# Предупреждение: материалы содержат ссылки на ресурсы в сети интернет, перед проведением занятия преподавателю необходимо проверить их работоспособность и содержание и в случае появления на информационном ресурсе сообщений, содержащих информацию, причиняющую вред здоровью и (или) развитию детей, согласно Федеральному закону "О защите детей от информации, причиняющей вред их здоровью и развитию" от 29.12.2010 N 436-ФЗ, не использовать их для проведения занятия.

**КЕЙС 4 Безопасное поведение в сети**

Всего занятий/часов: 4/8

Занятия:

|  |  |
| --- | --- |
| Номер занятия | Основное содержание |
| 1 | Персональная информация пользователя, как она может быть использована злоумышленниками |
| 2 | Правила безопасного обращения с персональными данными в социальных медиа |
| 3 | Правила взаимодействия со злоумышленниками. Что делать, если ваши персональные данные похищены |
| 4 | Урон репутации и правонарушения в сети |

**Занятие 1. Персональная информация пользователя, как она может быть использована злоумышленниками**

План занятия:

|  |  |  |
| --- | --- | --- |
| Номер блока | Продолжи-тельность, мин | Описание учебной работы |
| 1 | 15 | Теоретический блок: что такое персональная информация. Как и зачем злоумышленники похищают персональную информацию. |
| 2 | 5 | Демонстрация видео |
| 3 | 20 | Групповая работа: поиск схем мошенничества в интернете |
| 4 | 5 | Подведение итогов исследования |
|  | *10* | *перемена* |
| 5 | 20 | Теоретический блок: риски, связанные с похищением персональной информации |
| 6 | 10 | Групповая работа: анализ аккаунтов и выявление информации, которая может быть использована злоумышленниками. |
| 7 | 10 | Подведение итогов исследования |
| 8 | 5 | Итоговая рефлексия по занятию |
|  | 45+45 |  |

**Блок 1. Теоретическая часть.**

**Как злоумышленники из социальных сетей находят Вас в реальности**

1. ***Геолокация*.** Сюда входит все. Город, указанный в информации профиля, группы, в которых вы состоите «Интересная Москва» или «Подслушано. Омск». Город, указанный как место проживания у ваших родственников или у большинства ваших друзей. Геопривязка с помощью гаджета. И даже фон ваших фото. Не стоит указывать места, которые вы посещаете или собираетесь посетить, рассказывать о маршрутах передвижения. Также, не стоит передавать свой точный адрес незнакомым людям (передача адреса интернет-магазину для доставки – на Ваш страх и риск).
2. ***Информация, что Вы дома одни*.** Чаты и онлайн-дискуссии – это то место, где дети, как правило, открывают о себе многие вещи, которые нельзя открывать незнакомым людям. В интернет-пространстве нельзя говорить о том, один ли Вы дома, или, когда взрослые придут с работы, а также о том, где они работают и о том, какую аппаратуру, гаджет или аппарат взрослые купили недавно.

Кроме того, всё это нельзя говорить даже хорошо знакомому другу, сидящему по ту сторону экрана. Ведь ребёнок не знает, где в данный момент сидит его друг, и кто находится рядом с ним и читает всё это. Информацию в открытом профиле, открытое сообщение, а также болтовню по мобильному телефону может слышать и читать любой, незаметно стоящий за спиной ребёнка человек.

1. ***Место работы и учебы*.** Чтобы понять ваш статус для финансовой махинации, или узнать точку для шантажа и манипулирования стоит лишь посмотреть информацию о Вас. Не рекомендуется указывать свое место работы и учебы, если в этом нет необходимости.
2. ***Документы и данные банковской карты*.** Не следует хранить в сети копии своих документов, а также «привязывать» к аккаунтам банковские карты и электронные кошельки. В случае взлома преступники могут воспользоваться этими данными, чтобы украсть деньги со счёта или незаконно оформить кредит на Ваше имя. Никогда не разглашайте какие-либо финансовые подробности, например номер карты или пин-код, в комментариях и личной переписке. Даже если вам срочно надо сделать покупку.
3. ***Возраст*.** Указывать дату рождения предпочитают большинство пользователей, однако сообщая число, год и место своего рождения Вы невольно помогаете аферистам похитить Вашу финансовую информацию. Благодаря этим данным злоумышленники смогут попытаться узнать номера Вашего паспорта, страхового и пенсионного свидетельства, и других документов. В дальнейшем они могут использовать эту информацию в мошеннических целях. Кроме того, это подарок для педофила – введи в поисковик возраст и получи список потенциальных жертв. Если Вы боитесь, что кто-то забудет Ваш день рождения, то указывайте день и месяц.
4. ***Номер телефона*.** Различные мошенники с радостью воспользуются предоставленным в соцсетях номером телефона, не скрытым настройками приватности. Помимо того, что у многих пользователей банковские карты привязаны к телефонным номерам, рекламодатели также с удовольствием воспользуются Вашим номером. На оставленный в открытом доступе номер телефона может сыпаться «спам» или, например, сообщения от мошенников с требованием оплаты несуществующих кредитов.
5. ***Данные об отношениях*.** Встречаетесь Вы с кем-нибудь, находитесь в браке или в Ваших отношениях «все сложно» - не стоит выставлять эту личную информацию на ресурсах общего пользования. Статус, в соцсетях, раскрывающий информацию о Ваших отношениях, может также притягивать киберпреступников. Существует немало примеров, как доверчивые пользователи попадались в сети на удочку мошенников, получавших в приватной беседе данные личного характера (адрес, номер телефона или откровенные фотографии), которая в дальнейшем использовалась для шантажа.
6. ***Содержание личных фото и видео*.** Возможно, у Вас на фото случайно (или нет) засветился Ваш телефон с Вашим номером. Или Вы, находясь в хорошем расположении духа, решили опубликовать фото Вашего билета на футбольный матч, концерт или российского или заграничного паспорта. В идеале, совсем не стоит выкладывать свои фото и видео в сеть, но, если Вы считаете, что Вам нечего скрывать, то потратьте пару минут, чтобы проверить фото и затереть через редактор какие-то данные, которые смогут стать пищей для злоумышленника. Лучше публиковать в интернете только такие фотографии, которые могут быть представлены широкой публике, понимая что их могут увидеть родители или работадатели.
7. ***Информация о своих планах*.** Зачастую люди оставляют в сети информацию о своих планах уехать в отпуск или фиксируют все свои передвижения. А если накануне Вы похвастались дорогими приобретениями - новеньким телефоном, дорогой техникой или ювелирными украшениями в социальных сетях, то всё это может послужить приманкой для преступников, которые в Ваше отсутствие могут взломать квартиру или гараж.
8. ***Окружение*.** «Скажи мне, кто твой друг и я скажу, кто ты» - это фраза применима не только в реальной жизни, но и к виртуальной. По окружению человека в сетях можно многое понять. И даже если он скрывает свою личность и не публикует информацию, по качеству друзей и подписчиков Вы можете сделать определенные выводы – место проживание, учебы, работы, предполагаемый возраст и т.п.
9. ***Фото своих детей*.** Больше всего экспертов по интернет-безопасности беспокоит всеобщее размещение детских фотографий в интернете. Конечно, родители любят и гордятся своими детьми, но нельзя выставлять детские фото в открытом доступе. Они могут быть использованы для неблаговидных целей. Особенно это касается фотографий совсем маленьких голеньких младенцев.
10. ***Личные обращения на своей странице*.** Несмотря на то, что личные обращения ускоряют процесс поиска жилья, работы, соседей по квартире, однако не стоит делать это слишком широко. В данном случае подойдет два сценария действий. Первый – дать объявление только для своих друзей, второй – дать объявление в специализированной группе анонимно, чтобы в дальнейшем просмотреть откликнувшихся по лайкам, комментариям и репостам.

Если Вы думаете, что в сети «особенные» люди всегда очевидны, потому что у них стоит только одно фото, и очевидно украденное у какой-то модели, то Вы ошибаетесь. Злоумышленники запросто создают копии других реальных людей в социальных сетях. Также запросто они взламывают или покупают страницы других людей.

**Блок 2. Демонстрация видео**

|  |  |  |
| --- | --- | --- |
| **Платформа** | **Ссылка на материал** | **Тип материала** |
| Youtube | [**https://www.youtube.com/watch?v=uAL2rroE3jw**](https://www.youtube.com/watch?v=uAL2rroE3jw) | Оригинальное видео |

Сначала преподаватель демонстрирует видео на YouTube. На примере видео объясняет какие мошеннические схемы наиболее распространены в сети.

**Блок 3. Групповая работа: поиск схем мошенничества в интернете**

Учащиеся произвольно делятся на группы. Используя интернет, они ищут описание различных мошеннических схем в интернете и их конкретные примеры.

Каждая группа должна найти по 2 схемы в одной из тем:

1. Мошенничество с картами
2. Мошенничество интернет-магазинов
3. Мошенничество с телефоном
4. Мошенничество с выигрышами в конкурсах
5. Мошенничество с бесплатными услугами

На сбор примеров дается 10 минут.

Следующие 10 минут отводятся на доклад от каждой группы об обнаруженных ими схемах мошенничества.

**Блок 4. Подведение итогов.**

Что установлено?

Становились ли вы жертвой мошенничества?

Какая из схем мошенничества, по-вашему, наиболее сложная для распознавания и почему?

**Блок 5. Теоретическая часть.**

**Как злоумышленники могут навредить в социальных медиа**

1. ***Украсть личные данные*.** Если Вы на своей странице в социальной сети выкладываете подробную информацию о себе, прикрепляя все это своими фотографиями, то злоумышленники легко могут украсть Вашу личность, создав фейковую страницу от Вашего имени.
2. ***Вовлечь в мошенническую схему*. Е**сли Вы выкладываете Ваши фотографии или сканы документов, подтверждающих личность, то рискуете стать жертвой злоумышленников. При определенных обстоятельствах с помощью этой информации можно оформить кредит в банке, выполнить махинации в интернете, зарегистрировать фирму и осуществить другие незаконные действия.
3. ***Похитить деньги, выманить деньги*.** Это может быть реализовано как на основе личных данных (если Вы выкладываете в открытый доступ информацию о своей банковской карте), так и через друзей.
4. ***Кибербулинг*** (унижение или травля в Интернете). Можно стать жертвой травли в сети, на основе личных данных. Например, пользователи сети смогут сделать скрин Вашей страницы и выставить ее в какой-нибудь группе под названием «стиль улиц», где 10000 подписчиков будет обсуждать, как Вы безвкусно одеты, и как в таком виде можно появляться на людях.
5. ***Шантаж*.** На основе Ваших личных данных человек, может с Вами общаться долгое время, а потом начать Вас шантажировать, что выложит о Вас какую-либо информацию. Кроме того, человек может просто обманывать Вас, на самом деле, не владея никакой информацией.
6. ***Похищение*.** Если на своей странице Вы указываете геолокацию или Ваш постоянный маршрут, назначаете неизвестному человеку встречу, то Вы можете стать жертвой.
7. ***Нападение*.** Указывая свою геолокацию, Ваш обычный маршрут и, выставляя фотографии недавно купленных дорогих вещей, то Вы рискуете стать жертвой нападения.
8. ***Манипулирование сознанием*.** Различными способами манипулирования люди пытаются продать вещь, заманить на мероприятия или вечеринки, или даже использовать в политических движениях.
9. ***Вовлечение в деструктивные движения*.** Вовлекаются с различными целями, но имеют разрушительные последствия для самого человека.
10. ***Другое*.** Различные специфические ситуации, которые могут придумать злоумышленники.

**Блок 6. Групповая работа: анализ аккаунтов и выявление копий аккаунтов в социальных медиа, созданных мошенниками.**

Студенты произвольна делятся на группы. Сформированные группы выбирают себе любую публичную персону (Например: К.Собчак, А.Аршавин, Нюша, Тимати и т.п.).

Используя социальные сети: ВКонтакте, Фейсбук, Инстаграм, Одноклассники, Твиттер, группы ищут все аккаунты, позиционирующие себя как данная публичная персона. Совместно с преподавателем группы выявляют тот аккаунт, который с большей долей вероятности является истинным/оригинальным.

**Для выполнения задания можно воспользоваться признаками фейковых аккаунтов:**

1. Большинство записей на стене сделано в один временной промежуток (от 1 до 3 дней подряд);
2. Большое количество подписок на группы (более 400);
3. Большое количество друзей (более 400), при условии, что количество подписчиков значительно меньше, чем друзей;
4. Малое количество фотографий, при этом большинство фотографий однотипные (чаще портретные);
5. Все фотографии добавлены примерно в одно время;
6. Люди, изображенные на фотографиях пользователя, отсутствуют в его друзьях;
7. В списке друзей много заблокированных или удаленных (собачек);
8. У аккаунта много спама на стене от него самого или от его друзей;
9. Суммарно малое количество медиафайлов (аудио, видео);
10. Отсутствие подарков. У реальных пользователей, как правило, имеется несколько подарков;
11. Интересы слишком однотипны, или абсолютно разнообразны. Т.е. либо человек интересуется только парой тем и ничем больше, либо в огромном количестве интересов невозможно выделить хотя бы два преобладающих интереса.

**Блок 7. Подведение итогов исследования**

Что установлено?

Много ли фейков существует в сети?

Зачем кто-то притворяется другим человеком?

Вели ли когда-нибудь аккаунт, в котором представлялись другим человеком?

**Блок 8. Итоговая рефлексия**

Что вы узнали сегодня?

Какие опасности запомнились вам более прочих?

Какие еще способы защиты персональных данных можно ввести?

**Занятие 2. Правила безопасного обращения с персональными данными в социальных медиа**

План занятия:

|  |  |  |
| --- | --- | --- |
| Номер блока | Продолжи- тельность, мин | Описание учебной работы |
| 1 | 20 | Теоретический блок: Правила обращения с персональной информацией в сети |
| 2 | 20 | Индивидуальная практическая работа: изучить собственный аккаунт на признаки уязвимости опасностям |
| 3 | 5 | Подведение итогов исследования |
|  | *10* | *перемена* |
| 4 | 20 | Теоретический блок: как вычислить злоумышленника |
| 5 | 10 | Групповая работа: обнаружь злоумышленника. Открыть произвольные аккаунты и проверить их на соответствие признакам риска |
| 6 | 10 | Подведение итогов исследования |
| 7 | 5 | Итоговая рефлексия по занятию |
|  | 45+45 |  |

**Блок 1. Теоретическая часть.**

**Правила поведения в социальных сетях напрямую вытекают из опасностей:**

**1. *Не стоит публиковать геолокацию*.** Избегать указания точных адресов и названий мест. Не следует называть места, которые вы посещаете или собираетесь посетить, рассказывать о маршрутах передвижения. Малознакомым и незнакомым людям ни при каких обстоятельствах не передавать свой точный адрес (передача адреса интернет-магазину для доставки – на ваш страх и риск).

**2. *Не указывать свое место работы и учебы*,** если в этом нет необходимости. Несмотря на то, что это является важным показателем для тех, кто анализирует вашу страницу, для вас лично это снижает степень Вашей безопасности.

**3.** Поменьше распространяйтесь ***о своей личной жизни*** и не раскрывайте личной информации своих близких. Не публикуйте фото своих новорожденных племянников, никаких фото на фоне дома вашей мамы и т.п.

**4. *Возраст.*** Наименьшее из зол. Но, зная ваш возраст, на вас намного проще найти подробную информацию.

**5**. В идеале, совсем ***не стоит выкладывать свои фото и видео в сеть*,** но, если Вам очень хочется это сделать, то потратьте пару минут, чтобы проверить фото и затереть через редактор какие-то данные, которые смогут стать пищей для злоумышленника. Не забывайте затереть лица тех людей, о чьей безопасности вы беспокоитесь.

**6.** Несмотря на то, что ***личные обращения*** ускоряют процесс поиска жилья, работы, соседей по квартире, однако не стоит делать это слишком широко. В данном случае подойдет два сценария действий. Первый – дать объявление только для своих друзей, второй – дать объявление в специализированной группе анонимно, чтобы в дальнейшем просмотреть откликнувшихся по лайкам, комментариям и репостам.

**7.** Не отправлять ***копию (скрин) паспорта документов*** в социальных сетях малознакомым людям.

**8.** Не отправлять ***данные своей банковской карты*** на обратной стороне.

**9.** Обращайте внимание на ***ссылки, которые сбрасывают вам ваши друзья и особенно незнакомые люди.*** Подозрения должны вызвать те ссылки, которые состоят из адресов сервисов для сокращения линков: goo.gl, bit.ly и другие. Но тем не менее, даже если ссылка вроде как ведет на страницу внутри самой соц. сети, в которой происходит общение, необходимо к ней приглядеться пристальнее: может оказаться так, что вместо адреса odnoklassniki.ru там будет написано что-то вроде odnok1assniki.ru, и кликнув по ней, вы заразите свой компьютер кейлогером или трояном.

**10. *Информация, порочащая других людей или группу лиц*.** Публичные оскорбительные высказывания в адрес другого человека караются законом. То же самое относится к клевете, распространению заведомо ложных сведений, порочащих честь и достоинство, наносящих урон деловой репутации и т.д. Поэтому не пишите ничего «сгоряча» и старайтесь выяснять отношения при личном общении. Также не следует бездумно копировать на свою страницу информацию, порочащую какого-либо человека или организацию, поскольку это может оказаться клеветой.

**Блок 2. Индивидуальная практическая работа: изучить собственный аккаунт на признаки уязвимости опасностям**

Каждый из учеников самостоятельно открывает свой аккаунт в любой социальной сети, а также аккаунты 2х своих ближайших друзей.

При анализе своего аккаунта, ученики должны обнаружить уязвимости собственного аккаунта для злоумышленников. Есть ли какие-то файлы, соответствующие перечисленным в теоретической части опасностям.

Такой же проверке на уязвимости подвергаются аккаунты 2х ближайших друзей.

**Блок 3. Подведение итогов исследования**

Какие уязвимости вы обнаружили?

Как злоумышленник может воспользоваться данными уязвимостями?

Как, по-вашему, можно защитить данные уязвимости?

**Блок 4. Теоретический блок. Как вычислить злоумышленника**

1. ***Просит Ваши личные данные*.** Если незнакомый или малознакомый Вам человек просит прислать копию паспорта, фотографию обратной стороны банковской карты, то это должно насторожить. Официальные организации, например, с целью трудоустройства, в социальных сетях не пишут.
2. ***Просит прислать деньги*.** Если это малознакомый или неизвестный аккаунт, или фонд помощи кого-либо, то стоит задуматься.
3. ***Манипулирует Вами.*** Если малознакомый человек Вам сначала говорит такие слова, как «срочно», «очень нужно», то это стоит оценить критически.
4. ***Слишком мало/много подписок/друзей.*** Если страница фейковая, то человек пытается создать видимость, что это не так. Именно поэтому добавляет всех подряд в друзья и публикует много записей на стене. Если у создателя страницы в социальной сети мало друзей, то возможно он создал ее с определенной целью, например, следить за кем-то, и ему не нужна никакая активность.
5. ***Максимум публикаций на стене сделаны в один временной промежуток.*** Этот и предыдущий пункты говорят лишь о том, что к таким людям следует повнимательнее присмотреться.
6. ***Нет музыки, нет видео, нет групп* (или их наоборот более 400).**
7. ***Сообщения обезличены*** (при общении оказывается, что человек не видел Вашей личной информации или фото) или другая крайность – ***он знает о Вас все.***
8. ***Представляется профессионалом определенной области и предлагает участие в уникальном проекте лично для Вас.*** Например, реклама в Вконтакте не предусматривает рассылку в личных сообщениях.

Выполнение какого-то из этих пунктов не говорит о том, что человек является злоумышленником, это говорит лишь о том, что Вас должно это насторожить, чтобы Вы были повнимательнее.

**Блок 5. Групповая работа: обнаружь злоумышленника. Открыть произвольные аккаунты и проверить их на соответствие признакам риска.**

Ученики произвольно делятся на 4 группы по возрастной группе, которая будет подвергнута исследованию:

1 – от 14 до 17

2 – от 18 до 24

3 – от 25 до 30

4 – от 31 до 40

Разделившиеся группы, используя интернет, ищут в поисковике социальной сети случайные аккаунты, соответствующие по возрасту. Затем аккаунты проверяются по признакам злоумышленников.

Выявленные аккаунты составляются списком (не менее 5), к ним составить аргументы, почему они могут быть злоумышленниками.

**Блок 6. Подведение итогов исследования**

Что удалось обнаружить?

Какие основные опасности вы обнаружили?

Очевидны ли эти опасности?

**Блок 7. Итоговая рефлексия по занятию**

Что запомнилось больше всего из сегодняшнего материала?

Видели ли вы когда-нибудь раньше злоумышленников в сети, как вы понимали, что они опасны?

На сколько уязвим ваш собственный аккаунт?

Следите ли вы за безопасностью своих данных?

Как вы ведете себя когда вам пишет незнакомец?

**Занятие 3. Правила взаимодействия со злоумышленниками. Что делать, если ваши персональные данные похищены.**

**Продолжительность:** 2 ак.ч.

План занятия:

|  |  |  |
| --- | --- | --- |
| Номер блока | Продолжи-тельность, мин | Описание учебной работы |
| 1 | 15 | Теоретический блок: Правила взаимодействия со злоумышленниками. Методы профилактики, которые позволят минимизировать риск встречи со злоумышленником в сети |
| 2 | 20 | Групповая работа. Проверка групп «Отдам даром» |
| 3 | 10 | Итоги исследования |
|  | *10* | *перемена* |
| 4 | 10 | Теоретический блок: Кто может помочь при возникновении опасности в Интернете. |
| 5 | 20 | Групповая работа. Задание «Подбор кандидатов на должности» |
| 6 | 10 | Как защитить свою виртуальную персону |
| 7 | 5 | Итоговая рефлексия по занятию |
|  | 45+45 |  |

**Блок 1. Теоретическая часть.** **Что делать если вы столкнулись со злоумышленником в социальных медиа**

Методы профилактики, способствующие защите от злоумышленников:

1. ***Не стоит публиковать геолокацию***. Избегать указания точных адресов и названий мест. Не следует называть места, которые вы посещаете или собираетесь посетить, рассказывать о маршрутах передвижения. Малознакомым и незнакомым людям ни при каких обстоятельствах не передавать свой точный адрес (передача адреса интернет-магазину для доставки – на ваш страх и риск).

2. ***Не указывать свое место работы и учебы***, если в этом нет необходимости. Несмотря на то, что это является важным показателем для тех, кто анализирует вашу страницу, для вас лично это снижает степень Вашей безопасности.

3. Поменьше распространяйтесь ***о своей личной жизни*** и не раскрывайте личной информации своих близких. Не публикуйте фото своих новорожденных племянников, никаких фото на фоне дома вашей мамы и т.п.

4. ***Возраст.*** Наименьшее из зол. Но, зная ваш возраст, на вас намного проще найти подробную информацию.

5. В идеале, совсем ***не стоит выкладывать свои фото и видео в сеть***, но, если Вам очень хочется это сделать, то потратьте пару минут, чтобы проверить фото и затереть через редактор какие-то данные, которые смогут стать пищей для злоумышленника. Не забывайте затереть лица тех людей, о чьей безопасности вы беспокоитесь.

6. Несмотря на то, что ***личные обращения*** ускоряют процесс поиска жилья, работы, соседей по квартире, однако не стоит делать это слишком широко. В данном случае подойдет два сценария действий. Первый – дать объявление только для своих друзей, второй – дать объявление в специализированной группе анонимно, чтобы в дальнейшем просмотреть откликнувшихся по лайкам, комментариям и репостам.

7. Не отправлять ***копию (скрин) паспорта документов*** в социальных сетях малознакомым людям.

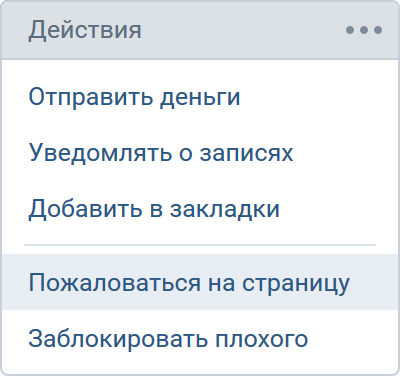
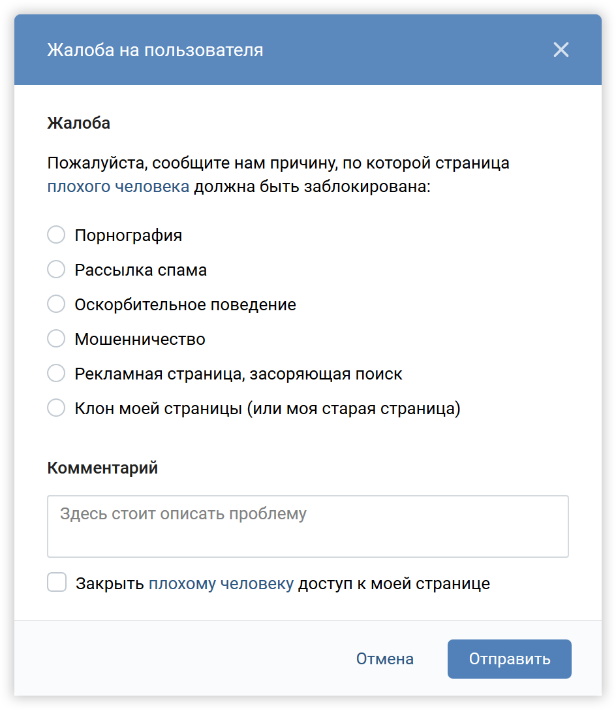
8. Не отправлять ***данные своей банковской карты*** на обратной стороне.

9. Обращайте внимание на ***ссылки, которые сбрасывают вам ваши друзья и особенно незнакомые люди****.* Подозрения должны вызвать те ссылки, которые состоят из адресов сервисов для сокращения линков: goo.gl, bit.ly и другие. Но тем не менее, даже если ссылка вроде как ведет на страницу внутри самой соц. сети, в которой происходит общение, необходимо к ней приглядеться пристальнее: может оказаться так, что вместо адреса odnoklassniki.ru там будет написано что-то вроде odnok1assniki.ru, и кликнув по ней, вы заразите свой компьютер кейлогером или трояном.

10.***Информация, порочащая других людей или группу лиц***. Публичные оскорбительные высказывания в адрес другого человека караются законом. То же самое относится к клевете, распространению заведомо ложных сведений, порочащих честь и достоинство, наносящих урон деловой репутации и т.д. Поэтому не пишите ничего «сгоряча» и старайтесь выяснять отношения при личном общении. Также не следует бездумно копировать на свою страницу информацию, порочащую какого-либо человека или организацию, поскольку это может оказаться клеветой.

**Что делать, если Вы уже столкнулись со злоумышленником**

1. Обратиться к администрации социальной сети. В обращении нужно указать ссылку, пожаловаться на нее, чтобы ее заблокировали. Сделать это не сложно. Ниже представлены скрины из социальной сети Вконтакте как это сделать.

1. На своей странице предупредить, что личные данные были похищены, что ими могут воспользоваться, будьте бдительны.



1. Если есть признаки, что какая-то мошенническая схема работает, значит, следует в этот же момент написать всем друзьям, что данные были похищены.
2. В случае если очень нужно выложить свой паспорт, визу, то следует затереть в фильтре, все важные и значимые данные (серия, номер и т. д.)
3. Если выкладывать результат своего творчества (фото и видео), то нужно делать на них свой электронный автограф (значок, ссылка на сайт, id в социальной сети и т.п.).
4. Написать заявление в полицию и приложить все скриншоты.
5. Перед тем как отправлять деньги фонду или частному лицу, проверьте:

* Детальные отчёты о поступлениях и тратах.
* Информацию о том, на что уйдут средства, а также конечную цифру сборов.
* информацию о человеке или фонде, который собирает средства.

Помимо этой информации об этом должна быть ссылка на официальный сайт. Если вы не уверены или не можете отыскать нужную информацию, задайте интересующие вопросы напрямую в фонд. Честные организации расскажут вам о себе и своей работе. Мошенники же часто создают эмоциональный шум, не предоставляя подробной информации. Списки фондов, которым можно доверять, есть на сайтах «Подари жизнь» и «Все вместе».

Обычно группы помощи животным являются не оформленной организацией, поэтому лучше сначала съездить, познакомиться и убедиться, а потом отправлять деньги.

1. Если Ваш друг просит у Вас деньги, то следует позвонить ему и спросить о произошедшем. Если вы общаетесь редко, попросите предоставить факты и номер телефона, по которому вы сможете связаться. Не переводите деньги человеку, пока не пообщаетесь с ним лично.
2. Если кто-то вымогает деньги, то следует сделать скрин переписки и написать заявление в полицию, а также не забыть пожаловаться в администрацию соц.сети.
3. Выигрыш призов или внезапное наследство. Вас попросят оплатить доставку подарка или работу юриста, который подготовит бумаги о наследстве. Чтобы раскусить мошенника, достаточно попросить доказательства о том, что выиграли именно вы, а не кто-то другой.
4. В группах «Отдам даром» участники предлагают обменять или просто подарить ненужные вещи. Чтобы получить бесплатную вещь, участник сообщества делает репост интересующей записи. После определённого времени даритель сам выбирает человека из списка поделившихся и договаривается о сделке. Отличить обман можно по следующим критериям:

* Закрытые комментарии и отсутствие подписи в объявлениях. В настоящих группах участники общаются и задают интересующие вопросы о товаре. В группах мошенников комментарии закрыты.
* Вас просят оплатить доставку. «Вещь уже ваша, нужно просто оплатить доставку», — заверяют недобросовестные дарители. В реальной жизни люди не будут заниматься доставкой ненужных им вещей.
* Передача вещей происходит не напрямую. Администрация настоящих групп в сделке не участвует, но в группах мошенников сделки происходят через гаранта. Гарант — посредник между получателем и дарителем. Он предостерегает вас о мошенничестве, а затем просит оплатить свои услуги и доставку товара. Позже гарант сообщает вам, что продавец оказался недобросовестным, и возвращает вам стоимость доставки, но стоимость своих услуг он не компенсирует.
* Мошенники используют фотографии из интернета. На всякий случай проверяйте изображения в поиске. Ниже приведен пример такого мошенничества:

1. Если Вы стали жертвой кибербулинга (унижение или травля в Интернете), то первое что нужно сделать, это понять, что Вы стали жертвой и из этого есть выход. Из этой ситуации есть несколько возможных путей выхода:

* Можно обратиться на горячую линию за помощью.
* Можно обратиться к юристу.
* Можно сразу сделать скрины и пойти в полицию.
* Если есть конкретные места где Вас травят, то Вы можете обратиться к администратору с жалобой, что Ваши личные данные распространяют, и их следует удалить. Если такого не происходит, то опять же делаете скрины и с ними к администратору соц сети.
* Можно просто перестать сидеть в сети и перейти в реальный мир.

1. В первую очередь, когда происходит угроза, следует сразу предупредить, что Вы сделали скрин и отнесете в полицию. В случае, если человек говорит, что у него есть связи в полиции, то можно сказать, что Вы обратитесь в генеральную прокуратуру, добавив скрин про связи в полиции.
2. В случае, если у кого-то есть Ваши фото и видео какого-либо характера, следует на своей странице сделать объявление о том, что Вас шантажируют фотошопом, с просьбой не обращать на это внимание. В случае, если это распространилось, можно пожаловаться администратору и отнести скрины в полицию, но лучше всего это сделать на этапе, когда Вас шантажируют.
3. Не следует встречаться с незнакомыми людьми и называть своего точного времени и места где собираетесь находиться, то же самое касается информации о Ваших близких людях.
4. Если Вы видите *признаки манипулирования сознанием*, то следует выйти из общения с этим аккаунтом, если Вам не хочется выходить, нужно сказать ему о том, что Вы видите, что Вами манипулируют.
5. *Вовлечение в деструктив*. Если Вас вовлекают (вовлекли) в деструктивное движение, самое простое это из него выйти. Если есть признаки прямого склонения к чему-либо (например, наркотики) нужно пожаловаться администрации в соц. сети или, если есть признаки нарушение законодательства, то эту информацию следует заскринить и передать службам.

**Блок 2. Групповая работа. Проверка групп «Отдам даром»**

Ученики произвольно делятся на 4 группы. Все группы работают в интернет пространстве в социальной сети Вконтакте.

Задание групп: найти группы «отдам даром», соответствующие запросу:

- 1 группа: более 10 тыс. участников;

- 2 группа: от 5 до 10 тыс. участников;

- 3 группа: от 1 до 5 тыс. участников;

- 4 группа: до 1 тыс.участников.

Каждая группа составляет список обнаруженных групп. Внутри групп «отдам даром» отбираются подозрительные сообщения. Ученики должны подготовить скриншоты и аргументы, почему они считают данные записи подозрительными.

**Блок 3. Итоги исследования**

Что удалось узнать?

Что подозрительного вы обнаружили в данных группах?

Как можно проверить безопасность данных объявлений?

**Блок 4. Кто может помочь при возникновении опасности в Интернете.**

Те, кто могут защитить тебя при возникновении опасности в Интернете:

1. Администраторы и модераторы платформы, на которой ты осуществляешь активность;

Обязанность администраторов и модераторов платформы следить за безопасностью участников общения, а также следить за соблюдением правил платформы. Большинство платформ по закону обязаны обеспечивать безопасность пользователям. Поэтому в случаях, когда вы наблюдаете нарушение закона, кто-то оскорбляет и угрожает кому-то, кто-то нарушает правила платформы; вы можете обратиться к администратору или модератору за тем, чтобы он разрешил эту ситуацию.

1. Другие пользователи платформы;

Среди пользователей есть множество людей, готовых помочь и заступиться за тех, кто подвергается опасности. Также, на различных платформах есть специальные группы, направленные на защиту различных групп пользователей. Они могут объяснить вам как вести себя в данной ситуации, лично заступиться за вас или помочь собрать доказательства для передачи в полицию.

1. Общественные защитники;

Существуют общественные организации, направленные на защиту прав пользователей интернета. Они могут объяснить вам как вести себя в данной ситуации, лично заступиться за вас или помочь собрать доказательства для передачи в полицию.

1. Полиция;
2. Уполномоченные органы;
3. Родители или взрослые, которым ты можешь доверять;

Взрослые могут знать о правилах реагирования на опасности в интернете или знать тех, к кому можно обратиться за информацией.

1. Учителя и представители администрации учебного заведения;
2. Психолог школьный, частный, при медицинском учреждении;

Психолог может знать о правилах реагирования на опасности в интернете или знать тех, к кому можно обратиться за информацией.

1. Антивирус;

Может защитить от ряда компьютерных вирусов, опасных ссылок и т.п.

1. Настройки приватности.

Настройками приватности можно отсеять доступ к аккаунту незнакомцам.

**Блок 5. Групповая работа. Задание «Подбор кандидатов на должности».**

Проанализировать аккаунты и подобрать наиболее подходящую кандидатуру на должность.

*«Учитель начальных классов»*

1. <https://vk.com/kateyka> (признаки интереса к сатанизму, кибербуллингу, алкоголю)
2. <https://vk.com/id8678030> (подходит)
3. <https://vk.com/id441174253> (17 лет)
4. <https://vk.com/id106519173> (не подходит по образованию)

*«Стюардесса»*

1. <https://vk.com/r_e_d_m_a_n> (подходит)
2. <https://vk.com/id299826820> (не подходит по возрасту)
3. <https://vk.com/o.storozhenko> (в декрете)
4. <https://vk.com/pesokpiter> (страница используется в коммерческих целях, нельзя сделать выводов о ее владельце)

*«Медсестра»*

1. <https://vk.com/nailartist_daryasemenova> (рабочая страница мастера маникюра)
2. <https://vk.com/id29854459> (признаки нарушения пищевого поведения)
3. <https://vk.com/id1700> (невозможно установить реальность пользователя)
4. <https://vk.com/venerka777> (подходит)

*«Водитель такси»*

1. <https://vk.com/a.mefed> (на фотографии пользователь разговаривает по телефону во время управления транспортным средством)
2. <https://vk.com/id532654085> (опасное вождение)
3. <https://vk.com/id640102> (подходит)
4. <https://vk.com/sheroukhov> (мастер тату, рабочая страница, нельзя сделать выводы о личности)

На что вы обращали внимание при подборе кандидатов?

Какие материалы, публикуемые пользователями, могут привлечь внимание работодателя? А какие оттолкнуть?

Почему важно поддерживать «порядок» на своей странице в социальных сетях?

**Блок 6.**

**Как защитить свою виртуальную персону:**

* не стоит переходить по подозрительным ссылкам;
* не открывать файлы, присланные незнакомыми людьми;
* уточнять у друзей, которые прислали файл, о его содержимом - есть вероятность, что аккаунт друга был взломан мошенниками;
* не устанавливать на компьютер неизвестные приложения и программы;
* не общайтесь с незнакомыми людьми в сети;
* не делитесь личной информациях в местах, где ее могут увидеть все пользователи Интернета;
* избегайте конфликтных ситуациях в сети, всегда найдутся люди, которые используют вашу конфликтность против вас;
* защищайте себя сами, не посещайте и не подписывайтесь на группы с материалами, которые способны оказать негативное влияние на психику;
* ограничьте доступ к личной информации ближайшими друзьями;
* не создавайте персону с «ворованными» фото и личной информацией;
* помните о том, что ваша информация доступна также вашим родителям, учителям, работодателям и т.п.
* будьте готовы нести ответственность за то, что вы делаете в сети.

**Блок 7. Итоговая рефлексия**

Что особенно запомнилось из сегодняшнего материала?

К кому вы готовы обратиться в случае опасности в сети?

Как вы можете защитить себя с помощью настроек приватности?

**Занятие 5. Урон репутации и правонарушения в сети**

«Свобода **одного человека заканчивается там**, где начинается свобода другого»

М. Бакунин

Продолжительность: 2 ак.ч.

План занятия:

|  |  |  |
| --- | --- | --- |
| Номер блока | Продолжи-тельность, мин | Описание учебной работы |
| 1 | 25 | Рассмотрение ситуации. Обсуждение |
| 2 | 20 | Рассмотрение ситуации. Обсуждение |
|  | *10* | *перемена* |
| 3 | 20 | Теория+обсуждение - Статья 282 УК РФ |
| 4 | 15 | Теория+обсуждение - Статья20.3 КоАП РФ |
| 5 | 10 | Итоговая рефлексия по занятию |
|  | 45+45 |  |

**Блок 1**

Преподаватель демонстрирует пост с фото (можно увеличить):



Источник фото: <https://www.newsweek.com/royal-baby-archie-harrison-danny-baker-bbc-meghan-markle-prince-harry-1420702>

**Обсуждение проблемной ситуации с учащимися:**

1. Кто изображен на фотографии?
2. К какому времени фотография относится?
3. Представленный скриншот свидетельствует о том, что фотография опубликована в соц.сети?
4. В какой?
5. С какой подписью?
6. Знаете ли вы обстоятельства, сопровождавшие эту публикацию?

**Подсказка:** фотографию разместил в своем твиттере радиоведущий ББС Дэнни Бейкер 8 мая 2019 г. В этот же день 8 мая 2019г. были опубликованы фото новорожденного правнука королевы Великобритании, мать которого является дочерью афроамериканки.

Реакция в твиттере: пост с фотографией и подписью был встречен критикой и обвинениями Дэнни Бейкера в расистских взглядах.

В ответ на критику Дэнни Бейкер разместил в твиттере сообщение с искренним извинением, что он предполагал, что это будет шутка, сравнивающая королевских особ с цирковыми животными в шикарной одежде и он никак не ожидал, что фото получит интерпретацию про обезьяну и расу. Пост с фото был им удален.

Реакция руководства ББС: несмотря на удаление фото и извинения Дэнни Бейкера 9 мая 2019 г. он был уволен с радиостанции.

**Читаем сообщение на сайте ББС:** https://www.bbc.com/russian/news-48215213

**Вопросы:**

1. Как Вы оцениваете ситуацию с размещением поста с фото и подписью в момент рождения правнука королевы Великобритании? (Возможные варианты ответов - Никак не связано с событием в королевской семье/ Шутка / Оскорбление и др. варианты)
2. Реакция руководства ББС, уволившего радиоведущего, по вашему мнению, адекватна? Чрезмерна? Почему?
3. Почему это фото с подписью пользователи сети посчитали оскорбительными, носящими характер расистских высказываний? (возможные варианты ответов - из-за событий, происходящих в это время / из-за обидных подписей (комментариев), другое…)
4. Где, по вашему мнению, грань между безобидной шуткой и оскорблением?
5. Какие особенности сетевого взаимодействия ослабляют или усиливают безобидную по мнению ее автора шутку, которая оборачивается оскорблением? (варианты ответов - массовость, скорость распространения, доступность множеству пользователей и проч….)
6. Известны ли вам подобные примеры, когда пользователь уверен, что его пост - всего лишь безобидная шутка, а в результате такой пост сопровождается серьезными проблемами?

**Блок 2**

Учащиеся знакомятся с двумя сообщениями (читают):

# В онлайн-версии газеты Известия: Супермодель Беллу Хадид обвинили в расизме за фото в Instagram

https://iz.ru/890382/2019-06-19/supermodel-bellu-khadid-obvinili-v-rasizme-za-foto-v-instagram

# На сайте ББС: Самарскую фирму оштрафовали за расовое оскорбление в рекламе

https://www.bbc.com/russian/rolling\_news/2015/09/150928\_rn\_samara\_advertisement\_insult

**Вопросы:**

1. На каком основании оштрафовали самарскую фирму за оскорбительную рекламу?
2. Почему фото Беллы Хадид в аэропорту пользователи сети посчитали оскорбительным, расистским? (возможный ответ - из-за событий, происходящих в это время / из-за обидных подписей (комментариев), из-за композиции фото, другое…)
3. Где по вашему мнению грань между безобидной шуткой/оскорблением/преступлением (нарушением закона)? (возможный ответ - зависит от того где прозвучала или размещена “шутка” - среди компании друзей или в сети интернет, кто “шутил” - физическое или юридическое лицо, контекст шутки (как в примере – размещение рекламы)…)
4. Какой совет можно дать пользователям сети, активно размещающим фото на своей странице соц.сетей (возможный ответ - перед размещением посмотреть на фото внимательно и подумать – не оскорбит ли оно чьи-либо чувства с учетом того, что станет доступно множеству пользователей сети, либо размещать свои посты для узкой группы друзей, духовные ценности и интересы которых пользователю хорошо известны)

**Блок 3**

**Теория+Обсуждение**

**Преподаватель задает вопрос учащимся:** Как вы думаете, когда, при каких обстоятельствах размещенное в сети интернет фото, либо высказывание могут быть квалифицированы как преступление?

**Ответ:** если представляет угрозу обществу

Преподаватель демонстрирует на экране (учащиеся также могут загрузить на своих компьютерах):

# Статья 282 УК РФ. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (действующая редакция).

Источник: https://www.zakonrf.info/uk/282/

1. Действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично, в том числе с использованием средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть "Интернет", лицом после его привлечения к административной ответственности за аналогичное деяние в течение одного года, -

наказываются штрафом в размере от трехсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет, либо принудительными работами на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо лишением свободы на срок от двух до пяти лет.

2. Действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично, в том числе с использованием средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть "Интернет":

а) с применением насилия или с угрозой его применения;

б) лицом с использованием своего служебного положения;

в) организованной группой, -

наказываются штрафом в размере от трехсот тысяч до шестисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет, либо принудительными работами на срок от двух до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо лишением свободы на срок от трех до шести лет.

**Задание:** ознакомиться со статьей закона, проанализировать, может ли Дэнни Бейкер быть обвинен в преступлении согласно Статье 282 УК РФ . Провести в виде обсуждения, выдвижения аргументов “за” и “против”

**Например, аргументы:**

|  |  |
| --- | --- |
| За | Против |
| Унижение достоинства человека по признакам расы? | Не возбуждал ненависть либо вражду? |
| Совершено публично, используя сеть Интернет? | … |
| … | … |

**Блок 4**

**Теория+обсуждение**

**Преподаватель задает вопрос учащимся:** что такое пропаганда?

**Ответ:** (от лат. propaganda — подлежащее распространению) — популяризация и распространение каких-либо идей…

(в самом общем смысле)

**Источник:** https://dic.academic.ru/dic.nsf/enc\_philosophy/991/%D0%9F%D0%A0%D0%9E%D0%9F%D0%90%D0%93%D0%90%D0%9D%D0%94%D0%90

Преподаватель демонстрирует на экране (учащиеся также могут загрузить на своих компьютерах):

**ст. 20.3 КоАП РФ Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены.**

Источник: <http://www.kodap.ru/razdel-2/glava-20/st-20-3-koap-rf>

СТ 20.3 КоАП РФ. Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами

1. Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами, - влечет наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей с конфискацией предмета административного правонарушения либо административный арест на срок до пятнадцати суток с конфискацией предмета административного правонарушения; на должностных лиц - от одной тысячи до четырех тысяч рублей с конфискацией предмета административного правонарушения; на юридических лиц - от десяти тысяч до пятидесяти тысяч рублей с конфискацией предмета административного правонарушения.

**Комментарий преподавателя:** Обратите внимание – фотографии, рисунки, которые пользователь может разместить в сети, перепостить могут содержать изображения “нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены” и за их размещение или репост может быть присуждено наказание.

**Вопрос учащимся:** почему?

**Ответ:** так как размещение материалов в сети интернет может быть квалифицировано как “публичное демонстрирование” и как пропаганда.

**Важно:** необходимо учитывать, что использование символики без цели пропаганды преступлением не является, например, в фильмах о Великой Отечественной войне.



**НЕ является правонарушением**

Кадр из кинофильма «17 мгновений весны». Символика использована без цели пропаганды



**Является правонарушением**

Фотография болельщиков футбольного матча. Символика на футболках используется для пропаганды собственных идей и демонстрируется публично

**Блок 5**

Итоговая рефлексия.

**Вопросы (задаются преподавателем и выводятся на экран):**

1. Является ли размещение пользователем информации в интернете (пост, репост, фото и др.):

* массовым распространением? (является)
* публичным демонстрированием? (является)
* пропагандой? (может являться)

1. Где грань между шуткой и оскорблением? От каких факторов она зависит? (контекст размещения, аудитория, композиция поста…)
2. Какие могут быть последствия такой “шутки”? (от осуждения в комментариях дургих пользователей, до урона репутации, увольнения с работы и в случае нарушения закона – наказания).
3. Если пользователь не знал, что его деяние может быть наказуемо, он освобождается от ответственности? (нет)
4. Комментарий пользователя “ раньше размещал подобные картинки на своей странице и наказаний не было, а сейчас….” – как на него можно ответить?

**Важные выводы (зафиксировать на доске):**

1. Размещение пользователем информации в интернете – пост, репост, фото – является массовым распространением, публичным демонстрированием, может быть признано пропагандой
2. Между безобидной (по мнению автора поста) шуткой и оскорблением другого человека (чувств других людей) может быть тонкая грань. Это зависит:

* от контекста (времени, когда размещена по мнению автора “шутка”)
* от аудитории, которая увидела эту “шутку” (в интернете ее могут увидеть миллионы пользователей)
* от композиции поста – фото, снабженное комментарием может приобрести иной смысл
* …других факторов

1. Последствия такой “шутки” могут быть разнообразными – от осуждения в комментариях других пользователей, до урона репутации, увольнения с работы и в случае нарушения закона – наказания.
2. Незнание закона не освобождает от ответственности. Законодательство постоянно меняется, то, что сейчас наказуемо только для юридических лиц, может стать наказуемо и для физических.