ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

В МОШЕННИЧЕСКИХ СХЕМАХ

Как **новые технологии** делают привычные способы обмана убедительнее

ВОЗМОЖНОСТИ ИИ

Как ИИ используют мошенники

Генеративные технологии позволяют сделать привычные схемы обмана **гораздо правдоподобнее**.

С их помощью злоумышленники могут:

- имитировать голос и внешность человека;
- создавать реалистичные фотографии, видео и сообщения;
- копировать оформление сайтов известных компаний.

Поэтому знакомый голос, лицо на экране или привычный дизайн сайта **уже не являются критериями подлинности**.



СЦЕНАРИЙ 1

«Сообщение от начальника»

Сотруднику звонит или пишет человек, выдающий себя за руководителя. Для убедительности могут использоваться **сгенерированные голос, фотография или видео**.

Дальше **человека предупреждают**, например, о проведении плановой «проверки» и переводят на якобы сотрудника правоохранительных органов.

Что делать: прервать разговор и самостоятельно связаться с руководителем по известному вам номеру.



СЦЕНАРИЙ 2

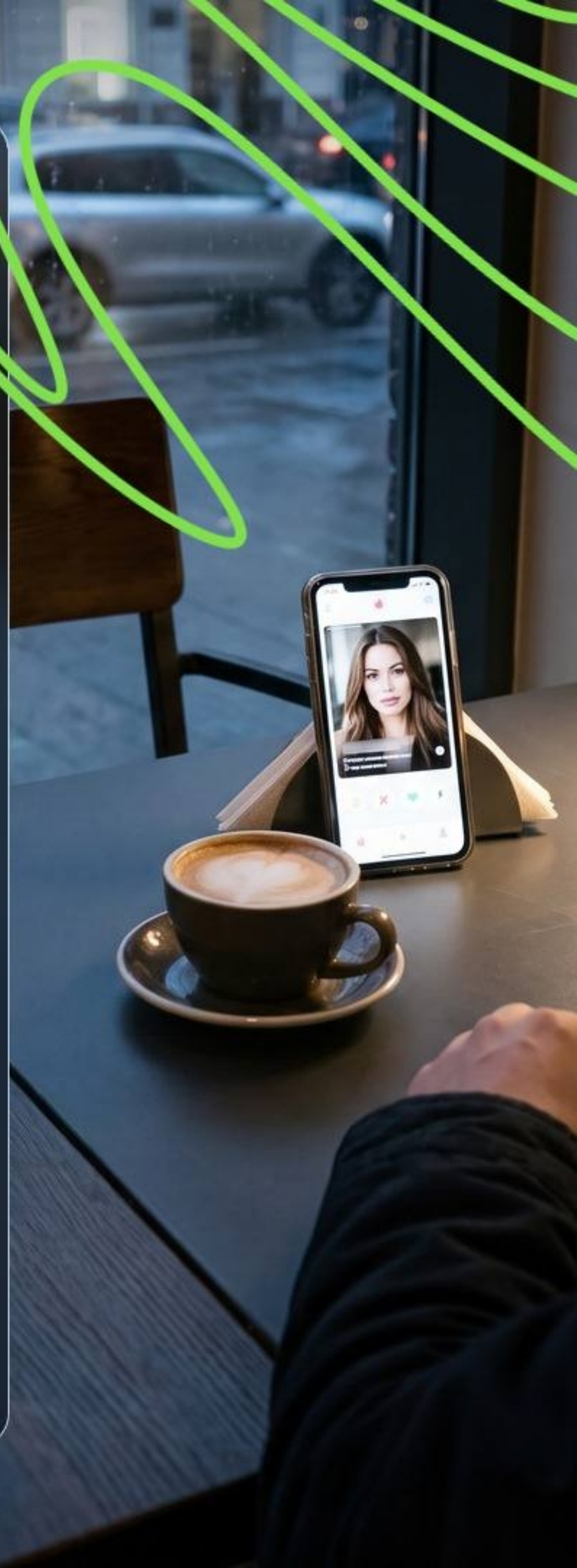
Знакомство с вымышленным собеседником

В **сервисах знакомств** мошенники могут использовать сгенерированные фотографии и голосовые сообщения.

Прикрываясь красивой девушкой или парнем, **аферист предлагает в чате:**

- “выгодно” заработать на инвестициях;
- перейти по фишинговой ссылке для приобретения билетов;
- одолжить деньги под предлогом “помощи”.

Если новое знакомство неожиданно переходит к теме денег и просьбам открыть ссылку — **прервите диалог**.



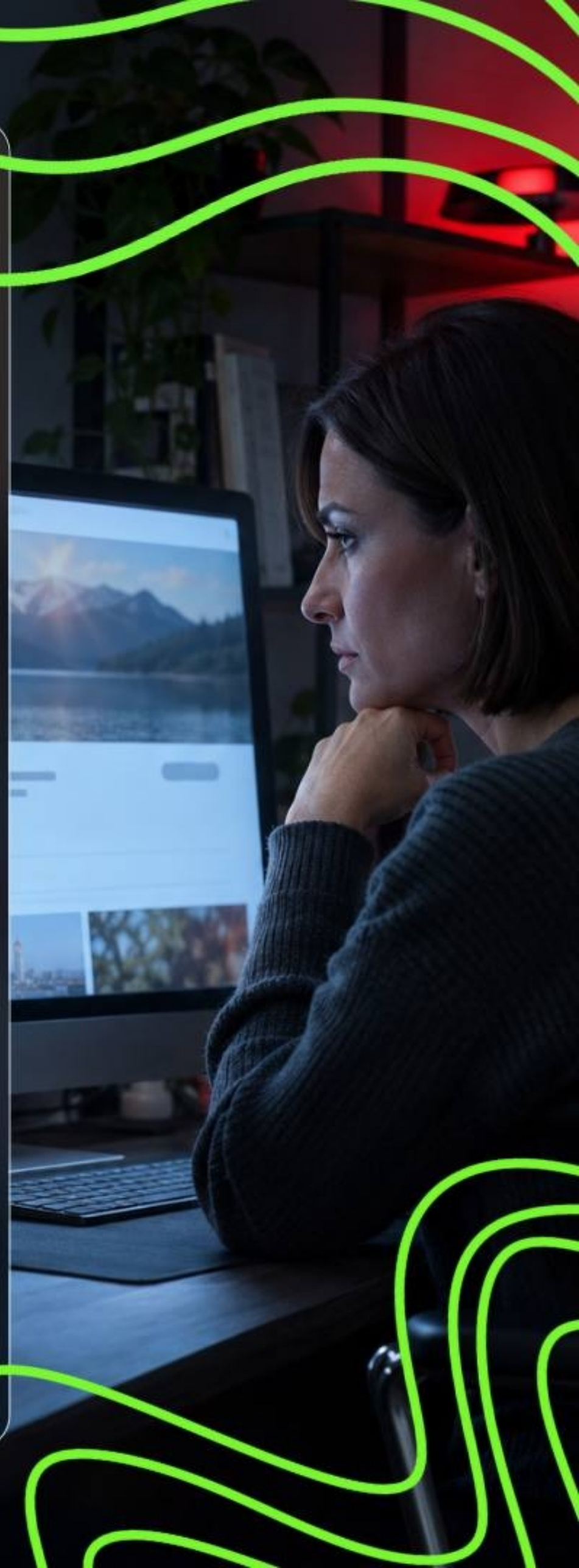
СЦЕНАРИЙ 3

Злоумышленники могут создавать ваши цифровые копии

Используя ИИ преступники могут **создавать ваших цифровых двойников** в соцсетях. Цели, которые преследуют злоумышленники:

Цели, которые преследуют злоумышленники:

- шантаж и предложения за деньги удалить опубликованную информацию;
- получение сведений у коллег и родственников о личной жизни, корпоративной или чувствительной информации;
- компрометация вашей личности для нанесения репутационного ущерба.



СЦЕНАРИЙ 4

Сайты-клоны

Злоумышленники могут использовать ИИ-технологии для создания **фишинговых сайтов** маркетплейсов или иных ресурсов.

Подделка может повторять:

- фирменный стиль;
- карточки товаров и отзывы покупателей;
- название адреса сайта.

Цель — похитить деньги с банковской карты или доступ к личному кабинету реального маркетплейса.

Поэтому важно проверять не только внешний вид страницы, **но и точный адрес сайта**.



СЦЕНАРИЙ 5

Сгенерированные изображения для шантажа

Используя технологии ИИ, преступники создают **компрометирующие фото жертвы**, а потом просят выкуп за нераспространение.

В такой ситуации важно:

- не выполнять требования аферистов;
- сохранить переписку и сведения об аккаунте;
- обратиться за помощью и сообщить в полицию.

Расчёт мошенников строится на страхе и желании человека **как можно быстрее решить внезапную проблему**.



Как защититься

Главное правило — не считать голос, фотографию или видео достаточным подтверждением личности.

Если **от имени знакомого человека или организации** вас просят перевести деньги, сообщить данные или срочно совершить какое-то сомнительное действие:



1

возьмите паузу и обдумайте все действия;

2

самостоятельно свяжитесь с человеком или организацией по известному номеру;

3

не сообщайте коды подтверждения и данные карты третьим лицам.

«

Развитие искусственного интеллекта заметно **усложняет распознавание мошеннических схем**. Сегодня знакомый голос, фотография, видеозапись или привычное оформление сайта уже не дают полной уверенности в том, что перед нами действительно тот человек или организация, за которых себя выдают злоумышленники.

Поэтому **должны меняться и наши привычки цифровой безопасности**. Если речь идёт о деньгах, персональных данных или срочной просьбе, информацию необходимо перепроверить самостоятельно — связаться с человеком или организацией через другой, заранее известный канал»

»



Артём Шейкин

Сенатор РФ, первый заместитель председателя Комитета Совета Федерации по конституционному законодательству и государственному строительству