

Министерство образования Московской области
ГАПОУ МО «Егорьевский техникум»

Методическая разработка

открытого классного часа на тему:
«Кибербезопасность»



Подготовили:
мастер п/о Пронин А.А.,
преподаватель Степанова С.Ю.

Егорьевск, 2020 г.

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:

- Ознакомить учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
- Выработать правила безопасного поведения в сети.
- 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.

Виртуальная реальность, как и любое пространство, несомненно, обладает и достоинствами и недостатками. Существование кибер-опасностей так же неоспоримо, как польза и удовольствие от использования Интернет-ресурсов. За безопасностью пользователей следят государственные структуры, а также и сотрудники Интернет сервисов, администраторы сайтов, модераторы. Однако ежедневно появляются новые жертвы, пострадавшие чаще всего из-за отсутствия грамотности в вопросах безопасности.

Угрозы в Сети. Спам и фишинг

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», так как их цель – «выудить» у вас ваши персональные данные.

Как защитить себя от спама и фишинга? 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

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. 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 недостижимости, «травить», оскорблять и провоцировать людей, кажется им забавным занятием. Как показывает практика, больше половины сетевых грубиянов являются детьми, скучающими в Интернете или не ладящими со сверстниками. Однако случаются и вполне взрослые профессиональные Интернет-скандалисты, для которых довести виртуального собеседника является своего рода искусством. Встретить сетевых хамов можно в любом уголке Интернета: в чатах, в социальных сетях, на сайтах знакомств, на форумах и по электронной почте. Необходимо уметь отличать их от нормальных собеседников, дабы не тратить время и нервы впустую. Если вы замечаете, что вам грубят, провоцируют на ссору или намеренно злят, самым верным решением будет немедленно закончить разговор или игнорировать сообщения данного пользователя на форуме/сайте. Не доставить грубияну удовольствия видеть ваш гнев или обиду будет лучшим наказанием для него, ибо его цель не достигнута.



Кибер-буллинг.

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. 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. 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 — повторяющиеся оскорбительные сообщения, направленные на жертву

3. Клевета — 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. Любому человеку присуще желание быть включенным в группу. Исключение же из группы воспринимается как социальная смерть.

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

8. Хеппислепинг — 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 нападения.
4. Игнорируй единичный негатив
5. Блокируй агрессоров.
6. Не стоит реагировать на агрессивные сообщения



Интернет-зависимость.

Проблема интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми. Официально медицина пока не признала интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления.

По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4—6%. Несмотря на отсутствие

официального признания проблемы, интернет-зависимость уже принимается в расчёт во многих странах мира.

Основные 5 типов интернет-зависимости таковы:

1. Навязчивый веб-серфинг— бесконечные путешествия по Всемирной паутине, поиск информации.

2. Пристрастие к виртуальному общению и виртуальным знакомствам— большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.

3. Игровая зависимость — навязчивое увлечение компьютерными играми по сети.

4. Навязчивая финансовая потребность— игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах



Самый простой и доступный способ решения зависимости — это приобретение другой зависимости. Любовь к здоровому образу жизни, общение с живой природой, путешествия по родному краю, творческие прикладные увлечения, занятия спортом, как правило, выводят человека из зависимости.

Памятка по безопасному поведению в Интернете

- Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

- Используйте нейтральное экранное имя, не выдающее никаких личных сведений.

- Защитите свой компьютер.

- Используйте надежные пароли и храните их в секрете.

- Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.

- Не допускайте грубости в интернете, блокируйте веб-агрессоров.

- Не добавляйте незнакомых людей в свои контакты

- Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки.