Методические материалы
для организации системы медиабезопасности

1. Информационная памятка для обучающихся о безопасном поведении и использовании сети интернет

(Министерство образования и науки Российской Федерации,
Департамент государственной политики в сфере общего образования,
Письмо от 14 мая 2018 г. № 08-1184 «О направлении информации»)

С каждым годом молодежи в интернете становится больше, а школьники - одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в Сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных про­грамм, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользо­вателю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие се­рьезный уровень защиты от вредоносных программ.
2. Постоянно устанавливай патчи (цифровые заплатки, которые ав­томатически устанавливаются с целью доработки программы) и дру­гие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим авто­матического обновления, включи его.
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных про­грамм инсталлироваться на твоем персональном компьютере.
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.
5. Ограничь физический доступ к компьютеру для посторонних лиц.
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников.
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистри­ровала бренд WECA, что обозначало словосочетание “Wireless Fidelity”, которое переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура Wi-Fi. Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в пе­реводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах явля­ется отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, ло­гины и какие-то номера.
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство.
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, одна­ко некоторые пользователи активируют ее для удобства использова­ния в работе или учебе.
4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту.
5. Используй только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводи именно «https://».
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди ра­ботают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей плане­ты. Многие пользователи не понимают, что информация, размещен­ная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть слу­чайных и незнакомых людей.
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Зло­умышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты за­гружаешь? Подумай, прежде чем что-то опубликовать, написать и за­грузить.
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место житель­ства, место учебы и прочее.
5. Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить твое местоположение.
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.
7. Для социальной сети, почты и других сайтов необходимо ис­пользовать разные пароли. Тогда если тебя взломают, то злоумышлен­ники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в за­конах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается прово­дить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны гос­ударственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства.
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или пере­хвата платежного пароля.
3. Выбери сложный пароль. Преступникам будет непросто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, воскли­цательный знак и т. п. Например, $tR0ng!.
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределя­ются в компьютерной сети. Обычно электронный почтовый ящик выгля­дит следующим образом: имя\_пользователя@имя\_домена. Также, кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше дове­рять тем, кого знаешь и кто первый в рейтинге.
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «те- ма13».
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS.
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность.
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах.
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорб­ления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя ве­сти и, если нет того, к кому можно обратиться, то вначале успокоить­ся. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.
2. Управляй своей киберрепутацией.
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.
5. Соблюдай свою виртуальную честь смолоду.
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
7. Бан агрессора. В программах обмена мгновенными сообщения­ми, в социальных сетях есть возможность блокировки отправки со­общений с определенных адресов.
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая по­мощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрос­лый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрыва­ющие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона.
4. Используй антивирусные программы для мобильных телефонов.
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.
6. После того как ты выйдешь с сайта, где вводил личную инфор­мацию, зайди в настройки браузера и удали cookies.
7. Периодически проверяй, какие платные услуги активированы на твоем номере.
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online-игры

Современные онлайн-игры - это красочные, захватывающие развле­чения, объединяющие сотни тысяч человек по всему миру. Игроки ис­следуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпус­каются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авториза­ции большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприят­ности, заблокируй его в списке игроков.
2. Пожалуйся администраторам игры на плохое поведение этого иг­рока, желательно приложить какие-то доказательства в виде скринов.
3. Не указывай личную информацию в профайле игры.
4. Уважай других участников по игре.
5. Не устанавливай неофициальные патчи и моды.
6. Используй сложные и разные пароли.
7. Даже во время игры не стоит отключать антивирус. Пока ты иг­раешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не уди­вишь, но с развитием интернет-технологий злоумышленники переме­стились в интернет и продолжают заниматься «любимым» делом.

Так появилась новая угроза: интернет-мошенничество или фи­шинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя ан­кета была взломана, то необходимо заблокировать ее и сообщить ад­министраторам ресурса об этом как можно скорее.
2. Используй безопасные веб-сайты, в том числе интернет­магазинов и поисковых систем.
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твое­му профилю в сети, а не ко всем.
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взло­мали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.
5. Установи надежный пароль (PI№) на мобильный телефон.
6. Отключи сохранение пароля в браузере.
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в ин­тернете, может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формиру­ется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, осо­бенности характера и рассказы о близких - все это накапливается в сети. Многие подростки легкомысленно относятся к публикации лич­ной информации в интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Коммента­рии, размещение твоих фотографий и другие действия могут не ис­чезнуть даже после того, как ты их удалишь. Ты не знаешь, кто со­хранил эту информацию, попала ли она в поисковые системы и со­хранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением при­чинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети.
2. В настройках профиля установи ограничения на просмотр твое­го профиля и его содержимого, сделай его только «для друзей».
3. Не размещай и не указывай информацию, которая может кого- либо оскорблять или обижать.

Авторское право

Современные школьники - активные пользователи цифрового про­странства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интел­лектуальную собственность. Термин «интеллектуальная собствен­ность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на про­дукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями. Авторские права - это права на ин­теллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего тру­да, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публич­но демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в интернете. Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаун­там до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

Десять фактов, которые нужно сообщить детям ради безопас­ности в интернете

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, c 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 детей делиться с вами их опытом в интернете. По­сещайте 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 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.
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.
11. Практические рекомендации по организации образовательного пространства для учащихся, использующих ИКТ технологии в обучении

Технологии обучения детей и подростков, использующих ИКТ технологии в обучении, обладают определенной спецификой. Разви­тие у таких учащихся познавательных способностей, расширение сферы их учебных интересов с использованием информационных компьютерных ресурсов требует «продвинутых» педагогических тех­нологий:

* специального учебно-методического и дидактического обеспече­ния;
* создания соответствующих организационных условий;
* подготовки кадров, которые смогут помочь учащимся в обуче­нии;
* подготовки технических возможностей учебного учреждения.

Организационно-методическая работа должна осуществляться не

только в учебной, но и во внеучебной деятельности учащихся.

Технологический алгоритм работы с детьми и подростками, гото­выми применять в познавательных целях новые информационные технологии, может состоять в следующем:

1. в составлении каталогов интересующих информационных ре­сурсов;
2. разработке печатных и электронных рекомендаций о способах формулирования запросов и поиска информации;
3. подготовке наборов «развивающих» информационных блоков для учащихся разного возраста.

В связи с задачами обучения увлеченность информационными технологиями граничит с понятием «компьютерной зависимости», поэтому вполне логичен вопрос: в какой момент такая увлеченность начинает становиться чрезмерной? На данном временном этапе фе­номен компьютерной зависимости нуждается в широком научном ис­следовании, в условиях экспериментальных лабораторий и во взаи­модействии педагогов с психологами и медиками. Актуальным стано­вится создание психодиагностической базы, которая должна строить­ся с учетом поведенческих, эмоциональных и личностных особенно­стей учащихся. В критерии диагностики могут входить следующие параметры:

* способность к самоконтролю и саморегулированию;
* развитие рефлексии своей деятельности;
* способность к антиципации: умению предвидеть последствия своих поступков;
* используемые психологические защиты (уход от проблем, пере­нос вины на других, оправдание, ответная агрессия и т. д.);
* развитость коммуникативных качеств и копинг-поведения.

Организация работы с учащимися предполагает проведение про­филактической работы в целях предупреждения появления компью­терной зависимости. Данная профилактическая работа может носить как локальный характер, обеспечивающий предупреждение возмож­ных неблагоприятных последствий, так и индивидуальный характер, направленный на предупреждение возможных неблагополучий инди­видуального развития конкретного учащегося через систему психоло­гической службы школы.

1. Памятка по медиабезопасности несовершеннолетних

(для родителей)

Интернет - прекрасное место для общения, обучения и отдыха. Но стоит понимать, что, как и наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна.

Приведем несколько рекомендаций, с помощью которых посещение интернета может стать менее опасным для ваших детей:

1. Посещайте интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения интернета.
2. Объясните детям, что если в интернете что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством.
3. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т. д.), использовании онлайн-игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее ника­кой личной информации.
4. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогул­ки, время возвращения домой, место работы отца или матери и т. д.
5. Объясните своему ребенку, что в реальной жизни и в интернете нет разницы между неправильными и правильными поступками.
6. Научите ваших детей уважать собеседников в интернете. Убеди­тесь, что они понимают, что правила хорошего тона действуют одина­ково в интернете и в реальной жизни.
7. Скажите им, что никогда не стоит встречаться с друзьями из интер­нета. Ведь люди могут оказаться совсем не теми, за кого себя выдают.
8. Объясните детям, что далеко не всё, что они могут прочесть или увидеть в интернете, - правда. Приучите их спрашивать о том, в чем они не уверены.
9. Не забывайте контролировать детей в интернете с помощью специального программного обеспечения. Это поможет вам отфиль­тровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

Советы родителям

Шаг 1: выбирайте сайты, которые можно посещать вашему ребен­ку, а какие нельзя (блокируйте доступ к неподходящим сайтам).

Шаг 2: увеличьте уровень защиты и конфиденциальности (создай­те отдельные учетные записи для разных пользователей).

Шаг 3: следите за тем, какие сайты посещают ваши дети.

Шаг 4: напоминайте детям, чтобы они не общались в интернете с незнакомцами.

Пусть интернет будет вам и вашим детям только в радость!

«Постарайтесь шагать рядом с ребенком по дороге жизни - и ему не нужно будет удирать в виртуальный мир».

1. Как научить детей отличать правду от лжи в интернете?

(информация для родителей)

Следует объяснить детям, что нужно критически относиться к по­лученным из сети интернет материалам, ведь опубликовать информа­цию в интернете может абсолютно любой человек. Объясните ребен­ку, что сегодня практически каждый человек может создать свой сайт и при этом никто не будет контролировать, насколько правдива раз­мещенная там информация. Научите ребенка проверять все то, что он видит в сети интернет. Как это объяснить ребенку?

* Начните, когда ваш ребенок еще достаточно мал. Ведь сегодня даже дошкольники уже успешно используют сеть интернет, а значит нужно как можно раньше научить их отделять правду от лжи;
* Не забывайте спрашивать ребенка об увиденном в сети интернет. Например, начните с расспросов, для чего служит тот или иной сайт.
* Убедитесь, что ваш ребенок может самостоятельно проверить прочитанную в сети интернет информацию по другим источникам (по другим сайтам, газетам или журналам). Приучите вашего ребенка со­ветоваться с вами. Не отмахивайтесь от их детских проблем.
* Поощряйте ваших детей использовать различные источники, та­кие как библиотеки, или подарите им энциклопедию на диске, напри­мер «Энциклопедию Кирилла и Мефодия» или Microsoft Encarta. Это поможет научить вашего ребенка использовать сторонние источники информации.
* Научите ребенка пользоваться поиском в сети интернет. Покажи­те, как использовать различные поисковые машины для осуществле­ния поиска.
1. «Интернет-зависимости» и их опасность для пользователей сети

Психологами отмечается распространенность в среде пользовате­лей, в том числе несовершеннолетних, случаев болезненного при­страстия к участию в сетевых процессах, так называемой «интернет­зависимости», проявляющегося в навязчивом желании неограничен­но долго продолжать сетевое общение. По данным различных иссле­дований, интернет-зависимыми сегодня являются около 10% пользо­вателей во всем мире. Нередко несовершеннолетние настолько при­вязываются к виртуальному миру и своему вымышленному персо­нажу, что забывают обо всем остальном. Для подростков интернет как виртуальная среда иногда кажется даже более адекватной, чем реальный мир. Возможность перевоплотиться в некую бестелесную «идеальную личность» открывает для них новые ощущения, которые им хочется испытывать постоянно или все более часто. Зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определенной деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр и интернет-зависимости. Специалисты отмечают, что в некоторой сте­пени указанная зависимость близка к патологической увлеченности азартными играми, а ее деструктивные эффекты схожи с возника- ющими при алкоголизме и наркомании, однако, в отличие от послед­них, имеют нехимическое происхождение. Высказывается мнение, что в подавляющем большинстве случаев такая зависимость - не са­мостоятельное состояние, а синдром в рамках другого психического расстройства. Таким образом, интернет-зависимость (как вид нехи­мической зависимости) - это навязчивая потребность в использова­нии интернета, сопровождающаяся социальной дезадаптацией и вы­раженными психологическими симптомами. Патология проявляется в разрушении обычного образа жизни, смене жизненных ориенти­ров, появлении депрессии, нарастании социальной изоляции. Проис­ходит социальная дезадаптация, нарушаются значимые обществен­ные связи.

Выделяется 5 основных типов интернет-зависимости с учетом то­го, к чему сформировалось пристрастие у конкретной личности: «ки­берсексу», виртуальным знакомствам, сетевым азартным играм, ком­пьютерным играм или навязчивому перемещению по Web-узлам:

1. Навязчивый веб-серфинг - бесконечные путешествия по Все­мирной паутине, поиск информации.
2. Пристрастие к виртуальному общению и виртуальным знаком­ствам - большие объемы переписки, постоянное участие в чатах, веб­форумах, избыточность знакомых и друзей в Сети.
3. Игровая зависимость - навязчивое увлечение компьютерными играми по сети.
4. Навязчивая финансовая потребность - игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные уча­стия в интернет-аукционах.
5. Пристрастие к просмотру фильмов через интернет, когда больной может провести перед экраном весь день, не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.

Основные признаки интернет-зависимости: 1) чрезмерное, немо­тивированное злоупотребление длительностью работы в сети, не обусловленное профессиональной, учебной или иной созидательной деятельностью; 2) использование интернета как преобладающего средства коммуникации; 3) создание и эксплуатация виртуальных образов, крайне далеких от реальных; 4) влечение к интернет-играм и (или) созданию вредоносных программ (без какой-либо цели); 5) субъективно воспринимаемая невозможность обходиться без ра­боты в сети.

При появлении указанных выше признаков следует обратиться за медицинской (психологической и (или) психиатрической) помощью, так в запущенном состоянии интернет-зависимость и игромания зна­чительно хуже поддаются коррекции.

1. Тест для выявления степени медиакомпетентности аудитории (Поттер Джеймс)

Поттер Джеймс выделил следующие уровни развития аудитории по отношению к медиа и предложил следующие вопросы к ним.

Познавательный уровень

1. Вспомните ваш любимый телесериал, затем выполните следу­ющие две задачи:
2. составьте список всех важных персонажей и опишите каждого подробно;
3. опишите события, которые, по-вашему, случатся в следующих сериях.

Эмоциональный уровень

1. Все эмоции имеют диапазон подэмоций, или подтипов. Напри­мер, эмоция опасения имеет подтипы ужаса, паники, борьбы, страха, испуга, предчувствия, беспокойства, нервозности, осторожности, приступа растерянности, волнения и т. д. Любой из них - тип опасе­ния, но каждый указывает на различный оттенок этого чувства. А сколько подтипов вы можете перечислить для чувства любви? Сколько - для печали?
2. Посмотрите телевизионную передачу и подсчитайте, сколько раз вы видите выражения чувств опасения, любви и печали?
3. когда вы видите выражение одного из этих чувств, способны ли вы классифицировать их подтип?
4. посмотрите несколько различных видов телевизионных про­грамм и отметьте, какие эмоции изображаются там наиболее ча- сто/редко.

Моральный уровень

1. Посмотрите несколько экранных медиатекстов приключенческо­го жанра, где отчетливо показано антиобщественное поведение (пре­ступление, насилие, ложь). Заметьте, как персонажи совершают эти действия. Пробуйте классифицировать этих персонажей по уровням морального развития:
2. поразмышляйте о медиатексте в целом и попытайтесь выявить намерения авторов и продюсеров; к которому моральному уровню аудитории они обращаются?
3. если бы вы создавали этот медиатекст и хотели ориентироваться на публику с более высоким уровнем медиавосприятия, что вы изме­нили бы в сценарии? [Potter, 2001, p. 34].

Ключ к оценке результатов тестирования, имея в виду те же уровни развития аудитории в области медиа.

Познавательный уровень

1. Ответы на часть (а) первого вопроса отражают вашу степень прозрачности интеллекта. Посмотрите, сколько персонажей вы пе­речислили? Сколько прилагательных или описательных фраз вы перечисляли для каждого персонажа? Заметьте разнообразие в описаниях: были ли они целиком основаны на физиологических данных? Или также перечислялись другие признаки типа индиви­дуальности (одежда, карьера, любимые жесты/особенности и т. д.)? Чем больше вы вспомнили подробностей, тем большее количество информации вы способны воспринимать/анализировать).

Ответы на часть (b) первого вопроса отражают степень флюидно- сти вашего интеллекта. Если вам было трудно размышлять о любых событиях медиатекста, у вас низка флюидность. Если вы показали немалые возможности воображения и творческого потенциала, у вас высокий уровень флюидности интеллекта.

Сравните ваше выполнение задач (a) и (b). Если вы выполнили (a) намного лучше, то у вас развитые способности собрать факты. Если вы делали намного лучше задание (b), то ваш интеллект флюиден, у вас развитое воображения и поиск новых перспектив. Развитие высо­кого уровня медиаграмотности требует, чтобы вы увеличили оба из этих типов интеллекта.

Эмоциональный уровень

1. Чем большее количество подэмоций перечислено вами, тем лучше вы настроены к пониманию тонкого изменения чувств, и тем более вы эмоционально грамотны.
2. Чтобы быть способным определить эмоции в других, нужна способность к сочувствию, к ощущению различий среди подэмоций. Теле/кинотексты насыщены эмоциями. Многие из них очень просто определить, но иные подэмоции ощутить труднее. Действительно ли вы были способны ощутить и понять более сложные эмоции? Спо­собны ли вы были увидеть типы эмоций, которые отличают комедии от приключенческих произведений?

Моральный уровень

1. Способны ли вы делать некоторые обобщения о том, на каком уровне развития находится тот или иной медийный персонаж? Если да, то вы можете ясно видеть конкретные примеры и обсуждать ваши выводы, опираясь на них. Тогда вы обладаете моральной грамотно­стью. Ваша моральная грамотность высока, если вы можете пони­мать, как можно изменить сюжеты медиатекстов, чтобы заинтересо­вать аудиторию различных типов медиавосприятия.
2. Возможные опасности, с которыми сопряжен доступ детей к сети интернет (информация для педагогов):
* Неприемлемые материалы. В интернете ребенок может столк­нуться с материалами, связанными с сексом, провоцирующими воз­никновение ненависти к кому-либо или побуждающими к соверше­нию опасных либо незаконных действий.
* Неприятности, связанные с нарушением законов или финансо­выми потерями. У ребенка могут обманным путем узнать номер ва­шей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что, в конечном счете, приведет к возникновению у вашей семьи проблем, связанных с нарушением законов.
* Разглашение конфиденциальной информации. Детей и даже под­ростков могут уговорить сообщить конфиденциальную информацию.

Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол и информация о семье, могут легко стать извест­ными злоумышленнику. Даже если сведения о вашем ребенке запра­шивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации.

* Проблемы технологического характера. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузи­вшего с веб-узла небезопасный код, в компьютер может попасть ви­рус, «червь», «троянский конь», «зомби» или другой код, разработан­ный со злым умыслом.

Вывод: не спешите доверять любым предложениям в Сети.

Использовать один простой пароль для электронной почты, ICQ или своих аккаунтов в социальных сетях - то же, что ключом от поч­тового ящика закрывать входную дверь. Оставляя много личной ин­формации в сети, вы рискуете сделать свои персональные данные до­ступными мошенникам, которые с их помощью могут от вашего име­ни рассылать электронные письма, вести ICQ-общение, совершать те­лефонные звонки или, проникнув в ваш компьютер, уничтожить цен­ные данные.

Выводы:

* Ограничьте объем информации о себе, находящейся в публичном доступе.
* Используйте только сложные пароли.
* Для разных учетных записей и сервисов используйте разные па­роли.
* Не передавайте свои логин и пароль третьим лицам