Методические рекомендации
по проведению единого информационного часа
для учащихся VII–XI классов учреждений общего среднего образования

Тема «Мы в интернет-пространстве: как защититься от манипуляций».

Инициативная группа учащихся может заранее подготовить мультимедийную презентацию, используя информационные материалы (приложение). Можно воспользоваться мультимедийной презентацией, подготовленной Национальным институтом образования.

Указанные материалы размещены на национальном образовательном портале: *http://www.adu.by / Главная / Образовательный процесс. 2022/2023 учебный год / Организация воспитания*.

Информационный час может проводить учитель обществоведения, педагог-психолог, педагог социальный, классный руководитель.

В качестве информационной основы рекомендуется использовать:

учебные издания:

Актуальные вопросы обеспечения информационной безопасности: пособие для педагогов учреждений образования, реализующих образовательные программы общего среднего образования / В.А. Арчаков [и др.]. – Минск: Национальный институт образования, 2021. – 168 с.: ил.;

Обществоведение: учебное пособие для 9 кл. учреждений общ. сред. образования с рус. яз. обучения / А.Н. Данилов [и др.]; под ред. А.Н. Данилова. – Минск: изд. «Адукацыя і выхаванне», 2019. – 225 с.: ил.;

Обществоведение: учебное пособие для 10 кл. учреждений общ. сред. образования с рус. яз. обучения / А.Н. Данилов [и др.]; под ред. А.Н. Данилова. – Минск: изд. «Адукацыя і выхаванне», 2020. – 240 с.: ил.;

Обществоведение: учебное пособие для 11 кл. учреждений общ. сред. образования с рус. яз. обучения / О.И. Чуприс [и др.] – Минск: изд. «Адукацыя і выхаванне», 2021. – 256 с.: ил.

Видеоролик: Кибербуллинг: как избежать травли в интернете – проект МТС Беларусь о кибербезопасности «Дети в интернете»: https://www.youtube.com/watch?v=-MTOE_wFPGM;

Видеоролик: Правила общения с незнакомцами в интернете – проект МТС Беларусь о кибербезопасности «Дети в интернете»: https://www.youtube.com/watch?v=x4dz6OC7V9s

«МЫ УЗНАЁМ»

Ведущий знакомит с содержанием информационных блоков (см. информационные материалы в приложении):

«Какие опасности подстерегают нас в интернете»;

«Манипулирование в интернете: вовлечение в деструктивные группы»;

«Методы защиты от манипулирования».

«МЫ РАЗМЫШЛЯЕМ»

Ведущий организует обсуждение информации, полученной в разделе «МЫ УЗНАЁМ».

Блок «Какие опасности подстерегают нас в интернете».

В XXI веке интернет-пространство становится важной средой виртуальной жизни и мощным средством социализации детей и молодежи – активных пользователей сетевых ресурсов. С одной стороны, интернет – это неиссякаемый источник информации, который помогает познавать мир и развиваться. Но наряду с положительными сторонами есть и негативные. Под воздействием интернета изменяются ценностные ориентации, духовно-нравственные приоритеты, трансформируется мировоззрение. Чрезмерно интенсивное взаимодействие с интернет-ресурсами связано с развитием ряда психологических расстройств (депрессивные состояния, тревога, агрессивность и т. д.). Но наиболее серьезной проблемой является негативное информационное влияние деструктивного контента на личностное развитие молодых людей, манипулирование их сознанием и поведением.

В Беларуси за распространение негативного контента владельцы сайтов, а также авторы электронных текстов и видеопродукции могут быть привлечены к административной и уголовной ответственности.

Предоставляется слово представителю органов внутренних дел.

Вопросы для обсуждения:

XXI век считается веком информации. Не так давно телевизор, компьютер и телефон были предметом роскоши. Сейчас подростки разбираются в технических средствах коммуникации лучше взрослых. Какие же проблемы появляются в связи со стремительным развитием средств массовой информации и коммуникации?

За последние годы информационное пространство кардинальным образом изменилось. Ведущую роль стал играть интернет, который выступает основным каналом для получения новостей и пространством для общения, особенно для подрастающего поколения. В связи с этим что бы вы посоветовали друг другу? Как можно использовать интернет с пользой для себя?

Социальные сети стали массовым явлением. Они в значительной степени формируют общественное мнение по различным вопросам. Многие люди имеют аккаунты в социальных сетях не потому, что им это необходимо, а потому, что это модно. Как вам кажется, какую роль играют социальные сети в жизни каждого человека и в жизни общества?

Насколько актуальна для нашего времени проблема медиабезопасности?

Знакомы ли вам такие понятия, как *кибербуллинг* и *буллинг*, *кибермошенничество*, *опасный контент*? Что они означают? Как можно противостоять этим угрозам?

Можете ли вы описать какой-нибудь неприятный случай, произошедший с вами или вашими друзьями в интернете?

В фокусе обсуждения: медиапространство, цифровые технологии, ценностные ориентации, духовно-нравственные приоритеты, информационные риски, негативный контент, деструктивное воздействие на психику и сознание, манипулирование сознанием и поведением, личная и общественная информационная безопасность, ответственное использование онлайн-технологий; отличие достоверных сведений от недостоверной информации, безопасной информации от вредной; ответственность, активность.

Блок «Манипулирование в интернете: вовлечение в деструктивные группы».

Все больше людей вместо живого общения и активного отдыха предпочитают проводить время за компьютером, смартфоном, погружаясь в виртуальный мир. Некоторые сайты, web-страницы, интернет-сообщества призывают детей и молодых людей входить в разные группы по интересам, увлечениям (музыкальному направлению, творческой деятельности и др.), могут быть посвящены определенному фильму, творчеству музыкального исполнителя, блогера и т.д. Такие группы оказывают положительное влияние, способствуют углублению знаний в определенной сфере, общению с единомышленниками. Но есть такие группы, которые оказывают вредное, негативное влияние. Подобные группы называют деструктивными (опасными, наносящими вред, уничтожающими, разрушающими само общество, его культуру, нарушающими благополучие, права, здоровье граждан).

***Вопросы для обсуждения*:**

Полученное нами из социальных сетей представление о мире и настоящий мир могут не совпадать, то есть социальные сети создают, можно сказать, живую иллюзию, особый мир. Известны ли вам лично случаи, когда кто-то из ваших знакомых пострадал из-за некачественной информации в средствах массовой коммуникации? Как вы думаете, кто чаще всего попадает в такие ситуации? Сформулируйте правила безопасности в социальной сети.

Что такое манипуляция? Какие наиболее распространенные способы манипулирования информацией вы можете назвать?

Вспомните какую-либо недавнюю ситуацию, когда вы после совершения определенного поступка осознали, что кто-то манипулировал вами: объявил вам одну цель, в то время как преследовал другую. Как вы догадались об этом? Как вы думаете, почему с вами так поступили?

Мы живем в информационном обществе, когда потоки информации становятся все больше и нам очень важно понять, как ориентироваться в этой информации, какую информацию считать достоверной, а какую фейком. Можете ли вы привести примеры фейковой информации, находящейся в интернете.

Возможна организация работы в интернете по распознаванию фейковой информации.

Какие признаки говорят о фейковой природе выбранных для примера текстов (иллюстраций)?

Встречались ли вы с проявлениями агрессии в обычной жизни? А в интернете? Какие виды киберагрессии вам знакомы? В какой роли вы с ними сталкивались? Как вам кажется, в чем причины агрессивного поведения в сети?

В фокусе обсуждения: манипулирование в интернет-сети, фейковая информация, защита от недостоверной информации, умение анализировать, сравнивать, обобщать информацию, культура общения в сетевом пространстве, ответственное и безопасное поведение в современной информационной среде, деструктивные группы и их негативное влияние на молодежь, деструктивные формы поведения (агрессия, употребление наркотических средств, терроризм), обесценивание общечеловеческих ценностей.

Информационный блок «Методы защиты от манипулирования».

Манипулирование представляет одну из главных угроз информационно-психологической безопасности, которая существует в интернет-среде. Ключевым умением, которым должен обладать пользователь интернета, чтобы предупредить пагубное воздействие на свое сознание, является способность распознать применение манипуляции.

***Вопросы для обсуждения*:**

По каким признакам можно определить, что тобой манипулируют в интернете?

Какие общие рекомендации для обеспечения безопасности в интернете следует выполнять?

Как можно использовать интернет с пользой для себя?

В фокусе обсуждения: манипулирование как одна из главных угроз информационно-психологической безопасности, осторожность в виртуальном общении, негативное воздействие на чувства и эмоции, обеспечение безопасности в интернете, методы противодействия манипуляции в интернете, умение контролировать и анализировать свои действия, развитие критического мышления, рациональное и эффективное использование интернета.

«МЫ ДЕЙСТВУЕМ»: ведущий подводит итоги.

Мы живём в очень насыщенной информацией среде. За месяц современные медиа производят столько информации, сколько человек XVII в. не получал за всю жизнь. Если в XX в. информация ещё являлась ценностью и её необходимо было уметь добывать, то в XXI в. в первую очередь необходимо уметь фильтровать и ставить барьеры для избыточной информации и фейков (ложной информации). Увеличение объёмов информации привело к потере доверия к ней. Это связано с тем, что в

социальных сетях отсутствует свойственная печатным изданиям проверка информации на достоверность. В результате достоверная информация и фейки стоят в одном ряду и между ними трудно найти отличия.

Современный человек не может отказаться от информации, получаемой через средства массовой информации и коммуникации. Но любую информацию человек должен критически осмысливать и определять, что для него полезно, а что нет, каким примерам следовать, на что не обращать внимания, чему можно подражать, а чему нельзя. Это и есть осознанный выбор человека.

В рамках данного этапа можно:

создать памятку-предупреждение «Как не стать слепым орудием в чужих руках»;

обсудить участие в оформлении странички школьного сайта «Медиабезопасность»; составлении каталога полезных интернет-ресурсов.

Приложение

Информационные материалы
для единого информационного часа для учащихся VII-XI классов
учреждений общего среднего образования
по теме «Мы в интернет-пространстве: как защититься от манипуляций»

Информационный блок «Какие опасности подстерегают нас в интернете».

Интенсивное внедрение цифровых технологий, применение специальных программных средств для продвижения медиапродуктов, создание виртуальных площадок для информирования, взаимодействия и общения пользователей принципиально изменили структуру мирового медиапространства. Печатные и телевизионные СМИ постепенно уступают свои позиции средствам массовой коммуникации в сети Интернет, где любой пользователь может стать участником публичного обсуждения самых разнообразных вопросов.

По мере увеличения роли интернета в жизни общества пользователи сталкиваются со специфическими информационными рисками, связанными с распространением негативного контента (содержания), противоречащего интересам стран, социально-правовым нормам государств, нарушающего права, законные интересы человека и оказывающего деструктивное (разрушающее) воздействие на его психику и общественное сознание.

В XXI веке интернет-пространство становится важной средой виртуальной жизни и мощным средством социализации детей и молодежи – активных пользователей сетевых ресурсов. С одной стороны, интернет – это неисчерпаемый источник информации, который помогает познавать мир и развиваться. Но наряду с положительными сторонами есть и негативные. Под воздействием интернета изменяются ценностные ориентации, духовно-нравственные приоритеты, трансформируется мировоззрение.

Чрезмерно интенсивное взаимодействие с интернет-ресурсами связано с развитием ряда психологических расстройств (депрессивные состояния, тревога, агрессивность и т. д.). Но наиболее серьезной проблемой является негативное информационное влияние деструктивного контента на личностное развитие молодых людей, манипулирование их сознанием и поведением.

Молодежь, особенно 14-18 лет, наиболее подвержена негативной пропаганде, так как является наиболее активным пользователем интернета. Этому возрасту присущи обостренное чувство справедливости, стремление к самовыражению, поиск ценностей и смысла жизни. Молодые люди полны внутреннего протеста, в силу отсутствия жизненного опыта и знаний они подвержены внушению и манипулированию.

Становление и развитие нынешнего молодого поколения происходит под влиянием факторов, повышающих потенциальные риски личной и общественной информационной безопасности. Неуправляемая информационная среда таит в себе возможные политические, экономические и коммуникационные угрозы. Последние, в свою очередь, связаны с межличностными отношениями интернет-пользователей (вовлечение в

преступную деятельность, киберпреследование, кибербуллинг и др.), что вызывает нарастание психоэмоциональной и социально-психологической напряженности в молодежной среде.

Классификация угроз в сети интернет.

Рассмотрим основные угрозы, с которыми могут столкнуться несовершеннолетние.

Контентные (содержательные) риски (негативный контент) – это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы и др.), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, пропаганду анорексии и булимии, самоповреждающего поведения, азартных игр, наркотических веществ, разжигающие расовую ненависть и т. д.).

Законодательство каждой страны предусматривает различные виды наказания за распространение подобной информации. В Беларуси за распространение негативного контента владельцы сайтов, а также авторы электронных текстов и видеопродукции могут быть привлечены к административной и уголовной ответственности.

К запрещенной для распространения среди детей относится информация:

побуждающая к совершению действий, представляющих угрозу жизни и (или) здоровью, в том числе к причинению вреда собственному здоровью;

способная вызвать желание употреблять наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную продукцию, принимать участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

отрицающая традиционные семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

оправдывающая противоправное поведение;

содержащая нецензурную брань;

содержащая информацию порнографического характера.

Неэтичная (искаженная) информация – та, которая противоречит принятым в обществе нормам морали и поведения: нецензурная брань, оскорбления и др. Контент, относящийся к категории неэтичного, также может быть направлен на манипулирование сознанием и действиями различных групп людей.

Столкнуться с негативным контентом учащиеся могут практически везде: на сайтах с полезными материалами, в социальных сетях, блогах, торрентах и видеохостингах. Зачастую подобную информацию можно получить по электронной почте в виде спама или сообщения. Киберпреступники активно пользуются тем, что сегодня в интернете можно найти ответ на любой вопрос, и распространяют свою вредоносную информацию под видом легальных данных.

Коммуникационные риски возникают в процессе общения и межличностного взаимодействия пользователей в интернете. В эту категорию попадают троллинг, буллинг, кибербуллинг (травля, агрессивное преследование

одного человека другим (другими)). С подобными рисками можно столкнуться в чатах, онлайн-мессенджерах (Twitter, Google talk, Skype и др.), социальных сетях, блогах, на сайтах знакомств, форумах.

Электронные (технические) риски определяются возможностями реализации угроз повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушения ее конфиденциальности или хищения персональных данных посредством вредоносных программ (вирусов, «червей», «троянских коней», шпионских программ, ботов и др.). К таким рискам относятся вредоносные программы, кибермошенничество (интернет-мошенничество), спам.

Потребительские риски возникают в результате нарушения экономических и финансовых аспектов взаимодействия в Сети. К ним относят опасность приобретения товара низкого качества, различных подделок, контрафактной и фальсифицированной продукции; потерю денежных средств без приобретения товара или услуги; хищение персональной информации с целью мошенничества.

Потребительские риски тесно связаны со следующими проявлениями:

- мошенничество в интернете:

- фишинг (получение доступа к чужим паролям);
- вишинг (выманивание у обладателя платежной карты конфиденциальной информации);
- фарминг (процедура скрытного перенаправления человека на ложный ip-адрес);
- кликфрод (использование обманных кликов на рекламную ссылку человеком, не заинтересованным в рекламном объявлении);
- «нигерийские письма» (выманивание у получателя письма финансовой помощи посредством обещания солидного вознаграждения).

- мошеннические интернет-магазины и др.

Важной проблемой взаимодействия с различными интернет-ресурсами является *формирование Интернет-зависимости,* которая характеризуется чрезмерным увлечением виртуальной средой и стремлением ухода от реальности. Она сопровождается психофизиологическими изменениями поведения, выраженным дискомфортом при невозможности получить доступ к компьютеру и интернету. Такое состояние приводит к социальной дезадаптации, проблемам с успеваемостью, депрессивным расстройствам.

Информационный блок «Манипулирование в интернете: вовлечение в деструктивные группы».

С каждым годом растет количество случаев, когда малознакомые (незнакомые) люди высказываются в сетях о том, что должен делать, писать, жить, как одеваться и т. д. конкретный человек. Чаще всего такие советы дают медийным персонам (политикам, артистам, блогерам и т. д.). Все это – не что иное, как самая элементарная манипуляция.

Прежде чем начинать работу с информацией в сети интернет, необходимо разобраться, что такое манипуляции.

Манипуляция – способ подчинения, управления людьми путем воздействия на них, программирование их поведения. Часто такое воздействие осуществляется скрытно и ставит своей задачей изменение мнений, побуждений и целей людей в нужном манипулятору направлении. Любой человек может влиять на другого через знания (манипулирование информацией) и чувства (манипулирование эмоциями).

Цель манипуляторов – добиться от людей того поведения, которое им нужно. Манипуляторы не считают других людей личностями, для них не имеет значения неприкосновенность личности, внутреннего мира другого человека.

Манипуляции дают наивысший результат, когда за демонстрируемой открытостью действий скрывается тщательно продуманная, спланированная и замаскированная схема достижения задуманного результата.

Наиболее распространенные способы манипулирования информацией:

- замалчивание фактов, одностороннее изложение сведений;
- дезинформация или создание фейков;
- ссылки на несоответствующие (неточные) источники;
- ссылки на слухи;
- преувеличение, обобщение, сравнение фактов, которые нельзя сравнивать;
- манипулирование статистическими данными;
- ссылка на «авторитетное мнение»;
- отвлечение внимания и др.

Интернет предоставляет нам много информации и, соответственно, поводов для ее обсуждения. При этом наше знание остается достаточно поверхностным. То, что все сведения нельзя перепроверить, является причиной создания фейков, возможностей для информационных искажений.

Фейк (англ. Fake – подделка) – ложная, недостоверная, сфальсифицированная информация об актуальных значимых фактах и событиях с целью ввести в заблуждение. Фейковым может быть контент практически любого вида: новость, изображение, видеоролик и даже страницы в социальных сетях.

Какие основные рекомендации по распознаванию фейков и защите от недостоверной информации дают сегодня практики и ученые? Приведем основные из них.

«Сначала проверь, потом поверь». Одна из главных причин веры в ложь, с которой мы сталкиваемся в Интернете, – это недостаточная критичность по отношению к информации, «интеллектуальная лень» как нежелание информацию проверить.

Исследования по психологии доказывают, что основной способ снизить риск стать жертвой фейковых новостей или недостоверной информации – это привычка к рассудительности. Люди, которые способны анализировать информацию, т. е. меньше доверяют своему первому впечатлению и склонны проверять информацию, не подвержены влиянию громких суждений и эмоциональных высказываний. Поэтому основной метод «борьбы» с фейками – это развитие критического мышления, которое совершенно правомерно относят к числу самых необходимых навыков XXI века и навыков человека будущего.

Все больше людей вместо живого общения и активного отдыха предпочитают проводить много времени за компьютером, телефоном, погружаясь в виртуальный мир. Некоторые сайты, web-страницы, интернет-сообщества могут призывать детей и молодых людей входить в разные группы по интересам, увлечениям (по музыкальному направлению, творческой деятельности (вокалу, рисованию и др.), кулинарии, могут быть посвящены определенному фильму, сериалу, творчеству музыкального исполнителя, актера, блогера и т.д.). Чаще всего такие группы оказывают положительное влияние, способствуют углублению знаний в определенной сфере, организации общения с единомышленниками.

Но среди таких групп можно выделить *группы, которые оказывают вредное, негативное влияние:*

- экстремистские (обучают использованию оружия, нанесению вреда зданиям, сооружениям, технике, в том числе посредством граффити и неуважительных надписей, призывают к убийствам и проведению выступлений протеста, террористических акций);
- религиозно-сектантские (призывают к вступлению в религиозные группы, которые считают себя исключительными, избранными, готовыми лишать жизни себя или других людей, разрушать памятники культуры, сооружения и имущество людей других религиозных взглядов);
- призывающие к причинению вреда собственному здоровью и организму;
- фанатские, нацистские и иные группы, призывающие к шокирующим, агрессивным, разрушительным действиям в отношении материальных объектов, людей других групп и др.

Подобные группы называют *деструктивными* (опасными, наносящими вред, уничтожающими, разрушающими само общество, его культуру, нарушающими благополучие, права, здоровье граждан).

В деструктивных группах происходит изменение норм, правил, привычного поведения. Человек начинает по-другому относиться к другим людям, событиям, своей жизни, не ценит то, что дает общество – право развиваться, учиться, общаться, реализовывать себя с пользой для себя, других людей, своей страны. Попасть под такое негативное влияние можно легко – если человек много читает в сети соответствующую информацию, смотрит видео и фото, участвует в играх, выполнении специальных заданий, общается с членами группы.

Ежедневно в социальных сетях службы информационной безопасности выявляют тысячи сообществ с участием несовершеннолетних, пропагандирующих деструктивные формы поведения (агрессия, употребление наркотических средств, терроризм, причинение себе вреда и прочее).

Подавляющее большинство подростков и молодежи уверены, что лично с ними, никогда ничего плохого в сети интернет не произойдет. Но, к сожалению, они ошибаются, так как подход к каждому человеку подбирается индивидуально.

Вовлечение в деструктивные группы *часто проходит по определенному сценарию.* Предварительно на основе анализа поисковых

запросов определяются потенциальные участники группы (жертвы). На первом этапе с вербовочного (управляющего) аккаунта осуществляется рассылка контактных сообщений, фраз: «привет», «кто ты», «могу я тебе помочь». Далее, если адресат отвечает, то переписка переадресовывается к реальному члену группы («консультанту», «помощнику»), который затем продолжает переписку с потенциальной жертвой.

После установления контакта «помощник» старается стать для новичка «другом», создать для него максимально комфортную и интересную среду, заинтересовать собой, группой, своими знаниями и увлечениями. «Друг» представляет свою выдуманную легенду, причем зачастую он является старшим по возрасту или даже взрослым человеком. Таким образом, создается определенный круг общения, который позволяет подростку почувствовать себя особым, успешным, принятым. Происходит стойкое формирование убеждения, что только в этом круге общения его понимают, принимают, а вне сообщества этого нет и не будет. Также на этом этапе тестируются возможности оказания влияния и управления подростком.

Далее возможно несколько вариантов взаимодействия с новичком.

1. Организаторами сообщества принимается решение о том, что подросток не подходит для сообщества, им сложно руководить, управлять, оказывать на него влияние. В этом случае контакты резко разрываются и подросток удаляется из зоны комфортного общения, подвергается давлению. Это, в конечном итоге, вынуждает его уйти из группы.

2. После проверки подросток может быть перенаправлен (получает приглашение) в основную группу (другой сайт, страница и т.д.), на котором происходит дальнейшая вербовка подростка.

3. Подросток остается на первичном ресурсе (в первичной группе), где происходит погружение подростка в более серьезный (глубокий) контент сообщества (общение на форуме, просмотр видеоматериалов, чтение книг, статей и т.д.). Такое погружение может происходить также посредством сбора группы, «специального» обучения и отработки определенных командных действий. Как правило, с наиболее активными и «перспективными» новичками проводится индивидуальная работа, подготовка к выполнению определенных функций («связной», «координатор», «боец» и т.д.).

В сообществе (группе) формируется активная информационная среда на основе различных интернет-технологий: предлагаются ссылки на сайты деструктивного содержания, специально создаются видеоролики, демотиваторы (демотиватор показывает враждебность общества для группы, конкретного человека, содержит негативный контент), рекламные баннеры, рассылается спам, создаются группы (ячейки) в социальных сетях.

Тесное взаимодействие с членами группы способствует обесцениванию общечеловеческих ценностей – семейных, духовно-нравственных, включающих в себя веру, совесть, обязанность и ответственность, различение хорошего и плохого. У подростка формируются нормы и правила сообщества, восприятие «исключительности» группы, готовность отстаивать ее интересы, выполнять поставленные ей задачи. Постепенно подросток втягивается в жизнь группы, причем так, что выйти из сообщества достаточно сложно.

Информационный блок «Методы защиты от манипулирования».

Манипулирование представляет одну из главных угроз информационно-психологической безопасности, которая существует в интернет-среде. Ключевым умением, которым должен обладать пользователь Интернета, чтобы предупредить пагубное воздействие на свое сознание, является способность распознать применение манипуляции.

Манипуляцию в интернете можно определить по нескольким признакам. В первую очередь пользователю необходимо обращать внимание на то, как представлена интересующая информация. Вероятность использования манипуляции существенно увеличивается в том случае, если в процессе работы с каким-либо информационным объектом, например, с текстом, отсутствуют ссылки на источник информации, в качестве источника информации представлен неизвестный эксперт, в тексте используются многократные повторы одной и той же информации, информация носит ярко выраженный оценочный характер.

В процессе общения в интернете необходимо проявлять осторожность, если отмечается отсутствие информации о собеседнике, используются непозволительные высмеивания, оскорбления в ваш адрес; воздействие на чувства и эмоции, собеседник пытается управлять ходом беседы и подводит к определенным выводам.

Для обеспечения безопасности в интернете следует выполнять общие рекомендации.

1. *Защищайте свои персональные данные.* В онлайне личные данные должны быть надежно защищены. Важно помнить: мы не всегда знаем, кто на самом деле сидит на другом конце линии и прячется под маской приятного виртуального собеседника.

2. *Создайте анонимную личность.* Для получения доступа к функциям отдельных сайтов, форумов, чатов или социальных сетей необходимо ввести персональную информацию. С осторожностью относитесь к тому, что запрашивает у вас ресурс: по возможности, используйте вымышленный ник, не связанный с настоящим именем или фамилией, указывайте общий адрес (например, только город или страну), не вводите свой номер телефона – детским сайтам эти данные не нужны, используйте опцию «скрывать мой электронный адрес», которая предоставляется большинством форумов для защиты пользователей от спама, не используйте свою фотографию в качестве аватара – лучше подобрать изображение, не относящееся к личной жизни.

3. *Выбирайте, с кем советоваться.* Подростки нередко проявляют интерес к вопросам сексуальности и вполне закономерно ищут нужную информацию в Сети. Однако если хочется поговорить на эту тему, обсудить личные ощущения или проблемы, лучше найти для этого человека, знакомого в реальной жизни, которому можно доверять.

4. *Сообщайте о противоправных действиях.* Если вас пытаются соблазнить, вызывают на смущающий разговор, обязательно сообщите об этом родителям или друзьям. К тому же современные ресурсы предоставляют возможность отправить модератору жалобу на сообщение или личное письмо – не стесняйтесь пользоваться этими функциями. Также рекомендуется сохранять

тексты электронных писем и беседы в чатах, сообщения SMS или MMS (например, в папке «Входящие сообщения») – их можно представить в качестве доказательств в милиции.

5. *Помните, что не всякий человек в онлайновой среде является тем, за кого себя выдает.* Собеседники могут притворяться ровесниками, чтобы создать атмосферу дружеских отношений и доверия, а затем перейти к встречам и возможному насилию в реальном мире.

Методы противодействия манипуляции в интернете можно разделить на три основные группы. *Первая группа* – методы противодействия, которые основаны на *умении контролировать и анализировать свои действия*.

1. Необходимо уметь отстаивать свою точку зрения, свои взгляды и убеждения в дискуссиях или спорах.

2. Необходимо подтверждать свою позицию фактами.

3. В случае, если дискуссия приобретает агрессивный характер, не стоит оправдываться или защищаться. Оправдываясь или защищаясь, человек резко теряет инициативу в дискуссии, оставаясь беззащитным перед манипулятором.

4. Важно знать свои слабые места и стараться обходить стороной обсуждение, которое может вызвать у вас негативные эмоции.

5. Необходимо доверять своей интуиции, если появляются сомнения в намерениях собеседника, а также в правдивости полученной информации.

Вторая группа методов направлена на *развитие критического мышления* – объективной оценки ситуации или события, способности человека поставить под сомнение поступающую информацию и даже собственные убеждения и выводы. Необходимо дать себе время и задать критические вопросы по поводу того, что вам предлагают. Приведите доводы «за» и «против» по поводу той информации, что вам преподносят. Для развития критического мышления необходимо обратить внимание на следующее.

1. Необходимо проверять поступающую информацию, искать ее источники, а также альтернативные позиции, которые могут подтвердить или опровергнуть представленную информацию.

2. Если имеет место активное влияние собеседника, то необходимо найти информацию о нем, его профиль в интернете, просмотреть его круг общения, возможно, и общение с самим кругом.

3. Ключевым элементом критического мышления являются ответы на вопросы: «Зачем мне нужно общаться с этим человеком?», «Почему я должен читать этот блог или прислушиваться к мнению этого человека»? и др. Вопросы подобного рода позволяют создать первичную защиту к восприятию информации манипулятивного характера.

Третья группа методов направлена на *рациональное и эффективное использование доступного инструментария интернет-ресурсов*. Для защиты от манипулирования человеку необходимо:

1. Использовать систему черных списков (выделение в особую группу собеседников, пытающихся манипулировать вами).

2. Использовать систему фильтрации нецензурных слов, которая позволяет испытывать меньший эмоциональный дискомфорт в общении с другими пользователями.

3. Не оставлять в интернете слишком много информации о себе. Эти сведения манипулятор сможет использовать для того, чтобы войти в круг вашего общения (прикрывшись общими интересами), либо выступить в роли интернет-тролля и подвергнуть критике вас и ваши интересы, «наклеить» на вас соответствующие ярлыки.

4. Во время дискуссии или поиска информации не позволять отвлекать себя от изначально интересующей темы.

5. При необходимости обратиться в центры безопасности или к администраторам Интернет-ресурсов с просьбой заблокировать агрессивного пользователя в случае столкновения с киберзапугиванием.

Усвоив указанные методы противодействия манипуляциям в интернете, пользователь получит возможность обеспечить собственную информационно-психологическую безопасность.

В процессе использования интернет-ресурсов необходимо отличать фейк от правды. Существует ряд приемов, чтобы обмануть, но есть и приемы, позволяющие распознать ложь. Назовем некоторые из них:

1. «Правило трех». Прежде чем принять за истину какую-либо информацию в Интернете, необходимо проверить ее еще, как минимум, в двух, не зависимых друг от друга, источниках.

2. Сравнение полученной информации с уже известной по этой теме. В поисках какого-либо материала не стоит полагаться на первые попавшиеся источники.

3. Проверка достоверности полученной информации у авторитетных экспертов (специалистов). Если того требует необходимость, можно проверить информацию, проконсультироваться с экспертами в данной области (в зависимости от характера информации в качестве эксперта может выступить учитель, педагог-психолог и др.).

4. Запрос у источника информации дополнительных деталей, подтверждающих истинность основного сообщения. Если на сайте нет контактов автора или же он вообще не указан, то, скорее всего, такая информация является перепечаткой, соответственно она могла утратить свою точность и истинный смысл.

Будьте всегда внимательны к Другому, который оказался рядом с Вами, и ко всему, что происходит вокруг. Не позволяйте собой манипулировать!

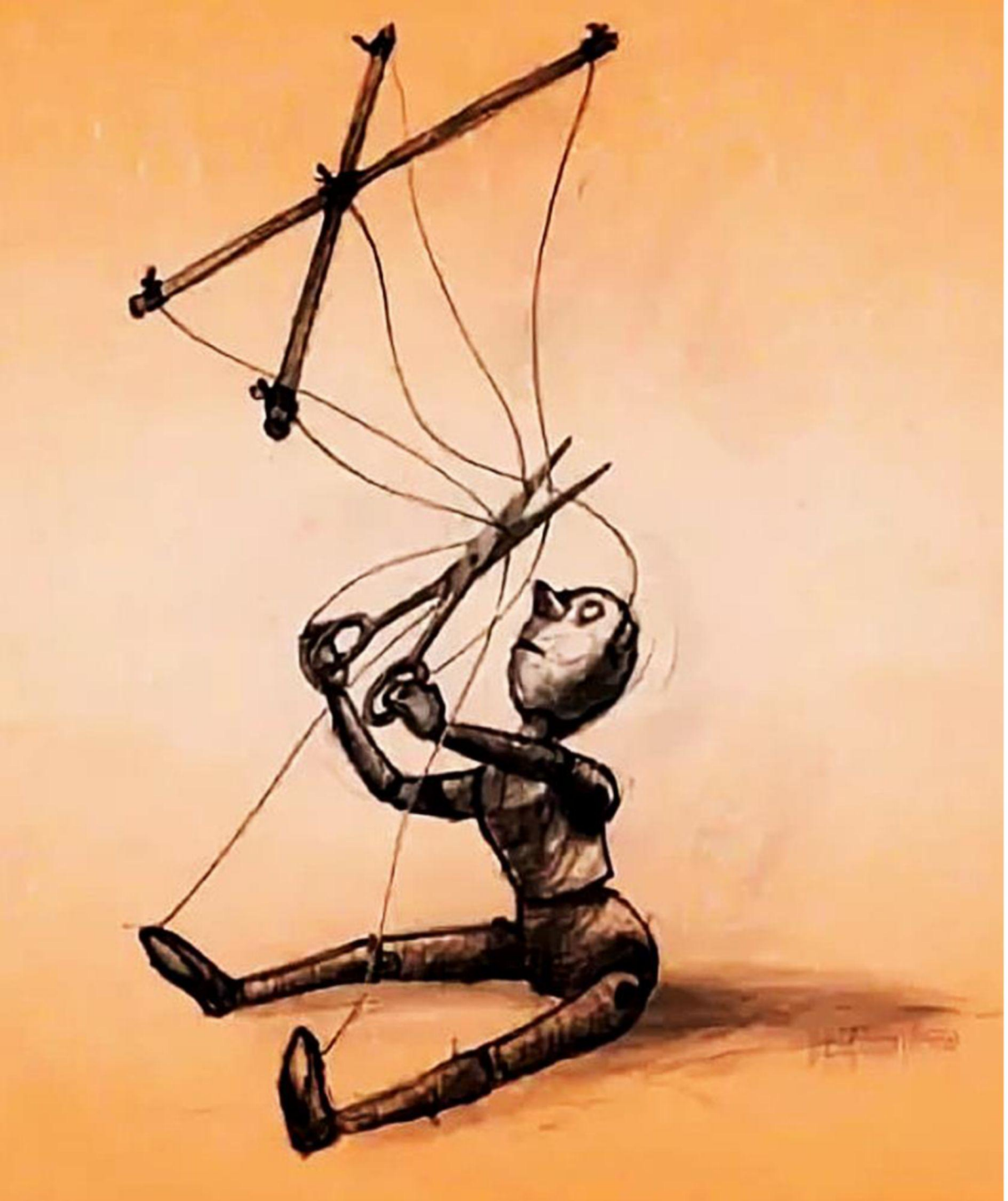
Использованные источники:

Актуальные вопросы обеспечения информационной безопасности: пособие для педагогов учреждений образования, реализующих образовательные программы общего среднего образования / В.А. Арчаков [и др.]. – Минск: Национальный институт образования, 2021. – 168 с.: ил.

Горина, Е. В. Коммуникативные технологии манипуляции в СМИ и вопросы информационной безопасности – дата доступа 03.03.2023: https://elar.urfu.ru/bitstream/10995/42384/1/978-5-7996-1807-0_2016.pdf

Строганов, В. Б. Методы противодействия манипуляции в Интернете – дата доступа 03.03.2023: https://elar.urfu.ru/bitstream/10995/83894/1/978-5-321-02538-3_2017_074.pdf

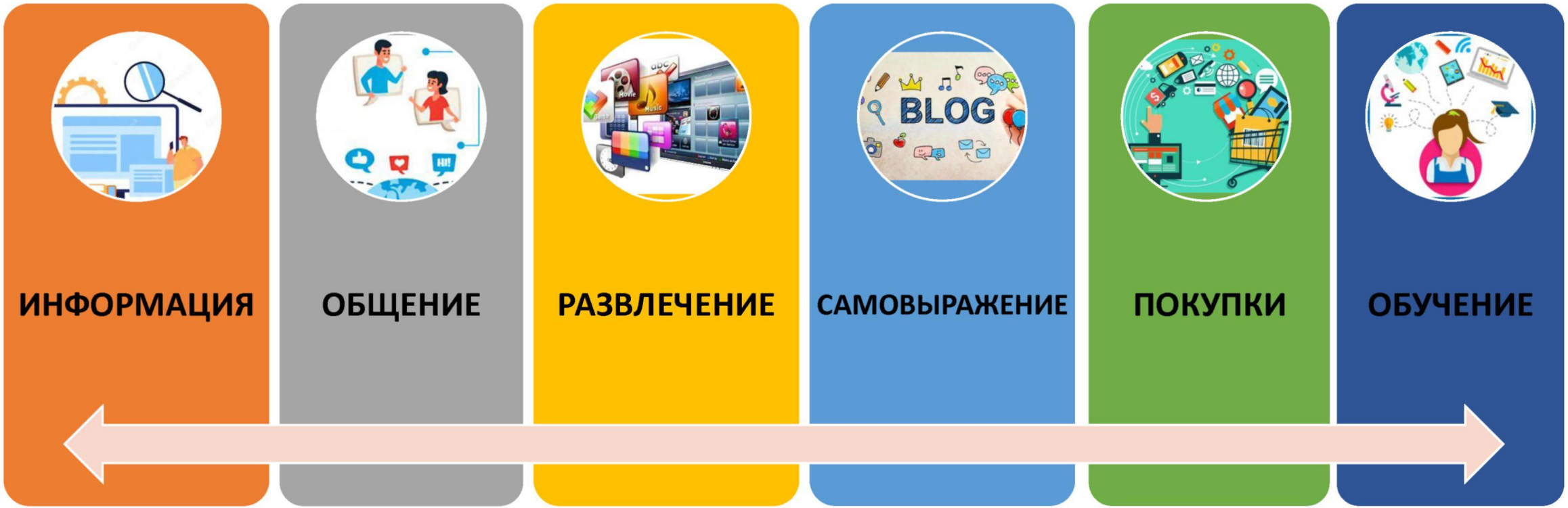
Г. У. Солдатова, С. В. Чигарькова, А. А. Дренёва, С. Н. Илюхина Профилактика деструктивного поведения подростков и молодежи в Интернете дата доступа: 03.03.2023: https://inpsycho.ru/files_new/2019/12/%D0%9F%D1%80%D0%BE%D1%84%D0%B8%D0%BB%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%BF%D0%BE%D0%B4%D1%80%D0%BE%D1%81%D1%82%D0%BA%D0%BE%D0%B2%20%D0%B8%20%D0%BC%D0%BE%D0%BB%D0%BE%D0%B4%D0%B5%D0%B6%D0%B8%20%D0%B2%20%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5.pdf



Единый информационный час **«Угрозы интернета – как защититься от манипуляций»**

Интернет-угрозы: какие опасности нас подстерегают в интернете

ЧЕМ ПОЛЕЗЕН ИНТЕРНЕТ?



Интернет-угрозы: какие опасности нас подстерегают в интернете

Интернет-риски

Контентные риски

- Негативный контент
- Искаженная информация
- Ресурсы, пропагандирующие насилие и др.

Коммуникационные риски

- Груминг
- Буллинг, кибербуллинг
- Троллинг

Электронные риски

- Вредоносные программы
- Кибермошенничество
- Спам

Потребительские риски

- Мошеннические интернет-магазины
- Мобильное и интернет-мошенничество (фишинг, вишинг, фарминг, кликфрод, «нигерийские письма»)

Компьютерные риски

Психологические проблемы

- Интернет-зависимость
- Игровая зависимость

Физиологические проблемы

- Гипотрофия мышц
- Ухудшение зрения
- «Туннельный синдром»
- Остеохондроз
- Лишний вес
- Ослабление иммунитета

Интернет-угрозы: какие опасности нас подстерегают в интернете

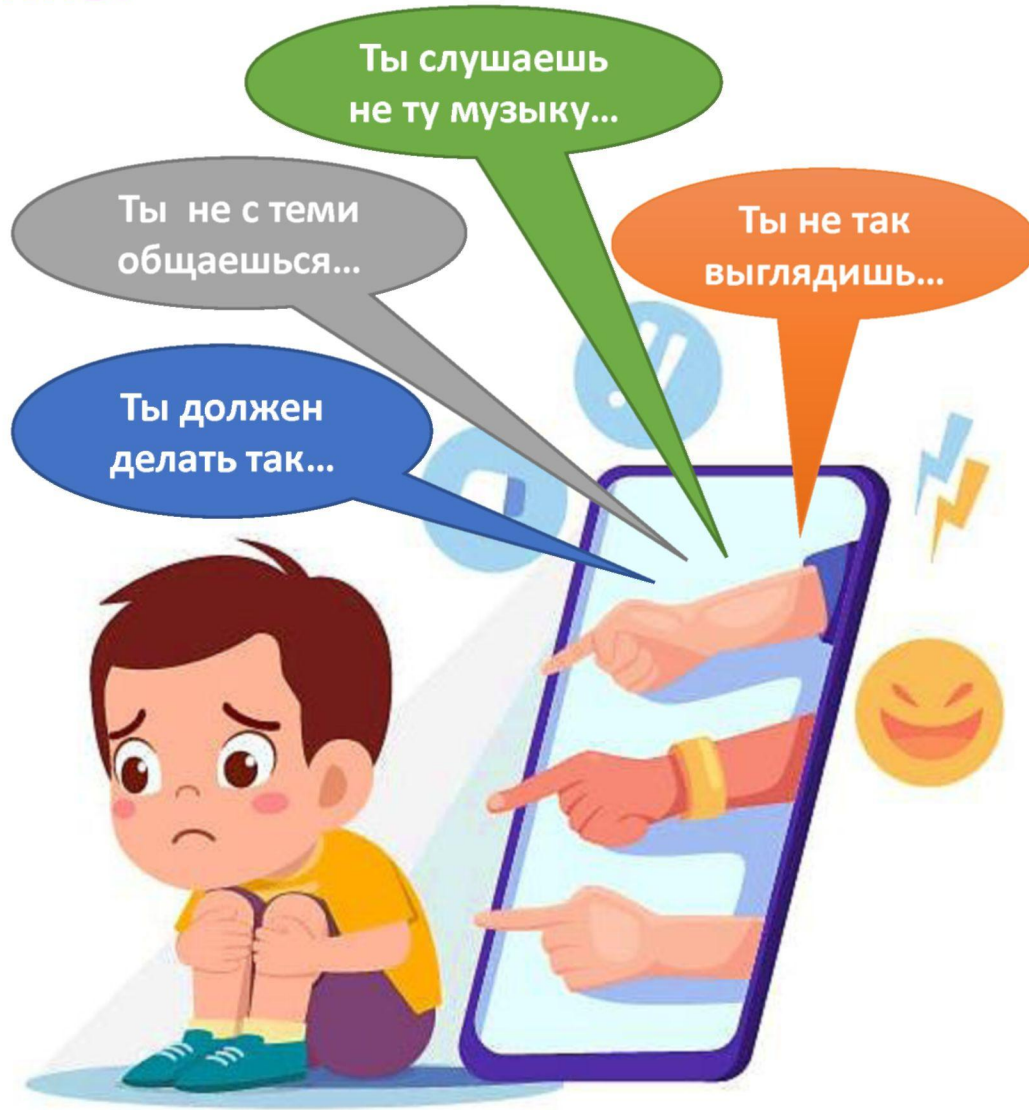
Список запрещенной для распространения среди детей информации, причиняющей вред их здоровью и развитию:

- побуждающая к совершению действий, представляющих угрозу жизни и (или) здоровью;
- способная вызвать желание употреблять наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную продукцию, принять участие в азартных играх, заниматься бродяжничеством, попрошайничеством и др.;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;
- отрицающая традиционные семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

Манипулирование в интернете. Вовлечение учащихся в деструктивные группы

МАНИПУЛЯЦИЯ – способ подчинения, управления людьми путем воздействия на них, программирования их поведения. Часто такое воздействие ставит своей задачей изменение мнений, побуждений и целей людей в нужном манипулятору направлении. Любой человек может влиять на другого через знания (манипулирование информацией) и чувства (манипулирование эмоциями).

Цель манипуляторов – добиться от людей поведения, которое им нужно. Манипуляторы не считают других людей личностями, для них не имеет значения неприкосновенность личности.



Манипулирование в интернете. Вовлечение учащихся в деструктивные группы

ФЕЙК (англ. Fake – подделка) – ложная, недостоверная, сфальсифицированная информация об актуальных значимых фактах и событиях с целью ввести в заблуждение.

Фейковым может быть контент практически любого вида: *новость*, *изображение*, *видеоролик* и даже *страницы в социальных сетях*.

Зачем распространяются фейки, вбросы, сенсации?

- Пиар, популярность, рост аудитории
- Попытка отвлечь внимание от действительно важных новостей, ввести в заблуждение
- Увеличение заработка
- Распространение паники, тревоги, неопределённости, провокация беспорядков, необдуманных действий

Манипулирование в интернете. Вовлечение учащихся в деструктивные группы

Интернет-сообщество — это группа людей в сети со схожими интересами.

Чаще всего такие группы оказывают положительное влияние, способствуют углублению знаний в определенной сфере, организации общения с единомышленниками.

Группы, которые оказывают вредное, негативное влияние на людей (деструктивные группы):

- **экстремистские** (обучают использованию оружия, нанесению вреда зданиям, сооружениям, технике, граффити и неуважительных надписей, призывают к убийствам и проведению выступлений протеста, террористических акций);
- **религиозно-сектантские** (призывают к вступлению в религиозные группы, которые считают себя исключительными, избранными, готовыми лишать жизни себя или других людей, разрушать памятники культуры, сооружения и имущество людей других религиозных взглядов);
- **призывающие к причинению вреда собственному здоровью и организму;**
- **фанатские, нацистские и иные группы**, призывающие к шокирующим, агрессивным, разрушительным действиям в отношении материальных объектов, людей, других групп иных увлечений, национальностей и др.

Манипулирование в интернете. Вовлечение учащихся в деструктивные группы

ВОВЛЕЧЕНИЕ В ДЕСТРУКТИВНЫЕ ГРУППЫ

1. Предварительно на основе анализа поисковых запросов определяются **потенциальные участники группы** («жертвы»).

2. Координатор устанавливает с «жертвой» **контакт,** вовлекает в диалог.

3. «Жертве» создают **комфортную и интересную среду для общения.**

4. Возможные варианты развития ситуации:

4.1. Если «жертва» не подходит для сообщества (ею сложно управлять, оказывать на нее влияние), то контакт резко разрывается.

4.2. Если «жертва» прошла проверку, то получает доступ к основной группе (другому сайту, странице и т.д.), в которой происходит дальнейшая вербовка.

4.3. «Жертва» остается на первичном ресурсе, где происходит погружение в более серьезный (глубокий) контент сообщества (общение на форуме, просмотр видеоматериалов, чтение книг, статей и т.д.).

Методы защиты от манипулирования

СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В ИНТЕРНЕТЕ

ИСПОЛЬЗУЙ СЛОЖНЫЕ ЛОГИНЫ И ПАРОЛИ

Если ты регистрируешься на сайте или соцсетях, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Не забудь выйти из своего аккаунта, если работаешь на чужом устройстве.

СПРОСИ СОВЕТ У ВЗРОСЛЫХ

Спрашивай взрослых о непонятных вещах, которые ты встречаешь в интернете: ты не знаешь, какой пункт выбрать, на какую кнопку нажать, как закрыть программу или окно. Взрослые помогут разобраться и подскажут: что можно делать в интернете, а что – не рекомендуется.

ОГРАНИЧЬ ИНФОРМАЦИЮ О СЕБЕ

Никогда не рассказывай о себе незнакомым людям в интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому о том, где работают твои родители и номера их телефонов. Эта информация может быть использована во вред тебе и твоим родителям.

НЕ ОТПРАВЛЯЙ СМС

Тебе предлагают скачать красивую картинку или интересный рингтон в интернете за SMS? Проверь номер, на который просят отправить сообщение, в любом поисковике. Возможно, это мошенничество, и тебе пришлют файл с вирусом или спишут со счета телефона солидную сумму денег.

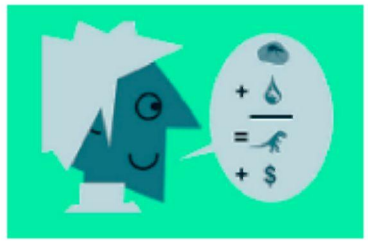
БУДЬ ВНИМАТЕЛЕН К СОЕДИНЕНИЯМ WI-FI

При выходе в Интернет через общественную Wi-Fi сеть, не совершай никаких покупок и оплаты, не проверяй личную электронную почту и не передавай конфиденциальную информацию. Злоумышленники могут похитить ваши пароли и данные. По возможности пользуйся мобильным интернетом, т.к. провайдер обеспечивает дополнительный уровень защиты от внешних угроз.

ОНЛАЙН-ОПЛАТА

Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы. Воздержись от онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги при отсутствии достоверных данных о том, что они являются теми, за кого себя выдают. Адрес безопасного ресурса начинается с https://.

Методы защиты от манипулирования



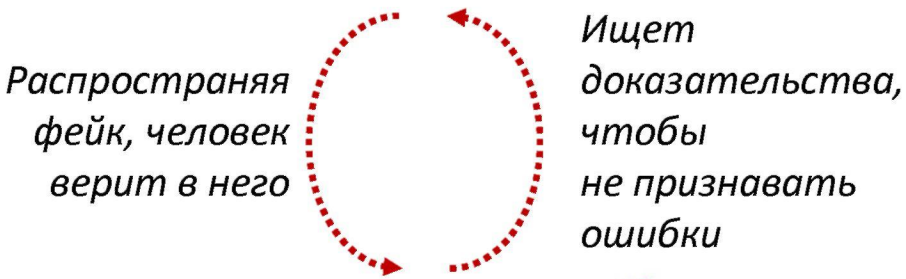
I группа
методы **противодействия, которые основаны на умении контролировать и анализировать свои действия**

II группа
методы **развития критического мышления**

III группа
методы **рационального и эффективного использования доступного инструментария интернет-ресурсов**

1. Использовать систему «**черных списков**» (выделение в особую группу собеседников, пытающихся манипулировать вами).
2. Использовать **систему фильтрации нецензурных слов**, которая позволяет испытывать меньший эмоциональный дискомфорт в общении с другими пользователями.
3. **Не оставлять** в интернете **слишком много информации о себе**. Эти сведения манипулятор сможет использовать для того, чтобы войти в круг вашего общения.
4. Во время дискуссии или поиска информации **не позволять отвлекать себя от изначально интересующей темы**.
5. При необходимости **обратиться в центры безопасности** или к администраторам интернет-ресурсов с просьбой заблокировать агрессивного пользователя в случае столкновения с киберзапугиванием.

Методы защиты от манипулирования



КАК РАСПОЗНАТЬ ФЕЙКОВЫЕ НОВОСТИ?

- **Проверьте факты и подлинность изображений.**

Достоверные новости, как правило, включают множество проверяемых фактических данных, цитаты экспертов и пр. Обращайте внимание на изображения – в соцсетях они могут быть отредактированы.

- **Проверьте источник и автора.**

Проверьте адрес страницы, на которой размещена новость. Если в адресе содержатся орфографические ошибки или используются редкие доменные расширения, – источник ненадежный. Обратите внимание на автора новости и/или мнения. Какая у него репутация, является ли он признанным экспертом в данной области?

- **Оцените комментарии.**

Ссылки и комментарии к статье могут автоматически создаваться ботами или нанятыми пользователями. Признак этого – однотипность комментариев. Сохраняйте критический настрой, чаще задавайте себе вопрос: для чего написана данная статья? Продвигает ли она чьи-то интересы, взгляды или идеи?

- **Проверьте другие источники.**

Сообщают ли о данном факте иные источники? Используется ли в статье цитирование с ссылками на авторитетные источники информации? Цитируются ли в статье достоверные источники?

Методы защиты от манипулирования

Замерзшая Венеция ?

Правда
или
Фейк?

Вот фото озера Байкал

Вот фото Венеции