**Конспект занятия для учащихся 12-16 лет**

**«Критический взгляд на Интернет»**

**Цель занятия:** формирование знаний учащихся о правилах безопасного пользования информационно-коммуникационными технологиями.

**Задачи:**  
*Обучающие:*  
1. Дать представление о возможных опасностях для пользователей сети «интернет».  
2. Дать представление о правилах цифровой безопасности.  
3. Сформировать представление о личной ответственности и бдительности в цифровом пространстве.

*Развивающие:*  
1. Развивать навыки анализа, сопоставления, обобщения при работе с информацией.

2. Формировать навыки эффективного общения, сотрудничества.  
3. Развивать критическое мышление.  
*Воспитательные:*  
1. Способствовать формированию ответственного поведения учащихся в цифровом пространстве.  
2. Формировать мотивацию к развитию и совершенствованию цифровой грамотности.  
3. Формировать культура общения, в том числе в сети «Интернет».

**Аннотация:** Занятие рассчитано на учащихся в возрасте от 12 до 16 лет и предполагает групповую работу учащихся по теме безопасности в информационном пространстве. В занятии применяются технологии развития критического мышления, позволяющие подросткам активно включаться в процесс формирования нового знания. Данная разработка может быть использована педагогами дополнительного образования, для классных руководителей, педагогов школ при организации воспитательных и профилактических мероприятий.

**Ход занятия**

**1. Вводная часть**

Мы живем в век информатизации. Созданы и продолжают развиваться условия для удовлетворения информационных и коммуникационных потребностей любого человека. Средствaми, обеспечивающими нас этими возможностями, является интернет, мобильная связь.  
На сегодняшний день мы не представляем своей жизни без мобильного телефонa, мессенджеров, электронной почты, поисковых систем. Однако наряду с несомненными позитивными появляются и негативные последствия широкого внедрения информационных технологий в нашу жизнь.  
Сегодня на нашем занятии мы постараемся критически взглянуть на современные информационно-коммуникационные технологии (ИКТ), определить пути безопасного взаимодействия человека с ними.

**2. Основная часть**

**Игра – брифинг**

Ведущий озвучивает утверждение, которое имеет две позиции. Команде нужно выбрать одну из представленных позиций и придумать три аргумента в ее защиту. Затем один представитель от команды представляет позицию команды и придуманные аргументы. Каждую позицию по новому утверждению представляет новый спикер.

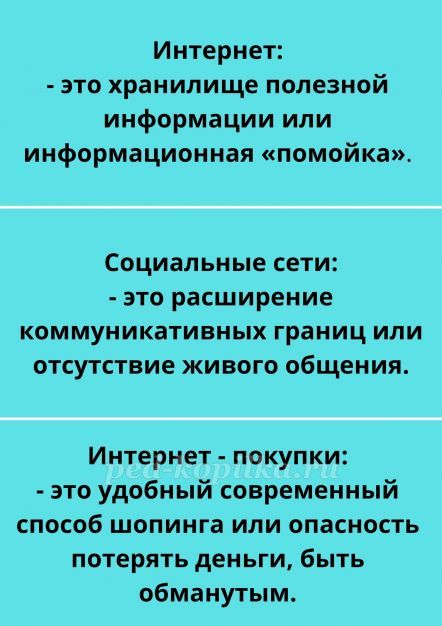
1. Интернет - это хранилище полезной информации или информационная «помойка».  
2. Социальные сети - это расширение коммуникативных границ или отсутствие живого общения.

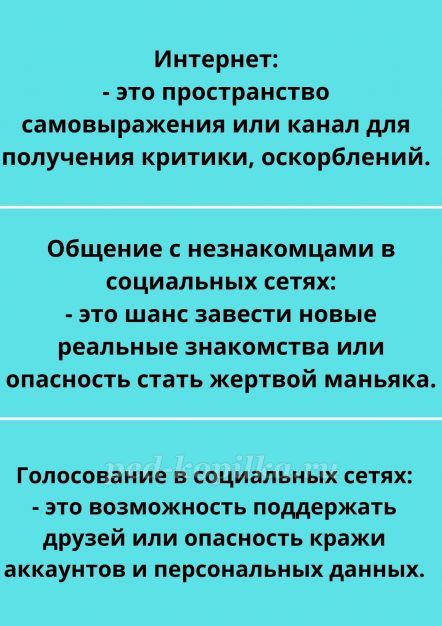
3. Интернет-покупки - это удобный современный способ шопинга или опасность потерять деньги, быть обманутым.

4. Голосование в социальных сетях - это возможность поддержать друзей или опасность кражи аккаунтов и персональных данных.  
5. Общение с незнакомцами в социальных сетях- это шанс завести новые реальные знакомства или опасность стать жертвой маньяка.  
6. Интернет- это пространство самовыражения или канал для получения критики, оскорблений.

7. Ведение страницы в социальных сетях - это возможность заявить о себе или опасность привлечь к себе нежелательное внимание посторонних людей.

*Карточки для вывода вопросов на экран:*







**Рассказ**  
Интернет – это наш друг и помощник. Но в каждой ситуации мы озвучивали, что для безопасного пользования благами Интернета необходимо соблюдать определенные условия. То есть, для того, чтобы безопасно пользоваться всеми преимуществами ИКТ, человек должен обладать ИКТ или цифровой компетенцией.  
  
*Посмотрим определение понятию «компетентность»:*а

**Компетентность** - наличие знаний, умений и навыков, необходимых для эффективной деятельности в определенной области.  
**Компетентность** - потенциальная готовность решать задачи со знанием дела; постоянное обновление знаний, владение новой информацией для успешного применения этих знаний в конкретных условиях.  
То есть компетентность – это не просто знания, но и действия, основанные на имеющихся знаниях, а также способность знания и опыт накапливать и обновлять.  
Цифровая компетентность подразумевает умение человека уверенно, безопасно и эффективно использовать цифровые технологии во всех сферах своей деятельности.

**Цифровую компетенцию можно разделить на четыре составляющих:**  
• Информационная компетенция – умение искать информацию, критически ее оценивать и проверять достоверность, умеет отфильтровывать лишнюю и вредоносную информацию.

• Коммуникативная компетенция – умение выстраивать социальное взаимодействие через сеть без рисков для себя и окружающих.  
• Техническая компетенция - умение работать в цифровом пространстве.  
• Потребительская компетенция – умение решать повседневные задачи, в том числе связанные с покупками через сеть.

**Мозговой штурм**

Сейчас мы продолжим работу в группах и создадим правила, которых необходимо придерживаться для обеспечения безопасности и эффективности при работе с цифровыми технологиями.  
***1 группа – разрабатывает правила информационной безопасности***  
**Пример правил:**

- нужно отказываться от изучения информации, побуждающей наносить вред себе или другим, содержащей призывы к жестокости или употреблению запрещенных веществ, поскольку данные виды информации запрещены Федеральным законом № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию», а также формирует негативный цифровой след.

- использовать в качестве источника информации официальные сайты государственных муниципальных организаций.

- и другие правила.

***2 группа – создает правила коммуникационной безопасности***  
**Пример правил:**

- В целях безопасности нельзя раскрывать личную информацию: настоящие имя, фамилию, телефон, адрес, номер школы, а также выкладывать свои фотографии и любую другую информацию.

- Нельзя вести себя невежливо и агрессивно, грубить, угрожать другим участникам.  
- Нельзя встречаться с Интернет-знакомыми в реальной жизни.  
- Необходимо использовать настройки безопасности и приватности.  
- и другие правила.

***3 группа – думает о правилах технической безопасности***  
**Пример правил:**

- В целях безопасности нельзя открывать вложенные файлы электронной почты и сообщений от неизвестного отправителя.

- Необходимо использовать настройки безопасности и приватности, чтобы не потерять свои аккаунты.

- Необходимо использовать современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ, а также антивирусные программы с автоматическим обновлением баз.

- Необходимо использовать ограничь физический доступ к компьютеру для посторонних лиц.

- и другие правила.

***4 группа – пишет правила потребительской безопасности***  
**Пример правил:**

- Необходимо использовать безопасные сайты, в том числе проверенные сайты интернет-магазинов и поисковых систем.

- Интернет-покупки должны быть согласованы с родителями.

- Не скачивать приложения из неизвестных источников.

- и другие.

Группам дается несколько минут на обдумывание, после чего спикер от группы озвучивает правила. Остальные группы могут уточнять и дополнять.  
**Решение кейсов**

Предлагаю обсудить конкретные ситуации и определить наиболее безопасные пути их решения.

1. Неизвестный человек добавляется к вам в друзья в социальной сети, некоторое время вы общаетесь на общие темы, затем он предлагает вам встретиться.  
*(Ответ: небезопасно встречаться с человеком, с которым вы познакомились через сеть)*.

2. После того как вы отказались встретиться с вашим интернет-знакомым, он пишет вам угрозы и оскорбления).

*(Ответ: сообщить родителям).*

3. Вам пришло электронное письмо о том, что происходит замена старого образца полиса ОМС на новый образец, и, чтобы подать заявление, необходимо пройти по ссылке ниже.

*(Ответ: не переходить по ссылке).*

5. Вам предлагается в течение 7 дней бесплатно пользоваться определенным приложением, а после пробного срока перейти на пользование на платной основе, поэтому необходимо привязать карту для списания средств, которое будет происходить по истечении 7 дней.

*(Ответ: не привязывать карту).*

6. В сообщении от вашего друга в социальной сети содержится просьба о голосовании за его работу со ссылкой на нее, но чтобы проголосовать, вам нужно ввести свои параметры доступа в социальную сеть.

*(Ответ: ничего не вводить, подозрительные сообщения и запросы сайтов игнорировать).*

7. При скачивании картинки или мелодии из Интернета тебя просят отправить СМС для подтверждения действия на сайте.

*(Ответ: не отправлять).*

**3. Заключительная часть**

**Синквейн**  
На основе анализа полученной информации группам учащихся предлагается написать синквейн.

В первой строке - пишем тему, о котором пойдет речь.

Во второй строке – описание объекта в двух прилагательных.

В третьей строке – действия в трех глаголах.

Четвертая строка – фраза из четырех слов, выражающая отношение к объекту.

Пятая строка – существительное, отражающее суть предмета.  
*Пример, составленный учащимися:  
Интернет.  
Безграничный, актуальный.  
Соединяет, обогащает, увлекает.  
Использовать можно, но осторожно!  
Паутина.*