обновляйте настройки технических средств безопасности.
4. Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Необходимо проверять информацию, увиденную в интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных. Расскажите об этих правилах вашим детям.
5. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок может продолжить поиск подобных ресурсов. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов.
6. Важно помнить, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую могут выступать более эффективными средствами для обеспечения безопасности вашего ребенка, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Интернет-зависимость — *навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. (Гриффит В., 1996). По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет. Исследователи отмечают, что большая часть Интернет-зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.*

Предупреждение интернет-зависимости

1. Оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.
2. Поговорите с ребенком о том, чем он занимается в интернете. Социальные сети создают иллюзию полной занятости — чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить — ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.
3. Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.
4. Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в интернет с помощью телефона или иных мобильных устройств во время урока.

Как справляться с интернет-зависимостью

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.
2. Не запрещайте ребенку пользоваться интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.

3. Ограничьте возможность доступа к интернету только своим компьютером или компьютером, находящимся в общей комнате — это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.
4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий — например, от бездумного обновления странички в ожидании новых сообщений.
5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями — при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с интернетом увлечения, которым он мог бы посвящать свое свободное время.
6. Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без интернета. Важно, чтобы ребенок понял — ничего не произойдет, если он на некоторое время «выпадет» из жизни интернет-сообщества.
7. В случае серьезных проблем обратитесь за помощью к специалисту. Информацию, куда обращаться вы можете найти в разделе Полезная информация.

информация с сайта http://detionline.com/helpline/rules/parents

Повысьте уровень безопасности вашего компьютора

Если на вашем компьютере установлена операционная система Microsoft® Windows® XP Service Pack 2, то можно использовать Windows Security Center. Эта программа позволяет просматривать информацию о состоянии защиты компьютера и изменять настройки, а также получать дополнительные сведения по вопросам безопасности.

Security Center показывает состояние трех важных компонентов безопасности: брандмауэра Интернета, антивирусных программ и службы автоматического обновления. Кроме того, он служит для перехода к другим разделам безопасности, а также поиска технической поддержки и ресурсов, имеющих отношение к защите компьютера.

Security Center работает в фоновом режиме, постоянно проверяя состояние трех наиболее важных компонентов.

Для того чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Центр обеспечения безопасности/Security Center;
- убедитесь, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).

Включить или отключить брандмауэр и автоматическое обновление вы можете непосредственно в Центре обеспечения безопасности.

Для управления защитой от вирусов обратитесь к настройкам установленного антивирусного

программного обеспечения.

Установите на вашем компьюторе антишпионские настройки или дополнительное антишпионское программное обеспечение

Шпионскими называются программы, выполняющие определенные действия (например, сбор личной информации или изменение настроек) без согласия и контроля пользователя. Они могут существенно замедлить работу системы и привести к нежелательным изменениям в важных настройках.

Такие программы трудно удалить. Антишпионское программное обеспечение поможет избавиться от шпионских и других нежелательных программ. Проверка компьютера может выполняться по расписанию в удобное для вас время.

Для того чтобы предотвратить появление шпионского программного обеспечения на вашем компьютере,необходимо убедиться в том, что включены основные средства Центра обеспечения безопасности вашей операционной системы.

Рекомендуется также для повседневной работы использовать учетную запись с ограниченными правами.

Для удаления шпионского программного обеспечения, попавшего на ваш компьютер, следует воспользоваться специальным антишпионским программным обеспечением, в частности, следующими программами: Windows Defender; Malicious Software Removal Tool.

Эти бесплатные программы вы можете загрузить с сайта http://www.microsoft.com/downloads

Для этого в строке Search в выпадающем списке выберите All Downloads, в строке справа введите название одного из указанных выше продуктов и нажмите кнопку Go.

Блокируйте доступ к неподходящим материалам

Один из наилучших способов защиты от нежелательной информации – это блокирование доступа еще до того, как она может быть получена.

Microsoft предлагает несколько таких способов.

Для того чтобы блокировать доступ к нежелательной информации в Internet Explorer® и MSN Explorer, нужно выполнить следующее:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/ Control Panel;
- в панели управления откройте Свойства обозревателя/Internet Options;
- в появившемся окне перейдите на вкладку Содержание/Content;
- в разделе Ограничение доступа/Content Advisor нажмите кнопку Включить/Enable;
- в появившемся окне введите пароль, который будет защищать вводимые вами ограничения от изменения детьми;
- в окне Ограничение доступа/Content Advisor вы можете блокировать доступ к нежелательной информации.

Повысьте уровень безопасности ребенка с электронной почтой OUTLOOK® EXPRESS.

Для повышения уровня безопасности при работе ребенка с электронной почтой в меню программы Outlook® Express в разделе Сервис/Tools выберите команду Параметры/Options.
Перейдите на вкладку Безопасность/Security.
При помощи переключателя выберите зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use вы можете уменьшить вероятность появления вирусов на вашем компьютере. Для этих же целей служит переключатель Не разрешать сохранение или открытие вложений, которые могут содержать вирусы/Do not allow attachments to be saved or opened that could potentially be a virus. Если же виру все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочку Предупреждать, если приложения пытаются отправить почту от моего имени/Warn me when other applications try to send mail as me.
Для защиты пересылаемых писем от подделки и от возможности перехвата и прочтения кем-либо, кроме указанного получателя, есть возможность Шифровать содержимое и вложения всех исходящих сообщений/Encrypt content and attachments for all outgoing messages и Подписывать все отправляемые сообщения/Digitally sign all outgoing messages.

Заблокируйте поступление спама

Чтобы блокировать поступление спама (нежелательной почты), необходимо воспользоваться почтовым сервером, имеющим защиту от спама (например, hotmail.com), или почтовым клиентом, имеющим спам-фильтр (например, Microsoft Outlook).
Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере hotmail.com, необходимо зайти в этот почтовый ящик и перейти по ссылке Options и в вертикальном меню выбрать вкладку Mail.
Перейдя по ссылке Junk E-mail Filter, вы можете изменить настройки фильтра нежелательной почты.
При помощи ссылки Block Senders, находящейся на вкладке Mail, вы можете добавить любого отправителя в список заблокированных, при этом почта от этого отправителя не будет поступать в ваш почтовый ящик.
В случае, если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.
Для настройки этого фильтра в меню Microsoft Outlook выберите Сервис/Tools, в открывшемся меню выберите команду Параметры/Options. В открывшемся диалоговом окне перейдите на вкладку Настройки/Preferences и нажмите кнопку Нежелательная почта/Junk E-mail.
В появившемся диалоговом окне вы можете внести изменения в настройки фильтра нежелательной почты.
Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

Создайте отдельные учетные записи для разных пользователей

Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой «Мои документы». Родитель может создать себе учетную запись администратора, дающую полный контроль над компьютером, а детям – ограниченные учетные записи. Пользователи с ограниченными учетными

записями не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение, включая большинство игр, медиаплееров и программ поддержки чатов.

Для того чтобы создать отдельную учетную запись для ребенка с ограниченными правами доступа для работы в Интернете, необходимо выполнить следующие действия:

- нажмите кнопкуПуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Учетные записи пользователей/User Accounts;
- в открывшемся окне выберите Создание учетной записи/Create a new account, введите ее имя;
- на этапе выбора типа учетной записи установите переключатель в положение Ограниченная запись/Limited;
- после нажатия кнопки Создать учетную запись/Create Account процесс создания учетной записи с ограниченными правами будет завершени ваш ребенок сможет выбрать ее при следующем входе в систему.

Повысьте уровень конфиденциальности при общении вашего ребенка в интернете с помощью INTERNET EXPLORER.

Сохранение конфиденциальности личной информации вашего ребенка при его работе в Интернете является важным механизмом безопасности.

Для того чтобы повысить уровень конфиденциальности при общении вашего ребенка в Интернете, выполните следующие действия:

- нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Свойства обозревателя/Internet Options;
- в появившемся окне перейдите на вкладку Конфиденциальность/Privacy;
- при помощи ползунка выберите необходимый уровень конфиденциальности.

Создавайте надежные пароли

Пароли – это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета кредитных карт, обратиться за ипотекой или даже общаться через Интернет от вашего имени. Вы можете не подозревать о таких действиях до тех пор, пока не станет слишком поздно. Создавать надежные пароли несложно. Для укрепления безопасности компьютера достаточно приложить незначительные усилия, с которыми можно познакомиться на сайте Microsoft по адресу http://www.microsoft.com/rus/athome/security/privacy/password.ms

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

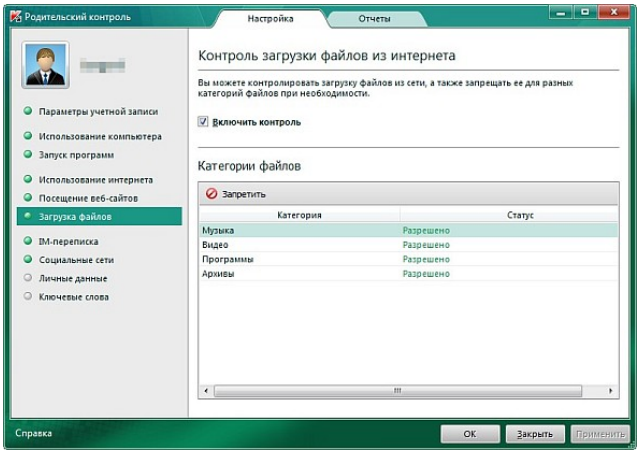
В настоящее время все большее распространение получают беспроводные сети. Это дает возможность

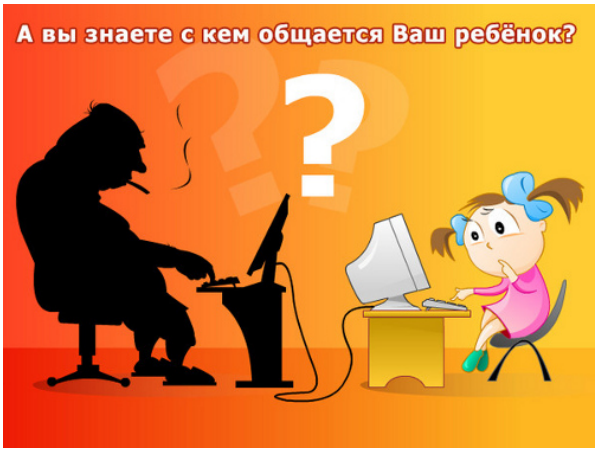
путешествовать по Интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности. Если вы устанавливаете беспроводную сеть дома или собираетесь активно использовать беспроводными сетями общего назначения, прочитайте соответствующие разделы брошюры и обратите особое внимание на информацию по безопасности. Принимайте необходимые меры предосторожности, пользуясь беспроводной связью!

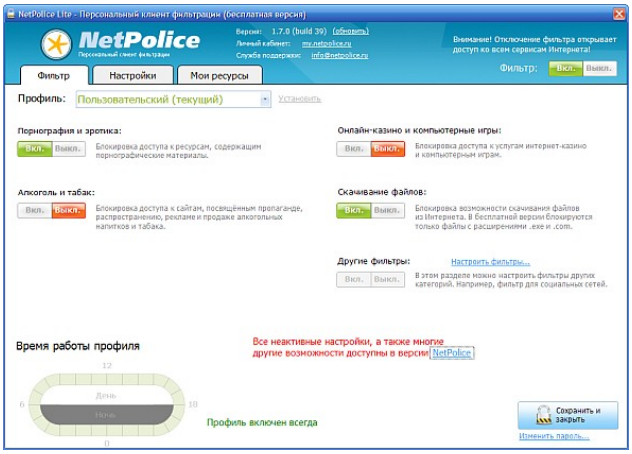
Обзор программ родительского контроля:

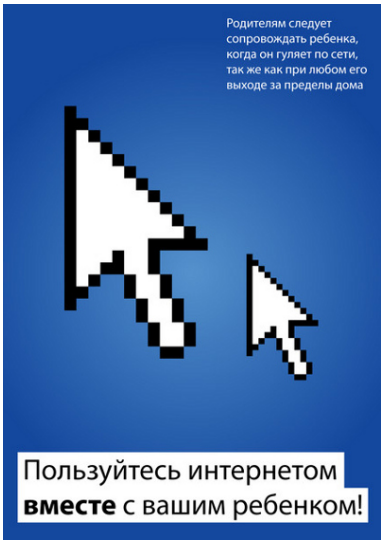
-KinderGate Родительский Контроль
-«Интернет Цензор»
-Детский интернет фильтр КиберПапа
-КиберМама™
-Детский браузер Гогуль
-Поисковая система детских сайтов "АгА"
-NetKids
-KidsControl
-«Один Дома»
-Система контроля доступа к интернету Rejector
-Интернет-фильтр SkyDNS

Приложение 6. ***Схемы, диаграммы, фотографии, карты, ксерокопии архивных материалов***






NetPolice Lite - Персональный клиент фильтрации (бесплатная версия)
NetPolice
Персональный клиент фильтрации
Версия: 1.7.0 (build 39) (обновить)
Личный кабинет: my.netpolice.ru
Служба поддержки: info@netpolice.ru
Внимание! Отключение фильтра открывает доступ ко всем сервисам Интернета!
Фильтр
Настройки
Мои ресурсы
Фильтр: Вкл. Выкл.
Профиль: Пользовательский (текущий)
Установить
Порнография и эротика:
Вкл. Выкл.
Блокировка доступа к ресурсам, содержащим порнографические материалы.
Онлайн-казино и компьютерные игры:
Вкл. Выкл.
Блокировка доступа к услугам интернет-казино и компьютерным играм.
Алкоголь и табак:
Вкл. Выкл.
Блокировка доступа к сайтам, посвящённым пропаганде, распространению, рекламе и продаже алкогольных напитков и табака.
Скачивание файлов:
Вкл. Выкл.
Блокировка возможности скачивания файлов из Интернета. В бесплатной версии блокируются только файлы с расширениями .exe и .com.
Другие фильтры:
Настроить фильтры...
Вкл. Выкл.
В этом разделе можно настроить фильтры других категорий. Например, фильтр для социальных сетей.
Время работы профиля
Все неактивные настройки, а также многие другие возможности доступны в версии NetPolice
12
День
6
10
Ночь
0
Профиль включен всегда
Сохранить и закрыть
Изменить пароль...


Родителям следует сопровождать ребенка, когда он гуляет по сети, так же как при любом его выходе за пределы дома
Пользуйтесь интернетом
вместе с вашим ребенком!


Безопасность ребенка в Интернете. Памятка родителям.
Договоритесь с ребенком, сколько времени он будет проводить в Интернете. Для каждого возраста должна быть своя норма – чем старше ребенок, тем дольше он может находиться в Сети
Приучите детей к тому, что нельзя раскрывать свои личные данные в Интернете. Если сайт требует ввода имени, помогите ребенку придумать псевдоним, не раскрывающий никакой личной информации.
Объясните детям, что в Интернете человек может быть не тем, за кого он себя выдает. Двенадцатилетняя девочка из чата может в реальной жизни оказаться сорокалетним дядей.
Расскажите ребенку, что такое Интернет-пространство. Объясните, что Интернет – это в первую очередь помощник в поиске информации и в образовании.
Предупредите ребенка о том, что в Сети он может столкнуться с опасным контентом (наркотики, порнография), кибербуллингом и злоумышленниками. При встрече с опасным контентом ребенок должен рассказать о нем родителям.
Расскажите ребенку о мошенничестве в Сети – розыгрышах, лотереях, тестах. Приучите его никогда без ведома взрослых не отправлять СМС, чтобы получить куда-то доступ или информацию из Интернета.
Беседуйте с детьми об их виртуальных друзьях. Если ребенок хочет встретиться с Интернет-другом в реальной жизни, то перед этим он обязательно должен посоветоваться с родителями.
Приз!
Приз!
РОССИЯ - БЕЗ ЖЕСТОКОСТИ К ДЕТЯМ!

http://images.rambler.ru/search?query=%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C+%D0%B2+%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5

безопасность в интернете

Приложение 7.
Примерная тематика открытых мероприятий

1. Родительское собрание “Компьютер в жизни школьника”. http://dorohovo-school.edusite.ru/p401aa1.html
2. 2.Родительское собрание “*Механизм обеспечения информационной безопасности учащихся в школе при использовании Интернета”, http://www.bibliofond.ru/view.aspx?id=563232*
3. Родительское собрание “Информацилнная безопасность”, - http://www.metod-kopilka.ru/page-4-1-12-18.html
4. Родительское собрание “Безопасность в сети интернет”, - http://moi-mummi.ru/publ/drugie_napravlenija_pedagogicheskoj_dejatelnosti/roditelskie_sobranija/roditelskoe_ranie_v_5_klasse_na_temu_quot_bezopasnost_detej_v_seti_internet_quot/94-1-0-460
5. Выступление классного руководителя на родительском собрании: «Информационная безопасность школьника»: - http://rudocs.exdat.com/docs/index-11939.html
6. Лекторий “Обеспечение информационной безопасности при работе с Интернет “,- http://do.gendocs.ru/docs/index-177396.html?page=3
7. Единое городское родительское собрание “Информационная безопасность семьи и ребенка”, - http://www.sibchildren.ru/egrs-2012
8. Родительский всеобуч, встреча с родительской общественностью: «Актуальные проблемы безопасностиобразовательной среды: мониторинг как инструмент выявления проблемных зон» ,- http://www.educom.ru/ru/works/education_prof/detail.php?ID=40915
9. Родительское собрание “Правила безопасности и этикета в Интернете для подростка.”, - http://shuruto.blogspot.ru/2009/07/blog-post_