**СЦЕНАРИЙ УРОКА ДЛЯ 8-9 КЛАССОВ**

| **№ слайда и /или дидактич. материал** | **Деятельность спикера** | **Деятельность учащихся** | **Тайминг** |
| --- | --- | --- | --- |
| **ЭТАП 1: ПРОБЛЕМНАЯ ДИСКУССИЯ «ЧТО ТАКОЕ ДИПФЕЙКИ И ЧЕМ ОНИ ОПАСНЫ ДЛЯ НАШИХ ФИНАНСОВ»** | **14 мин.** |
| Слайд 1 | **ПРЕДСТАВЛЕНИЕ**«Здравствуйте, ребята (учащиеся / друзья), педагоги, родители! Меня зовут….., я являюсь….» *(коротко о своей деятельности в области финансов и/или финансовой грамотности).* | Учащиеся разделены на 4 группы, на первом этапе могут сидеть не по группам, а как обычно.Слушают. | **1****мин.** |
| Слайд 1 | Вводит в тему: «Наша встреча посвящена одной из важнейших тем современного мира – финансовому мошенничеству в цифровой среде». Обращается к классу: «Что вы знаете о финансовом мошенничестве в цифровой среде? Какие виды финансового мошенничества в цифровой среде вы знаете, слышали, возможно, даже имели негативный опыт?»Если учащиеся затрудняются отвечать, спикер помогает им с ответами.Продолжает: «В процессе управления личными (семейными) финансами у каждого человека возникают определенные риски, одним из которых является финансовое мошенничество. Современный мошенник часто оказывается на шаг впереди своей жертвы. В мире, где процветают цифровые технологии, на сегодняшний день уже существуют несколько мошеннических схем в цифровой среде, которые используются для кражи денег. Давайте рассмотрим наиболее распространенные из них». | Слушают.Отвечают на вопросы лектора:* фальшивые (мошеннические) звонки;
* взлом банковских счетов;
* кража личных данных;
* вымогательство с использованием фальшивых видео и аудио образов и т. д.

Слушают. | **1****мин.** |
| Слайд 2 | **Спикер: «Фишинг.** Это ситуация, при которой мошенник старается обманом получить доступ к важной финансовой информации: логинам и паролям для входа в личные кабинеты, данным банковских карт и паспортов, кодам верификации, личным фотографиям, важной переписке — всему тому, что может помочь ему заполучить ваши деньги.Например, если на сайте «Авито» продавец предлагает вам оплатить покупку на сайте avit0-d0stavka.mysite.com, – это одна из разновидностей фишинга. Другой вариант: вас могут попросить ввести логин и пароль от личного кабинета на сайте или номер и код от мессенджера, чтобы «получить подарок».Далее спикер задает вопрос: «А вы или ваши знакомые/родные/друзья сталкивались с фишингом?» (принимает 1–2 ответа). | Могут рассказать об этом виде мошенничества, если знают.*Если учащиеся проявляют инициативу в ответах, то можно дать возможность кому-то из них рассказать о фишинге.*Отвечают на вопрос спикера. | **1 мин.** |
| Слайд 3 | Продолжает: **«**Следующий вид мошенничества – это **социальная инженерия,** когда используются различные манипулятивные методы воздействия на сознание и поведение человека. Все данные человек предоставляет сам – под действием обманной манипуляции, угроз и игры на чувствах потенциальной жертвы. Наиболее часто встречающимися каналами социальной инженерии являются электронная почта, сайты, социальные сети, мессенджеры. А вот звонки составляют всего 8%. Что подтверждает наш тезис об увеличивающейся доле мошенничества в цифровой среде».Задает вопрос: «А вы или ваши знакомые/родные/друзья сталкивались с социальной инженерией?» (принимает 1–2 ответа). | Могут рассказать об этом виде мошенничества, если знают.*Если учащиеся проявляют инициативу в ответах, то можно дать возможность кому-то из них рассказать о социальной инженерии.*Отвечают на вопросы спикера. | **1 мин.** |
| Слайд 4 | Переходит к следующему виду: **«Предложение заработать в интернете.** Подвидов таких предложений сегодня очень много: это и платное «обучение», и покупка необходимого оборудования для начала работы, это и фиктивное трудоустройство онлайн для сбора документов и оформления микрозаймов и пр.».  | Могут рассказать об этом виде мошенничества, если знают.*Если учащиеся проявляют инициативу в ответах, то можно дать возможность кому-то из них рассказать о мошеннических предложениях получения дохода в интернете.* | **1 мин.** |
| Слайд 5 | Продолжает: «Еще один вид – это **финансовые пирамиды.** Современные финансовые пирамиды тоже ушли в цифровую среду, они маскируются под инвестиции, в том числе в криптовалюту, кэшбэк-сервисы, сетевые магазины, совместные покупки и многое другое. Кроме того, финансовые пирамиды все еще остаются популярными у мошенников в **социальных сетях**, которые являются удобным инструментом для общения, в том числе с незнакомыми людьми. В интернете процветают мошеннические **лотереи, викторины, победы в конкурсах, подарочные карты и многое другое.**  Но сегодня мы поговорим об одном из видов мошенничества, который является достаточно новым. Он связан с использованием искусственного интеллекта и нейросетей. Это так называемые дипфейки». | Могут рассказать об этом виде мошенничества, если знают.*Если учащиеся проявляют инициативу в ответах, то можно дать возможность кому-то из них рассказать о финансовых пирамидах. Но необходимо следить за временем, т.к. это только разминка.* | **1 мин.** |
| Слайд 6Приложение № 1 (все приложения доступны по ссылке: <https://disk.yandex.ru/d/qj7MGFi2BMNcow>)  | Продолжает: «Поднимите, пожалуйста, руки те, кто слышал о дипфейках, а, возможно, и видел дипфейки». Пока ученики поднимают руки, возможно, дают комментарии, спикер или его помощник переключают экран на видеоролик.И далее предлагает: «Давайте посмотрим вместе короткий видеоролик о дипфейках в жизни современного человека. После просмотра ролика мы с вами обсудим следующие вопросы (сейчас я их назову устно, а после просмотра видео мы их выведем на слайде):1. Что такое дипфейк?
2. Применимость дипфейков в жизни человека – «светлая» сторона.
3. Применимость дипфейков в жизни человека – «темная» сторона».

Включает видеоролик.После просмотра видеоролика спикер обращается к классу: «Итак, вы теперь знаете, что дипфейки существуют во многих сферах жизни человека. Наша задача с вами узнать о темной стороне этого явления и суметь защитить себя и своих близких от финансовых кибермошенников, использующих дипфейки». | Поднимают руки те, кто знаком с этим понятием.Смотрят видеоролик. | **3****мин.** |
| Слайд 7 | Переключает на презентацию и задает первый вопрос: «В чем суть явления «дипфейк», рассмотренного в ролике?»После ответов учеников спикер уточняет: «Термин «дипфейк» появился в 2017 году на интернет-площадке Reddit, а в 2020-м уже официально [попал в словари](https://www.merriam-webster.com/words-at-play/deepfake-slang-definition-examples).Слово deepfake раскрывает принцип действия: это слова deep (сокращение от deep machine learning – умное машинное обучение) и fake (подделка). Дипфейком может быть видео или аудио.Что нужно для создания дипфейк-видео?* исходное видео в хорошем качестве;
* фото или видео человека, которого нужно внедрить в дипфейк;
* программное обеспечение для обработки данных».

Спикер обращается к аудитории: «А где, на ваш взгляд, применяются дипфейки, если мы говорим о положительной стороне явления?» | Отвечают на вопрос.Возможные варианты ответов:* это обучение нейросети выдавать одно изображение и голос за другое;
* это наложение изображения и действий одного человека на другого;
* это машинное обучение и постоянный рост вычислительных мощностей;
* быстрая генерация сложных объектов.

Отвечают на вопрос. Ответы могут содержать такую информацию:* в новых компьютерных играх;
* короткие видео в социальных сетях (мотивационные ролики с известными личностями);

социальная реклама, где главные герои – всем известные персонажи. | **1 мин.** |
| Слайд 8 | После ответов учеников спикер уточняет: «Эта технология выглядит необычно и интересно. Системы воссоздания голоса появились из лучших побуждений. Например, чтобы немые люди могли печатать текст и тем самым «говорить». Ярким примером также является реклама: в 2020 году СберБанк запустил серию роликов с Жоржем Милославским (персонаж из фильма «Иван Васильевич меняет профессию»). А в 2021 году компания «МегаФон» показала рекламу с молодым актером Брюсом Уиллисом. В обоих случаях это были дипфейки (*сам спикер может предварительно посмотреть ролики по ссылкам* [*https://www.youtube.com/watch?v=rEcjVsZQb0c*](https://www.youtube.com/watch?v=rEcjVsZQb0c) *и* [*https://www.youtube.com/watch?v=8GXIT5qvQH0*](https://www.youtube.com/watch?v=8GXIT5qvQH0)*, чтобы составить своё представление*). |  | **1****мин.** |
| Слайд 9 | Спикер обращается к аудитории: «Еще недавно использование дипфейков было для мошенников очень дорогим делом, однако с развитием искусственного интеллекта создание дипфейка становится более дешевым и простым:1. Первый значительный инцидент [произошел](https://www.sberbank.ru/ru/person/kibrary/articles/kak-zashchitit-biznes-ot-deepfake-moshennikov) в 2019 году, когда директор британской энергетической компании перевел на счет мошенников 243 тысячи долларов по звонку «своего руководителя». Мошенникам удалось настолько точно сымитировать голос шефа, что жертва была уверена, что выполняет его поручение.
2. Мошенники клонировали голос известного рэпера, создали с его помощью несколько новых композиций и выставили их на продажу как демозапись нового альбома. Фанаты перечисли 13 тысяч долларов мошенникам.
3. В начале 2024 года в интернете появился ролик, где женщина отвечает на звонок в мессенджере. Она слышит голос своего сына, который отправляет ей номер телефона и просит перевести на него одну тысячу рублей на подарок другу. При этом реальный сын сидит рядом с ней».
 | Слушают. | **1****мин.** |
| Слайд 10 | Обращается к классу: «Почему, на ваш взгляд, возникла такая проблема? В чем причина того, что люди попадаются на уловки мошенников, использующих дипфейки?»Принимает ответы учеников и поясняет: «Люди попадаются, так как не знают, что такое дипфейки, как это определить и как проверить. Как вы увидели, от дипфейков мошенников страдают разные категории людей, ведь они все по-разному воспринимают информацию. Существуют разные способы защиты от дипфейков, каждый из них должен быть представлен доходчиво и интересно для каждой группы людей. Этим мы и займемся во второй части нашего урока: попробуем создать разнообразные источники просветительской информации, чтобы люди не попадались на уловки финансовых мошенников и становились более финансово грамотными». | Отвечают на вопрос. Ответы могут содержать такую информацию:* люди не знают об этом явлении и не могут распознать проблему;
* часто срабатывает эффект неожиданности, когда дело касается близких людей;
* люди не способны критически мыслить, когда дело касается возможности быстрой прибыли;
* одинокие пожилые люди нуждаются в общении и часто покупаются на эту уловку мошенников;
* увлечения людей (музыка, животные, кино) могут стать причиной попадания на уловки мошенников. Каждому хочется стать первым, кто услышал песню любимого исполнителя, или помочь бездомным животным, а может быть, поговорить с любимым актером (вдруг это действительно он).
 | **2****мин.** |

|  |  |
| --- | --- |
| **ЭТАП 2: СОЗДАНИЕ СОЦИАЛЬНОЙ РЕКЛАМЫ** **«КАК ЗАЩИТИТЬ СЕБЯ ОТ ФИНАНСОВЫХ МОШЕННИКОВ, ИСПОЛЬЗУЮЩИХ ДИПФЕЙКИ»** | **14 мин.** |

| **№ слайда и /или дидактич. материал** | **Деятельность спикера** | **Деятельность учащихся** | **Тайминг** |
| --- | --- | --- | --- |
| Слайд 11Бумага, маркеры, карандаши, ножницы, ватман и пр. | Спикер: «Итак, вы разделены на 4 группы. Каждая группа готовит свой просветительский продукт. Задача работы в группе – рассказать о рисках финансового мошенничества с использованием дипфейков и о том, как их опознать и как не попасться на их уловки с учетом особенностей восприятия информации данной целевой группой.Давайте посмотрим на слайд, какие целевые группы у у вас:группа №1 – дети (7–12 лет, ваши младшие братья / сестры);группа №2 – подростки и молодежь (ваши сверстники);группа №3 – люди среднего возраста (ваши родители);группа №4 – люди пенсионного возраста (ваши бабушки / дедушки). | Разделены на 4 группы.Рассаживаются для удобной работы в группе.Задают уточняющие вопросы, если появились. | **1****мин.** |
| Слайд 12Приложение №2 (все приложения доступны по ссылке: <https://disk.yandex.ru/d/qj7MGFi2BMNcow>) | Формы, которые вы можете выбрать:* видеоролик для мессенджеров / соцсетей;
* пост для соцсетей;
* сообщение для мессенджеров;
* статья для онлайн-издания (газеты, журнала);
* статья для интернет-портала по финансовой грамотности (или для портала «Госуслуги» и пр.);
* статья для бумажной газеты, журнала;
* подкаст;
* письмо для e-mail рассылки;
* рекламное сообщение в автобусе / трамвае / метро (аудиовизуальное);
* листовка, буклет;
* плакат;
* рассказ для соцработника;
* что-то на усмотрение группы.

В качестве источника информации вы можете использовать статьи, которые рассказывают о дипфейках и о том, как их распознать, или черпать информацию из интернета. Однако будьте внимательны, информация может быть представлена на сайтах с разной степенью достоверности. Нужно быть внимательными при выборе источника, лучше брать информацию с официальных сайтов, в том числе исследовательских институтов, государственных платформ, компаний, занимающихся антивирусным обеспечением, экспертов в области кибербезопасности. Есть ли у вас вопросы?»Если есть вопросы, отвечает.Объявляет время работы в группах – 10 минут.Также сообщает, что если нужны бумага, маркеры, карандаши, ножницы, ватман, то можно взять у спикера. Для тех, кто решил делать плакат, можно использовать доску или флипчарт. | Берут распечатку приложения №2.Задают вопросы, если имеются. Если есть необходимость, то берут у спикера бумагу, маркеры, карандаши, ножницы, ватман и пр. | **2****мин.** |
| Слайд 13 | Организует работу в группах. Подходит к каждой группе, помогает при необходимости, ориентирует по каналам представления информации для разных целевых групп.Подсказка для спикера:Рекомендуемые каналы представления информации для разных целевых групп:* видеоролик для мессенджеров / соцсетей (1, 2, 3)
* пост для соцсетей (1, 2, 3)
* сообщение для мессенджеров (2, 3)
* статья для онлайн-издания (газеты, журнала) (2, 3)
* статья для интернет-портала по финансовой грамотности (или для портала «Госуслуги» и пр.) (3, 4)
* статья для бумажной газеты, журнала (3, 4)
* подкаст (2, 3)
* письмо для e-mail рассылки (3, 4)
* рекламное сообщение в автобусе / трамвае / метро (аудиовизуальное) (3, 4)
* листовка, буклет (3, 4)
* плакат (4)
* рассказ для соцработника (4)
 | Работают в группах над созданием просветительского продукта (могут передвигаться по кабинету (аудитории). При необходимости консультируются у спикера. | **8****мин.** |
| Слайд 14 | Объявляет о том, что заканчивает время, за 2 минуты, просит приготовить свои просветительские продукты. Если это видеоролик, то нужно скинуть на компьютер (через мессенджер или соцсети), чтобы можно было продемонстрировать на экране. Или через флешку перекинуть на смарт-доску.Аудиопродукт учащиеся смогут продемонстрировать через свой телефон или также через компьютер.Сообщает о необходимости выбрать того, кто будет презентовать продукт (возможно, не один, а несколько человек). | Заканчивают разработку своего просветительского продукта, готовятся к его презентации. | **3****мин.** |

|  |  |
| --- | --- |
| **ЭТАП 3: ПРЕЗЕНТАЦИЯ СОЦИАЛЬНОЙ РЕКЛАМЫ И ТРЕНИНГ** | **14 мин.** |

| **№ слайда и /или дидактич. материал** | **Деятельность спикера** | **Деятельность учащихся** | **Тайминг** |
| --- | --- | --- | --- |
| Слайд 14ФлипчартСмарт-доска / проектор и экран | Объявляет очередность презентации *(на усмотрение спикера, рекомендуется в заявленном порядке: от 1 к 4 группе или наоборот, но не вразброс).*Объявляет задачу для учеников тех групп, которые не выступают:«Вам нужно определить:1. подходит ли выбранный формат для данной целевой группы;
2. какие признаки дипфейков были заложены в просветительский продукт для предостережения».

После выступления каждой группы спикер задает обозначенные выше вопросы участникам всех остальных групп (это нужно делать достаточно динамично, без длительного обсуждения).И так повторяется после каждого выступления. | Выступает группа № 1, остальные внимательно слушают и смотрят. Отвечают на вопросы спикера по выступлению группы № 1.Выступает группа № 2, остальные внимательно слушают и смотрят. Отвечают на вопросы спикера по выступлению группы № 1.Выступает группа № 3, остальные внимательно слушают и смотрят. Отвечают на вопросы спикера по выступлению группы № 3.Выступает группа № 4, остальные внимательно слушают и смотрят. Отвечают на вопросы спикера по выступлению группы № 4. | **8 мин.** |
| Приложение №3Приложение №4(все приложения доступны по ссылке: <https://disk.yandex.ru/d/qj7MGFi2BMNcow>) | Для формирования умения опознавать дипфейки и проверять сообщения на наличие дипфейков проводится мини-тренинг. Если у спикера в распоряжении изначально было чуть больше времени, то можно рассмотреть два дипфейка (приложения № 3 и приложение № 4), если нет, то только один – приложение №3. Сообщает задание: «Сейчас включим запись видеосообщения в мессенджере от мамы своему сыну. Ваша задача – определить, как действовать в этой ситуации, как отреагировать на просьбу».Включает видеозапись – приложение №3.Дает слово командам, комментирует ответ. И сразу же спрашивает: «Как вы опознали, что это дипфейк?» Предлагает посмотреть исходную запись: «А теперь давайте посмотрим исходную запись – это сотрудник федерального методического центра повышения финансовой грамотности на базе РАНХиГС (ФМЦ РАНХиГС) – Екатерина Михайловна Медякова – специально в обучающих целях записала это видео. А в роли «Мамы» выступила тоже преподаватель ФМЦ РАНХиГС, соавтор этого урока – Нина Рафаэловна Гукасова», – показывает фото из приложения № 3.Если у спикера есть дополнительное время, то продолжает: «Сейчас включим запись видеосообщения от взрослой дочери своей матери – женщине пенсионного возраста (приложение № 4), задача у вас такая же – определить стратегию поведения в данной ситуации, как ответить на просьбу».Включает видеозапись – приложение № 4.Дает слово командам, комментирует ответ.Завершает занятие:«Друзья! Мы с вами познакомились с дипфейками, увидели на примере достаточно публичного человека – Нины Рафаэловны, как можно подделать видеозапись, ведь у нее много видеолекций размещено в сети на различных ресурсах, она часто выступает на конференциях и вебинарах. Но и у непубличного человека сегодня большой объем видео находится в публичном доступе, в первую очередь в соцсетях. Поэтому всем нужно быть особенно внимательными!» | Внимательно слушают спикера.Смотрят видеозапись.Отвечают. Могу быть даны следующие ответы: * Нужно позвонить своей маме по телефону и все уточнить.
* Нужно просто проигнорировать, так как это мошенники.
* Видно, что это дипфейк и мама не настоящая (глаза немного странные, как будто бы стеклянные, небольшая рассинхронизация видео и звука, проскакивает нечеткое изображение и пр.). Могут быть даны другие ответы.

Смотрят видеозапись.Смотрят видеозапись.Отвечают. Могу быть даны ответы, подобные предыдущим.  | **6 мин.** |

|  |
| --- |
| **ЭТАП 4: РЕФЛЕКСИЯ, ПОДВЕДЕНИЕ ИТОГОВ (3 МИНУТЫ)** |

| **№ слайда и /или дидактич. материал** | **Деятельность спикера** | **Деятельность учащихся** | **Тайминг** |
| --- | --- | --- | --- |
| Слайд 15 | «Давайте еще раз проговорим:* Что такое дипфейк?
* Как опознать дипфейки?
* Как не попасться на уловки финансовых мошенников, использующих дипфейки?»

Дает обратную связь отвечающим на вопросы, повторяя кратко сказанное учениками. Не дает оценок. Не ставит отметок. | Слушает краткие ответы учащихся, комментирует при необходимости. | **2 мин.** |
| Слайды 16–19 «Что можно сделать, чтобы повысить свою финансовую грамотность» | «Обратите внимание, что сюжеты, связанные с финансовой грамотностью, часто встречаются в классической литературе. Прочитав эти книги, вы можете по-новому взглянуть на сюжет. Если же вы хотите проверить свои знания по финансовой грамотности, здесь вы можете увидеть список тематических олимпиад, в которых вы можете участвовать».Обращает внимание на информацию, размещенную на слайдах 18–19, о дополнительных ресурсах по финансовой грамотности: мультфильмах, подкастах, которые можно посмотреть и послушать вместе со своими родителями.Тем, кому интересна тема финансовой грамотности, рекомендует обратиться к информации на портале моифинансы.рф, на котором размещено много полезных образовательных и информационных материалов, и в социальных сетях портала.Прощается с детьми. | Смотрят на слайды, делают фото ссылок.Задают дополнительные вопросы спикеру. | **1 мин** |