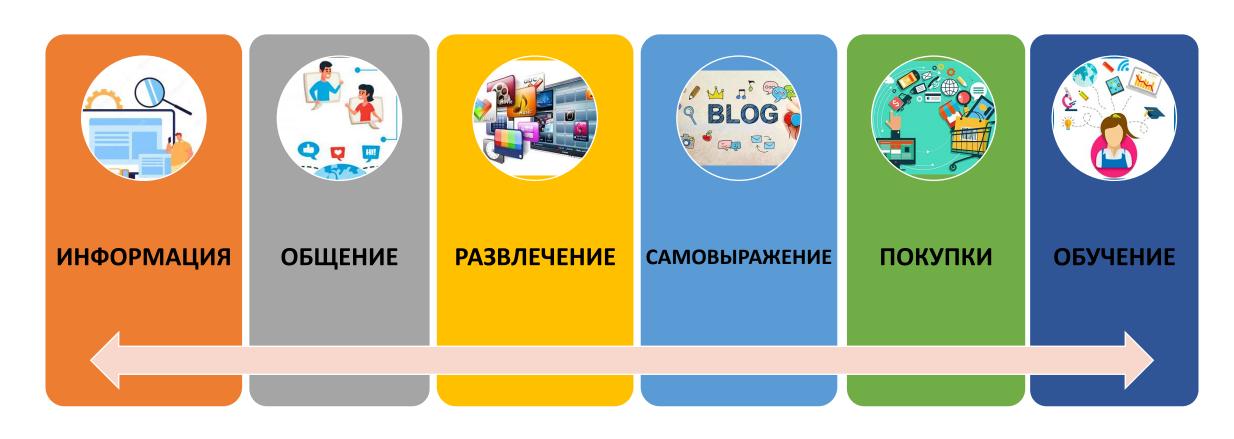


Единый информационный час «Угрозы интернета как защититься от манипуляций»



Интернет-угрозы: какие опасности нас подстерегают в интернете

ЧЕМ ПОЛЕЗЕН ИНТЕРНЕТ?





Интернет-угрозы: какие опасности нас подстерегают в интернете

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»)



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 <u>положительное влияние</u>, 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.).



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://.











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

ІІ 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.









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?



Замерзшая Венеция?





Вот фото озера Байкал



Вот фото Венеции