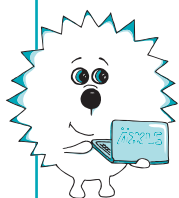


Современные дети и подростки легко осваивают компьютер, мобильные устройства и умело пользуются ими. При этом их навыки в области безопасности отстают от способности осваивать новые приложения. Если вовремя объяснить подросткам правила поведения в Интернете, это уберезет их от мошенников, травли и других проблем. Одна из форм работы, которая вам поможет выстроить диалог об информационной безопасности в Сети, – психологическая мастерская.



Безопасность в социальной сети: психологические мастерские для подростков

И.С. Адмиральская,

психолог, специалист по семейному
консультированию

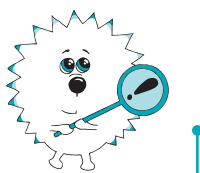
Разговаривая с подростками о безопасности в Сети, родители придерживаются одной тактики – напугать и выдать список запретов. В таком контексте дети не готовы слышать и слушать, потому что у них «включаются» типичные для этого возраста реакции отрицания и обесценивания родительской тревоги.

Психологическая мастерская – это формат групповых встреч, в ходе которых участники интенсивно погружаются в выбранную тему, разрешают какую-либо проблемную ситуацию, исследуют себя в этой ситуации.

Такой формат встреч предоставляет учащимся возможность **выработать собственные способы безопасного пребывания в Сети**. В ходе мастерской вы не даете подросткам готовые



решения или рекомендации. Ваша задача – рассказать о существующих ловушках сетевого пространства, возможных видах мошенничества и противоправного поведения пользователей, привести реальные примеры, а затем предложить учащимся самим выработать защитные стратегии, которые им действительно подойдут.



Внимание

Как показывает практика, если человек принял участие в выработке решения, он с большей готовностью будет приводить его в жизнь.

Предлагаемые далее психологические мастерские охватывают разные стороны сетевого присутствия человека: правила безопасности, связь между активностью/популярностью и отношением человека, социальная сеть как инструмент агрессии и преследования (приложения 1–3).

Алгоритм проведения мастерской:

1. Задание учащимся. Предложите для обсуждения вопрос или проблему. Задача участников – обменяться мнениями, прояснить собственные позиции относительно заданной темы, сделать выводы.

2. Информационный блок. Предложите учащимся дополнительную информацию по теме.

3. Финальная дискуссия. Зафиксируйте на доске все выводы и заключения.

При проведении психологической мастерской помните, что подростки прекрасно справляются с формулировкой выводов и решений проблемных ситуаций без подсказок со стороны. Более того, тот факт, что взрослый доверяет самостоятельно спроектировать стратегии безопасности, позволяет им с большим интересом и ответственностью подойти к этой задаче.

Подростки очень признательны, когда взрослые принимают их всерьез и признают их право на самостоятельность, на пробы и ошибки. В рамках мастерских у них есть возможность потренировать эту самостоятельность и ответственность, поэтому не пользуйтесь готовыми решениями, приведенными ниже в качестве примеров. Предоставьте учащимся самостоятельно сформулировать свои идеи и выводы, которые наверняка окажутся более точными, актуальными и работающими.





Приложение 1

Мастерская «Основы безопасности в социальной сети»

Цель: сформировать у подростков представление о разнице между частным и общим в социальной сети, о присутствии в этом анонимном пространстве криминального интереса и о различных механизмах влияния на поведение пользователя.

Материалы и оборудование: бумага, ручки, экран, проектор.

Примечание. Пригласите к участию в мастерской учителя информатики – он может продемонстрировать на примерах конкретные техники мошенничества в социальных сетях.

Ход мастерской

Во многих сетях можно управлять видимостью/невидимостью записей и ограничивать к ним доступ (для всех, для избранной группы лиц). Насколько эти меры безопасности надежны и как защитить личную информацию от внимания тех, для кого она не предназначена?

1. Задание учащимся

Разделите класс на группы по три-четыре человека и дайте инструкцию: «Если бы вы вели урок для учащихся 2-го класса, посвященный поведению в социальной сети, какие правила вы с ними обсудили бы? Выпишите эти правила и обоснуйте их».

Примеры правил поведения в социальной сети

- 1) Никогда не публикуйте номер школы, в которой вы учитесь, свой домашний адрес, фотографии школы, номер своего телефона.
- 2) Не соглашайтесь на встречи с незнакомыми людьми, даже если они предлагают вам подарок или сводить вас в кино, в ресторан быстрого питания.
- 3) Не рассказывайте, как зовут ваших родителей, где они работают и во сколько возвращаются домой после работы.
- 4) Не сообщайте, когда вы находитесь дома одни.
- 5) Не рассказывайте, когда вы собираетесь уехать с родителями из дома на долгий период и т. д.
- 6) Не нажимайте на ссылки, которые вам прислали незнакомые люди.



2. Информационный блок

Существует много способов воспользоваться доверием пользователя в социальной сети. В своем исследовании К. Вонг с коллегами описал пять из них. Некоторые из этих способов требуют специальных знаний и умений, а некоторые доступны даже «дикому» в отношении техники аферисту.

Установка приложений, требующих доступа к персональным данным. Ваш профиль, фотографии и даже то, что вы обычно лайкаете, – источник ценной персональной информации, которая практически никак не защищена. Как только вы открываете доступ какому-нибудь приложению к своим личным данным, эта хрупкая защита падает. Конкретные люди, стоящие за данной программой, могут использовать ваши данные в своих целях.

Обычно для того, чтобы поиграть в какую-нибудь игру в социальной сети или пройти забавный тест, нужно нажать кнопку «установить», под которой часто уже стоит галочка или предупреждение о том, что приложение получит доступ к спискам друзей, личной информации, адресу электронной почты, альбомам. Кроме этого, входя на какой-нибудь сайт через аккаунт в социальной сети, мы вбиваем в специальные окошки на этом сайте свой пароль от этой сети. Дальше все довольно просто – у злоумышленника есть все ключи к вашему профилю (и к профилям тысяч других людей), и он в зависимости от целей может ими распоряжаться по своему усмотрению.

Рассылка спама. Любой из пользователей сети может послать вам сообщение, отметить вас на фотографии или пригласить в группу. В сообщении, посте с фотографией или в материалах группы могут содержаться ссылки на вредоносные программы, которые незаметно «утаскивают» у вас то, на что их запрограммировал создатель. Чаще всего это ваши логин-пароль, данные пластиковых карт, которые хранятся в системе, если вы (или ваши родители) когда-нибудь оплачивали что-то через Интернет с помощью карт. Эта задача требует всего лишь двух шагов – сформировать у вас доверие к тому, от кого прилетит «троянский конь», и убедить вас кликнуть на ссылку.

Фальшивые аккаунты. Пользуясь брешью в безопасности любой социальной сети можно создать в ней аккаунт, используя личные данные и фотографию любого реально существующего человека. Например, бразильский специалист по вопросам компьютерной безопасности Нельсон Нето доказал, что в течение 24 часов можно стать другом любого активного пользователя сети Facebook. В ходе эксперимента он выбрал жертву и создал фальшивый аккаунт, используя фотографию и фамилию ее начальника. Сначала Нельсон отправил запросы на дружбу друзьям друзей этого начальника, затем непосредственно его друзьям, а затем и жертве. Минимальное время, которое потребуется на подобную многоходовую операцию – 7,5 часа. Дальше полученную информацию злоумышленник может использовать по своему усмотрению – например, в ходе расследования дела о похищении сына Евгения Касперского было доказано, что преступники узнали маршруты его передвижений на странице в социальной сети.

Вход на сайты через профиль в социальной сети. Этот способ получения доступа к вашей личной информации также активно используется злоумышленниками. Вы хотите почитать или посмотреть что-нибудь интересное, смешное или про котиков и решаете



экономить время на создании логина и пароля, и «светите» данные своего аккаунта в очередном неизвестном месте.

Ботнеты – сеть компьютеров с запущенными на них ботами – программами, которые направляют на компьютер жертвы без ее ведома и дают злоумышленнику возможность выполнять некие действия с использованием ресурсов зараженного компьютера. Эти программы также могут предоставлять доступ к личным данным и данным кредитных карт, а также публиковать от вашего имени в социальных сетях «зараженные» вирусами личные сообщения и посты.

Наше поведение в социальных сетях также подвержено влиянию различных условий, как и поведение в реальной жизни. Эти условия активно изучаются и описываются – не только учеными, но и специалистами, так или иначе заинтересованными в том, чтобы повлиять на ваше поведение – социальными инженерами.



Социальная инженерия – технология управления поведением человека без использования технических средств. Основана на использовании человеческих слабостей. Одни из самых известных социальных инженеров – Кевин Митник, братья Бадир и человек, скрывающийся под ником Архангел. Братья Бодир сказали в интервью: «Полностью от сетевых атак застрахован лишь тот, кто не пользуется телефоном, электричеством и ноутбуком».

Один из простых феноменов называется **эффект взаимности** – если кто-то поставил лайк под моей фотографией или постом, я чувствую необходимость «лайкнуть» его контент, чтобы сохранять баланс между «брать» и «давать». В рамках социальной инженерии этим эффектом пользуются для того, чтобы лавинообразно увеличить список друзей и сформировать узнаваемость профиля. За узнаваемостью следует доверие. От лица популярного пользователя с большим кредитом доверия можно транслировать разные идеи, что-то продавать, на кого-то влиять и получить доступ к каким-то ценным или эксклюзивным ресурсам, частной информации.

Основатель компании Fueled Рамит Чавла в рамках социального эксперимента создал специальное приложение, которое ставило от лица пользователя лайки в социальных сетях. За этими лайками следовали ответные лайки. И если бы социальные сети не запретили это приложение, никто из пользователей не мог бы отличить, кто ставит лайк его посту – программа или живой человек.

3. Финальная дискуссия

Предложите учащимся распознать действие технологий социальной инженерии, подобных эффекту взаимности.



Комментарий для педагога-психолога. Есть еще эффект «дружбы» в социальной сети, когда к человеку, который ставит вам лайки, формируется ничем не обоснованное доверие. Большее доверие к человеку, у которого много виртуальных друзей, чем к человеку, у которого их почти нет. Убеждение, что человек, с которым у вас много общих друзей, похож на вас и т. д. Ощущение, что человек кажется вам близко знакомым, формируемое на основе информации из его частной жизни, которой он делится с посетителями своей страницы. Формирование мнения о человеке на основе его страницы без учета того, что то, чем он делится с читателями, может не соответствовать истине или быть выборочным содержанием его жизни (только веселое, приятное и симпатичное, например).

В ходе данной психологической мастерской помогите учащимся прийти к выводу об иллюзорности тех представлений о других людях, которые можно составить на основе их профилей.



Приложение 2

Мастерская «Мой имидж в социальной сети»

Цель: сформировать у учащихся представление о том, как жизнь их сетевого аватара может отражаться на реальной жизни и каким образом можно управлять этим влиянием.

Материалы и оборудование: бумага, ручки, экран, проектор.

Ход мастерской

Как мы чувствуем себя, когда наш пост никто не лайкнул? Что происходит с нами, когда мы наблюдаем, как кто-то другой в социальной сети выкладывает фото с любимым человеком, прекрасными видами, нарядной одеждой, группой друзей? Насколько нам важно быть популярными в социальной сети?

1. Задание учащимся

Объедините участников в группы по четыре-пять человек и предложите обсудить разные стратегии сетевого присутствия, например: кто-то постит только котиков, кто-то любит публиковать селфи, кто-то делится впечатлениями от фильмов и т. д. Предложите подросткам собрать коллекцию способов ведения аккаунта – от «любителей котиков и селфи» до «молчаливо лайкающих чужие фото».



2. Информационный блок

Осенью 2016 года маркетолог Роман Зарипов «придумал» миллионера Бориса Борка: инвестировал в этот проект около 50 тыс. руб., Роман превратил случайно выбранного пенсионера в звезду социальных сетей. Он продемонстрировал пользователям сценки из его жизни в дорогих интерьерах с участием красивых девушек на фоне автомобилей представительского класса. Аккаунт Бориса лавинообразно оброс друзьями, после чего Роман Зарипов объявил о мистификации.

Этот случай не может наводить на мысли о том, сколько Борисов Борков окружает нас в действительности и не делаем ли мы из собственного аккаунта что-то подобное для получения лайков и восхищений, для питания своей самооценки. Мы сами выбираем, чем делиться в сети и что продемонстрировать. Сколько людей делают из своего аккаунта собственного дубля, который более удачлив, отлично проводит время, любим, успешен? И как они справляются с той пропастью, которая разделяет их сетевого двойника и реальную личность?

Исследование, выполненное под эгидой Национального института психического здоровья (США) показало, что **чем больше времени человек проводит в социальных сетях, тем выше риск развития у него депрессии**. Можно предположить, что в группе риска оказываются одинокие люди. В те моменты, когда социальные сети наполняются свидетельством чужого веселья (например, в новогодние каникулы), они оказываются особенно незащищены. Кроме этого, в зоне риска – подростки, поскольку именно в этом возрасте мнение сверстников становится очень важным, а социальная сеть – это территория легко высказываемых мнений. **Совет.** Найдите и покажите учащимся короткую социальную рекламу, демонстрирующую последствия создания в социальной сети неправдоподобной истории о себе.

3. Финальная дискуссия

Предложите учащимся обсудить вопрос: «Как сделать свое присутствие в социальной сети эмоционально безопасным и “отстегнуть” от него самооценку?».



Приложение 3

Мастерская «Анонимность в социальных сетях»

Цель мастерской: сформировать у подростков понимание того, какие возможности и опасности кроются за анонимным присутствием в социальной сети (т. е. не под своими именем и фамилией) и в каких случаях эта анонимность полезна, а в каких – небезопасна.

Материалы и оборудование: бумага, ручки, экран, проектор.



Ход мастерской

Анонимность в социальных сетях – это возможность поставить на аватар чужую фотографию или картинку, создать сразу несколько профилей с разными псевдонимами, использовать чужое изображение и личные данные при создании своей странички. В некоторых виртуальных пространствах это возможность анонимно комментировать чужие записи. Так, в любой социальной сети вы найдете десятки страниц якобы принадлежащих известным певцам или актерам, в реальности не имеющим отношения к этим публичным персонам.

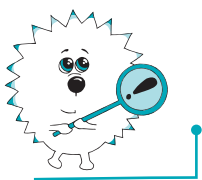
1. Задание учащимся

Разделите класс на несколько групп по три-четыре человека. Одним группам дайте задание описать плюсы и возможности анонимности в социальных сетях, другим – описать минусы и опасности анонимности в социальных сетях. И тех и других попросите привести примеры и обосновать их.

Комментарий для педагога-психолога. Например, среди плюсов может быть возможность просто общаться, не задумываясь о том, что и почему о тебе (реальном) подумают. Среди минусов – страх, что другие анонимные пользователи могут свободно выражать агрессию в твой адрес.

2. Информационный блок

Анонимность в социальной сети расширяет границы дозволенного и создает иллюзию, что действуете не вы, а некто другой (ваш аватар) – а партнер по общению тоже не совсем настоящий человек, а просто картинка на экране вашего смартфона. В этой ситуации дегуманизации намного легче написать что-то обидное, агрессивное или оскорбляющее другого.



Внимание

Сетевая анонимность становится питательной средой для кибербуллинга – травли, унижения, преследования со стороны группы, где в качестве инструментов выступают социальные сети и электронная почта.

О кибербуллинге начали серьезно говорить после того, как в 2008 году в Японии прокатилась волна подростковых самоубийств, так или иначе связанных с угрозами, шантажом и дезинформацией в электронных средствах связи. Ученики рассылали друг другу, педагогам и родителям сообщения с фальшивых аккаунтов, взламывали телефоны друг друга и размещали в открытом доступе фото интимного характера и т. д.

В России в социальных сетях школьниками создаются специальные группы, в которых класс высмеивает конкретного одноклассника – размещает видео и фото с его участием, снимает на камеру и затем распространяет сцены издевательств и т. д. Кроме этого, электронные



средства связи используются для прямых атак – рассылки сообщений с угрозами и текстом унижающего содержания, звонков.

Кроме кибербуллинга, анонимность в социальных сетях дает возможность злоумышленникам пользоваться доверием пользователей, выдавая себя за других людей – учеников соседней школы, например. Имея аккаунт с симпатичной фотографией и более-менее реалистичной информацией, можно за несколько недель выстроить прочный контакт практически с любым подростком и потом воспользоваться его доверием. Важно понимать, где пролегает грань между предьявленностью и анонимностью, и каковы этические ограничения поведения в социальных сетях.

3. Финальная дискуссия

Предложите учащимся выработать правила, касающиеся собственной анонимности и взаимодействия с чужой анонимностью.

Например, одно из важных правил, касающихся анонимности, – запрет на публичное сообщение другому человеку о том, кто «стоит» за анонимным аватаром, если вам стала известна его личность.

Другое правило – действовать в сети так, как если бы вам персонально пришлось отвечать за последствия своих слов. Помните о том, что по ту сторону экрана сидит живой человек, которому может быть обидно, грустно, одиноко.

Глоссарий

Аватар (от англ. *Avatar*, просторечное – áва, аватáрка) – визуальное представление пользователя в интернет-среде. Термин пришел из традиции индуизма, где обозначает проявление снизошедшего в материальный мир Бога. Поскольку проявление есть отображение не целого, но лишь его части, аватар пользователя также служит для отображения некоей части его Я.

Аккаунт – учетная запись посетителя той или иной веб-страницы, позволяющая гостю перейти в статус зарегистрированного пользователя. Сегодня невозможно присоединиться ни к одной социальной сети, не имея там аккаунта.

Блог (англ. *blog*, от *web log* – интернет-журнал событий, интернет-дневник, онлайн-дневник) – веб-сайт, основное содержимое которого регулярно добавляемые записи, содержащие не только текст, но и изображения или мультимедиа. Для блогов характерны недлинные записи, упорядоченные в обратном хронологическом порядке (последняя



запись сверху). Термин «блог» был придуман Йорном Баргером 17 декабря 1997 года. Людей, ведущих блог, называют блогерами. Совокупность всех блогов Сети принято называть блогосферой.

Ботнет – компьютерная сеть, состоящая из некоторого количества хостов (компьютеров, серверов, подключенных к локальной или глобальной сети) с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета – это программа, скрытно устанавливаемая на устройство жертвы и позволяющая злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Ботнеты обычно используются для нелегальной или неодобряемой деятельности.

Бот (сокращение от слова «робот») – специальная программа, функция которой – имитация действий живого человека.

Лайк (от англ. *Like* – «нравится», «одобряю») – условное выражение одобрения материалу, пользователю, фотографии, выполняемое нажатием одной кнопки (отсюда «лайкнуть» – одобрить, поддержать).

Логин (англ. *login, login name, username – user* «пользователь, жарг. юзер» + *name* «имя») – имя (идентификатор) учетной записи пользователя в компьютерной системе.

Никнейм, или ник (англ. *Nickname* – первоначально «кличка, прозвище», от средне-английского *an eke name* – «другое имя», перешедшее в одинаково звучащее *a nick name*) – сетевое имя, псевдоним, используемый пользователем в Интернете, обычно в местах общения (в блогах, на форумах, в чатах).

Профиль (или профайл) – то же, что и аккаунт, учетная запись. Личная страничка, где пользователь размещает о себе различную информацию, выкладывает видео, аудио и другие материалы. Управлять страницей можно после того, как пройдена процедура авторизации – введен логин и пароль.

Социальная сеть – бесплатная площадка в Интернете, где можно самостоятельно публиковать какую-то информацию и обмениваться ею с другими людьми.

Спам – автоматизированные массовые рассылки корреспонденции рекламного характера. В отличие от простой рекламы такая рассылка не имеет целевой аудитории – ее шлют огромному количеству людей без конкретной цели: просто надеясь на то, что какая-то небольшая часть адресатов заинтересуется предложением.



Сценарий родительского собрания «Медиабезопасность школьника»

Цель медиаобразования – защитить учеников от противоправного и манипулятивного воздействия СМИ и интернета. Предлагаем провести родительское собрание в форме интерактивной игры.

Обсудите с родителями опасные ситуации, в которые могут попасть дети, и способы выхода из них. Так вы сможете предупредить криминальные посягательства на учащихся не только в интернете, но и на улице.



ВАЖНАЯ ИНФОРМАЦИЯ

Участники	Родители учеников 6–8-х классов
Цель	Формировать ответственное отношение родителей к деятельности детей в медиапространстве
Задачи	Познакомить родителей с положениями Федерального закона от 21.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Рассказать о распространенных в медиапространстве манипуляционных приемах и научить им противостоять
Материалы и оборудование	Доска, мультимедийный проектор или вопросы для игры в распечатанном виде
Примерное время	40 минут

40 мин 

Ход родительского собрания

Допматериалы 

Вопросы и ответы для игры на **с. 4**.

Ведущий: Добрый день, уважаемые родители! Тема нашей встречи – медиабезопасность. Мы поговорим о том, как защитить наших детей от информации, которая может причинить им вред.

Вы знаете, как классифицируют информационную продукцию для детей?

Родители: Классифицируют информационную продукцию по категориям. Она бывает для детей:

- до шести лет и обозначается 0+;
- шести лет (6+);
- двенадцати лет (12+);
- шестнадцати лет (16+).

Информационную продукцию, которая запрещена для детей, обозначают 18+ или сопровождают текстом «запрещено для детей».

Какую информацию нельзя распространять среди детей?

Родители: Среди детей запрещено распространять информацию, которая:

- побуждает к действиям, которые угрожают их жизни и (или) здоровью, в том числе к самоубийству;
- вызывает желание попробовать наркотики, психотропные и одурманивающие вещества, сигареты, алкоголь, играть в азартные игры, заниматься проституцией, бродяжничеством или попрошайничеством;
- оправдывает насилие и жестокость, провоцирует насилие по отношению к людям или животным;
- отрицает семейные ценности, пропагандирует нетрадиционные сексуальные отношения и формирует неуважение к родителям и другим членам семьи;
- оправдывает противоправное поведение;
- содержит нецензурную брань или порнографию;
- раскрывает сведения о несовершеннолетнем, который пострадал в результате противоправных действий или бездействия.

Ведущий: Уважаемые родители, предлагаю вам сыграть в игру – аналог телевизионной передачи «Своя игра». Для игры вам необходимо разделиться на команды.

Участники делятся на команды по 8–10 человек.

Ведущий: В игре три номинации:

1. «Дети и Интернет» – вопросы, которые связаны с поведением детей в Интернете. Вопросы этой номинации помогут нам понять, как помочь ребенку.

2. «Жизненные ситуации» – ситуации, с которыми сталкиваются дети в Интернете и на улице. Ваша задача – предложить решения.

3. «Блицвопросы» – вопросы на быстроту реакции. Ваша задача – дать краткий и аргументированный ответ по проблеме.

В каждой номинации четыре вопроса разной категории сложности и стоимости – от 100 до 400 баллов.

Команды по очереди выбирают номинацию и уровень вопроса. На обдумывание – 2 минуты. После того как команда ответит, могут высказаться остальные участники. Когда все варианты будут озвучены, я назову правильный ответ. Выигрывает команда, которая заработает большее количество баллов.

Команды по очереди выбирают номинацию, вопрос и отвечают.

В конце игры ведущий подводит итоги, награждает команду победителей, предлагает родителям, у которых возникли вопросы по теме собрания, побеседовать индивидуально.

Светлана ПРОХОРОВА, канд. пед. наук, доцент, научный руководитель
МОУ «Салмановская средняя общеобразовательная школа»

Таисия СЕРКОВА, заместитель директора по научно-методической работе
МОУ «Салмановская средняя общеобразовательная школа»

Номинация «Дети и интернет»

100 баллов

Вопрос: Как отследить, какие сайты посещает ребенок в ваше отсутствие?

Ответ: Посмотреть историю браузера. Если история удалена, сделать звонок провайдеру и попросить распечатку всех сайтов с учетом потраченного трафика. Установить специальную программу родительского контроля.

200 баллов

Вопрос: Как выявить признаки интернет-зависимости у ребенка?

Ответ: Если поведение не изменилось, успеваемость в школе не ухудшилась, настроение и самочувствие хорошее – причин для тревоги, скорее всего, нет. Стоит беспокоиться, если ребенок:

- проводит за компьютером больше времени, чем прежде;
- предпочитает виртуальное общение реальному (пропускает школу, перестал выходить гулять);
- плохо спит и ест;
- склонен к частым перепадам настроения, неадекватно (агрессивно) реагирует на просьбу выключить компьютер;
- тревожен, угнетен при невозможности быть онлайн, постоянно вспоминает о делах в сети;
- неохотно рассказывает или скрывает, чем занят в сети (что ищет, во что играет).

300 баллов

Вопрос: Как справиться с интернет-зависимостью?

Ответ: Создать дома теплую и дружескую атмосферу, чтобы дети не убегали в виртуальную реальность за поддержкой и общением. Проводить с ребенком больше времени. Не перекладывать роль воспитателя на телевизор и компьютер. Ограничить время пребывания за монитором (и быть в этом примером). Быть твердым, если ребенок выпрашивает лишний час, чтобы посидеть в сети. Чаще хвалить за любые достижения в реальной жизни. Увлечь активным видом спорта. Если решить проблему компьютерной зависимости своими силами не получается, обратиться за помощью к психологу.

400 баллов

Вопрос: Что делать, если ребенок увидел в интернете неуместные материалы?

Ответ: Не реагировать слишком остро: ребенок не должен чувствовать излишнего смущения, чтобы он мог свободно говорить о подобных случаях в будущем. Акцентировать внимание школьника на том, что это не его вина. Удалить все следы от материала: ссылки из кеш-памяти, файлы cookie и журнал просмотренных веб-страниц. Поговорить с ребенком о том, как избежать подобных ситуаций в будущем.

Номинация «Жизненные ситуации»

100 баллов

Ситуация: Вы получили на электронную почту письмо: «Дорогой друг! Я миссис Сесе-секо, вдова бывшего президента Заира Мобуту Сесе-секо. Я вынуждена написать Вам в связи с обстоятельствами. Я вместе со своим мужем и двумя сыновьями Альфредом и Башером переехали в Марокко, где мой муж умер от рака. У меня есть банковский счет на сумму 18 000 000 долларов. Мне нужно ваше желание помочь нам – чтобы вы получили эти деньги для нас. Я представлю Вас моему сыну Альфреду, который имеет право получить их. Я хочу инвестировать эти деньги, но не хочу, чтобы было известно, что это делаю я. Мне хочется приобрести недвижимость и акции транснациональных компаний, а также вложиться в надежные и неспекулятивные дела, которые Вы посоветуете. Искренне Ваша, миссис Мариам М. Сесе-секо».

Вопрос: Как действовать?

Ответ: Игнорировать такие письма. Это пример так называемого нигерийского письма. Этот вид мошенничества был распространен в Нигерии, отсюда и название. Как правило, мошенники просят у получателя письма помощи в многомиллионных денежных операциях, при этом обещают солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманивают все более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам и тому подобное.

200 баллов

Ситуация: В 2 часа ночи ваш сын (дочь) получил(а) СМС: «Брось 50 рублей на номер 89063838665. Очень надо. Позже объясню. Санек (Натка)».

Вопросы: Что вы посоветуете ребенку? Какие признаки манипуляции использованы?

Ответ:

1. Ни в коем случае не отправлять деньги. Это обман.
2. Рассылка (обычно массовая) – кто-нибудь, да попадется. Для подписи использовано распространенное имя. Подчеркнуто личное обращение – как будто от близкого знакомого. Запрашиваемая сумма небольшая – проще отдать, чем проверить. Расчет на усталость и снижение бдительности в 2 часа ночи.

300 баллов

Ситуация: Ваня решил зарегистрироваться в онлайн-игре. Для регистрации он сообщил адрес личной электронной почты, на которую должна прийти ссылка. Через несколько минут Ваня получил электронное письмо с оскорблениями.

Вопрос: Что делать?

Ответ: Объяснить, что не следует отвечать на подобные сообщения, особенно от незнакомых людей. Если оскорбления не прекращаются, изменить адрес электронной почты ребенка.

Настроить параметры работы с почтой так, чтобы сообщения от нежелательного адресата поступали в отдельную папку.

Если адрес отправителя неизвестен – отправить копию его сообщения поставщику услуг интернета и попросить удалить этот адрес электронной почты.

400 баллов

Ситуация: Катя прибежала с улицы и рассказала, что к ней подошла гадалка и предложила погадать. Девочка отказалась. Тогда гадалка сказала, что девочка не узнает, что случится с ее мамой. Вопрос: О чем поговорить с девочкой? Ответ: Рассказать о манипуляционных элементах, которые использовала гадалка:

- скрыла настоящую цель воздействия. Ни один манипулятор не скажет, чего он от вас хочет на самом деле;
- выделила социальную роль и оказала направленное воздействие. Все имеют роли: мать, дочь, бабушка. Манипулятор использует их, чтобы усилить воздействие на человека;
- драматизировала ситуацию. Чтобы заставить сомневаться, человека пугают последствиями;
- сделала акцент на реальную потребность (иметь маму). Страх за близкого отвлекает от опасности, которая грозит человеку.

Номинация «Блицвопросы»

100 баллов

Вопрос: Следует ли запрещать детям Интернет?

Ответ: Нет, запретный плод – сладок. Ребенок найдет способ пользоваться сетью. Лучше, чтобы взрослые были союзниками, а не врагами.

200 баллов

Вопрос: Как ограничить доступ детей к запрещенным сайтам?

Ответ: Установить на компьютер специальную программу, которая также позволит определить, сколько времени ребенок провел в сети. Использовать встроенные средства родительского контроля, которые блокируют опасные сайты, программы, игры.

300 баллов

Вопрос: Полезно ли детям показывать советские мультфильмы?

Ответ: Да. В них нет насилия, каждый из них учит важным ценностям: дружбе, уважению, любви.

400 баллов

Вопрос: Вы узнали, что ребенок попал в секту. Что делать?

Ответ: Не пытаться активно разубеждать новообращенного сектанта – это испортит отношения. Постараться сохранить доверительные отношения. Получить консультацию у психолога. Немедленно обратиться в правоохранительные органы, обратиться за помощью в школу.