

A man with dark hair and a serious expression is the central focus. His face is partially obscured by a translucent digital overlay on the right side, featuring binary code (0s and 1s), a network graph with glowing nodes, and a green line graph. The background is dark with faint, glowing blue and green digital patterns and code snippets.

МАКСИМ ГРОМОВ

ДИПФЕЙК

Как ИИ крадет ваши деньги, голос и личность.
Пошаговое руководство по цифровой
безопасности в эпоху нейросетей.

Максим Громов
ДИПФЕЙК: Как ИИ крадет
ваши деньги, голос и личность.
Пошаговое руководство
по цифровой безопасности
в эпоху нейросетей

<https://litres.ru/74397132>

SelfPub; 2026

Аннотация

ДИПФЕЙК: Как ИИ крадет ваши деньги, голос и личность. Пошаговое руководство по цифровой безопасности в эпоху нейросетей.

Раньше, чтобы украсть деньги, мошенникам нужны были коды из SMS. В 2026 году им достаточно трех секунд записи вашего голоса из соцсетей. Технологии дипфейков стерли границу между правдой и вымыслом: теперь верить своим глазам и ушам в интернете смертельно опасно для вашего кошелька.

Эта книга — независимое кибер-расследование и пошаговый гид по выживанию в цифровом мире. Максим Громов простым языком, без заумных терминов, раскрывает теневые схемы ИИ-мошенничества и дает конкретные инструменты защиты.

Вы узнаете:

- Как распознать поддельный звонок от близкого или начальника за 30 секунд.
- Как ИИ взламывает банковскую биометрию и как это предотвратить. Пять скрытых маркеров текста, написанного враждебной нейросетью.
- Как защитить пожилых родственников от голосовых роботов-вымогателей.

Защитите себя и свою семью, пока технологии не использовали против вас!

Содержание

Дисклеймер (Отказ от ответственности)	5
Введение. Когда твой собственный голос лжет твоей маме	7
Глава 1. Дипфейки голоса: как раскусить фальшивый звонок от близкого	9
Глава 2. ИИ-Ф	15
Конец ознакомительного фрагмента.	16

Максим Громов
ДИПФЕЙК: Как ИИ
крадет ваши деньги,
голос и личность.

Пошаговое руководство
по цифровой безопасности
в эпоху нейросетей

Дисклеймер (Отказ
от ответственности)

Важная информация и правовое ограничение:

Данная книга носит исключительно ознакомительный, информационный и образовательный характер и направлена на повышение цифровой грамотности населения. Все описанные схемы мошенничества приведены исключительно в целях демонстрации уязвимостей систем безопасности для последующей защиты от них.

Автор и издательство не призывают к совершению про-

тивоправных действий и категорически осуждают любое неправомерное использование технологий искусственного интеллекта. Автор не несет ответственности за любые прямые или косвенные убытки, кражу данных или финансовые потери, возникшие в результате действий третьих лиц (киберпреступников) или из-за халатного отношения читателя к личной цифровой гигиене. Применяя методы защиты из этой книги, читатель самостоятельно несет ответственность за безопасность своих устройств и банковских счетов.

Введение. Когда твой собственный голос лжет твоей маме

Представьте ситуацию: вашей маме или близкому человеку среди ночи звоните вы. Ваш голос, ваши интонации, ваше привычное «привет, тут такое дело...» и даже характерное покашливание. Вы взволнованно просите срочно перевести деньги на незнакомую карту, потому что попали в беду. Перепуганный родственник, не сомневаясь ни секунды, отправляет все свои сбережения. А через час выясняется, что вы в это время спокойно спали, а с вашей мамой разговаривал... робот.

Это не сценарий фантастического фильма. Это суровая реальность **2026 года**.

Искусственный интеллект принес человечеству колоссальный прорыв, но одновременно с этим он дал в руки мошенников и хакеров абсолютное оружие. Эпоха, когда обман в интернете можно было распознать по корявому тексту с кучей ошибок или странному акценту «сотрудника безопасности банка», официально закончена.

Сегодня нейросети пишут безупречные персональные письма от имени вашего генерального директора, генерируют видеозвонки, на которых вы видите лицо своего знакомого, и взламывают аккаунты, имитируя вашу биометрию. Мы

оказались в мире, где цифровая личность любого человека может быть скопирована, украдена и использована против него за несколько минут.

Эта книга написана не для того, чтобы напугать вас и заставить выбросить смартфоны. Моя цель как автора — выдать вам четкий, понятный и непробиваемый алгоритм защиты. Я разложил по полочкам самые опасные теневые ИИ-схемы этого года и превратил их в простые инструкции по кибер-выживанию.

Вы узнаете, как защитить свои деньги, как настроить гаджеты, чтобы перекрыть лазейки для нейросетей, и как внедрить в семье простые правила, которые не сможет обойти ни один самый продвинутый дипфейк в мире.

Пришло время вернуть контроль над своей цифровой жизнью. Переворачивайте страницу.

Глава 1. Дипфейки голоса: как раскусить фальшивый звонок от близкого

Самым опасным, массовым и циничным оружием киберпреступников стали **дипфейки голоса (Voice Cloning)**. Мошенники научились филигранно имитировать интонации, тембр и дефекты речи любого человека. Хуже всего то, что для создания идеальной цифровой копии вашего голоса преступникам больше не нужно записывать вас часами — современным нейросетям достаточно всего **трех секунд чистого аудио** из ваших соцсетей, голосовых сообщений в мессенджерах или случайного телефонного звонка.

Схема работает безупречно, потому что бьет по самому уязвимому месту — по эмоциям. Когда в трубке звучит испуганный, но до боли знакомый голос вашего ребенка, супруга или родителя, заявляющий, что он попал в беду, критическое мышление мгновенно отключается.

Как мошенники воруют ваш голос

Сбор материала: Злоумышленники сканируют ваши открытые профили. Видео в VK, короткие ролики, кружочки в Telegram или голосовые сообщения в открытых чатах — всё это идеальный материал для обучения ИИ.

Провокация по телефону: Если записей в сети нет, вам просто звонят с незнакомого номера. Вы поднимаете трубку, говорите: «Да, алло, слушаю вас». Этого «да, алло» уже достаточно, чтобы робот вырезал ваш голос и пустил его в обработку.

Генерация текста: Преступники вводят в специальную нейросеть нужный им текст (например, требование перевести деньги), и ИИ озвучивает его вашим точным голосом.

Техника защиты 1. Семейный кодовый пароль

Ни один, даже самый продвинутый искусственный интеллект в мире не может прочитать мысли человека. Единственный стопроцентный способ защитить свою семью от голосовых дипфейков — это внедрить **семейный кодовый пароль**.

Соберите своих близких (особенно пожилых родителей и детей) и договоритесь об одном секретном слове или фразе, которую знаете только вы. Это может быть кличка вашего первого домашнего питомца, девичья фамилия бабушки или любое абсурдное слово (например, «зеленый чемодан»).

Правило безопасности: Если вам или вашим близким поступает экстренный звонок с просьбой о деньгах, первое, что нужно сказать в трубку, спокойно и без паники: «**Назови наше семейное кодовое слово**». Если на том конце

провода мошенник, робот начнет уходить от ответа, злиться, давить на жалость или просто бросит трубку.

Техника защиты 2. Тест на «цифровую склейку»

Искусственный интеллект генерирует речь невероятно качественно, но физику обмануть сложно. Если вы подозреваете, что разговариваете с роботом, обратите внимание на следующие маркеры:

Идеальная тишина на фоне: Нейросети создают голос в стерильной цифровой среде. Если ваш «близкий» утверждает, что попал в аварию или сидит в отделении полиции, но вокруг него стоит абсолютная, гробовая тишина без единого шороха — это повод насторожиться.

Странные паузы: Роботу нужно время (доли секунды), чтобы обработать ваш ответ и сгенерировать новую реплику. Если в разговоре возникают неестественные, одинаковые по длительности паузы перед каждым ответом — перед вами ИИ.

Механические вдохи: Обратите внимание на то, как «человек» дышит. Нейросети часто вставляют звуки вдоха в случайные места невпопад с логикой предложения.

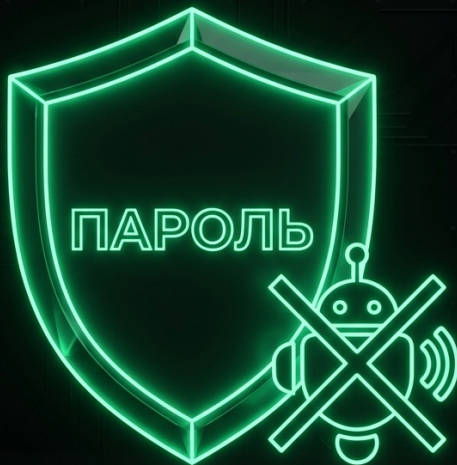
Инструмент выживания: Чек-лист экстренных действий при странном звонке

Если вам позвонил близкий человек и просит денег, выполните три шага строго по порядку:

Сбросьте звонок. Не продолжайте диалог.

Перезвоните сами. Наберите этого человека по его обычному номеру телефона (или через сотовую связь, или в мессенджере, где вы всегда общаетесь). Если его телефон занят или недоступен — не паникуйте. Мошенники часто используют автодозвон, чтобы «забить» линию жертвы.

Напишите текстовое сообщение. Задайте в чате интимный вопрос, ответ на который знает только он (например: *«Что мы ели сегодня на завтрак?»* или *«В какой куртке ты сегодня вышел из дома?»*).



Глава 2. ИИ-Ф

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.