

Научная статья  
УДК 32.019.57+ 32.019.51+316.4  
EDN WKLQSO



## Социально-политические проблемы мессенджера «Телеграм» и перспективы для государственного мессенджера «Макс»

Илья Игоревич Рогов<sup>1</sup>, Юлия Валентиновна Логинова<sup>2</sup>

<sup>1,2</sup>Финансовый университет при Правительстве Российской Федерации, Москва, Россия

<sup>1</sup>IRogov@fa.ru, SPIN-код: 7273-3953, <https://orcid.org/0009-0003-6181-5692>

<sup>2</sup>jul.cool@mail.ru, SPIN-код: 2212-5449, <https://orcid.org/0000-0002-8854-5886>

### Аннотация

**Введение.** В статье рассматриваются проблемы, которые коснулись мессенджера «Телеграм». После начала специальной военной операции, ухода и блокировки зарубежных мессенджеров, «Телеграм» испытал скачкообразный рост: подписчики, трафик, монетизация. Однако Федеральный закон №41-ФЗ от 1 июня 2025 г. внес существенные изменения в привычную коммуникацию. Были изменены и ужесточены условия выдачи наличных через банкоматы, Госуслуги получили функцию самозапрета на оформление сим-карт и введен запрет на передачу сим-карт, микротранзакции с обязательной биометрией клиента и т.д. В частности, деловая переписка, которую госслужащие вели через WhatsApp\* и Телеграм, была запрещена. На практике сказанное означает, что ФЗ-41 ограничил возможности мессенджера. Проблемы у платформы возникли после неоднократных обращений государственных органов к владельцам и администрации мессенджера удалить или ограничить доступ к контенту, нарушающего законодательство РФ.

**Цель.** На основе анализа проблем мессенджера «Телеграм» разработать рекомендации для госмессенджера «Макс».

**Материалы и методы.** Методологическую основу исследования составили концептуальный анализ и дискурс-анализ. Чтобы определить актуальность проблем мессенджера «Телеграм», были проанализированы научные статистические исследования зарубежных авторов, посвященные двум проблемам: кибермошенничество и публикация недостоверной информации. Проанализированные исследования опубликованы в зарубежных научных изданиях в 2025 г., старт исследований – не позднее 2021 г. В фокусе анализа киберпреступности группы Чикагского университета такие темы, как: кража учетных данных пользователей, пиратское ПО, темные медиа, ресурсы управления соцсетями без согласия пользователей, хакерское ПО. Анализ недостоверного контента был проведен группой университета Сапиенца в Риме по оценке монетизации «теорий заговора» QAnon и COVID-19.

**Результаты.** Анализ цепочек репостов и информационных потоков привел зарубежных исследователей к определенным выводам. В данной статье проводится дискутирование с этими итогами. Анализ киберпреступности проведен по каналам открытого профиля, что фактически является анализом лояльности пользователей к контенту, но не активности пользователей в сегменте. Анализ недостоверного контента проведен только по «теориям заговора», что не позволяет охватить все форматы недостоверности. Во второй части статьи проанализированы статистические данные по русскоязычным каналам в Телеграм и Макс, которые формируют новостную повестку или пытаются управлять ею. Анализ проведен на основе данных TG Stat, Maxstat.

**Выводы.** Политическая повестка не является востребованным лидером по медиапотреблению. Рядовых пользователей привлекают темы, напрямую не связанные с политическими проблемами. Высокий уровень вовлечения вызывают привлекательно оформленный дизайн мессенджера. Отсюда и рекомендации для госмессенджера «Макс»: сконцентрироваться на темах и контенте, востребованном в обществе, работать над интерфейсом (UX/UI дизайн).

**Ключевые слова:** мессенджер, госмессенджер, «Телеграм», «Макс», киберпреступность, недостоверный контент, «темные медиа», «теории заговора», UX/UI дизайн

**Для цитирования:** Рогов И. И., Логинова Ю. В. Социально-политические проблемы мессенджера «Телеграм» и перспективы для государственного мессенджера «Макс» // Государственное и муниципальное управление. Ученые записки. 2026. № 2. С. 166–175. EDN WKLQSO

Original article

## Problems with Telegram messenger and prospects for the state messenger MAX

Ilya I. Rogov<sup>1</sup>, Julia V. Loginova<sup>2</sup>

<sup>1,2</sup>Financial University under the Government of the Russian Federation, Moscow, Russia

<sup>1</sup>IRogov@fa.ru, SPIN-код: 7273-3953, <https://orcid.org/0009-0003-6181-5692>

<sup>2</sup>jul.cool@mail.ru, SPIN-код: 2212-5449, <https://orcid.org/0000-0002-8854-5886>

### Abstract.

**Introduction.** This article examines the problems affecting the Telegram messenger. Following the start of Special military operation of Russia and the demise and blocking of foreign messengers, Telegram experienced rapid growth in subscribers, traffic, and monetization. However, Federal Law No. 41-FZ of June 1, 2025, limited the messenger's capabilities. The platform's problems arose after repeated requests from government agencies to the messenger's owners and administration to remove or restrict access to content that violated Russian law.

**Purpose.** To determine the relevance of the Telegram messenger's problems, the author analyzed scientific statistical studies by foreign authors on two issues: cyberfraud and the publication of false information. The analyzed studies were published in foreign scientific journals in 2025, with further research to begin no later than 2021. The University of Chicago's cybercrime analysis focuses on topics such as credential theft, pirated software, dark media, social media management resources without user consent, and hacking software. An analysis of inaccurate content was conducted by a team from Sapienza University in Rome to assess the monetization of QAnon and COVID-19 conspiracy theories.

**Materials and methods.** The methodological basis of the research was conceptual analysis and discourse analysis. To determine the relevance of the problems of the Telegram messenger, scientific statistical studies by foreign authors devoted to two problems were analyzed: cyberbullying and the publication of false information. The analyzed studies will be published in foreign scientific publications in 2025, and the start of research will be no later than 2021. The cybercrime analysis by the University of Chicago group focuses on such topics as: theft of user credentials, pirated software, dark media, social media management resources without user consent, and hacker software. The analysis of the unreliable content was carried out by the Sapienza University of Rome group to assess the monetization of the "conspiracy theories" QAnon and COVID-19.

**Results.** An analysis of repost chains and information flows led international researchers to certain conclusions. The author of the article discusses these findings. The cybercrime analysis was conducted on open profile channels, which effectively analyzes user loyalty to content, not user activity within the segment. The analysis of inaccurate content was conducted only for conspiracy theories, which does not cover all forms of inaccuracy. The second part of the article analyzes statistical data from Russian-language channels that shape the news agenda or attempt to control it. The analysis is based on official TG Stat and maxstat results.

**Conclusions.** The political agenda is not a sought-after leader in media consumption. Ordinary users are attracted to topics that are not directly related to political issues. The attractive design of the messenger causes a high level of engagement. Hence the recommendations for the state messenger "Max": focus on topics and content that are in demand in society, work on the interface (UX/UI design).

**Keywords:** messenger, state messenger, Telegram, MAX, cybercrime, inaccurate content, dark media, conspiracy theories, TG Stat, UX/UI design

**For citation:** Rogov I.I., Loginova Ju.V. Problems with Telegram messenger and prospects for the state messenger MAX. *State and Municipal Management. Scholar Notes.* 2026;(2):166–175. (In Russ.). EDN WKLQSO

## Введение

После начала специальной военной операции глобальные мессенджеры ушли из Российской Федерации или были заблокированы по решению властей. На фоне образовавшейся ниши в медиа-рынке произошел рост платформы «Телеграм», что было связано как с личностью основателя (Павел Дуров из России), так и с высокой узнаваемостью нейминга: «Телеграм» переключался с широко распространенными русскими словами, как «телеграмма», «телеграф». У Telegram произошел резкий скачок популярности, трафика, платформа заняла значительный сегмент рынка.

За краткий период после начала СВО «Телеграм» стал флагманской платформой для обсуждения политических проблем. На эту тему уже были проведены научные исследования, которые показали довольно противоречивые результаты: от глобальной поддержки [1, с. 247] до максимально непредсказуемых оценок, когда Телеграм-каналы стали пространством политической борьбы, согласования решений и экспертной рефлексии [2, с. 123].

Однако все Интернет-платформы, особенно мессенджеры находятся под прямым или косвенным контролем властей или сотрудничают со спецслужбами – или напрямую, или через корпорации, которые ими управляют. Мир облетели сводки, что ряд иранских высокопоставленных деятелей были убиты во время 12-дневной войны (13–24 июня 2025 г.), поскольку за ними следили через WhatsApp<sup>1</sup>. Даже если предположить, что журналисты гонятся за сенсациями, сам факт настораживает и заставляет принять меры.

Согласно исследованию, которое проводилось в 2024 году, когда аудитория «Телеграм» составляла 800 млн. активных пользователей и которое основано на данных TG Stat, в России «Телеграм» используют 45,8 % населения. Наиболее востребованным являются новостной контент – 85 %, развлекательный – 62 % и образовательный – 58%. [3, с. 37] Средний пользователь подписан от 25 до 50 каналов.

Рост трафика «Телеграм» вызвал пропорциональный рост активности пользователей, что вызвало повышенный интерес к владельцу «Телеграм», Павлу Дурову. Так, во Франции предпринимателя задержали, и, хотя президент Макрон отрицал политические мотивы, его слова не вызвали доверия<sup>2</sup>. Власть и правоохранительные органы Российской Федерации пошли по иному пути: замедлению подвергся сам мессенджер. Одновременно на рынок выведен госмессенджер MAX. Хотя отдельные представители власти опровергают блокировку «Телеграм»,<sup>3</sup> очевидно, что платформа потеряет существенную часть рынка.

Замедление «Телеграм» вызвало недовольство в обществе. В связи со сказанным уместно проанализировать восприятие «Телеграм» в западных странах. Поскольку информация в медиа нуждается в перепроверке и не всегда может быть верифицируема, исследование сконцентрировано на анализе научных зарубежных исследований, в фокусе которых находится именно «Телеграм». В фокус анализа попали научные работы, выпущенные после 2022 г. Гипотеза: анализ научной периодики, как взвешенной оценки мессенджера, позволит выявить общие проблемы и общие ожидания от мессенджера – как в русскоязычном, так и в англоязычном секторах, а также сформулировать направления развития для госмессенджера MAX.

<sup>1</sup> Израильская разведка отследила Ханию через WhatsApp\*. Журналист Манье: разведка Израиля отследила Ханию через WhatsApp\*. URL: <https://lenta.ru/news/2024/08/01/izrajskaya-razvedka-otsledila-haniyu-cherez-whatsapp/> (дата обращения – 05.03.2026) (\*Принадлежит Meta Platforms Inc. – организация признана в РФ экстремистской, ее деятельность запрещена на территории РФ)

<sup>2</sup> Reuters: Дурова обвинили в отказе сотрудничать с властями Франции. URL: <https://vz.ru/news/2024/8/26/1284001.html> (дата обращения – 05.03.2026)

<sup>3</sup> В Госдуме ответили на вопрос о возможной блокировке Telegram. Горелкин: запуск национального сервиса не приведет к блокировке Telegram. URL: <https://ria.ru/20250605/telegram-2021097196.html> (дата обращения – 05.03.2026)

### Материалы и методы

Запрос по поисковому слову «Телеграм» выдает 13856 результатов по поиску E-Library и 1842 результата в категории «ВАК» по поиску «Киберленинки». Однако большая часть статей носит описательный характер. Статей, публикующих статистические итоги, мало. Авторами была поставлена цель – найти зарубежные научные материалы на тему статистических исследований мессенджера «Телеграм». Анализ проведен на основе данных TG Stat, Maxstat. Исползованные методы: концептуальный анализ, логико-аргументативный анализ (причинно-следственные основы и подмены), компаративный (сравнительный) и дискурс-анализ.

### Анализ киберпреступности на платформе «Телеграм»

С более чем 1 млрд активных пользователей в месяц в 2026 г. и слабой модерацией контента Telegram стал привлекательной платформой для различных киберпреступлений [4]. Преимущества для людей, желающих заняться киберпреступностью, заключаются в следующих особенностях Telegram:

- низкий порог входа в платформу: регистрация быстрая и доступная, без проверки личности;
- нетребовательность к индивидуальным навыкам для пользователя. Если работа в сетях Даркнета требует высоких индивидуальных навыков в обходе форм государственного контроля и контроля от корпораций, умения пользоваться специализированным ПО, контактирование с «Телеграм» – обычный клик по экрану смартфона;
- простые инструменты (например, чат-боты) позволяют создавать и распространять контент любого рода, просто заимствуя готовый из сети Интернет или файлообменников и переносить его на площадку без ущерба для владельца канала (сообщества).

В исследовании «DarkGram: Анализ каналов киберпреступной активности крупного масштаба на Telegram», исследовательская группа – Сайяк Саха Рой, Эльхам Пураббас Вафа, Кобра Ханмохаммади и Ширин Нилизаде проанализировали 339 англоязычных каналов Telegram, совокупно содержащих 23,8 млн подписчиков (с нижним порогом в 10 тыс. подписчиков) и касающихся кибердеятельности, в т.ч. – и киберпреступлений [4, с. 2]. Исследование было проведено в августе 2025 г. Анализ проводился по пяти направлениям: кража учетных данных пользователей; пиратское ПО; темные медиа; ресурсы управления соцсетями без согласия пользователей; хакерское ПО.

Было проанализировано 53 605 постов; внимание было уделено как контенту, который распространяют владельцы данных каналов, так и их взаимодействию с пользователями.

Анализ показал, что 28,1 % постов приводят к фишинговым URL, 38 % постов содержат вредоносное и шпионское ПО. Несмотря на это, 70–80 % эмодзи-реакций на посты оказались положительными, что свидетельствует как о том, что подписчики не осознают глубину проблемы, так и о том, что подписчики равнодушны к возможности заражения собственного компьютера вирусным содержанием. Статистические результаты приведены в табл. 1.

**Таблица 1 – Описательная статистика каналов киберпреступной активности по данным исследований Техасского университета<sup>1</sup>**

Table 1 – Descriptive statistics of cybercrime channels based on research data from the University of Texas

Категория	Посты		Подписчики		Категория		Пересылки	
	Мин./Макс.	Медиана /Среднее	Мин./Макс.	Медиана /Среднее	Мин./Макс.	Медиана /Среднее	Мин./Макс.	Медиана /Среднее
Кража учетных данных (69)	1/3159	102 /520	10 215 /604 772	28 500 /47 132,25	1 /19 300	23/65,99	0/483	0/0,39
Пиратское ПО (124)	1/841	63,5 /95,16	11 030 /741 259	31 200 /52 415,89	1 /93 627	397 /3138,78	0/504	1/6,58
Ресурсы Даркнет (42)	3/290	35,5 /60,5	10 481 /253 507	18 450 /29 763,11	1 /44 573	259 /1079,25	0/597	1/7,75
Темные медиа (36)	2/400	25/56,64	15,902 /387,599	60,000 /102,347,89	1 /796,961	24,395.5 /47,027,21	0/2569	14/89,03
Манипуляция соцсетями (68)	1/1227	8/49,15	10,319 /123,09	720,750 /28,321	441 /40,757	326,5 /753,78	0/117	0/5,01

<sup>1</sup> Таблица составлена на основе данных DarkGram: A Large-Scale Analysis of Cybercriminal Activity Channels on Telegram Sayak Saha Roy and Elham Pourabbas Vafa. The University of Texas at Arlington; Kobra Khanmohamaddi, Sheridan College; Shirin Nilizadeh. The University of Texas at Arlington arXiv preprint. August 13–15, 2025. URL: <https://www.usenix.org/system/files/usenixsecurity25-roy.pdf> (дата обращения – 05.03.2026). P. 4842.

Исследователи обнаружили, что посты, которые были использованы для сбора и утечки данных, в подавляющем большинстве случаев (93 %) вели через чат-бота к стороннему приложению, которое запускалось с согласия пользователя и затем скрыто занималось фишингом. В качестве аргумента использовался текстовый анализ и визуальный. До 29 % постов использовали слово «proof / proofs» (доверие) и 85 % постов содержали скрины успешной регистрации. Из этого был сделан вывод, что пользователи «не осознают» глубину проблемы.

С подобным утверждением можно не согласиться. Анализу подверглись открытые каналы, специализирующиеся на кибердеятельности: рабочая группа и не скрывала, что они анализируют открытый сегмент «Телеграм». В закрытые группы и сообщества исследователи не заходили и приглашений не получали. Следовательно, и прочие пользователи, которые подвергались фишингу, знали, что подписались на открытый канал, которые специализируется на киберпреступности. Вовлекающие слова («доверие»), как и скрины, выполняли функцию лид-магнитов и триггеров, однако известно, что если пользователь изначально не нацелен совершить покупку, то эффективность этих маркетинговых инструментов низкая. В таком случае можно сделать вывод, что пользователи все прекрасно осознавали. Дело, таким образом, в другом.

При анализе темных медиа и пиратского контента статистика показала следующее. В 34,6% публикаций файл был прикреплен в виде вложения, а 43,1% переводили пользователя на внешние сайты [4, с. 4840] Из этого был сделан вывод о вредоносности Telegram как платформы.

Данное утверждение также вызывает серьезные сомнения. На практике «темные медиа» и «пиратский контент» означали распространение сериалов и медиафайлов, недоступных в данной стране (например, в США недоступен ряд аниме-сериалов, распространяемых по подписке в азиатских странах). В борьбе за рынок корпорации поглощают более мелкие фирмы, устраняют конкурентов и обвиняют конкурентов в нарушении законодательства. Однако из объема проанализированных данных, порнографической продукции не было выявлено, что объясняется спецификой просмотренных каналов: каналы открытого профиля. Данная же продукция распространяется в основном в закрытом сегменте «Телеграм». Цифра в 43,1 % постов, которые переводят пользователя на внешний ресурс, свидетельствует лишь о том, что «Телеграм» используется как рекламная площадка данного внешнего ресурса (без гарантии, что представляет из себя сам ресурс). Таким образом, под «темными медиа» на практике имеется ввиду «распространение пиратского контента».

Оставляя в стороне вопросы авторского права и этичность распространения пиратского контента, отметим, что именно этот вид контента привлек до 80 % пользователей из проанализированных 339 каналов на 23,8 млн подписчиков. Анализ вовлеченности, лайков и реакций показал, что пользователи, целенаправленно ищущие вредоносное и пиратское ПО, в подавляющем проценте осторожны и не оставляют цифровых следов. Аналогична связь между количеством пересылок и ростом числа подписчиков. Рост пересылок ведет к росту числа подписчиков. Пересылки более 100 единиц в неделю приводят к росту до 27,4 %, но весь трафик сконцентрирован на развлекательном (хотя и пиратском) контенте.

Итак, анализ киберпреступности проведен по каналам открытого профиля, что фактически является анализом лояльности пользователей к контенту, но не активности пользователей в сегменте.

Цифры и данные, приведенные выше, позволяют сделать вывод, что основная масса пользователей, которая потребляет запрещенный контент в «Телеграм», находится в «умеренно-серой» зоне. Возможно, пиратское медиа – проблема для корпораций, но точно не проблема безопасности.

#### **Анализ недостоверного контента в Telegram**

Недостоверный контент, как-то – фейковая информация, откровенно ложная информация и т.п., был проанализирован в исследовании «Заговор денежной машины: раскрытие схемы конспирологических каналов Telegram и их модель получения прибыли» [5, с. 5229–5246]. Авторы – Винченцо Императи, Массимо Ла Морджиа, Алессандро Мей, Альберто Мария Монгардини и Франческо Сасси из Института Сапиенца (Рим) – проанализировали контент в жанре «теории заговора», касающийся таких востребованных тем, как «высадка на Луну», «убийство Кеннеди», «отрицание Холокоста», «фальсификация смерти Элвиса Пресли» и разнообразные теории заговора «11 сентября».

Хочется отметить, что авторы данной статьи согласны с глобальными выводами: теориями заговора общество реагирует на сложную и трудно верифицируемую информацию. Также теории заговора содержат антиистеблишментский контент (идеи, литературу и проч.). Telegram (с его слабой модерацией контента) представляет благодатную платформу не только для распространения подобного контента, но и для его монетизации.

Данной рабочей группой были проанализированы 120 тыс. Телеграм-каналов с нижним порогом в 5 тыс. подписчиков. Первый вывод: анализ германоязычных и англоязычных каналов (120 тыс.) показал, что 17 % прямо или косвенно связаны с «теориями заговора» или постят подобный контент. Эта тревожная новость, указывающая на антиистеблишментскую направленность пользователей. Второй и главный вывод, который сделала рабочая группа – Telegram-каналы «теории заговора» нацелены на монетизацию. Так, по замерам, более 900 тыс. уникальных пользователей прошли все этапы «карты пути клиента» (CJM), т.е. совершили клик по чат-боту с последующей покупкой услуг или пожертвованием. Наибольшей востребованностью пользовались: теория заговора QAnon и COVID-19. Замер, который провели исследователи, показал, что медиаконтент использовался для краундфандинга и сбора пожертвований. Отдельно стоит вопрос, насколько вся эта деятельность подпадает под определение «мошенничества» в разных странах, но, поскольку контент в «Телеграм» проходит со слабой верификацией, деятельность подобного рода приносит не только высокие охваты, но и прибыль.

Отметим и более высокую покупательную способность контента типа QAnon и COVID-19. В отличие от более распространенных теорий заговора, как «отрицание Холокоста» и «11 сентября», контент, в которых только повышаются охваты и реакции, эти теории заговора способствовали монетизации. Пожертвования на данный контент свидетельствуют об имеющемся в обществе неудовлетворении властью, деятельностью государственных органов и т.д. Как отмечают исследователи, «crowdfunding projects sponsored by conspiracy channels collected millions of dollars donated» (продвигаемые каналами теории заговора собрали миллионы долларов пожертвований – перевод авторов): 906 тыс. спонсоров пожертвовали, в общей сложности, 91 млн долл. [5, с. 5230].

В чем суть теорий заговора QAnon и COVID-19? QAnon – преступная клика высшего истеблишмента реализует античеловеческие социальные проекты; COVID-19 – вакцинация на самом деле является биологическим оружием. Фактически, одна является продолжением другой. Люди, которые спонсируют (донатят) подобному контенту, выражают таким образом протест против официальной информации, распространяемой властями. По мнению авторов, нивелируются «теории заговора» публичным и открытым обсуждением наболевших проблем. Практика наблюдений за поведением адептов «теорий заговора» в публичном пространстве свидетельствует, что у них отсутствуют аргументы, кроме их собственных домыслов. Будучи вынесены на публичное обсуждение, эти аргументы не выдерживают критики. Когда же они преподнесены как запрещенный контент (Даркнет, «темные медиа»), «теории заговора» создают эффект инклюзивности и информационного дефицита.

Динамика роста-спада каналов «теории заговора» укладывается в параболическую функцию: появление в январе (месяц взят для примера), быстрый набор подписчиков к маю, пик май-июнь с постепенным спадом и охлаждением аудитории. Причины этого понятны: появление нового контента «теории заговора» включает вау-эффект, эффект вброса, сенсационности и сообщество, ожидающее подобной информации, быстро реагирует. Если правильно высчитать сумму доната – так, чтобы он был необременителен для пользователя в обмен на «закрытую информацию», то перспектива собрать значительные суммы пожертвований возрастает. Поскольку же теоретики заговора не располагают реальными данными и доказательствами, покупка приватной информации разочаровывает пользователя, и тот отписывается. Эксплуатация подписчиков для финансовой выгоды никогда не приносила длительных связей или стабильного дохода, но, поскольку каналы «теории заговора» создаются для быстрой монетизации, после массовых отписок владельцы поддерживают такой канал в «полумертвом состоянии», публикуя вторичный и не очень вовлекающий контент.

Дальше группа итальянских исследователей выявила «fake charity campaigns that are outright scams» («фальшивые благотворительные компании, которые являются откровенным мошенничеством» – перевод авторов) [5, с. 5231]. Это позволяет сделать вывод об общих проблемах как русскоязычного, так и англоязычного сектора Telegram: известно, что после начала СВО появились фейковые Telegram-каналы военкоров, мошеннические Telegram-каналы, занимающиеся «сбором пожертвований» и т.д.

Анализ монетизации показал, что стратегия пожертвований приносит больше дохода нежели краудфандинг или партнерские программы. Это обусловлено как техническими, так и социальными факторами. На практике «стратегия пожертвований» – это кнопка доната в канале. Ее можно настроить, обладая аудиторией всего в 100 подписчиков. Визуально кнопка помещается под постом. Если пост выполняет функцию лид-магнита, то вероятность вовлечения повышается. Этот факт был отмечен еще в первом, рассмотренном нами исследовании (слова типа «proof/proofs» (доверие)

и посты с вовлекающими скринами). Соответственно, подписчики жертвуют селебрити (лидеру мнений), на которого подписаны. Краудфандинг – это коллективный сбор заинтересованных людей, группы поддержки. На практике краудфандинг, как правило, реализован на конкретные цели. Такая инициатива может вызвать энтузиазм (что, например, было заметно в российском кластере в первые два года СВО), но требует конкретного осязаемого результата (и собиратели пожертвований отчитывались в обмундировании и иных закупленных вещах). Но «теории заговора» – контент совершенно иного рода. Они не могут быть монетизируемы через инициативный, ограниченный во времени, сбор пожертвований.

Социальная причина состоит в привычке рядового человека и нормах социума к активностям такого рода. Анализ Телеграм-каналов английского сектора (Канада, США) показал высокие проценты сбора пожертвований, как например, «Конвой свободы – 2022»: акция водителей-дальнобойщиков против введения вакцинных паспортов. Добровольное финансирование подобных общественных движений является частью северо-американской политической культуры. В большинстве обществ Старого Света это не так. Наоборот, «стратегия пожертвований» – простой, финансово-необременительный донат, кнопка которого прикреплена сразу под влогом (видеопостом) на практике превращается в функцию лояльности, личной поддержки.

Итак, анализ недостоверного контента проведен итальянскими исследователями только по «теориям заговора», что не позволяет охватить все форматы недостоверности. Фактически был проведен анализ антиистеблишментских симпатий среднего человека, который пользуется мессенджером «Телеграм». Общая же категория «недостоверного контента» охватывает широкий спектр тем и каналов. С точки зрения авторов статьи, анализировать статистику этого контента необходимо начинать с каналов новостного формата (так называемых «новостников»). «Теории заговора» являются контентом не широкого, но узкого профиля, что не позволяет адекватно оценить заявленную тему.

#### **Анализ текущей ситуации мессенджера MAX.**

По данным аналитики, пять наиболее популярных категорий в мессенджере MAX (по состоянию на 20.04.2026): новости и СМИ, познавательное, образование, семья и дети, бизнес. Политика занимает седьмое место. По количеству подписчиков самые популярные: MAX • Анонсы, Кремль.Новости, Мир сегодня с Юрием Подолякой, РИА Новости, Standoff 2, Mash, Прямой Эфир • Новости, СОЛОВЬЕВ, Central TikTok, TikTok Prime<sup>1</sup>, из них 4 канала с политической направленностью. Brand Analytics в рейтинге Топ-100 каналов российского мессенджера MAX по уровню вовлеченности аудитории наиболее популярные каналы СОЛОВЬЕВ, РИА НОВОСТИ, Мир сегодня с Юрием Подолякой, RT на русском, КРЕМЛЬ новости, ВЕСТИ, Царьград, Операция Z: военкоры русской весны, ТАСС, Мир Михаила Онуфриенко<sup>2</sup>. Можно наблюдать, что есть пересечения по ряду каналов. По большей части наиболее популярные по количеству подписчиков и уровню вовлеченности каналы входят в категорию «новости и СМИ».

Мессенджер Max имеет существенные отличия от других мессенджеров: интеграция с госуслугами, подписание документов, потенциальная интеграция с СБП, включен в белый список и минимизированы проблемы коммуникаций, отечественное ПО. Однако есть и ряд недостатков, таких как недоверие пользователей из-за недостаточной осведомленности населения о возможностях мессенджера, создания искусственной потребности в регистрации, новизна продукта и блокировка зарубежных мессенджеров [7, с. 155–157].

Несмотря на активную популяризацию мессенджера и его позиционирование, наличие ряда существенных преимуществ, продукт находится в активной фазе роста, но еще отсутствуют некоторые функции и рекламные инструменты. Что тоже необходимо учитывать при использовании данного мессенджера в продвижении и социально-политическом контексте. Однако повышается стоимость привлечения контакта и к середине года ожидается появление рекламного кабинета<sup>3</sup>.

<sup>1</sup> Аналитика MAX-каналов: каналы, публикации, тренды и реклама. URL: <https://maxstat.ru/catalog> (дата обращения – 20.04.2026).

<sup>2</sup> Brand Analytics представляет Топ-100 каналов в российском мессенджере MAX по итогам 4 квартала 2025 года URL: <https://brandanalytics.ru/blog/top-100-popular-channels-max> (дата обращения – 20.04.2026)

<sup>3</sup> Рекламный рынок MAX в 2026 году: цены, инструменты, прогнозы URL: <https://www.sostav.ru/blogs/288427/82781> (дата обращения – 20.04.2026)

### Выводы. Перспективы для МАХ

Итак, общий обзор проанализированных исследований зарубежных ученых демонстрирует, что подписчики, которые становятся пользователями каналов, распространяющих хакерский контент и «теории заговора», реагируют только на личную, индивидуальную полезность. Этим объясняется как осознанность подписки на каналы, распространяющие незаконное ПО, так и на каналы, которые собирают пожертвования на протестную деятельность. Однако это не доказывает преступность самой платформы.

Следует сказать и несколько слов в защиту «Телеграм». Единственный вывод, который можно сделать из сказанного – «Телеграм» стал площадкой распространения альтернативных мнений, альтернативного медиапространства. Это обусловлено скоростью распространения информации, простотой в подписке и регистрации, простотой в монетизации. Но этими же особенностями обладает любой мессенджер.

Алгоритмические платформы – в Российской Федерации – это VK Музыка, VK Клипы, за рубежом – известные, но запрещенные в России мессенджеры, предоставляют контент, основываясь на уже просмотренном пользователем. В зарубежных научных журналах периодически публикуются новые и новые исследования, типа «способствует ли радикализации алгоритм рекомендаций Ютуб и направляет ли он пользователей ко все более экстремистскому контенту?» Подписочные платформы, как «Телеграм» и госмессенджер МАХ, работают по иной схеме: поиск ведется по конкретным поисковым словам. Чтобы подписаться на канал пиратского контента, канал «теорий заговора» и канал Даркнета («темных медиа»), пользователь должен знать точное название этого канала. Это означает, что подписочные каналы в большей степени зависят от социальных контактов, нежели алгоритмические. В этом сегменте средний пользователь больше защищен от фишинга и вредоносных действий.

В начале статьи публиковалась разбивка по контенту, который предпочитают пользователи. Хотя замер делался в 2024 г. (после начала СВО), обращает на себя внимание низкий уровень интереса к политическим новостям: 85 % новостного, самого востребованного контента, не включают только политический контент, но находятся в широком спектре «Новости и СМИ».

По данным TG Stat на 05 марта 2026 г., лидер при замере по количеству подписчиков, «ОКХ Новости» с 5 754 557 подписчиков находится в разделе «криптовалюты»<sup>1</sup>. Первый канал, помеченный категорией «политика» – Дмитрий Медведев с 1 783 669 подписчиками – занимает только 46 место. Канал Медведева – единственный политический в топ-50. Высокий показатель у политических каналов в категориях «охват» и «цитируемость». Здесь канал Дмитрия Медведева на третьем месте с охватом одного поста в 2,2 млн., плюс в списке первых 50 каналов всего три канала с тегом «политика»: Вячеслав Володин с 1 374 542 подписчиками, «ТАКТИКАРЬ» с 6 777 подписчиками и «Саня во Флориде» с 965 242 подписчиками. По цитируемости топ-10 занимают каналы крупных новостных агентств, т.е. каналы, существующие не как самостоятельный элемент коммуникации, но структурная часть крупного медиахолдинга. Первый политический канал в топ-50 по цитируемости – «ЕЖ» со всего 598 082 подписчиками – занимает только 16 (шестнадцатую) позицию. На 18 (восемнадцатой) позиции – Минобороны России с 613 079 подписчиками. Всего в топ-50 по цитируемости – 13 (тринадцать) каналов<sup>2</sup>.

Возможно отметить, что все каналы категории «Новости и СМИ» содержат политические новости как флагманский тренд. Но возможно возразить и подчеркнуть то, что каналы Медведева, Володина, «Саня во Флориде», помеченные как «политические», с тем же успехом могут быть отнесены к блогосфере. Главное же то, что «цитируемость» обеспечивается перекрестной цитируемостью, когда одна новость многократно проходит по медиополю, и каждый крупный участник медиапространства обязан цитировать эту новость, чтобы быть в трендах. Разрыв же между категорией «охваты» и «количество подписчиков» наводит на мысль, что люди активно реагируют на блогосферу, на селебрити. Если убрать блогосферу как категорию, то все политические активности сведутся лишь к реакциям на новости от крупных медиахолдингов.

При сравнении данных TG Stat ру-кластера с англо- и германоязычным кластером «Телеграм», приходим к выводу, что львиная доля подписчиков «Телеграм» не имеет отношения к политике или не интересуется ею. Отсюда – все исследования про киберпреступность и недостоверный контент повисают в воздухе.

<sup>1</sup> Рейтинг Telegram-каналов. TGStat. URL: <https://tgstat.ru/> (дата обращения – 05.03.2026)

<sup>2</sup> Там же.

Личная позиция одного из авторов сформировалась на основе следующего опыта. Автор статьи на протяжении трех лет ведет курсы по SMM (СММ) и созданию контента. Студенты направления «Реклама и связи с общественностью», «Связи с общественностью в политике и бизнесе». Выборка варьировалась от 80 чел. (3 группы) до 180 чел. (5 групп). Опрашивая студентов, автор пришел к тем же выводам, что и статистика, которую демонстрирует TG Stat: большинство людей предпочитают юмор и развлечения, но никак не политическую тематику. Конечно, личные наблюдения и организованные среди студентов фокус-группы не являются исчерпывающим аргументом, но они являются ценным фактологическим материалом для замера эмоционального настроения общества.

Чтобы снизить негативные реакции, эмоциональный негатив, повысить охваты и т.д., публикуемые материалы должны соответствовать ожиданиям общества. Отсюда первая и главная рекомендация для госмессенджера МАХ: соответствовать ожиданиям развлекательного контента, общей направленности «Новости и СМИ», не акцентированного на политике. Вторая рекомендация – создать благоприятные для проправительственных, но неофициальных блогеров именно в категории «политика». Третья рекомендация относится к вопросу, который не был проанализирован в данной статье, однако по опыту общения авторов, важен для ежедневного использования: это – UX/UI дизайн. UX/UI дизайн – это дизайн пользовательского интерфейса и удобства приложения.

В затронутом вопросе проблема, освещаемая в статье, выходит на новый уровень: удобство и комфорт, достигаемые дизайном пользовательского интерфейса, значительно снижают негатив и повышают лояльность рядовых пользователей [6, с. 1355].

Визуальный комфорт и интуитивно-понятный интерфейс – факторы, которые позволили мировым мессенджерам, теперь запрещенным в Российской Федерации, занять лидирующие позиции по охватам и подписчикам в мире. В этих мессенджерах наблюдается та же динамика, что и в Телеграм: большая часть подписчиков ориентированы на новости, развлечения, образовательный контент. Соответственно, продвинутый UX/UI дизайн госмессенджера МАХ, лояльность администрации госмессенджера к востребованным в обществе видам контента являются условиями его успешности в российском обществе.

#### Список источников

1. Смирнов Н. Н. Эффективность кадровой политики как фактор обеспечения национальной безопасности России (на основе анализа контента Телеграм-каналов в период мобилизации) // Сетевое издание «Академическая мысль». 2022. № 4 (21). С. 246–249. <https://doi.org/10.32986/978-5-93673-193-8-2018-1-162>. EDN: SCILZS
2. Ляховенко О. И. Телеграм-каналы в системе экспертной и политической коммуникации в современной России // Galactica Media: Journal of Media Studies. 2022. Том 4. № 1. С. 114–144. <https://doi.org/10.46539/gmd.v4i1.230>. EDN: HSTPMV
3. Ежов Д. А. Особенности репрезентации современных государств в публичных телеграм-каналах // Российский социально-гуманитарный журнал. 2024. № 1. С. 35–48. <https://doi.org/10.18384/2224-0209-2024-1-1419>. EDN: HZTHOO
4. Sayak Saha Roy, Elham Pourabbas Vafa, Kobra Khanmohammadi, Shirin Nilizadeh. DarkGram: A Large-Scale Analysis of Cybercriminal Activity Channels on Telegram. arXiv preprint August 13-15, 2025. URL: <https://www.usenix.org/system/files/usenixsecurity25-roy.pdf> (дата обращения – 05.03.2026). <https://doi.org/10.48550/arXiv.2409.14596>
5. Vincenzo Imperati, Massimo La Morgia, Alessandro Mei, Alberto Maria Mongardini, Francesco Sassi. 2025. “The Conspiracy Money Machine: Uncovering Telegram’s Conspiracy Channels and their Profit Model.” In: 34th USENIX Security Symposium (USENIX Security 25), pp. 5229-5246. URL: <https://www.usenix.org/system/files/usenixsecurity25-imperati.pdf> (дата обращения – 05.03.2026). <https://doi.org/10.48550/arXiv.2310.15977>
6. Агеева А. Д., Петросян Л. Э. Дизайн интерфейсов (UI) и пользовательский опыт (UX) // Международный научный журнал «Вестник науки». 2024. № 6 (75). Том 1. Июнь. EDN: OGZMTT
7. Дискин Е. И., Малютин М. Р. Мессенджер Мах как инструмент модернизации электронного правительства: анализ трансформации взаимодействия граждан и государства // Вопросы государственного и муниципального управления. 2026. № 1. С. 144–169. <https://doi.org/10.17323/1999-5431-2026-0-1-144-169>. EDN: HKZCPE

## References

1. Smirnov N. N. The Effectiveness of Personnel Policy as a Factor of Ensuring the National Security of Russia (Based on the Analysis of the Content of Telegram Channels During the Mobilization Period). *Online publication "Akademicheskaja mysl"*. 2022;4(21):246–249. (In Russ.). <https://doi.org/10.32986/978-5-93673-193-8-2018-1-162>. EDN: SCILZS
2. Lyakhovenko O. I. Telegram channels in the system of expert and political communication in modern Russia. *Galactica Media: Journal of Media Studies*. 2022;(1):114–144. (In Russ.). <https://doi.org/10.46539/gmd.v4i1.230>
3. Ezhov D. A. Features of the representation of modern states in public telegram channels. *Russian Social and Humanitarian Journal*. 2024;(1):35–48. (In Russ.). <https://doi.org/10.18384/2224-0209-2024-1-1419>. EDN: HZTHOO
4. Sayak Saha Roy, Elham Pourabbas Vafa, Kobra Khanmohammadi, Shirin Nilizadeh. DarkGram: A Large-Scale Analysis of Cybercriminal Activity Channels on Telegram. arXiv preprint August 13-15, 2025. Available from: <https://www.usenix.org/system/files/usenixsecurity25-roy.pdf> (Accessed 5 March 2026). <https://doi.org/10.48550/arXiv.2409.14596>
5. Vincenzo Imperati, Massimo La Morgia, Alessandro Mei, Alberto Maria Mongardini, and Francesco Sassi. 2025. *The Conspiracy Money Machine: Uncovering Telegram's Conspiracy Channels and their Profit Model*. In: 34th USENIX Security Symposium (USENIX Security 25), pp. 5229–5246. URL: <https://www.usenix.org/system/files/usenixsecurity25-imperati.pdf> (accessed 03/05/2026) <https://doi.org/10.48550/ARXIV.2310.15977>
6. Ageeva A.D., Petrosyan L.E. Interface design (UI) and user experience (UX). *International scientific journal "Bulletin of Science"*. 2024;6(75)1. June. (In Russ.). EDN: OGZMTT
7. Diskin E.I., Malyutin M R. Messenger Max as a tool for modernizing e-government: an analysis of the transformation of interaction between citizens and the government'. *Public Administration Issues*. 2026;(1):144–169. (In Russ.). <https://doi.org/10.17323/1999-5431-2026-0-1-144-169>. EDN: HKZCPE

## Информация об авторах

И. И. Рогов – кандидат философских наук, доцент кафедры массовых коммуникаций и медиабизнеса, Финансовый университет при Правительстве Российской Федерации.

Ю. В. Логинова – кандидат экономических наук, доцент кафедры массовых коммуникаций и медиабизнеса, Финансовый университет при Правительстве Российской Федерации.

## Information about the authors

I. I. Rogov – Cand. Sci. (Philosophy), Associate Professor of the Department of Mass Communications and Media Business of Financial University under the Government of the Russian Federation.

Ju. V. Loginova – Cand. Sci. (Econ.), Associate Professor of the Department of Mass Communications and Media Business of Financial University under the Government of the Russian Federation.

**Вклад авторов:** все авторы сделали эквивалентный вклад в подготовку публикации.

Авторы заявляют об отсутствии конфликта интересов.

**Contribution of the authors:** the authors contributed equally to this article. The authors declare no conflicts.

Статья поступила в редакцию 05.03.2026; одобрена после рецензирования 30.04.2026; принята к публикации 12.05.2026.

The article was submitted 05.03.2026; approved after reviewing 30.04.2026; accepted for publication 12.05.2026.