План-конспект занятия
Персональные данные и личная информация. Защита персональных данных в сети Интернет.

Тема занятия: Защита персональных данных и личной информации в сети Интернет»
Целевая аудитория: школьники в возрасте от 9 до 11 лет.
Цель занятия: ознакомление учащихся с понятием "персональные данные", формирование теоретических знаний и практических навыков безопасного поведения в сети Интернет.
Задачи занятия:
образовательные: формирование устойчивых знаний по теме «персональные данные».
развивающие: развитие коммуникационной компетенции, навыков индивидуальной практической деятельности.
воспитательные: формирование ответственного отношения к персональным данным и личной информации.
Тип занятия: изучение нового материала, обобщение и систематизация знаний.
Форма деятельности: фронтальная.
Методы обучения: словесно-визуальный.
Оборудование: проектор, проекционный экран, персональный компьютер.

Ход урока:

Организационный этап (1 мин.): приветствие обучающихся, концентрация внимания обучающихся, определение их собранности и готовности к уроку.

Объявление темы и целей урока
Актуализация знаний } **(5 мин.):**

Наш классный час хотелось бы начать с такого стихотворения, давайте прочитаем:

Как узнать про все на свете?
Ну конечно, в Интернете!
Там музеи, книги, игры,
Музыка, живые тигры!
Можно все, друзья, найти
В этой сказочной сети!

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения

и развития. Интернет – это безграничный мир информации. Здесь вы найдете много интересного и полезного для учёбы, в Интернете можно общаться со знакомыми и даже заводить друзей.

Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них - дети, которые могут не знать об опасностях мировой паутины. Интернет - это не только кладезь возможностей, но и источник угроз.

Таким образом, кроме хорошего, в виртуальном мире есть и плохое. Неправильное поведение в Интернете может принести вред не только вам, но также вашим друзьям, родным и близким.

Сегодня по статистике 80 % школьников проводят почти три часа в день в Интернете, при этом большую часть времени проводя в социальных сетях, сообщая сведения от своих физических данных до сведений о семье и материальных возможностях.

Опрос детей, направленный на демонстрацию школьникам актуальности предложенной темы классного часа:

Поднимите руки те ребята, кто ежедневно пользуется Интернетом;

Поднимите руки те ребята, кто зарегистрирован в социальных сетях;

Поднимите руки те ребята, кто оставлял в Интернете информацию о себе, такую как фамилия, имя, отчество, дата рождения, номер телефона, фотографии и тд.

Давайте прочитаем еще одно стихотворение, и вы попробуете догадаться о чем же мы будем говорить сегодня:

Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!
Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото
В Интернет не помещай
И другим не сообщай.

Может быть, кто-то догадался, о чем мы будем сегодня беседовать? (Дети высказывают свои предположения).

Итак, сегодня тема нашего урока звучит так: "Персональные данные и их защита в сети Интернет" и для начала мы должны разобраться с Вами "а что же является персональными данными и у каждого ли человека они есть?".

Основная часть урока (24 мин.):

Этап	Действия учителя	Действия детей
Первичное усвоение новых знаний (9 мин.)	Учитель рассказывает: персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Таких идентифицирующих данных огромное множество, к ним относятся: *фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр*. Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком конкретном человеке идет речь будет невозможно. Получается, что персональные данные - это не просто ваши фамилия или имя, персональные данные - это набор данных, их совокупность, которые позволяют идентифицировать вас. ***Учитель проводит опрос детей: какие еще примеры персональных данных вы знаете?***	Дети внимательно слушают учителя. Дети перечисляют примеры известных им категорий персональных данных (Например: № школы, данные свидетельства о рождении, место

		работы, паспортные данные, данные водительского удостоверения, пол, состояние здоровья и тд. Биометрические данные: отпечатки пальцев, цвет глаз, ДНК.
	Учитель принимает ответы детей: Все верно! Учитель рассказывает: таким образом, мы можем сделать вывод, что любые сведения, по которым можно узнать человека, относятся к персональными (или личными) данными. 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 своим близким. Мы создаем своего виртуального 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 имеет никакого отношения. Однако в настоящее время информация о человеке, его персональные данные превратились в дорогой товар, который используется по-разному: • кто-то использует эти данные для того, чтобы при помощи рекламы продать какую-то	Дети внимательно слушают учителя.

	вещь; • кому-то вы можете просто не нравиться, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе; • с помощью персональных данных мошенники, воры, могут украсть деньги, шантажировать и заставлять совершать какие-то действия; • и многое другое. ***Учитель проводит опрос детей: сталкивался ли кто-то из вас с подобными ситуациями в Интернете и как вы поступили?***	Дети приводят личные примеры, делятся историями из своей жизни.
	Учитель принимает ответы детей: Совершенно верно! Вы правильно поступили! Ни в коем случае нельзя: - сообщать незнакомым людям свои личные данные; - проходить в Интернете по незнакомым ссылкам и тд.	Дети внимательно слушают учителя.
	Учитель рассказывает: сегодня в социальных сетях недоброжелатели могут не только оскорблять человека в сообщениях, но и взламывать страницу жертвы или создавать поддельные страницы на имя жертвы, где будет размещаться унизительный контент, распространяться обидные и непристойные сообщения. Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными. Наибольший процент открытых профилей	

	наблюдается у детей в возрасте от 9 до 12 лет, зарегистрировавшихся в социальных сетях, несмотря на возрастные ограничения (регистрация возможна с 14 лет). Каждый третий ребенок выкладывает информацию о себе в максимально полном объеме (ФИО, возраст, фото, № школы, № телефона, домашний адрес, интересы, хобби). Помимо того, что дети предоставляют открытый доступ к той или иной информации о себе, они нередко общаются в интернете с малознакомыми людьми и высылают информацию о себе. На первый взгляд может показаться, что сведения о наших увлечениях и интересах не будут являться персональными данными, поскольку только по этим сведениям нельзя идентифицировать конкретного человека. Однако если незнакомый человек захочет вступить с нами в контакт ему будет достаточно проанализировать наши страницы в социальных сетях, чтобы узнать увлечения и интересы и, используя полученную информацию начать разговор. Таким образом, возникает два главных вопроса: 1) как правильно распоряжаться личной информацией? 2) кому и в каком объеме можно ее предоставлять? Я не призываю вас придя сегодня домой удалить все свои аккаунты в социальных сетях или вообще перестать пользоваться Интернетом, а только хочу донести до вас простые советы, которые научат ответственнее относиться к своим личным данным и осознавать те риски, с которыми вы можете столкнуться в очередной раз блуждая по всемирной сети: 1. В первую очередь необходимо ограничить	

	объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких; 2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни; 3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает; 4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете; 5. Используйте только сложные пароли, разные для разных учетных записей и сервисов; 6. Старайтесь периодически менять пароли; 7. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее); 8. Систематически проверяйте свои домашние компьютеры на наличие вирусов; 9. Делайте резервную копию важных данных.	
Первичная проверка понимания (4 мин.)	Учитель предлагает школьникам проверить как они усвоили данную тему и задает вопросы: 1) Относятся ли такие сведения о человеке, как: фамилия, имя, отчество, домашний адрес и номер телефона к его персональным данным? *(да)*; 2) Место работы ВАШИХ родителей будет ли являться ВАШИМИ персональными	Дети внимательно слушают вопросы. Тот, кто знает правильный ответ поднимает руку и отвечает.

	данными? *(нет);* 3) Друг устраивает вечеринку в выходные, и все ваши друзья приглашены. Правильно ли будет разместить дату, время и место на сайте, потому что тогда у каждого будут детали этой встречи? *(нет);* После получения ответа от детей, учитель просит пояснить почему не стоит размещать такие сведения в общем доступе в сети Интернет? Учитель слушает мнения детей, подтверждает правильный ответ *(к этим сведениям могут иметь доступ посторонние люди);* 4) Может ли человек контролировать размещение своих фотографий в сети Интернет, если он выложил их в социальные сети? *(нет);* После получения ответа от детей, учитель просит пояснить, почему нельзя контролировать дальнейшее распространение фотографий в сети Интернет? Учитель слушает мнения детей, подтверждает правильный ответ *(они могли быть скопированы другим пользователем, до того как человек сам удалил их);* 5) Если незнакомый человек попросит вас в Интернете отправить ему ваши персональные данные, как вы поступите? *(не стану отправлять, в случае сомнения посоветуюсь с родителями или учителем).*	Дети делятся своими рассуждениями. Дети делятся своими рассуждениями. Дети делятся своими рассуждениями.

Первичное закрепление (7 мин.)	Учитель рассказывает: дети всегда были и есть самой уязвимой и незащищенной категорией граждан. В современном мире особенно хочется оградить детство, самый светлый и волшебный период жизни, от всего разрушающего: от равнодушия и жестокости, от войн и тяжелых болезней, от ненужной информации и раннего взросления. Только взрослые могут сделать детство ярким и беззаботным. Так, сотрудниками Роскомнадзора специально для детей был создан персональные данные.дети . Учитель поясняет как найти вышеуказанный ресурс в сети Интернет, используя проектор и проекционный экран, наглядно его демонстрирует, рассказывая о его содержании и возможностях *(советы детям, тесты, игры, мультимедиа, информация о конкурсах).* *При отсутствии доступа к сети Интернет, учитель демонстрирует презентацию, содержащую скриншоты страниц портала.* Учитель переходит в раздел портала *мультимедиа* по адресу: http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/multimedia/videorolik_o_zawite_detskih_personalnyh_dannyh1 и предлагает детям посмотреть видеоролик, после чего совместно обсудить действия мальчика. Учитель спрашивает детей: - Почему подобные действия, которые совершил мальчик, могут привести к таким последствиям, которые мы увидели в видеоролике. *(Правильный ответ: мальчик сфотографировал чемодан, добавил в социальную сеть фото с хэштегами, указав, что его семья уезжает на море на 2 недели, также отметил геолокацию. Злоумышленник воспользовался этими сведениями и ограбил квартиру).*	Дети внимательно слушают учителя. Дети визуально знакомятся с порталом персональныеданные.дети (внимание детей направлено на проекционный экран) Дети внимательно смотрят видеоролик. Дети принимают участие в беседе, высказывают свое мнение.

Рефлексия (подведение итогов занятия) (1 мин)	Учитель спрашивает детей: - Ребята вам понравилось занятие? - Как вы думаете, тема, о которой мы сегодня с вами беседовали, является полезной для вас? Учитель: Все верно! Мы всегда должны помнить, что необходимо грамотно и ответственно распоряжаться своими личными данными как в сети Интернет, так и в реальном мире. И если вы сомневаетесь, как правильно поступить в той или иной ситуации, когда кто-то попросил вас предоставить свои персональные данные всегда посоветуйтесь со взрослым человеком, которому доверяете.	Дети слушают вопросы учителя, все вместе дают ответы.
Ответы на вопросы (3 мин)	Учитель предлагает детям задать вопросы по теме занятия.	Дети задают вопросы.

План-конспект занятия
Персональные данные и личная информация. Защита персональных данных в сети Интернет.

Тема занятия: Защита персональных данных и личной информации в сети Интернет»
Целевая аудитория: школьники в возрасте от 12 до 14 лет.
Цель занятия: ознакомление учащихся с понятием "персональные данные", формирование теоретических знаний и практических навыков безопасного поведения в сети Интернет.
Задачи занятия:
образовательные: формирование устойчивых знаний по теме «персональные данные».
развивающие: развитие коммуникационной компетенции, навыков индивидуальной практической деятельности.
воспитательные: формирование ответственного отношения к персональным данным и личной информации.
Тип занятия: изучение нового материала, обобщение и систематизация знаний.
Форма деятельности: фронтальная, индивидуальная.
Методы обучения: словесно-визуальный.
Оборудование: проектор, проекционный экран, персональный компьютер.

План проведения урока:

1. Показ видеоурока (диск с видеозаписью прилагается) для учащихся, в котором говорится, что такое персональные данные, какие бывают персональные данные, правила защиты персональных данных, какие последствия могут возникнуть, если не соблюдать правила их защиты ***– 10 минут*.**
2. Практическая часть, которая включает в себя разбор ситуаций по вопросам защиты персональных данных и пути их решения: ***- 5 минут.***

Пример 1:

Добрый день! Меня зовут Марина, мне 14 лет. Недавно кто-то взломал мой аккаунт в «ВКонтакте» и стал размещать на моей стене неприличные изображения. А еще оскорблять от моего имени друзей в комментах и в личке. Обо всем я узнала от подруги, так как на даче, где я была, не было интернета. Я восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили меня из друзей и добавили в «черный список», а кое-кто даже перестал со мной разговаривать. Я несколько лет вела эту страницу, у меня была почти тысяча подписчиков, а теперь все пропало. Подскажите, как мне поступить? Как вернуть доверие подписчиков?

Ответ на пример 1:

В данном случае мы имеем дело со взломом аккаунта школьницы с целью нанесения вреда её репутации. В этой ситуации можно порекомендовать следующие действия:

- Сменить пароли к аккаунтам на других онлайн-ресурсах.
- Удалить все неприятные сообщения со своей страницы.
- Извиниться перед читателями написав пост.
- Постараться лично поговорить с самыми близкими друзьями и объяснить им ситуацию.

Чтобы избежать подобной проблемы, следует предпринять следующие шаги:

- Использовать сложные пароли и двухэтапную систему
- Аутентификации.
- Установить антивирусные программы на все устройства, с
- которых осуществляется выход в интернет.
- Соблюдать правила предосторожности при входе в аккаунт
- с чужого компьютера.
- Соблюдать правила поведения при столкновении с поддельными страницами.

Пример 2:

Здравствуйте! Меня зовут Настя, мне 15 лет. Недавно я познакомилась с парнем в социальной сети. Он был знакомым моей подруги и показался мне интересным. Мы стали общаться, оказалось, что у нас много общего. Мы рассказывали друг другу о себе, о том, где учимся, путешествуем. Вообще-то я скрытная, и профиль у меня только для друзей, но с ним я, кажется, позволила себе лишнего. Однажды он предложил встретиться. Я немного испугалась и отказала ему. Он сказал, что знает, где я учусь и где живу, обещал подстеречь по дороге из школы домой. Я не знаю, правда это, или он меня просто запугивает. Мне действительно страшно. Теперь одна, без подруги, я в школу не хожу. Подскажите, как мне быть?

Ответ на пример 2:

В этой ситуации можно порекомендовать следующие действия:

- Внимательно перечитать историю переписки и понять, какая персональная информация могла попасть к шантажисту.
- Внимательно изучить общие контакты и понять, какую информацию о шантажист мог узнать косвенно.
- Рассказать или показать историю переписки взрослым (родителям, учителям), чтобы они могли предпринять действия по защите школьницы, вплоть до обращения в правоохранительные органы.

- В случае если шантажист снова выйдет на связь, сообщить ему обо всех предпринятых действиях и добавить его в «чёрный список».

Чтобы избежать подобной проблемы, следует предпринять следующие шаги:

- С большой осторожностью добавлять незнакомцев в друзья и вступать с ними в переписку, даже если они являются друзьями друзей.
- Не сообщать личную информацию незнакомцам. Даже если она кажется безобидной, она может быть легко использована против жертвы.

Пример 3:

Доброго времени суток! Я Артем, учусь в 9-м классе. Однажды на уроке информатики я зашел в свой аккаунт в социальной сети и забыл выйти. Через неделю один из моих одноклассников создал паблик, в которой он выкладывает скриншоты моей личной переписки с друзьями и гадкие комментарии к ним. Там нет ничего такого, но это все равно неприятно. Надо мной все смеются. Я и раньше не был самым популярным в классе, а теперь стал настоящим изгоем. Что мне делать? Можно ли удалить этот паблик? Как наказать одноклассника?

Ответ на пример 3:

В данном случае мы имеем дело с кибербуллингом — травлей, организованной с помощью электронных средств связи.

В этой ситуации школьнику можно порекомендовать следующие действия:

•Сменить пароль от аккаунта и временно закрыть его.

•Написать в службу поддержки социальной сети письмо с просьбой удалить паблик, приложив скриншоты из самого паблика и из личной переписки, подтвердив тем самым неправомерное использование личных данных одноклассником.

•Если ситуация повторится, и после удаления будет создан новый паблик, написать в службу поддержки социальной сети письмо с просьбой удалить аккаунт пользователя, нарушившего правила пользования ресурсом.

•Рассказать о ситуации взрослым (родителям или учителям) и попросить их вмешаться в ситуацию в школе.

3. После разбора ситуаций учащимся предлагается пройти с помощью интерактивной доски тест, размещённый в сети «Интернет» по адресу: http://персональныеданные.дети/zadaniya/personalnye_dannye/ , а в случае отсутствия соответствующего оборудования раздать один тест на парту ***– 5 минут.***

Ответ на тест

1) – 4

2) – 2
3) – 2
4) – 2
5) – 2
6) – 2,3
7) – 1
8) – 1,4

4. Подведение итогов: Опрос учащихся, что нового они узнали после урока, остались ли вопросы после прослушанного материала, понравился ли урок? ***– 5 минут.***

План-конспект занятия
Персональные данные и личная информация. Защита персональных данных в сети Интернет.

Тема занятия: Медиаурок «Защита персональных данных в сети Интернет»
Целевая аудитория: школьники в возрасте от 9 до 18 лет.
Цель занятия: ознакомление учащихся с понятием "персональные данные", формирование теоретических знаний и практических навыков безопасного поведения в сети Интернет.
Задачи занятия:
образовательные: формирование устойчивых знаний по теме «персональные данные».
развивающие: развитие коммуникационной компетенции, навыков индивидуальной практической деятельности.
воспитательные: формирование ответственного отношения к персональным данным и личной информации.
Тип занятия: изучение нового материала, обобщение и систематизация знаний.
Форма деятельности: фронтальная.
Методы обучения: словесно-визуальный (ознакомления с новым материалом в форме просмотра медиаурока).
Оборудование: проектор, проекционный экран, персональный компьютер (иное оборудование, позволяющее демонстрировать аудио-видеофайлы).

Ход урока:
1. Организационный этап: приветствие, готовность к уроку.
2. Постановка темы и целей урока. Введение.
- «Персональные данные» - что такое персональные данные и какие они бывают;
- опасности в сети Интернет при использовании личной информации.

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность.
Таких идентифицирующих данных огромное множество, к ним относятся:
фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.
Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь будет невозможно.
Получается, что персональные данные - это не просто ваши фамилия или имя, персональные данные - это набор данных, их совокупность, которые позволяют идентифицировать вас.

В целом можно сказать, что персональные данные - это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.

3. Трансляция видеоролика «ВГТРК» (11 минут).

4 . После просмотра ролика обсуждение с учащимися основных тезисов и смысловых направлений видеосюжета (10 минут):

- ошибки при размещении информации в сети Интернет;
- как избежать разглашения своих персональных данных: допустимый объем информации при размещении в сети.

5. Просмотр видеоурока: кибербуллинг (5 минут) Обсуждение.

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.

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 вы хотите сохранить определенный уровень конфиденциальности и хорошую репутацию в сети, эти «следы» необходимо контролировать. Важно знать, что они

хранятся и на серверах разработчиков приложений и онлайн - ресурсов и удалить их оттуда практически невозможно. Поэтому всегда надо крайне внимательно относиться к той информации, которую вы выкладываете в сеть, а также к тому, что вы делаете в интернете, какие ресурсы посещаете, какие файлы скачиваете, какие поисковые запросы делаете.

Персональные данные, размещенные в сети Интернет самим субъектом персональных данных, становятся общедоступными, и доступ к ним получает неограниченный круг лиц. Причем в пользовательских соглашениях многих социальных сетей изначально поставлено условие согласия пользователей на общедоступность и согласие на право пользования ими третьими лицами. Поэтому, регистрируясь в социальных сетях, необходимо внимательно читать условия регистрации и правила пользования сайтом.

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.

6. Просмотр видеоурока: как защитить свои персональные данные (7 минут).

Обсуждение: как защитить гаджеты от вредоносных программ.

1. Установите на гаджеты специальные почтовые фильтры и антивирусные программы. Они могут предотвратить, как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.
3. Используйте проверенные сайты. Прежде чем вводить свои данные убедитесь, что вы находитесь именно на том ресурсе, на который хотели попасть, а не поддельный (фишинговый) странице, созданной мошенниками. Всегда обращайте внимание на адресную строку браузера. Адрес поддельной страницы может отличаться всего на одну букву, которую легко не заметить.
4. Систематически проверяйте свои домашние компьютеры на наличие вирусов.
5. Делайте резервную копию важных данных.

6. Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.
7. При использовании мобильных устройств отключайте функции, которые не нужны в данный момент времени (например: геолокация, Wi-Fi).
8. При установке приложений на мобильные устройства внимательно читайте условия пользовательского соглашения.
9. 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 лучше используйте для поиска нужных ресурсов надежные поисковые системы, например Яндекс.
10. Прежде чем вводить персональные данные в Интернете, убедитесь, что ресурс использует защищенное соединение. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры Https://

7. Заключение:

- подведение итогов: что усвоено, что нового узнали;
- вопросы учащихся по теме урока.

План-конспект занятия
Персональные данные и личная информация. Защита персональных данных в сети Интернет.

Тема занятия: Портал «Персональные данные.дети»
Целевая аудитория: школьники в возрасте от 9 до 18 лет.
Цель занятия: ознакомление учащихся с информационно-познавательным порталом «Персональные данные.дети»
Задачи занятия:
образовательные: закрепление и актуализация знаний по теме «персональные данные».
развивающие: развитие коммуникационной компетенции, навыков индивидуальной практической деятельности.
воспитательные: формирование ответственного отношения к персональным данным и личной информации.
Тип занятия: изучение нового материала.
Форма деятельности: фронтальная.
Методы обучения: словесно-визуальный (ознакомления с новым материалом в форме постраничного просмотра вебсайта).
Оборудование: проектор, проекционный экран, компьютер с доступом к сети Интернет (иное оборудование, позволяющее посещать и демонстрировать сайт в сети интернет).

Ход урока

В 2015 году Роскомнадзором для несовершеннолетних пользователей сети Интернет был запущен информационно-образовательный портал «Персональные данные. Дети», цель которого — в доступной и интересной форме объяснить детям и подросткам правила безопасного обращения с персональными данными в сети.

Информация, размещенная на данном сайте, рекомендована как для изучения в рамках уроков безопасности в сети Интернет, так и может быть изучена самостоятельно.

Знакомство с порталом следует начинать с вкладки «О проекте», где представлены те персонажи, образы которых будут использованы в играх, тестах и информационных материалах, размещенных на портале.

Первым персонажем является девочка Галя, учащаяся в гимназии вместе со своим лучшим другом Васей. У нее много друзей, с которыми она активно общается в социальных сетях, не заботясь при этом о защите информации, в том числе своих персональных данных. Галя считает, что вся информация, которую

она отправляет через Интернет, надежно защищена и попадает только к адресатам.

Вася, одноклассник Гали, - еще один персонаж портала. Вася как любой подросток активно пользуется hi-tech и всеми преимуществами, которые представляет электронный мир. Среди друзей считается продвинутым «защитником» информации. Вася неодобрительно относится к беспечности Гали и обучает её – как защитить персональные данные.

Главная задача Васи научить Галю пользоваться Интернетом безопасным для неё образом, поскольку он понимает, что такое поведение напрямую влияет на информацию о частной жизни Васи и его семьи, поскольку Галя стала его близким другом и имеет доступ к его личной информации.

Также на портале представлены еще два персонажа — Хакер и Агент. Хакер неплохо разбирается в построении компьютерных сетей и способах передачи информации. Может взломать аккаунт, чтобы использовать информацию в своих целях или продать ее.

Важно помнить, что персональные данные являются объектом хакерских атак. Хакеры-взломщики в обход систем защиты добывают конфиденциальную информацию. Они взламывают компьютеры, создают и распространяют компьютерные вирусы и вредоносные программы, в том числе целью таких действий является сбор и перехват личной информации, баз персональных данных.

Агент занимается промышленным шпионажем. Собирает информацию о нужных людях через интернет, иногда покупая ее у хакеров.

Агент является олицетворением современных транснациональных интернет корпораций. Он собирает информацию о жизни, привычках подростков для последующего агрессивного маркетинга, манипулирования сознанием.

Следующим этапом знакомства с порталом «Персональные данные. Дети» должна стать вкладка сайта «Персональные данные», содержащая определение такой категории, как персональные данные, и иных, связанных с понятием личной информации, терминов. В первую очередь дети знакомятся с самим понятием персональных данных — то есть информации о конкретном человеке, тех данных, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность.

Портал содержит разъяснение, что подобных идентифицирующих данных огромное множество (фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.).

Важно понимать, что персональные данные - это не просто фамилия или имя, персональные данные - это набор данных, их совокупность, которые позволяют идентифицировать человека.

Также, проходя по ссылке «Что такое ПДн?» несовершеннолетние знакомятся с такими понятиями как, например, кибербуллинг (киберзапугивание), основной площадкой которого являются социальные сети, в которых можно не только оскорблять человека в сообщениях, но и взламывать страницу жертвы или создавать поддельные страницы на имя другого человека, где размещается унизительный контент, распространяются обидные и непристойные сообщения.

Для большей наглядности дети могут ознакомиться с примерами кибербуллинга.

Один из примеров:

«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.»

Также на портале дети могут познакомиться такими понятиями, как:

- специальные персональные данные, к которым относится расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.;

- биометрические персональные данные, представляющие собой сведения о биологических особенностях человека, являющиеся уникальными, принадлежащими только одному человеку (отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.);

- набор цифр как персональные данные или «кодовые данные» (номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты);

- «большие данные» или Big data (то есть, те цифровые следы, которые оставляют в сети Интернет все действия его пользователей: размещенная информация в сети Интернет, высказывания на форумах, «лайки» новостей и многое другое — информация о посещенных сайтах, о совершенных покупках, о вашем географическом месторасположении и пр.).

Портал не только раскрывает понятия персональных данных и иных сопутствующих терминов. Также во вкладке «Правила» на портале «Персональные данные. Дети» содержится информация о том, как:

- защитить гаджеты от вредоносных программ;

- общаться в Сети;

- защитить персональные данные в Сети;

Кроме того, советы в данной вкладке даются и в стихах.

Итак, защитить персональные данные в Сети можно с помощью следующих действий:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.

3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.

4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.

5. Используйте только сложные пароли, разные для разных учетных записей и сервисов.

6. Старайтесь периодически менять пароли.

7. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

А защитить гаджеты от вредоносных программ возможно с помощью следующих несложных и выполнимых правил:

1. Установите на гаджеты специальные почтовые фильтры и антивирусные программы. Они могут предотвратить, как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

2. Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.

3. Используйте проверенные сайты.

4. Систематически проверяйте свои домашние компьютеры на наличие вирусов.

5. Делайте резервную копию важных данных.

6. Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.

На портале также размещены следующие Правила общения в сети:

1. Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.

2. Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем

разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.

3. Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в Интернете, тем более если вы не знаете их в реальной жизни. 4. При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений, матерных слов – читать такие высказывания так же неприятно, как и слышать.

5. Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайтесь уладить конфликты с пользователями мирным путем, переведите все в шутку или прекратите общение с агрессивными пользователями. Ни в коем случае не отвечайте на агрессию тем же способом.

6. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.

7. Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.

8. Не используйте Сеть для распространения сплетен, угроз или хулиганства.

9. С осторожностью встречайтесь в реальной жизни с онлайн-знакомыми, лучше не делать этого без разрешения родителей или в отсутствие взрослого человека. Если вы хотите встретиться с новым интернет-другом, постарайтесь пойти на встречу в сопровождении взрослого, которому вы доверяете.

На портале имеются Тесты на тему защиты персональных данных, проходя которые можно проверить свои знания о персональных данных и способах их защиты.

Во вкладке «Тесты» представлены ситуации, в которые попадают уже знакомые нам персонажи, с вариантами ответов – как стоит вести себя и поступать

Портал «Персональные данные.дети.» также содержит Игры («Лабиринт», «Найди 10 отличий») и раскраску на тему защиты персональных данных.

Игра «Найди 10 отличий» состоит в том, чтобы найти на фотографии с вечеринки 10 обидных изменений, которые внёс некий недоброжелатель,

отредактировав её, а в игре «Лабиринт» предлагается переслать сообщение от Гали к Васе, предварительно «зашифровав» его.

На портале можно посмотреть и видеоролики о защите детских персональных данных, который размещен во вкладке «Мультимедиа».

Здесь же размещены результаты конкурсов, проводимых Роскомнадзором среди учеников школ России. Во вкладке «Конкурсы» можно ознакомиться не только с их результатами, но и увидеть, какие рисунки и коллажи создали дети по теме защиты персональных данных в сети Интернет.

План-конспект занятия
Персональные данные и личная информация. Защита персональных данных в сети Интернет.

Тема занятия: Тестирование.
Целевая аудитория: школьники в возрасте от 9 до 18 лет.
Цель занятия: контроль полученных знаний.
Задачи занятия:
образовательные: закрепление знаний по теме «персональные данные».
развивающие: развитие коммуникационной компетенции, навыков индивидуальной практической деятельности.
воспитательные: формирование ответственного отношения к персональным данным и личной информации.
Тип занятия: изучение нового материала, обобщение и систематизация знаний.
Форма деятельности: фронтальная, индивидуальная.
Методы обучения: проверка знаний, умений и навыков.
Оборудование: персональный компьютер.

План урока:
1. Организационная часть (2 мин)
2. Актуализация знаний (5 мин)
3. Решение теста (20 мин)
4. Проверка теста (10 мин)
5. Подведение итогов (3 мин)

Ход урока.
1. Организационная часть. (Приветствие, проверка посещаемости).
2. Актуализация знаний.
3. Ответы на вопросы:

Что такое информация?
Какие виды информации существуют?
Какая информация относиться к личной?

Решение тестового задания.
Указать, что вопрос может содержать несколько правильных ответов.

1. Персональные данные состоят из:
1. ФИО, возраст, домашний адрес и номер телефона;
2. - Группа крови, отпечатки пальцев, медицинские диагнозы;
3. - Сведения об образовании, фотографии;
4. - Все вышеперечисленное. Персональные данные - это информация, по которой можно идентифицировать человека.

2. Можешь ли ты контролировать размещение своих фотографий в сети Интернет, если выкладываешь их в социальные сети?

1. - Да;
2. - Нет.

3. Друг устраивал вечеринку в выходные. Правильно ли будет разместить фотографии на своей странице в социальной сети, что бы все знали детали этой встречи.

1. - Да;
2. - Только если все участники дали свое согласие.

4. Какие файлы ты разместишь в социальных сетях?

1. - Все, что захочу, это смешно и интересно - моим друзьям понравится!
2. - Сначала подумаю. Буду ли я чувствовать себя комфортно, если родители, учителя увидят то, что я публикую?
3. - Фотографии, ФИО, адрес.

5. Может ли твой друг заходить в твой аккаунт и отправлять от твоего имени сообщения?

1. - Да, потому что он мой друг, и я ему доверяю
2. - Нет. Имея доступ к моему аккаунту, друг может иметь доступ не только к тем файлам, которые я разрешил смотреть, но и ко всем остальным данным.

6. При заполнении онлайн-формы для ввода данных, которые будут опубликованы, какие данные не стоит указывать

1. - Никнэйм или псевдоним;
2. - ФИО;
3. - Адрес, где ты живешь;
4. - Адрес, где ты учишься.

7. Какие последствия могут наступить, если ты отметишь друга на фото?

1. - Массовое распространение фотографии в сети, если не настроена приватность учетной записи;
2. - Никаких последствий не будет;
3. - Ничего не случится, мой друг просто станет популярнее.

8. Если у тебя есть сомнения, дать ли людям, с которыми общаешься в сети больше личной информации о себе, что ты сделаешь?

1. - Расскажешь взрослому и попросишь совет;
2. - Расскажешь другу (подруге) и попросишь совет;
3. - Отправишь личные данные и посмотришь, что будет;
4. - Не отправишь личные данные.

9. Что относится к специальным персональным данным?

1. - национальность, политические убеждения;
2. - фотография, отпечатки пальцев;
3. - паспортные данные, данные ИНН, СНИЛС.

10. Что относится к биометрическим персональным данным?

1. - национальность, политические убеждения;
2. - фотография, отпечатки пальцев;
3. - паспортные данные, данные ИНН, СНИЛС.

11. Как правильно составлять пароль для входа в аккаунт социальной сети?

1. - состоящий из даты рождения (чтобы было быстрее набирать);
2. - состоящий из имени либо фамилии (чтобы было легче запомнить);
3. - состоящий из букв разных регистров, цифр, символов;

12. С помощью чего лучше сохранить пароль для входа в аккаунт социальной сети?

1. запомнить (например, с помощью мнемонического правила);
2. записать на листке и хранить рядом со смартфоном;
3. хранить с помощью специальной программы;
4. сказать своим друзьям, чтобы они напомнили, если пароль забуду или потеряю.

13. Что делать, если мне показалось, что мой пароль стал известен другому человеку:

1. - следить за содержанием аккаунта и поменять пароль, если что-то измениться;
2. - изменить пароль сразу;
3. - не менять пароль, если он надежный.

14. Будучи в гостях, Вам понадобилось срочно проверить электронную почту. Друг разрешил воспользоваться своим компьютером. Что делать, чтобы обезопасить свой аккаунт?

1. - продиктовать другу логин и пароль, чтобы друг сам проверил почту.
2. - самостоятельно проверить почту и после завершения работы быстро закрыть браузер;
3. - проверить почту, использую опции «чужой компьютер» или «не сохранять пароль», после завершения сеанса выйти из аккаунта;

15. Вы долгое время переписывались со своим ровесником и он предложил встретиться в парке и просит обменяться телефонами. Что Вы будете делать?

1. - нужно предварительно созвониться, обменяться фотографиями и только потом можно встретиться;

2. - свой номер телефона нужно указывать не в виртуальной переписке, а только при личной встречи;
3. - предложить собеседнику созвониться, используя видеозвонок и уже после этого встретиться, предупредив при этом родителей.

16. Вы всей семьёй планируете уехать на отдых в другой город. Когда лучше сообщить об этом своим друзьям?

1. - заранее сообщить куда и на сколько, чтобы не звонили и не писали, зная, что меня не будет в городе;
2. - незадолго до выезда, не уточняя, куда едем и на сколько;
3. - во время пребывания на отдыхе, заодно и выслать фотографии с отдыха;
4. - после приезда, рассказав обо всех впечатлениях.

17. Как правильно пользоваться сетями WiFi в общественных местах?

1. - заходить на все сайты, которые пожелаешь (бесплатно);
2. - заходить на все сайты, кроме своего аккаунта в соцсетях;
3. - заходить на все сайты, кроме банковских приложений;
4. - не пользоваться сетями WiFi, потому что это опасно.

18. Нужно ли устанавливать и использовать антивирус на ПК?

1. - нет, современные компьютеры обладают нужными средствами защиты;
2. - установить, обновлять и включать один раз в день для полной проверки;
3. - установить, обновлять и включать при необходимости проверки скачиваемых файлов;
4. - установить, держать всегда включенным и регулярно обновлять.

19. На электронную почту пришло письмо с незнакомого адреса с прикрепленным файлом. Что безопасно с ним сделать?

1. - открыть файл и посмотреть, что же там;
2. - не открывать файл, а сразу же удалить;
3. - проверить файл антивирусом.

20. На электронную почту пришло письмо от Вашего друга (знакомого) с прикрепленным файлом. Что безопасно с ним сделать?

1. - открыть файл и посмотреть, что же там;
2. - не открывать файл, а сразу же удалить;
3. - проверить файл антивирусом;
4. - созвониться с другом и спросить, действительно ли он отправил файл. И только после этого открывать файл.

21. Вам пришло сообщение от Вашего друга (знакомого) со ссылкой на Интернет-страницу. Какие Ваши действия?

1. - спросить у отправителя, что и с какой целью он Вам прислал;
2. - перейти по ссылке и посмотреть, что там;

3. - не переходить по ссылке, а сообщение удалить.

22. Как можно обезличить свои персональные данные?

1. - удалить ФИО;
2. - удалить фото;
3. - удалить адрес и место учебы.

23. Что такое «кибербуллинг»?

1. - компьютерная игра;
2. - оскорбление, запугивание, унижения человека в сети Интернет;
3. - приложение для смартфона.

24. Что делать, если Вас начали оскорблять либо запугивать в социальных сетях?

1. - угрожать и оскорблять в ответ;
2. - сообщить взрослым;
3. - не отвечать на оскорбления и угрозы.

25. Как правильно регистрироваться в социальных сетях?

1. - быстрее внести все свои персональные данные и поскорее начать общаться в социальной сети;
2. - внимательно прочитать пользовательское соглашение и Политику обработки персональных данных, и только после этого начать регистрацию;
3. - вносить минимально-необходимый объем персональных данных.

26. Что такое цифровой след?

1. - след на компьютере после внесения цифровых символов;
2. - информация о посещенных сайтах, совершенных покупках, местонахождение (геолокация);
3. - лайки в социальных сетях, комментарии.

27. Нужно ли защищать свой гаджет от вредоносных программ?

1. - нет, я посещаю одни и те же сайты;
2. - да, установив специальные почтовые фильтры;
3. - да, установив антивирусные программы.

28. Как узнать, что Интернет-сайт использует защищенное соединение?

1. - на главной странице сайта указано, что сайт защищен;
2. - в адресной строке сайта указан протокол http://;
3. - в адресной строке сайта указан протокол https:// и присутствует иконка «замка».

29. Можно ли встречаться с человеком, с которым Вы познакомились в социальных сетях?

1. - да, пойду один/одна, чтобы ни кто не мешал общаться и ни в коем случае не говорить родителям, чтобы не волновать;
2. - нет, общаться лучше только в социальных сетях;
3. - да, только в присутствии близкого друга либо родственника, заранее предупредив родителей.

30. Можно ли удалить информацию о себе, заблокировав свою страницу в социальной сети?

1. - да, информацию обо мне в социальной сети уже никто не увидит;
2. - нет, вся информация, которую я выкладывал в социальной сети, копируется другими сайтами, и полностью удалить ее из Интернета невозможно.

№ вопроса	№ ответа	№ вопроса	№ ответа	№ вопроса	№ ответа
1	4	11	3	21	1
2	2	12	1, 3	22	1
3	2	13	2	23	2
4	2	14	3	24	2, 3
5	2	15	3	25	2, 3
6	2, 3	16	4	26	2, 3
7	1	17	2, 3	27	2, 3
8	1	18	4	28	3
9	1	19	3	29	3
10	2	20	3, 4	30	2