

# РАЗГОВОРЫ

## О ВАЖНОМ

Сценарий занятия

**Кибербезопасность**

**3-4 классы**

23 января 2023г.

## ВНЕУРОЧНОЕ ЗАНЯТИЕ для обучающихся 3–4 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.

**Планируемые результаты.**

**Личностные:**

- освоение роли пользователя цифровых ресурсов и сервисов;
- развитие самостоятельности и ответственности на основе представлений о безопасном поведении в сети;
- овладение навыками адаптации в условиях развития информационно-коммуникационных технологий;
- развитие навыков сотрудничества со взрослыми и сверстниками в различных социальных ситуациях.

**Метапредметные:**

- универсальные познавательные учебные действия (базовые логические и начальные исследовательские действия, а также работа с информацией);
- освоение начальных форм познавательной рефлексии;
- овладение сведениями о сущности и особенностях цифровых объектов, процессов и явлений окружающего мира;
- участие в коллективном обсуждении вопросов занятия, формулирование своего мнения в процессе беседы.

**Продолжительность занятия:** 30 минут.

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

**Комплект материалов:**

- сценарий,
- методические рекомендации,
- видеофрагменты,
- презентация.

**Структура занятия****Часть 1. Мотивационная.**

Организация беседы, которая опирается на личный опыт обучающихся по использованию цифровых устройств с выходом в интернет, позволяет обеспечить мотив к знакомству с заявленной темой. Продолжением вводной части является просмотр выступления Натальи Ивановны Касперской, российского предпринимателя в сфере информационных технологий, главы группы компаний InfoWatch [Инфо-вОтч].

**Часть 2. Основная.**

В основной части занятия учитель предлагает проанализировать несколько ситуаций-кейсов, в которых представлены угрозы со стороны мошенников, и познакомить/сформулировать основные правила цифровой безопасности в сети Интернет: защита профиля, защита личной информации, фишинговые ссылки, социальная инженерия.

**Часть 3. Заключение.**

Обобщение обсуждаемого на занятии материала.

**СЦЕНАРИЙ ЗАНЯТИЯ****Часть 1. Мотивационная.****Учитель.**

Ребята, здравствуйте! Сегодня наша тема связана с безопасностью. Вспомните, что мы говорили о безопасности на дорогах. Почему надо соблюдать правила дорожного движения?

*(Ответы детей: правила дорожного движения надо соблюдать, чтобы не попасть в аварию).*

**Учитель.**

Но правила существуют не только для безопасного движения на дороге. Существуют правила и для наших цифровых устройств, которыми мы пользуемся каждый день.

*Методический комментарий. При организации беседы важно обращаться к опыту обучающихся, но при этом учитель должен учитывать, что не у всех детей есть цифровые устройства (компьютеры, телефоны).*

**Учитель.**

Наши цифровые устройства – компьютеры, телефоны во многом нам помогают. Например, быстро найти какую-то информацию, оперативно связаться друг с другом. Но, используя наши устройства, важно знать, что при этом есть и определённые риски, которые существуют в цифровом пространстве. Об этом нам расскажет Наталья Ивановна Касперская, специалист в сфере информационных технологий, глава группы компаний InfoWatch [Инфо-вОтч].

***Демонстрация выступления Н. И. Касперской.*****Учитель.**

О рисках использования устройств и важности соблюдения правил в цифровом пространстве мы с вами услышали, а теперь обсудим некоторые простые правила для собственной безопасности в интернете.

**Часть 2. Основная.****Учитель.**

Помогать нам сегодня на занятии будет Антон Корюшкин, который живёт в городе Нижнефорельске. Он ходит в кружок цифровой безопасности, поэтому расскажет нам о ситуациях, в которых его друзья подверглись атакам мошенников. Посмотрим первый сюжет.

***Демонстрация видео (интерактивное задание в формате анимационного фрагмента).***

*Методический комментарий.*

*Задача основной части занятия – анализ нескольких ситуаций-кейсов*

*(интерактивных заданий в формате анимационных фрагментов): защита профиля, защита личной информации, фишинговые ссылки, социальная инженерия. Выбор ситуаций-кейсов, которые предложит для анализа учитель в своём классе, зависит от организационных условий и уровня подготовки обучающихся. Также учитель определяет формат работы с ситуациями-кейсами: фронтальное обсуждение со всем классом или анализ выбранных заданий в группах обучающихся.*

*Порядок работы с каждой ситуацией-кейсом (интерактивное задание в формате анимационного фрагмента) строится по следующему алгоритму:*

- просмотр первой части ролика;*
- обсуждение ситуации по предложенным вопросам;*
- формулирование правила-вывода;*
- проверка правила-вывода на основе просмотра второй части ролика.*

*При организации групповой работы учитель предлагает, после просмотра первой части видео, обучающимся сначала обсудить между собой варианты ответов на поставленный вопрос, а потом представить коллективный результат.*

### **Ситуация-кейс «Защита личной информации» (интерактивное задание в формате анимационного фрагмента).**

*Цель: зачем и как защищать личную информацию?*

*Описание 1 части видео: Арина купила билет на выставку и сфотографировала его, а затем выложила фото билета в социальных сетях, чтобы друзья за неё порадовались.*

*Вопрос: что в действиях Арины опасно?*

*Ответы детей: увидеть фото билета, а затем использовать его данные может мошенник.*

*Описание 2 части видео: запись Арины прочитал мошенник, который позже показал фото билета из личного профиля и по нему прошёл на представление, а Арина уже не смогла воспользоваться купленным билетом.*

*Правило: необходимо быть предельно осторожными, если выкладываете информацию в сети. И чтобы дополнительно себя обезопасить в интернете, используйте фильтр «для близких друзей».*

### **Ситуация-кейс «Защита профиля» (интерактивное задание в формате анимационного фрагмента).**

*Цель: как защитить свой профиль в социальных сетях от взлома?*

*Описание 1 части видео: Жанна – блогер. Однажды она не смогла войти*

в свой аккаунт (учётную запись), а её пользователи получили информацию о том, что Жанне надо прислать деньги на лечение её любимого животного.

*Вопрос:* почему Жанна не смогла войти в свой аккаунт? Как вы думаете, что сделали подписчики Жанны?

*Ответы детей:* её аккаунт заблокировали, его «взломали» мошенники. Если мы получили подозрительное письмо, надо связаться и уточнить информацию у человека, от которого было получено письмо.

*Описание 2 части видео:* но её поклонники-подписчики знали, что у неё аллергия на животных, поэтому они сразу поняли, что аккаунт «взломан», и пожаловались модератору социальной сети. Модератор оперативно заблокировал страницу.

*Правило:* на всех сервисах используйте разные пароли и меняйте их раз в полгода. Пароли должны содержать более 8 символов, включая строчные и заглавные буквы. Также можно подключить дополнительное подтверждение входа, это поможет защитить профиль от мошенников.

### **Ситуация-кейс «Фишинговая ссылка» (интерактивное задание в формате анимационного фрагмента).**

*Цель:* как не попасть на «удочку» кибермошенников?

*Описание 1 части видео:* Ваня познакомился в сети с девочкой, и они стали переписываться. В процессе общения Ваня поделился информацией о кино, а новая подруга предложила сходить посмотреть фильм и скинула Ване ссылку, чтобы он оплатил билеты. Ваня перешёл по ссылке и оплатил билеты. Но билеты не пришли, а девочка перестала выходить на связь.

*Вопрос:* какую ошибку допустил Ваня при общении с девочкой в сети?

*Ответы детей:* Ваня поверил, что он общается с реальной девочкой. Ваня ввёл данные и не проверил ссылку.

*Описание 2 части видео:* оказалось, что Ваня стал жертвой фишинга, а мошенникам удалось заполучить реквизиты личной карты Вани. Поэтому её пришлось заблокировать и выпустить новую.

*Правило:* прежде чем знакомиться в социальных сетях, просмотрите страничку пользователя – похожа ли она на настоящий профиль, есть ли информация (посты) о каких-то событиях или от друзей. Лучше не переходить по незнакомым ссылкам, так как любая из них может быть опасной. Прежде чем ввести свои данные, проверьте адресную строку, любимая уловка мошенников – использовать схожие буквы. Покупку билетов необходимо делать только на проверенных официальных сайтах.

*Методический комментарий.*

Если позволяет уровень подготовки класса, то можно дополнительно в этом кейсе 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.

### **Ситуация-кейс «Социальная инженерия» (интерактивное задание в формате анимационного фрагмента).**

*Цель:* как распознать обман в интернете?

*Описание:* Кира очень любит одну музыкальную группу. И однажды ей в личном сообщении написал продюсер и сообщил, что ей предлагают принять участие в просмотре-кастинге. Но для этого необходима фотосессия, за которую надо заплатить. Продюсер попросил перевести деньги как можно быстрее. Кира перевела деньги и стала собираться на просмотр-кастинг, но продюсер почему-то пропал.

*Вопрос:* какую ошибку допустила Кира?

*Ответы детей:* Кира поверила, что ей написал настоящий продюсер, и ввела свои данные, оплатив фотосессию.

*Описание 2 части видео:* ведь на самом деле Кира переписывалась с мошенником.

*Правило:* если вам пришло сообщение от незнакомца, то необходимо постараться собрать о нём дополнительную информацию – попросить его представиться, проверить его информацию и попросить прислать больше информации о том, что вам предлагают. Помните, что мошенники всегда будут вас торопить, чтобы у вас не было возможности и времени разобраться в ситуации, чтобы уточнить и проверить полученную информацию.

*Методический комментарий.*

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

### **Часть 3. Заключительная.**

**Учитель.**

Ребята, давайте ещё раз назовем правила, которые мы узнали, обсуждая ситуации, о которых нам рассказал Антон Корюшкин.

*(Ответы детей).*

**Учитель.**

Почему важно соблюдать эти правила? Объясните.

*(Ответы детей).*

Обсудите эти важные правила безопасности с родителями, а в заключение давайте 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.*

*Методический комментарий.*

*При подготовке видео для занятия были использованы материалы просветительского проекта «Цифровой ликбез»: <https://digital-likbez.datalesson.ru/>.*