

ВОРОНКА ВОВЛЕЧЕНИЯ

КАК ПОДРОСТКУ НЕ СТАТЬ ПРЕСТУПНИКОМ ПОНЕВОЛЕ

Окончание. Начало — на стр. 1

Андрей АФАНАСЬЕВ. Представьте себе ленту популярного юмористического паблика: обычные шутки идут вперемишку с пропагандой насилия, антисемейными установками, депрессивными изображениями или видеороликами. Достаточно любой реакции на такой материал, чтобы социальная сеть её зафиксировала. Причём реакция — это не только лайк, комментарий или репост: если пользователь задержался на публикации чуть дольше обычного, алгоритм уже воспринимает это как проявление интереса. После этого платформа начинает показывать всё больше похожих материалов.

Я сам столкнулся с этим во "ВКонтакте": после мониторинга нескольких депрессивных групп раздел рекомендаций в течение двух недель был заполнен схожими сообщениями, видео и контактами. Алгоритм сделал простой вывод: раз я это смотрю, значит, мне это интересно. Так социальная сеть, устроенная вокруг удержания внимания, стремится замкнуть человека в эхо-камере. Платформа улавливает интерес пользователя и начинает последовательно усиливать эту тему, нередко доводя её до гротескной формы.

"ЗАВТРА". То есть перед нами не случайный сбой и не безобидная особенность рекомендаций, а сама логика платформ, ведь чем сильнее человека тревожат, раздражают или пугают, тем дольше его удаётся удерживать внутри системы?

Андрей АФАНАСЬЕВ. Именно так. Социальные сети существуют прежде всего как коммерческие проекты. Они требуют огромных расходов на серверы, инфраструктуру, обслуживание, работу специалистов, а зарабатывают главным образом на рекламе. Чем дольше пользователь находится внутри платформы, тем больше рекламных публикаций он видит и тем больше дохода приносит.

Деструктивный контент в этой системе особенно выгоден: он резче, эмоциональнее, сильнее цепляет и надёжнее удерживает внимание. Постепенно человек замыкается в такой среде, накручивается на определённую тему и попадает в информационную петлю: ему предлагают аналогичные группы, видео, похожих людей, и выйти из этого становится всё труднее. Наверняка у многих были такие знакомые: ещё недавно с человеком можно было говорить о чём угодно, но потом он погрузился в определённый информационный поток, и постепенно все разговоры начали сводиться к одной теме, делая общение невозможным. Это и есть эффект эхо-камеры.

Когда человека уже накрутили алгоритмы, в эту среду приходят кураторы — конкретные люди, которым от пользователя нужно конкретное действие. Они используют технологии, характерные для закрытых деструктивных групп: замкнутость, активную обработку новичков, постоянное внимание к человеку сразу после входа в чат. Ем начинать писать: "Привет, как дела? Давай дружить. Где ты учишься? Где работают родители?" Будьте настороже: если незнакомые люди в закрытом сообществе слишком активно интересуются вашей жизнью, семьёй и кругом общения, велика вероятность, что дальше вас попытаются использовать.

Затем вокруг одной сверхценной идеи концентрируются все темы чата, формируется система фильтрации инакомыслящих, появляются идеологические рейды в чужие обсуждения и собственный жаргон, позволяющий отличать "своих" от "чужих". Почему это выгодно социальным сетям? Потому что накрученные на определённую тему люди начинают спорить, доказывать друг другу свою правоту, втягиваясь в бесконечные конфликты, а главное — проводить всё больше времени в сети, принося платформам доход. Главная мысль здесь проста: социальные сети — это не столько индустрия развлечений, сколько индустрия эксплуатации, причём эксплуатации нас самих.

"ЗАВТРА". Если главным показателем успеха платформы является время, проведённое пользователем перед экраном, то нетрудно сделать вывод, что ей невыгоден образованный и самостоятельный человек.

Андрей АФАНАСЬЕВ. Именно поэтому для социальных сетей целевой аудиторией оказываются дети и подростки. У них есть ценный ресурс, которого взрослые чаще всего лишены, — свободное время. Это позволяет им дольше оставаться в сети и приносить платформам больше дохода. По этой причине цепляющий деструктивный контент оказывается особенно выгодным. И это не теория заговора, а давно описанный и исследованный механизм.

У Джарона Ланье, американского публициста и разработчика, работавшего в крупных технологических компаниях, в том числе в "Майкрософте" и "Мете", признанной в России экстремистской организацией, есть хорошая книга "Десять аргументов за то, чтобы удалить свои аккаунты в социальных сетях" — своего рода исповедь человека, увидевшего изнутри, как устроена эта индустрия. Одна из главных мыслей Ланье состоит в том, что борьба за внимание неизбежно приводит к доминированию самого скандального и провокационного контента. Именно поэтому действительно познавательный контент чаще приходится искать самостоятельно, тогда как алгоритмы продвигают прежде всего эмоционально заряженные публикации.

Другой важный принцип связан с беспрецедентным вмешательством в жизнь человека. Вы поговорили с другом о том, что неплохо было бы заняться бегом, а спустя некоторое время видите рекламу кроссовок или спортивного инвентаря. Социальные сети собирают огромный массив поведенческих данных и используют его для воздействия на человека. Отсюда возникает агрессивное навязывание информации, незаметное управление вниманием и продвижение тех, кто зарабатывает на обмане. Хороший пример — так называемые инфобизнесмены, продавцы "успешного успеха", которых платформы продолжают активно продвигать, поскольку они приносят прибыль.

В 2021 году бывшая сотрудница "Фейсбука" Фрэнсис Хауген обнародовала внутренние документы компании. Из них следовало, что алгоритмы платформы отдавали преимущество эмоционально заряженному и конфликтному контенту, поскольку он повышал вовлечённость. Платформа выявляла интересы человека и могла подмигивать в его ленту материалы, противоречащие его убеждениям, чтобы вызвать более сильную реакцию, втянуть пользователя в спор и удержать в сети дольше.

Отдельно стоит вспомнить исследование "Фейсбука" об эмоциональном заражении, опубликованное в 2014 году. Тогда исследователи

изменяли эмоциональную окраску новостной ленты и наблюдали, как это влияет на собственные публикации пользователей. Вывод оказался простым: эмоциональные состояния способны передаваться через цифровую среду. Иными словами, человек может зайти в социальную сеть в спокойном состоянии, а выйти из неё раздражённым, подавленным или агрессивным, даже не осознавая, в какой момент это произошло. Поэтому важно контролировать своё внутреннее состояние. Если после попадания в какую-то группу, чат или обсуждение вы замечаете, что начинаете кого-то ненавидеть, сильнее тревожиться, хуже себя чувствовать или всё время возвращаться к одной и той же болезненной теме, лучше от такого пространства отписаться. Не случайно появился термин "дум-скроллинг" — зависимость от тревожных новостей и бесконечного прокручивания негативного контента. И здесь возникает главный вопрос: как сохранить личность, ясность мышления и внутреннее равновесие в среде, которая во многом питается нашими негативными эмоциями?

"ЗАВТРА". Получается, главный риск даже не в самом деструктивном контенте, а в том, что человек перестает замечать, как его собственная реакция стала результатом дрессуры?

Андрей АФАНАСЬЕВ. Да, именно поэтому я бы выделил несколько основных правил.

Первое — не поддаваться эмоциям. Если вас хотят раскрутить на опасную тему, давить часто будут не на худшие, а на лучшие качества: чувство справедливости, сострадание, желание защитить слабого, при этом указывая на "плохих людей", от которых якобы все беды.

Второе — во всём сомневаться. Социальные сети должны быть для вас средой нулевого доверия, потому что по своей природе это пространство постоянных манипуляций.

Третье — не выполнять никаких заданий в сети, поскольку вы не можете заранее знать их окончательный смысл. Манипуляторы используют простые поручения как способ отбора наиболее внушаемых людей: поставить лайк, написать комментарий, пройти по ссылке, что-то переслать. Так они вычисляют тех, кто поддаётся управлению, а затем могут вести их дальше, использовать, шантажировать или втягивать в более серьёзные действия.

Четвёртое — ничего не репостить по просьбе. Один из частых рисков в Интернете связан с распространением запрещённых или экстремистских материалов. Человек может нарушить закон не только тогда, когда сам пишет прямой призыв или оскорбительный текст, но и тогда, когда публично распространяет чужой материал. В некоторых ситуациях публичная реакция на запись тоже может работать как распространение, если делает материал видимым для других пользователей. В федеральный список экстремистских материалов Минюста входят книги, фильмы, песни, изображения, тексты и другой контент, и всё запомнить невозможно, поэтому вас могут подставить, предложив "поделиться интересной песней" или "распространить статью", а затем использовать этот репост для шантажа.

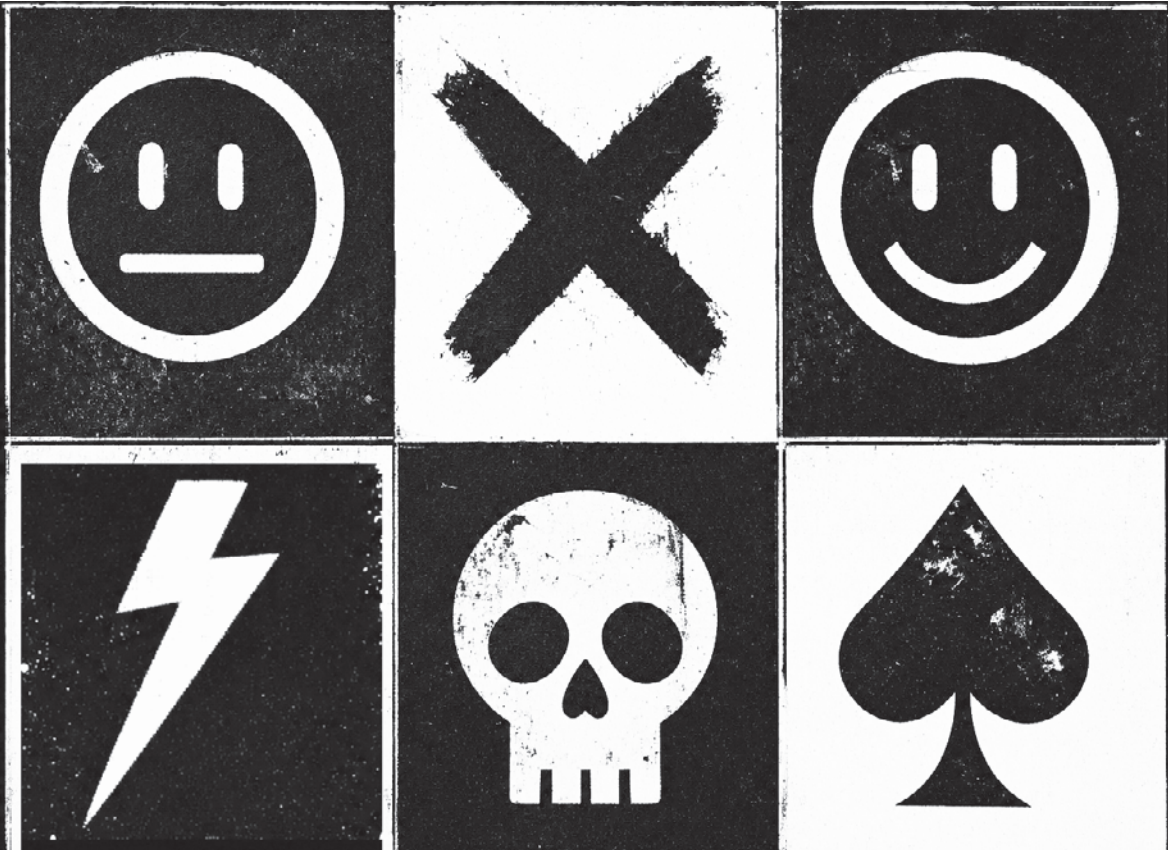
Пятое — избегать групп, где главной идеей становится ненависть. Логика "мы ненавидим плохих, значит, мы хорошие" не работает: ненависть остаётся разрушительным чувством, даже если её оправдывают благими намерениями.

Шестое — сравнивать себя не с другими, а с самим собой в прошлом. Если через месяц, два месяца или год после подписки на группу ваша жизнь изменилась к худшему, от источника этого влияния лучше отписаться. Главная опасность в том, что сетевые манипуляторы почти всегда приходят в вашу жизнь под видом друзей. Их признаки — назойливость, чрезмерное любопытство, настоячивые попытки выяснить, где вы учитесь, с кем общаетесь, какие у вас проблемы дома. Ключевой признак — стремление настроить ребёнка против родителей. Манипуляторы понимают, что именно родители представляют для них угрозу, пытаясь защитить ребёнка, а потому они стараются их обесценить. Если вы видите подобные манипулятивные попытки, это один из важнейших признаков схемы.

В Интернете человек может столкнуться с рисками, о которых заранее не подумал. Надо помнить, что ответственность может наступать за распространение контента из федерального списка экстремистских материалов, публичную демонстрацию нацистской символики, возбуждение ненависти либо вражды, унижение человеческого достоинства, публикации, связанные с фейками, неуважением к символам воинской славы или иными запрещёнными формами публичного высказывания. В одних случаях речь идёт об административной ответственности, в других — об уголовной, и граница зависит от состава, тяжести и конкретных обстоятельств правонарушения. Особенно важно понимать: риск возникает не только тогда, когда человек сам пишет прямой призыв или оскорбительный текст, но и тогда, когда он публично распространяет чужой материал. Поэтому нельзя легкомысленно относиться к репостам, комментариям, публикациям и обсуждениям, где речь идёт о народах, религиях, нациях, социальных группах или других сообществах.

То же самое касается терроризма. Например, статья 205.5 Уголовного кодекса РФ называется "Организация деятельности террористической организации и участие в деятельности такой организации". Когда человек слышит такую формулировку, он часто представляет себе тайные собрания, подвалы, символику, тренировки и конспиративные встречи, но в эпоху Интернета участие может выглядеть куда менее очевидно: закрытый чат, обсуждение запрещённых действий, регулярное присутствие в группе, где подобные действия планируются или поддерживаются. В зависимости от обстоятельств всё это может получить серьёзную правовую оценку.

Приведу конкретный пример, не называя региона. Украинские террористы и мошенники завербовали неблагополучного подростка, после чего он создал закрытый чат и начал обсуждать там подготовку теракта в школе. Естественно, он стал приглашать туда друзей и одноклассников: кто-то то писал, кто-то просто состоял в чате и читал сообщения, кто-то, возможно, до конца не понимал, во что его втягивают. Со временем этот чат вычислили, и в школу пришли не только за самим организатором, но и за другими участниками. Понятно, что окончательную оценку в таких случаях даёт суд, и степень ответственности каждого человека зависит от множества обстоятельств. Но сам пример показывает: нужно быть крайне внимательным к тому, куда вас добавляют, в каких чатах вы состоите и что там



обсуждается, чтобы случайно не оказаться среди вовлечённых в правонарушение.

Теперь о телефонных мошенниках. Главное правило, которое нужно запомнить железно: сотрудники полиции, МВД, ФСБ, прокуратуры, Следственного комитета и других силовых ведомств не звонят по телефону, чтобы обсуждать подробности уголовных дел. Такие вопросы по телефону не решаются. Поэтому, если вам звонит человек и представляется сотрудником полиции, следователем, работником прокуратуры или ФСБ, разговор нужно сразу прекращать: не спорить, не оправдываться, не доказывать, что вы ни в чём не виноваты, а просто положить трубку. Если вы действительно будете интересны следствию или окажетесь связаны с каким-то делом, вас вызовут официальной повесткой либо к вам придут лично. Пока человек не показал удостоверение и не действует в установленном законом порядке, для вас он просто неизвестный собеседник.

"ЗАВТРА". Понимание этого поможет распознать большинство мошеннических уловок, но схемы постоянно меняются.

Андрей АФАНАСЬЕВ. Да, схем очень много, поэтому важнее запомнить не каждую из них, а общий принцип. Первое правило цифровой гигиены — не отвечать на незнакомые номера. Если человеку действительно нужно с вами связаться, он найдёт официальный способ или выйдет на вас через знакомых и родственников; за незнакомым же номером чаще всего скрываются мошенники, навязчивые продавцы, банки, операторы или опросы, которые вам не нужны.

Второе правило связано с тем, что социальные сети, звонки и мессенджеры должны быть для вас средой нулевого доверия. Если после короткого разговора вам предлагают продолжить общение в мессенджере, это тревожный сигнал, потому что мошенники стараются увести переписку туда, где проще давить на человека, присылать ссылки, файлы и инструкции. Особенно осторожными нужно быть в тех случаях, когда на "Авито" или другой площадке вам сразу предлагают перейти в "Telegram".

Третье правило — насторожиться всякий раз, когда вам говорят, что хотят помочь вам или вашему родственнику. "Ваш друг попал в беду", "Вас пытаются обмануть", "Мы спасаем ваши деньги" — именно с таких фраз часто начинается мошенническая схема, поскольку никто не должен по телефону втягивать вас в срочные действия, переводы, установку приложений или выполнение секретных инструкций.

Четвёртое правило особенно важно: никогда не выполняйте требований шантажистов. Сегодня мошенники всё чаще пытаются не просто украсть деньги, а заставить человека совершить глупость или преступление: что-то перевести, записать, сфотографировать, испортить, поджечь, а затем использовать это как повод для давления, угрожая уголовным делом, кредитами, неприятностями у родственников или публикацией переписки. В такой ситуации нужно сразу прекратить разговор и обратиться к родителям, учителям или в полицию. Нельзя думать, что, если выполнить одно требование, всё закончится: после первого будет второе, затем третье, и каждое следующее окажется опаснее предыдущего. Это всегда игра на повышении.

Следующее правило — не верить своим глазам и ушам. Мы живём во время фейков и дипфейков, когда вам может позвонить человек с известного номера, с привычной аватаркой и знакомым голосом, но на самом деле это будет мошенник, использующий технологию подмены голоса. Если якобы родственник или знакомый вдруг просит деньги, код из СМС или требует срочно что-то сделать, задайте нестандартный проверочный вопрос, ответ на который знаете только вы.

Схема вовлечения часто начинается с безобидных заданий. Подростку предлагают "интересную игру": зарегистрироваться, отправить номер телефона, данные маминной карты, заполнить простое поручение, к примеру, сфотографировать что-то рядом с домом, затем перейти по геолокации, сфотографировать трамвай, здание администрации или мост. За каждое задание платят небольшие деньги, и всё выглядит как игра, пока куратор не сообщат, что получил фотографии стратегических объектов, и не начинает шантажировать ребёнка перепиской, требуя выполнить уже более опасное поручение. Так работает воронка: человека приучают к мелочам, заставляют отправлять геолокацию, фотографии и данные, а затем переводят к действиям с тяжёлыми последствиями. Если с вами произошло что-то подобное, нужно сразу обращаться к родителям, учителям, родственникам или в полицию. Например, подростку предлагают пробраться по крыше электрички и снять видео за деньги. Он думает, что просто делает ролик, но на заднем плане может оказаться завод, железная дорога или другой стратегический объект, а в файле могут сохраниться геометки. В результате человек, сам того не понимая, пере-

даёт информацию куратору и оказывается вовлечён в преступление.

Главный принцип прост: в Интернете нельзя выполнять задания от незнакомых людей, какими бы простыми, смешными или безопасными они ни казались. По данным МВД и компаний, занимающихся кибербезопасностью, число мошеннических схем, нацеленных на детей и подростков, заметно растёт. Чаще всего всё начинается с объявлений в мессенджерах: "простая работа", "лёгкие деньги", "заработок на простых заданиях". Организатор создаёт мошенническую схему и распределяет роли между участниками: один ведёт переписку с жертвами, другой оформляет переводы, третий администрирует каналы, четвёртый занимается выводом средств. Каждый видит лишь небольшую часть общей конструкции и уверен, что выполняет законное поручение за скромное вознаграждение. Обычно такая система существует несколько недель, после чего разваливается. В какой-то момент к родителям может прийти сотрудник полиции и сообщить, что с устройства или IP-адреса их сына либо дочери совершались мошеннические действия. Подросток мог не осознавать, что участвует в преступлении, однако если потерпевшим причинён значительный ущерб, речь может идти не только о правовой оценке действий, но и о возмещении вреда. Даже в случаях, когда возраст ещё не позволяет привлечь несовершеннолетнего к уголовной ответственности, финансовые последствия зачастую ложатся на семью, а при определённых обстоятельствах могут затронуть и самого подростка в будущем. Именно поэтому к любым предложениям о заработке в Интернете, особенно обещающим быстрый доход без усилий, следует относиться крайне осторожно. Лёгкие деньги редко встречаются в обычной жизни, а в Сети их практически не бывает.

Одна из наиболее распространённых схем связана с так называемыми бегунками. Объявления выглядят как обычная подработка: "курьер по доставке наличных", "работа с наличностью", "быстрые выплаты". Со стороны всё кажется безобидным: не наркотики, не кладки, а всего лишь перевозка денег, почти как работа инкассатора. В действительности мошенники сначала обманывают человека, нередко пожилого, а затем направляют исполнителя забрать наличные, распределить их по банкоматам, перевести на указанные счета и оставить себе заранее оговорённый процент. Подобных курьеров устанавливают достаточно быстро: телефон фиксирует маршруты перемещения, банкоматы оборудованы камерами наблюдения, а финансовые операции оставляют цифровой след. В результате такой "подработки" человек может оказаться фигурантом уголовного дела о мошенничестве.

Пожоя история — дроперы. Здесь уже не нужно куда-то ехать: используется банковская карта. На неё приходят деньги, после чего человек переводит их дальше. Легенда может быть любой: "тестирование банковского продукта", "оператор лотереи", "перевод выигрышей", "белые деньги". Но если на вашу карту приходят чужие средства, а вы отправляете их дальше, вы становитесь частью схемы по выводу похищенных денег.

То же самое касается объявлений вроде "Возьму в аренду ваш аккаунт на "Авито", "Нужен аккаунт в мессенджере для работы". Преступнику нужен ваш профиль, чтобы с него обманывать других людей, рассылать сообщения, размещать объявления или вести переписку, прикрываясь вашей личностью. Если с вашего аккаунта будут совершены противоправные действия, вам потом придётся доказывать, что это были не вы. Поэтому доступ к аккаунтам нельзя передавать никому, а старые профили лучше удалить или надёжно защитить.

Ещё одна массовая схема связана с предложениями "тестировать оборудование". Человеку присылают небольшой блок с сим-картами и антеннами — так называемый сим-бокс — и говорят, что его нужно просто включить в розетку. Легенда может быть любой: тестирование сотового оператора, проверка связи, обслуживание оборудования. На самом деле такие устройства используются для мошеннических звонков: преступники звонят через интернет-телефонию, но для жертвы вызов выглядит как обычный звонок с мобильного номера. Если человек соглашается поставить такое устройство у себя дома, он фактически помогает мошенникам связываться с потерпевшими и рискует стать участником преступной схемы.

Мы живём в непростое время, когда на нас охотится огромное количество людей, готовых использовать доверчивость, любопытство, желание заработать или просто невнимательность. Поэтому берегите себя и помните: если в Интернете вам предлагают лёгкие деньги, чаще всего их платят за то, чтобы сделать вас частью чужого преступления.

"ЗАВТРА". Чёткая и ёмкая формулировка. Спасибо, Андрей Анатольевич!

Беседовал Алексей ГОНЧАРОВ

* соцсети компании "Мета", признанной экстремистской и запрещённой в РФ

Газета "ЗАВТРА" зарегистрирована Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия. Свидетельство ПИ № ФС 77-22122 от 24 октября 2005 года.

Учредитель и издатель — ООО "Редакция газет-еженедельника "Завтра" (119146, г.Москва, Фрунзенская наб., 18, пом. VII).

Тел. редакции: (903) 131-53-97

Адрес редакции: 119146, г. Москва, Фрунзенская наб., 18, пом. VII.
E-mail: zavtra@zavtra.ru Электронная версия: <http://zavtra.ru/>
Служба распространения: (499) 246-88-52 (т./ф).

Отпечатано в АО "Красная Звезда" (125284, г. Москва, Хорошевское шоссе, 38, тел.: (495) 941-32-09, (495) 941-34-72, (495) 941-31-62, <http://www.redstarprint.ru>, e-mail: kr_zvezda@mail.ru).

Тираж 11 900

Заказ № 4501-2026

Дата выхода в свет — 14.10.2026 г. Подписано в печать 13.10.2026 г. в 14.00, по графику — в 14.00