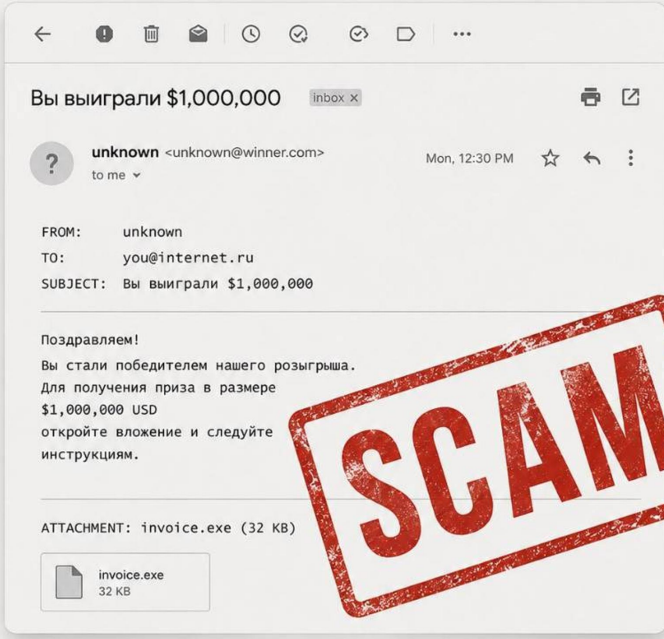
Back Archive Report spam Delete Move to More

SPAM VS SCAM

ИСТОРИЯ МОШЕННИЧЕСТВА В ИНТЕРНЕТЕ



НИКИТА КУЛИКОВ

Никита Куликов

SPAM vs SCAM: история мошенничества в интернете

https://litres.ru/74737492
SelfPub; 2026

Аннотация

SPAM или SCAM? Это одно и тоже или есть разница? В этой книге мы ответим на главный вопрос: где та грань, которая отделяет надоедливый спам от опасного скама? И ответ здесь парадоксален. Спам – это количественная категория. Это шум, который можно измерить в терабайтах и миллионах писем. Скам – это категория качественная. Это целенаправленное действие, основанное на психологическом давлении. Спам вас утомляет. Скам вас разрушает. Спам можно удалить. От скама можно потерять всё.

Мы живём в удивительное и опасное время. Интернет дал нам свободу, информацию и возможность общаться без границ. Но он же дал мошенникам доступ к нашему кошельку, нашей личной жизни и нашей психике.

В этой книге я хочу, чтобы вы научились видеть разницу. Чтобы вы перестали быть статистикой. Чтобы вы защитили себя и своих близких. Потому что в интернете, как и в жизни,

бесплатный сыр бывает только в мышеловке. И чем красивее и заманчивее предложение, тем острее зубья этой ловушки.

Содержание

ВВЕДЕНИЕ 6
Глава 1. Рождение цифрового мусора 10
Глава 2. Виды спама в современном мире 21
Глава 3. Почему спам не исчезает 35
Конец ознакомительного фрагмента. 39

Никита Куликов
SPAM vs SCAM: история мошенничества в интернете

ТИТУЛЬНЫЙ ЛИСТ

SPAM vs SCAM
ИСТОРИЯ МОШЕННИЧЕСТВА В ИНТЕРНЕТЕ

Никита Куликов

ВВЕДЕНИЕ

Два письма в вашем почтовом ящике

Каждое утро миллиардов людей по всему миру начинается одинаково. Чашка кофе, сонный взгляд на экран смартфона или монитора, и – привычное движение пальцем или мышью. Мы открываем почту, мессенджеры, социальные сети. И почти всегда находим там то, что не просили.

Это письма, которые никто не ждал. Предложения, которые никто не заказывал. Угрозы, которые не имеют под собой оснований. И обещания, которые никогда не будут исполнены. Этот цифровой мусор, эта информационная грязь преследует человечество с первых дней существования электронной почты. Но за десятилетия своего существования она прошла долгий путь эволюции – от безобидной рекламной рассылки до изощрённой социальной инженерии, способной уничтожить компанию, разрушить семью и лишить человека всех сбережений за считанные минуты.

Я уже более восьми лет занимаюсь вопросами цифровой безопасности. Я видел, как менялись мошенники. Как они учились, адаптировались, совершенствовали свои инструменты. Как они перешли от «принцев из Нигерии» к дипфейкам и нейросетям. Как они перестали быть одиночками в тёмной комнате и превратились в транснациональные

корпорации с офисами, отделами продаж и годовыми бюджетами, сравнимыми с бюджетами небольших государств.

Эта книга – не сухой учебник по кибербезопасности. Это живая история человеческой доверчивости и человеческой же жадности. Это рассказ о том, как технологии меняют нас и как мы меняем технологии. Это экскурсия в мир, где грань между рекламой и преступлением становится всё тоньше, а иногда и вовсе исчезает.

Вас ждут реальные судебные дела, биографии самых известных интернет-аферистов, психологические портреты жертв, разбор конкретных схем и подробные инструкции по защите. Мы поговорим о том, почему умные и образованные люди попадаются на уловки, которые кажутся смешными и примитивными. Мы разберём, как работают мошеннические колл-центры изнутри, как выводятся украденные деньги и почему правоохранительные органы во всём мире проигрывают битву за цифровое пространство.

Но самое главное – мы ответим на главный вопрос: где та грань, которая отделяет надоедливый спам от опасного скама? И ответ здесь парадоксален. Спам – это количественная категория. Это шум, который можно измерить в терабайтах и миллионах писем. Скам – это категория качественная. Это целенаправленное действие, основанное на психологическом давлении. Спам вас утомляет. Скам вас разрушает. Спам можно удалить. От скама можно потерять всё.

В этой книге я хочу, чтобы вы научились видеть разницу.

Чтобы вы перестали быть статистикой. Чтобы вы защитили себя и своих близких. Потому что в интернете, как и в жизни, бесплатный сыр бывает только в мышеловке. И чем красивее и заманчивее предложение, тем острее зубья этой ловушки.

Мы живём в удивительное и опасное время. Интернет дал нам свободу, информацию и возможность общаться без границ. Но он же дал мошенникам доступ к нашему кошельку, нашей личной жизни и нашей психике. Сделайте глубокий вдох. Отложите телефон. И начните читать. Потому что знание – это действительно сила. И единственное лекарство от скама.

Оглавление

ВВЕДЕНИЕ
Глава 1. Рождение цифрового мусора
Глава 2. Виды спама в современном мире
Глава 3. Почему спам не исчезает
Глава 4. Что такое SCAM и чем он отличается от SPAM
Глава 5. Психология жертвы: почему умные люди попадаются
Глава 6. Основные типы интернет-мошенничества
Глава 7. Битва технологий: искусственный интеллект в руках мошенников

Глава 8. Человеческий фактор. Как не стать жертвой
Глава 9. Крупнейшие скам-операции в истории
Глава 10. Юридические аспекты. Что делает государство
Глава 11. Будущее спама и скама
ЗАКЛЮЧЕНИЕ

Глава 1. Рождение цифрового мусора

1.1. Первое спам-письмо в истории

Чтобы понять природу спама, мы должны отправиться в далёкий 1978 год. Мир ещё не знает персональных компьютеров в том виде, в котором мы привыкли их видеть. Компания Apple только что выпустила Apple II, но это всё ещё игрушка для энтузиастов, а не массовый продукт. IBM ещё не представила свой персональный компьютер – это случится только в 1981 году.

Сеть Arpanet – прародительница современного интернета – объединяет всего около четырёхсот узлов, большинство из которых находятся в университетах, военных лабораториях и исследовательских центрах США. Доступ к сети имеют лишь избранные: учёные, инженеры, военные. Это закрытый клуб, где действуют неписаные правила этикета, а нарушения караются общественным осуждением.

Именно в этой среде 3 мая 1978 года происходит событие, которое навсегда изменит интернет. Сотрудник компании Digital Equipment Corporation (DEC) по имени Гэри Тюрк, маркетолог по профессии, отправляет массовое электронное письмо. В нём он приглашает коллег на презентацию новых моделей компьютеров DEC-20, которые должны были составить конкуренцию продукции IBM. Письмо было отправле-

но на 393 адреса – практически на все адреса в западной части США, которые были доступны на тот момент. Тюрк позже оправдывался, что хотел оповестить как можно больше людей о важном событии, но, по сути, это была первая массовая рассылка коммерческой рекламы.

Реакция не заставила себя ждать. Уже через несколько часов почтовые ящики пользователей Arpanet начали заполняться гневными ответами. Люди возмущались: как кто-то посмел нарушить их личное пространство? Электронная почта в то время воспринималась как инструмент для научной коммуникации, а не как рекламная площадка. Тюрка обвиняли в неуважении к сообществу, в нарушении сетевого этикета, в «спаме». Позже он получил строгий выговор от руководства Arpanet, а его письмо стало хрестоматийным примером того, как делать не надо.

Самое интересное, что термин «спам» тогда ещё не использовался. Его введут чуть позже, в 1980-х годах, когда другой пользователь по имени Ричард Дип вернёт в оборот слово из скетча «Монти Пайтона». В том скетче группа викингов в ресторане начинает громко и навязчиво петь песню о консервированной ветчине «Spam», перекрывая все остальные разговоры. Так и спам-письма – они заглушают всё остальное, заполняя информационное пространство бессмысленным и раздражающим шумом. Слово прижилось и стало нарицательным.

Но вернёмся к первому спаму. Его последствия оказались

гораздо серьёзнее, чем можно было предположить. Тюрк фактически открыл ящик Пандоры. Он показал, что интернет – это среда, в которой можно распространять любую информацию, независимо от желания получателя. И самое главное – это можно делать почти бесплатно. Если традиционная реклама требовала затрат на печать, рассылку, эфирное время, то электронное письмо стоило копейки. Один раз нажал кнопку «Отправить» – и твоё сообщение у миллиона человек. Это было революционно и одновременно опасно.

1.2. Эволюция спама в 1980-х и 1990-х годах

В 1980-е годы спам оставался относительно редким явлением. Доступ к интернету был у небольшого числа людей, и все они были либо учёными, либо военными. Сообщества были компактными, и нарушителей быстро вычисляли и «отключали» от сети. Однако с коммерциализацией интернета в середине 1990-х ситуация кардинально изменилась. Появились первые провайдеры, доступные широкой публике: AOL, CompuServe, Prodigy. Миллионы людей впервые подключались к сети. И вместе с ними пришли маркетологи.

Первый коммерческий спам-бум пришёлся на 1994 год. Юристы Кантер и Сигел из Аризоны разослали письма тысячам пользователей Usenet (аналог современных форумов) с предложением юридических услуг по оформлению грин-карт. Их метод был грубым, но эффективным. Они просто скопировали все адреса из дискуссионных групп и отправи-

ли одно и то же письмо всем подряд. Реакция была сокрушительной – их завалили проклятиями и угрозами, провайдеры заблокировали их аккаунты, но они заработали сотни тысяч долларов.

Этот случай стал поворотным. Мошенники и рекламщики поняли: спам работает. Даже если 99,9% людей игнорируют письмо, 0,1% от миллиона – это тысяча клиентов. А тысяча клиентов при минимальных затратах на рассылку – это огромная прибыль.

К концу 1990-х годов спам превратился в настоящую эпидемию. Почтовые ящики пользователей захлёстывали предложения о «быстром обогащении», «чудо-таблетках», «бесплатном порно» и «выгодных кредитах». Провайдеры начали внедрять первые антиспам-фильтры, но технологии отставали от изобретательности спамеров. В 1997 году компания Microsoft купила Hotmail и столкнулась с тем, что до 90% входящих сообщений были спамом. Это стало сигналом для всей индустрии: нужно что-то делать.

В 1998 году появился первый закон, регулирующий спам, – в США (штат Вашингтон), но он касался только местных рассылок.

В 2003 году был принят федеральный CAN-SPAM Act, который, впрочем, не запретил спам полностью, а лишь обязал указывать опцию отписки и не использовать ложные заголовки. Многие спамеры просто проигнорировали этот закон.

Параллельно развивалась инфраструктура спама. Появились «спам-фермы» – серверы, специально настроенные для массовых рассылок. Спамеры начали использовать прокси-серверы и подмену адресов, чтобы скрыть своё местоположение.

В начале 2000-х годов возникло целое подпольное сообщество, где продавали базы email-адресов, шаблоны писем и программное обеспечение для рассылок. Цена за миллион адресов колебалась от 100 до 1000 долларов в зависимости от качества базы.

1.3. Как спамеры обходят фильтры

Борьба со спамом с самого начала напоминала бесконечную гонку вооружений. Как только создавался новый фильтр, спамеры тут же находили способ его обойти. Рассмотрим основные методы, которые они использовали и продолжают использовать.

Первый способ – подмена адреса отправителя (spoofing). Спамеры научились маскировать свои письма под сообщения от авторитетных компаний: Microsoft, PayPal, банков. Это не только помогало пройти через фильтры, но и повышало доверие получателя. Технически это было несложно: достаточно указать в заголовке письма чужой адрес. Современные почтовые серверы научились проверять подлинность отправителя (SPF, DKIM, DMARC), но и спамеры адаптировались – они используют взломанные аккаун-

ты реальных людей, чтобы письма приходили с легитимных адресов.

Второй способ – изменение содержания. Фильтры искали ключевые слова: «бесплатно», «виагра», «заработай». Спамеры стали заменять буквы в словах: «бесплатно», «Vi@gr@», «заработай». Они использовали символы, похожие на буквы, вставляли случайные пробелы и переносы строк, чтобы сбить алгоритмы. Например, слово «спам» могло выглядеть как «с п а м» или «sp@m». Фильтры на основе регулярных выражений не могли распознать такие вариации. Позже появились более умные фильтры, использующие машинное обучение, но спамеры начали применять генеративные модели для создания уникальных текстов.

Третий способ – вложение изображений. Вместо текста спамеры начали отправлять письма, состоящие целиком из одной картинки. Фильтры не могли прочитать текст на картинке, а человек прекрасно видел рекламное предложение. Это был период «имидж-спама» (image spam), который достиг пика в 2006–2007 годах. Доля таких писем в общем спам-трафике достигала 50%. Потребовалось внедрение OCR (оптического распознавания символов) в антиспам-системы, чтобы анализировать текст на изображениях. Спамеры ответили тем, что стали добавлять на картинки шум, искажать текст, использовать случайные цвета и фрагменты, чтобы OCR ошибался.

Четвёртый способ – использование ботнетов. Вме-

сто того чтобы отправлять все письма с одного сервера, спамеры заражали сотни тысяч домашних компьютеров. Каждый компьютер становился маленьким почтовым сервером. Отследить все эти IP-адреса было практически невозможно. Ботнеты стали основой спам-индустрии в 2000-х. Самый известный ботнет – Conficker (2008) – заразил более 10 миллионов компьютеров. Другой, Rustock, отправлял до 30 миллиардов писем в день. Борьба с ботнетами требовала скоординированных усилий провайдеров, антивирусных компаний и правоохранительных органов.

Пятый способ – «отравление» байесовских фильтров (Bayesian poisoning). Байесовские фильтры обучаются на примерах спама и хороших писем. Спамеры начали добавлять в письма случайные безобидные слова (например, отрывки из книг, научные термины), чтобы сбить статистику и сделать письмо похожим на легитимное. Это заставляло фильтры ошибаться.

Шестой способ – использование легитимных сервисов. Спамеры часто регистрируются на бесплатных почтовых сервисах (Gmail, Yahoo) и отправляют письма оттуда. Это сложнее заблокировать, потому что IP-адреса принадлежат уважаемым компаниям. Также они используют сервисы массовых рассылок (Mailchimp, SendGrid), которые не всегда проверяют содержание писем.

Сегодня, в эпоху нейросетей и больших данных, методы стали ещё более изощрёнными. Спамеры используют генера-

тивные модели (GPT-4 и аналоги) для создания уникальных писем для каждого адресата. Текст меняется, заголовки меняются, предложения меняются – всё для того, чтобы пройти через фильтры машинного обучения. Более того, они используют данные из утечек, чтобы персонализировать письма: обращаться по имени, упоминать место работы, недавние покупки. Это делает спам почти неотличимым от легитимной корреспонденции.

1.4. Экономика спама: почему это до сих пор выгодно

На первый взгляд, спам кажется анахронизмом. В 2024 году по данным компании Kaspersky, антиспам-фильтры отсеивают до 98,7% всех нежелательных сообщений. Почему же спамеры продолжают тратить время и ресурсы? Ответ прост: экономика.

Стоимость отправки миллиона писем сегодня составляет менее 0,1 доллара. Если учесть, что в мире есть миллиарды почтовых ящиков, то потенциал аудитории практически бесконечен. Даже при конверсии 0,001% (один человек из ста тысяч) спамер получает 10 клиентов с миллиона писем. Если средний чек составляет 100 долларов (а это очень скромная оценка), то с рассылки он зарабатывает 1000 долларов при затратах в 0,1 доллара. Маржинальность – 99,99%. Это объясняет, почему спам не исчезает, несмотря на все усилия по борьбе с ним.

Кроме того, спам стал индустрией с чётким разделением труда. Есть кураторы баз данных – они продают и покупают адреса электронной почты. Есть сервис-провайдеры – они предоставляют инфраструктуру для рассылок. Есть копирайтеры – они пишут убедительные письма. Есть аналитики – они тестируют разные варианты писем и выбирают лучшие. Это полноценный бизнес с оборотами в миллиарды долларов.

Рассмотрим основные бизнес-модели спама.

Фармацевтический спам. Один из самых прибыльных сегментов. Спамеры рекламируют поддельные лекарства (виагру, средства для похудения, стероиды). Покупатель платит деньги, но получает пустышку или опасное вещество. По оценкам исследователей, доход от фармацевтического спама составляет миллиарды долларов в год. В 2010 году была закрыта крупная спам-сеть Spamit, которая зарабатывала на продаже поддельных лекарств. Её организатор, Игорь Гусев, до сих пор в розыске.

Спам с предложением «быстрого заработка». Это могут быть пирамиды, инвестиционные схемы, лохотроны. Жертве предлагают вложить небольшую сумму и получить огромную прибыль. Естественно, деньги исчезают.

Фишинговый спам. Письма, которые выглядят как сообщения от банка, налоговой, почтовой службы. Цель – выманить логины, пароли, данные карт. Этот вид спама наиболее опасен для обычных пользователей.

Спам с вирусами. Письма с вложениями (обычно .exe, .zip, .doc с макросами), которые содержат вредоносные программы. Открываешь файл – и твой компьютер становится частью ботнета или шифруется.

«Нигерийские письма» (419 scam). Хотя это скорее скам, чем спам, они часто рассылаются массово. Мошенники представляются принцами, вдовами миллионеров, военными и просят помочь вывести деньги за небольшое вознаграждение. Жертва платит «комиссию» и ничего не получает.

Спам для накрутки трафика. Спамеры рассылают письма со ссылками на сайты, чтобы увеличить посещаемость и заработать на рекламе. Это может быть порно, пиратский контент, фейковые новости.

Экономика спама также включает в себя «партнёрские программы». Спамеры получают процент от каждой продажи, совершённой по их ссылке. Это создаёт целую сеть мотиваций: чем больше писем отправил, тем больше вероятность, что кто-то купит.

Интересно, что спамеры часто используют психологические уловки, чтобы повысить конверсию. Они играют на жадности («выиграйте миллион»), страхе («ваш аккаунт взломают»), любопытстве («кто-то искал вас в социальных сетях»), срочности («предложение действует только сегодня»). Эти же приёмы используются в легитимном маркетинге, но спамеры доводят их до крайности.

Почему спам до сих пор не исчез? Потому что он приносит прибыль. Пока есть люди, которые покупают поддельные лекарства, верят в «быстрый заработок» и переходят по ссылкам, спам будет существовать. И пока стоимость рассылки остаётся близкой к нулю, а конверсия – пусть и крошечная, но достаточная для окупаемости, спамеры будут продолжать свою деятельность.

Более того, спам-индустрия постоянно оптимизируется. Существуют готовые платформы для рассылок, базы адресов, шаблоны писем – всё это продаётся на теневых форумах. Стать спамером сегодня может кто угодно, даже без технических знаний. Достаточно купить доступ к сервису рассылки и базу адресов. Это делает спам ещё более доступным и распространённым.

Глава 2. Виды спама в современном мире

2.1. Email-спам: классика жанра

Email-спам остаётся самым распространённым видом нежелательных сообщений. По данным Statista, в 2024 году спам составлял примерно 46% от всего мирового почтового трафика. Это почти 150 миллиардов писем в день. Если представить, что каждое письмо – это лист бумаги, то ежедневно человечество производит гору макулатуры, которая могла бы покрыть небольшую страну. И большая часть этого мусора отправляется автоматически, без участия человека.

Классификация email-спама выглядит так:

1. Рекламный спам. Продвижение товаров и услуг. Чаще всего это нелегальные продукты: поддельные лекарства, фитнес-добавки, стероиды, контрафактные часы. Но встречается и вполне легальная реклама – от агрессивных маркетологов, которые не спрашивали согласия клиентов. Например, небольшие интернет-магазины могут покупать базы адресов и рассылать свои каталоги. Формально это нарушение, но на практике такие рассылки часто остаются безнаказанными.

2. Мошеннический спам (скам). Письма с целью выманить деньги или личные данные. Об этом мы подробно по-

говорим во второй части книги. Здесь лишь отметим, что скам-письма часто маскируются под рекламу или уведомления от банков.

3. Фишинговый спам. Разновидность мошенничества, но выделенная в отдельную категорию из-за своей массовости и опасности. Письма от «банков», «налоговых», «почтовых служб». Они содержат ссылки на поддельные сайты, где жертва вводит свои данные.

4. Спам с вирусами. Письма с вложениями, которые содержат вредоносные программы. Открываешь файл – и твой компьютер становится частью ботнета или шифруется. Часто такие письма маскируются под счета, резюме, фотографии.

5. «Нигерийские письма» (419 scam). Хотя это скорее скам, они рассылаются массово. Мошенники представляются принцами, вдовами миллионеров, военными и просят помочь вывести деньги за небольшое вознаграждение.

Интересный факт: большинство email-адресов собираются автоматически. Специальные программы-краулеры сканируют сайты, форумы, соцсети и выцепляют все строки, похожие на адрес электронной почты. Если вы хоть раз оставили свой email на непроверенном сайте – можете не сомневаться, он уже продан десяткам спамерских баз. Существуют даже специальные сервисы, которые за небольшую плату находят «свежие» базы адресов, собранные за последние месяцы. Чем свежее база, тем выше конверсия.

Почему email-спам до сих пор жив? Потому что элек-

тронная почта остаётся основным каналом деловой и личной коммуникации. Миллиарды людей проверяют почту каждый день. И даже если 99% писем отсеиваются фильтрами, оставшийся 1% может принести прибыль. Кроме того, спамеры постоянно совершенствуют методы обхода фильтров. Они используют легитимные почтовые сервисы, подмену адресов, шифрование содержимого, чтобы письмо не было распознано как спам.

В 2023 году исследователи из компании Cisco Talos обнаружили новую волну email-спама, который использовал легитимные сервисы Google и Microsoft для рассылки. Письма приходили с реальных адресов Gmail и Outlook, что автоматически повышало доверие. Внутри было вложение с вредоносным макросом. Такие атаки сложно отследить, потому что они используют инфраструктуру уважаемых компаний.

2.2. SMS-спам и телефонный спам

С приходом мобильных телефонов спам перекочевал и на этот канал связи. В некоторых странах, особенно в США и Китае, SMS-спам является серьёзной проблемой. Особенность SMS-спама в том, что его сложнее фильтровать. Операторы связи внедряют спам-фильтры, но они далеки от идеала. Кроме того, SMS-спам часто использует подмену номера отправителя (spoofing). Вы получаете сообщение, которое выглядит так, будто его отправил ваш банк, а на самом деле это мошенники.

В России SMS-спам тоже распространён. Многие пользователи получают сообщения о «выигрыше в лотерею», «блокировке карты», «задолженности по кредиту». Мошенники используют психологическое давление: «Срочно позвоните по номеру», «Ваш аккаунт будет удалён». Если перезвонить, можно попасть на платную линию или на мошенника, который выманит данные.

Телефонный спам – это не только сообщения. Это и бесконечные звонки с предложениями кредитов, страховок, ремонта. В 2019 году Федеральная торговая комиссия США зафиксировала более 5 миллиардов нежелательных звонков за один месяц. И это только те, что были зарегистрированы. В России аналогичная проблема. По оценкам аналитиков, каждый житель крупного города получает в среднем 3–5 спам-звонков в неделю. Особенно активны коллекторы, банки и микрофинансовые организации.

С развитием технологий появился новый вид телефонного спама – «робозвонки» (robocalls). Это автоматические звонки с записанным голосом. Они могут имитировать голос реального человека, использовать интерактивные меню («Нажмите 1, чтобы соединиться с оператором»). Робозвонки дешевы и позволяют охватить тысячи людей за час. Власти разных стран пытаются бороться с ними, но пока безуспешно.

В 2021 году в России был принят закон, обязывающий операторов связи блокировать звонки с подменных номеров.

Однако мошенники научились обходить и это: они используют SIM-боксы (устройства, которые подключаются к сотовой сети и могут отправлять тысячи SMS и звонков). Борьба продолжается.

2.3. Спам в мессенджерах

С ростом популярности мессенджеров спамеры быстро переключились и на них. Это идеальная среда: высокая доставляемость, низкий порог входа, возможность использовать ботов.

Рекламные каналы. Вас добавляют в каналы без вашего согласия. Это могут быть каналы с порно, ставками, «быстрым заработком». Выйти из канала можно, но иногда это неочевидно. Кроме того, спамеры создают каналы-клоны известных брендов, чтобы обманывать подписчиков.

Личные сообщения от ботов. «Привет! Я Аня, ищу парня для серьёзных отношений. Зайди на мой сайт...» Или «Привет! Я зарабатываю 5000 рублей в день, хочу научить тебя». Боты могут имитировать живое общение, отвечать на вопросы, отправлять фото.

Фишинг в группах. В крупных группах появляются сообщения с ссылками на поддельные сайты. Часто они маскируются под «полезные советы», «конкурсы», «бесплатные курсы».

Спам часто маскируется под цепочки: «Перешли это сообщение 10 друзьям, и тебе на телефон придёт 1000 руб-

лей». Это классический «счастливый спам», который, помимо того что раздражает, может содержать ссылки на вирусы. Также распространены мошенничества с «кодом подтверждения»: злоумышленник пытается получить ваш код для входа в аккаунт, представляясь другом или службой поддержки.

В России мессенджеры понемногу учатся бороться со спамом. Они, например, блокируют тысячи аккаунтов ежедневно. Но поскольку создание нового аккаунта занимает минуту, борьба идёт с переменным успехом. Другой мессенджер ввёл ограничения на пересылку сообщений (не более 5 чатов одновременно), чтобы замедлить распространение спама.

Однако спамеры находят новые лазейки. Например, они используют «серые» SIM-карты, зарегистрированные на подставных лиц. Или покупают аккаунты, созданные давно (так называемые «отлежавшиеся» аккаунты), чтобы обойти ограничения для новых пользователей. Это делает борьбу сложной и дорогостоящей.

2.4. Спам в комментариях и SEO-спам

Один из самых старых видов спама – это комментарии на сайтах и форумах. Боты автоматически оставляют сообщения под статьями, в обсуждениях, в гостевых книгах. Обычно это ссылки на мошеннические или рекламные сайты. Зачем это делается? Во-первых, для продвижения сайтов в поисковых системах. Чем больше ссылок на сайт в интернете,

тем выше его позиция в Google или Яндексе. Это называется SEO-спам. Во-вторых, это прямой маркетинг. Человек может случайно кликнуть на ссылку и перейти на сайт мошенников.

SEO-спам стал настоящей проблемой для владельцев сайтов. Google постоянно обновляет свои алгоритмы, чтобы бороться с накруткой ссылок, но спамеры тоже не дремлют. Они используют новые методы: создают целые сети сайтов, которые ссылаются друг на друга, размещают комментарии на авторитетных платформах, используют скрытый текст. В 2021 году исследователи из компании Sitelock обнаружили, что более 80% всех вредоносных программ распространяются именно через спам-комментарии и взломанные плагины для сайтов.

Существует несколько разновидностей SEO-спама:

1. Спам в комментариях блогов. Боты оставляют комментарии вида «Отличная статья! Заходите на мой сайт...». Часто такие комментарии не имеют отношения к теме.

2. Спам на форумах. Регистрируются новые пользователи, которые оставляют сообщения с ссылками. Иногда они пишут осмысленные посты, чтобы не быть забаненными, а в подписи ставят ссылку.

3. Спам в гостевых книгах. Устаревший, но всё ещё встречающийся вид.

4. Спам в социальных закладках. Добавление ссылок на сайты в сервисы закладок (например, Reddit, Pinterest) с

целью накрутки.

5. Спам в вики-проектах. Добавление ссылок в статьи Википедии или других вики. Модераторы борются с этим, но не всегда успешно.

6. «Дропнутые» домены. Спамеры покупают старые домены с хорошей историей и размещают на них ссылки. Это позволяет обходить фильтры поисковых систем.

Для борьбы с SEO-спамом поисковые системы используют сложные алгоритмы, которые анализируют качество ссылок, релевантность, естественность. Но спамеры постоянно адаптируются. Это бесконечная гонка.

2.5. Социальный спам

Социальные сети превратились в огромный спам-полигон. Мошенники создают тысячи фальшивых аккаунтов, которые оставляют спам-комментарии под популярными постами («Заработайте 5000 рублей в день!»), отправляют личные сообщения с предложениями, публикуют посты в группах с ссылками.

Особенно опасен спам в Instagram[1] и TikTok, где молодёжь менее критично относится к незнакомым предложениям. Мошенники используют красивые фото, обещания быстрого заработка, «секретные схемы». Они могут взламывать реальные аккаунты и рассылать спам от имени ваших друзей.

---

[1] Компания Meta (Facebook и Instagram) признана в РФ экстремистской организацией и запрещена в России

Мета[2] ежегодно тратит миллиарды долларов на борьбу с ботами и спамом. Нейросети компании анализируют миллиарды публикаций в день и блокируют подозрительные аккаунты. Но спамеры используют прокси-сервера, меняют IP-адреса, используют виртуальные SIM-карты – и цикл продолжается.

В ВКонтакте также распространён спам. Это и сообщения от фейковых аккаунтов, и комментарии под постами, и «приглашения в группы». Администрация ВК борется с этим, но полностью искоренить спам не удаётся.

Социальный спам опасен не только навязчивостью, но и тем, что он часто используется для фишинга. Ссылки ведут на поддельные страницы входа в соцсети, где жертва вводит логин и пароль. После этого аккаунт взламывают и используют для дальнейших атак.

2.6. Спам в поисковой выдаче (поисковый спам)

Поисковый спам – это метод манипуляции поисковой выдачей. Спамеры создают сайты, которые выглядят как легитимные, но на самом деле содержат вредоносный код или перенаправляют на мошеннические ресурсы. Они используют «чёрные» методы SEO: скрытый текст, клоакинг (показ разных страниц поисковику и пользователю), накрутку поведенческих факторов.

---

[2] Компания Meta (Facebook и Instagram) признана в РФ экстремистской организацией и запрещена в России

Один из самых распространённых видов поискового спама – «фарм-сайты». Это сайты, которые генерируют контент автоматически или копируют его с других ресурсов. Их цель – получить трафик из поиска и перенаправить его на рекламные или мошеннические страницы.

Также существует «спам в результатах поиска» – когда по запросу пользователя появляются ссылки на поддельные сайты, которые выглядят как официальные. Например, по запросу «скачать мессенджер» можно попасть на сайт с вирусом.

Поисковые системы (Google, Яндекс) постоянно совершенствуют алгоритмы борьбы с поисковым спамом. Они используют машинное обучение, анализ ссылочной массы, оценку качества контента. Но спамеры находят новые способы обхода. Например, используют «дорвей-сайты» (doorway), которые создают тысячи страниц с ключевыми словами, а затем перенаправляют пользователей на нужный сайт.

2.7. Спам в мобильных приложениях и push-уведомления

С развитием мобильных технологий появился новый канал спама – push-уведомления. Многие приложения запрашивают разрешение на отправку уведомлений, а затем используют его для рекламы. Пользователь может отключить уведомления в настройках, но не все это делают.

Также существует спам в мобильных приложениях: при скачивании бесплатного приложения вы можете получить в комплекте рекламный модуль, который показывает навязчивые баннеры и всплывающие окна. Иногда такие модули содержат вредоносный код.

В 2022 году исследователи из компании Avast обнаружили более 50 приложений в Google Play, которые содержали агрессивную рекламу и скрытые функции. После жалоб приложения были удалены, но проблема остаётся.

2.8. Спам в играх и виртуальных мирах

Онлайн-игры – ещё одна площадка для спама. В чатах игр (World of Warcraft, CS:GO, Dota 2) постоянно появляются сообщения о продаже игровой валюты, аккаунтов, «буста» рейтинга. Мошенники могут предлагать «бесплатные скины» или «читы», но в результате крадут аккаунт или деньги.

В виртуальных мирах (Second Life, VRChat) также встречается спам. Пользователи могут получать сообщения с рекламой, ссылками на мошеннические сайты. Иногда спамеры используют ботов, чтобы заполонить чат.

2.9. Спам в облачных хранилищах и совместных документах

С развитием облачных технологий появился новый вид спама – спам в облачных хранилищах (Google Drive, Dropbox, OneDrive). Злоумышленники делятся папками с

пользователями, содержащими рекламу или вредоносные файлы. Или добавляют пользователей в совместные документы с рекламным текстом.

Также существует спам в календарях (Google Calendar, iCloud). Мошенники отправляют приглашения на события с рекламой или фишинговыми ссылками. Пользователь может случайно принять приглашение и подписаться на спам.

2.10. Спам в интернете вещей (IoT)

С ростом числа умных устройств (холодильники, чайники, лампочки) появился новый канал для спама. Злоумышленники могут взламывать устройства и использовать их для рассылки спама или участия в ботнетах. В 2016 году ботнет Mirai, состоящий из заражённых IoT-устройств, устроил крупнейшую DDoS-атаку, которая обрушила Twitter, Spotify и другие сервисы. Хотя это не спам в чистом виде, это показывает уязвимость IoT.

2.11. Спам в голосовых помощниках и умных колонках

Голосовые помощники (Alexa, Google Assistant, Siri) также могут быть использованы для спама. Злоумышленники могут создавать «навыки» (skills), которые при активации начинают рекламировать товары или услуги. Или использовать уязвимости в системе распознавания речи, чтобы заставить помощника выполнить нежелательные действия.

В 2021 году исследователи продемонстрировали атаку «DolphinAttack», которая позволяла отправлять голосовые команды на устройства, используя ультразвук, неслышимый для человека. Это открывает новые возможности для спама и мошенничества.

2.12. Статистика и тенденции

По данным компании Kaspersky, в 2024 году доля спама в мировом почтовом трафике составила 46%. Это означает, что почти каждое второе письмо – спам. В абсолютных цифрах это около 150 миллиардов писем в день.

Страны-лидеры по объёму исходящего спама: США, Россия, Китай, Индия, Бразилия. Однако география спама постоянно меняется. Спамеры используют серверы в разных странах, чтобы обходить блокировки.

Типы спама (по данным за 2024 год):

Реклама – 30%

Фишинг – 25%

Вредоносные вложения – 20%

«Нигерийские письма» – 10%

Другое – 15%

С развитием искусственного интеллекта спам становится более персонализированным и опасным. Нейросети позволяют создавать уникальные письма для каждого получателя, что снижает эффективность фильтров. Ожидается, что к 2027 году доля спама, созданного с помощью ИИ, достигнет

50%.

2.13. Заключение

Мы рассмотрели основные виды спама в современном мире: email, SMS, мессенджеры, социальные сети, поисковую выдачу, мобильные приложения, игры, облачные хранилища, IoT и голосовых помощников. Спам вездесущ. Он проник во все каналы коммуникации и продолжает эволюционировать.

Главный вывод: спам – это не просто надоедливая реклама. Это сложная индустрия, которая использует технологические уязвимости и человеческую психологию. И хотя антиспам-фильтры становятся всё лучше, полностью искоренить спам не удаётся. Поэтому каждый пользователь должен быть бдительным и знать, как защититься.

В следующей главе мы поговорим о том, почему спам не исчезает, несмотря на все усилия. Мы рассмотрим экономические, юридические и технологические причины. А затем перейдём к скаму – более опасному явлению, которое требует отдельного разговора.

Глава 3. Почему спам не исчезает

3.1. Экономика спама: прибыль превыше всего

Главная причина живучести спама – это экономика. Пока рассылка приносит прибыль, спамеры будут находить способы обходить фильтры и законы. Давайте разберём эту экономику подробно.

Стоимость рассылки. Отправить миллион электронных писем сегодня стоит менее 0,1 доллара. Это достигается за счёт использования ботнетов (сетей заражённых компьютеров), бесплатных почтовых сервисов и дешёвых серверов в странах с мягким законодательством. Спамеру не нужно покупать марки, конверты или платить за эфирное время. Достаточно арендовать сервер за 10–20 долларов в месяц и запустить скрипт.

Конверсия. Даже при очень низкой конверсии спам окупается. Например, если из миллиона писем только 10 человек совершат покупку (конверсия 0,001%), а средний чек составит 100 долларов, то доход составит 1000 долларов. При затратах в 0,1 доллара прибыль – 999,9 долларов. Маржинальность – 99,99%. Это объясняет, почему спамеры не сдаются: даже минимальный отклик приносит огромную прибыль.

Бизнес-модели. Спам-индустрия включает несколько

уровней:

Кураторы баз данных – продают и покупают адреса электронной почты. Цена за миллион адресов колеблется от 100 до 1000 долларов в зависимости от качества (свежести, географии, наличия дополнительных данных).

Сервис-провайдеры – предоставляют инфраструктуру для рассылок: серверы, прокси, программы для обхода фильтров.

Копирайтеры – пишут убедительные тексты. Часто используются нейросети для генерации уникальных писем.

Аналитики – тестируют разные варианты писем (A/B-тестирование) и выбирают наиболее эффективные.

Партнёрские программы – спамеры получают процент от каждой продажи, совершённой по их ссылке. Это создаёт сеть мотиваций: чем больше писем отправил, тем больше вероятность, что кто-то купит.

Основные источники дохода:

Фармацевтический спам. Поддельные лекарства (виагра, средства для похудения, стероиды). Покупатель платит, но получает пустышку или опасное вещество. По оценкам, доход от фармацевтического спама – миллиарды долларов в год.

«Быстрый заработок». Инвестиционные пирамиды, лохотроны, «секретные схемы». Жертва вкладывает деньги и теряет их.

Фишинг. Кража логинов, паролей, данных карт. Укра-

денные данные продаются на теневых форумах.

Вредоносные программы. Распространение вирусов, шифровальщиков, троянов. Злоумышленники получают выкуп или используют заражённые компьютеры для других атак.

Накрутка трафика. Спамеры рассылают ссылки на сайты, чтобы увеличить посещаемость и заработать на рекламе.

Психология прибыли. Спамеры играют на жадности, страхе, любопытстве. Они используют срочность («только сегодня»), авторитет («от имени банка»), социальное доказательство («тысячи довольных клиентов»). Эти же приёмы используются в легитимном маркетинге, но спамеры доводят их до крайности.

Масштаб. По оценкам компании Cisco, мировой ущерб от спама составляет около 200 миллиардов долларов в год (включая потери в продуктивности, затраты на фильтры, мошенничество). Это делает спам одной из самых прибыльных нелегальных индустрий.

3.2. Юридическая безнаказанность

Спам остаётся низкорисковым занятием для преступников. Во многих странах законы о спаме существуют, но они либо слабые, либо плохо исполняются.

США. Закон CAN-SPAM Act (2003) разрешает рассылки при условии наличия опции отписки и достоверной информации об отправителе. Однако закон не запрещает сам спам,

а лишь регулирует его. Штрафы за нарушение – до 16 000 долларов за письмо, но на практике доказать вину спамера почти невозможно. Многие спамеры находятся за пределами США.

Европейский Союз. GDPR (2018) требует явного согласия пользователя на получение писем. Это строже, чем в США. Но GDPR распространяется только на легальный бизнес. Теневые рассыльщики игнорируют закон, а поймать их сложно, так как они используют серверы в юрисдикциях с мягким законодательством.

Россия. Закон «О рекламе» (№38-ФЗ) запрещает распространение рекламы без согласия абонента. Закон «О персональных данных» (№152-ФЗ) требует согласия на обработку данных. Однако штрафы невелики (до 500 000 рублей для юридических лиц), а Роскомнадзор может привлечь к ответственности только легальные компании. Мошенники, сидящие в другой стране, остаются недосягаемыми.

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.