

Что такое фейковые новости. Разбор для детей и родителей

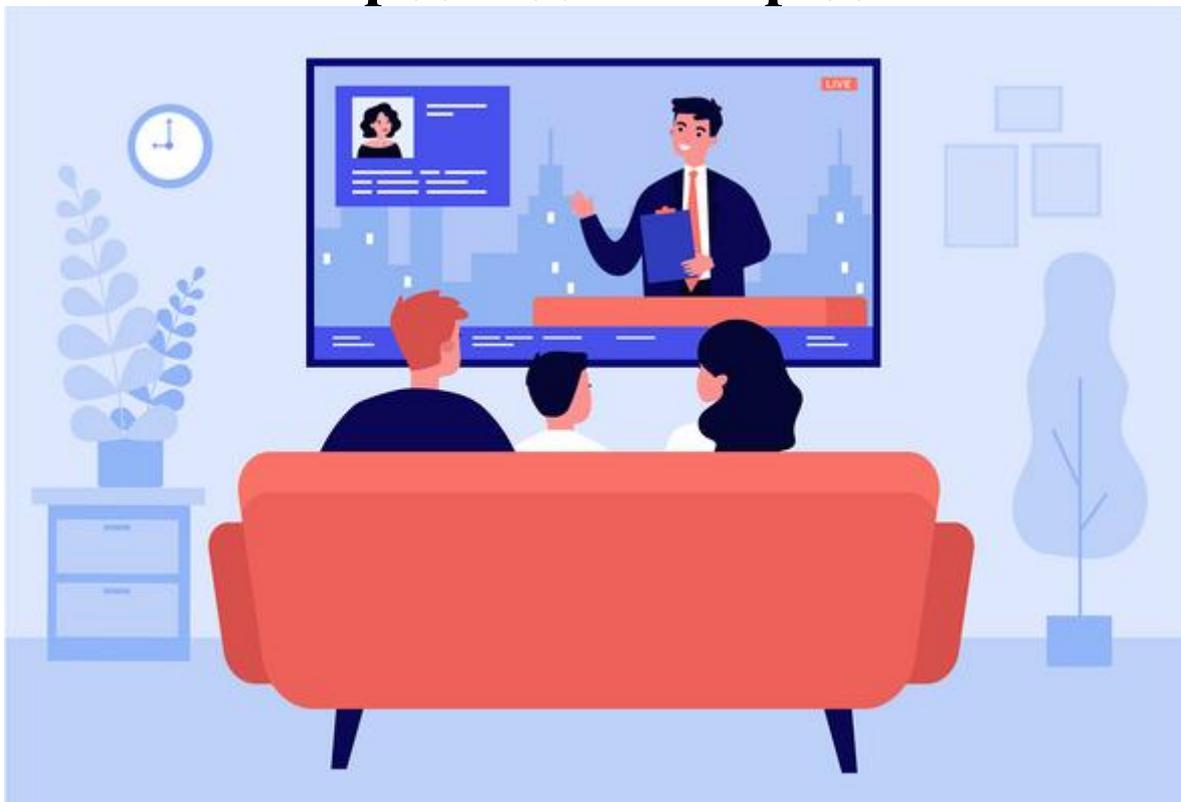


Иллюстрация: shutterstock / BRO.vector

Интернет даёт нам моментальный доступ к любой информации. Не только полезной и важной, но и недостоверной и заведомо ложной. Как научить ребёнка понимать, что перед ним обманка, рассказывает Андрей Сиденко, руководитель направления «Лаборатории Касперского» по детской онлайн-безопасности.

Почему фейков стало больше

Люди всегда приукрашали или искажали информацию. Рассказывая какие-либо истории, мы порой склоны добавлять что-то от себя, приукрашивать и даже исказить информацию (случайно или намеренно). И если раньше распространение такой информации ограничивалось кругом общения, то с распространением интернета, телефона, мессенджеров и других технологий выросли и масштабы, и аудитория, которая такую информацию может получить.

Теперь фейковый контент могут видеть сразу миллионы людей, а границы реальности стали все больше размываться. И речь здесь не только о полностью выдуманных новостях или роликах, в которых нет ни слова правды. Всё чаще мы сталкиваемся с контентом, правдивым лишь отчасти или составленным без должной фактической проверки. Намеренные подделки используются и для пропаганды, то есть манипулирования общественным мнением.

К неверному пониманию информации может привести спешка или невнимательность. В итоге этот фейковый контент формирует неверные представления в обществе. А иногда даже играет ключевую роль в том, что человек принимает неверные или даже опасные для него и окружающих решения.

Соцсети и мессенджеры отчасти стали дополнительным стимулом к массовому распространению фейковых новостей. Ведь там порой практически без ограничений и модерации может быть выложен любой контент. А с помощью определённых инструментов его легко раскручивать и выводить в топ.

Недостоверные новости — это, как правило, эмоционально окрашенные истории, которые получают много лайков и перепостов. А соцсети учитывают в том числе эту статистику, зачастую не фокусируясь на проверке того, насколько текст соответствует действительности. То есть алгоритмы позволяют раскручивать такой контент максимально быстро.

Конечно, соцсети активно модерируют контент, которым делятся пользователи. Но, как правило, это происходит автоматически с использованием специализированных технологий, поэтому далеко не всё удастся отследить. А иногда даже возникают курьезные случаи.



Видео и фото тоже можно подделать

Развитие технологий, в частности машинного обучения и нейросетей, привело к появлению и бурному развитию ещё одного вида подделок — дипфейков, то есть фото, видео или аудио, созданных при помощи специальных методов обработки

данных о человеке (фотографий, записей голоса и видео) с применением нейросетей.

Различные манипуляции с изображениями существовали ещё до появления компьютеров. Один из известных фейков — это фотография [фей](#), которую сделали две сестры в 1917 году. Подростки сумели ввести в заблуждение не только своих родителей, но и многих учёных (и, по некоторым источникам, даже самого сэра Артура Конан Дойла), хотя использовали достаточно простые методы. Они просто вырезали изображения фей из книги и прикрепили их к деревьям шпильками для шляп. Тем не менее подделка оказалась настолько успешна, что понадобилось несколько десятилетий, чтобы раскрыть её.

Дипфейки создаются на основе более продвинутых технологий. Они позволяют перенести лицо и мимику в новое видео, поменять речь человека и движения его губ, делать своего рода виртуальные копии людей. До недавнего времени подобное редактирование требовало достаточно большого уровня компетенций, но теперь достаточно базовых навыков

программирования. Современные программы позволяют создавать вполне правдоподобные видео- и аудиозаписи без наличия серьёзных технических навыков. Единственное, создание такого контента требует большого количества исходных данных (фото-, видео- и голосового контента).

Между исследователями, которые создают алгоритмы генерации дипфейков, и теми, кто анализирует способы их обнаружения, идёт своего рода гонка: когда обнаруживается несовершенство подделки, на её основе создают способ обнаружения, но следующее поколение алгоритмов уже исправляет эти недостатки.

Например, в 2018 году исследователи [обнаружили](#) одну особенность: в поддельных видео люди редко моргают. В современных дипфейках «проблем» с морганием уже нет. Есть идея определять сгенерированные фотографии людей по отражениям в глазах. Она может быть полезна, например, для обнаружения мошеннических профилей в соцсетях, прикрывающихся дипфейк-фотографиями, но это возможно только на фотографиях очень хорошего качества, оба глаза должны быть хорошо видны.

Как и любая технология, дипфейк может использоваться в разных целях. Это востребованный приём в кино-, рекламной и игровой индустрии ([вспомнить](#) хотя бы новый сериал или фильм по мотивам популярной космической саги). Есть примеры создания крайне достоверных дипфейк-видео: [Том Круз](#), показывающий фокусы и играющий в гольф, и альтернативное [обращение](#) королевы Елизаветы на Рождество на Channel 4.

Согласно результатам одного недавнего исследования, люди больше [доверяют](#) новостям в видеоформате и чаще делятся ими. К сожалению, эта особенность человеческой психики играет на руку злоумышленникам. Например, недавно в социальных сетях активно распространялось поддельное видео с образом Олега Тинькова. Оно было нацелено на вымогательство денег. А в 2019 году голосовой дипфейк был использован для разговора от имени руководителя одной зарубежной компании в сфере энергетики. Мошенники убедили его подчинённого перевести на их счёт 220 тысяч евро. В 2020 году с помощью дипфейк-технологии злоумышленники украли у банка в ОАЭ 35 миллионов долларов. Схема, в которой участвовали 17 человек, включала в себя подделанный голос и фальшивые электронные письма.

У многих фейковых видео плохое качество, поэтому их распространяют через соцсети. Мошенники рассчитывают, что пользователям, листаящим ленты соцсетей, покажется убедительным даже примерно похожий персонаж и логотип известного банка рядом. Подобным способом подделать могут кого угодно. Вероятно, количество случаев, когда злоумышленники будут использовать дипфейки, продолжит расти.

Как защитить себя и ребёнка от фейков

Важно: deepfake-технологии сами по себе не являются ни плохими, ни хорошими. Всё дело в том, для чего их используют.

И всё же — как уберечь ребёнка от шквала недостоверной информации? Регулярно повторять, что интернет — это огромное скопление не только фактов, но и мнений. Информация, которая туда поступает, создаётся обычными людьми. Далеко не все умеют взвешенно и осторожно обращаться с фактами.

Нужно скептически относиться к любой информации в сети и проверять её в разных источниках, прежде чем предпринимать какие-то действия. Перепроверяйте любые крайне щедрые предложения или предложения, которые требуют немедленного действия, например перейти по ссылке или перевести деньги.

Учите и учитесь сомневаться, не принимать всё на веру — это важный навык. То же касается дипфейков. Если вам попалось видео или голосовая запись, где известная личность предлагает поучаствовать, например, в беспроигрышной лотерее, не верьте сразу. Лучше перепроверить. Только мошенники обещают много денег просто так, и уж тем более никто из официальных лиц или банков не рекламирует бесплатную раздачу выплат или бонусы в 50%. Если вы видите в рекламном объявлении предложение большого количества денег, это должно насторожить.

Технологии монтажа развиваются очень быстро. Ищите данные в официальных источниках (например, на официальном сайте компании, от имени которой предлагается выплата или акция), прежде чем соглашаться на заманчивые предложения. И пользуйтесь защитными решениями с антифишинговыми технологиями на всех устройствах — они предупредят об опасности при переходе на мошеннические сайты.



Как определить, что новость фальшивая

Есть правила, которых стоит придерживаться, прежде чем распространять новость дальше. Особенно это касается сенсаций, которые затрагивают остроактуальные темы:

Иллюстрация: shutterstock / Sensvector

- Обязательно найдите информацию об авторе статьи, попробуйте найти другие его материалы и выяснить, какая у него репутация. Если в тексте, в котором содержатся выводы, претендующие на уникальность, автор не указан, это повод насторожиться.
- Проверяйте дату публикации: информация может быть просто-напросто устаревшей.

Небрежно составленные новости часто грешат большим количеством ошибок и опечаток. Фейковыми часто бывают новости, заголовки которых слишком эмоциональны, которые апеллируют к чувствам читающих их людей

и стремятся задеть за живое. Старайтесь воспринимать их не так эмоционально, отделять сухие факты от оценочных характеристик. А ещё проверяйте, соответствует ли содержание новости заголовку.

Приучайте себя и детей проверять новости и искать подтверждение информации в нескольких не зависимых друг от друга источниках. Если нет отсылки к первоисточнику, это повод задуматься, насколько правдива информация. Хороший признак, если в тексте содержатся ссылки, чтобы читатель мог самостоятельно проверить факты.

Возможен вариант, что новость оказывается шуткой, поэтому стоит проверять репутацию издания/сайта/портала, где она была опубликована изначально.

Главный совет — учите детей оценивать информацию непредвзято, объясняйте, что убеждения могут повлиять на восприятие информации. Но, конечно, в первую очередь нужно научиться этому самим.