

# РАЗГОВОРЫ

# О ВАЖНОМ

Сценарий занятия

Кибербезопасность

8-9 классы

23 января 2023 г.

# **ВНЕУРОЧНОЕ ЗАНЯТИЕ**

## **для обучающихся 8–9 классов по теме**

### **«КИБЕРБЕЗОПАСНОСТЬ»**

**Цель занятия:** формирование культуры безопасного и эффективного использования цифровых ресурсов и устройств, знакомство с основами безопасности в сети и повышение уровня цифровой грамотности.

**Формирующиеся ценности:** жизнь, права и свободы человека.

**Продолжительность занятия:** 30 минут.

**Рекомендуемая форма занятия:** эвристическая беседа. Занятие предполагает использование видеороликов и анимационных видеофрагментов, учебную игру и включает в себя анализ информации, групповую работу.

#### **Комплект материалов:**

- сценарий;
- методические рекомендации;
- комплект интерактивных заданий;
- иллюстративные материалы и инструкции к игре;
- видеоролики.

#### **Структура занятия**

##### **Часть 1. Мотивационная.**

Анонс темы и просмотр мотивационного ролика.

##### **Часть 2. Основная.**

Обсуждение с просмотром анимационных фрагментов. Разбор предлагаемых ситуаций и вывод правил безопасного и эффективного использования цифровых ресурсов. Обсуждение вопросов, связанных с правилами поведения в интернете.

##### **Часть 3. Заключение.**

Подведение итогов занятия: фиксация правил, которые узнали обучающиеся, просмотр закрепляющего видеоролика.

## СЦЕНАРИЙ ЗАНЯТИЯ

### **Часть 1. Мотивационная** (до 5 минут).

#### **Учитель.**

Ребята, сегодня мы с вами поговорим о том, с чем постоянно сталкивается современный человек — это использование Интернета для решения повседневных задач: для учебы, общения, творчества, профессиональной деятельности. Возможности, доступные нам благодаря подключению к сети, могут принести много пользы, но там же можно столкнуться и с разными угрозами. Важно использовать доступ в Интернет с умом, эффективно и безопасно. Как и в реальной жизни, в Интернете стоит придерживаться некоторых правил, именно их мы сегодня с вами обсудим. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская — глава компании InfoWatch [Инфо-вОтч].

#### *Демонстрация видео с Н. И. Касперской.*

#### **Учитель.**

В продолжение занятия предлагаю вам разобрать несколько ситуаций, которые иногда случаются в сети. Вы выступите в роли сторонних наблюдателей и предложите свои решения.

### **Часть 2. Основная** (до 20 минут).

*Методический комментарий.* В основной части представлено два вида заданий.

#### **1. Интерактивное задание в форме анимационных фрагментов.**

Рекомендуется групповой вариант работы, но возможен и фронтальный. *Порядок работы с каждой ситуацией-кейсом строится по следующему алгоритму:*

- *просмотр первой части видеоклипа;*
- *обсуждение ситуации в группе и формулировка правил-выводов безопасного поведения;*
- *обсуждение правил-выводов безопасного поведения;*
- *проверка правила-вывода на основе просмотра второй части ролика.*

**2. Работа с заданиями-карточками,** описывающими конкретные ситуации, с которыми обучающиеся могут столкнуться в реальной жизни.

Предложена следующая тематика ситуаций-кейсов:

- 1) фишинговые ссылки;
- 2) социальная инженерия;
- 3) защита личной информации;
- 4) защита профиля.

Количество заданий учитель определяет самостоятельно.

### **Работа с интерактивным заданием**

#### **Учитель.**

Мы посмотрим небольшой ролик с ситуацией, которая знакома каждому из вас, ведь все мы общаемся с друзьями и заводим новые знакомства. Смотрим первую часть ролика и думаем, что случилось и как можно было предотвратить эту ситуацию.

#### ***Видео-кейс № 1. Фишинговые ссылки.***

##### **Учитель.**

Друзья, предлагаю вам поделиться на группы и попробовать сформулировать правила, которые можно предложить использовать, чтобы не оказываться в подобных ситуациях.

*(Ребята делятся на мини-группы по 4 человека и обсуждают возможные правила. На эту работу отводится 1–2 минуты.)*

А теперь обсудим получившиеся у вас правила. Что вы можете посоветовать делать в подобных ситуациях?

*(От каждой группы один обучающийся предлагает одно правило. Учитель фиксирует на доске.)*

##### **Учитель.**

Мы с вами обсудили, что пошло не так в ситуации Вани, теперь давайте досмотрим ролик и узнаем, какие цифровые привычки и правила нам предлагают создатели ролика, чтобы не попасться на удочку мошенников.

#### ***Продолжение демонстрации видео-кейса № 1. Фишинговые ссылки.***

##### ***Методический комментарий.***

*Дополнительно в этом кейсе можно обсудить значение слова «фишинговая» ссылка. Действия мошенников называют «фишингом» из-за английского слова «фиш», что означает «рыба» или «рыбачить», то есть буквально мошенники стараются «выудить» информацию у пользователя.*

**Учитель.**

Есть ещё одна ситуация, которую описывает в своем блоге герой мультфильма. Давайте посмотрим его, следите за сюжетом и поведением персонажей.

### ***Видео-кейс № 2. Социальная инженерия.***

**Учитель.**

Как вы считаете, какую ошибку допустил герой мультфильма? Каких правил надо придерживаться, чтобы не попадать в ловушки, в которые попала Кира? Давайте, как и в предыдущем случае, сначала обсудим это по группам, а потом все вместе.

*(Работа по группам, обсуждение и последующие ответы обучающихся.)*

**Учитель.**

Вы отлично справились, давайте досмотрим видео и узнаем, какие правила поведения в интернете мы с вами должны запомнить.

### ***Продолжение демонстрации видео-кейса № 2. Социальная инженерия.***

*Методический комментарий.*

*Социальная инженерия — разные виды манипуляций и обмана, цель которых заставить человека раскрыть личные данные, получить доступ к его личной и финансовой информации.*

**Учитель.**

Я предлагаю вам посмотреть другую ситуацию, которая произошла с любительницей классического искусства Ариной. Как и в прошлый раз, будьте внимательны и отмечайте поведение персонажей, чтобы ответить на мой вопрос. Смотрим.

### ***Видео-кейс № 3. Защита личной информации.***

**Учитель.** Как думаете, что произойдет дальше? Что в этой ситуации в поведении Арины вы считаете опасным? Есть ли здесь ошибка? На что мы должны обращать внимание и быть настороже, чтобы не попасть в такие же ситуации, как Арина? Поработайте, пожалуйста, в тех же группах, а потом обсудим ваши предложения.

*(Работа по группам, обсуждение, ответы обучающихся.)*

**Учитель.**

Ребята, вы молодцы, сейчас мы посмотрим развязку, узнаем не только, что случилось с Ариной, но и то, как обезопасить свою личную информацию и какие правила в этом помогут.

***Продолжение демонстрации видео-кейса № 3. Защита личной информации.***

**Учитель.**

Сейчас мы посмотрим ещё один ролик, где рассказывается история Жанны. Предлагаю узнать, что с ней приключилось и как друзья смогли прийти на помощь. Следите за сюжетом, у меня будет вопрос для вас.

***Видео-кейс № 4. Защита профиля.***

**Учитель.**

Как вы считаете, почему в аккаунте появилась такая информация? Как друзья Жанны поступят дальше? Что важно помнить и соблюдать, чтобы сохранить свой профиль в безопасности? Попробуйте составить правила, которые помогут вам обезопасить ваш профиль в социальной сети.

*(Работа по группам, обсуждение, ответы обучающихся.)*

**Учитель.**

Вы хорошо справились с заданием. Теперь время узнать, как правильно защищать свой профиль, какие правила для этого нужно знать.

***Продолжение демонстрации видео-кейса № 4. Защита профиля.***

**Учитель.**

Ребята, давайте ещё раз назовем правила, которые мы узнали на нашем занятии сегодня? Почему важно их соблюдать, как вы думаете?

*(Ответы обучающихся, обсуждение.)*

## **Работа с заданиями-карточками**

### **Учитель.**

Ребята, предлагаю вам посмотреть на знакомые действия и ситуации со стороны. Сыграем в игру и проверим, как хорошо вы умеете пользоваться цифровыми сервисами и приложениями.

*Методический комментарий.*

*Учитель делит обучающихся на команды (3–4 команды). Каждая команда получает карточку с описанием ситуации, дополнительно карточка выводится на экран (при наличии технических условий). Также возможен и фронтальный формат работы.*

Командам необходимо ответить на два вопроса:

1. Какую ошибку герой или героиня ситуации допустили?
2. Какие правила для пользователя можно вывести из этой ситуации?

На обсуждение каждой ситуации дается 3 минуты. Дальше каждая группа представляет результаты обсуждения.

Учитель сверяет полученные результаты с ключом к заданию.

### **Карточка-задание №1**

*Ваша одноклассница Катя ведет видеоблог про образ жизни, увлечения, учебу. Она делится всем тем, чем живет современный школьник. Катя выкладывает на свой канал рассказы о своей жизни, увлечениях, занятиях. В очередном выпуске своего блога Катя решает попробовать один из популярных форматов — прямой эфир с обзором комнаты.*

*В начале эфира Катя сообщает, что сегодняшнюю встречу она ведет из дома, называя свой адрес.*

*В одном из кадров она показывает, что есть у неё в комнате, как она все украсила к Новому году, где делает уроки, какие у неё хобби, заходит в комнату к брату, который с друзьями разучивает на гитаре новую песню.*

*Во время эфира в кадр попадает фамильная реликвия — шкатулка с уникальными украшениями.*

### **Учитель.**

Подумайте, в чем могли быть ошибки Кати? Что она сделала не так, и о чем нужно помнить, когда что-то выкладываешь в сеть?

*Работа обучающихся в группах.*

### **Учитель.**

Время для обсуждения закончилось, давайте обсудим, какие ошибки совершила Катя, и что можно ей посоветовать?

*Ответы обучающихся (по одному пункту поочерёдно от каждой группы), комментарии и дополнения учителя в соответствии с ключом к заданию.*

### **Ключ к заданию.**

- не оставляйте информацию о себе и родственниках в открытом доступе: домашний адрес, телефоны, номер школы, свой возраст, геолокации;
- в прямом эфире, где у вас нет заранее подготовленного текста и сценария вы говорите все, что придет в голову и ненамеренно можете сообщить информацию потенциально опасную для вашей безопасности;
- не размещайте фото или видео, на которых видно обстановку вашей квартиры, все то, что может притягивать мошенников;
- не выкладывайте фото или видео с участием ваших родственников, друзей без их разрешения;
- используйте настройку «для близких друзей», чтобы контролировать доступ к своему профилю и информации о себе.

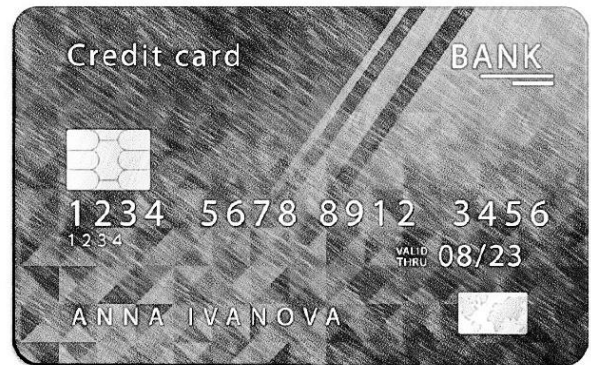
### **Учитель.**

Отлично, спасибо за ваши ответы! На данном примере стало понятно, что даже в таких знакомых ситуациях могут быть подводные камни.

*Дополнительно к этому заданию обучающимся можно предложить набор фотографий и обсудить, стоит ли размещать их в социальных сетях, и объяснить почему.*

*Примеры фотографий (полный набор и ключ к заданию представлены в дополнительных материалах).*





**Карточка-задание №2.1** (команды получают разные варианты карточек).

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. persik1234
2. ANNa11
3. A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

### **Карточка-задание №2.2**

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. Jack4321
2. ANNa11
3. A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

### **Карточка-задание №2.3**

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789
2. ANNA\_JACK
3. A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

### **Карточка-задание №2.4**

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она выбирает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789
2. ANNAPERSIK
3. A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

### **Учитель.**

Обсудите, какие из вариантов паролей надежные, какие нет, и почему? Надёжный ли пароль выбрала Аня? Сформулируйте правила, о которых нужно помнить при создании паролей.

*Работа обучающихся в группах.*

### **Учитель.**

Время для обсуждения закончилось, давайте обсудим надежность паролей, представленных на карточках, и выбор Ани.

*Ответы обучающихся, комментарии и дополнения учителя в соответствии с ключом к заданию.*

### **Ключ к заданию.**

- на всех карточках последний пароль подходит под критерии надежного пароля: содержит специальные знаки, заглавные буквы, цифры, при этом комбинация не связана с пользователем;
- не следует использовать общеизвестные факты для создания паролей (ваши имя, возраст, дату рождения, клички животных, имена близких родственников и т. п.);
- легко взломать пароли, состоящие только из цифр или букв;
- не следует использовать элементарные пароли типа 123456..., абвгд...;
- подключайте дополнительное подтверждение входа — двухфакторную аутентификацию.

**Учитель.** Проверить надежность пароля можно на сайте [2ip.ru/passcheck](http://2ip.ru/passcheck). Предлагаю проверить, за какой период можно взломать пароли, которые были представлены у вас на карточках.

*Обучающиеся проверяют надежность паролей*

*persik1234 – ненадежный, возможно взломать за 254 часа*

*ANNa11 – ненадежный, возможно взломать за 14 секунд*

*Jack4321 – ненадежный, возможно взломать за 910 минут*

*123456789 – ненадежный, возможно взломать за 0 секунд*

*ANNA\_JACK – ненадежный, возможно взломать за 1889 часов*

*ANNAPERsIK – ненадежный, возможно взломать за 588 минут*

*A!-2na1234 – надежный, может быть взломан за 6810 лет*

*A!-7n9aj234 – надежный, может быть взломан за 544770 лет*

*Дополнительно к этому заданию учитель может предложить ребятам проверить на надежность свои пароли от социальных сетей.*

### **Часть 3. Заключение (до 5 минут).**

#### **Учитель.**

Сегодня мы обсудили некоторые случаи, когда пользователи не задумываются о последствиях своих действий в сети. Случаются такие ситуации, безусловно, не специально. Наша ответственность как пользователей цифровых сервисов быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь, когда мы знаем об угрозах, то можем соблюдать простые правила и оставаться в безопасности. Давайте закрепим результат занятия и послушаем ещё несколько рекомендаций от эксперта компании VK [вэ-ка] Константина Сидоркина и популярного российского певца Егора Крида.

*Демонстрация видео с К. Сидорковым.*

*Демонстрация видео с Е. Кридом.*