**МКОУ «Араблярская средняя общеобразовательная школа» Курахский район РД**

**Открытый урок**

**на тему:**

**«Бережное отношение к персональным данным»**

****

**Подготовил учитель информатики: Магомедов Э.К.**

**2019г.**

**Тема: Бережное отношение к персональным данным.**

**Класс: 7-11 класс**

**Цель:**повышение цифровой компетентности школьников в сфере управления персональными данными в интернете.

**Задачи:**

1. Формировать у школьников представлений о приватности и персональных данных, а также способах попадания данных в интернет и их распространения в сети.
2. Помочь осознать школьникам ценность персональных данных, последствия неосторожного обращения с информацией личного характера в интернете и необходимость ее защиты.
3. Формировать у школьников навыки управления персональными данными при работе с различными онлайн-ресурсами, приложениями и устройствами.

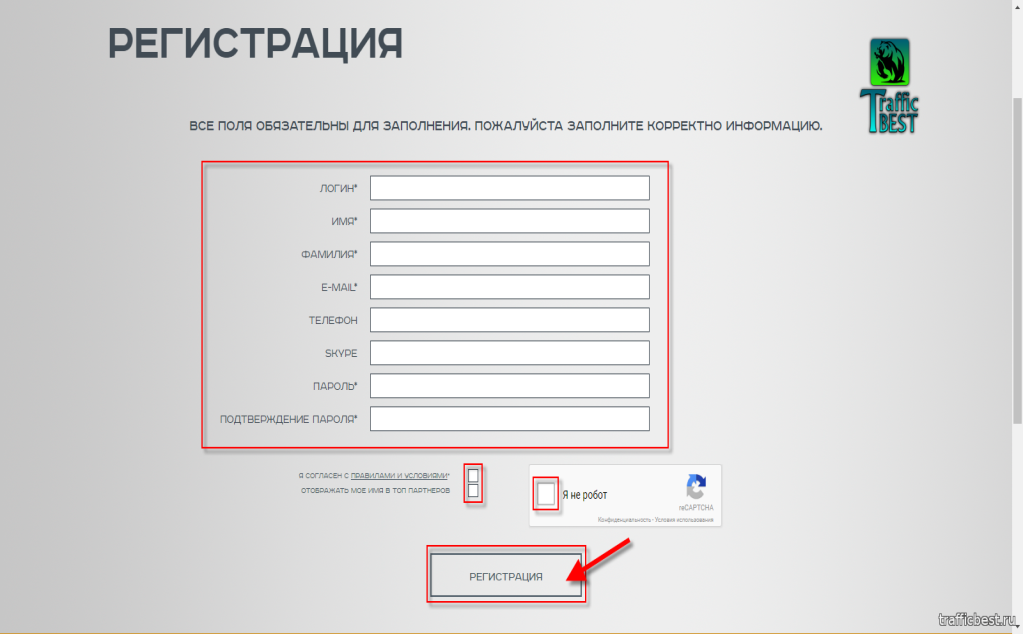
**Ход занятия**

Здравствуйте! Ребята, сегодня у нас с вами не совсем обычный урок. Для того чтобы понять о чем мы поговорим с вами, ответьте, пожалуйста, на мои вопросы:

1. Есть ли у вас страничка в социальной сети, и кто помогал вам настраивать там приватность? Что вы знаете про приватность вообще?
2. Какую информацию о себе вы сообщаете и не сообщаете незнакомым людям в интернете?
3. А вы сталкивались когда-нибудь со взломом вашего аккаунта? Что вы предприняли? Делитесь ли вы подобной информацией в интернете?

Как вы уже должны были догадаться, мы будем разговаривать о персональных данных и бережном отношении к ним.

Чтобы подробнее разобраться в этом вопросе, ведущий предлагает ученикам выполнить следующее задание: «Представьте, что в интернете появился новый популярный ресурс. Он объединяет возможности уже существующих ресурсов: социальных сетей, видеохостингов, викисред, онлайн-каналов, а также содержит новые уникальные возможности для учебы и отдыха. Большинство ваших друзей уже зарегистрированы на новом ресурсе, поэтому вам не терпится тоже туда поскорее попасть. Для этого вам всего лишь нужно заполнить простую регистрационную форму». После этого ведущий раздает ученикам формы регистрации и просит их заполнить. На выполнение этого задания отводится 5 минут. Затем ведущий собирает заполненные формы и говорит участникам группы о том, что после регистрации на ресурсе вся информация из профиля, кроме пароля, становится доступной для всех пользователей, зарегистрированных на сайте, а если профиль открыт, то и для посторонних. Что же говорит о нас информация, размещенная в профиле? Чтобы получить ответ на этот вопрос, ведущий, в случайном порядке, раздает заполненные профили участникам группы и ставит перед ними задачу: угадать, чей это профиль, и написать свою догадку на полученном листке с профилем. На выполнение этой задачи также отводится 5мин. Когда все участники выполнят задание, ведущий просит каждого по очереди озвучить логин хозяина профиля, а затем высказать и обосновать предположение по поводу его личности.



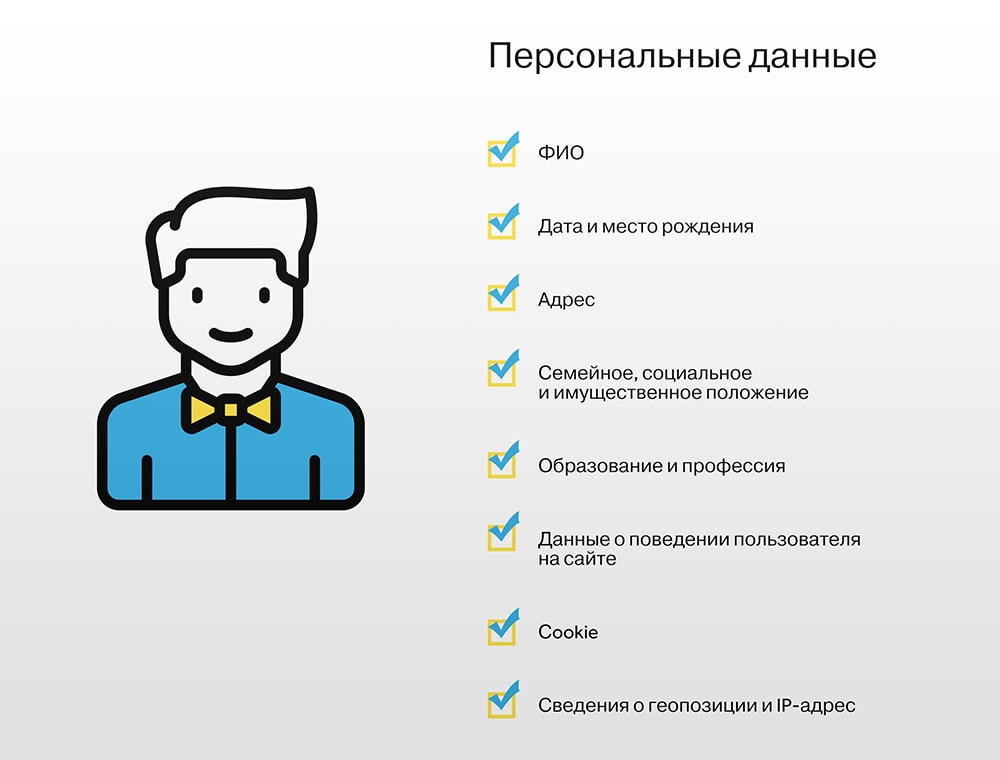
Обсуждение

• Какой профиль было угадать проще/труднее всего?

• Что помогло/помешало угадать личность хозяина профиля?

• Какими соображениями мы руководствуемся, заполняя профили?

Итак, подведем итог. Как можно было убедиться в ходе выполнения упражнения, персональные данные позволяют нам установить или идентифицировать личность человека. Чем больше информации о себе я размещаю в интернете, тем проще другим пользователям установить мою личность. Информация, размещенная нами в интернете, влияет на нашу репутацию в сети и помогает находить новых друзей со сходными увлечениями и интересами. Каждый из нас имеет право самостоятельно принимать решение о том, какую информацию о себе размещать в интернете. Ведь очень часто мошенники пользуются нашими персональными данными в преступных целях.



**Персональные данные**

Сегодня реальность во многом заменяется виртуальным миром. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

• кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;

• кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить

вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;

• с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги,

шантажировать вас и заставлять совершать какие-то действия;

• и многое другое.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.



**Кибербуллинг или киберзапугивание.**

Развитие коммуникационных технологий изменило нашу жизнь. Обычные процессы отношений между людьми с помощью Интернета, приобретают в цифровом мире новые особенности.

Скорость распространения информации в сети Интернет уже через мгновение позволяет делиться своими жизненными новостями, фотографиями и общаться с множеством людей.

Доступ к размещаемой вами информации может быть ограничен только кругом вашего общения или быть доступным неограниченному кругу лиц. Однако оборот личной информации в сети может приводить к проблемам, когда незнакомцы, прохожие или даже друзья используют информацию безответственно и без учёта права на неприкосновенность частной жизни. Так появился кибербуллинг и возможность при помощи технологий проявлять негативные качества, делать это анонимно, не опасаясь ответной реакции.

Основной площадкой кибербуллинга стали социальные сети. В них можно не только оскорблять человека в сообщениях, но и взламывать страницу жертвы или создавать поддельные страницы на имя жертвы, где размещается унизительный контент, распространяются обидные и непристойные сообщения.

Независимо от формы проявления кибербуллинг может причинить значительный вред жертве, а в крайних случаях привести к самым трагическим последствиям.



Как и их коллег – хулиганов в физическом мире, кибер-хулиганов пытаются убедить перестать нарушать права других людей. Разница в том, что кибер-хулиганы в состоянии скрыть свою личность в Интернете, что затрудняет возможность оперативного пресечения такой деятельности.

**Риски, которые влечёт обмен информацией в Интернете**

К сожалению, реальность такова, что люди выдают слишком много информации о себе в Интернете, испытывая при этом ошибочное убеждение, что принадлежащая им информация является конфиденциальной, но как только информация попадает в Сеть, контролировать ее дальнейшее использование уже практически невозможно. Кто, когда и в каких целях может воспользоваться такими данными, прогнозировать невозможно.

• В Интернете нет кнопки «Удалить», чтобы удалить информацию, размещённую в Интернете. Вы

можете пожалеть о создании, например, комментария в виде замечания по отношению к любому

человеку, потом, удалив его в течение часа, крайне удивиться, что этот комментарий уже прочитан

десятками или сотнями людей и столько же людей перенаправили его по разным адресам.

**Пример 1:**

Именинник после празднования дня рождения выложил в сеть отрицательный комментарий по поводу подарка одного из своих гостей, после чего он подвергся резкой критике со стороны других пользователей, которые в диалоге раскрывали место проведения праздника и свое отношение к нему, на именинника было оказано огромное давление, что привело его к необходимости принести публичные извинения.

• Возможно, вы осторожный и аккуратный человек, и, прежде чем, выложить фотографию или

информацию в сеть воспользовались настройками приватности. Соответственно, к информации,

которую размещаете Вы, имеет доступ ограниченный круг лиц, определённый Вами. Однако следует всегда знать и понимать, что вы не будете иметь никакого контроля в случае, когда ваши друзья скопировали информацию и распространили ее в дальнейшем, при этом, не спросив вашего мнения или разрешения.

**Пример 2:**

Девушка разместила в сети сообщение для своих онлайн друзей, где пожаловалась, что её бросил парень.

Она обвинила своего бывшего парня в том, что он применил к ней физическую силу, толкнул ее на лестнице, после чего она упала и ударилась. Её друзья по сети высказали ей слова поддержки, используя ненормативную лексику по отношению к парню. В таком контексте они обсуждали его личные данные, в том числе имя, фото, адрес проживания, при этом приводили подробности его личной жизни, не имея на это никаких оснований и подтверждений тем фактам, которые были изложены. А другие пользователи сети встали на сторону бывшего парня и решили отомстить за него, после чего разместили в сети личные данные девушки с фотографиями и сопутствующими обидными комментариями.

• Смартфоны с подключением к Интернету и высоким качеством камер стали доступными и недорогими для среднего потребителя. Пользователи смартфонов часто становятся свидетелями различных инцидентов, которые происходят в общественной жизни и моментально публикуют снятое на фото или видео в Интернете. Некоторые Интернет-форумы пользуются популярностью среди своих пользователей благодаря так называемому «мастерству раскрытия личности лиц, размещенных в онлайн-видеороликах». Даже если вы или ваши друзья оставляют в сети неструктурированную и разрозненную информацию о вас на разных сайтах, есть те кто может находить способы собирать всю имеющуюся о вас информацию без вашего ведома.

**Специальные персональные данные**

К специальным персональным данным относятся: расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

Таким образом, специальные данные характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу социальную принадлежность к определенным группам. Например, человек может сказать: я демократ или я христианин. По таким данным можно сформировать представление о человеке.

Следует заметить, что приведенный перечень персональных данных не является исчерпывающим и может включать в себя еще множество иных идентификационных данных.

**Биометрические персональные данные**

Биометрические персональные данные представляют собой сведения о наших биологических особенностях.

Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются.

Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились

считывать.



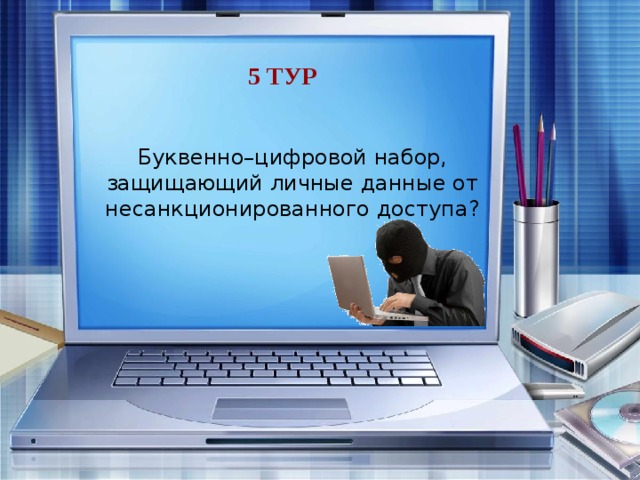
К таким данным относятся: отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.

**Набор цифр как персональные данные**

Существуют персональные данные, которые представляют собой набор цифр. Благодаря такому набору цифр нас можно определить как конкретного человека, установить нашу личность.

Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты.

Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке.



Шифрование этих данных может производиться государством. Например, когда ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию.

Шифрование может производиться банковской организацией, например, номер банковской карты тоже индивидуальный, он не повторяется и принадлежит исключительно держателю банковской карты.

**Большие данные**

Каждое наше действие, совершаемое в сети Интернет, оставляет определенный цифровой след.

Такие следы оставляет информация, которую вы добровольно размещаете в сети Интернет, например, фотографии в социальных сетях, высказывания на форумах, «лайки» новостей и многое другое.

Кроме того, цифровые следы оставляет та информация, о наличии которой вы можете и не подозревать, например, информация о посещенных сайтах, о совершенных покупках, о вашем географическом месторасположении и пр.

Если обработать всю эту информацию, то получится очень точный портрет («профайл»), который можно использовать для принятия решений в отношении конкретного человека. Например, направить ему адресную рекламу в соответствии с предпочтениями, «лайками» или отказать в поступлении на работу и пр.



Сегодня информационные технологии позволяют обрабатывать и анализировать огромные объемы данных для выявления новой информации, представляющей ценность для принятия различных решений.

Представьте себе данные о следах всех пользователей сети Интернет России или другой страны, которые они оставили за последние 10 лет.

Этот колоссальный объем информации, подлежащий обработке и анализу, получил название Big Data или Большие данные.

При этом Большие данные получают не только благодаря Вашим цифровым следам, их добывают из иных источников, например, с помощью датчиков погоды или геолокационных систем.

- На этом, я хочу завершить свой урок.