УДК 004.056

СМС-БОМБЕРЫ: ЧТО ЭТО ТАКОЕ И КАК ОНИ ИСПОЛЬЗУЮТСЯ?

© **Овечкин Р. А., Юдалевич Н. В., 2025**
Иркутский государственный университет, г. Иркутск

В статье рассматривается феномен SMS-бомберов — программ и сервисов, предназначенных для массовой рассылки SMS-сообщений на один целевой номер. Приводится исторический экскурс появления SMS-бомбинга и эволюции его использования. Проанализированы технические особенности реализации SMS-бомберов, включая принцип их работы, существующие типы (легальные маркетинговые и нелегальные вредоносные версии), платформы распространения (скрипты, веб-сервисы, боты и приложения) и меры противодействия со стороны операторов связи. Отдельное внимание уделено использованию SMS-бомбинга в мошеннических схемах: описаны примеры фишинговых атак, социальной инженерии, шантажа, а также способы проверки актуальности украденных данных через SMS-атаку. Рассмотрены возможные виды ущерба от применения SMS-бомберов — финансовый (прямые потери средств, затраты компаний на трафик), эмоциональный (стресс и паника жертв), репутационный (подрыв доверия к каналам связи) и технический (перегрузка инфраструктуры, сбои сервисов). Проанализировано текущее законодательное регулирование данного явления в Российской Федерации: приведены нормы административной ответственности за рассылку спама и обсуждается сложность квалификации SMS-бомбинга как преступления. В заключение предлагаются рекомендации по защите от SMS-бомбинга для пользователей (в том числе методы самозащиты) и для операторов связи (технические и организационные меры), подводятся итоги исследования и намечаются перспективы развития механизмов противодействия SMS-бомбингу.

Ключевые слова: SMS-бомбер; SMS-бомбинг; спам-атака; фишинг; социальная инженерия; мобильная безопасность; кибермошенничество; кибербезопасность

Что такое SMS-бомбер. SMS-бомбер представляет собой специальное программное обеспечение или онлайн-сервис, предназначенный для массированной отправки множества SMS-сообщений на один и тот же номер телефона в короткий промежуток времени [1].

По своей сути SMS-бомбинг является разновидностью спам-атаки на мобильный телефон: цель заключается в том, чтобы завалить телефон жертвы сотнями сообщений и тем самым создать перегрузку или помеху в работе устройства [5]. SMS-бомбинг может применяться как относительно безобидно (например, для розыгрышей или агрессивной рекламы), так и в качестве кибератаки — способа преследования, вымогательства либо элемента сложной мошеннической схемы [1]. В англоязычной терминологии данное явление также известно как SMS spam flooding или SMS/OTP bombing, подчёркивая метод — «бомбардировку» устройства жертвы потоком сообщений.

История появления. Первые случаи использования SMS-бомберов датируются началом 2000-х годов, когда мобильная связь и SMS-сервисы стали массовыми. Изначально SMS-бомберы применялись энтузиастами и злоумышленниками как инструмент сетевой мести или хулиганства в интернете [3]. Так, конкуренты в бизнесе или нечистоплотные политтехнологи могли использовать SMS-бомбинг, чтобы временно вывести из строя связь оппонента. По данным экспертов, подобные приёмы отмечались, например, в период предвыборных кампаний: в день выборов конкуренты через SMS-бомбер намеренно заваливали телефон штаба соперника бесчисленными сообщениями, мешая координации его работы [3]. Со временем явление вышло за рамки «шуток» и стало использоваться злоумышленниками для более серьёзных целей — от мести частным лицам до отвлекающих манёвров при кибератаках. К настоящему времени SMS-бомберы превратились в доступный инструмент, который может приобрести или запустить практически любой желающий: существуют открытые скрипты и готовые сервисы, позволяющие за небольшую плату (а иногда и бесплатно) организовать спам-атаку на чей-либо телефон [1,3]. Это привело к тому, что SMS-бомбинг стал широко распространённым явлением, требующим внимания со стороны специалистов по кибербезопасности и регуляторов.

Технические особенности

Принцип работы. Типичный SMS-бомбер функционирует по простому алгоритму: злоумышленник задаёт целевой номер телефона и параметры атаки (количество сообщений, частоту отправки и пр.), после чего программа автоматизирует отправку сообщений на этот номер. Отправка сотен SMS реализуется через многочисленные запросы к SMS-шлюзам или сервисам отправки сообщений. Многие нелегальные бомберы злоупотребляют легитимными сервисами — например, используют онлайн-формы «восстановления пароля» различных сайтов, подставляя номер жертвы [1]. В результате сайты (банки, соцсети, интернет-магазины) невольно отправляют на телефон жертвы множественные SMS с кодами подтверждения или уведомлениями. Если на стороне целевого веб-ресурса не стоят ограничения (капча, таймаут между запросами), скрипт-бомбер способен запрашивать отправку десятков сообщений в минуту [1]. Другая техника — использование собственных SMS-шлюзов или SIM-центринов: продвинутые бомберы могут напрямую рассылать сообщения через подключённые GSM-модемы или через API операторов. Однако такой способ требует больших ресурсов; чаще применяют именно многочисленные параллельные запросы через доступные точки отправки SMS. В результате телефон жертвы получает лавину SMS (иногда до нескольких сотен или тысяч за атаку) от разных отправителей и с разным содержимым. Современные SMS-бомберы также могут комбинировать SMS-спам с массовыми авто-звонками (Voice over IP) для усиления эффекта, хотя основная нагрузка обычно идёт через текстовые сообщения.

Типы SMS-бомберов. Можно условно разделить все инструменты SMS-бомбинга на легальные и нелегальные. Легальные аналоги — это маркетинговые рассылщики, используемые компаниями для рекламы (обычно они работают с согласия получателей и соблюдают закон о рекламе). Нелегальные же версии — те самые бомберы, которые применяются без согласия адресата с целью спама или атаки. Если классифицировать технически, то SMS-бомберы бывают нескольких видов:

1. Самостоятельные программы и скрипты. Это программное обеспечение, которое злоумышленник запускает на своём компьютере или сервере. В открытом доступе можно найти множество таких скриптов. Например, на платформе GitHub представлено более 700 проектов SMS-бомберов на разных языках программирования [1]. К популярным относятся скрипты на Python (например, TBomb [1]), Java, PHP и др. Эти программы позволяют вручную настроить параметры атаки (интервалы, количество сообщений) и часто требуют минимальных навыков программирования для запуска.

2. Веб-сервисы SMS-бомбинга. В интернете существуют специальные сайты, где функционал бомбера предоставляется как услуга. Пользователю достаточно зарегистрироваться, указать номер цели, выбрать продолжительность атаки и оплатить услугу (либо воспользоваться ограниченной бесплатной версией). Веб-сервисы берут на себя всю «грязную работу» по отправке SMS. Некоторые из них монетизируются за счёт рекламы или микроплатежей, предлагая дешёвый и доступный спам как сервис [1].

3. Боты в мессенджерах. Всё большую популярность получают боты в Telegram и аналогичных платформах, выступающие в роли SMS-бомберов [3]. Достаточно найти соответствующего бота, отправить ему команду с номером — и бот начнёт атаку, зачастую бесплатно или за символическую плату. Телеграм-боты удобны тем, что не требуют ни установки ПО, ни навыков — управляются простыми командами, скрывая при этом личность инициатора за инфраструктурой Telegram.

4. Мобильные приложения. Существуют и Android-приложения, распространяемые через форумы или альтернативные магазины (в официальных сторах они запрещены). Такие приложения дают аналогичный функционал — выбор цели и запуска бомбардировки — прямо со смартфона злоумышленника. Однако их применение рискованно: работая с телефона, атакующий может легче быть выявлен по SIM-карте или IP-адресу.

В таблице 1 представлен сравнительный обзор основных типов SMS-бомберов, их особенностей и примеров.

Таблица 1. Типы SMS-бомберов и их характеристики

Тип инструмента	Пример / платформа	Особенности
Программа/скрипт	TBomb (Python-скрипт)	Требует запуска на ПК/сервере; высокая настраиваемость; нужные технические навыки; сложно отследить при использовании прокси.
Веб-сервис (онлайн)	SMS spam websites (анонимные)	Доступ с браузера; часто платный или с рекламой; минимальные усилия пользователя; оператор сервиса может регистрировать данные атакующего.
Бот в мессенджере	Боты в Telegram (например, «Мирай»)	Управление через чат-команды; быстро и удобно; часто бесплатно; относительная анонимность (скрыт за аккаунтом мессенджера).
Мобильное приложение	APK «SMS Bomber» для Android	Запуск с мобильного; ограниченные ресурсы отправки; высокий риск деанонимизации (через данные телефона и сети).

Платформы распространения. Как видно из таблицы, распространение SMS-бомберов происходит на самых разных платформах: от репозиториев исходного кода (GitHub, GitLab), где выкладываются скрипты, до специализированных веб-сайтов и каналов в Telegram. Существует целое подпольное сообщество, обменивающееся новыми методами и скриптами бомбинга. Для пользователей, не знакомых с программированием, доступны готовые решения — это существенно снизило порог входа для потенциальных злоумышленников [1]. Популярности SMS-бомбинга способствуют три фактора: минимальные затраты, относительная безнаказанность и простота использования [1]. В большинстве случаев такие атаки совершаются анонимно, и отследить инициатора крайне сложно, особенно если он принимает меры предосторожности (например, использует VPN, анонимные аккаунты, оплачивает криптовалютой услуги bombera) [1]. Тем не менее, существуют уязвимые места: некоторые публичные SMS-центры и сервисы, предоставляющие бомбинг, требуют регистрации с реальными данными и могут выдать их правоохранителям по запросу [1].

Мобильные операторы и противодействие. Операторы связи хорошо осведомлены о проблеме SMS-спама и бомбинга. Многие внедряют системы фильтрации и ограничения на сетевом уровне. Например, если с одного источника на номер поступает слишком много сообщений за короткий период, такая активность может быть распознана как аномальная и автоматически заблокирована. Однако сложность в том, что при SMS-бомбинге сообщения обычно приходят с разных номеров и сервисов, затрудняя простую фильтрацию. Операторы предлагают абонентам услуги типа «Антиспам»: подключив ее, клиент может отсеивать массовые рассылки и подозрительные сообщения. Современные смартфоны также имеют встроенные функции: блокировка отправителя или фильтрация сообщений от неизвестных номеров. Но против распределённой атаки (десятки разных отправителей) эти меры помогают не полностью [1]. Сети операторов испытывают и техническую нагрузку: множество «лишних» SMS занимают ресурсы SMS-центров. В отдельных случаях отмечались перегрузки инфраструктуры — так, если злоумышленники инициируют сотни тысяч SMS через бомбинг, это способно повлечь сбои в доставке легитимных сообщений и увеличить расходы оператора и сервис-провайдеров на SMS-трафик [12]. В ответ операторы внедряют лимиты и капчи на своих сервисах отправки (например, при попытке отправить более N сообщений подряд требуется дополнительная проверка) [1].

В целом, технически запустить SMS-бомбу несложно: достаточная распространённость готовых решений и слабая защищённость многих онлайн-сервисов от автоматизированных запросов сделали эту атаку доступной. Ниже рассмотрим, с какой целью злоумышленники применяют SMS-бомберы и как именно они вписываются в схемы мошенничества.

Применение в мошенничестве

SMS-бомбинг широко используется злоумышленниками в разнообразных мошеннических схемах как вспомогательное средство. Ниже описаны наиболее распространённые сценарии, в которых фигурирует SMS-бомбер, а также группы людей и организаций, становящиеся жертвами таких атак.

Фишинговые атаки и социальная инженерия. Одной из основных сфер применения SMS-бомбера является сочетание спам-атаки с последующим фишингом — выманиванием у жертвы конфиденциальных данных. Схема обычно развивается следующим образом:

- массовая рассылка SMS на номер жертвы — в ход идут сообщения якобы от банков,

госучреждений, сервисов с кодами подтверждения и т.п. (жертва получает десятки SMS подряд);

- дезориентация жертвы — поток сообщений вызывает у человека панику и растерянность. Одновременно может поступать звонок от мошенника, представляющегося, например, сотрудником сотового оператора или службы безопасности банка [5];
- выманивание данных — под предлогом «помощи» лжесотрудник сообщает, что на телефонной линии заметна атака (спам), и предлагает подключить защиту, для чего просит продиктовать коды из полученных SMS или персональные данные [5]. Поскольку жертва напугана непрерывными уведомлениями, она с большей вероятностью соглашается выполнить инструкции;
- хищение информации/денег — получив код из SMS (например, код подтверждения входа в банковский аккаунт), мошенник сразу же использует его для доступа к счетам или оформляет на жертву онлайн-кредит. Таким образом осуществляется кража средств или данных.

Рис. 1. Упрощённая схема мошенничества с использованием SMS-бомбера и последующего фишинг-звонка (социальной инженерии). Злоумышленник инициирует спам-атаку, затем под видом «оператора» выманивает у жертвы коды и получает доступ к её счетам.

Подобные случаи документировались многократно. Например, в 2024 г. фонд поддержки пострадавших от преступлений (ФПП) сообщал о схеме, когда мошенники заваливают жертву спамом, а затем предлагают подключить услугу «антиспам» — и под этим предлогом требуют коды из SMS [5]. Главная цель — усыпить бдительность жертвы, отвлечённой шквалом сообщений, и добиться разглашения ею секретной информации. Эксперты подчёркивают, что напуганного, перегруженного информацией человека легче обмануть [2].

Пример реальной атаки. Журналистка одного российского издания столкнулась с мощным SMS-бомбингом: за вечер ей пришло 36 сообщений от 14 различных организаций, причём большинство содержали коды для входа в личные кабинеты банков и магазинов, которыми она не пользуется [8]. Параллельно от оператора поступали уведомления о попытках платежей по её номеру, а от двух МФО — SMS с кодами подтверждения займа. Эта комбинация свидетельствовала о сложной атаке: мошенники, вероятно, использовали её данные для попыток входа в финансовые сервисы, намеренно вызвали волну SMS на её телефон, а затем могли связаться, чтобы выудить коды. Жертва успела заблокировать свою SIM-карту, что временно прервало атаку. Однако, когда она восстановила работу номера, спам-атака возобновилась, и злоумышленники переключились на её мессенджеры и социальные сети, рассылая уже туда запросы на восстановление паролей [8]. Лишь длительная блокировка SIM (на 48 часов) заставила мошенников отступить. Данный случай демонстрирует, насколько упорными могут быть мошенники, сочетая SMS-бомбер с другими методами давления.

Оформление онлайн-займов (мошенничество с МФО). Ещё одна резонансная схема, выявленная экспертами в 2021 году, связана с оформлением микрозаймов на имя жертвы с помощью SMS-бомбера [2]. Алгоритм действий таков: преступники получают персональные данные человека (паспорт, телефон) из утечки, затем через бомбер регистрируют его номер на десятках онлайн-сервисов и одновременно подают заявки на микрокредиты в МФО [2]. Телефон жертвы в этот момент получает непрерывный поток из ~200 SMS с кодами подтверждения регистрации [2]. Далее мошенники выходят на связь (в мессенджере) под видом помощников, обещающих разобраться с «атакой», и просят прислать скриншот экрана с входящими SMS [2]. На скриншоте, помимо мусорных сообщений, отображаются и коды из SMS (в превью), чего жертва может не осознать. Получив скриншот, злоумышленники выуживают нужные кодовые числа и завершают оформление микрозайма на имя пострадавшего [2]. Деньги мгновенно выводятся на их счета, а жертва остаётся с долгом перед МФО. Эксперты отмечают коварство схемы: мошенник напрямую не запрашивает код (что люди уже привыкли не передавать), а просит лишь скриншот, поэтому психологический «блок» у жертвы не срабатывает [2]. Такой случай был зафиксирован Qrator Labs в 2021 году в России [2]. Данный пример показывает, что SMS-бомбер служит инструментом отвлечения и давления, позволяющим совершить финансовое мошенничество нового типа.

Шантаж и буллинг. SMS-бомбинг также применяется как средство мести или запугивания в личных конфликтах. Злоумышленник, обладая возможностью запустить спам-бомбу, может целенаправленно терроризировать чужой телефон,

не давая ему «замолкнуть» ни на минуту. В наших днях большинство подобных случаев — это месть обиженных телефонных мошенников самим жертвам: например, если потенциальная жертва распознала звонок афериста и грубо оборвала разговор, мошенники нередко мстят, подписывая её номер на спам-рассылки [3] Отмечены случаи, когда коллекторы или недоброжелатели использовали SMS-бомбер, чтобы вызывать у должника постоянный дискомфорт, дестабилизировать его эмоциональное состояние (что можно трактовать как кибербуллинг) [1]. Несмотря на кажущуюся «невредность» (ведь это всего лишь сообщения), такой целенаправленный спам способен нанести серьёзный психологический стресс и воспрепятствовать нормальному использованию телефона. Например, описаны эпизоды, когда жертва бомбинга не могла дозвониться в скорую помощь из-за бесконечных всплывающих SMS, что уже создаёт прямую угрозу [3]

Подмена номеров и мошенничество от имени компаний. Более сложный вид SMS-атак — когда бомбинг провоцируется от лица корпораций. Злоумышленники могут воспользоваться уязвимостями API или процедур отправки сообщений компаний, чтобы инициировать массовую рассылку якобы от имени этих компаний. В 2023 году отмечен трёхкратный рост частоты SMS-атак на банки и маркетплейсы: преступники рассылали клиентам этих организаций сообщения от их имени [4]. По сути, это разновидность DDoS-атаки на коммуникацию: вызывая массовую рассылку, нападающие одновременно перегружают коммуникационные каналы компаний и сеют хаос среди пользователей, получающих ложные уведомления. Представитель компании Servicepipe пояснил, что жертвами в таких случаях выступают сами компании, которым приходится нести расходы за рассылку SMS и разбираться с негативной реакцией клиентов [4]. Подобные атаки могут приводить к сбоям: эксперты зафиксировали случаи, когда боты отсылали до 600 тысяч сообщений в сутки одному банку, что стоило организации до 2 млн рублей прямых затрат [12]. Кроме финансового ущерба, страдает репутация — клиенты получают спам от имени банка и утрачивают доверие. Таким образом, SMS-бомбинг стал элементом киберпреступлений против бизнеса, где он служит для проверки актуальности украденных номеров (если SMS-код пришёл, значит номер активен) [12], для вывода из строя клиентских уведомлений и даже для прямого экономического урона (трата средств компании на отправку).

Целевые группы жертв. Исходя из приведённых сценариев, можно выделить основные категории, на которых нацелены SMS-бомберы:

- частные лица, особенно менее технически подкованные пользователи — они чаще поддаются панике и уловкам социальной инженерии. В зоне риска пожилые люди, соцработники, клиенты банков — т.е. все, чей номер мог утечь в сеть;
- активные клиенты онлайн-сервисов — их данные (номера) фигурируют во множестве баз, и при утечке такой базы именно эти люди получают наибольшее число спам-SMS;
- компании с большой клиентской базой (банки, онлайн-ритейл, маркетплейсы) — как объект косвенной атаки через их коммуникационные сервисы;
- лица, вступившие в конфликт с мошенниками или хакерами — например, разоблачившие телефонного аферисту, конкуренты в бизнесе, публичные персоны. Для них бомбинг становится способом мести и давления.

Итак, SMS-бомбер — многоцелевой инструмент в арсенале мошенников и хулиганов. Рассмотрим, какой ущерб он способен причинить и почему его применение опасно.

Возможный ущерб от SMS-бомберов

Использование SMS-бомбера, особенно в неблаговидных целях, может приводить к разноплановым негативным последствиям — от материальных потерь до угроз жизни и здоровью. Разберём основные виды ущерба.

Финансовый ущерб. Прямая материальная потеря для конкретной жертвы возникает, если SMS-бомбер задействован в схеме кражи денег (как описано выше в случае с фишингом и кредитами). Жертва может лишиться денежных средств со счета или получить на своё имя долг (оформленный кредит) [2]. Кроме того, существует косвенный финансовый ущерб для компаний и операторов. Банки, онлайн-сервисы и сами операторы несут расходы на отправку всех этих спровоцированных SMS. По оценкам, одна массированная атака на банк через SMS-бомбер способна стоить организации до нескольких миллионов рублей из-за счетов за SMS-трафик и необходимости восстановительных мер [12]. Массовый SMS-спам также может приводить к оттоку клиентов: если номер банка неоднократно замечен в «спаме», клиенты могут начать игнорировать и настоящие уведомления, что косвенно бьёт по бизнесу. Репутационный урон (см. ниже) также конвертируется в денежные потери. В целом, SMS-бомбинг повышает издержки на коммуникацию для всех вовлечённых сторон, вынуждая тратить средства на фильтры, антиспам и расследования инцидентов.

Эмоциональный стресс и психологический ущерб. Жертвы SMS-бомбинга часто испытывают сильный стресс. Непрекращающиеся сигналы телефона — звонки, уведомления — вызывают чувство тревоги, паники и беспомощности. Человек не понимает, что происходит, боится пропустить что-то важное или, наоборот, опасается открыть лишнее сообщение. Такое состояние может негативно сказаться на психике, особенно у уязвимых лиц. Врачи отмечают, что постоянный

информационный шум способен привести к нервному перенапряжению, бессоннице. Если бомбинг применяется как форма буллинга, жертва может испытывать длительный психологический дискомфорт, страх пользоваться телефоном. Преступники сознательно рассчитывают на панику жертвы [5], зная, что в таком состоянии она совершит ошибки (раскроет данные или выполнит требования). Таким образом, эмоциональный ущерб — ключевой элемент эффективности SMS-атаки. Помимо индивидуальных страданий, он может иметь и социальное измерение: массовые SMS-рассылки панического содержания (например, ложные сообщения о ЧС) способны посеять страх среди больших групп людей.

Репутационный риск. Для организаций и сервисов, чьи имена вовлечены в SMS-бомбинг, возникает репутационный ущерб. Например, если злоумышленник рассылает спам от имени известного банка или госслужбы (подделывая подпись отправителя), получатели начинают ассоциировать бренд с навязчивым спамом. Даже разобравшись, что это была атака, часть аудитории сохраняет негативный осадок. Более того, телефонные номера отправителей могут попасть в черные списки. Было отмечено, что в России крупные рассылочные номера операторов блокировались мобильными устройствами пользователей после всплеска спам-активности, и затем легитимные сообщения по этим каналам не доходили до адресатов [12]. Компаниям приходится оправдываться перед клиентами и восстанавливать доверие, тратить ресурсы на PR-кампании, разъясняя ситуацию. Со стороны индивидуальных жертв может пострадать их цифровая репутация: например, номер телефона, активно «засвеченный» в спаме, могут начать избегать знакомые, опасаясь вирусов, или заблокируют автоматические фильтры. Таким образом, SMS-бомбер может опосредованно вредить чьему-то доброму имени и коммуникационной надежности.

Технические проблемы и сбои. Массовая рассылка SMS — это нагрузка на техническую инфраструктуру. Если атака масштабна, возможны следующие проблемы:

- Перегрузка телефона жертвы. Большой объем входящих SMS может переполнить память устройства (особенно устаревших моделей) или привести к зависанию приложения сообщений. Постоянные уведомления затрудняют использование смартфона для обычных задач, вплоть до необходимости его временно отключить [1].
- Блокировка SIM-карты. Некоторые жертвы, пытаясь остановить бомбинг, вынуждены временно блокировать свою SIM (через оператора) или даже менять номер. Это прямое неудобство и технический ущерб — фактически человек теряет возможность связи на время или навсегда теряет прежний контактный номер. В известном примере (описанном выше) журналистка смогла прекратить атаку только выключив SIM-карту на двое суток [8].
- Сбои в сетях и сервисах. Как упоминалось, атаки на компании могут вывести из строя их SMS-шлюзы. Также, если бомбинг сгенерировал сотни тысяч запросов на сторонние сайты, возможны DDoS-эффекты — снижется скорость работы этих сайтов, они могут временно становиться недоступными для нормальных пользователей [12]. У операторов связи перегрузка на SMS-центрах теоретически может вызвать задержки в доставке сообщений для широкого круга абонентов, хотя крупные операторы имеют значительный резерв пропускной способности. Тем не менее, рост спам-атак до 20 % за полгода, отмеченный в 2023 г., заставил телеком-компании признать проблему серьёзной [12].

Опасность для жизни и безопасности. В критических ситуациях SMS-бомбинг может создавать прямую угрозу: например, если человек ждёт важного сообщения (кода подтверждения авторизации при входе в аккаунт, сообщения от врача, сигнала тревоги), поток лишних SMS может привести к пропуску жизненно важной информации. Кроме того, отвлекающие звонки, идущие параллельно с SMS-атакой, могут помешать вовремя позвонить в экстренную службу. Такие риски редки, но их нельзя исключать.

Подытоживая, ущерб от SMS-бомбера выходит далеко за рамки «неудобства от спама». Он комплексный: материальный, психологический и системный. Именно по этой причине законодательство пытается реагировать на данный феномен, вводя ответственность за массовые рассылки.

Законодательство и правовая ответственность

Вопрос квалификации SMS-бомбинга с правовой точки зрения сложен. В российском законодательстве нет прямого упоминания «SMS-бомбера» или «SMS-бомбинга», однако отдельные аспекты этого явления подпадают под существующие нормы.

Законодательное регулирование спам-рассылок. Массовая рассылка сообщений без согласия адресата рассматривается как нарушение законодательства о рекламе, если эти сообщения носят рекламный характер. К SMS-бомберам это применимо в той степени, в какой они используются для рассылки рекламы или навязанных услуг. В апреле 2024 года в РФ был принят закон, существенно повышающий штрафы за спам по сетям электросвязи. Согласно Федеральному закону от 06.04.2024 №78-ФЗ (внесены изменения в ст.3.5 и 14.3 КоАП РФ), установлены штрафы за незаконную рассылку рекламы в сообщениях: для граждан — от 10 до 20 тыс. руб., для должностных лиц — 20–100 тыс. руб., для юридических лиц — 300 тыс. — 1 млн руб. [9]. Ранее штрафы были значительно ниже (2–2,5 тыс. руб. для граждан) [10]. Таким образом, государство ужесточило ответственность за SMS-спам. Однако важно

отметить: этот закон нацелен прежде всего на нежелательные рекламные рассылки. Если SMS-бомбер используется для мошенничества или травли (не реклама), то формально данные нормы могут не охватывать такие действия [10]. Тем не менее, зачастую мошенники прикрываются мнимыми «акциями» или «предложениями», что позволяет привлечь их к ответственности и по закону о рекламе.

Административная ответственность. В случаях, когда факт массовой рассылки сообщений доказан, но состав более тяжкого преступления отсутствует, виновные могут привлекаться к административной ответственности. Как раз упомянутая статья 14.3 КоАП РФ (нарушение законодательства о рекламе) — основной инструмент. Даже до ужесточения закона суды применяли штрафы по 2–2,5 тыс. руб. к физическим лицам за рассылку спама по SMS (Вопрос #66410 ОТВЕТСТВЕННОСТЬ ЗА СМС БОМБЕР — Юргород). Теперь эти штрафы выросли до 10–20 тыс. Но на практике выявить конкретное физлицо, запустившее SMS-бомбер, нелегко. Если же обнаружен организатор нелегального сервиса (юридическое лицо), ему грозит крупный штраф до 1 млн руб. и блокировка ресурса. Также Роскомнадзор может ограничивать доступ к онлайн-сервисам, распространяющим вредоносные рассылки.

Уголовная ответственность. Привлечение к уголовной ответственности за использование SMS-бомбера возможно, если будут усмотрены признаки конкретного преступления: например, мошенничество (ст.159 УК РФ) — если с помощью бомбинга похищены деньги; либо неправомерный доступ к компьютерной информации (ст.272 УК РФ) — если действия квалифицировать как атаку на информационные системы (скажем, DDoS на сервисы компаний). Однако сам по себе факт рассылки множества сообщений обычно не образует состава уголовного преступления. В Уголовном кодексе РФ напрямую не предусмотрено наказание за «бомбардировку сообщениями». Тем не менее, если применение SMS-бомбера стало частью мошеннической схемы, ответственность наступит за мошенничество в целом. Так, злоумышленники, оформившие кредит на жертву с помощью бомбера, понесут ответственность по ч.2 ст.159 УК (мошенничество, причинение значительного ущерба гражданину). Разработка и распространение вредоносных программ, к коим можно отнести специализированные SMS-бомберы для атак, теоретически подпадает под ст.273 УК РФ («Создание, использование и распространение вредоносных программ»). Однако применяется эта статья в основном к вирусам и trojan-программам, и прецедентов по ней относительно SMS-бомберов пока не известно. Можно заключить, что SMS-бомбер в чистом виде трудно квалифицировать юридически, и многие злоумышленники чувствуют себя относительно безнаказанно [1]. Максимум, что грозит обычному «шутнику», запустившему бомбер на чужой телефон, — административный штраф, и то если пострадавший обратится в полицию и есть возможность отследить виновника.

Тем не менее, правоприменительная практика постепенно формируется. В СМИ периодически появляются сообщения о задержаниях групп, распространявших услуги SMS-бомбинга. Их привлекают к ответственности либо за сопутствующие нарушения (мошенничество, вымогательство), либо за незаконную предпринимательскую деятельность, либо по ст.274.1 УК РФ (неправомерное воздействие на критическую инфраструктуру) — если атака расценивается как подрывающая функционирование значимых ресурсов. В 2023 году обсуждалась инициатива законодателей дополнительно пресекать массовые звонки и сообщения, в том числе путем блокировки номеров-инициаторов спама на уровне операторов [11]. Операторы связи со своей стороны теперь по закону обязаны создавать систему приема жалоб на спам-звонки и SMS [9], и сотрудничать с регулирующими органами для пресечения подобных нарушений.

В целом, законодательство старается идти в ногу с новой угрозой, хотя и несколько запоздало. Уже действующие нормы позволяют наказывать за SMS-спам, но мошеннические применения SMS-бомбера часто выходят за рамки простого «спама» и требуют комплексного подхода (привлечение по совокупности преступлений). Следующим шагом может стать признание SMS-бомбинга формой атаки на средства связи, с отдельной статьёй или квалифицирующим признаком в УК. Пока же основная нагрузка по борьбе ложится на технические меры защиты и информирование населения.

Защита от SMS-бомберов

Учитывая описанные риски, вопрос защиты от SMS-бомбинга актуален как для рядовых пользователей, так и для операторов связи и онлайн-сервисов. Ниже приведены рекомендации и меры, способные снизить ущерб от таких атак.

Методы защиты для пользователей:

Не паниковать и не реагировать на подозрительные сообщения. Если на телефон посыпались десятки SMS, важно понимать, что это, скорее всего, атака. Ни в коем случае не переходить по ссылкам из неожиданных SMS и не вводить личные данные. Мошенники рассчитывают на поспешные действия — не дайте себя обмануть.

Блокировка номеров и сообщений. Современные телефоны позволяют блокировать конкретного отправителя. Хотя при бомбинге отправители разные, можно включить режим «Не беспокоить» или фильтрацию всех неизвестных номеров в настройках сообщений. Это временно скроет поток уведомлений. В стандартных приложениях есть раздел «Антиспам» или «Черный список», где можно активировать эти функции.

Отключение телефона на время атаки. Самый простой и радикальный способ — выключить смартфон на 10–15 минут. Большинство бомбер-сервисов проводят атаку в течение ограниченного времени (обычно ~20 минут) [1]. Если устройство недоступно, скрипт не сможет доставить SMS, и атака прекратится. После паузы можно снова включить телефон — спам, скорее всего, уже закончится.

Смена SIM-карты (в крайнем случае). Если атаки повторяются, стоит обратиться к оператору и сменить SIM-карту с сохранением номера или даже сменить сам номер телефона. Это кардинально решит проблему, хотя и доставит неудобства (необходимо оповестить контакты о новом номере).

Бдительность при общении. В период или сразу после бомбинг-атаки вероятен звонок мошенников. Следует критически относиться к любым входящим звонкам, где у вас требуют коды или данные. Настоящие сотрудники банка никогда не попросят продиктовать код из SMS. Это золотое правило.

Антивирусные приложения. Держите на смартфоне актуальный антивирус, который может предупреждать о известных спам-номерах и фишинговых ссылках. Он не остановит бомбардировку, но предупредит, что ссылка в SMS ведёт на опасный сайт, если вы случайно нажмёте.

Советы операторам связи: Операторы располагают техническими возможностями для противодействия SMS-бомбингу на сетевом уровне. Рекомендуется:

Внедрение автоматических фильтров. Системы глубокого анализа трафика могут выявлять аномалии — например, один номер получает >100 SMS за 5 минут. В таком случае оператор может временно блокировать поток сообщений на этот номер, предупредив адресата и предложив помощь.

Блокировка по сигнатурам. Многие SMS-бомберы оставляют типичные шаблоны (однотипные тексты, последовательность запросов). Выявление и блокировка сообщений, соответствующих этим шаблонам, снизит эффективность атак.

Сервисы «Антиспам» для клиентов. Как опцию, операторы могут предоставлять услугу фильтрации, когда все сообщения с незарегистрированных в сети номеров или из интернета не доставляются абоненту, либо доставляются в специальную папку. Клиент сам решает, включать это или нет.

Сотрудничество с онлайн-сервисами. Операторы и крупные сервис-провайдеры (банки, порталы) должны обмениваться информацией о случаях бомбинга. Например, компания может уведомить оператора, что ее сервис подвергся атаке (массовая рассылка кодов), чтобы оператор блокировал эти SMS на стороне получателей.

Обратная связь и помощь пострадавшим. Внедрить простой способ для клиента сообщить о спам-атаке (например, короткий номер для SMS-жалобы). При получении жалобы оператор мог бы быстро переключить режим приема SMS для абонента на безопасный, фильтрующий режим. Такие меры уже рекомендованы регулятором и начинают реализовываться [9].

Обучение персонала кол-центров. Клиенты, столкнувшиеся с бомбингом, могут звонить в поддержку в панике. Важно, чтобы сотрудники контакт-центра были знакомы с понятием SMS-бомбинг и могли грамотно instruктировать: успокоить абонента, объяснить, что делать (как отключить телефон, что не сообщать никому коды). Это повысит лояльность клиентов и эффективность противодействия.

Защита онлайн-сервисов и компаний: Организации, чьи сервисы могут быть использованы для SMS-рассылки, должны предпринять шаги, чтобы их ресурсы не превращались в орудие бомберов. Во-первых, ограничение частоты отправки SMS на один номер — например, не более 1–2 сообщений в минуту для функций вроде «восстановить пароль». Во-вторых, капча или защита от ботов на формах, запрашивающих отправку SMS (регистрация, подтверждение входа). Уже сейчас многие внедрили такие ограничения, именно узнав о случаях нелегитимного использования их сервисов для бомбинга [1]. Во-третьих, мониторинг логов: всплеск запросов на отправку кодов — сигнал безопасности о возможной атаке. Крупные компании интегрируют эти сигналы в системы антифрода.

Наконец, повышение осведомлённости пользователей — важная линия обороны. Проведение просветительских кампаний (статьи, памятки, push-уведомления от банков с предупреждениями о новом виде мошенничества) поможет людям не попасться на уловки даже если их телефон подвергся спам-атаке. Чем больше людей знают о существовании SMS-бомберов, тем труднее мошенникам воспользоваться неожиданностью.

Заключение

Итоги. В ходе работы проанализировано явление SMS-бомбинга — от его технической природы до социальных последствий. SMS-бомбер эволюционировал из шуточного скрипта для «заваливания» телефона спамом в опасный инструмент киберпреступников. Сегодня он используется в различных мошеннических схемах: для кражи денег посредством фишинга, для оформления псевдокредитов, для мести и запугивания, а также для атак на коммуникационную инфраструктуру компаний. Техническая доступность таких средств (множество готовых программ и сервисов) и сложность их обнаружения породили рост числа атак, что подтверждают данные экспертов [4,12]. Ущерб от SMS-бомбера многообразен: помимо прямых финансовых потерь жертв и компаний, это психологический прессинг, подрыв доверия к системам связи, перегрузка сетей. Законодательство, хотя и не содержит пока прямой статьи за «SMS-атаку», тем не менее позволяет

привлекать виновных к ответственности через нормы о спаме и мошенничестве. В 2024 году существенно увеличены штрафы за рассылку спам-СМС, что должно служить сдерживающим фактором [9]. Однако основной упор делается на технологические меры защиты и образовательные инициативы.

Перспективы. В дальнейшем стоит ожидать как совершенствования атак (например, комбинирования SMS-бомбинга с OTP-ботами для автоматического перехвата одноразовых паролей), так и развития средств противодействия. Перспективным направлением является внедрение искусственного интеллекта для детектирования аномалий SMS-трафика в реальном времени у операторов — это позволит блокировать спам-атаки в их зародыше. Также возможна работа над международным регулированием спам-рассылок, ведь часто бомберы оперируют через зарубежные онлайн-сервисы. Что касается правовой базы, можно прогнозировать появление разъяснений Пленума Верховного Суда или новых поправок, которые дадут судам инструменты для квалификации действий SMS-бомберов (например, как создание помех в работе средств связи). В сфере кибербезопасности тема SMS-бомбинга уже включается в программы Security Awareness — обучающие курсы для сотрудников компаний по распознаванию и реагированию на подобные инциденты.

Таким образом, проблема SMS-бомберов — это вызов цифровой эпохи, требующий совместных усилий государства, бизнеса и пользователей. Только комбинация технических решений (фильтрации и защиты), законодательных мер и информированности общества позволит эффективно противостоять этому виду кибератак. Данная работа внесла вклад в исследование темы, систематизировав сведения о природе SMS-бомбинга и способах борьбы с ним. В дальнейшем более глубокого изучения заслуживают вопросы точного юридического определения SMS-атак и разработка специализированных средств их предотвращения, что и намечается в перспективах развития. ■

1. СМС-бомберы: спам как элемент кибератаки [Электронный ресурс] // SecurityMedia.org, 12.07.2022. – URL: https://securitymedia.org/info/sms-bombery-spam-kak-element-kiberataki.html (дата обращения: 27.03.2025).

2. Эксперты предупредили о новой схеме мошенничества с МФО и СМС-бомберами [Электронный ресурс] // РБК, 24.10.2021. – URL: https://www.rbc.ru/finances/24/10/2021/6172908a9a79472d4c8e56b9 (дата обращения: 27.03.2025).

3. Петров И. Конвейер с письмом: мошенники заваливают жертв спамом перед атакой [Электронный ресурс] // Известия, 30.08.2024. – URL: https://iz.ru/1750770/ivan-petrov/pismetco-v-konveiere-moshenniki-zavalivaiut-zhertv-spamom-pered-atakoi (дата обращения: 27.03.2025).

4. Курашева А. Банки и маркетплейсы столкнулись с трехкратным ростом частоты SMS-атак [Электронный ресурс] // Ведомости, 02.04.2023. – URL: https://www.vedomosti.ru/technology/articles/2023/04/03/969177-banki-i-marketpleisi-stolknulis-s-trehkratnim-rostom-chastoti-sms-atak (дата обращения: 27.03.2025).

5. Россиян предупредили о схеме мошенничества с SMS-бомберами [Электронный ресурс] // Аргументы и Факты, 30.08.2024. – URL: https://aif.ru/society/safety/chto-za-tehniku-sms-bombinga-ispolzuyut-moshenniki (дата обращения: 27.03.2025).

6. В России ввели штрафы за спам-звонки до 1 млн рублей [Электронный ресурс] // РБК, 06.04.2024. – URL: https://www.rbc.ru/society/06/04/2024/6611478a9a79470bb5f189d0 (дата обращения: 27.03.2025).

7. Федеральный закон от 06.04.2024 № 78-ФЗ «О внесении изменений в статьи 3.5 и 14.3 Кодекса Российской Федерации об административных правонарушениях» [Электронный ресурс] // Официальный интернет-портал правовой информации, 06.04.2024. – URL: http://publication.pravo.gov.ru/Document/View/0001202404060025 (дата обращения: 27.03.2025).

8. Что за технику SMS-бомбинга используют мошенники? [Электронный ресурс] // Аргументы и факты, 03.09.2024. – URL: https://aif.ru/society/safety/chto-za-tehniku-sms-bombinga-ispolzuyut-moshenniki#:~:text=%D0%96%D1%83%D1%80%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%BA%D0%B0%20%D0%B7%D0%B0%D0%B1%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BB%D0%B0%20%D1%81%D0%B2%D0%BE%D1%8E%20SIM,%D1%81%C2%A0%D0%BA%D0%BE%D0%B4%D0%B0%D0%BC%D0%B8%20%D0%B4%D0%BB%D1 (дата обращения: 27.03.2025).

9. Путин подписал закон о штрафах за спам-звонки [Электронный ресурс] // Известия, 06.04.2024. – URL: https://iz.ru/1678116/2024-04-06/putin-podpisal-zakon-o-shtrafakh-za-spam-zvonki#:~:text=%D1%88%D1%82%D1%80%D0%B0%D1%84%D0%B0%20%D0%BD%D0%B0%20%D0%B3%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%20%D0%B2%20%D1%80%D0%B0%D0%B7%D0%BC%D0%B5%D1%80%D0%B5,%D1%80%D1%83%D0%B1%D0%BB%D0%B5%D0%B9%C2%BB%2C%20%E2%80%94%20%D1%83%D0%BA%D0%B0%D0%B7%D0%B0%D0%BD (дата обращения: 27.03.2025).

10. С 6 апреля 2024 года изменяется размер штрафов за СМС-спам звонки [Электронный ресурс] // Targetsms, 06.04.2024. – URL:https://targetsms.ru/blog/1612-s-6-aprelya-2024-goda-izmenyaetsya-razmer-shtrafov-za-sms-spam#:~:text=%D1%80%D0%B5%D0%BA%D0%BB%D0%B0%D0%BC%D0%B5,%D1%82%D0%B5%D0%BF%D0%B5%D1%80%D1%8C%20%D0%B1%D1%83%D0%B4%D1%83%D1%82%20%D0%BF%D0%BB%D0%B0%D1%82%D0%B8%D1%82%D1%8C%20%D1%81%D1%83%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%20%D0%B1%D0%BE%D0%BB (дата обращения: 27.03.2025).

11. Госдума поддержала введение штрафов за спам-звонки [Электронный ресурс] // rg.ru, 06.04.2024. – URL: https://rg.ru/2024/03/19/gosduma-podderzhala-vvedenie-shtrafov-za-spam-zvonki.html (дата обращения: 27.03.2025).

12. Банки подвергаются атакам SMS-бомберов все чаще [Электронный ресурс] // Клерк, 06.04.2024. – URL: https://www.klerk.ru/buh/news/594553/

СПИСОК ЛИТЕРАТУРЫ:

Банки подвергаются атакам SMS-бомберов все чаще [Электронный ресурс] // Клерк, 06.04.2024. – URL: https://www.klerk.ru/buh/news/594553/

В России ввели штрафы за спам-звонки до 1 млн рублей [Электронный ресурс] // РБК, 06.04.2024. – URL: https://www.rbc.ru/society/06/04/2024/6611478a9a79470bb5f189d0 (дата обращения: 27.03.2025).

Госдума поддержала введение штрафов за спам-звонки [Электронный ресурс] // rg.ru, 06.04.2024. – URL: https://rg.ru/2024/03/19/gosduma-podderzhala-vvedenie-shtrafov-za-spam-zvonki.html (дата обращения: 27.03.2025).

Курашева А. Банки и маркетплейсы столкнулись с трехкратным ростом частоты SMS-атак [Электронный ресурс] // Ведомости, 02.04.2023. – URL: https://www.vedomosti.ru/technology/articles/2023/04/03/969177-banki-i-marketpleisi-stolknulis-s-trehkratnim-rostom-chastoti-sms-atak (дата обращения: 27.03.2025).

Петров И. Конвейер с письмом: мошенники заваливают жертв спамом перед атакой [Электронный ресурс] // Известия, 30.08.2024. – URL: https://iz.ru/1750770/ivan-petrov/pismetco-v-konveiere-moshenniki-zavalivaiut-zhertv-spamom-pered-atakoi (дата обращения: 27.03.2025).

Путин подписал закон о штрафах за спам-звонки [Электронный ресурс] // Известия, 06.04.2024. – URL: https://iz.ru/1678116/2024-04-06/putin-podpisal-zakon-o-shtrafakh-za-spam-zvonki#:~:text=%D1%88%D1%82%D1%80%D0%B0%D1%84%D0%B0%20%D0%BD%D0%B0%20%D0%B3%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%20%D0%B2%20%D1%80%D0%B0%D0%B7%D0%BC%D0%B5%D1%80%D0%B5,%D1%80%D1%83%D0%B1%D0%BB%D0%B5%D0%B9%C2%BB%2C%20%E2%80%94%20%D1%83%D0%BA%D0%B0%D0%B7%D0%B0%D0%BD (дата обращения: 27.03.2025).

Россиян предупредили о схеме мошенничества с SMS-бомберами [Электронный ресурс] // Аргументы и Факты, 30.08.2024. – URL: https://aif.ru/society/safety/chto-za-tehniku-sms-bombinga-ispolzuyut-moshenniki (дата обращения: 27.03.2025).

С 6 апреля 2024 года изменяется размер штрафов за СМС-спам звонки [Электронный ресурс] // Targetsms, 06.04.2024. – URL:https://targetsms.ru/blog/1612-s-6-aprelya-2024-goda-izmenyaetsya-razmer-shtrafov-za-sms-spam#:~:text=%D1%80%D0%B5%D0%BA%D0%BB%D0%B0%D0%BC%D0%B5,%D1%82%D0%B5%D0%BF%D0%B5%D1%80%D1%8C%20%D0%B1%D1%83%D0%B4%D1%83%D1%82%20%D0%BF%D0%BB%D0%B0%D1%82%D0%B8%D1%82%D1%8C%20%D1%81%D1%83%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%20%D0%B1%D0%BE%D0%BB (дата обращения: 27.03.2025).

СМС-бомберы: спам как элемент кибератаки [Электронный ресурс] // SecurityMedia.org, 12.07.2022. – URL: https://securitymedia.org/info/sms-bombery-spam-kak-element-kiberataki.html (дата обращения: 27.03.2025).

Федеральный закон от 06.04.2024 № 78-ФЗ «О внесении изменений в статьи 3.5 и 14.3 Кодекса Российской Федерации об административных правонарушениях» [Электронный ресурс] // Официальный интернет-портал правовой информации, 06.04.2024. – URL: http://publication.pravo.gov.ru/Document/View/0001202404060025 (дата обращения: 27.03.2025).

Что за технику SMS-бомбинга используют мошенники? [Электронный ресурс] // Аргументы и факты, 03.09.2024. – URL: https://aif.ru/society/safety/chto-za-tehniku-sms-bombinga-ispolzuyut-moshenniki#:~:text=%D0%96%D1%83%D1%80%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%BA%D0%B0%20%D0%B7%D0%B0%D0%B1%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BB%D0%B0%20%D1%81%D0%B2%D0%BE%D1%8E%20SIM,%D1%81%C2%A0%D0%BA%D0%BE%D0%B4%D0%B0%D0%BC%D0%B8%20%D0%B4%D0%BB%D1 (дата обращения: 27.03.2025).

Эксперты предупредили о новой схеме мошенничества с МФО и СМС-бомберами [Электронный ресурс] // РБК, 24.10.2021. – URL: https://www.rbc.ru/finances/24/10/2021/6172908a9a79472d4c8e56b9 (дата обращения: 27.03.2025).

SMS-bombers: what are they and how are they used?

© **Ovechkin R., Iudalevich N., 2025**

This paper examines the phenomenon of SMS bombers — software and services designed for mass sending of SMS messages to a single target number. A historical overview of the emergence of SMS bombing and the evolution of its usage is provided. The technical features of SMS bombers are analyzed, including their operating principles, existing types (legal marketing versus illicit malicious versions), distribution platforms (scripts, web services, bots, and apps), and countermeasures by telecommunications operators. Special attention is paid to the use of SMS bombing in fraudulent schemes: examples of phishing attacks, social engineering, extortion, as well as methods of verifying stolen data relevance via SMS flooding are described. Possible forms of damage from the use of SMS bombers are discussed – financial (direct monetary losses, companies' messaging costs), emotional (stress and panic of victims), reputational (erosion of trust in communication channels), and technical (infrastructure overload, service outages). The current legislative regulation of this phenomenon in the Russian Federation is analyzed: norms of administrative liability for spam distribution are presented, and the challenges of qualifying SMS bombing as a criminal offense are discussed. Finally, recommendations for

protection against SMS bombing are offered for users (including self-protection methods) and for telecom operators (technical and organizational measures). The paper concludes with outcomes of the study and outlines prospects for developing countermeasures against SMS bombing.

Keywords: SMS bomber; SMS bombing; spam attack; phishing; social engineering; mobile security; cyber fraud; cybersecurity