ТИПОВАЯ ПРОГРАММА ПРОВЕДЕНИЯ ВНЕКЛАССНОГО УРОКА

Тема: Защита персональных данных в сети Интернет.

Цель: - знакомство учащихся с персональными данными;
- ознакомление с правилами защиты своих персональных данных в сети Интернет.

Форма проведения: занятие.

Ход проведения урока:

1. Что такое персональные данные? Продолжительность: 5 минут.
2. Демонстрация видеороликов. Продолжительность: 5 минут.
3. Правила безопасного использования персональных данных в сети интернет. Продолжительность: 10 минут.
4. Проведение викторины. Продолжительность: 15 минут.
5. Обсуждение итогов занятия. Продолжительность: 5 минут.

1. Что такое персональные данные?

Сегодня очень много времени как взрослые, так и подростки, дети проводят в виртуальном мире. Вы (подростки, дети) знакомитесь, общаетесь и играете в Интернете; у Вас есть друзья, с которыми в настоящей жизни Вы и не встречались, но доверяете таким людям больше, чем близким. Вы выкладываете информацию о себе. Вы полагаете, что это безопасно, потому что Вы делитесь всего лишь информацией о себе и к Вашей обычной жизни вроде бы это не относится.

На самом деле 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 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. Сегодня мы рассмотрим варианты защиты своих данных. Я расскажу Вам как правильно создавать надежные пароли для своих аккаунтов, попробуем с вами создать надежные пароли, поговорим об умных вещах и расскажу о портале ПД.

Чтобы вы лучше понимали что такое персональные Роскомнадзор открыл информационно-развлекательный сайт для детей и подростков http://персональныеданные.дети, направленный на изучение вопросов, связанных с защитой прав субъектов персональных данных.

Работа сайта направлена, в первую очередь на изучение вопросов, связанных с защитой прав субъектов персональных данных.

В настоящее время на сайте представлены правила «Как защитить гаджеты от вредоносных программ», «Как общаться в Сети», «Как защитить персональные данные в сети», а также размещены интерактивные материалы (презентации, тесты, игры), объясняющие основы информационной безопасности детям, а также целью которых является закрепление прочитанного материала.

В рамках игровой формы, созданной на портале, есть и действующие персонажи, которые сопровождают посетителей Интернет-сайта во всех разделах-играх, конкурсах, тестах.

Для проверки своих знаний на портале реализована возможность прохождения тестов, который состоит всего из 8 вопросов, поэтому не займет много времени. В случае, как верно, так и неверно данного ответа посетителю будет предоставлена информация о правильном ответе после указания каждого из вариантов.

Посетив данный портал Вы будете иметь представление о том, что такое персональные данные, как правильно использовать виртуальное пространство, как и какой информацией можно делиться в Интернет-среде, какие шаги в виртуальном мире необходимо делать с осторожностью, как возможно защитить свою информацию в интернете.

Перечень данных, который можно отнести к персональным, четко не определен в законах. Поэтому набор данных, позволяющий определить или идентифицировать тебя среди множества других людей является персональными

Ты никогда не можешь знать точно, кто имеет доступ к информации, которую публикуешь на сайте. То, что ты разместишь на сайте, может повлиять на твою личную безопасность - особенно, если говоришь людям, где собираешься быть в определенное время

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

На данный момент персональные данные разделяются на:

общие;

биометрические;

специальные.

Что относится к каждому типу информации? Запомнить не так трудно.

К ***общим*** относят имя, фамилию, отчество, образование человека. Также сюда включают сведения о фактическом месте проживания, прописке. Трудоустроенные граждане (например, дети после 14-16 лет) имеют еще и данные о месте работы, заработке.

Специальная информация персонального типа - это данные, которые помогут в полной мере охарактеризовать человека. В основном то, что не относится к общему типу. Речь идет о расовой и половой принадлежности, политических и религиозных взглядах. Помимо всего прочего, сюда относят медицинские заключения о состоянии здоровья.

Биометрические данные, как нетрудно догадаться, - это не что иное, как биологические материалы, служащие для идентификации гражданина. У каждого человека это ДНК, радужка глаз, а также данные о росте и весе. Сюда относят еще фотографии и видеоролики. Они тоже помогают установить личность человека.

Позже мы разберем, какие данные Вы с легкостью готовы сообщить в Интернете, а какие скроете от посторонних лиц.

2. Демонстрация роликов.

3. Правила безопасного использования персональных данных в сети интернет.

Защита персональных данных на своем устройстве

Для удаления «цифровых следов» с компьютера после работы в интернете очистите *журнал посещений* (в браузере) и *историю поисковых запросов* (в аккаунте сайта-поисковика). С помощью средств операционной системы и браузера или специализированных приложений вы можете удалить автономные веб-страницы, временные файлы из интернета, а также cookies (небольшие фрагменты данных, которые отправляются онлайн-ресурсом и хранятся на компьютере пользователя; они помогают сайтам «запоминать» пользователей и их индивидуальные предпочтения), которые также могут многое рассказать о вашей работе в сети. Все это вы сможете сделать, только если обладаете необходимыми правами (например, администратора).

Защита персональных данных на чужом устройстве

При входе в свой аккаунт с чужого устройства всегда выбирайте опцию *«чужой компьютер», «не сохранять пароль», «безопасный ввод»* и т.д. (на странице онлайн-ресурса). В этом случае вы можете быть уверены, что никто не войдет в ваш аккаунт после вас.

Чтобы не оставить цифровых следов на чужом устройстве, используйте режим *инкогнито* (в браузере). Благодаря ему история поисковых запросов и посещенных страниц не сохраняется в браузере, а сайты не загружают cookies на устройство.

Осторожно, онлайн-мошенники!

Прежде чем вводить свои персональные данные в интернете, необходимо убедиться, что вы находитесь именно на том ресурсе, на который хотели попасть, а не на поддельной (фишинговой) странице, созданной мошенниками.

Существует несколько простых способов убедиться в подлинности ресурса:

Всегда обращайте внимание *на адресную строку браузера*.

Адрес поддельной странички может отличаться всего на одну букву, которую легко не заметить, например: в адресе www.odnoklassniki.ru может быть пропущена всего одна буква «s», но это будет уже совсем другой сайт.

Не стоит переходить на ресурсы *по ссылкам*, которые вы получили по электронной почте или в личной переписке и которые требуют *ввода персональных данных* — многие из них ведут на поддельные сайты. Забейте адрес в адресную строку самостоятельно, а еще лучше — используйте для поиска нужных ресурсов надежные поисковые системы, например, Яндекс.

Прежде чем вводить персональные данные в интернете, убедитесь, что ресурс, на котором вы находитесь, использует *защищенное соединение*. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры *https://* вместо привычной *http://*, то такое соединение использует шифрование при передаче ваших персональных данных. В этом случае злоумышленникам будет гораздо сложнее перехватить ваши персональные данные и воспользоваться ими.

Комплексные *антивирусные программы* также могут помочь защититься от мошенников. Многие из них содержат базы данных опасных и ненадежных ресурсов и способны предупреждать о возможной опасности, блокируя переход по фишинговым ссылкам. Следует помнить о том, что только одновременное соблюдение всех этих правил может надежно защитить от мошенников.

Защита персональных данных от третьих лиц

Используя вкладку *«настройки приватности»* (на странице онлайн-ресурса), запретите другим пользователям отмечать вас на фотографиях и упоминать в постах. Ограничьте круг лиц, которые могут комментировать ваши записи. Как правило, добавление пользователя в *«черный список»* автоматически лишает его возможности просматривать и комментировать ваши посты, а также упоминать вас в своих постах.

Если другой пользователь использует ваши персональные данные, например фотографии, без вашего согласия, вы можете пожаловаться в *службу поддержки ресурса* (на странице онлайн-ресурса), приложив доказательства нарушения. Если другой пользователь, разместив недостоверную или устаревшую информацию, нанес существенный урон вашим чести и достоинству, вы можете обратиться в суд.

4. Проведение викторины.

Викторина 1: Что такое персональные данные?

Проверим Ваши знания об Интернете: насколько хорошо вам знакомы различные онлайн-ресурсы:

ВОПРОСЫ ВИКТОРИНЫ:

1) **Instagram (**всего за один месяц со своего старта этот сервис набрал более 1 000 000 пользователей**) Подсказка: это сервис быстрого обмена фотографиями и видеозаписями.**
2) **Facebook (**В Австралии повестка в суд, размещенная на странице пользователя этого ресурса, является юридически обязательной**) Подсказка: Сегодня этот ресурс-крупнейшая в мире социальная сеть.**
3) **ВКонтакте** (Этот ресурс начинался как закрытое приложение к форуму СПбГУ). Подсказка: Сегодня это самая популярная социальная сеть в России.
4) **Яндекс (**Слоганом одной из рекламных компаний этого ресурса была фраза «Найдется всё»**) Подсказка: Этот ресурс является четвертым по популярности поисковиком в мире.**
5) **YouTube (**Если бы этот ресурс был голливудской кинокомпанией, у него было бы достаточно материала для выпуска 60 000 новых фильмов каждую неделю) **Подсказка: Для просмотра всех роликов, размещенных на этом ресурсе, понадобится 1700 лет.**
6) **Whatsapp (**Это приложение позволяет пользователям смартфонов бесплатно обмениваться мгновенными сообщениями**) Подсказка: название это ресурса созвучно с фразой, которая переводится как «Что происходит?»**

ОБСУЖДЕНИЕ ВОПРОСОВ ВИКТОРИНЫ:

- *Какие факты больше всего удивили вас?*
- *Что объединяет все отгаданные онлайн-ресурсы? (обмен информации, сбор информации) для получения полного доступа ко всем возможностям этих сайтов на них обязательно необходимо зарегистрироваться.*

Викторина 2: Мой профиль.

Как мы уже сказали, что все сайты объединяет то, что **для получения полного доступа ко всем возможностям этих сайтов на них обязательно необходимо зарегистрироваться.**

Наверняка процедура регистрации хорошо вам всем знакома. Как правило, она предполагает заполнение регистрационной формы или профиля.

Вызываются 2 девочки и 2 мальчика.

«Представьте, что в Интернете появился новый популярный ресурс - он объединяет возможности уже существующих ресурсов: социальных сетей, видеохостингов, онлайн-каналов, а также содержит новые, уникальные возможности для учебы и отдыха. Большинство ваших друзей уже зарегистрировано на новом ресурсе, поэтому и вам не терпится тоже туда поскорее попасть. Для этого вам всего лишь нужно заполнить простую регистрационную форму» (дается 5 минут для заполнения форм).

Создание учетной записи

Логин*	
Пол*	Мужской Женский
Возраст*	
Электронная почта*	
Номер мобильного телефона	+7 (___)_____-_____-_____
Пароль*	
Страна	
Город	
Семейной положение	
Skype	
Место работы/учебы	
Интересы	
Любимая музыка	
Любимые кинофильмы	

Создать учетную запись

Итак, форма заполнена и теперь вся информация из профиля, кроме пароля, становится доступной для всех пользователей, зарегистрированных на сайте, а иногда и для посторонних.

Угадайте, чей это профиль? (раздает первый, второй и т.д.)

ОБСУЖДЕНИЕ ВОПРОСОВ ВИКТОРИНЫ:

- *Какой профиль было угадать проще/тяжелее?*
- *Что помешало/помогло угадать личность хозяина профиля?*
- *Какими соображениями вы руководствовались, заполняя форму?*

Итоги викторины:

Итак, теперь вы знаете и должны понимать, что информация, размещенная в профилях, называется персональными данными.

Персональные данные - это любая информация, которая имеет отношение к конкретному человеку.

Как можно было убедиться в ходе упражнения, персональные данные позволяют нам установить или идентифицировать личность человека. Чем больше информации о себе мы размещаем в Интернете, тем проще другим пользователям установить личность. Информация, размещенная нами в Интернете, влияет на нашу репутацию в Сети и помогает находить новых друзей со сходными увлечениями и интересами.

Викторина 3: Информационный светофор.

Каждый из нас сам принимает решение, какую персональную информацию выкладывать в Интернете, а какую нет.

Подумайте и ответьте: какую информацию о себе вы с легкостью готовы выложить в Интернет для всех (имя, возраст, пол и т.д.), а какой бы информацией вы ни за что не поделились (номер телефона, адрес, вес)?

ВИДЫ ПЕРСОНАЛЬНЫХ ДАННЫХ:

1) **Регистрационные идентификационные данные (**паспортные данные, пароли, пин-коды)

2) **Физические характеристики (**внешние данные, биометрические данные, состояние здоровья)

3) **Пространственная локализация (**фиксация местоположения, перемещения**)**

4) **Материально-экономическое положение (**движимое, недвижимое имущество, зарплата, накопления и т.д.**)**

5) **Официальные статусы (**семейное положение, достижение, награды, наличие судимостей и т.д.)

6) **Профессиональная занятость (**включая образование**)**

7) Социальные связи (информация о родственниках, друзьях, знакомых, принадлежность к любым группам**)**

8) **Образ жизни и поведенческие установки (**мировоззрение, ценности, интересы и хобби, привычки, вкусы)

9) **Психологические особенности (**черты характера, знания, способности, умения, навыки)

10) **Хроника личных событий**

ОБСУЖДЕНИЕ ВОПРОСОВ ВИКТОРИНЫ:

- Какой вид информации набрал больше голосов, а какой меньше?
- Какой вы готовы делиться более/менее охотно? Почему?

Викторина 4: Как защитить персональные данные.

В сети Интернет нужно использовать надежный пароль.

Прежде чем я расскажу вам о признаках надежного пароля давайте поговорим о **10 самых популярных паролях среди пользователей Интернет:**

1) PASSWORD или слово ПАРОЛЬ написанный латиницей
2) QWERTY и другие варианты раскладки клавиатуры
3) Простые числовые последовательности (12345.., 87654.., 111111…и т.д.)
4) Сочетание простых числовых и буквенных символов (абвг1234, аааа1111 и т.д.)
5) Сочетание личных имен собственных (имя, фамилия) и значимых чисел (года рождения, номера телефона) САША2000, ИВАНОВ2001
6) Популярный молодежный сленг (ФИТОНЯШКА, ОЛОЛО и тд.)
7) Популярные виды спорта (ХОККЕЙ)
8) Популярные имена (Анастасия, виктория)

ПРИЗНАКИ НАДЕЖНОГО ПАРОЛЯ:

- ✓ Он должен состоять из 8-16 символов
- ✓ Включать в себя буквы, цифры и специальные символы

- ✓ Включать в себя символы в верхнем и нижнем регистре
- ✓ Не следует использовать слова, словосочетания, а также комбинации, которые можно легко угадать
- ✓ Целесообразно использовать двухэтапную аутентификацию с помощью мобильного телефона
- ✓ Для каждого аккаунта необходимо иметь свой пароль
- ✓ Необходимо менять пароли ко всем аккаунтам раз в 3-6 месяцев
- ✓ При столкновении с попыткой взлома одного из аккаунтов, необходимо поменять пароли на всех аккаунтах

СПОСОБЫ СОСТАВЛЕНИЯ НАДЕЖНОГО ПАРОЛЯ:

Для получения сложного , но легко запоминающегося пароля можно использовать любое слово, зашифровав его с помощью одного из следующих методов:

ТРАНСЛИТЕРАЦИЯ: Если взять любое слово русского языка и набрать его на латинской раскладке, то получится бессмысленное сочетание символов.

СМЕЩЕНИЕ ПО КЛАВИАТУРЕ: Если при написании слова каждый раз смещаться по клавиатуре на одну клавишу влево, мы используем «простое смещение». Если менять направление смещения по или против часовой стрелки, мы используем «сложное смещение».

ИЗВЕСТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ: например, использовать первые буквы двенадцати месяцев года.

ЧЕРЕДОВАНИЕ СИМВОЛОВ: Любой пароль можно усложнить, добавив последовательность цифр или знаков, которые можно чередовать с зашифрованным словом. Например, П1А2Р3О4Л5Ь6

Можно также усложнить пароль путем: пишем ПАРОЛЬ на английской раскладке, добавляем через букву цифры, но в обратном порядке.

5. Обсуждение итогов занятия.

Существует много каналов, по которым наши персональные данные попадают в Интернет. Что-то выкладываем мы сами, что-то пишут о нас наши друзья и знакомые, определенную информацию собирают приложения и онлайн-ресурсы. Все наши «цифровые следы» хранятся в наших компьютерах и смартфонах. Если мы хотим сохранить определенный уровень конфиденциальности и хорошую репутацию в сети, эти «следы» необходимо контролировать. Важно знать, что «цифровые следы» также хранятся на серверах разработчиков приложений и онлайн-ресурсов и удалить их оттуда практически невозможно. Поэтому всегда нужно крайне

внимательно относиться к той информации, которую мы выкладываем в сеть, а также к тому, что мы делаем в интернете: какие ресурсы посещаем, какие файлы скачиваем, какие делаем поисковые запросы и т.д.

На первый взгляд может показаться, что отдельные «цифровые следы» не представляют угрозы для нашей конфиденциальности. Например, многое ли можно узнать о человеке по его хобби или гастрономическим предпочтениям? Однако важно понимать, что в интернете потоки персональных данных объединяются друг с другом. В целом такая обобщенная информация может дать достаточно полное представление о человеке. Современные технические средства легко позволяют объединить «цифровые следы» одного пользователя в единый портрет или профайл и идентифицировать его. Существуют сайты, которые специально собирают информацию о пользователях в коммерческих целях, например, для рекламы, маркетинговых исследований. Всегда нужно помнить о том, что практически любое наше действие в интернете оставляет после себя неизгладимый «цифровой след», и по возможности стремиться контролировать свои персональные данные, попадающие в сеть.