

**Государственное автономное образовательное учреждение  
среднего профессионального образования Республики Крым  
«Ялтинский медицинский колледж»**

Воспитательное мероприятие  
Дистанционный классный час  
на тему:  
Свободное время с пользой

Подготовила: Беляева Т.Б.

2020

**Цель:** Ознакомить и 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

**. Основная часть**

1. Создание никнейма.
2. 20 шокирующих фактов о социальных сетях.
3. Угрозы в сети. (Сообщения детей. Домашнее задание)
  - Спам и фишинг
  - Грубость в Интернете
  - Кибер-буллинг
  - Интернет-зависимость

Пять советов, которые помогут обеспечить безопасность в Интернете.

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.

### **Создание никнейма..**

Это упражнение позволило презентовать себя. Это не совсем просто. Виртуальное пространство социальных сетей дает возможность личности действовать анонимно или дискутировать под выдуманным именем. Дискуссия может быть частью игры и положительным элементом в общении, но она одновременно может быть опасным инструментом манипулирования сознанием и нести для человека угрозу.

Поскольку, сегодня наш классный час о виртуальном мире, давайте придумаем себе никнейм. ( Дети записывают никнейм на своем бейджике).

Ник пользователя - это виртуальное имя, которое он выбирает при регистрации на ресурсе. Ник может быть совершенно любым - от вашего имени-фамилии до названия любимого цветка.

Ник, он же никнейм, произошел от английского слова nickname и переводится как "кличка" или "прозвище".

Сегодня никнейм в Интернете, является вашим лицом в сети, которое при желании может отражать вашу истинную сущность, стремления и характер. Никнейм в сети это не просто способ самоидентификации среди таких же, как и вы, сетевых жителей, это также начало названия вашего почтового ящика типа "nickname@адрес\_сервиса.ru", имя для входа на форум, в чат, в онлайн игру, да и в любой другой сервис в котором будет необходимо представиться [1].

Для чего пользователи придумывают ники? (Ответы детей)

### **1. 20 шокирующих фактов о социальных сетях**

1. Причиной каждого третьего в мире развода являются социальные сети.
2. Приблизительно пятнадцатью процентами пользователей социальные сети применяются для организации слежки. Это большей частью практикуется спецслужбами.
3. Среди пользователей соцсетей 37% публикуют в них малоинтересные сведения о собственной личной жизни.
4. Исследованиями установлено, что нахождение в соцсетях ведет к увеличению риска самоубийства, так как человек до минимума сводит свое общение с окружающими и отрешается от действительности.
5. В соответствии со статистикой количество преступлений на сексуальной почве, направленных на несовершеннолетних, выросло из-за соцсетей в 26 раз.
6. Ежегодно около 100 человек лишаются жизни из-за сообщения, оставленного в соцсетях, и эта цифра возрастает.
7. Социальные службы используют для вербовки своих агентов не только спецслужбы, но и различные группировки, в том числе террористической направленности.
8. Социальные сети сужают кругозор человека: он становится зависим от пустых и ненужных сообщений.
9. Чрезмерная увлеченность соцсетями, по данным исследований, ведет к снижению иммунитета, сердечно-сосудистым болезням и душевной дисгармонии. Активные, но не

дающие развития мыслительные процессы наряду с малой подвижностью способствуют развитию заболеваний эндокринной системы.

10. В соцсетях знакомится каждая пятая семья в мире.
11. Средний пользователь посещает аккаунт дважды в день.
12. У среднего пользователя друзьями числится 195 человек.
13. К 2010 году доступ к соцсетям имело уже 96% населения всей планеты.
14. Наиболее активна Интернет-аудитория в России: средний пользователь проводит в нем 6,6 часов в неделю, просматривая 1307 Интернет-страниц.
30. 80% компаний мира подбирают сотрудников с помощью соцсетей.
15. У Бритни Спирс и Эштона Катчера фолловеров столько же, сколько населения в Ирландии, Панаме или Норвегии.
16. Популярные соцсервисы продолжают хранить удаленные пользователями изображения.
17. По числу пользователей лидирует Facebook – 1 миллиард.
18. В сети популярность социальных сетей по результатам проведенного опроса составила: Одноклассники - 73%, Вконтакте - 62%, Facebook - 18%, Twitter - 9%, Livejournal - 3%, LiveInternet - 2% и 1% не знает о сетях ничего.
19. Еженедельно в социальных сетях дети проводят: от 7 до 14 часов – 23%, 14-21 час – 57% и больше 21 часа – 20%.
20. Каждый пятый ребенок из семи дней недели один тратит на соц.сеть [2].

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.

## 1. 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*» (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 [3].

### 1. Грубость в интернете. Как не испортить себе настроение при общении в сети и не опуститься до уровня «веб-агрессора»

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 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 аське, 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.

. Психологи утверждают, что агрессия другого человека - это просьба о любви. Возможно, этому человеку не хватает друзей, теплых отношений, быть может он одинок, или у него неприятности. Будьте внимательны, не торопитесь отвечать на грубость.

### 1. Кибер-буллинг.

Кибер-буллинг (cyber-bullying), подростковый виртуальный террор, получил свое название от английского слова bull — бык, с родственными значениями: агрессивно нападать, бередить, задирать, придирается, 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 буллициды — 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 (holýwar — 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 [4].**

##### **1. 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. Например, в Финляндии молодым людям с интернет-зависимостью предоставляют отсрочку от армии.

*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 [5].

**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.**

### **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**

Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка (🔒) рядом с адресной строкой, который обозначает безопасное соединение.

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. Настройте список пользователей,

которые могут просматривать ваш профиль или фотографии. Подходите избирательно к предложениям дружбы

### **Интернет ресурсы.**

1. <http://nick-name.ru/about/>
2. <http://smonews.ru/48-shocking-facts>
3. <http://www.kaspersky.ru/internet-security-center/threats/spam-phishing>
4. <http://psyfactor.org/lib/cyber-bullying.htm>
5. [http://www.nvppl.ru/show\\_dict\\_812.htm](http://www.nvppl.ru/show_dict_812.htm)
6. <http://www.microsoft.com/ru-ru/security/default.aspx>
7. <http://www.saferunet.ru/teenager/>
8. <http://liubavyshka.ru/>

### **Приложение**

#### **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.

### Смайлики к игровой ситуации

