РАЗГОВОРЫ О ВАЖНОМ

Методические рекомендации

Кибербезопасность

1-2 классы

23 января 2023 г.

ВНЕУРОЧНОЕ ЗАНЯТИЕ
для обучающихся 1–2 классов по теме
«КИБЕРБЕЗОПАСНОСТЬ»

Цель занятия: формирование культуры безопасного и эффективного использования цифровых ресурсов и гаджетов, 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,
– презентации.

Структура занятия

Часть 1. Мотивационная.

Как бы мы, лично, ни относились к использованию различных устройств с выходом в Интернет, цифровизация неизбежно входит в нашу деятельность, обеспечивает взаимодействие родителей и общение детей, развитие общества в целом. По сути, младшие школьники уже пришли в школу с тем, что цифровые устройства – это неотъемлемая часть их повседневной жизни: учёбы, общения, игр и так далее. И признанием важности этого направления является выделение в нормативно-правовых документах результатов, связанных с цифровой грамотностью и безопасностью в Интернете. Например, в Федеральном государственном образовательном стандарте указано на необходимость овладения обучающимися «современными технологическими средствами в ходе обучения и в повседневной жизни, формирование у обучающихся *культуры пользования информационно-коммуникационными технологиями (далее ИКТ)»*[1], а также выделена задача в рамках учебного предмета «Окружающий мир»: «формирование навыков здорового и безопасного образа жизни на основе выполнения правил безопасного поведения в окружающей среде, в том числе *знаний о небезопасности разглашения личной и финансовой информации при общении с людьми вне семьи, в сети* и опыта соблюдения правил безопасного поведения при использовании личных финансов».[2] В рабочей программе учебного предмета «Окружающий мир» также определён результат в области «*ориентирования в признаках мошеннических действий, защита персональной информации, правила коммуникации в мессенджерах и социальных группах*»[3]. Отсюда и возникает актуальность такой темы, как *кибербезопасность*. Под кибербезопасностью понимается совокупность

[1]Федеральный государственный образовательный стандарт начального общего образования. Утверждён приказом Министерства просвещения Российской Федерации 31 мая 2021 г., № 286, [Электронный ресурс]. – С.2.
[2] Там же – С.48
[3] Примерная основная образовательная программа начального общего образования (Одобрена решением федерального учебно-методического объединения по общему образованию, протокол от 15 сентября 2022 г. № 6/22), [Электронный ресурс] – С.351.

правил и практик защиты от атак злоумышленников в цифровом пространстве. Познакомимся с некоторыми понятиями более подробно.

Аккаунт (учётная запись) – опознавательная информация о пользователе, которая указывается при регистрации на тех или иных сервисах и сайтах.

Профиль – это расширенная совокупность личной, финансовой и другой информации пользователя.

Блогер – пользователь, который ведёт журнал событий в интернете.

Фишинг – вид интернет-мошенничества, при котором мошенники пытаются заполучить личные данные человека через поддельные ссылки, сайты, уведомления и т. п. «Фишингом» такие мошеннические действия называются из-за английского слова «фиш», что означает «рыба» или «рыбачить», то есть буквально мошенники стараются «выудить» информацию у пользователя.

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

Овершеринг – новое слово, обозначающее явление, о котором широко заговорили еще в 2013 году, буквально «чрезмерно много делиться». Это избыточное размещение информации личного характера о себе или других людях в общедоступных источниках, в частности, в социальных сетях.

С учётом этого на данном занятии и предлагаются для рассмотрения несколько ситуаций-кейсов, в которых представлены правила действий при распространённых атаках мошенников: защита профиля, защита личной информации, фишинговые ссылки, социальная инженерия.

Это небольшое вступление необходимо, чтобы учитель сознал важность этого разговора. Цель данного занятия – формирование культуры безопасного и эффективного использования цифровых ресурсов и гаджетов, знакомство с основами безопасности в сети и повышение уровня цифровой грамотности. И начинается оно с просмотра выступления Натальи Ивановны Касперской, российского предпринимателя в сфере информационных технологий, главы группы компаний InfoWatch [Инфо-вОтч]. В своём выступлении она кратко говорит о важности соблюдения определённых правил при использовании цифровых устройств, так как это не только свобода и доступность, но и риски. Особое внимание эксперт уделяет рискам,

связанным со здоровьем, а также осознанию того, что цифровое устройство всегда собирает и хранит информацию.

Часть 2. Основная

Задача основной части занятия – анализ нескольких ситуаций кейсов: демонстрация видео (интерактивное задание в формате анимационного фрагмента).

Все четыре кейса представляют собой анимационные видеоролики, в которых действие происходит в городе Нижнефорельске. Сквозной персонаж Антон Корюшкин ходит в кружок цифровой безопасности и рассказывает о ситуациях, в которых его друзья подверглись атакам мошенников.

Анализ предложенных ситуаций позволяет сделать выводы и сформулировать правила, соблюдение которых поможет защититься от угроз мошенников. 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.

Количество ситуаций-кейсов, которые предложит для анализа учитель в своём классе, зависит от организационных условий и уровня подготовки обучающихся. Рассмотрим содержание каждого кейса.

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 профиль от взлома?

Описание 1 части видео: Жанна – блогер. Однажды она не смогла войти в свой аккаунт, 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? Какие действия выполнили подписчики?

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 новом 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.

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

Цель: как распознать обман в интернете?

Описание 1 части видео: Кира очень любит одну музыкальную группу. И однажды ей в личном сообщении написал продюсер и сообщил, что ей предлагают принять участие в просмотре. Но для этого необходима фотосессия, за которую надо заплатить. Продюсер попросил перевести деньги как можно быстрее. Кира перевела деньги и стала собираться на просмотр, но продюсер почему-то пропал.

Вопрос: какую ошибку допустила Кира?

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

Часть 3. Заключение

В заключение занятия учитель обобщает представленный материал и подводит итоги: «Ребята, давайте ещё раз назовем правила, которые мы узнали из видео? Почему важно их соблюдать? Объясните». Дополнительно используется обращение К. Сидоркова, эксперта компании VK [вэ-кА].

При подготовке ситуаций-кейсов были использованы материалы просветительского проекта «Цифровой ликбез»: https://digital-

likbez.datalesson.ru/

При **наличии возможности** рекомендуется предусмотреть ведение обучающимися **дневника внеурочных занятий «Разговоры о важном».**

В таком «дневнике» могут отмечаться:

– тема занятия;

– ценности, обсуждаемые в ходе занятия;

– основные выводы обучающегося, сделанные по итогам занятия;

– ссылки на полезные медиаресурсы и образовательные проекты по тематике занятия;

– творческие задания и темы для обсуждения с родственниками и друзьями;

– любая другая информация по теме занятия.

Структура такого «дневника» и организация его ведения определяютсяобразовательной организацией самостоятельно.