

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОСВЕЩЕНИЯ РОССИИ)

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный педагогический университет им. В. Шаталова»

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
для педагогов по организации и проведению просветительских
мероприятий с подростками и родителями по вопросам
обеспечения информационной безопасности и профилактики
компьютерной зависимости у обучающихся**

*Издание методических рекомендаций осуществляется в рамках выполнения Государственного задания
Министерства просвещения Российской Федерации № 1024122500024-1-5.3.1;6.2.3;6.2.1;5.1.1
по теме «Механизмы обеспечения безопасности детства в контексте социально-культурных изменений
во взаимодействии социальных институтов, семей и детей с разной социальной активностью»*

УДК 371
ББК 74.2
М54

*Рекомендовано к изданию на заседании учёного совета
ФГБОУ ВО «Донецкий государственный педагогический университет
им. В. Шаталова»
(протокол № 16 от 27.06.2025 г.)*

Рецензенты:

Зябрева С.Э. – кандидат педагогических наук, доцент, заведующий кафедры педагогики и методики преподавания иностранных языков ФГБОУ ВО «ДГПУ им. В. Шаталова»;

Картавцева А.П. – кандидат педагогических наук, доцент, доцент кафедры педагогики Филиала Кузбасского государственного технического университета им. Т. Ф. Горбачева в г. Прокопьевске.

М54 **Рудковская И. В.**, Методические рекомендации для педагогов по организации и проведению просветительских мероприятий с подростками и родителями по вопросам обеспечения информационной безопасности и профилактики компьютерной зависимости у обучающихся / И.В. Рудковская. – Горловка Изд-во ФГБОУ ВО «ДГПУ им. В. Шаталова», 2025. – 52 с.

ISBN 978-5-907859-44-9

УДК 371
ББК 74.2

ISBN 978-5-907859-44-9

СОДЕРЖАНИЕ

Пояснительная записка	4
1. Основные термины и понятия	5
2. Список сокращений	7
3. Теоретические аспекты информационной безопасности	8
3.1. Ключевые понятия проблем информационной безопасности	8
3.2. Классификация Интернет-угроз	8
3.3. Информационная безопасность подростков в современном мире: психологические аспекты проблемы	9
3.4. Психолого-педагогические подходы к развитию ресурсов устойчивости подростков к интернет-рискам и угрозам	10
4. Информационная безопасность в современных образовательных учреждениях	12
4.1. Современное состояние обеспечения информационной безопасности в образовательных учреждениях	12
4.2. Урочная и внеурочная деятельность по обеспечению информационной безопасности детей-подростков	14
4.3. Критерии оценки состояния информационной безопасности детей и подростков (рекомендации для родителей, педагогов)	15
4.4. Урочная и внеурочная деятельность по обеспечению информационной безопасности подростков	17
Список литературы	23
Приложения	56
Приложение 1. Анкета для выявления оценки осведомленности учащихся разных возрастов о понятии «Информационная безопасность»	26
Приложение 2. Памятка для родителей «безопасность подростков в Интернете:	26
Приложение 3. Урок – лекция «что такое информация и ее роль в нашей жизни»	29
Приложение 4. Урок – беседа «каким источникам информации следует доверять»	31
Приложение 5. Урок – диспут «Интернету: да или нет?».	32
Приложение 6. Урок – практическая работа «обработка информации»	33
Приложение 7. Урок – конференция «любимый источник информации»	34
Приложение 8. Классный час на тему: «Основы информационной безопасности подростков»	35
Приложение 9. Единый тематический час на тему: «Безопасность подростков в сети Интернет: виды интернет-преступлений и способы их предупреждения»	37
Приложение 10. Родительское собрание: «Безопасность детей в сети Интернет»	39
Приложение 11. Занятия с элементами тренинга для педагогов, подростков и их родителей Тема: Безопасность подростков в Интернет-сети	47

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

За последнее десятилетие сеть Интернет прочно вошла в жизнь современного общества и стала важным современным источником информации и средством общения. Подрастающее поколение сегодня не может себе представить мир без смартфона и планшета, браузера и онлайн-игр. Стремительное развитие электронных средств информации и коммуникации заставляет задуматься над тем, как они влияют на образ жизни, воспитание и личностное становление подрастающего поколения. И задача взрослых рассказать подросткам об основных правилах безопасного использования сети Интернет.

Исходя из данных Института развития Интернета можно четко констатировать, что сегодня Интернетом пользуются 76% россиян. Растет и число школьников, ежедневно использующих социальные сети. Результаты мониторинга Фонда «Национальные ресурсы образования», проведенного среди 2500 школьников от 13 до 18 лет в 84 регионах России, показывают, что 50% ребят заходят в социальные сети более девяти раз в день. Чаще всего школьники используют социальные сети для переписки с друзьями – 83%, для чтения постов и просмотра новостной ленты – 74%, для прослушивания музыки – 70%, для размещения фотографий – 26%. Технический прогресс делает информацию все более доступной.

И если раньше основными угрозами, которые таит в себе увлечение компьютером и Интернетом, взрослые считали нарушение зрения, осанки, развитие зависимости и нежелательный контент, то сегодня все чаще называются такие явления, как потеря конфиденциальности, кибербуллинг, фейкньюз, финансовое мошенничество. 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. Поэтому школы и родители должны осуществлять взаимодействие по формированию у подростков базовых знаний, связанных с правилами безопасного пользования Интернет-ресурсами.

Цель методических рекомендаций – разносторонняя поддержка направления работы образовательных организаций региона по обеспечению информационной безопасности подростков. Пособие поможет педагогам актуализировать и дополнить свои представления о нормативно-правовых основах обеспечения информационной безопасности подростков, о существующих рисках и угрозах в данной сфере; и составить план воспитательной работы по взаимодействию с подростками и родителями для обеспечения информационной безопасности подростками и работы по реализации основных направлений деятельности по обеспечению информационной безопасности в образовательной организации

Результатом использования данных методических рекомендаций должно стать овладение руководителями образовательных организаций, педагогами, обучающимися и их родителями опытом контроля деятельности подростков 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 кибербезопасности, 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.

Методические рекомендации предназначены для руководителей учебных учреждений, педагогов и родителей по обеспечению информационной безопасности подростков и разработаны в рамках темы «Механизмы обеспечения безопасности детства в контексте социально-культурных изменений во взаимодействии социальных институтов, семей и детей с разной социальной активностью».

1. 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.

Видеохостинг – 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-what-is.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/glossarii>

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

Кибербуллинг (cyber-bullying) – агрессивное, 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. 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>

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

Интернет-зависимость (или Интернет-аддикция) – 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/>

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.

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/%C3%F5%F6%F1%F5%F2%F5%F2%FF%F9_%FD%FA%F0%F0%FD

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: ФИО пользователя; его 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%E%8%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 этикет (нетикет)** – правила поведения, общения в Сети традиции и культура интернет-сообщества, которых придерживается большинство. <http://ru.wikipedia.org/wiki/>

2. СПИСОК СОКРАЩЕНИЙ

1. **Ace** – “**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 сообщениями 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», «права», «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-ай], по-русски чаще говорят [j/w]. URI – это последовательность символов, идентифицирующая абстрактный или физический ресурс. Ранее назывался Universal Resource Identifier – универсальный идентификатор ресурса.
21. **Акеу** – 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 также обезопаситься от деятельности органов государственной безопасности, известной под названием анализ трафика. Сервис Тог 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.

3. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Ключевые понятия проблем информационной безопасности

Документ, который регламентирует информационную безопасность государства – Доктрина информационной безопасности Российской Федерации – система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646- [Доктрина...,2016]

Согласно Доктрине, информационная безопасность рассматривается как состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В Российском законодательстве информационная безопасность детей рассматривается как состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [2]. Такую защищенность ребенку могут и должны обеспечить, прежде всего, значимые взрослые.

Рассмотрим некоторые ключевые понятия проблем касающихся информационной безопасности детей и подростков:

Информационная грамотность – поиск, интерпретация, оценка различных источников информации, работа с видами учебных, деловых и научно-популярных текстов.

Информационная культура – совокупность материальных и духовных ценностей в области информации.

Медиаграмотность – это грамотное использование подростками их родителями и педагогами инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков. Медиаграмотность является компонентом информационной культуры. Наличие информационной культуры предполагает также степень овладения личностью навыками поиска, передачи, обработки и анализа информации, особыми методами и технологиями.

Здесь следует говорить, как о формировании медиаграмотности (о грамотности в области восприятия, понимания, интерпретации текстов СМИ), так и об информационной грамотности (комплексе наиболее общих умений и навыков работы с информацией).

Информационный иммунитет – способность личности отражать негативное влияние информационной среды, выражающаяся в умении выявлять информационные угрозы, определять степень их опасности и умело противостоять им. Адекватное восприятие и оценка информации, ее критическое осмысление на основе нравственных и культурных ценностей.

Часто педагоги подменяют вышеобозначенные понятия.

Трудности с трактовкой связаны с тем, что как педагогический феномен информационная безопасность стала рассматриваться относительно недавно. Данные понятия обосновывались представителями разных научных школ и направлений. Основополагающим в решении споров стало принятие Федерального закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Законодатель и определил главенство терминологии. Таким образом, первичная информационная безопасность, комплекс мер и мероприятий в формировании информационной безопасности способствует развитию информационной грамотности, информационной культуры, медиаграмотности. И, как итог, информационный иммунитет – интегративное качество, позволяющее ребенку чувствовать себя защищенным, социализированным, способным успешно жить и развиваться в современном мире.

3.2 Классификация Интернет-угроз

Электронная безопасность

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

Вредоносные программы

Вредоносные программы – это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное программное обеспечение и различные формы вредоносных кодов.

Спам

Спам – это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

Кибермошенничество

Кибермошенничество – это один из видов киберпреступлений, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Контентные риски

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

Неподобающий контент

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, 3 считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Незаконный контакт

Незаконный контакт – это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

Киберпреследования

Киберпреследование – это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование. Защита детей от информационных угроз и рисков Интернет-ресурсов связана с формированием медиаграмотности. В образовательных учреждениях данная задача может решаться педагогами с использованием различных форм медиаобразования.

Медиа-грамотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.

Медиаобразование выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, способствует осознанному участию детей и подростков в медиасреде и медиакультуре, что является одним из необходимых условий эффективного развития гражданского общества. Защиту детей от информации, причиняющей вред их здоровью и безопасности, прежде всего, семья и школа. Это задача не только семейного, но и школьного воспитания. Проведение уроков медиа безопасности планируется в образовательных учреждениях на постоянной основе, начиная с первого класса, в рамках школьной программы (в том числе уроков ОБЖ).

Цель проведения уроков медиа безопасности – обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

К информации, запрещенной для распространения среди детей и подростков, относится информация:

- 1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- 2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- 3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- 4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- 5) оправдывающая противоправное поведение;
- 6) содержащая порнографического характера. На сайте «Дети онлайн» родители и педагоги найти рекомендации, которые помогут вам обеспечить медиабезопасность детей и подростков в сетях Интернет и мобильной (сотовой) связи. Также значимой является работа с родителями по формированию у них базовых знаний, связанных с правилами безопасного пользования Интернет-ресурсами.

3.3 Информационная безопасность подростков в современном мире: психологические аспекты проблемы

Появление новых технологий воздействует на общество в целом, однако последствия этого влияния разнятся в тех или иных возрастных группах. Представители различных возрастных и социальных групп превратились в активных пользователей новых технологий, возраст дебюта столкновения с новыми технологиями постепенно снижается. В целом можно говорить о том, что средства массовой коммуникации (СМК) становятся одним из ведущих институтов социализации, формируя картину мира, транслируя ценности, задавая нормы и паттерны поведения, а также стратегии социального взаимодействия. Более того, с появлением и развитием новых медиа именно они начинают играть первостепенную роль, отстраняя привычные формы медиа.

В литературе появилось и активно используется понятие «цифровое поколение», указывающее на новое поколение детей и подростков, социализация которых происходит в эпоху существования новых коммуникативных технологий, новых медиа [Livingstone, 2018]. Исследователи предлагают говорить об информационной социализации, ибо дети и подростки оказываются в совершенно новой ситуации – словами «... подрастающее поколение развивается в принципиально новом социальном и информационном пространстве, в котором слова «информационная культура» являются не абстрактным понятием, но живой реальностью» [Марцинковская, 2012].

Реальность, в которой живут современные дети и подростки, не сравнима с той, в которой социализировались их родители. С одной стороны, скорость, с которой дети и подростки осваивают новые технологии, не имеет аналогов в прошлом. Как следствие, отношения, которые складываются между поколениями родителей и детей, приобретают определенную специфику. С другой стороны, этот процесс можно сопоставить с тем, что происходит в ситуации столкновения с инокультурной средой, когда дети и подростки оказываются проводниками адаптации к новой культуре.

Формируется информационное пространство, своего рода социокультурное пространство, в котором живут и действуют люди, возникает новый язык интернет-коммуникации. Интернет – это не только популярный источник, а также средство коммуникации. Причем развитие социальных сетей модифицирует коммуникацию, вносит свою специфику в выработку норм,

регламентирующих взаимодействие участников коммуникации, трансформирует понимание того, где проходит граница между публичной и частной сферами.

Результаты отечественных и европейских исследований свидетельствуют о том, семилетние дети уже используют Интернет без контроля со стороны родителей, а в возрасте двенадцати лет подростки имеют более или менее регулярные контакты в различных социальных сетях. 38,8% пользователей популярных социальных сетей составляют дети и подростки в возрасте до 18 лет [Информационная безопасность ..., 2017]

Эмпирические исследования последних лет подтверждают, что у детей и подростков «нормализуется» процесс постоянного нахождения в Интернете, пребывания в контакте с другими. Как следствие, возникает так называемое «проблемное использование Интернета», которое характеризуется некоторой когнитивной озабоченностью Интернетом, когда индивид едва ли способен контролировать использование Интернета, а выход в Сеть позволяет избавиться от эмоционального дистресса, успокоиться [Livingstone, 2018].

На основе исследований, направленных на анализ риска, которому подвергаются дети и подростки, используя Интернет, представляется возможным говорить о четырех общих категориях риска [Livingstone, 2018].

Во-первых, это риск, связанный с содержанием материалов, представленных в Интернете. Речь идет о тех ситуациях, в которых дети получают доступ к нелегальной информации, несущей вред их здоровью и развитию (в наибольшей степени это касается насилия, сексуального содержания, ненависти, самоубийства, наркотиков).

Во-вторых, это риск, связанный с контактами. Используя социальные сети, а также участвуя в дискуссиях (чаты, форумы и пр.) дети и подростки могут завести нежелательное знакомство с кем-то, кого они потом могут встретить в реальной жизни. С нашей точки зрения, нежелательные контакты характеризуются еще и тем, что подростки в социальных сетях становятся объектом пропаганды, как следствие, подвергаются радикализации, а в результате вовлекаются в террористическую активность. Этот аспект необходимо подвергнуть самому тщательному анализу и изучению, принимая во внимание показатели радикализации и роста экстремизма в подростково-молодежной среде [Тихонова; Ernst-Vintila, 2016].

У нежелательных контактов в Сети есть и еще одна сторона. Дети и подростки, бесконтрольно использующие Интернет, становятся жертвами кибербуллинга. Эта форма буллинга имеет еще более негативные последствия, чем буллинг в реальной ситуации, ибо расширяется круг наблюдателей; такой вариант буллинга в меньшей степени регулируем, чем школьный буллинг, кроме того, материалы, помещенные в Сети, сохраняются там в течение длительного времени [Инф. Безопасность..., 2017]

Избыточное пребывание в Интернете связывается с уязвимостью по отношению к значительному числу явлений, угрожающих подростку, будь то насилие, нарушение приватности, столкновение с изображениями порнографического содержания.

На основании результатов недавнего исследования, проведенного Московским институтом психологии (РФ) и посвященного изучению социальных представлений о здоровье в группах детей и подростков (наряду с вопросами о здоровье мы задавали вопросы, направленные на выявление особенностей стиля жизни детей и подростков), можно говорить о том, что из 479 опрошенных учеников вторых классов (возраст от 7 до 9 лет) 375 учеников заявили, что используют Интернет с различной частотой – от одного раза в месяц до ежедневного использования, 117 из них (31,2%) подвергались оскорблениям в Интернете. Для учеников седьмых классов результаты таковы: из 419 опрошенных 412 используют Интернет, причем в 12–14-летнем возрасте это становится в наибольшей степени повседневной практикой; 154 ученика из 412 заявили о том, что становились объектами оскорблений в Интернете. Сравнение с помощью фи-критерия (1,83, $p < 0,05$) говорит в пользу того, что подростки в большей степени констатировали факты оскорблений, чем дети, что может быть объяснено рядом факторов, среди которых – более высокая активность в Сети, особенности подросткового возраста и др. [Информационная безопасность..., 2017].

Все эти факты, несомненно, указывают на крайнюю важность и необходимость разработки и реализации ряда мер, адресованных детям, подросткам, а также их родителям в связи с угрозами различного рода, обусловленными бесконтрольным использованием Интернета.

Сегодня специалисты заняты поиском того, как сделать информацию, распространяемую посредством СМК, безопасной для детей и подростков, а также научить их самих, а также их родителей пользоваться Интернетом, снизить негативное влияние различных факторов. Однако даже разработанные меры не улучшат ситуацию автоматически. Чрезвычайно важно снизить для подростков риски, связанные коммуникацией посредством Интернета, и это первостепенная задача ближайшего окружения детей и подростков.

3.4 Педагогические условия обеспечения безопасности деятельности подростков в информационной цифровой среде

XXI век – это время технологий, которые присутствуют во всех сферах жизни современного человека. Подрастающее поколение, живущее в современном мире, легко осваивает компьютерную технику и информационные технологии, чувствуя себя в этом мире комфортно, потому что реальный и виртуальный миры стали неразделимы в их сознании и жизни.

В словаре финансовых терминов информационная среда рассматривается как совокупность технических и программных средств хранения, обработки и передачи информации, а также социально-экономических и культурных условий реализации процессов информатизации [Словарь фин. Терм]

Информационная цифровая среда обладает большим образовательным потенциалом. Реализация функционала информационной цифровой среды позволяет эффективно решать различные задачи как обучения, так и воспитания [Пустовойтов, Корнейков, 2021].

Мультимедийное гипертекстовое содержание, интерактивные методы и формы обучения, виртуальная образовательная среда – эти и другие атрибуты современного образования позволяют вовлечь школьников-подростков в учебно-воспитательный процесс, дают возможность учителю для профессионального творчества на основе использования средств ИК-технологий.

Вместе с тем, информационная цифровая среда несет на себе не только положительный потенциал для образования подростков, но и угрозы. Интернет пользуется особой популярностью у детей, в частности у подростков, потому что он предлагает им широкий спектр возможностей для выражения их индивидуальности, удовлетворения их образовательных и

коммуникативных потребностей. Об этом хорошо осведомлены интернет-террористы, интернет-мошенники, интернет-агрессоры и интернет-насилыники, которые открыто или скрыто продают наркотические средства, алкоголь и другие психоактивные вещества, занимаются половой распущенностью, пропагандой жестокости и насилия, расовой и национальной неприязни, агрессивного и суицидального поведения и т. П. Подросток не способный без помощи взрослого сообщества на адекватном критическом уровне оценить опасность получаемой информации чаще, чем люди других возрастных категорий попадает в «ловушки» подобного рода интернет-дельцов. Поэтому защита детей-подростков от интернет-угроз является первостепенной задачей не только для России, но и для всех развитых стран мира.

Выявление сущности влияния информационных угроз на подрастающее поколение и создание на этой основе действенного барьера негативному влиянию глобальной сети на молодежь – одна из ключевых задач системы образования, решение которой позволяет обеспечить защиту молодежи от негативного контента и угроз глобальной сети [Корнейков, 2021].

В этой связи следует выделить ряд педагогических условий, которые должны обеспечить безопасность деятельности подростков в информационной цифровой среде:

1. Целенаправленное формирование у подростков навыков безопасной работы в глобальной сети. Для этого в рамках учебных предметов (информатика, обществознание, право, основы безопасности жизнедеятельности) можно разбирать кейс-задания с реальными ситуациями, возникающими в цифровой среде, и способы их решения. Основные угрозы, с которыми сталкиваются подростки в цифровой среде можно подразделить на две группы: содержательный компонент, наносящий вред и действия со стороны злоумышленников (взлом аккаунтов, кибербуллинг) и вредоносного программного обеспечения (потеря, кража данных). Неоднократная встреча с данными угрозами может иметь последствия для нормального физического и психического развития детей и подростков, например, нарушение сна, избыточный вес, негативные эмоциональные состояния, суицидальное поведение и др. (Приложения 1-9).

Систематическое просвещение в сфере информационной безопасности подростков и их родителей. Это необходимо для согласованности действий всех участников образовательного процесса, а также повышает эффективность формирования общей информационной культуры. Поэтому основной задачей педагогов и родителей становится обеспечение безопасного взаимодействия детей и подростков с цифровой средой. В целом информационная безопасность для детей подразумевает состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и физическому, психическому, духовному, нравственному развитию (Приложение 10; 11).

1. Формирование профессионально-педагогической компетентности педагогов в сфере информационной безопасности. Для этого можно организовывать тренинговые занятия, позволяющие выделить наиболее опасные угрозы и осознать имеющиеся ресурсы и способы защиты от них (Приложение 12).

2. Организация исследовательской деятельности обучающихся. Исследовательская работа по изучению способов защиты от интернет-рисков и угроз может осуществляться в рамках программ внеурочных занятий, или через организацию работы школьных научных обществ, в рамках социального проектирования и т. П. (Приложение 12).

3. Привлечение к проведению мероприятий представителей различных заинтересованных ведомств и организаций. В качестве совместных мероприятий могут выступать круглые столы и интернет-батлы, открытые обсуждения и дискуссии.

Для того, чтобы обеспечить информационную безопасность обучающихся в образовательном учреждении, необходимо осуществить совместную деятельность руководства данного учреждения, педагогического коллектива и родителей обучающихся по снижению риска причинения недостоверной, агрессивно окрашенной информацией вреда физическому, психическому и духовно-нравственному здоровью и (или) развитию детей. Целесообразно обозначить необходимость повышения степени вовлеченности родителей в обеспечение информационной безопасности детей в сети Интернет. Чтобы действовать эффективно, родители должны быть обеспечены информацией по профилактике воздействия информационных угроз на здоровье и развитие их ребенка. Задача педагогов – обеспечить родителей данной информацией, организуя совместную работу педагогов, родителей и детей.

4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННЫХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

4.1. Современное состояние обеспечения информационной безопасности в образовательных учреждениях

На современном этапе компьютеризация и информатизация образовательных учреждений переживает этап стремительного роста.

Интернет стал необходимым условием системы компьютерного образования, так как охватывает общественный строй важнейших первоисточников – электронные библиотеки, музеи, тематические подборки материалов, профессиональные справочники, словари, клубы по интересам, а так же потому, что зачаток компьютерной грамотности на данный момент невозможен без очевидного демонстрирования и изучения способов выхода в Интернет, нахождение данных, взаимодействия с электронной почтой и возможностями персональных коммуникаций.

Оснащенные компьютерами классы в образовательных учреждениях без доступа к сети Интернет расцениваются как дефективные.

Интернет не только помогает детям в изучении простых и самых важных моментов информационных технологий, он также является местом для контакта детей и молодежи, пространством для их самореализации и созидания. Своеобразным примером служит лабораторный проект, в котором обучаемый разрабатывает свою Веб-страницу, где он описывает себя и свою семью, а также собственные интересы.

Создание и введение Интернета в школы, увеличит уровень и качество образовательных программ: это вероятность владеть заключительными данными, создавать дистанционное образование, тесты онлайн, учить иностранные языки, разрабатывать страницы образовательных учреждений в Интернете, на которых будет предоставлена интересующая информация, как для учителей, так и для обучающихся и их родителей.

Употребление Интернета в педагогическом процессе реализует способ увеличения интереса обучаемых и их взаимодействия со своими сверстниками, в том числе и за границей (получение разной информации, данных и жизни разных стран), возможность пользоваться электронными ресурсами: исследованиями, газетами, книгами, журналами, которые создаются в режиме онлайн.

Тем не менее, Интернет, независимо от образовательных задач, нередко применяется детьми для забав, например, сайтов подозрительного содержания (сайты сект, террористических организаций, сайты, для детей, не достигших восемнадцати лет и другие).

Ввиду того, что ученики часто увлекаются нахождением в сети Интернет, даже не находясь в школе, такие сети становятся назойливым замыслом и отрицательно сказываются на нервной системе детей из-за трудности проверки посещаемых сайтов. Еще одна проблема, которая стоит перед внедрением в школы Интернета это обязательный минимум защиты сети. Сеть в образовательных учреждениях обязана находиться под защитой от незапланированного проникновения, вандализма и взлома, а также, кражи и порчи информационных источников.

В соответствии с экономической и социальной ситуацией государства существует два элементарных противопоказания для устройства глобальной системы охраны данных:

1. Низкий доход образовательной информатизации;
2. Недостаток высококвалифицированного персонала для устройства системы охраны.

Благодаря этому очень важно гарантировать легкое, результативное и полноценное решение для создания информационной безопасности в образовательном учреждении [Турбина, 2022].

К счастью, в данный момент на рынке рекомендуется ряд возможностей для защиты сети. Такие возможности являются значительными и всецело идентичными для использования на уровне образовательных учреждений.

Так какой же именно способ защиты следует посоветовать для установления в школы?

Во-первых, установка, которая называется межсетевым экраном и реализует пакетную фильтрацию. Первостепенная функция такой установки давать возможность для выхода в Интернет для обучаемых и педагогов, но не пропускать сеть школы посторонних.

Во-вторых, если школы поддерживают связь в сети (друг с другом или с вышестоящими органами управления), рекомендуется пользоваться оборудованием виртуальных защищенных сетей, которые не допустят посторонних до важной и скрытой информации, а также увеличат надзор за доступом, выполняемым межсетевым экраном.

Первым из необходимых методов охраны данных стало противовирусное предупреждение. Другой, важный, но менее известный способ: контентная фильтрация. Технически она осуществляется разными способами, но ее целью является изолировать обучаемых от неоправданного контента. Намерения по компьютеризации школ совершенствуются и результатом всего этого должно послужить оснащение школ ресурсами информационной безопасности.

На данный момент большое внимание стало уделяться системе снабжения информационной безопасностью Net Школ. [NetSchool] «Net Школа» как составляющая школьного информационного пространства Нагибин Вячеслав ВикторовичМакарова Людмила Андреевна_2005

Net Школа совокупное информационное детище, которое содержит:

1. Устройство неделимой информационной среды образовательного учреждения: общеобразовательных школ, институтов, университетов, лицеев и тому подобное.
2. Дистанционное обучение в пределах образовательного процесса: подготовка способных детей, подготовка нетрудоспособных детей, подготовка приболевших детей, подготовка в системе дополнительного образования, подготовка детей из деревень и сельских поселений и так далее.
3. Устройство неделимой образовательной среды муниципального образования, для передачи данных для других образовательных учреждений, управлений образования, дошкольных учреждений и других. (система «Сетевой Город»).

При обучении в Net Школах решаются следующие задачи (таблица 2):

Задачи, решаемые при обучении в Net Школе на разные направления

Объект направления	Решаемые задачи
Администрация школы	получение и обобщение информации об учебном процессе для принятия решений; ведение личных дел сотрудников, учеников, родителей для создания отчетов; ведение расписания уроков, школьных и классных мероприятий; мониторинг движения учащихся; создание системы школьного документооборота; автоматизированное составление отчетности для управления образования;
Для обучающихся и родителей	доступ к электронному дневнику, куда автоматически выставляются оценки и где помечаются задолженности по предметам; доступ к последней версии расписания; получение отчетов об успеваемости и посещаемости, в том числе родители могут получать отчёты на мобильный телефон.
Для учителей-предметников	ведение электронного классного журнала, календарно-тематических планов, просмотр отчетов; организация тестирования (в т.ч. подготовка к ЕГЭ) с мощным механизмом подготовки и проведения тестирования всего класса; работа с мультимедийными учебными курсами, подключенными к электронному классному журналу; организация проектной деятельности; ведение индивидуальных портфолио учащихся и учителей; доступ к федеральному перечню учебных изданий и готовым планам к учебникам, утвержденным Министерством образования РФ;
Для всех участников учебно-воспитательного процесса	единая среда обмена информацией в рамках школы (доска объявлений, каталог школьных ресурсов, механизм портфолио, внутренняя электронная почта, форум, список именинников и т.п.), что улучшает взаимопонимание и сотрудничество между всеми участниками учебного процесса.

Важное свойство Net Школы в том, что большинство из этих задач реализуются совокупно, опираясь на единый доступ. Такая школа не только допускает сформировать единую информационную среду в образовательном учреждении, но также привлекает сотрудников школы, обучаемых и их родителей. Net Школа упорно подготавливается к потребностям определенного учебного заведения:

1. Можно эффективно наблюдать за изменениями в учебном процессе;
2. Можно устанавливать какой угодно тип учебного периода: полугодие, четверть или триместр;
3. Тактичный выбор оценок (не обязательно 5-балльная) шкала;
4. Тактичное устройство подгрупп по предметам и профилям в учебном плане;
5. Можно включить какое угодно число вариантов календарно-тематического планирования по предметам в классе;
6. Можно исключить какие угодно данные в документе Excel до следующего редактирования или печатания.

Исключительность данного вида состоит в его сетевой сложности. Net Школу возможно внедрить лишь на единственный компьютер, при этом выход в систему можно будет осуществлять с любого технического устройства (компьютера), подключенного к локальной сети образовательного учреждения. На компьютерах пользователей необходимо только ввести соответствующую стандартную программу браузера. Выход в Интернет при этом не требуется, потому что подключение осуществляется к серверу Net Школы.

При условии, когда в образовательных учреждениях проведен Интернет, то через него можно воспользоваться ресурсами данной школы. Возьмем, к примеру, электронные дневники, при подключении к сайту школы родителям предоставляется возможность просмотра дневников своих детей. Не менее важно сказать, что человек не обязательно должен сидеть при этом на рабочем месте, он имеет возможность выйти в систему с любого компьютера.

Это первая в России система, дающая возможность соорудить информационную среду образовательного учреждения, используя компьютер любого вида и с любой базой. Превосходство Net Школы для образования единой информационной среды заключается:

1. Net Школа это в первую очередь комплексная программа образовательного учреждения, а не система, выполняющая один тип деятельности (работу директора, завуча или другого персонала);
2. Такая программа вызывает инициативу в образовательном процессе, как ее сотрудников, так и обучающихся, и особенно их родителей;
3. Школа учит сотрудников, как правильно необходимо работать в сети, общей групповой работе, привлекает пользоваться современными технологиями;

4. Предоставляет шанс разрабатывать и сливать в систему свои учебные материалы.
5. Отстаивает международный эталон учебных курсов;
6. Высокоразвитая система взаимодействия между пользователями и совместной работой над проектами (доска объявлений, каталог школьных ресурсов, личное портфолио);
7. Школа обладает высокоразвитыми ресурсами для дистанционного обучения в рамках образовательной системы;
8. Спроектировано совершенно новое решение – «Сетевой Город» – для развития единого учебного пространства образовательных учреждений.

Таким образом, оценка состояния обеспечения информационной безопасности показал, что на данный момент устройство системы информационной безопасности лишь отчасти зависит от типа учебного заведения. В конечном итоге требуется присутствие дополнительного уровня безопасности для лицеев и гимназий в результате своеобразности и индивидуальности программ этих видов учебных заведений.

4.2. Организация информационно-безопасного образовательного процесса в школе. Взаимосвязь с родителями школьников в решении проблемы

Использование компьютерных технологий в учебном процессе отвечает психофизиологическому развитию учащихся, допускает простоту в организации занятий, оказывает заметное влияние на содержание, формы и методы обучения. Применение мультимедийных презентаций позволяет сделать уроки более интересными, включает в процесс восприятия не только зрение, но и слух, эмоции, воображение, помогает детям глубже погрузиться в изучаемый материал, сделать процесс обучения менее утомительным, позволяет повысить эффективность и мотивацию обучения. А ведь в настоящее время учителя сталкиваются с проблемой снижения уровня познавательной активности учащихся на уроке, нежеланием работать самостоятельно, да и просто учиться [Владимирова Л. П].

Благодаря использованию мультимедийных технологий в обучении:

1. Увеличивается активность учащихся на уроке.
2. Появляется возможность оперативного тестирования учащихся.
3. Экономится время и предоставляется возможность решения большего числа задач.
4. При проведении урока с использованием мультимедийных технологий соблюдается основной принцип дидактики – наглядность, что обеспечивает оптимальное усвоение материала школьниками, повышает эмоциональное восприятие, развивает пространственное воображение и все виды мышления у подростков.

С другой стороны, стремительное развитие компьютерных технологий качественно меняет окружающую жизнь и порождает множество новых проблем, в частности, проблему формирования информационной культуры и безопасности среди подрастающего поколения.

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. Компьютер и Интернет, как всякие сложные технологические продукты, наряду с неоспоримыми преимуществами могут нанести серьезный вред ребенку. Одним из главных вопросов, связанных с компьютеризацией, является изучение влияния компьютера на организм, психическое состояние и развитие ребенка [Полат Е.С].

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». 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 то же 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 [Полат Е.С.]. 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;
- разработка методического пособия «Интернет – ресурсы для образовательного процесса»;
- установка программ-фильтров на школьные компьютеры;
- проведение лектория для родителей учащихся по режиму доступа детей к образовательным ресурсам;
- памятка родителям «Десять фактов, которые нужно сообщить подросткам ради безопасности в Интернет».

Существует множество программ, позволяющих ограничить время работы за компьютером, отфильтровать содержимое Интернета, обезопасить маленького пользователя. Они называются программами Родительского контроля. Родительский контроль встроен в Windows Vista. Это дает возможность контролировать использование компьютера ребенка в четырех направлениях:

- a. ограничивать время, которое он проводит за экраном монитора,
- b. блокировать доступ к некоторым сайтам,
- c. блокировать доступ к другим интернет-сервисам,
- d. 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 [Полат Е.С.]. 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» [Полат Е.С.].

В школе может быть создан Общественный Совет по вопросам регламентации доступа к информации в Интернете, в состав которого входят представители администрации школы, учителя, учащиеся, родители. Основная функция Совета – контроль использования учащимися ресурсов сети Интернет.

Также должен быть разработан пакет документов, регламентирующий работу Совета: 1. Положение об Общественном совете школы по вопросам регламентации доступа к информации в Интернете. Инструкция для сотрудников средней общеобразовательной школы и членов Общественного Совета школы о порядке действий при осуществлении контроля за использованием учащимися сети Интернет [Полат Е.С.].

В помощь классным руководителям для проведения классных часов и родительского лектория могут быть разработаны: Памятка учащимся «О чем надо знать при работе в Интернет. Памятка родителям по управлению безопасностью детей в Интернет. В помощь учителям-предметникам могут быть разработаны методические рекомендации:

1. Памятка по оформлению методических материалов для размещения на сайте.
2. Памятка по составлению мультимедийной презентации [Полат Е.С.]. 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

4.3 Критерии оценки состояния информационной безопасности детей и подростков (рекомендации для родителей, педагогов)

Информационная среда основывается на предметности культуры общества и выступает как фактор развития ребенка, образующий динамическую систему взаимодействий участников информационного пространства. Параметрами информационной среды выступают ценностно-целевые установки, определяющие вектор воздействия, насыщенность (ресурсный потенциал), структурированность (способ и средства организации функционирования), виды и формы коммуникации в медиапространстве, эффекты воздействия, в том числе развивающие эффекты. Системообразующим основанием выделения и операционализации критериев стало требование создания оптимальных психологических условий личностного и умственного развития ребенка.

Признаком нарушения информационной безопасности стало содержание или форма коммуникативного акта, инициированного или проектируемого образовательными ресурсами, выступающие как факторы риска нарушения психического развития детей.

Основные направления воздействия информационной продукции на здоровье и развитие ребенка, релевантные критериям информационной безопасности:

- мировосприятие, базовое доверие к миру, система представлений о мире, природе, обществе и личности. Основы базового доверия формируются в раннем возрасте и определяются постоянством, устойчивостью, прогнозируемостью поведения матери и ее эмоциональным принятием ребенка (Э.Эриксон, К.Хорни, А.Адлер, Д.Винникотт, М.И.Лисина, Д.Боулби, Д.Б.Эльконин). Доверие человека к миру как базовая установка личности формируется на ранних этапах онтогенеза, выступая как база открытости к взаимодействию с миром и его исследованию, доверия к себе, развития идентичности личности.

Необходимым условием возникновения доверия является удовлетворение базовой потребности ребенка в безопасности. Доверие – свойство человека наделять явления и объекты окружающего мира и других людей, их возможные будущие действия и свои собственные предполагаемые действия характеристиками доброжелательности, безопасности, надежности, стабильности. Мировосприятие, развиваясь на протяжении всей жизни человека определяет картину мира как угрожающего, враждебного, непредсказуемого, либо как безопасного, справедливого, в котором торжествуют силы добра и справедливости;

- ценностно-смысловая система – формирование ценностных ориентаций, усвоение моральных норм, ценностей, этических представлений, соответствующим нравственным гуманистическим идеалам;

- коммуникативная компетентность, включая сформированность мотивов общения, овладение средствами и способами эффективного общения и умения конструктивно разрешать конфликты; позитивный образ и ожидания в отношении общения и взаимодействия с родителями, учителями, сверстниками, друзьями как партнерами равноправного общения; оптимизацию родительско-детских отношений, формирование установок уважения, доверия, толерантности, равноправия в семейных отношениях; позитивный опыт дружеских отношений.

- познавательное развитие, включая предоставление содержательной, достоверной, научно-обоснованной информации, адекватной возрасту ребенка и создающей зону ближайшего развития; использование интерактивных методов, позволяющих ребенку реализовать познавательную активность и способствующих развитию познавательной мотивации и широких интересов;

- поведение – усвоение просоциальных моделей поведения и исключение или минимизацию моделей и образцов девиантного и делинквентного (противоправного) поведения, включая агрессивное поведение и насилие в любых его формах;

- личностное развитие – развитие Я-концепции и позитивной самооценки, самопринятия и самоуважения ребенка, активности, самостоятельности, воли на основе презентации адекватных задач развития образцов для социальной, личностной, гражданской, этнической, гендерной и половой идентификации и обеспечения условий сохранения личностной целостности и интеграции;
- эмоциональное развитие как стабилизация эмоционального статуса, формирование эмпатии, высших чувств, фрустрационной устойчивости, предупреждение страхов, тревожности, депрессии, дисфории, эйфории, лабильности;
- формирование толерантности установок толерантного сознания и поведения личности, исключая этноцентризм и культуроцентризм, ксенофобию, мигрантофобию, шовинизм.

Выделение критериев оценки состояния информационной безопасности детей и подростков учитывает:

1. Ресурсный потенциал информации;
2. Содержание и форму информационного контента возрастной особенности аудитории;
3. Наличие условий для личностного и умственного развития детей и подростков;
4. Наличие условий для сохранения психического и психологического здоровья и благополучия детей и подростков;
5. Морально-нравственное содержание информационной продукции; художественно-эстетические качества информационной продукции.

Критерии для оценки состояния информационной безопасности и негативного воздействия на личностное, когнитивное развитие детей и подростков, их эмоциональное состояние и психологическое благополучие:

1. Соответствие информационной нагрузки возрастным и индивидуальным особенностям детей и подростков.
2. Развитие мировосприятия детей и подростков и их психологического благополучия, формирования у детей и подростков позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке.
3. Ценностное, моральное, нравственно-этическое развитие детей и подростков.
4. Усвоение системы семейных ценностей и представлений о семье.
5. Развитие системы социальных и межличностных отношений и общения детей и подростков.
6. Удовлетворение и развитие познавательных потребностей и интересов ребенка, детской любознательности, исследовательской активности.
7. Когнитивное развитие детей и подростков.
8. Развитие творческих способностей детей и подростков.
9. Формирование толерантности личности, установок толерантного сознания и поведения.
10. Развитие личности, Я-концепции, социальной (гражданской, этнической, гендерной) и личностной идентичности детей и подростков.
11. Эмоционально-личностное развитие и эмоциональное состояние.
12. Риски десоциализации, развития и закрепления девиантного и противоправного поведения, включая такие формы поведения как: агрессивное поведение и применение насилия, жестокости по отношению к людям и животным; совершение действий, представляющих угрозу жизни и (или) здоровью ребенка, в том числе причинение вреда своему здоровью, суицид; употребление наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий, алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на их основе; участие в азартных играх; занятие проституцией; бродяжничество; попрошайничество; нетрадиционные и девиантные сексуальные отношения; противоправное поведение и (или) преступления.

4.4. Урочная и внеурочная деятельность по обеспечению информационной безопасности подростков

Урок «Интернет-безопасность» (5-11 классы)

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

- 1) информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;
- 2) информирование обучающихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);
- 3) ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;
- 4) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);
- 5) предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

В ходе уроков Интернет-безопасности обучающиеся должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно-телекоммуникационных сетях, а именно: критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации; отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной; избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации; распознавать признаки злоупотребления их неопытностью и

доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность; распознавать манипулятивные техники, используемые при подаче рекламной и иной информации; критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях; анализировать степень достоверности информации и подлинность ее источников; применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

В рамках урока «Интернет-безопасность» в 5-6 классах целесообразно ознакомить обучающихся: – с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи; – как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет; – как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Рекомендуется продемонстрировать возможности детских поисковых систем <http://kids.quintura.ru>, <http://agakids.ru>, детского браузера <http://www.gogul.tv>, а также познакомить с детскими социальными сетями: <http://cyberpapa.ru/>, http://kinderonline.ru/detskiy_portal.ml, <http://1dnevnik.ru/>, <http://www.detkino.ru>.

Для отбора содержания урока могут быть использованы материалы сайта www.detonline.com (видеоматериалы, материалы электронного журнала «Дети в информационном обществе», материалы Линии помощи), а также материалы других сайтов, содержащих информацию по безопасному использованию сети Интернет. Большое значение для эффективности урока Интернет-безопасности имеет не только содержание, но и форма его проведения. Целесообразно использовать для 5-6 классов – урок-путешествие, урок-викторину, урок-соревнование, урок-игру, беседу.

Полезные ссылки:

- 1) <http://www.microsoft.com/> – о правилах безопасного поведения в сети Интернет с элементами интерактива;
- 2) <http://www.nachalka.com/> - учебное видео «Как обнаружить ложь и остаться правдивым в Интернете»;
- 3) <http://content-filtering.ru/> - информационно-аналитический ресурс «Ваш личный Интернет». В ходе урока «Интернет-безопасность» в среднем звене целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве: ФЗ РФ № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищённости, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.); № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в подростке порочные наклонности, сформировать у подростка искажённую картину мира и неправильные жизненные установки.)

Ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможны следующие формы проведения урока: урок-пресс-конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными администраторами.

Полезные ссылки:

- 1) <http://www.microsoft.com/> - молодёжная история с элементами интерактива;
- 2) <http://content-filtering.ru/> – информационно-аналитический ресурс «Ваш личный Интернет»;
- 3) www.icensor.ru

Интернет-фильтр. В рамках урока «Интернет-безопасность» в старших классах целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности подростков, которые отражены в российском законодательстве (см. рекомендации для проведения **урока-беседы ««Каким источникам информации следует доверять» (Приложение 4)** Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов: – информация, причиняющая вред здоровью и (или) развитию детей; – информация, запрещенная для распространения среди детей; – информация, ограниченная для распространения среди детей определенных возрастных категорий. На уроке необходимо затронуть следующие аспекты: перечень рисков, подстерегающих ребенка в сети Интернет; рекомендации по грамотному использованию электронной почты; технологии безопасного общения в средах мгновенного обмена сообщениями.

Необходимо обеспечить обучающихся инструкциями по безопасному общению в чатах; советами по профилактике и преодолению Интернет-зависимости; общими правилами по безопасности детей в сети Интернет. Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете: нежелательные программы; защита личных данных; мошенничество; виртуальные друзья; пиратство; on-line-игры; этика; критический подход к информации. Обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации. Ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм «Интернет-безопасность», дискуссия, дебаты, встреча со специалистами медиасферы, системными администраторами и т.д.

Полезные ссылки:

- 1) <http://www.kaspersky.ru> – антивирус «Лаборатория Касперского»;
- 2) <http://www.onlandia.org>. – безопасная web-зона;
- 3) <http://www.interneshka.net> – международный онлайн-конкурс по безопасному использованию Интернета;
- 4) <http://www.saferinternet.ru> – портал Российского Оргкомитета по безопасному использованию Интернета;
- 5) <http://content-filtering.ru/> – Интернет СМИ «Ваш личный Интернет»;

6) <http://www.rgdb.ru> – Российская государственная детская библиотека.

По итогам проведения уроков возможно провести итоговое анкетирование по теме «Информационная безопасность» (Приложение 1).

1. Анкетирование обучающихся

Для изучения проблемы информационной безопасности в сети Интернет и отношения к ней подростков разрабатываются анкеты, позволяющие проанализировать современную ситуацию в образовательной среде. Анкетирование предполагается проводить в форме анонимного опроса как на бумажных носителях, так и в электронном виде.

Примерные формы анкет представлены в Приложении 1 и Приложении 2. Предлагаем провести тест-опросник для родителей на выявление ранних признаков компьютерной зависимости у несовершеннолетних. И тест для обучающихся на выявление знаний об информационных угрозах.

2. Проведение урока-диспута «Интернету: да или нет?»

Цель: формирование устойчивых жизненных навыков при работе в сети Интернет. Диспуту предшествует предварительная подготовка обучающихся по предложенной тематике.

Перечень вопросов для обсуждения выявляется в результате анкетирования обучающихся. Примерные вопросы для обсуждения:

1. Для чего нужен Интернет?
2. Какие существуют риски при использовании Интернетом, и как их можно снизить?
3. Какие виды мошенничества существуют в сети Интернет?
4. Как защититься от мошенничества в сети Интернет?
5. Что такое безопасный чат?
6. Виртуальный собеседник предлагает встретиться, как следует поступить?
7. Как вы можете обезопасить себя при использовании услугами мгновенных сообщений?

4. Проведение компьютерной игры для младших подростков. В рамках классного часа или урока информатики (окружающего мира) обучающимся 5-6 классов целесообразно предложить компьютерную игру о правилах поведения в сети Интернет «Прогулка через ИнтернетЛес» <http://www.wildwebwoods.org/>, где в игровой форме показано какие опасности могут встречаться при работе в сети Интернет, рассказано о сетевом взаимодействии и об этикете, а также о защите прав детей.

5. Флэш-мобы по проблемам информационной безопасности *Флэшмоб* – это интернет-технология, которая позволяет любому множеству людей договориться друг с другом, чтобы синхронно осуществить какое-то определенное, заранее согласованное действие. *Флэшмоб* – это неожиданное для окружающих появление людей в заранее установленном месте и заданное время. При этом, как правило, участники совершают некоторые заранее определенные действия, которые кажутся непонятными и нелогичными для посторонних людей. Соответственно, сам по себе моб представляет собой кратковременную акцию (обычно около 5 минут), с заранее разработанным планом действий, яркую. Флэшмоб как заранее спланированная массовая акция, в которой большая группа людей появляется в общественном месте, выполняет заранее оговоренные действия (сценарий) и затем расходится.

Цель флешмоб-акции: привлечение внимания детей, их родителей и педагогов к проблемам информационной безопасности.

Правила флэшмоба

1. Флешмоб вне рекламы, вне политики (никто из участников не платит и не получает денег).
2. Действие должно казаться спонтанным (участники не собираются в месте события до акции).
3. Точное время начала и конца проведения (каждый участник должен точно выполнить указанное в сценарии временное условие, часы должны быть синхронизированы).
4. Точное следование сценарию (креативный подход только в оговоренных случаях).
5. Флешмоб не должен вызывать негативных эмоций, агрессивной реакции случайных зрителей.
6. Действия моберов не должны пересекаться с чертой дозволенного законодательством. После акции не должно оставаться мусора.
7. После акции нужно мгновенно разойтись с места действия в разные стороны, не подавая виду, что произошло что-то необычное.

Примеры флэшмоба:

- замирание, группа людей вдруг неожиданно замирает посреди людного места на 1-2 минуты. Потом дальше продолжают идти как ни в чем не бывало;
- танец, например, в крупном гипермаркете группа людей начинает танцевать, потом присоединяются остальные участники акции;
- еще один сценарий — собирается народ и вдруг все достают бинокли, подзорные трубы, свернутые газеты, или просто внимательно смотрят в течение 5 минут на здание института (к примеру). Потом все расходятся, а прохожие в недоумении начинают разглядывать что там на здании. Сценарий флэшмоба можно придумать самый разный, главное неожиданность, удивить собравшихся темой.

Виды флэшмобов

Классический флешмоб.

Главная цель – удивить случайных зрителей. Полит-моб или социо-моб. Это акции с социальным или политическим оттенком. Они являются более простым, оперативным и 36 безопасным способом выражения общественного мнения или привлечения внимания к тем или иным проблемам. Неспектакльный моб (Реальный флешмоб) – это акции, в которых

участники пытаются смоделировать тонкое, порой едва уловимое социокоммуникативное пространство, в котором на первом месте стоит переживание самих участников. Он может быть незаметен для окружающих. Нет задачи произвести впечатление на внешнего зрителя. Действия участников настолько приближены к повседневности, что их образ начинает «мерцать». Становится непонятным видны ли действия, выполняемые по сценарию, или это всего лишь действия обычного прохожего, случайно повторившего, что написано в сценарии.

Варианты для примера:

- споткнуться;
- вспоминать, есть моб. телефон в кармане или нет, затем доставать его и класть обратно;
- внимательно читать учебник/газету около входа в кабинет и что-то в голове считать, слегка шевеля губами и закидывая глаза;
- тщетно пытаться завязать шнурки;
- пытаться застегнуть или расстегнуть заевшую молнию на курточке, сумке;
- отряхивать испачканную одежду;
- переписывать информацию с какой-нибудь рекламы;
- играть на ходу в игры на мобильном.

Алгоритм подготовки флэшмоба

1. Сформулировать цель флэшмоба.
2. Определитесь с тем, что вы будете делать во время флэшмоба. Успех проведения флэшмоба зависит от оригинальности, живости и притягательной силы мероприятия. Избегайте устраивать флэшмоб по образцу мероприятия, которое уже было где-то проведено.
3. Посмотрите предыдущие флэшмобные мероприятия на YouTube (прекрасный источник идей).
4. Организуйте свой флэшмоб. Вам потребуются добровольцы, желающие участвовать во флэшмобе, (Вы также можете привлечь ресурсы класса, в котором вы учитесь, театральную или танцевальную группу, в которую вы входите или другие группы людей, с которыми вы проводите время. Спросите своих друзей или членов семьи, не хотят ли они также принять в этом участие).
5. Обеспечьте свою группу четкими инструкциями. Для успешного проведения вашего флэшмоба потребуется, чтобы участвующие точно знали, что нужно делать. Лучше всего провести репетицию заранее, но если это невозможно, то, по крайней мере, снабдить участников очень четкими инструкциями (онлайн или по электронной почте и т.д.) относительно того, что надеть, когда и где нужно быть, что делать.
6. Подготовьте нужный реквизит и костюмы. Лучше попросить участников принести свой реквизит или организовать самим (такие, как, газеты, мобильные телефоны, планшеты и др.)
7. Ознакомьтесь с ограничениями, действующими на данной местности. Проведите тщательное исследование территории, на которой вы собираетесь провести флэшмоб. На данной местности могут пролегать границы безопасности, правовые или физические ограничения. Чтобы избежать проблем с законом, важно не создавать опасные заграждения, не нарушать технику безопасности.
8. Закончите, сделав вид, что ничего не произошло. Сразу после окончания флэшмоба, не позволяйте участникам расслаиваться и говорить или начинать разговоры с толпой. Они должны смешаться с толпой и уйти до заката солнца так, как будто ничего не произошло.

Источники информации: wikipedia.ru- материал о флэшмобе из Википедии – свободной энциклопедии. Probuem.ru – что такое флэшмоб? Flashmob.tamboff.ru – что такое flashmob?. Yasa.yandex.ru – каталог сайтов о флэшмобе.

6. Проведение родительского собрания. Родительские собрания целесообразно проводить по уровням общего образования – для младших и старших подростков (основное общее образование, среднее общее образование) (Приложение 10).

В начале родительского собрания рекомендуется провести анонимное анкетирование, которое позволит выявить отношение родительской общественности к внедрению в образовательный процесс ИКТ. По результатам анкетирования будет определена дальнейшая стратегия работы ОУ по безопасности детей в сети Интернет. После анкетирования проводится беседа по проблеме доступа ребенка к сети Интернет, в которой поднимаются наиболее актуальные вопросы (Приложения 4, 6) Далее даются рекомендации родителям по работе детей в сети Интернет (с учетом возрастных особенностей) В конце родительского собрания всем родителям предлагается памятка по безопасности детей в сети Интернет при помощи программных средств (Приложение 10).

7. Глобальная сеть: правила пользования.

Линия помощи «Дети-подростки онлайн» представляет рекомендации для родителей. Как защитить ребенка от столкновения с вредоносной информацией в сети? Как научить его справляться с последствиями таких встреч?

Знакомства в Интернете

При общении в сети существует угроза подвергнуться рискам, связанным с контактами с другими людьми, не всегда знакомыми в реальной жизни. Особенно опасен груминг – установление дружеских отношений с подростком целью вступления в сексуальные отношения. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника подростка. Общаясь лично («в привате»), преступник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

1. Будьте в курсе, с кем взаимодействует в Интернете Ваш ребенок. Старайтесь регулярно проверять список его контактов, чтобы убедиться, что он лично знает всех, с кем общается.
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.

3. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), нельзя использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.

4. Если ребенок интересуется контактами с людьми намного старше его, следует обратить на это внимание и провести с ним разъяснительную беседу.

5. Не позволяйте ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствие взрослого человека. Если ребенок желает встретиться с новым Интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

6. Интересуйтесь тем, куда и с кем ходит Ваш ребенок.

Кибербуллинг

Кибербуллинг – преднамеренное и протяженное во времени агрессивное поведение по отношению к жертве, осуществляемое одним человеком или группой людей посредством различных электронных сервисов.

Предупреждение 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. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

3. Научите детей правильно реагировать на обидные слова или действия других пользователей.

4. Объясните детям, что информация, которую они выкладывают в Интернете, может быть использована против них.

5. Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования сетью.

Кибермошенничество

Кибермошенничество – один из видов киберпреступлений, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный или иной ущерб.

Предупреждение кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться с взрослыми перед тем, как воспользоваться теми или иными услугами сети.

2. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.

Интернет-магазины:

– 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 выдачей кассового чека;

– сравните цены в разных Интернет-магазинах;

– позвоните в справочную магазина;

– обратите внимание на правила Интернет-магазина;

– выясните, сколько точно вам придется заплатить.

Противозаконный и неэтичный контент

Контентные риски – это материалы (тексты, картинки, аудио, видеофайлы, ссылки сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду наркотиков и действий, причиняющих вред физическому и психическому здоровью. Столкнуться с рисками такого рода можно практически везде: сайты, социальные сети, блоги, торренты, видеохостинги. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Предупреждение столкновения с неэтичным или противозаконным контентом:

1. Установите на компьютер специальные программные фильтры (при нажатии на вылетающий баннер вместо страницы будет всплывать пустое окно) или специальные программы, называемые системами родительского контроля (они позволяют родителям решать, какое содержимое могут просматривать их дети).

2. Приучите ребенка советоваться с взрослыми и немедленно сообщать о появлении подобного рода нежелательной информации.

3. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда.

4. Научите их спрашивать о том, в чем они не уверены.

5. Старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

Вредоносные программы

Вредоносные программы – различное программное обеспечение (вирусы, черви, «тройные кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Они также способны снижать скорость обмена данными с Интернетом и даже 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. Предупреждение столкновения с вредоносными программами:

1. Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Подобные программы наблюдают за трафиком и могут предотвратить 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 игр.

3. Периодически старайтесь полностью проверять свои домашние компьютеры.

4. Делайте резервную копию важных данных.

5. Старайтесь периодически менять пароли (например, от электронной почты), но не используйте слишком простые пароли. Если ребенок все же столкнулся с какой-либо угрозой в сети, и она оказала на него негативное влияние. 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 наказывать. Постарайтесь внимательно выслушать рассказ о том, что произошло, понять, насколько серьезно произошедшее и в какой степени это могло повлиять на ребенка. 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.

Если ситуация связана с насилием в Интернете в отношении ребенка, то необходимо узнать информацию об агрессоре, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. П.). Жестко настаивайте на том, чтобы ребенок избегал встреч с незнакомцами, особенно без свидетелей. Проверьте все новые контакты ребенка за последнее время. Соберите наиболее полную информацию о происшествии как со слов ребенка, так и помощью технических средств – зайдите на страницы сайта, где был ребенок.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646). URL: https://www.mid.ru/ru/foreign_policy/official_documents/1539546/
2. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию, введено понятие информационной безопасности детей, рассмотрены виды информации, причиняющей вред здоровью и (или) развитию детей» // Российская газета № 297, 31.12.2010. – URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=489460>
3. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности РФ» // URL: <http://pravo.gov.ru>
4. Безмальный, В. Ф. Обеспечение безопасности детей при работе в Интернет. – [Электронный ресурс] – URL: <http://www.ifap.m/librarv/book331.pdf>
5. Владимирова, Л. П. Сетевые профессиональные сообщества учителей / Л. П. Владимирова. – URL: <http://distant.ioso.ru/for%20teacher/25-11-04/sps.htm..>
6. Власенко, М. С. Обеспечение информационной безопасности несовершеннолетних в сети интернет: современное состояние и совершенствование правового регулирования / М.С. Власенко // Вестник Волжского университета. – 2019. - №3. – С. 99-101.
7. Войскунский, А. Е. Психология и Интернет / А. Е. Войскунский. – М. : Акрополь, 2010. – 439 с.
8. Гордин, А.И. Информационная социализация детей и подростков: учеб. Метод. Пособие / А.И. Гордин, О.В. Гордина // Иркутск: Изд-во «Иркут». 2019. – 118 с.
9. Гордин А.И., Гордина О.В. Практикум формирования безопасного информационного поведения: рабочая тетрадь / Сост. А. И. Гордин, О. В. Гордина. – Иркутск: Изд-во «Репроцентр +», 2023. – 131 с.
10. Ельчанинова, Н. Б. Проблемы обеспечения информационной безопасности несовершеннолетних: правовые аспекты / Н. Б. Ельчанинова // Южный федеральный университет. – 2017. - № 5. – С. 167-169.
11. Есенкожа, Е. М., Касен, Г. А. Психолого-педагогическая профилактика интернет-аддикций на основе формирования медиаграмотности учащихся подростковых классов» / Е. М. Есенкожа, Г. А. Касен // Развитие технологий здоровьесбережения в современном обществе // Материалы международной научно-практической конференции/ ответственный редактор: Л.К. Тропина. – Екатеринбург: Издательство: Уральский федеральный университет, 2015. – С. 323-352.
12. Завалишина О.В. Моделирование процесса педагогической поддержки подростков, склонных к проявлению интернет-зависимости / О.В. // Научный журнал КубГАУ. – 2011. - №70(06). – URL : <http://ej.kubagro.ru/2011/06/pdf/11.pdf>
13. Калинина, Н. В. Профилактика рисков интернет-активности обучающихся: субъект-порождающее взаимодействие / Н. В. Калинина // Образование личности. – 2017 - № 1. – с. 12-17.
14. Информационная безопасность детей и подростков в современном мире: психологические аспекты проблемы // Психология и право – 2017. – Том 7. -№1.
15. Коптелова, Н. И., Попов, В. А. Социально-педагогическая профилактика компьютерной зависимости у подростков в общеобразовательных учреждениях / Н. И. Каптелова, В. А. Попов // Молодой ученый. – 2015. - №24. – С. 970-973.
16. Корнейков, Е. Н. Психолого-педагогическая безопасность молодежи в информационной цифровой среде: сущность понятия / Е. Н. Корнейков // Векторы психологии: психолого-педагогическая безопасность личности в современной образовательной среде [Электронный ресурс] : III Междунар. Заочная науч.-практ. Конф. (Гомель, 1 июля 2021 года) : сборник материалов / Гомельский гос. Ун-т им. Ф. Скорины ; редкол.: Т. Г. Шатюк (гл. ред.) [и др.]. – Электрон. Текст. Дан. (объем 8,17 Mb). – Гомель : ГГУ им. Ф. Скорины, 2021. – С. 51-54. – URL: https://conference.gsu.by/sites/default/files/202112/Сборник_Векторы%20психологии_2021.pdf.
17. Марцинковская, Т.Д. Информационная социализация в изменяющемся информационном пространстве [Электронный ресурс] // Психологические исследования. – 2012. – Т. 5. - № 26. – С. 7. – URL: <http://psystudy.ru>
18. Менделевич, В. Д., Садыкова, Р. Г. Зависимость как психологический и психопатологический феномен (проблемы диагностики и дифференциации) / В. Д. Менделевич, Р. Г. Садыкова // Вестник клинической психологии. – 2003. – №2. – Т.1. – С.153–158.
19. Мышко, Ф. Г., Каменева, Т. Н. Риски коммуникации подростков в интернет-пространстве / Ф. Г. Мышко, Т. Н. Каменева // Мир науки. Социология, филология, культурология. – 2022. – Т. 13. - № 4 // URL : <https://sfk-mn.ru/PDF/37SCSK422.pdf>
20. Нынук, Р. Н. Информационная безопасность детей в Российской Федерации: проблемы реализации / Р. Н. Нынук // Криминалистика: вчера, сегодня, завтра. – 2023. - № 2 (26) – С. 110–118.
21. Полат, Е. С. Проблема информационной безопасности в образовательных сетях рунет / Е. С. Полат // URL: <http://www.ioso.ru/distant/library/publication/infobez.htm/http://www.humanities.edu.ru/db/msg/84168.>
22. Пустовойтов, В. Н., Корнейков, Е. Н. Методологические принципы подготовки педагогов к воспитательной деятельности в условиях цифровизации образовательного пространства / В. Н. Пустовойтов, Е. Н. Корнейков // Современные наукоемкие технологии. – 2021. - № 3. – С. 177-181. – URL: <https://top-technologies.ru/ru/article/view?id=38552>
23. Савельев, А. И. Проблема информационной безопасности несовершеннолетних в сети Интернет / А. И. Савельев // Юридическая наука и правоохранительная практика. – 2016. - № 2 (36). – С. 59–66.
24. Скобина, Е. А. Проблемы защиты детей в интернет-пространстве / Е. А. Скобина // Издательство Молодой ученый. – Чита, 2018. – 62 с.
25. Словарь финансовых терминов. Цифровой актив: основные понятия и термины [Электронный ресурс] – URL: <https://www.finam.ru/publications/section/dictionary/>.
26. Солдатова, А. В. Проблемы обеспечения информационной безопасности детей в сети «Интернет»/ А. В. Солдатова // Уральский Федеральный университет. – 2018. – С. 775-786.
27. Титор, С. Е. Информационная безопасность несовершеннолетних: опыт организации отдельных субъектов Российской Федерации / С. Е. Титор // Цифровая социология. – 2022. – Т. 5. – № 4. – С. 98–105.

28. Тихонова, А.Д. Проблема вовлечения в террористическую деятельность посредством использования социальных сетей. Доклад на конференции «Коченовские Чтения», 10–12 ноября 2016 г.
29. Турбина, Р. В. Педагогические подходы к обеспечению информационной безопасности детей-подростков в сети Интернет / Р.В.Турбина. – Текст : непосредственный // Молодой ученый. – 2022. - №10 (405). – С. 106-108. – URL: <https://moluch.ru/archive/405/89378/>
30. Энциклопедия информационной безопасности. [Электронный ресурс] -: URL : <http://www.securelist.com/ru/encvclped>
31. Davis, S. A. A cognitive-behavioral model of pathological Internet use / S. A. Davis // Computers in Human Behavior. – 2020. – Vol. 17, № 2. – P. 187–195.
32. Livingstone, S., Haddon, L. Risky experience for children online: charting European research on children and the Internet // Children and society. 2018. Vol. 22. P. 314–323.
33. NetSchool Сетевой город. Образование. О продукте, 2001. – URL: <http://www.net-school.ru>

Полезные материалы для подготовки уроков и мероприятий, посвященных Интернет-безопасности школьников

1. URL: https://xn-b1aew.xn-p1ai/Internet_for_kids Официальный портал МВД России «Безопасный Интернет – детям».
2. URL: <https://www.saferunet.ru/> Центр безопасного Интернета в России.
3. URL: <http://i-deti.org/> Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт.
4. URL: <http://www.fid.su/> Фонд развития Интернет.
5. URL: <http://www.ifap.ru/library/book099.pdf>– «Безопасность детей в Интернете», компания Microsoft.
6. URL: <http://www.oszone.net/6213/> - «Обеспечение безопасности детей при работе в Интернет».
7. URL: <https://www.google.ru/safetycenter/families/start/basics/> Центр безопасности Google.
8. URL: <http://shperk.ru/sovety/avtoritet.html> – Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном.
9. URL: <http://habrahabr.ru/company/mailru/blog/252091/> «Безопасность в интернете: готовы ли пользователи противостоять киберугрозам?».
10. URL: <https://pandia.ru/text/78/639/36613.php> Урок безопасности «Правила общения в Интернете!» (для подростков 12-15 лет).
11. URL: <https://proshkolu.ru/user/litvinatm59/blog/144290/> Тренинг «Безопасность в сети Интернет».
12. URL: <https://www.novayagazeta.ru/articles/2016/05/16/68604-gruppy-smerti-18>
13. URL: <http://www.all-psy.com/stati/detail/5185/1/>

Электронные ресурсы

1. Безмалый, В. Ф. Обеспечение безопасности детей при работе в Интернет. – [Электронный ресурс] – URL:[http://www.ifap.m/librarv/book331 .pdf](http://www.ifap.m/librarv/book331.pdf)
2. Безопасность детей в Интернете – URL : <http://www.microsoft.com/rus/childsafetv>
3. Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт. – [Электронный ресурс]. – URL :<http://i-deti.org/>
4. Борьба с вредоносными программами – URL : <http://support.kaspersky.ru/vimses>
5. Горбачева, Е. В. Административно-правовое обеспечение информационной безопасности несовершеннолетних. [Электронный ресурс] – URL: <http://www.dissercat.com/content/administrativno-pravovoe-obespechenie-informatsionnoi-bezopasnosti-nesoversheninikh#ixzz2TZYiXTYN>
6. Грег Шипли. Основы безопасности ИТ. [Электронный ресурс] – URL : [http://www.ccc.ru/magazine/depot/03_04/read. Html70501.htm](http://www.ccc.ru/magazine/depot/03_04/read.Html70501.htm)
7. Дети и интернет, какие опасности скрывает всемирная паутина. / Методическое пособие для родителей. – URL: <http://www.pandia.ru/text/77/115/462.php>
8. Детская безопасность в Интернете. [Электронный ресурс]. – URL: <http://www.debotaniki.ru/2012/09/detskava-bezopasnost-v-intemetu/>
9. Дети в Интернете: кто предупрежден, тот вооружен. – URL: <http://do.znate.ru/docs/index-26385.html>
10. Десять фактов, которые нужно сообщить детям ради безопасности в Интернете/ - URL : <http://do.znate.ru/docs/index-32759.html>
11. Ежеквартальный журнал для педагогов, психологов и родителей «Дети в информационном обществе» издаётся Фондом Развития Интернет с 2009 года. Научная поддержка: факультет психологии МГУ имени М.В. Ломоносова и Федеральный институт развития образования МОИРО. Информационная поддержка: Министерство образования и науки Российской Федерации. Выпуски №1 – 11- URL: <http://deti-online.com/journal/numbers/11>
12. 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 : <http://www.fid.su/projects/journal/>
13. Интерактивный курс «Основы безопасности детей и молодежи в интернете». [Электронный ресурс]. – URL: <http://www.microsoft.com/eeesti/haridus/veebivend/koomiksid/ms/html/etusivu.htm>
14. Интернет-угрозы: троллинг и кибербуллинг. – [Электронный ресурс]. – URL: <http://intemetua.com/internet-ugrozi-trolling-i-kiberbulling>
15. Интернет-угрозы и эффективное противодействие им в отношении пользователей. – URL : <http://www.saferunet.ru/>
16. Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным. – URL : <http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html>

17. Мельников В.И. Информационная безопасность и защита информации. [Электронный ресурс]. – URL : http://www.books.demetri.ws/inf_books_25
18. OS.zone.net – Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль» - URL : <http://www.oszone.net/6213/>
19. 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/>
20. Родителям о безопасном Интернете. – URL : <http://74322s004.edusite.ru/p67aal.html>
21. 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.rgdb.by/innocuous-internet>
22. Тест на выявление Интернет-зависимости. – URL : <http://www.psvhelp.ru/internet/test.php>
24. Энциклопедия информационной безопасности. [Электронный ресурс]/ – URL : <http://www.securelist.com/ru/encyclopedia>

Анкета для выявления оценки осведомленности учащихся разных возрастов о понятии «Информационная безопасность»:

1. Как вы понимаете, что такое информация?
2. Какие источники информации вам известны?
3. Зачем нужна информация?
4. Нужно ли иметь много информации?
5. Какая информация считается опасной?
6. Какая информация считается необходимой?
7. Откуда ребенок получает информацию?
8. Кому из источников информации вы больше доверяете?
9. Какой из источников информации можно считать наиболее надежным?
10. Какая информация является избыточной?
11. Зачем использовать избыточную информацию?
12. Сколько времени вы проводите в Интернете?
13. Какую информацию нельзя разглашать в Интернете?
14. В каких целях вы используете Интернет?
15. Знаете ли вы чем опасны социальные сети?
16. Какие источники информации являются для вас наиболее значимыми?
17. При использовании информационных ресурсов заботитесь ли вы о необходимости оценки достоверности информации?
18. Как часто вы обращаетесь к Интернету в поиске информации?
19. С каких устройств вы чаще выходите в Интернет?
20. Какие сайты в Интернете вы считаете наиболее надежными?

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ «БЕЗОПАСНОСТЬ ПОДРОСТКОВ В ИНТЕРНЕТЕ:

Информационно-коммуникативные технологии становятся новым инструментом в образовании и воспитании школьника, события Всемирной паутины все больше интересуют подростков. Но не стоит забывать, что Интернет таит в себе множество опасностей.

Вы знаете, что в ваше отсутствие ребенок смотрит в Интернете? Какие сайты посещает со своего телефона? Ведь Интернет состоит не только из «соцсетей», образовательных и развлекательных порталов, в нём есть множество сайтов, пропагандирующих порнографию, межнациональную и религиозную рознь, насилие, употребление наркотиков и алкоголя, да и мошенников в нем хоть пруд пруди. Всё это может травмировать психику ребенка, ударить по семейному бюджету и неизвестно чем обернуться в будущем. Большинство родителей осознают эту проблему, но немногие из них не знают, как правильно защитить своих детей от такого рода информации.

В нашем современном мире пользователи Сети становятся все моложе. Благодаря Интернету дети открывают для себя новый мир, получают огромное количество информации, знакомятся и общаются, занимаются творчеством. Но для успешного и безопасного путешествия по «всемирной паутине» необходимо знать как о ее возможностях, так и о ловушках, подстерегающих пользователя в Интернете.

Безопасность в Интернете детей от 13 до 17 лет

Подростки, как правило, проходят через период низкой самооценки; ищут поддержку у друзей и неохотно слушают родителей. Те, кто постарше – ищут свое место в мире и пытаются обрести собственную независимость. 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 в этом возрасте их дети используют Интернет. Подростки скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Большинство пользуются чатами, общаются 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.

Советы по безопасности

- В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми.
- Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет.
- Следует указать список запрещенных сайтов, часы нахождения в Сети и руководство по общению в Интернете (в том числе и в чатах).
- Держите компьютеры с подключением к Интернету в общих комнатах.
- Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются, так, как если бы речь шла о друзьях в реальной жизни. Спрашивайте о людях, с которыми подростки общаются, используя мгновенный обмен сообщениями, и убедитесь, что эти люди им знакомы.
- Знайте, какими чатами и досками объявлений пользуются дети и с кем они общаются. Поощряйте использование модерлируемых чатов и настаивайте, чтобы подростки не общались с кем-то в приватном режиме.
- Настаивайте, чтобы они никогда не соглашались на личные встречи с друзьями из Интернета без вашего сопровождения на первой встрече (или сопровождения другого взрослого, которому вы доверяете). Объясните, что, если виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к заботе подростка о собственной безопасности.

- Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Познакомьте их с информационно-развлекательный сайтом, для детей и подростков открытым Роскомнадзором <http://персональныеданные.дети/>.
- Научите детей не загружать программы, музыку или файлы без вашего разрешения. Объясните, что иначе подростки могут нарушить авторские права и тем самым закон.
- Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между полами, расскажите детям о порнографии в интернете и противоправности ее распространения, направьте их на хорошие сайты о здоровье, вреде ранних половых контактов, предупреждении подростковой беременности.
- Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- Возьмите за правило знакомиться с сайтами, которые посещают подростки. Убедитесь, что дети не посещают сайты с оскорбительным содержанием, не публикуют личную информацию или свои фотографии.
- Напоминайте детям об ответственном, достойном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете.
- Обсудите с подростками азартные сетевые игры и их возможный риск. Напомните, что для детей это незаконно.
- Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает.
- Сообщите о негативном контенте в компетентные органы

УРОК – ЛЕКЦИЯ «ЧТО ТАКОЕ ИНФОРМАЦИЯ И ЕЕ РОЛЬ В НАШЕЙ ЖИЗНИ»

Тема. Что такое информация и ее роль в нашей жизни.
Цель. Познакомить учащихся с понятием информации, ее ролью в нашей жизни, видами и методами ее получения.
Задачи:

- 1. Познакомить учащихся с общим понятием информации;
- 2. Рассказать о видах и методах получения информации;
- 3. Научить обобщать, систематизировать и расширять знания о полученной информации.

Тип урока: комбинированный.
Форма организации работы детей: заслушивание материала, запись в тетрадь.
Форма организации работы учителя: форма обучения для раскрытия нового материала – урок – лекция.
Техническое обеспечение: компьютер, мультимедийный проектор, интерактивная доска.

План урока

Организационный момент.
Приветствие. Проверка состава класса.
Актуализация знаний.
Изучение нового материала.

Весь мир пронизан большим потоком информации, поэтому познавая весь окружающий мир, человек и его сознание имеет дело с информацией. Она помогает правильно оценивать события, происходящие вокруг, принять обдуманное решение, сделать соответствующие и правильные выводы.

На интуитивном уровне мы понимаем, что информация – это тот багаж знаний, который мы пополняем в течении всей нашей жизни. Несмотря на это, информация является сильным средством воздействия на личность и общество в целом. Человек, который владеет наибольшим объемом знаний и информации на любой вопрос находится в более выигрышном положении по сравнению с остальными. Слово «информация» происходит от лат. «informatio», что означает «сведения». Существует большее количество определений на данный термин, но в обыденной жизни мы понимаем его, как знания, сведения, сообщение. Информация позволяет человеку повысить уровень осведомленности знаний, касающихся какого-либо объекта.

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Сама по себе в мире информация не существует. Всегда имеется источник, производящий информацию и объект, которым информация воспринимается.

В роли объекта получения информации могут выступать: человек, устройство, животное и т.д. То есть информация всегда предназначена для кого-то. А способы же получения информации могут быть различны, например, когда мы слушаем радио или смотрим телевидение, когда сидим за компьютером, ноутбуков, любым гаджетом, имеющим выход в Интернет, когда читаем газету, журнал или книгу, в результате беседы, дискуссии с любым человеком, когда дотрагиваемся до какого-либо предмета или пробуем на вкус незнакомую нам еду.

При этом одну и ту же информацию каждый человек будет воспринимать по-разному. Информация несет в себе все разнообразие окружающего мира, при этом порождает все ее различные виды.

Так, например, существует информация для определенного вида людей, специализирующихся в какой-либо научной области: математике, биологии, химии, физике. Такую информацию называют научной.

Так же, для любого человека важную роль имеют средства массовой информации: газеты, журналы, книги, радио, телевидение. Каждый из этого источника распространяет любой вид информации: научно-популярную, политическую. Именно с их помощью человек узнает о новых событиях, моментах и явлениях, происходящих вокруг нас.

Таким образом, говоря об информации необходимо учитывать то, что всем объемом знаний обладать человек не может, но пополнять этот объем необходимо постоянно.

Таблица 3 – Виды информации

Вид информации	Способ и форма	Пример
1	По способу восприятия	Зрительная Слуховая Тактильная Обонятельная Вкусовая
2	По форме представления	Звуковая Мультимедийная Числовая Графическая Текстовая
3	По общественной значимости	Личная Общественная Научная Обыденная Эстетическая
4	Положительная или отрицательная	Опасная Надежная Вредная

		Избыточная Полезная Бесполезная Доступная Недоступная Достоверная Недостоверная
--	--	---

Методы получения и использования информации можно разделить на 3 группы:
Эмпирические (наблюдение, эксперимент, сравнение, измерение, опрос, интервьюирование, тестирование и т.д.)
Теоретические (от абстрактного к конкретному, идеализация, формализация, идеализация, аксиоматизация)
Эмпирико-теоретические (абстрагирование, анализ, синтез, индукция, дедукция и т.д.)
Закрепление нового материала.
Задаются вопросы по усвоенному материалу.
Подведение итогов урока.
Сообщение домашнего задания.
Записи в тетрадях.

УРОК – БЕСЕДА «КАКИМ ИСТОЧНИКАМ ИНФОРМАЦИИ СЛЕДУЕТ ДОВЕРЯТЬ»

Тема. Каким источникам информации следует доверять.

Цель. Познакомить учащихся с различными источниками получения информации.

Задачи:

1. Научить формировать навыки отбора информации;
2. Научить отсеивать недостоверную и избыточную информацию.

Тип урока: *комбинированный.*

Форма организации работы детей: заслушивание материала, беседа с учителем, запись в тетрадь.

Форма организации работы учителя: форма обучения для раскрытия нового материала – урок-беседа.

План урока

Организационный момент.

Приветствие. Проверка состава класса.

Актуализация знаний.

Изучение нового материала

Время не стоит на месте и информационный прогресс, к счастью, тоже. Как мы знаем, в современном обществе существует большое количество источников для получения информации. С каждым годом этих источников становится все больше и пути их получения доводятся до совершенства.

А какие источники информации известны вам?

Как вы считаете, каким источникам из названных стоит доверять, а каким нет? Почему?

В пример мы возьмем два источника информации: Интернет и газеты.

Интернет, это то ресурс, без которого современное общество, а в частности молодое поколение, уже не видит смысла. Все гаджеты, смартфоны, компьютеры оснащены данной функцией для получения любой информации. Но тем не менее, вся ли информация, находящаяся в сети Интернет имеет положительное свойство и является достоверной? Как вы считаете?

Интернет для нас стал неким наркотиком, ведь большинство начинают свой день и заканчивают, сидя в социальных сетях. Мы не только получаем оттуда необходимую для нас полезную или опасную информацию, но также и оставляем данные о нас самих, что может плохо обернуться.

Посмотрите вокруг, когда вы просто идете по улице, каждый человек, идущий вам навстречу, определенно будет в руках с телефоном. Это как раз и называется зависимостью или по-другому потребностью в данном предмете. Все это проникает в наше сознание, и мы уже не обращаем внимание на красоту за пределами телефона.

Когда мы заходим в сеть Интернет за необходимой информацией, нужно ли эту информацию отбирать и как это делать?

Информацию необходимо отбирать, ссылаться на источники или проверенные сайты. Чаще используется данный источник получения информации, так как считается, что с помощью него можно проще найти весь необходимый поток знаний.

Что же касается печатных изданий, в данном случае это газета, она тоже является источником получения информации, но уже не имеющим статуса современного источника. Является менее используемым.

Но следует задаться вопросом, а все ли, что печатается в газетах является достоверной информацией? Как вы считаете?

То, что мы можем прочитать в газетах, исходит от нас самих, от таких же людей, их называют журналистами. Именно они получают необходимую информацию, после чего она обрабатывается, проходит еще несколько этапов, прежде чем печатается в газету. Но достоверной она быть не может. Не так услышана или понята, ее уже нельзя считать верной.

Поэтому из любого источника необходимо уметь правильно оценивать информацию, находить правильную и отсеивать ненужную.

Закрепление нового материала.

Задаются вопросы по усвоенному материалу.

Подведение итогов урока.

Сообщение домашнего задания.

Записи в тетрадях.

УРОК – ДИСПУТ «ИНТЕРНЕТУ: ДА ИЛИ НЕТ?»

Тема: «Интернету: да или нет?»
Цель: научить обучающихся видеть и находить положительные и отрицательные стороны сети Интернет.

- Задачи:**
- 1. Повторить и обобщить знания об информационных технологиях.
 - 2. Развивать познавательный интерес и творческую активность школьников.
 - 4. 3. Развивать у школьников умение излагать мысли.
 - 5. Воспитать уважение к сопернику, стойкость, волю к победе, находчивость, умение работать в команде.
 - 6. Развивать логическое мышление, память, внимательность.

Тип урока: комбинированный
Форма организации работы детей: Выступление обучающегося с докладом. Игра по командам.
Форма организации работы учителя: форма обучения для раскрытия нового материала – урок - диспут. Выступление учителя.

Подготовительный этап:
Для проведения урока необходимо: составить вопросы для рассмотрения обучающихся, лист ранжирования, канцелярские принадлежности, разделить класс на 2 команды, подготовить презентацию «История сети Интернет».
Заранее класс делится на 2 команды. Первая команда выступает за положительные стороны сети Интернет, вторая команда рассматривает отрицательные стороны Интернета. Выбираются капитаны из каждой команды. Придумывают название и девиз.

Ход урока

Организационный момент
Приветствие. Проверка состава класса.
Актуализация знаний
Изучение нового материала. Игра.
Выступление обучающегося с презентацией по теме: «История сети Интернет». Поиск положительных и отрицательных сторон сети Интернет. Представления команд (название, девиз). Слово капитана команды сторонников Интернета. Слово капитана команды противников Интернета. Беседа, работа с листами ранжирования, подведение итогов. Заключительное слово учителя.
Учитель выполняет роль ведущего, который принимает или отвергает аргументы сторон и следит за тем, чтобы они не повторялись. Участники команд готовят аргументы «за» и «против» Интернета и оформляют свои доводы в письменной форме. Капитаны команд готовят небольшую речь, в которой обосновывают свою позицию. Одной из задач урока является выявить наиболее важные положительные и отрицательные позиции Интернета. Для этого каждой команде раздается лист ранжирования.
Лист ранжирования (таблица 3)

Табл. 3

Лист ранжирования

№	Название аргумента (проблемы)	1 2 3 4 5	6	7	8 9 Итого	Место
1						
2						
3						
4						
5						
6						
7						

В графу «Название аргументы» учащиеся вносят свои доводы или аргументы, которые они вынесли перед участниками диспута. Далее сравниваются проблемы по порядку, начиная с 1-ой.
Принцип ранжирования:
Если одна проблема будет важнее другой, то ставим 2:0, где 2 балла ставим более важной проблеме.
Если проблемы имеют одинаковую важность, тогда ставим 1:1.
Считаем итоговые баллы по каждой проблеме и подводим итог (выносим место) какая из проблем наиболее актуальна для обучающихся нашего класса.
Таким образом, каждая группа подводит итог и находит самые важные стороны, и наиболее актуальную проблему сети.
Закрепление нового материала.
Подведение итогов урока.
Во время урока мы смогли выделить положительные и отрицательные стороны Интернета. При обобщении всего вышесказанного можно сделать вывод, что Интернет представляет собой важный источник информации, который стоит использовать, при этом не забывая, что он несет не только положительную оценку, но и отрицательный эффект.
Сообщение домашнего задания.

УРОК – ПРАКТИЧЕСКАЯ РАБОТА «ОБРАБОТКА ИНФОРМАЦИИ»

Цель: научить учащихся отбирать наиболее важную и значимую информацию.

Задачи:

1. Обучать дифференцировать информацию.
2. Отбирать наиболее значимую информацию.
3. Работать в команде.
4. Логически мыслить.

Тип урока: *самостоятельная работа.*

Используемое оборудование: карточки.

План урока

Организационный момент.

Приветствие. Проверка состава класса.

Актуализация знаний.

Изучение нового материала.

На каждую парту выдается карточка с текстом. Учащиеся читают текст, после чего им предлагается сортировать информацию по нескольким признакам, наиболее значимым для них.

Признаки информации:

Опасная – безопасная;

Актуальная – неактуальная;

Важная – неважная;

Полезная – бесполезная;

Эмоциональная – не эмоциональная;

Понятная – непонятная;

Доступная – недоступная;

Адресная – безадресная.

Происходит дискуссия. Учащиеся доказывают почему они отнесли данный вид информации к определенному признаку.

Закрепление нового материала.

Подведение итогов урока.

Сообщение домашнего задания.

УРОК – КОНФЕРЕНЦИЯ «ЛЮБИМЫЙ ИСТОЧНИК ИНФОРМАЦИИ»

Тема: Любимый источник информации.

Цель: рассмотреть наиболее предпочтительный и используемый источник информации у нескольких обучающихся.

Задачи:

1. Выявить источники информации, которые чаще всего предпочитают учащиеся;
2. Обратить внимание почему именно данный источник информации используют учащиеся.

Тип урока: *комбинированный.*

Форма организации работы детей: рассказ своих докладов.

Форма организации работы учителя: форма обучения урок-конференция. Заслушивание докладов.

План урока

1. Организационный момент.
2. Приветствие. Проверка состава класса.
3. Актуализация знаний.
4. Изучение нового материала.
5. Заслушиваются доклады нескольких учащихся.
6. Закрепление нового материала.
7. Подведение итогов урока.
8. Педагог делает выводы по рассказанным докладам, ставит оценки за рассказ.
- 9 Сообщение домашнего задания.

КЛАССНЫЙ ЧАС НА ТЕМУ: «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДРОСТКОВ»

Цель: в ходе проведения классного часа подростки должны научиться делать более безопасным и полезным свое общение в интернете и иных информационно-телекоммуникационных сетях; дать рекомендации по безопасному использованию всемирного источника информации.

Задачи:

- выявить отношение подростков к интернету;
- сформировать у подростков знания правильного поиска информации в интернете;
- проинформировать подростков об отрицательных и положительных сторонах интернета;
- развивать умения видеть положительные и негативные стороны в работе с компьютером,

Ожидаемые результаты:

В ходе проведения классного часа дети должны научиться делать более безопасным и полезным свое общение в интернете и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- критически относиться к информационной продукции, распространяемой в Интернете;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Оборудование: компьютер, мультимедийный проектор, экран, тест на знание правил поведения в сети Интернет; тест на Интернет-зависимость; презентация «Интернет-зависимость у подростков»; таблица «плюсы» и «минусы» Интернета, буклеты-памятки.

Ход мероприятия

1. Организационный момент

Учитель: Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Интернет - это не только кладёз возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них - дети, которые могут не знать об опасностях мировой паутины. Очень большое внимание при работе с интернетом необходимо уделять именно вопросам безопасности. И ответить на вопросы: «Какие опасности подстерегают нас в интернете?» и «Как их избежать?» нам поможет этот классный час.

«Нам в интернете всё знакомо! Мы в интернете словно дома!»

А сейчас предлагаю вам проверить готовность к интернету и выполнить простой тест.

Тест на знание правил поведения в сети Интернет:

1. Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.
 - а) попрошу его фото, и потом отправлю своё;
 - б) посоветуюсь с родителями.
2. В чате тебя обзвали очень грубыми словами.
 - а) в ответ сделаю тоже самое;
 - б) прекращу разговор с этим человеком.
3. Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.
 - а) потребую доказательств, что она плохая;
 - б) сразу откажусь.
4. Пришло сообщение с заголовком «От провайдера» – запрашивают твой логин и пароль для входа в Интернет.
 - а) вышлю только пароль: они сами должны знать логин.
 - б) отмечу письмо как Спам.

Посчитай, сколько получилось ответов «А» и сколько «Б».

4 «А» - Тебе ещё многому надо научиться.

3 «А» и 1 «Б» - Внимательно прочитай памятку по безопасному поведению в Интернете.

2 «А» и 2 «Б» - Неплохо, но ты защищён лишь наполовину.

1 «А» и 3 «Б» - Ты почти справился, но есть слабые места.

4 «Б» - Молодец! К работе в сети Интернет готов!

Обсуждение вопроса: «Какие опасности подстерегают нас в Интернете?»

- угроза заражения вредоносным программным обеспечением;
- доступ к нежелательному содержанию;
- контакты с незнакомыми людьми с помощью чатов или электронной почты;
- неконтролируемые покупки;
- интернет-зависимость;
- интернет – преступники и их деятельность в сети.

Учитель: вот сколько опасностей подстерегает нас в интернете, давайте с вами подумаем и обсудим, что делать и как всего этого избежать.

1. Спрашивай взрослых.
2. Установи фильтр.

3. Не спеши открывать файлы.
4. Не спеши отправлять SMS.
5. Осторожно с незнакомыми.
6. Будь дружелюбен.
7. Не рассказывай о себе.

Учитель: Интернет прочно вошел в жизнь практически каждого человека. Очень многие уже не представляют свою жизнь без этого достижения техники. Однако это достижение рождает множество проблем, которые требуют незамедлительного решения.

«Интернет зависимость» – это широкий термин, обозначающий большое количество проблем поведения и контроля над влечениями.

Некоторые признаки виртуальной зависимости:

1. Пристрастие к виртуальным знакомствам – избыточность знакомых и друзей в сети Интернет.
2. Навязчивая потребность в сети – игра в онлайн-азартные игры.
3. Информационная перегрузка (навязчивый web-серфинг) – бесконечные путешествия по сети, поиск информации по базам данных и поисковым сайтам.

Тест на интернет – зависимость

Ответы на каждый вопрос даются по пятибалльной шкале:

1 – очень редко, 2 – иногда, 3 – часто, 4 – очень часто, 5 – всегда.

1. Как часто Вы обнаруживаете, что задержались в сети дольше, чем задумывали?
2. Как часто Вы забрасываете свои домашние обязанности, чтобы провести больше времени в сети?
3. Как часто Вы предпочитаете развлечения в интернете общению с друзьями?
4. Как часто Вы строите новые отношения с друзьями по сети?
5. Как часто Ваши знакомые жалуются по поводу количества времени, что Вы проводите в сети?
6. Как часто из-за времени, проведенном в сети страдает Ваше образование и/или работа?
7. Как часто Вы проверяете электронную почту, прежде чем заняться чем-то другим?
8. Как часто страдает Ваша эффективность или продуктивность в работе из-за использования интернета?
9. Как часто Вы сопротивляетесь разговору или скрываете, если Вас спрашивают о том, что Вы делали в сети?
10. Как часто Вы отодвигаете на второй план неприятные мысли о своей жизни, заменяя их успокаивающими мыслями об интернете?
11. Как часто Вы чувствуете приятное предвкушение от предстоящего выхода в сеть?
12. Как часто Вы боитесь, что жизнь без интернета станет скучной, пустой и безынтересной?
13. Как часто Вы раздражаетесь, кричите, если что-то отрывает Вас, когда Вы находитесь в сети?
14. Как часто Вы теряете сон, когда поздно находитесь в сети?
15. Как часто Вы чувствуете, что поглощены интернетом, когда не находитесь в сети, или воображаете, что Вы там?
16. Как часто вы замечаете свои слова «еще пару минут...», когда находитесь в сети?
17. Как часто Вы пытаетесь безуспешно урезать время пребывания в сети?
18. Как часто Вы пытаетесь скрыть количество времени пребывания в сети?
19. Как часто Вы предпочитаете находиться в сети вместо того, чтобы встретиться с людьми?
20. Как часто Вы чувствуете подавленность, плохое настроение, нервничаете, когда Вы не в сети, что вскоре исчезает, стоит Вам выйти в интернет?

Теперь подсчитайте общую сумму баллов.

При сумме баллов 50-79 стоит учитывать серьезное влияние интернета на вашу жизнь.

При сумме баллов 80 и выше, у Вас с высокой долей вероятности интернет-зависимость и Вам необходима помощь специалиста.

Учитель: А сейчас, ребята, предлагаю вам посмотреть презентацию «Интернет-зависимость у подростков».

Учитель: «Надеюсь, ребята, мы привели достаточно причин для того, чтобы вы хотя бы задумались о своем пристрастии к интернету? Если вы и без того уже давно заметили за собой непреодолимую тягу постоянно находиться в он-лайне, вам безусловно пригодятся советы о том, как избавиться от интернет-зависимости.»

Рекомендации подросткам

1. Используйте реальный мир для расширения социальных контактов. Реальный мир, жизнь человека – это постоянное освоение, расширение и преобразование реальности, и внутренней, и внешней. Таким путем человек становится совершеннее.
2. Определите свое место и цель в реальном мире. Ищите реальные пути быть тем, кем хочется. Избегайте простых способов достигать цели: бесплатный сыр – только в мышеловке.
3. Виртуальная реальность заполняет «дыры» в жизни. Живите без «заплаток»!
4. Компьютер – это всего лишь инструмент, усиливающий ваши способности, а не заменитель цели.
5. Развивать в виртуальной реальности то, что для вас не важно в реальной жизни, – нельзя. Делайте то, что хотите, в реальной жизни!
6. Ищите друзей в реальности. Виртуальный мир дает только иллюзию принадлежности к группе и не развивает никаких действительных навыков общения.
7. Наполняйте жизнь положительными событиями, поступками.
8. Имейте собственные четкие взгляды, убеждения.
9. Избегайте лживости и анонимности в виртуальной реальности.
10. Пребывайте «здесь и сейчас», а не «там».
11. Научитесь контролировать собственное время и время за компьютером.

Учитель: Интернет – это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что, как и наш реальный мир, всемирная паутина может быть и весьма опасна.

Самостоятельная работа по группам: «плюсы» и «минусы» Интернета

Задание: ученикам предлагается самим подумать и перечислить положительные и отрицательные стороны Интернета. Например, в интернете можно найти: прогноз погоды, новости, чат, магазины и др.

Заполняется таблица.

Положительные стороны Интернета:

- развитие технического прогресса;
- доступ к разнообразной информации;
- доступность и легкость покупок.

Отрицательные стороны Интернета:

- широкие знакомства – зависимость;
- теряется навык реального общения;
- портится язык (словарный запас);
- меняются цели человека;
- виртуальная реальность замещает действительную.

Подведем итоги классного часа (Рефлексия)

Учитель: А теперь подведём итоги нашего классного часа. У вас на столе лежат три картинки. Выберите и положите перед собой ту, которая соответствует вашему настроению.

Классный час понравился. Узнал что-то новое.

Классный час понравился. Ничего нового не узнал.

Классный час не понравился. Зря время потерял.

Учитель: «Сегодня мы познакомились с основными правилами поведения в сети Интернет, постарайтесь их соблюдать. А на память об этом классном часе я хочу подарить каждому из вас памятку по безопасному поведению в интернете».

Памятка по безопасному поведению в сети интернет

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей интернета и причинения возможного ущерба, вы должны предпринимать следующие меры предосторожности при работе в сети Интернет:

- Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
- Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.
- Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
- Всегда сообщайте взрослым обо всех случаях в интернете, которые вызвали у вас смущение или тревогу.
- Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в интернете. О подобных предложениях немедленно расскажите родителям.
- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.

ЕДИНЫЙ ТЕМАТИЧЕСКИЙ ЧАС НА ТЕМУ: «БЕЗОПАСНОСТЬ ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ: ВИДЫ ИНТЕРНЕТ-ПРЕСТУПЛЕНИЙ И СПОСОБЫ ИХ ПРЕДУПРЕЖДЕНИЯ»

ВВЕДЕНИЕ

Компьютерные преступления являются преступной деятельностью, которая предполагает использование информационных технологий для незаконного или несанкционированного доступа к компьютерной системе с намерением повреждения, удаления или изменения данных компьютера. Компьютерные преступления также включают мероприятия, такие как электронное мошенничество, злоупотребление устройствами, кража личных и технических данных, а также создание помех. Эти преступления не обязательно связаны с повреждением физических свойств. Они скорее относятся к манипуляции конфиденциальными данными и критически важной информации. Они включают такие мероприятия, как кража программного обеспечения. Эти преступные действия связаны с нарушением прав и конфиденциальности информации, а также краже и незаконной переработке важной информации. Различные типы компьютерных преступлений обусловили необходимость внедрения и использования новых и более эффективных мер безопасности.

Подготовительный этап

1. Предложение темы обучающимся.
2. Подбор материала из интернет-источников, газет, журналов.
3. Подготовка выступлений, обучающихся по заданной тематике.

План проведения единого тематического часа

Тема: Безопасность подростков в сети Интернет: виды интернет-преступлений и способы их предупреждения.

Цель: ознакомить обучающихся с основными интернет-угрозами и способами их предотвращения.

Задачи:

- 1) способствовать предотвращению интернет-преступлений в молодежной среде;
- 2) способствовать сплоченности коллектива.

Место проведения: кабинет

Оборудование: проектор и компьютер для просмотра видеороликов.

Время проведения: 45 минут.

Возрастная категория: 12-16 лет

Ход единого тематического часа

Часто подростки подвержены негативному влиянию извне, а так как Интернет на данный момент является неотъемлемой частью жизни, то именно там современных школьников и студентов и подстерегает большое количество опасностей.

1) Мошенничества, связанные с Интернет-магазинами.

Через Интернет могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно, поэтому желательно проверять сертификаты на предлагаемую продукцию

2) Фишинг.

Вид интернет-мошенничества, цель которого – получить все данные, содержащиеся на вашей электронной карте. Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою электронную карту просят указать пин-код и данные, содержащиеся на ней. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счете.

3) Интернет-попрошайничество.

В последнее время, в Интернете стали появляться объявления от благотворительной организации, детского дома, приюта или просто от родителей с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

4) Вредоносные программы.

Сущность вируса – переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники. Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы. После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная. Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения,

5) Социальные сети.

Социальные сети являются одним из способов вовлечения студентов в шантаж или же запрещенные РФ группы, подталкивающие молодых людей к совершению каких-либо противозаконных действий (насилие, жестокость). Социальные сети активно используются злоумышленниками для вовлечения детей и подростков в распространение порнографических материалов с участием несовершеннолетних посредством сети Интернет. В ходе электронного общения создаются условия, побуждающие подростка направить свои откровенные фотографии. После их получения данные изображения распространяются на тематических форумах, файлообменных системах и фото и видеопорталах.

6) Кибербуллинг.

Зачастую злоумышленнику становятся известны анкетные данные подростка, и тогда происходит так называемый «трóллинг» или травля (размещение в Интернете на форумах, в дискуссионных группах, в вики-проектах провокационных сообщений с целью собственного развлечения и созданием конфликтов между участниками). Это необходимо для установления круга знакомых, учителей и родителей подростка с целью направления им полученных провокационных фотографий, а возможно и с целью шантажа и выманивания определенной денежной суммы.

7) Интернет-знакомства.

Мошенники с сайтов знакомств – это особый тип людей, способный втираться в доверие к людям, очаровывать их с целью завладеть деньгами, имуществом. Им свойственно обычно глубокое знание психологии, умение построить общение так, что жертвы сами, добровольно отдают им материальные ценности. Причем в такую ловушку могут попасть как девушки, так и юноши.

8) Звуковые наркотики.

Особую популярность звуковые наркотики приобрели в 2009 году, однако и в 2025 году данный вид интернет-мошенничества имеет место. Реклама аудио наркотиков осуществляется посредством массовой рассылки писем на электронные почтовые адреса пользователей и на номера в системах быстрого обмена сообщениями. Доступ к прослушиванию аудиофайлов возможен после введения специального цифрового кода, получение которого происходит исключительно после оплаты в виде отправки смс-сообщения. Ресурсы, предлагающие такого рода продукцию, располагаются на площадях зарубежных провайдеров и зарегистрированы по фиктивным анкетным данным.

Заключение

Впервые мир узнал о компьютерных преступлениях в начале 70-х годов прошлого века, когда в Америке было выявлено довольно большое количество таких деяний. Как известно – наиболее опасные преступления – это те, которые носят экономический характер. Изначально, как показывает история, органы уголовной юстиции боролись с ней при помощи традиционных правовых норм о преступлениях против собственности: краже, присвоении, мошенничестве, злоупотреблении доверием и тому подобное. Однако вскоре практика показала, что такой подход не отвечает всем требованиям сложившейся ситуации, поскольку многие преступления в сфере компьютерной деятельности не охватываются традиционными составами преступлений. Принятый в недавнем прошлом кодекс содержит целую главу, включающую в себя три статьи, связанные с интернет-преступлениями.

РОДИТЕЛЬСКОЕ СОБРАНИЕ: «БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ»

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

Задачи:

1. Обсудить проблему зависимости подростков от Интернета;
2. Познакомить родителей с угрозами, с которыми подростки могут столкнуться в Интернете;
3. Совместно найти пути решения данной проблемы.

Подготовительные мероприятия:

- анкетирование учащихся по теме собрания;
- подготовка памятки для родителей.

Ход родительского собрания

Классный руководитель:

С большими, красными глазами

Сию я ночи напролёт,

Пока с утра над небесами

Светило медленно встаёт.

Одну и ту же слышу «песню»,

Что стал похожим на сову,

Ведь я уже не первый месяц

В сети безвылазно живу.

Все мы родители, поднимите руки те, чьи дети являются активными пользователями социальных сетей?

Наши дети растут и взрослеют в виртуальном пространстве, несмотря на все запреты и ограничения. Сегодня поздно, да и глупо отрицать влияние всемирной сети на детей. Нужно задуматься о правильном ее использовании.

Интернет пестрит сообщениями, что сети несут один вред: вместо уроков школьники сутками стучат по клавишам, пытаются привлечь внимание мнимых друзей... Другая сторона, наоборот, ратуют за «социалки», доказывая, что только с помощью этих общественных монстров можно реализовать себя, как личность.

Так социальные сети добро или зло?

Предлагаю разобраться на конкретных примерах.

У меня на столе стоят две чаши, в эту мы будем складывать наши аргументы за социальные сети, а в эту против

Мотивация к деятельности. Тренинг.

Родители рассаживаются по кругу лицом друг к другу, передавая из рук в руки приятный на ощупь мягкий мячик, высказывают свою точку зрения и аргументы по предлагаемому вопросу.

Вопросы:

1. Чем является компьютер в вашей семье?
2. Портит ли здоровье компьютер?
3. Сколько времени проводит за компьютером Ваш ребенок?
4. Опасаетесь ли Вы компьютерной зависимости Вашего ребенка.
5. Сколько времени Вы сами проводите за компьютером?
6. Как Вы относитесь к компьютерным играм?
7. Играет ли Ваш ребенок в компьютерные игры?
8. Знаете ли Вы название игр?
9. Контролируете ли Вы поведение ребенка в Интернете?
10. Обсуждаете ли Вы с ребенком сайты, которые он посещает?
11. Есть ли на вашем компьютере программа «Родительский контроль»

Компьютерная зависимость. Многим родителям нравится, что дети не балуются, не носятся по улице, а мирно сидят дома за компьютером. В результате, взрослые порой не подозревают, какую информацию черпает их ребенок из компьютера. Постепенно ребенок проводит за компьютером все больше времени. Отдельно различают психологическую зависимость от Интернета (сетеголизм) и от компьютерных игр (кибераддикция).

Первые признаки развития зависимости у ребенка и взрослого:

- если ест, пьет чай, готовит уроки у компьютера или смотрите телевизор,
- провели хотя бы одну ночь у компьютера,
- прогулял школу – сидел за компьютером,
- приходите домой, и сразу к компьютеру,
- испытывает эйфорию, хорошо себя чувствует за компьютером, и наоборот,
- ощущает пустоту, раздражение, когда вынужден заниматься чем-то другим или лишен компьютера,
- увеличивает число времени, проводимое за компьютером, в ущерб другим занятиям – работе, учебе, домашним делам, полностью или частично теряя к ним интерес,
- вступает в конфликт с близкими людьми из-за своей деятельности, что ведет ко лжи относительно того, что он делает,
- предвкушает следующий сеанс жизни в виртуальной реальности, что также поднимает настроение и захватывает все помыслы.

Опасности, которым подвергаются подростки в Интернете

Запретные сайты

Статистика пугает: 9 из 10 подростков в возрасте от 8 до 16 лет сталкивались с порнографией в сети, около 17% регулярно заглядывают на запретные ресурсы, около 6% готовы претворить увиденное там в жизнь. Дети могут столкнуться в Интернете с пропагандой насилия, жестокости, расовой нетерпимости. Информация в сети обновляется каждую секунду, и отследить ее очень трудно. Ребенок может случайно зайти на сайт, где ему распишут, насколько приятны на вкус наркотики. На ненадежных сайтах можно легко подхватить компьютерный вирус. И наконец, даже на доброжелательных ресурсах, во всплывающем окне может оказаться фотография обнаженного тела и более откровенные сцены, не предназначенные для детских глаз.

Меры борьбы

Самое главное – поддерживать доверительные отношения с подростком и заранее рассказать ему о том, с чем можно столкнуться во всемирной паутине. Изясняйтесь понятными словами: расскажите, что Интернет похож на мир за окном вашей квартиры, такой же интересный и насыщенный, но в нем встречаются и темные подворотни, и страшные незнакомцы, и опасные притоны, где ребенку, в целях его безопасности, лучше «не гулять». Сравнивайте Интернет с привычным ребёнку реальным миром. Так он быстрее освоится в виртуальном мире и запомнит правила безопасности. Так дети научатся ориентироваться в Интернете быстрее. С подростком 11-12 лет отправляйтесь на «Интернет-прогулку» только вдвоем. Пусть он сидит за клавиатурой и орудует мышкой, главное, чтобы вы контролировали весь маршрут его следования. Если ребенок пользуется Интернетом в одиночку, рассмотрите вариант конкретной фильтрации, используйте Интернет-няню. Подростки, особенно младшие, находят в Интернете много лишнего, а эта программа будет контролировать содержание веб-страничек, которые посещает ребенок, сохранит текст всех запросов, которые он посылает в поисковые системы, заблокирует доступ на сайты, которые вы внесли в «черный список» вашего компьютера. Установите на свой компьютер хороший антивирус и все время держите его включенным.

Опасность по почте – E-MAIL

«Подхватить» компьютерный вирус можно не только блуждая по закоулкам сети, но и в собственном почтовом ящике. Здесь же «водится» спам – рассылки сообщений рекламного характера. Кроме того, по почте или в ICQ можно получить сообщения, содержание которых окажется явно не для детских глаз: не первый год родители жалуются, что виртуальные хулиганы рассылают файлы или ссылки на сайты с веселыми компьютерными играми. Дети охотно рассматривают их содержимое, но внезапно во весь экран всплывает оскал мертвеца. Даже для психики взрослого такой поворот событий будет неожиданным. Не бойтесь рассказывать об этом своему ребенку, помните фразу: «Предупрежден, значит вооружен».

Меры борьбы

Зарегистрируйте для подростка не один, а несколько почтовых ящиков. Объясните ребенку, что свой домашний e-mail лучше давать только тем людям, которых он лично знает. Нельзя публиковать его на сайтах или в электронных анкетах, где их может обнаружить любой незнакомец. Электронные адреса друзей и родных также следует держать в секрете. Поставьте спам-фильтр. Если спам все-таки проникает в почтовый ящик, пусть ребенок запомнит: отвечать на спам-письма категорически воспрещается! Откликнувшись, мы даем подтверждение: да, этот электронный адрес действует, мы им пользуемся. Обязательно расскажите ребенку о том, что ни при каких обстоятельствах нельзя открывать вложенные файлы, которые пришли с неизвестных адресов. Объясните ребенку, что файлы могут содержать вирусы, способные уничтожить абсолютно все на вашем компьютере. В том числе его любимые игры и фото.

Чаты, форумы, сайты знакомств

Общаться – это прекрасно, но что, если за подростка выдает себя взрослый с совсем недетскими намерениями? Домогательствам педофилов в интернете ежегодно подвергаются 30% юных пользователей. Схемы стандартные: знакомство под вымышленным именем, выяснение интересов ребенка, потом предложение о встрече, чтобы «обменять постеры», а подростки очень доверчивы...

Меры борьбы

Объясните подростку, что его новые знакомые из чатов могут быть обманщиками. Даже если он прислал свою фотографию, это ни о чем не говорит. Объясните, что откровенничать с незнакомыми людьми опасно. Запретите ребенку публиковать в Интернете свой адрес, домашний телефон, номер мобильного, возраст, настоящую фамилию. Расскажите, что в Интернете люди общаются, не видя настоящего лица. Это игра, где каждый придумывает себе образ. Кстати, задумайтесь, почему ваш ребенок делится своими переживаниями с неизвестным человеком, а не с вами?

Онлайновые магазины, виртуальные казино

Прощайте папина зарплата и мамин аванс! Именно онлайновые ресурсы лидируют в списке причин, побуждающих ребенка воровать деньги у родителей. При желании здесь можно купить абсолютно все: легально – любой диск или игру, нелегально – оружие и наркотики. Устоять перед виртуальным казино и взрослому нелегко, а уж подростку...

Меры борьбы

Как и в случае с запретными сайтами, контролируйте доступ ребенка к нежелательным ресурсам, находитесь рядом или используйте специальную программу. Расскажите ребенку о том, что легких денег не существует, а вот попасть в неприятную ситуацию можно легко. Если он настойчиво ищет виртуальный заработок, может быть, имеет смысл подыскать ему подработку?

Игровая приставка или игровые программы

Игры неизбежно вызывают сильное эмоциональное перенапряжение, поэтому первое знакомство с ними должно состояться не раньше 7 лет. В виртуальном мире ребенок представляет себя сказочным героем, суперменом, оставаясь наяву неповоротливым и избалованным маменькиным сыночком. Игра дает возможность раскрепоститься. Также есть большой риск попасть в игровую зависимость и надолго уйти в виртуальный мир. Таких «невозвращенцев» зовут «игроманы», они знают об играх больше, чем об окружающей действительности. Подросткам 11-12 лет можно проводить за играми не более двух раз по

20-30 минут в день с перерывом на два часа (лучше на свежем воздухе). Подросткам до 16 лет допустимо проводить в играх около 40-50 минут 2-3- раза в день, и обязательно делать перерыв час-полтора.

Техника безопасности

Не ставьте игровую приставку в детской комнате, чтобы дозировать доступ к ней. Сразу же договоритесь, сколько часов в день будет проводить ребенок за игрой.

Скрытые угрозы

Жестокие игры или игры с элементами насилия, игры для взрослых. Выход один – тщательно проверять игру и в первый раз играть вместе.

Вас должно насторожить, если подросток после конфликтов или ссор сразу бросается к мобильному телефону или к компьютеру. Обратите внимание на ваши отношения с ребенком. Не стал ли компьютер в вашей семье заменой общения? Не ищет ли ребенок в сети внимания и любви, которых ему не хватает в семье?

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, следует установить ряд правил, с которыми должен согласиться и ваш ребенок. Если вы не уверены, с чего начать, вот несколько рекомендаций, как сделать посещение Интернета для детей полностью безопасным.

1. Поощряйте подростков делиться с вами их опытом в Интернете. Посещайте по возможности Сеть вместе с детьми.
2. Научите детей доверять интуиции. Если их в Интернете что-либо беспокоит, им следует сообщить об этом вам.
3. 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.
4. Настаивайте на том, чтобы дети никогда не выдавали своего адреса, номера телефона или другой личной информации: например, места учебы или любимого места для прогулки.
5. Объясните детям, что разница между правильным и неправильным одинакова как в и Интернете, так и в реальной жизни.
6. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.
7. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ - является кражей.
8. Скажите детям, что им никогда не следует встречаться с незнакомыми «друзьями» из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.
9. Скажите детям, что не все, что они читают или видят в Интернете, – правда. Приучите их спрашивать вас, если они не уверены в подлинности информации.
10. 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.

Если ребенок слишком много времени уделяет общению в Интернете с людьми, с которыми в реальной жизни он не знаком, понимание и поддержка семьи и родителей дадут возможность вернуться в реальность безболезненно. Ребенок должен ощущать себя нужным и любимым не только среди виртуальных «друзей», но и в настоящем обществе. Виртуальное общение только тогда может стать ненужным, когда реальная жизнь станет более интересной и насыщенной хорошими событиями.

Социальные сети помимо «отречения» от реального мира могут нести и другую опасность. Именно дети чаще всего становятся участниками различных группировок, ведущих противозаконный и аморальный образ жизни. Люди, навязывающие свое мнение в виртуальном пространстве, могут повлиять на ребенка психологически. Особенно вредному влиянию подвержены подростки, находящиеся на стадии «поиска смысла жизни». Поэтому родители должны быть бдительны и принимать меры, особенно если стали заметны некоторые из перечисленных признаков зависимости от Интернета у их детей:

1. Радикальное изменение привычек использования Интернета, как-то навязчивое стремление просиживать за компьютером, или, наоборот, резкий спад интереса у ребёнка в отношении социальных сетей и Интернета в целом.
2. Изоляция.
3. Спад успеваемости.
4. Скрытие информации от родителей, блокирование счетов в социальных сетях от родителей, удаление истории просмотра страниц Интернета.
5. Бодрствование в ночное время.
6. Получение детьми телефонных звонков с закрытых номеров.
7. Сомнительные подарки и т.д.

"В Последнее время в социальных сетях VK распространились так называемые «группы смерти» "Синий кит", "Тихий дом", в которых пропагандируется идея суицида. Для привлечения подростков предлагается вступить в игру, финалом которой является совершение самоубийства"

Суть игры "Синий кит" заключается в том, что каждый игрок должен выполнить 50 заданий. Для начала игрокам нужно порезать вены и нарисовать на руке с помощью лезвия силуэт кита. Последним из заданий является суицид, и его нужно выполнить обязательно. В противном случае организаторы игры грозят расправиться с родителями игрока.

С детьми в социальных сетях работают системно и планомерно, шаг за шагом подталкивая к последней черте. В России с ноября 2015-го по апрель 2016 года, насчитали 130 (!) суицидов детей, почти все они были членами одних и тех же групп в интернете, жили в благополучных и любящих семьях. Новые смерти анонсированы там же.

О «группах смерти» и подростковых суицидах в последние дни писали много - статьи о причинах, о случаях, о вреде Интернета, о контроле за детьми, о том, что «родители сами виноваты», или наоборот, что процесс это неуправляемый, об ужасе и неизвестности. Общий фон - страх и паника.

Родители бросились проверять профили детей в соцсетях. И многие нашли «касания» – в ленте, в группе, в чате. Нашли и... растерялись. Что же с этим делать теперь?

Ведь ребенок уже достаточно взрослый - не ограничишь общение, не уберешь интернет, не запретишь и не закроешь от мира. Есть информация, нет понимания, что с ней делать.

Как родителям распознать надвигающуюся беду:

Ваша семья – в группе риска – если:

- родители постоянно заняты на работе, а выходные заполнены бытом,
- ребенок загружен обучением, дополнительными кружками,
- много, активно и постоянно общается в соцсетях,
- слушает советы ровесников чаще, чем ваши,
- в семье взаимодействие на уровне «привет-пока», «все в порядке?»»,
- отсутствуют разговоры «о жизни», «о смысле», «о сексе», «о смерти», «о любви».

Первое, что может и должно помочь – это здоровая и сильная привязанность между родителем и ребенком. Если этого нет – дети легче поддаются чужому влиянию и управлению.

Итак, действуем!

Сначала действия конкретные.

1. Первое, что необходимо сделать, это понаблюдать и проанализировать жизнь и поведение вашего ребенка.

Будьте внимательны, благожелательны, не пытайтесь сразу выяснить, что и откуда, и ни в коем случае не «наезжайте», даже если вам стало страшно.

2. Если в жизни ребенка много «виртуала», должно быть столько же или больше реальной жизни - общения, действий. Игры, квесты, головоломки, скалолазание, батуты, бассейн, борьба, действия руками – шитье, лего, сборка моделей, квиллинг, скрапбукинг, вырезание, выпиливание и т.д. Делать то, что дает телесные ощущения, показывает объем пространства, создается собственными руками, дает ощущение значимости.

Все это не ради наград или для вас, а ради собственного удовольствия.

А чтобы начать процесс, когда «ничего не хочет» - начните делать что-то вместе – раз в неделю устраивайте активное совместное время без телефона и компьютера (у вас тоже их не должно быть).

3. Реально оцените нагрузки у ребенка по обучению, обязательствам, «нужным» действиям.

Если контакт с ребенком потерян - он не хочет с вами разговаривать. Чем в большем стрессе находится ребенок, тем больше он желает другой жизни (чаще подсознательно).

Снижайте нагрузки, требования, меняйте режим дня и его содержание.

4. Оцените количество правил в жизни вашего подростка – насколько много у него «нужного» и «необходимого». Столько же или больше должно появиться времени на «бесполезное». Устраивайте дни, когда правила отменяются, позволяйте иногда их нарушать, поддержите, когда ребенок хочет что-то изменить, отменить и не делать.

5. Проследите за «звуковым фоном» вокруг ребенка (наушники, телевизор, постоянные разговоры по телефону) – выключите работающий телевизор, устраивайте «дни тишины» – без музыки и видео, выезжайте в интересные места, где ограничено постороннее общение. Цель – погрузить в тишину, в собственные мысли, в «здесь и сейчас», притормозить быструю смену «картинок и звуков» вокруг.

6. Научите ребенка техникам переключения, «выхода из транса» виртуальности – умыться, потопать ногами, громко крикнуть. Сделать что-то необычное, быстрое, с привлечением органов чувств – звук, телесное действие, запах.

7. Научите ребенка методам «сохранения сознания». Когда страшно, паника, тревожность, непонимание, что происходит – выключить компьютер, побыть в тишине, выспаться, принять душ, сделать дыхательные упражнения, поговорить с близким взрослым.

8. Устройте ребенку возможность быть где-то значимым, делать что-то нужно и полезное, лучше в команде.

Если отправляете в лагерь, обратите внимание на цель и смысл лагеря. Если снова научить чему-то, если в лагере управляют взрослые и нужно делать, что говорят – ищите другой. Лучше всего найти проектный лагерь – где группа детей создает что-то, где есть выбор – делать или не делать, где будет собственная цель и желание ее реализовать.

Можно пойти в театральную студию – там есть «проживание» разных ролей, перевоплощение, совместное творчество, ощущение собственной значимости.

9. Если есть признаки того, что ребенок недосыпает, постарайтесь повлиять на режим сна. В постоянно «недоспавшем» состоянии снижается критичность, ухудшается память, увеличивается тревожность и внушаемость, падает иммунитет.

Здоровый и достаточный сон дает возможность упорядочивания информации, восстановления на всех уровнях – и физически, и психологически.

Рекомендую ночью установить запрет на интернет и телефон – это важно.

10. Учите ребенка критическому мышлению – задавать «неудобные» вопросы, протраивать логические цепочки, говорить «нет» или «я подумаю» на непонятные предложения. И в первую очередь давайте возможность ребенку спрашивать в семье и получать ответы - «зачем мне это надо?», «почему я должен это делать?».

11. Есть ли у вашего ребенка ощущение, что его любят «просто так»?

Задайте себе вопрос, если бы ваш ребенок не был успешен, не достигал, не делал и т.д. – вы бы им гордились? А он знает ваш ответ?

Есть ли у вашего ребенка в семье ощущение общности, командности, что семья, это не «я, сестра, мама, папа», а «МЫ»? Нужны совместные обсуждения важных семейных вопросов, своя зона ответственности в семье, доверие и открытое обсуждение любых вопросов.

12. И самое важное в этой теме.

Чтобы у ребенка не возникло желания уйти из жизни, он должен видеть настоящую, живую, яркую жизнь – вашу жизнь. Если вы сами живете безрадостно, серо и уныло - откуда у детей возьмется желание становиться взрослыми и «Жить Жизнь»?

Вы готовы менять отношения с ребенком и на более глубоком уровне? – вот четыре действия, ведущие к возвращению близости и понимания в отношения с ребенком.

1. Сформировать ритуалы семейного приветствия, прощания и общения, направленные на «завладение» ребенком. Взгляд «глаза в глаза», глубокие прочувствованные объятия, разговоры только с ребенком (не между делом), общее дело, приносящее радость не результатом, а процессом.

При приветствии - посмотреть в глаза, назвать по имени, показать радость от встречи, сказать об этой радости, обнять или просто дотронуться, спросить о времени, проведенном врозь (с искренней заинтересованностью).

При прощании - посмотреть в глаза, назвать по имени, обнять или просто дотронуться, немного поговорить о совместных планах после расставания.

Семейное общение - проводить периодические семейные собрания для обсуждения достижений, мыслей, чувств членов семьи, для построения совместных планов и распределения ответственности каждого в семейном быту.

Личное общение – философские разговоры о смысле жизни и о смерти, о любви, ненависти, о личном – об интересах ребенка, увлечениях, мыслях, мечтах, разочарованиях.

При общении нельзя осуждать, оценивать, советовать без запроса, помогать исправлять ошибки или говорить, что это была ошибка, требовать «правильного» поведения, следить, гордиться достижениями и разочаровываться от неудач ребенка.

Только активно слушать, поддерживать, помогать, когда просит помощи, наблюдать и быть рядом, когда нужно, уважать ребенка как личность во всем многообразии ее проявлений. Быть не другом, но наставником.

2. Дать «стержень привязанности», который будет дорог ребенку, то, что он будет хранить в своем сердце и не захочет отпустить. Это знаки безусловной любви.

Эмоциональная теплота, наслаждение от общения, восхищение самим фактом его существования, теплота в голосе позволяют ребенку почувствовать, что в вашем присутствии он может быть таким, какой он на самом деле, что может поделиться всеми переживаниями.

По вашему общению, глазам, действиям и словам ребенок должен понимать, что он желанный, особенный, важный, что его ценят и уважают вне зависимости от полученных оценок или наград.

Забудьте о словах «горжусь тобой за...», «если ты ... (закончишь четверть хорошо...), то...».

Гордость может быть только за то, что это - ваш ребенок, а достижения такая же часть жизни, как и неудачи.

3. Поощряйте просьбы о помощи, не стимулируйте независимость и самостоятельность специально — с возрастом они «придут» сами.

Ребенок в любом возрасте должен знать, что может обратиться к вам за помощью в любом вопросе, что может рассчитывать на вас в любой ситуации, опереться на вас, «спрятаться», если нужно, и вновь побыть ребенком, если хочется.

Проблема в том, что мы берем на себя слишком много ответственности за достижение зрелости нашими детьми. Подталкивая ребенка к самостоятельности и зрелости раньше, чем он будет к этому готов, мы вызываем панику и стремление найти вам «поддерживающую» замену – сверстников, группу по интересам, наставника в сети.

Стоит помнить, что единственный путь к настоящей независимости лежит через зависимость.

4. Будьте ориентиром, проводником для вашего ребенка.

Когда начинается школа, родители склонны считать, что их часть «работы» по ответам на все детские «почему» закончена. Мы больше предоставляем рассказывать о мире учителям и тренерам, чем самим постоянно объяснять и показывать, как устроены те или иные вещи в окружающем мире.

Так стоит ли удивляться, что дети начинают искать ответы везде, где готовы их дать, кроме как спросить у родителей?

Да, мы часто теряемся и прекращаем быть для ребенка проводником от неуверенности – ведь современные дети знают о мире компьютеров и интернета больше нас. Их язык, кажется иным, музыка непохожа на нашу, даже задачки в школе – другие.

Но мы забываем при этом, что уверенный вид наших детей не означает такое же уверенное понимание жизни – они не понимают, кто они и куда идут, а совета спрашивают у ровесников, знающих не больше них, но уверенно раздающих рекомендации. И такая информация в итоге не дает настоящей «картинки мира».

И здесь наша, родительская задача – оставаться для ребенка проводником.

Сообщать, что значат те или иные события, что происходит от таких действий, а что – от других, кто этот человек и почему он ведет себя именно так, как создаются обстоятельства и какой смысл в определенных действиях.

Конечно, большинство рекомендаций предполагают изменения образа жизни вашей семьи, изменение отношения к себе и к ребенку, а в первую очередь – большую внимательность, желание вникать, меняться и помогать.

Совета «сделайте так, и будет вам счастье» – не существует. Как и везде, нужно приложить усилия.

Но жизнь вашего ребенка того стоит.

Приложение №1

Цели данного опроса:

- определить степень влияния Интернета на современных школьников;

- узнать, на что тратят время современные юные пользователи в сети Интернет; определить, насколько ситуацией владеют их родители.

Обобщенные результаты социологического опроса позволят организовать соответствующую работу среди учащихся и их родителей.

Метод проведения опроса – анкетирование.

Анкета для учащихся

1. Сколько времени в день, обычно, вы проводите в сети Интернет?
а) 3-6 ч, б) более 6 ч, в) 1-2 ч, г) другое количество времени.
2. Для чего вы, в основном, используете сеть Интернет?
а) общение (соцсети, мессенджеры и др.), б) учеба, в) игры онлайн, г) мультимедиа (фото, музыка, фильмы и т.д.).
3. Зарегистрированы ли вы хотя бы в одной социальной сети?
а) да, б) нет.
4. Где вы пользуетесь социальными сетями чаще всего (место)?
а) дома,
б) на уроке,
в) на перерыве в школе, по дороге домой, во время других дел и т.д.
5. Случалось ли такое, что вы не успевали выполнить важное задание (домашнюю работу, поручение) из-за долгого временипрепровождения в сети?
а) часто,
б) иногда,
в) редко,
г) никогда.
6. Смогли бы вы успешно учиться без помощи Интернета?
а) да,
б) нет,
в) не знаю.
7. Смогли бы вы успешно саморазвиваться без помощи Интернета?
а) да,
б) нет,
в) не знаю.
8. Как часто вы выходите в сеть Интернет?
а) часто,
б) иногда,
в) редко.
9. Для чего вы, в основном, пользуетесь социальными сетями?
а) общение со знакомыми, с которыми можете видеться и видите в реальной жизни,
б) общение с людьми, с которыми вы не можете видеться в реальной жизни по каким-либо причинам,
в) поиск групп по интересам,
г) для новых знакомств,
д) другое (написать).
10. Считаете ли вы социальные сети всемирным злом, «наркотиком», «плохой» тенденцией?
а) да,
б) нет,
в) не знаю.
11. Влияет ли социальная сеть на ваши поступки в реальной жизни (отношение к людям, покупки, участие в мероприятиях и т.д.)?
а) да,
б) нет,
в) не знаю.
12. Какие группы вам более интересны в социальной сети?
а) группы коллективов из реальной жизни,
б) клубы любителей...,
в) развлекательные группы,
г) группы брендов, которыми вы пользуетесь.
13. Какие группы в соц. сетях наиболее опасны, ваше мнение. _____

Анкета для родителей

1. Сколько времени в день, обычно, Ваш ребёнок проводит в сети Интернет?
а) 3-6 ч, б) более 6 ч, в) 1-2 ч, г) другое количество времени, д) не знаю.
2. Для чего Ваш ребёнок, в основном, использует сеть Интернет?
а) общение (соцсети, мессенджеры и др.), б) учеба, в) игры онлайн, г) мультимедиа (музыка, фильмы и т.д.), д) не знаю.
3. Зарегистрирован ли Ваш ребёнок хотя бы в одной социальной сети?
а) да, б) нет, в) не знаю.
4. Где Ваш ребёнок пользуется социальными сетями чаще всего (место)?
а) дома, б) на уроке, в) на перерыве в школе, по дороге домой, во время других дел и т.д. г) не знаю.
5. Случалось ли такое, что Ваш ребёнок не успевал выполнить важное задание (домашнюю работу, поручение) из-за долгого времяпрепровождения в сети?
а) часто,
б) иногда,
в) редко,
г) никогда,
д) не знаю.
6. Смог ли бы Ваш ребёнок успешно учиться без помощи Интернета?
а) да,
б) нет,
в) не знаю.
7. Смог ли бы Ваш ребёнок успешно саморазвиваться без помощи Интернета?
а) да,
б) нет,
в) не знаю.
8. Как часто Ваш ребёнок выходит в сеть Интернет?
а) часто,
б) иногда,
в) редко,
г) не знаю.
9. Для чего Ваш ребёнок, в основном, пользуется социальными сетями?
а) общение со знакомыми, с которыми видится в реальной жизни,
б) общение с людьми, с которыми не может видаться в реальной жизни по каким-либо причинам,
в) поиск групп по интересам,
г) для новых знакомств,
д) другое(написать),
е) не знаю.
10. Считаете ли Вы социальные сети всемирным злом, «наркотиком», «плохой» тенденцией?
а) да,
б) нет,
в) не знаю.
11. Влияет ли социальная сеть на поступки Вашего ребёнка в реальной жизни (отношение к людям, покупки, участие в митингах и т.д.)?
а) да,
б) нет,
в) не знаю.
12. Какие группы вашему ребёнку более интересны в социальной сети?
а) группы коллективов из реальной жизни,
б) клубы любителей...,
в) развлекательные группы,
г) группы брендов, которыми он пользуется,
д) не знаю.
13. Какие группы в соцсетях наиболее опасны, ваше мнение. _____

Советы по безопасности в возрасте от 11 до 17 лет. (Для родителей)

1. Совместно с подростками необходимо обсудить с ребенком «черный список» запрещенных сайтов и часы проведения в Интернете, а также руководство по общению в Интернете (в особенности в чатах).
2. Не забывать беседовать с детьми об их виртуальных друзьях, а так же о том, чем они занимаются, будто разговор ведется о реальных друзьях.
3. Компьютер, подключенный к Интернету, должен находиться в общей комнате.
4. Средства блокирования вредоносных сайтов использовать как дополнение к стандартному родительскому контролю.
5. Научить подростка не устанавливать программы без разрешения. Обговорить, что он может случайно загрузить вирусы или иное нежелательное программное обеспечение.
6. Приучить подростка сообщать о любых тревогах или угрозах, связанных с Интернетом. Подсказать, что он в безопасности, если сам рассказал о своих переживаниях.
7. Научить не делиться своей личной информацией, используя средства электронной почты, систем мгновенного обмена сообщениями, чатов, регистрационных форм, личных профилей и при регистрации на online-конкурсы.
8. Самим не забывать знакомиться с сайтами, которые посещает подросток.
9. Поговорить о том, что нельзя использовать Интернет для распространения сплетен, хулиганства или угроз другим людям.
10. Следить за тем, чтобы ребенка подросток уважал других в Интернете. Проверить, что он знает правила хорошего поведения, которые действуют везде – даже в виртуальном мире.

**Занятия с элементами тренинга
для педагогов, подростков и их родителей
Тема: Безопасность подростков в Интернет-сети**

Современные подростки не представляют себе жизнь без гаджетов. А как иначе – ведь это часть их жизни. Гаджеты меняются и совершенствуются параллельно развитию и росту ребенка. Для старшего поколения компьютеры, телефоны – это введенные в их жизнь новшества, во многом облегчающие работу, общение. У взрослых есть опыт жизни без гаджетов. Это опыт прогулок во дворе, на улице, общения в школе, где не было тотального контроля со стороны родителей, а была личная ответственность за свои поступки. Был опыт поиска информации через книги, энциклопедии, к тому же книги и кинофильмы были источниками получения знаний об этических нормах, способах взаимодействия и общения со сверстниками, определяли ценности и нравственные принципы. Современные подростки даже не задумываются, а многие не предполагают, что была жизнь без гаджетов, без Интернет-ресурсов.

Цель: Повышение цифровой компетентности в Интернет-сети.

Задачи:

- Определение безопасного использования Сети.
- Определение опасности и способов ее избежать.
- Определение способов предотвращения опасности и обращение за помощью.
- **Оборудование:** интерактивная доска

Использованы источники:

1. Азбука безопасности. В Интернете <http://azbez.com/safety/internet>
2. Акции детского портала Tvidi.Ru."Правила безопасности в сети Интернет" <http://www.fid.su/projects/saferinternet/year/actions/tvidi/>
3. Анкета «Интернет и пятиклассники». http://ludmilakarnazhitska.blogspot.com/2010/11/blog-post_21.html
4. Безопасный компьютер и Интернет для детей: новая программа повышения квалификации преподавателей АПКППО //Microsoft в образовании. — [Электронный ресурс]. - Электрон. дан. – сор. 2008 – URL : <http://www.ms-education.ru>.
5. Википедия – свободная энциклопедия http://ru.wikipedia.org/wiki/Компьютерный_вирус

Упражнение 1.

Экспресс-диагностика:

1. Сколько вам лет?
2. С какого возраста вы являетесь активным пользователем Интернет-сети?
3. Сколько времени в день вы являетесь активным пользователем Интернет-Сети?
4. Сколько времени в день вы являетесь пассивным пользователем Интернет-Сети?
5. Оцените по шкале 0-100% А) пользу, В) вред Интернета.

Упражнение 2. «Мозговой штурм».

Группа разбивается на три команды. Записывают «Пользу», «Вред», «Опасности» Сети.

Ведущий на доске записывает ответы каждой команды.

Упражнение 3. Обсуждение в командах.

Что делать если...

- взломали вашу страничку в соцсетях,
- навязывают игру сомнительного содержания (агрессивная, эротическая, суицидальная);
- предлагают встретиться незнакомцы;
- просят переслать паспортные данные, адрес, телефон и т.д.

Обсуждение.

Упражнение 4. Знакомство с видами персональных данных (какую информацию мы даем о себе при регистрации в социальных сетях: логин, пол, возраст, номер мобильного телефона, адрес, место учебы, интересы и т.д.)

Обсуждение около 5 мин.

Упражнение 5. «Личное-публичное»

Участники по очереди (можно обсуждать в командах, парах или индивидуально) меняют «безличную информацию» на «персональную информацию», например:

Безличная информация:	Персональная информация:
«Москва – город-герой»	«Я живу в»
«Шарик – небольшая сфера»	«Моего пса зовут ...»
«Луна – искусственный спутник Луны»	«Я мечтаю побывать.....»

Обсуждение: насколько легко/трудно устанавливать отношение между собой (личная информация) и безличной информацией? Как вы понимаете фразу «отсутствие информации – это тоже информация»?

Упражнение 6. «Информационный светофор»

Участники получают по 5 красных и по 5 зеленых стикеров. Они должны записать, какую информацию они с легкостью могут выложить в Интернет –зеленый стикер (например, имя, пол, возраст и т.д.), а какой информацией они не поделились бы в Сети (например, адрес, телефон и т.д.).

После этого ведущий записывает на доске виды персональных данных и обсуждает их с группой.

Обсуждение: Какой вид персональных данных набрал больше всего зеленых/красных стикеров? Почему? Какой информацией мы делимся более/менее охотно? Почему?

Упражнение 7. «Секретная информация»

Участникам предлагается написать на листочке какой-либо свой секрет (можно шуточный, если доверие в группе невысокое). По команде ведущего участники передают свой листочек сидящему слева, берут – у сидящего справа. Со следующей командой – следующая передача. И так, пока не вернется свой листок.

Обсуждение: Что вы чувствовали, когда ваш секрет находился в чужих руках? Что вы чувствовали, когда чужой секрет находился в ваших руках? Хотелось ли прочитать? Поделиться с кем-то? Случалось ли вам выкладывать аналогичную информацию в Сеть?

Подведение итогов.

Понятно ли вам понятие «персональные, личные» данные?

Изменилось ли ваше представление о пользе и вреде Интернета?

Эмоциональный отклик по всему занятию.

Законы, обеспечивающие безопасность детей и подростков в Интернете.

В России на протяжении нескольких лет предпринимаются разноплановые действия по созданию механизмов, обеспечивающих безопасность детей в Интернете. В 2010г. был принят Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» [13]. Например, им определен состав вредного контента, предусмотрена возрастная маркировка информационных материалов, а также установлены требования к обороту информационной продукции. В 2012 году Президентом России была утверждена Стратегия развития воспитания в Российской Федерации на период до 2025 года. Цель стратегии – сокращение числа детей. Пострадавших от противоправного контента в интернет-среде. В результате совместной работы ведомств, парламентариев, российских субъектов проделана следующая работа: Министерство культуры России в 35 субъектах реализует проект по отбору сайтов, благоприятных для детей. На сегодняшний день отобрано порядка 750 таких ресурсов. Обеспечен доступ к музейным фондам через виртуальные музеи, возможен просмотр фильмов, спектаклей выдающихся отечественных режиссеров кино и театров (на платформе интернет-портала «Культура»). Роспотребнадзор принял решение о закрытии 3900 интернет-страниц в связи с содержащейся там информацией, угрожающей психическому здоровью детей. Роскомнадзор ведет активный мониторинг исполнения закона о противодействии нецензурной брани в СМИ.

Тесты-опросники на выявление ранних признаков компьютерной зависимости у несовершеннолетних

Тесты позволяют определить уровень компьютерной зависимости учащихся образовательных учреждений разной возрастной категории.

Тесты-опросники состоят из двух блоков: первый блок заполняется учащимися, второй – родителями учащихся.

Инструкция. Внимательно прочтите десять вопросов. Каждый из них Вы должны оценить как верный или неверный. Если вопрос кажется Вам верным или преимущественно верным, поставьте «Да», если неверным – «Нет».

Блок I. Тесты для учащихся образовательных учреждений

Вариант 1.

1. Часто ли Вы замечаете, что проводите в онлайн больше времени, чем намеревались? (да / нет)
2. Часто ли Вы пренебрегаете домашними делами, чтобы провести больше времени в сети? (да / нет)
3. Часто ли окружающие интересуются количеством времени, проводимым Вами в сети? (да / нет)
4. Замечете ли Вы, что Ваша успеваемость в школе стала хуже из-за того, что на учебу у Вас не остается времени, так как Вы слишком много времени проводите в сети? (да / нет)
5. Часто ли Вы представляете, как вновь окажетесь в Интернете? (да / нет)
6. Часто ли Вы ощущаете, что жизнь без Интернета скучна, пуста и безрадостна? (да / нет)
7. Часто ли Вы ругаетесь, кричите или иным образом выражаете свою досаду, когда кто-то пытается отвлечь Вас от пребывания в сети Интернет? (да / нет)
8. Часто ли Вы пренебрегаете сном, засиживаясь в Интернете допоздна? (да / нет)
9. Чувствуете ли Вы оживление, возбуждение, находясь за компьютером? (да / нет)
10. Появились ли у Вас нарушения сна и/или изменился ли режим сна, с тех пор как Вы стали использовать компьютер ежедневно? (да / нет)

Вариант 2.

1. Вам приходилось просить учителей, родителей заменить хотя бы часть знаний компьютерными играми? (да / нет)
2. Вы чувствуете, что Вам не всегда удастся сразу же прекратить компьютерную игру? (да / нет)
3. Вы чувствуете себя раздраженным или усталым, если долго не играете на компьютере? (да / нет)
4. Обычно Вы занимаетесь компьютерными играми больше, чем планировали? (да / нет)
5. Вам приходилось срочно закрывать окно с компьютерной игрой или сайта, когда приходили родители, учителя, друзья? (да / нет)
6. Вам приходилось садиться за компьютерную игру, чтобы исправить себе настроение (например, чувство вины, раздражительности) или просто, чтобы успокоиться? (да / нет)
7. Возникают ли у Вас головные боли после игры за компьютером? (да / нет)
8. Пренебрегаете ли Вы приемом пищи из-за компьютерной игры? (да / нет)
9. Пренебрегаете ли Вы личной гигиеной из-за компьютерной игры? (да / нет)

10. В обычной жизни чувствуете ли Вы пустоту, раздражительность, подавленность, которые исчезают при игре за компьютером? (да / нет).

Подсчет результатов: производится специалистами, проводившими тестирование.

«Да» – 1 балл,

«Нет» – 0 баллов.

Полученные баллы суммируются.

0 – 3 балла – низкий уровень компьютерной зависимости.

4 – 6 балла – средний уровень компьютерной зависимости.

7 – 10 баллов – высокий уровень компьютерной зависимости.

Блок II. Тесты для родителей

Вариант 1.

Ваш ребенок, ...

1. Приходя домой, первым делом садится за компьютер? (да / нет)

2. Забросил домашние дела, учебу, стал непослушным? (да / нет)

3. Раздражителен, груб, если его отвлекают от компьютера? (да / нет)

4. Совершает прием пищи, не отрываясь от компьютера? (да / нет)

5. Не знает, чем себя занять, если компьютер недоступен или сломался? (да / нет)

6. Не способен контролировать время, проводимое за компьютером? (да / нет)

7. Тратит много денег на компьютерные игры? (да / нет)

8. Перестал общаться с друзьями, все больше времени проводит в онлайн? (да / нет)

9. Посещает различные запретные сайты? (да / нет)

10. Постоянно говорит о компьютерных играх, об общении в Интернете? (да / нет)

Вариант 2.

Ваш ребенок, ...

1. Испытывает раздражение при необходимости закончить игру? (да / нет)

2. Из-за компьютерной игры жертвует времяпровождением с семьей, родными? (да / нет)

3. После компьютерной игры жалуется на головные боли, возникает сухость слизистой оболочки глаз? (да / нет)

4. Высказывает желание проводить в Интернете больше времени? (да / нет)

5. Во время компьютерной игры полностью отрешается от реальной действительности, целиком переносясь в мир игры? (да / нет)

6. Из-за компьютерной игры пренебрегает питанием, личной гигиеной? (да / нет)

7. В результате систематического времяпровождения за компьютером, потерял интерес к учебе, к спортивным секциям, кружкам? (да / нет)

8. Преимущественно находится в хорошем настроении, занимаясь компьютерными играми или общением онлайн? (да / нет)

9. Проводя длительное время в Интернете, нарушает режим дня? (да / нет)

10. Предпочитает общение с виртуальными друзьями, чем с реальными? (да / нет).

Подсчет результатов: производится родителями.

«Да» – 1 балл,

«Нет» – 0 баллов.

Полученные баллы суммируются.

0 – 3 балла – низкий уровень компьютерной зависимости; родители могут справиться с возникшей проблемой самостоятельно (см. рекомендации);

4 – 6 балла – средний уровень компьютерной зависимости, для решения проблемы необходима консультация специалиста (психолога);

7 – 10 баллов – высокий уровень компьютерной зависимости, чрезмерное увлечение компьютером, которое может привести к психологической зависимости ребенка; родители не могут справиться с возникшей проблемой самостоятельно, поэтому необходимо обратиться за помощью к специалисту (психологу, психотерапевту).

Научное издание

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

для педагогов по организации и проведению просветительских мероприятий
с подростками и родителями по вопросам обеспечения информационной
безопасности и профилактики компьютерной зависимости у обучающихся

Составитель:

Инесса Валериевна Рудковская

Технический редактор:

Н. А. Сытник

Компьютерная вёрстка и макетирование:

К. С. Морарь

За достоверность представленной информации и ссылок
ответственность несёт составитель

Подписано к изданию 27.06.2025 г.

Формат 60x84/16. Бумага 80 г/м².

Усл.-печ. л. – 5,03. Уч.-изд. л. – 3,12.

Усл.-изд. л. – 2,90.

Тираж 300 экз. Зак. № 63.

Издательство ФГБОУ ВО «Донецкий государственный
педагогический университет им. В. Шаталова»

Справка ГЛАВСТАТА ДНР Серия АА № 08-22/1277 от 05.03.2020
284626, ДНР, г. о. Горловка, г. Горловка, ул. Рудакова, 25