**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 |