# МКОУ «Сюгютская СОШ»

# Классный час «Безопасность в сети Интернет»

# (в 11классе)

**Провела кл.руководитель :Сеферова М.М**

**Цель**: обратить внимание учащихся на возможные угрозы в сети Интернет, повысить грамотность учащихся в вопросах безопасности в сети, формировать общепринятые нормы поведения в сети.

**Задачи**:

1. Ознакомить учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.

2. Выработать правила безопасного поведения в сети.

3. Выработать  необходимость использования в сети общепринятых нравственных норм поведения.

**Ожидаемые результаты:**

- повышение уровня осведомленности учащихся о проблемах безопасности при использовании сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз;

-формирование культуры ответственного, этичного и безопасного использования Интернета.

**Содержание**

1. Введение. Вступительное слово учителя

-Угрозы в сети. (сообщения детей)

- Спам и фишинг

- Грубость в Интернете

- Кибер-буллинг

- Интернет-зависимость

2.Пять советов, которые помогут обеспечить безопасность в Интернете

* 1. Создание памятки по безопасному поведению в интернете

1. **Введение.**

Мы живем в век информационных технологий, достаточно много времени проводим в сети в поисках информации, готовясь к занятиям, или просто отдыхая. Мы общаемся с друзьями, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Очень важно научиться правильно вести себя в сети Интернет, знать правила безопасности и этичного поведения. Сегодня мы с вами об этом и поговорим.

**Угрозы в Сети. (Сообщения подготовлены учащимися в качестве д/з)**

1. **Спам и фишинг ( уч-ся)**

*Спам* — это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга.

Во время чтения электронной почты или просмотра страниц в Интернете следует помнить про мошенников, которые стремятся похитить ваши личные данные или деньги, а, как правило, и то, и другое. Такие мошеннические действия или схемы называются *«фишингом»* (от английского слова «fish», что означает «рыба» или «рыбачить»), так как их цель – «выудить» у вас ваши персональные данные.

Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками. Как защитить себя от спама и фишинга?

*Советы от команды экспертов «Лаборатории Касперского»*

- Заведите себе несколько адресов электронной почты .  
Лучше всего иметь по крайней мере два адреса электронной почты.

- Личный адрес электронной почты.  
Этот адрес должен использоваться только для личной корреспонденции.

- «Публичный» электронный адрес.  
Используйте этот электронный адрес для регистрации на общедоступных форумах и в чатах, а также для подписки на почтовую рассылку и другие интернет-услуги.

- Никогда не отвечайте на спам.

- Подумайте, прежде чем пройти по ссылке «Отказаться от подписки».

- Своевременно обновляйте браузер.

1. **Грубость в интернете**. Как не испортить себе настроение при общении в сети и не опуститься до уровня «веб-агрессора» (3 гр.)

Существует в Интернете особая категория пользователей, с которой лучше никогда не встречаться. Это так называемые сетевые хамы и форумные тролли, развлекающиеся провокациями своих собеседников в Интернете.

Зачем они это делают? Чтобы получить удовольствие от негативной реакции других людей. Такие пользователи преднамеренно идут на конфликт и доводят собеседника до нервного срыва, который может выплеснуться в онлайн. Чаще всего этим занимаются люди с комплексами неполноценности, которых обижают в реальной жизни – и потому они пытаются отыграться в Интернете. Анонимность в Сети позволяет им представлять себя совершенно другими и – главное – быть уверенными в своей безнаказанности, поэтому они пишут и делают такие вещи, которые в реальной жизни никогда бы не рискнули сотворить в присутствии оппонента. По причине как неизвестности, так и недосягаемости, «травить», оскорблять и провоцировать людей, кажется им забавным занятием.

1. **Кибер-буллинг**. (4гр)

Кибер-буллинг (cyber-bullying), подростковый виртуальный террор, получил свое название от английского слова bull — бык, с родственными значениями: агрессивно нападать, бередить, задирать, придираться, провоцировать, донимать, терроризировать, травить. В молодежном сленге является глагол аналогичного происхождения — быковать.

Итак, кибер-буллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе. Кибер-буллинг включает целый спектр форм поведения, на минимальном полюсе которого — шутки, которые не воспринимаются всерьез, на радикальном же — психологический виртуальный террор, который наносит непоправимый вред, приводит к суицидам и смерти. Есть также понятие буллицида — гибели жертвы вследствие буллинга.

Исследователи выделили восемь основных типов буллинга:

1**. Перепалки, или флейминг** — обмен короткими эмоциональными репликами между двумя и более людьми, разворачивается обычно в публичных местах Сети. Иногда превращается в затяжной конфликт (holywar — священная война). На первый взгляд, флейминг — борьба между равными, но при определенных условиях она может превратиться в неравноправный психологический террор. Неожиданный выпад может вызвать у жертвы сильные эмоциональные переживания.

2**. Нападки,** постоянные изнурительные атаки (harassment) — повторяющиеся оскорбительные сообщения, направленные на жертву

3**. Клевета** (denigration) — распространение оскорбительной и неправдивой информации.

4. Самозванство, перевоплощение в определенное лицо— преследователь позиционирует себя как жертву, используя ее пароль доступа к аккаунту в социальных сетях, ведет переписку.

5**. Надувательство**, выманивание конфиденциальной информации и ее распространение— получение персональной информации и публикация ее в интернете или передача тем, кому она не предназначалась.

6. **Отчуждение** (остракизм, изоляция). Любому человеку присуще желание быть включенным в группу. Исключение же из группы воспринимается как социальная смерть.

7**. Киберпреследование** — скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.

8. **Хеппислепинг (**Happy Slapping — счастливое хлопанье, радостное избиение) — название происходит от случаев в английском метро, где подростки избивали прохожих, тогда как другие записывали это на камеру мобильного телефона. Сейчас это название закрепилось за любыми видеороликами с записями реальных сцен насилия.

Различия кибербуллинга от традиционного реального обусловлены особенностями интернет-среды: анонимностью, возможностью фальсификации, наличием огромной аудитории, возможностью достать жертву в любом месте и в любое время.

*Несколько советов, для преодоления этой проблемы:*

1. Не спеши выбрасывать свой негатив в кибер-пространство.

2. Создавай собственную онлайн-репутацию, не покупайся на иллюзию анонимности.

3. Храни подтверждения фактов нападений.

4. Игнорируй единичный негатив

5. Блокируй агрессоров.

6. Не стоит реагировать на агрессивные сообщения

Классный руководитель.

**2.Пять советов, которые помогут обеспечить безопасность в Интернете**

(от Центра безопасности компании Microsoft)

- Защитите свой компьютер

Постоянно обновляйте все программное обеспечение (включая веб-браузер). Установите законное антивирусное программное обеспечение. Брандмауэр должен быть всегда включен. Установите на беспроводном маршрутизаторе защиту с помощью пароля. Всегда проверяйте флеш-накопители (или USB-накопители). Не переходите по ссылкам и не нажимайте кнопки во всплывающих сообщениях, которые кажутся подозрительными.

- Обеспечьте защиту секретной личной информации

Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

- Используйте надежные пароли и храните их в секрете.

Придумайте пароли, представляющие собой длинные фразы или предложения и содержащие сочетание строчных, прописных букв, цифр и символов. Используйте на разных сайтах разные пароли.

- Позаботьтесь о своей безопасности и репутации в Интернете

Узнайте, какая информация о вас существует в Интернете, а также периодически производите оценку найденных сведений. Создавайте себе положительную репутацию.

- Более безопасное использование социальных сетей

Никогда не публикуйте информацию, которую вы не хотели бы видеть на доске объявлений. Периодически анализируйте, кто имеет доступ к вашим страницам, а также просматривайте информацию, которую эти пользователи публикуют о вас.

***3.Создание памятки по безопасному поведению в интернете.***

Дети выписывают на листочки самые главные советы по безопасности в сети и прикрепляют на баннер – памятку по безопасному и этичному поведению в сети Интернет.

**Классный руководитель.**

**Памятка**

**по безопасному поведению в Интернете**

* 1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
  2. Используйте нейтральное экранное имя, не выдающее никаких личных сведений.
  3. Защитите свой компьютер.
  4. Используйте надежные пароли и храните их в секрете.
  5. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
  6. Не допускайте грубости в интернете, блокируйте веб-агрессоров.
  7. Не добавляйте незнакомых людей в свои контакты.
  8. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
  9. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.
  10. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах.