12+

Данила Щербаков

Эпоха синтетического доверия



Данила Щербаков

Эпоха синтетического доверия

«Издательские решения»

Щербаков Д.

Эпоха синтетического доверия / Д. Щербаков — «Издательские решения»,

Эпоха синтетического доверия — это первое масштабное исследование индустрии обмана XXI века. Дипфейки, романтический скам, криптопирамиды, звонки от «службы безопасности» — как устроены схемы, которые каждый день крадут миллиарды? Почему умные люди попадаются на глупые разводы? И как защитить себя, близких и бизнес в мире, где голос и лицо больше не доказательство? Книга, после которой вы уже никогда не поверите звонку с незнакомого номера.

© Щербаков Д.
© Издательские решения

Содержание

Эпоха синтетического доверия 6
Содержание 7
Введение. Смерть наивности 8
Один звонок 9
Почему «наивность» умерла 10
Как устроена книга 11
Вместо эпиграфа 12
Часть I. Анатомия обмана 13
Три поколения обмана 14
Что изменилось: экономика обмана 16
Мошенник как предприниматель 17
Новая невидимость 18
Эволюция жертвы 19
Две системы: быстрая и медленная 21
Эмоциональный хайджек 22
Иллюзия исключительности 23
Принцип доверия по умолчанию 24
Нормализация абсурда 25
Что делать с этим знанием 26
Что говорит наука о психопатии 28
Треугольник мошенничества 29
Когда давление создаёт организация 30
Двойная жизнь и самообман 32
Две стороны одного конвейера 33
Почему общество проигрывает психологически 34
Сигналы внутри организации 35
Часть II. Арсенал иллюзий 36
Откуда пошло название 37
Конец ознакомительного фрагмента. 38

Эпоха синтетического доверия

Данила Щербаков

© Данила Щербаков, 2026

ISBN 978-5-0071-4859-7
Создано в интеллектуальной издательской системе Ridero

Эпоха синтетического доверия

Как мошенничество перепрошило современный мир

Содержание

Введение. Смерть наивности 4

Часть I. Анатомия обмана 9

Глава 1. Эволюция аферист: от карманника до CEO теневой корпорации 10

Глава 2. Взлом мозга: почему умные люди попадаются на глупые разводы 22

Глава 3. Психопатология успеха: кто такие современные мошенники и как они оправдывают свои действия 34

Часть II. Арсенал иллюзий 46

Глава 4. Социальная инженерия 2.0: когда «службой безопасности» звонит нейросеть 47

Глава 5. Романтика скама: ловушки одиночества и фейковые отношения 59

Глава 6. Крипто-пирамиды и NFT-пузыри: как жадность монетизируется в реальном времени 72

Глава 7. Дипфейки и синтез реальности: конец эры «увидеть — значит поверить» 85

Часть III. Теневая экосистема 97

Глава 8. Конвейер лжи: как устроены современные колл-центры и даркнет-маркетплейсы 98

Глава 9. Дроповоды и отмывочные линии: невидимые солдаты финансовой войны 111

Глава 10. Государство и скам: когда мошенничество становится инструментом геополитики 124

Часть IV. Иммунитет общества 138

Глава 11. Цифровая гигиена: как защитить себя, своих родителей и свой бизнес 139

Глава 12. Оружие возмездия: как ИИ и блокчейн помогают ловить аферистов 153

Глава 13. Кризис доверия: как общество адаптируется к миру тотального обмана 167

Эпилог. Будущее без иллюзий 181

Приложения 187

Приложение А. Хронология: как менялся обман 188

Приложение Б. Глоссарий 191

Приложение В. Мифы и факты 194

Приложение Г. Памятка «Пять красных флагов» 196

Приложение Д. Семейное соглашение о безопасности 197

Приложение Е. Как говорить с близким, которого могут обманывать 199

Приложение Ж. Календарь цифровой гигиены 201

Приложение З. Карточка на случай инцидента (для бизнеса) 202

Приложение И. Куда обращаться 203

Приложение К. Самопроверка: насколько вы защищены 205

Приложение Л. Рекомендуемое чтение 207

Введение. Смерть наивности

Мы привыкли думать, что мошенничество — это удел маргиналов. Карманники в метро, гадалки на вокзалах, продавцы поддельных шуб. Но посмотрите вокруг. Мошенничество больше не является преступлением на обочине общества. Оно стало его фундаментом.

Сегодня индустрия обмана оценивается в триллионы долларов. Это не просто криминал; это высокотехнологичная индустрия с собственными HR-отделами, скриптами, аналитическими центрами и службами поддержки. Мошенники первыми внедряют искусственный интеллект, они первыми тестируют новые уязвимости человеческой психики и опережают законодателей на десятилетия.

Главная проблема современного мира заключается не в том, что нас обманывают. Главная проблема в том, что **само понятие истины размыто**. В эпоху дипфейков, ботов и алгоритмических пузырей мы больше не можем доверять своим глазам и ушам. Доверие — социальный клей, на котором держалась человеческая цивилизация, — стало уязвимостью. И именно эту уязвимость эксплуатирует современная индустрия обмана.

Эта книга — не просто сборник советов «как не перевести деньги на левый счет». Это попытка понять, как устроена машина обмана, почему наш мозг, созданный для выживания в саванне, беспомощен перед алгоритмами, и как нам научиться жить в мире, где каждая цифровая улыбка может быть сгенерирована кодом.

Один звонок

Начнём с картины, которую легко представить. Условный пример: обычный вторник, середина рабочего дня. Человек сидит над срочным отчётом, телефон лежит рядом. Звонит неизвестный номер. Голос вежливый, спокойный, профессиональный. Он называет имя, фамилию, последние четыре цифры карты. Сообщает, что только что зафиксирована попытка вывести деньги со счёта, и просит не прерывать разговор.

Через двадцать минут человек выходит на улицу, чтобы «безопасно» установить приложение, о котором ему рассказали. Через сорок — всё уже случилось. Он не глупец и не жадина. Он образован, внимателен, читал о подобных схемах. Просто на этот раз ему позвонили в момент, когда голова была занята другим, и голос в трубке звучал так, как должен звучать голос человека, который хочет помочь.

Это условная история, но каждый её элемент основан на реальных схемах, о которых сообщают банки и правоохранительные органы разных стран. И именно такие истории, а не героические аферы из кино, составляют ткань современной преступности. Они незаметны, массовы и разрушительны для тех, кто попал.

Почему «наивность» умерла

Название введения может показаться слишком громким. Что значит «смерть наивности»? Люди всегда обманывали друг друга. Вопрос в масштабе и условиях.

Раньше наивность была в некотором смысле допустимой роскошью. Если вас обманывали, это был локальный эпизод: один торговец, один рынок, один город. Общество умело справляться с этим: репутации, слухи, суды, поручительства. Доверие передавалось от человека к человеку, и обманщика рано или поздно узнавали в лицо.

Сегодня обманщик может быть в другой стране, говорить на вашем языке без акцента, знать о вас больше, чем знает сосед, и работать одновременно с тысячами людей. Репутацию не накопишь, потому что личность подделывается. Слухи не успевают распространиться. А суды бессильны там, где преступник недосягаем.

В таких условиях наивность перестаёт быть невинной чертой характера. Она становится *уязвимостью*, которую можно эксплуатировать массово. Умирает не доверие вообще, а доверие по умолчанию: готовность верить на слово любому, кто звучит убедительно.

Что эта книга обещает и чего не обещает

Честность требует сказать заранее.

Книга не обещает полной защиты. Такой защиты не существует, и тот, кто её обещает, либо заблуждается, либо продаёт что-то. Любой человек в плохой день, в состоянии стресса, истощения или горя может стать жертвой.

Книга не обещает простых рецептов вроде «никому не верьте». Мир, в котором никому нельзя верить, невыносим, и он тоже проигрывает преступникам: параноидальное общество парализовано, а изоляция — лучший друг мошенника.

Книга обещает понимание. Если вы знаете, как устроен механизм, вы замечаете его в действии. Если вы понимаете, *почему* ваша психика реагирует на определённые сигналы, вы можете построить привычки, которые срабатывают даже тогда, когда эмоции берут верх.

И она обещает уважение к жертвам. Мы будем говорить о тех, кто обманут, без снисхождения и без осуждения. Обмануть можно любого. Разница лишь в том, как точно подобран ключ.

Как устроена книга

Книга состоит из четырёх частей.

Часть I «Анатомия обмана» объясняет, кто такие мошенники и как работает человеческая психика, делающая обман возможным. Это фундамент: без него остальное превращается в набор страшных историй.

Часть II «Арсенал иллюзий» описывает конкретные инструменты: телефонные схемы, романтические аферы, финансовые пирамиды, технологии синтеза реальности.

Часть III «Теневая экосистема» показывает обратную сторону: как устроена индустрия, которая стоит за единичными обманами, от колл-центров до международной политики.

Часть IV «Иммунитет общества» посвящена тому, что можно сделать: личные привычки, технологии защиты, изменения в институтах и новая культура доверия.

Каждая глава заканчивается кратким резюме и вопросами для размышления. Примеры основаны на реальных, публично описанных событиях; там, где история условная, это сказано прямо. Цифры в книге приводятся как порядки величин и ориентиры, потому что статистика мошенничества неточна по своей природе: многие случаи никогда не попадают в отчёты.

Вместо эпиграфа

Если вам нужна одна мысль, с которой стоит войти в эту книгу, пусть она будет такой: **быть обманутым не стыдно, стыдно делать вид, что с тобой этого не случится**. Всё остальное мы будем разбирать по порядку.

Часть I. Анатомия обмана

Глава 1. Эволюция аферист: от карманника до CEO теневой корпорации

В 1925 году в Париже скромный господин в хорошем костюме пригласил нескольких торговцев металлоломом в дорогой отель. Он представился заместителем генерального директора министерства почт и телеграфов и сообщил по секрету: Эйфелева башня обветшала, содержать её слишком дорого, и правительство решило её продать на слом. Тендер закрытый. Огласка нежелательна.

Один из торговцев, Андре Пуассон, был уязвлён тем, что его раньше не звали в «серьёзные» круги. Он выиграл «тендер», заплатил взятку чиновнику, чтобы ускорить сделку, и отдал деньги. Чиновником был Виктор Люстиг, и он уже ехал в Вену с чемоданом наличных. Пуассон так стыдился своей доверчивости, что не пошёл в полицию. Люстиг вернулся и повторил трюк.

Эта история стала хрестоматийной не потому, что она смешна. Она показывает главное: **аферист продаёт не товар, а историю, в которой жертве отведена лестная роль**. Менялись эпохи, инструменты и масштабы, но эта формула осталась прежней.

Анатомия одной аферы: как Люстиг строил свою историю

Стоит присмотреться к «продаже Эйфелевой башни» внимательнее, потому что почти каждый её элемент встречается в современных схемах.

Правдоподобная предпосылка. Башню строили как временное сооружение для Всемирной выставки 1889 года, и разговоры о её сносе действительно велись. Затраты на содержание были реальной темой в прессе. Люстиг не выдумал ситуацию с нуля. Он взял правдивую деталь и достроил вокруг неё вымысел. Лучшая ложь всегда опирается на кусочек истины.

Антураж. Встреча проходила не в кафе, а в роскошном отеле «Крийон», где останавливались дипломаты. Фирменные бланки, печати, уверенный тон. Обстановка работала как доказательство: если человек принимает в таком месте, значит, он тот, за кого себя выдаёт.

Отбор жертв. Люстиг не приглашал первых встречных. Он выбирал честолюбивых торговцев, которые мечтали выйти на новый уровень. Позже он рассказывал (по крайней мере, так утверждают его биографы), что искал людей, которых легко задеть за самолюбие.

Секретность. Сделку объявили конфиденциальной. Это решало сразу две задачи: объясняло, почему о «продаже» никто не слышал, и мешало жертве посоветоваться с кем-то, кто мог бы заметить обман.

Взятка как способ закрыть дело. Здесь самый тонкий ход. Когда Пуассон засомневался, Люстиг намекнул, что чиновнику нужна «благодарность». Жертва предложила взятку сама и тем самым стала соучастницей. Человек, участвовавший в сомнительном деле, редко идёт в полицию: ему есть что скрывать.

Если заменить «Эйфелеву башню» на «закрытый инвестиционный пул», «отель» на «красивый сайт», а «взятку» на «комиссию за разблокировку», получится сценарий любой современной аферы. Меняется декорация, не драматургия.

Судьба самого Люстига тоже поучительна. Он скрылся в Америке, активно работал там в 1920—1930-х годах, был арестован за фальшивомонетничество и умер в тюрьме в 1947 году. Часть связанных с ним анекдотов, включая известную историю о ссуде, взятой у знаменитого гангстера, носит легендарный характер, и достоверно проверить её невозможно. Это ещё одна черта мира обмана: вокруг мошенников быстро вырастает мифология, и отличить факты от красивых рассказов бывает трудно.

Три поколения обмана

Историю мошенничества удобно разделить на три эпохи, каждая из которых меняла не саму суть обмана, а его *масштаб* и *стоимость*.

Первая эпоха: личный контакт. Карманник, напёрсточник, гадалка, «продавец» золотых часов. Мошенник работал лицом к лицу. Его главным ресурсом было умение читать людей: взгляд, одежда, походка, интонация. Масштаб ограничивался физическим присутствием: один человек мог обмануть десятки, в лучшем случае сотни людей за карьеру. Риск был высоким: жертва видела лицо и могла позвать полицию.

Любопытно, что многие приёмы этой эпохи пережили столетия. «Испанский узник», классическая афера, известная ещё с конца XVIII века, строилась так: к жертве обращался человек, рассказывавший о богатом заключённом в испанской тюрьме, который готов щедро заплатить за помощь в освобождении. Нужно было лишь внести небольшую сумму на «взятки» и «оформление». Затем возникали новые «непредвиденные расходы». Если вы читали современное «нигерийское письмо» (о нём ниже), вы читали «испанского узника» в электронной упаковке.

Вторая эпоха: масс-медиа и почта. Появление почты, телеграфа, а затем телефона разорвало связь между аферистом и местом преступления. Теперь не нужно было стоять перед жертвой.

В 1919—1920 годах Чарльз Понци в Бостоне за считанные месяцы собрал миллионы долларов, пообещав инвесторам 50% прибыли за 45 дней. Он утверждал, что зарабатывает на разнице цен международных почтовых купонов: купоны можно было купить дёшево в одной стране и обменять на марки в другой. Сама идея арбитража имела под собой реальные основания. Беда была в том, что операции такого масштаба на практике были почти невозможны из-за бюрократии и ограниченного числа купонов. Выплаты старым вкладчикам шли за счёт денег новых. Схема, которая теперь носит его имя, потребовала лишь газетных публикаций, уверенного обаяния и репутации успешного бизнесмена. Когда журналисты и финансовые аналитики начали задавать вопросы о том, сколько купонов вообще существует в природе, пирамида рухнула за считанные недели.

Следующий скачок пришёл вместе с массовым телевидением и государственной неразберихой. В России 1990-х «МММ» Сергея Мавроди превратила рекламный ролик с вымышленным героем Лёней Голубковым в национальный феномен: миллионы людей вложили сбережения в пирамиду, которая рухнула в 1994 году. Мошенничество впервые стало *публичным шоу*, а доверие к бренду заменило доверие к человеку. В стране, где многие только начали сталкиваться с рынком, где рушились старые гарантии и ещё не появились новые, рекламный герой в скромной куртке, «простой мужичок», вызывал больше доверия, чем официальные банки.

Заметим: ни Понци, ни Мавроди не были «карманниками». Они продавали *идею*: идея справедливости, доступа к тайному знанию, возможности «догнать» тех, кто уже разбогател. Это было мошенничество нового типа: обман через инфраструктуру доверия, а не через личный контакт.

Третья эпоха: интернет. С появлением электронной почты стоимость контакта упала почти до нуля. Знаменитые «нигерийские письма», известные как скам «419» по номеру статьи нигерийского уголовного кодекса, рассылались миллионами. Над ними смеялись из-за корявой грамматики и абсурдных историй о наследстве. Но смеялись зря: *корявость была частью фильтра*. Письмо, в которое поверит лишь самый доверчивый, экономит время мошенника: не нужно тратить усилия на тех, кто всё равно бросит на полпути. Тот, кто дошёл до третьего письма и готов отправить первые деньги, с высокой вероятностью дойдёт до конца.

Интернет добавил ещё два ключевых изменения. Во-первых, **анонимность**: жертва не видит лица, не знает страны и не может проверить, существует ли организация. Во-вторых, **масштабируемость**: одно и то же письмо или сайт можно показать миллионам людей практически без дополнительных затрат. То, что раньше требовало армии агентов, теперь делает один компьютер.

Что изменилось: экономика обмана

Чтобы понять современное мошенничество, нужно отказаться от образа одинокого хитреца. Сегодня это **бизнес-процесс**.

В нём есть:

— **Разделение труда.** Одни собирают базы данных (утечки, парсинг соцсетей), другие создают сайты и приложения-приманки, третьи ведут разговор с жертвой, четвёртые выводят и обналичивают деньги.

— **Скрипты и A/B-тестирование.** Тексты сообщений и сценарии звонков проверяются на конверсию так же, как рекламные кампании. Побеждает формулировка, которая чаще вызывает нужную реакцию.

— **Аналитика и обратная связь.** Операторы получают отчёты, лучшие сотрудники получают бонусы, слабые заменяются.

— **Услуги «под ключ».** Модель «преступление как услуга» (crime-as-a-service) позволяет новичку без технических навыков купить готовый набор: фишинговую страницу, список жертв, инструкцию. Порог входа в профессию упал до нескольких десятков долларов.

Эта индустриализация изменила главное: **себестоимость одной попытки обмана стремится к нулю**. Если рассылка стоит копейки, достаточно, чтобы клюнул один из тысяч. Мошенникам больше не нужно быть убедительными для всех. Им нужно быть убедительными для немногих, но показать себя как можно большему числу людей.

Вот простая иллюстрация. Допустим, мошенник рассылает миллион сообщений, и лишь одно из десяти тысяч приводит к потере денег. Это сто пострадавших. Если средняя потеря составляет пятьдесят тысяч рублей, общий ущерб достигнет пяти миллионов, и это при том, что 99,99% получателей не поддались на обман. Для отдельного человека вероятность стать жертвой ничтожна. Для общества суммарный ущерб колоссален. Именно эта асимметрия объясняет, почему многие продолжают считать мошенничество чем-то «не про меня», пока оно не случится с ними.

Мошенник как предприниматель

Показательна судьба Бернарда Мэдоффа. Он не прятался в тени: возглавлял совет директоров биржи NASDAQ, был уважаемым филантропом, управляющим фондом, куда стояли в очереди за право вложить деньги. Его пирамида рухнула в декабре 2008 года, на фоне мирового финансового кризиса, когда клиенты начали массово требовать свои деньги и их просто не оказалось. Мэдофф признал, что на счетах, которые он показывал клиентам, значилось около 65 миллиардов долларов, но значительная часть этих сумм была фиктивной. Реальные потери вкладчиков оценивались десятками миллиардов долларов. В 2009 году он был приговорён к 150 годам тюрьмы.

Мэдофф продавал не доходность, а *эксклюзивность* и *стабильность*. Его фонд не обещал заоблачных процентов. Он показывал скромные, но подозрительно ровные результаты год за годом, и именно эта ровность создавала впечатление мастерства. Люди верили не цифрам, а ощущению, что они допущены в закрытый клуб. Многие из его клиентов были представителями одних и тех же общин и профессиональных кругов: доверие передавалось по цепочке знакомств. Исследователи называют это *аффинитивным мошенничеством*: обман, который распространяется внутри группы, где люди доверяют друг другу по признаку общей идентичности.

Это важный урок: самые крупные аферы редко выглядят как афера. Они выглядят как легальный бизнес с офисом, лицензиями, красивыми отчётами и благодарными клиентами. Граница между «агрессивным маркетингом», «серой схемой» и откровенным обманом бывает тонкой, и именно в этой полосе работают самые изобретательные люди.

Показательно и другое. Сигналы тревоги существовали давно: независимые аналитики ещё в начале 2000-х указывали, что результаты фонда математически невероятны. Регуляторы получали жалобы и предупреждения. Но репутация Мэдоффа оказалась сильнее аргументов. Институты не проверили то, что считали «слишком известным, чтобы быть обманщиком». Доверие к человеку заменило проверку фактов.

Новая невидимость

Старый мошенник был виден. Его можно было описать, нарисовать фоторобот, проследить. Современный остаётся *невидимым* по трём причинам.

— **Дистанция.** Звонок идёт из другой страны, через цепочку подменных номеров и облачных АТС. Жертва и преступник могут находиться в разных часовых поясах и никогда не встретиться.

— **Анонимность платежей.** Криптовалюты, цепочки подставных счетов и «дропы» (людей, чьи банковские карты используются для транзита денег) разрывают след между украденной суммой и конечным получателем.

— **Юрисдикционный разрыв.** Следователь одной страны почти не может принудить к сотрудничеству полицию другой. Пока идут межгосударственные запросы, деньги давно разошлись по десяткам счетов.

Именно поэтому раскрываемость таких преступлений остаётся пугающе низкой, а большинство жертв даже не обращается в полицию: стыд, неверие в результат, усталость от бюрократии.

Эволюция жертвы

Если мошенник менялся, то менялась и жертва. В эпоху личного контакта обманутым оказывался человек, которого мошенник мог увидеть, оценить и выбрать. Сегодня выбор делает *алгоритм*: он ищет тех, кто оставил следы в утечках, кликал по определённым рекламам, проявлял интерес к конкретным темам. Вас выбирают не по лицу, а по цифровой тени.

В то же время изменилась и среда, в которой человек принимает решения. Мы живём в потоке информации, у нас не хватает времени вникать в детали, и мы привыкли полагаться на быстрые сигналы: логотип, количество отзывов, «галочку» верификации, знакомый голос. Каждый из этих сигналов подделывается, и мошенники научились подделывать именно их. Мы словно ходим по городу, где вывески можно переклеить за секунду, а прохожие давно перестали проверять адреса.

Почему это работает до сих пор

Если сравнить Люстига с современным колл-центром, различия очевидны. Но есть то, что связывает их через столетие, и это *человеческая психика*. Любая афера, от «продажи» Эйфелевой башни до дипфейк-звонка от «директора», опирается на одни и те же рычаги:

— **Авторитет** (министерство, банк, служба безопасности, начальник);

— **Срочность** (сегодня, сейчас, пока не поздно);

— **Секретность** (никому не говорите, это закрытая информация);

— **Эксклюзивность** (мы выбрали именно вас);

— **Страх и надежда**, два полюса, между которыми человеческий разум охотно теряет критичность.

Социальный психолог Роберт Чалдини в своих работах о механизмах влияния описал многие из этих принципов: авторитет, дефицит, социальное доказательство, взаимность. Мошенничество не изобретает новых законов психологии. Оно просто использует известные против интересов человека.

Технологии меняют лишь упаковку. Поэтому следующая часть книги посвящена не технике, а тому, что происходит в вашей голове в тот момент, когда вы нажимаете кнопку «Подтвердить».

Главное из главы

— Мошенник продаёт не товар, а *историю*, в которой жертве отведена привлекательная роль.

— Эпохи обмана различаются не сутью, а масштабом: личный контакт, затем масс-медиа, затем интернет с нулевой стоимостью контакта.

— Современное мошенничество — это бизнес-процесс с разделением труда, скриптами и аналитикой.

— Самые крупные аферы выглядят как легальный бизнес. Репутация обманщика может служить его лучшей защитой.

— Психологические рычаги (авторитет, срочность, секретность, эксклюзивность, страх и надежда) остаются прежними. Меняются каналы и инструменты.

Вопросы для размышления

— Какие элементы «продажи Эйфелевой башни» вы узнаёте в современных сообщениях и звонках, которые получали сами или ваши знакомые?

— Почему человек, ставший соучастником сомнительной сделки, реже обращается в полицию? Как это используют мошенники?

— Что даёт больше защиты: умение распознать конкретную схему или привычка проверять любое неожиданное предложение независимо от того, как оно выглядит?

Глава 2. Взлом мозга: почему умные люди попадаются на глупые разводы

«Со мной такого не случится. Я же IT-специалист / юрист / профессор». Это первая фраза, которую произносят жертвы, когда к ним приходит осознание произошедшего.

Когнитивное искажение, известное как «иллюзия уязвимости», заставляет нас верить, что обманывают только глупых, жадных или пожилых людей. Но статистика неумолима: среди жертв сложных финансовых афер и романтических скамов огромный процент составляют высокообразованные люди с высоким IQ.

Почему? Потому что мошенники не взламывают ваши пароли. Они взламывают вашу лимбическую систему.

Почему «умный» не значит «защищённый»

Начнём с развенчания самого популярного утешения: «Обманывают тех, кто недостаточно образован». Исследования жертв мошенничества показывают более сложную картину. Образование и интеллект сами по себе не гарантируют защиты, а иногда создают дополнительный риск: уверенность в собственной проницательности притупляет осторожность. Человек, привыкший успешно решать сложные задачи, склонен считать, что решит и эту, самостоятельно, без совета, «разберусь сам».

Есть и более точное наблюдение. Мошенничество нацелено не на *знания*, а на *состояние*. Профессор может разбираться в тонкостях квантовой физики и при этом принять сообщение о «блокировке карты» за чистую монету, если оно пришло в момент, когда он опаздывает на лекцию и телефон разряжается. Защита зависит не от IQ, а от того, сколько у вас в данный момент свободных когнитивных ресурсов: времени, внимания, спокойствия, сна.

Показательны и данные о том, кто реже или чаще теряет деньги. По сообщениям американских регуляторов, молодые взрослые нередко чаще сообщают о том, что столкнулись с мошенничеством и потеряли деньги, а пожилые люди реже, но теряют в среднем гораздо более крупные суммы, поскольку накопили больше сбережений. Это не противоречит друг другу. Это означает, что уязвимы все, просто разными способами.

Две системы: быстрая и медленная

Чтобы понять, что происходит в голове жертвы, полезна идея, которую популяризировал психолог и нобелевский лауреат Даниэль Канеман. Человеческое мышление можно условно представить как работу двух систем.

Система 1 быстрая, автоматическая, эмоциональная. Она мгновенно узнаёт лица, оценивает угрозы, реагирует на тон голоса. Она работает без усилий и почти без нашего участия.

Система 2 медленная, аналитическая, требует внимания. Она проверяет, считает, сравнивает, сомневается. Но она энергозатратна, легко утомляется и включается только тогда, когда мы её «зовём».

В обычной жизни Система 1 справляется с большинством задач, и это хорошо: иначе мы бы не успевали жить. Но у неё есть уязвимость: *она склонна верить тому, что звучит правдоподобно и вызывает эмоцию*. Мошенники строят свои схемы так, чтобы *не позволить Системе 2 включиться*. Давление времени, страх, секретность, постоянное присутствие собеседника на линии — всё это инструменты блокировки медленного мышления.

Эмоциональный хайджек

Когда вам звонит «сотрудник банка» и сообщает, что на ваше имя берут кредит, или «полицейский» говорит, что ваш сын сбил человека, происходит биологическая реакция. Миндалевидное тело (амигдала) в вашем мозге фиксирует угрозу и отключает префронтальную кору — ту самую часть мозга, которая отвечает за логику, критическое мышление и анализ.

Это называется «эмоциональный хайджек» (захват мозга эмоциями). В этот момент вы физиологически не способны мыслить рационально. Мошенники знают это. Их скрипты написаны так, чтобы вызвать панику за первые 15 секунд разговора. Они не дают вам времени на то, чтобы префронтальная кора снова включилась.

Здесь стоит сделать уточнение: термин «эмоциональный хайджек» предложил писатель и психолог Дэниел Гоулман, и он служит упрощённой метафорой. Реальная нейробиология сложнее: мозг не «выключает» одну область и «включает» другую, как рубильник. Но суть метафоры подтверждается исследованиями стресса: острый стресс, сопровождающийся выбросом гормонов вроде кортизола и адреналина, ухудшает работу систем, отвечающих за планирование, самоконтроль и гибкое мышление, и усиливает опору на привычные автоматические реакции. Человек в панике действительно думает хуже, у́же и быстрее.

Из этого следует важный практический вывод. Для защиты не нужно «быть умнее». Нужно *разорвать цепочку стресса* до принятия решения: положить трубку, выдохнуть, выйти на воздух, позвонить близкому человеку. Это обычные физические действия, но они возвращают контроль.

Иллюзия исключительности

Другая ловушка — лесть и чувство собственной значимости. Инвестиционные скамы часто нацелены на успешных мужчин среднего возраста. Жертве не говорят: «Переведи деньги». Ей говорят: «Мы отобрали вас для участия в закрытом пуле, потому что видим в вас стратегическое мышление». Жадность здесь вторична. Первично — эго. Мозг вырабатывает дофамин от предвкушения не только денег, но и подтверждения собственного статуса.

Эта ловушка опасна тем, что сигнал она подаёт приятный. Никто не чувствует тревоги, когда ему говорят, что он особенный. Страх заставляет проверять и сомневаться, а лесть заставляет расслабляться. Поэтому «позитивные» схемы (приглашение в закрытый клуб, «эксклюзивное» предложение, личный менеджер) нередко оказываются эффективнее «негативных».

К этому добавляется эффект сверхуверенности. Психологи многократно показывали, что люди склонны завышать способность распознавать ложь. Обобщающие исследования показывают, что в среднем точность людей в различении правды и лжи лишь немного превышает случайное угадывание. Мы уверены, что «чувствуем», когда нам врут, но на практике наши ощущения работают лишь чуть лучше подбрасывания монеты. А профессиональный обманщик, к тому же, умеет эти ощущения обходить: он говорит уверенно, не отводит взгляд, не противоречит себе, потому что отрепетировал свою роль.

Принцип доверия по умолчанию

Социальный психолог Тим Левайн предложил теорию, которую называют «теорией умолчания истины». Суть проста: по умолчанию мы склонны верить тому, что нам говорят. Не потому, что мы глупы, а потому, что общение невозможно без базового допущения о правдивости собеседника. Если бы мы проверяли каждое слово, ни один разговор не состоялся бы.

Это эволюционно оправданная настройка: в небольшой общине обман встречался редко, а проверка была дорогой. Но в мире, где собеседник может находиться на другом континенте и работать по скрипту, эта настройка становится уязвимостью. Мошенник пользуется тем, что мы вежливо верим.

Следствие: переломить ситуацию можно только *триггером*, то есть заранее установленным условием, после которого мы переходим из режима «верю» в режим «проверяю». Таким триггером служит просьба о деньгах, коде или данных. Любая такая просьба, особенно неожиданная, должна автоматически переключать нас на проверку.

Социальные рычаги: авторитет, дефицит, доказательство

Психолог Роберт Чалдини в работах о влиянии описал ряд принципов, которые лежат в основе большинства схем обмана.

Авторитет. Мы склонны подчиняться тем, кто выглядит или звучит как представитель власти. Знаменитые эксперименты Стэнли Милгрэма 1960-х годов показали, что значительная часть обычных людей готова выполнять неприятные указания, если их отдаёт человек, воспринимаемый как авторитет. Когда голос в трубке называется «следователем» или «сотрудником службы безопасности», срабатывает та же привычка: власти положено подчиняться.

Дефицит. Мы ценим то, что вот-вот исчезнет. «Предложение действует только сегодня», «осталось три места», «окно возможностей закрывается». Ограничение по времени побуждает действовать, не взвешивая.

Социальное доказательство. Мы ориентируемся на поведение других. Если «все вкладываются», значит, это безопасно. Классические эксперименты Соломона Аша 1950-х годов показали, как сильно групповое мнение способно подавить собственное восприятие человека. В цифровой среде социальное доказательство подделывается легко: фейковые отзывы, боты, «довольные клиенты» в чатах.

Взаимность. Если нам что-то дали, мы чувствуем обязанность отплатить. Мошенники предлагают «бесплатную консультацию», «подарок», небольшой «пробный» выигрыш, чтобы создать долг, который потом легче взыскать.

Последовательность. Мы стремимся вести себя в соответствии с ранее сделанным выбором. Один раз согласившись, мы чувствуем давление согласиться снова. Это подводит нас к следующему разделу.

Нормализация абсурда

Современный мошенник редко начинает с требования перевести все сбережения. Он использует технику «нога в двери». Сначала просит подтвердить коды из SMS, затем — скачать «безопасное приложение», затем — оформить «страховку». Каждый шаг кажется логичным продолжением предыдущего. Жертва варится как лягушка в медленно нагревающейся кастрюле, пока не оказывается в финансовой пропасти.

Приём «нога в двери» описан в психологии ещё в 1960-х: исследователи Джонатан Фридман и Скотт Фрейзер показали, что человек, согласившийся на маленькую просьбу, с большей вероятностью согласится и на большую. Мелкое согласие меняет самовосприятие: «я человек, который помогает» или «я человек, который выполняет требования».

Небольшое уточнение к известной метафоре: настоящая лягушка из постепенно нагреваемой воды, как показывают наблюдения биологов, всё же выпрыгивает, когда становится слишком горячо. Но человек, в отличие от лягушки, не чувствует «температуры»: он не видит критической точки, потому что каждый отдельный шаг выглядит разумным. Метафора остаётся полезной именно как образ нечувствительности к постепенным изменениям.

Эскалация приводит и к другому эффекту. Чем больше человек вложил (денег, времени, эмоций), тем труднее ему остановиться. Экономисты называют это «ошибкой невозвратных затрат»: мы продолжаем вкладываться в проигрышное дело, потому что уже вложились. Мошенники превращают этот механизм в рабочий инструмент: «чтобы вернуть деньги, нужно ещё внести комиссию».

Страх потерять сильнее радости приобрести

Ещё одна опора мошеннических схем — *неприятие потерь*. Работы Даниэля Канемана и Амоса Тверски показали, что боль от потери обычно ощущается сильнее, чем радость от равного по размеру выигрыша. Поэтому самые эффективные скрипты строятся не вокруг обещания выгоды, а вокруг угрозы потери: «ваши деньги украдут», «ваш счёт заблокируют», «вам грозит уголовное дело».

Дело не в том, что страх делает людей глупыми. Просто угроза потери включает режим защиты, в котором главная цель — немедленно остановить ущерб. А мошенник предлагает готовое «решение»: перевести деньги на «безопасный счёт», установить «защитное» приложение. Жертва не думает, что это ловушка, потому что действует в логике спасения.

Условный пример: анатомия одного «успешного» разговора

Посмотрим на типичный сценарий со стороны психологии. Это обобщённая картина, а не запись реального разговора.

— Авторитет и срочность. Звонящий представляется сотрудником службы безопасности и сразу говорит о срочной угрозе. Включается страх, Система 2 блокируется.

— Доказательство осведомлённости. Он называет имя и последние цифры карты. Возникает ощущение, что «он правда из банка».

— Изоляция. Он просит не прерывать связь и никому не рассказывать. Социальный контроль выключен.

— Ступенчатые просьбы. Сначала простое действие, затем более серьёзное. Каждый шаг закрепляет согласие.

— Выход из ситуации. Жертве предлагают «решение», и она облегчённо хватается за него.

Ни на одном шаге не требовалось, чтобы человек был глуп. Требовалось лишь, чтобы он оказался в нужном эмоциональном состоянии и не имел под рукой «внешней проверки».

Что делать с этим знанием

Знать, что вашей психикой можно управлять, неприятно, но полезно. Из этого вытекает несколько принципов.

— Не полагайтесь на хладнокровие. Стресс снижает качество решений у всех. Защита должна работать *заранее*: правила, которые вы установили в спокойном состоянии.

— Создайте триггеры. «Просьба о деньгах или кодах от незнакомца означает паузу и проверку». «Звонок с требованием срочности означает, что я перезваниваю сам».

— Ставьте паузу между импульсом и действием. Достаточно нескольких минут и смены обстановки. Прогулка, стакан воды, звонок близкому.

— Привлекайте второго человека. Любая схема опирается на изоляцию. Свежий взгляд со стороны разрушает её.

— Следите за состоянием. Усталость, голод, тревога, горе, праздничная суета — время повышенной уязвимости. В такие периоды проще быть осторожнее с финансовыми решениями.

— Отказывайтесь от стыда. Человек, которому не стыдно обсудить подозрительный звонок, защищён лучше, чем человек, считающий себя «слишком умным, чтобы попасться».

Главное из главы

— Обман нацелен на состояние человека, а не на его интеллект. Образование и опыт не дают гарантии защиты.

— Острый стресс ухудшает аналитическое мышление. Скрипты мошенников созданы, чтобы вызвать его и не дать остыть.

— Лесть и чувство исключительности работают не слабее страха.

— По умолчанию мы склонны верить собеседнику, и это уязвимость, а не глупость.

— Рычаги влияния (авторитет, дефицит, социальное доказательство, взаимность, последовательность) работают независимо от технологии.

— Эскалация малых просьб превращает человека в соучастника собственного обмана.

— Лучшая защита — заранее установленные правила и привычка делать паузу.

Вопросы для размышления

— В каком состоянии вы чаще всего принимаете необдуманные решения: усталость, спешка, тревога, радость? Что вы можете заранее изменить в таких ситуациях?

— Какой «триггер проверки» вы можете установить для себя и близких уже сегодня?

— Почему рассказ о том, что вас обманули, так тяжело даётся людям? Как изменилась бы ситуация, если бы стыд исчез?

Глава 3. Психопатология успеха: кто такие современные мошенники и как они оправдывают свои действия

Если попросить человека нарисовать мошенника, чаще всего получится вариация на тему обаятельного хищника: холодный взгляд, гладкая речь, ни капли совести. Кино приучило нас к этому образу. Реальность куда прозаичнее и тревожнее: **большинство людей, совершающих мошенничество, не похожи на злодеев ни снаружи, ни, как правило, в собственных глазах.**

Миф о «врождённом аферисте»

Психологи действительно описывают набор черт, который встречается у обманщиков чаще, чем у остальных. В 2002 году Делрой Паулхус и Кевин Уильямс предложили термин «тёмная триада»: нарциссизм (потребность в восхищении и ощущение собственной исключительности), макиавеллизм (манипулятивность, расчётливость, цинизм) и субклиническая психопатия (импульсивность, бесчувственность, неспособность к эмпатии).

Эти черты помогают обманывать: человек, который не мучается чужой болью, легче лжёт в глаза. Но у «тёмной триады» есть два важных ограничения.

Во-первых, это **континуум, а не диагноз**. Выраженные нарциссические или манипулятивные черты встречаются и у успешных руководителей, и у политиков, и у вполне законопослушных людей. Сами по себе они не делают человека преступником.

Во-вторых, среди тех, кто совершает финансовые преступления, много людей без этих черт вовсе. Классические исследования «беловоротничковой» преступности показывают: типичный нарушитель часто выглядит вполне обычно, ему за сорок, он занимает ответственную должность и ранее не имел проблем с законом. Именно поэтому организации так долго не замечают, что внутри что-то идёт не так.

Что говорит наука о психопатии

Слово «психопат» в обиходе стало почти ругательством, поэтому стоит уточнить, о чём идёт речь. Канадский психолог Роберт Хэйр разработал широко используемый опросник для оценки психопатических черт. Он описывает два блока: *межличностно-аффективный* (поверхностное обаяние, грандиозное самомнение, склонность ко лжи, отсутствие раскаяния и эмпатии) и *поведенческий* (импульсивность, безответственность, склонность к рискованному образу жизни).

Распространённость выраженной психопатии в общей популяции, по оценкам исследователей, невелика, порядка одного процента, но в местах лишения свободы она заметно выше. В одном известном исследовании корпоративных специалистов Пола Бабиака и Роберта Хэйра психопатические черты в выраженной форме обнаружили примерно у четырёх процентов участников выборки, что выше, чем в обществе в целом. Эти цифры нужно воспринимать осторожно: выборки были небольшими, а границы между «успешным сильным характером» и расстройством размыты. Но они подсказывают, что среди тех, кто способен убедительно обманывать и не терзаться последствиями, действительно встречаются люди с такими чертами.

Важно не сделать из этого ложный вывод. **Большинство людей с психопатическими чертами не совершают мошенничества, а большинство мошенников не являются психопатами.** Ярлык «чудовище» удобен, но он мешает видеть массовую реальность, где обман совершают обычные люди в обычных обстоятельствах.

Треугольник мошенничества

Куда полезнее вопрос не «кто такой мошенник?», а «**при каких условиях обычный человек превращается в него?**». Ответ даёт «треугольник мошенничества», модель, которую в середине XX века сформулировал криминолог Дональд Кressей. Он беседовал с сотнями заключённых, осуждённых за растраты, и пытался понять, как приличные люди оказывались на скамье подсудимых. Для нарушения нужны три вещи:

— **Давление.** Долги, потеря работы, план продаж, который невозможно выполнить, страх позора. Человеку кажется, что обычными путями выхода нет.

— **Возможность.** Слабый контроль, доступ к чужим деньгам или данным, отсутствие проверок. В цифровой среде эта сторона треугольника выросла до гигантских размеров: расстояние, анонимность и отсутствие свидетелей убирают естественные тормоза.

— **Рационализация.** Внутренний монолог, который позволяет совершить поступок и остаться «хорошим человеком».

Третья сторона самая интересная. Без неё большинство людей просто не смогли бы жить с собой.

Кressей наблюдал, что у многих растратчиков проблема была «неразделимой»: человек считал, что не может поделиться ею ни с кем, не потеряв лицо. Это очень похоже на ловушку жертв из предыдущих глав: стыд и изоляция питают обман с обеих сторон.

Когда давление создаёт организация

Давление не всегда исходит от личных обстоятельств. Иногда его создаёт сама организация. Один из известных примеров связан с банком Wells Fargo. В 2016 году выяснилось, что сотрудники при жёстких планах продаж открывали клиентам огромное количество счетов и карт без их ведома, чтобы выполнить показатели. Банк был оштрафован, а число сомнительных счетов оценивалось миллионами. Многие участники этой практики не считали себя мошенниками. Они говорили себе, что делают то, что требует система, и боялись потерять работу.

Этот случай поучителен: **когда вознаграждение привязано к цифре, а контроль формален, организация сама воспитывает нарушителей**. Менеджеры, поставившие недостижимую цель, и сотрудники, нашедшие нелегальный способ её достичь, оказываются в одной ловушке. Подобные эпизоды показывают, что борьба с мошенничеством включает не только поиск «плохих людей», но и пересмотр систем стимулов.

Как совесть договаривается сама с собой

В 1957 году социологи Грешем Сайкс и Дэвид Матза описали «техники нейтрализации»: приёмы, которыми люди заранее снимают с себя вину. Узнать их в современных мошеннических историях несложно.

— **«Я не виноват»** (отрицание ответственности). «Меня заставили. Такая система. У меня не было выбора».

— **«Никто не пострадал»** (отрицание вреда). «Банк всё вернёт. Страховка покроет. Эти деньги всё равно лишние».

— **«Жертва сама виновата»** (отрицание жертвы). «Нормальный человек не поверит в такое. Жадность, глупость и наивность должны наказываться».

— **«Судьи не лучше»** (осуждение осуждающих). «Банки обманывают клиентов легально, чиновники воруют миллиардами, а меня одного считают преступником».

— **«Это ради высшего»** (апелляция к высшим ценностям). «Я кормлю семью. Я помогаю родным. Я не сделал бы этого, если бы не необходимость».

Заметьте, что ни одна из этих фраз не звучит как «я хочу украсть». Каждая звучит как объяснение, почти как справедливость. Так работает психика: она не разрешает нам нарушать собственные нормы, но охотно переписывает сами нормы.

Исследователи поведенческой этики показали ещё одну любопытную вещь: большинство людей готовы нарушать правила в небольших масштабах, пока могут сохранять образ себя как честного человека. Они «чуть-чуть» приукрашивают, «слегка» округляют, «немного» одалживают. Такой «запас допустимого» разный у разных людей, но у большинства он существует. Опасность в том, что запас растягивается: каждый успешный маленький обман расширяет границы допустимого.

Эффект «ступеньки»

Редко кто из мошенников начинает с крупного обмана. Чаще путь выглядит как цепочка маленьких компромиссов: подправить отчёт «всего на этот месяц», присвоить небольшую сумму «взаймы», пообещать клиенту то, чего нет, «пока дела не наладятся». Каждый шаг ненамного хуже предыдущего, поэтому критический порог не ощущается.

Исследователи называют это «скользкой дорожкой»: когда каждое следующее нарушение лишь чуть-чуть больше предыдущего, мы почти не замечаем перемены. Понци, по рассказам современников, поначалу действительно рассчитывал заработать на почтовых купонах и лишь потом оказался в ситуации, когда выплаты старым вкладчикам приходилось покрывать деньгами новых. Многие пирамиды начинаются как честная попытка бизнеса и превращаются в обман, когда признать провал становится страшнее, чем продолжить врать.

Условный пример. Руководитель небольшого инвестиционного фонда допускает убыток и решает не показывать его в отчёте, «чтобы не пугать клиентов, пока рынок не восстановится». Через квартал рынок не восстановился, и теперь нужно скрывать уже две потери. Чтобы выплатить деньги одному клиенту, он занимает у другого. Через год он ведёт двойную бухгалтерию, и пути назад нет, потому что признание означает не только убыток, но и обвинение в обмане. Он не просыпался с мыслью «стану мошенником». Он просто на каждом этапе откладывал неприятную правду.

Двойная жизнь и самообман

Отдельная тема — как мошенники живут сами с собой. Многие из них поддерживают две идентичности: публичную (успешный предприниматель, заботливый муж, щедрый благотворитель) и скрытую (человек, создавший обман). Эти идентичности не обязательно конфликтуют, потому что рационализации помогают держать их раздельно.

Показательны истории крупных финансовых пирамид: основатели нередко искренне верили, что «вот-вот вернут всё», что обман временный, что в конце концов всё сложится. Самообман — самый надёжный союзник долгого мошенничества. Человек, который сам верит в свою ложь, убедительнее того, кто её сознательно разыгрывает.

Это объясняет и поведение многих организаторов после разоблачения: они часто не воспринимают себя как преступников, а говорят о «трудных обстоятельствах», «недопонимании» и «несправедливом преследовании».

Две стороны одного конвейера

Современная индустрия обмана устроена так, что внутри неё работают очень разные люди.

Организаторы принимают решения, строят схемы, вкладывают в инфраструктуру. Среди них чаще встречаются те самые расчётливые и харизматичные люди с выраженными манипулятивными чертами.

Исполнители (операторы колл-центров, администраторы фейковых сайтов, «дропы») зачастую вовсе не считают себя преступниками. Они говорят себе, что просто работают по скрипту, звонят по списку, получают зарплату. Разделение труда делает ответственность размытой: оператор не видит, чем закончится звонок, а владелец бизнеса вообще не разговаривает с жертвами. Каждое звено цепи может сказать: «Я лишь маленькая часть».

Принуждённые. Отдельная и мрачная категория. Расследования международных организаций и журналистов последних лет описывают «скам-комплексы» в Юго-Восточной Азии (в частности, в Мьянме и Камбодже), где людей, заманенных объявлениями о высокооплачиваемой работе, удерживают силой и заставляют вести мошеннические переписки. В 2023 году Управление Верховного комиссара ООН по правам человека оценило число таких людей в сотни тысяч человек по региону. Для таких работников картина обратная: они одновременно и орудие обмана, и его жертвы. Это напоминает, что за экраном обманщика не всегда сидит тот, кого мы вообразили.

Почему общество проигрывает психологически

Образ «злодея» удобен: он создаёт иллюзию, что мошенники отличаются от нас. Тогда достаточно хорошо присматриваться и держаться подальше от «неправильных» людей. Но если мошенничество совершается в основном обычными людьми под воздействием обстоятельств, выгод и самообмана, то защита должна быть другой.

Нужно не только учить граждан распознавать приманки, но и менять среду, в которой возможен обман: устранять «одиночную подпись» на крупных платежах, вводить независимый контроль, делать невозможным то, что слишком легко. Старый принцип безопасности «доверяй, но проверяй» оказывается не просто лозунгом, а условием, при котором меньше людей будет соблазнено переступить черту.

Сигналы внутри организации

Специалисты по расследованию корпоративных злоупотреблений давно перечисляют «красные флаги», связанные с поведением сотрудников, у которых есть доступ к деньгам. Ни один из них не является доказательством, но их совокупность стоит внимания.

— Образ жизни заметно превышает известные доходы.

— Человек не берёт отпуск и никому не передаёт свои задачи.

— Он единолично контролирует весь процесс от начала до конца.

— Он болезненно реагирует на проверки и вопросы.

— Он находится под сильным личным финансовым давлением.

— Документы постоянно «временно» отсутствуют, а объяснения расплывчаты.

Обратите внимание: большая часть этих сигналов указывает на *слабость контроля*, а не на «плохую натуру». Организация, в которой один человек может незаметно распоряжаться деньгами, создаёт соблазн для многих. Поэтому лучшая профилактика — разделение обязанностей, регулярные проверки и культура, в которой вопросы воспринимаются как норма.

Главное из главы

— Типичный мошенник не обязательно психопат или «злодей». Среди нарушителей много людей, оказавшихся в обстоятельствах давления и возможности.

— Треугольник мошенничества (давление, возможность, рационализация) объясняет, как обычные люди переступают черту.

— Рационализации («никто не пострадал», «все так делают») позволяют сохранять образ себя как честного человека.

— Организация может сама создавать давление и воспитывать нарушителей.

— В индустрии обмана работают организаторы, исполнители и принуждённые, и ответственность каждого различна.

— Лучшая защита сочетает личную бдительность и системные меры: контроль, прозрачность, разделение полномочий.

Вопросы для размышления

— Какие рационализации вам приходилось слышать (или произносить) в мелких бытовых нарушениях? Чем они отличаются от тех, что описаны в главе?

— Какие условия в вашей организации или окружении могли бы создать давление, толкающее людей к нарушению правил?

— Как изменилось бы ваше отношение к «дропам» и исполнителям мошеннических схем, если вы узнаете, что часть из них принуждена или обманута?

Часть II. Арсенал иллюзий

Глава 4. Социальная инженерия 2.0: когда «службой безопасности» звонит нейросеть

Социальная инженерия звучит как что-то из мира хакеров, но на деле это древнее искусство: заставить человека самому открыть дверь. Взломщик может часами подбирать отмычку, а может просто позвонить в дверь, представившись курьером. Во втором случае ему не нужны технологии, ему нужна история, которой поверят.

В цифровую эпоху «дверью» стали банковское приложение, корпоративная почта и мессенджер. А «курьером» теперь может оказаться кто угодно, включая программу, которая не устаёт, не путается в показаниях и говорит на любом языке.

Откуда пошло название

Термин «социальная инженерия» в мире информационной безопасности связан с именем Кевина Митника, одного из самых известных хакеров конца XX века. Любопытно, что он сам неоднократно подчёркивал: чаще всего ему не приходилось взламывать системы технически. Достаточно было позвонить сотруднику, правдоподобно представиться коллегой и попросить помощи. Позднее Митник стал консультантом по безопасности и написал книги о том, как человеческий фактор перевешивает любую технику. Он умер в 2023 году, но его главная мысль остаётся актуальной: **самое слабое звено любой системы защиты — человек, который хочет быть вежливым и полезным**

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.