The Blocking Ladder. Part Two: From Throttling to Isolation (2025–2026)

The first part of the "Ladder of Blocks" was released in the spring of 2025 and ended with a prediction: we listed the likely next steps in the escalation of Russian internet censorship — from a total block of Telegram and statistical detection of VPNs to the transition from "blacklists" to "whitelists" and the split of the Runet into domestic and international segments. Some of these steps belonged to the near term, some to the distant future. A year has passed, and almost all of them have been taken, and some at a pace that even the pessimistic scenario did not anticipate.

This second part traces the events of 2025 and the first half of 2026 and shows how individual measures — rolling mobile internet shutdowns, "whitelists", the throttling of WhatsApp and Telegram, forcing users onto the state messenger MAX, the detection of bypass protocols, shifting the burden of censorship onto businesses, and the first steps toward traffic separation — come together into a single control architecture. If the previous stage could be described by the formula "ban access to the unnecessary", the new one is more accurately captured by the formula "allow access only to the necessary". There is no prediction here: we record what has already happened, using verifiable sources. The first part can be read here: https://ozi-ru.net/art1.html

Table of contents

Chapter 1. Introduction: the year the forecast became a chronicle

The first part of this study closed in the spring of 2025 with a forecast.[1] Drawing on the logic of escalation, we listed the likely next steps on the "blocking ladder": the full blocking of Telegram, the introduction of statistical methods for detecting VPNs, a shift to blocking large blocks of IP addresses, the tactics of "grey lists" and deliberate degradation of connection quality, the move from "blacklists" to "whitelists," and, finally, the full isolation of the Runet. Some of these steps we placed in the near term, others in the distant future. The move to "whitelists," for example, was described as a technically complex scenario "in the more distant future."

A year has passed, and in that time almost every step listed has been taken — some at a pace that not even the pessimistic forecast anticipated. Telegram is blocked. Next-generation VPN protocols are detected by behavioral markers. Blocks of IP addresses belonging to major

[1] The Blocking Ladder. Part One // Internet Protection Society. URL: https://ozi-ru.net/art1.html (Лестница блокировок. Часть первая // Общество защиты интернета URL: https://ozi-ru.net/art1.html)

hosting providers and CDNs are added to the registry in batches. "Whitelists" have turned from a theoretical construct into a working mechanism deployed across most of the country's regions. And the drive to divide traffic into domestic and international — once a metaphor of a "digital iron curtain" — has become the subject of specific meetings at the Ministry of Digital Development, complete with specific limit figures.

Moreover, the 2025–2026 period added to the "ladder" things the earlier analysis had not treated as central instruments: rolling shutdowns of mobile internet, now an everyday occurrence across the whole country, and the coercion of tens of millions of users into a state messenger. If the previous stage of censorship can be summed up by the formula "deny access to the superfluous," the new stage is more accurately described by the formula "allow access only to the necessary." This is a qualitative shift: from targeted filtering to control over the very possibility of connection.

The aim of this part is to trace the events of 2025 and the first half of 2026, to show how individual measures add up into a single architecture of control, and to record the facts with verifiable sources. There is no forecast in this part: we record what has already happened.

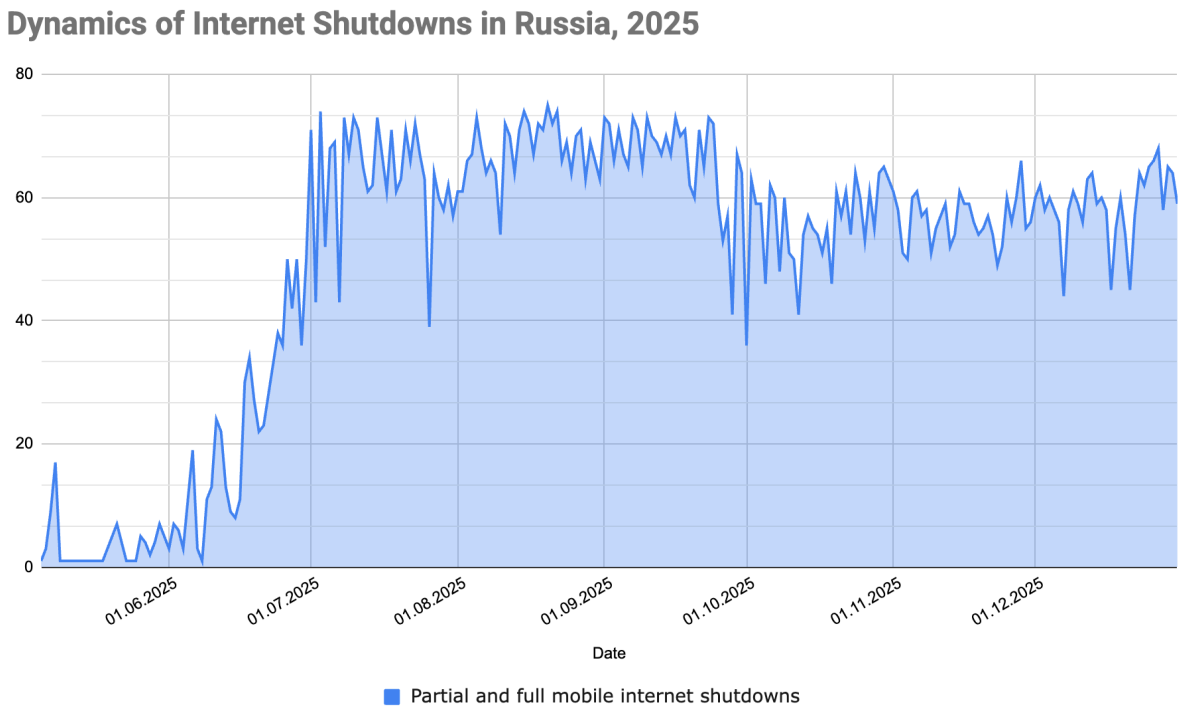
A note on terms. Throughout the period described, the state almost nowhere uses the word "blocking" in relation to the largest services. The official formulations are "throttling," "partial restriction," "measures of compulsion." As with YouTube in the summer of 2024, the actual result (the impossibility of using the service) is achieved by technical means without any formal announcement. Wherever official rhetoric and the actual state of affairs diverge, we will keep the two apart.

Chapter 2. The Year of the Shutdown

The main innovation of 2025 was mass shutdowns of mobile internet — a practice that in a few months moved from isolated episodes to a nationwide norm. The scale is visible in the annual statistics of the Na Svyazi project (which works together with the Internet Protection Society), which keeps a monthly count of shutdown cases. In May 2025 observers recorded only 68 cases for the month. By June the number had grown almost tenfold, to 652. The peak came at the height of summer: 1,967 cases in July and 2,099 in August — more than were recorded worldwide in all of 2024 (296 shutdowns in 54 countries, according to Access Now). By autumn the intensity stabilized at a high level: 1,725 cases in October, 1,693 in November, and 1,823 in December. In total, 12,024 incidents were recorded for 2025.[2]

[2] Monthly statistics of rolling mobile-internet shutdowns for 2025 — the Na Svyazi project (in cooperation with the Internet Protection Society); summary data is also in the Wikipedia article "Internet shutdowns in Russia." URL: https://ru.wikipedia.org/wiki/Отключения_интернета_в_России (Помесячная статистика веерных отключений мобильного интернета за 2025 год — проект "На Связи" (в сотрудничестве с Обществом защиты интернета); сводные данные также в статье Википедии "Отключения интернета в России".)

Chart 1. Dynamics of mobile-internet shutdowns in Russia, 2025



The chart shows the dynamics of rolling mobile-internet shutdowns in Russia over 2025: the vertical axis is the number of regions where partial or full shutdowns were recorded during a 24-hour period, the horizontal axis is the dates from May to December. There is no earlier data on the chart: before the so-called "victory parades" there was no established practice of shutting down mobile internet in Russia. The curve visibly falls into three phases. Until early June, the values hover near zero with rare single spikes up to 15–19 regions. From the first days of June, the line rises almost vertically and, over three or four weeks, climbs from single digits to more than 70 regions. From July to September it holds a high plateau in the 55–75 region corridor, with strong day-to-day fluctuations. In the autumn, after a brief dip at the turn of September and October, the curve does not fall off but settles in the range of 45–68 regions through the end of the year — shutdowns turn from a one-off event into a permanent background.

1. The parade as the starting point (May 2025)

The first mass shutdown to draw universal attention came during the "celebrations of the 80th anniversary of Victory." From 7 to 9 May 2025, mobile communications and internet were restricted in Moscow and more than thirty regions.[3] No substantive official explanation was

[3] Shutdowns in Russia: what is happening with mobile internet // Forbes Russia. URL: https://www.forbes.ru/tekhnologii/542902 (Шатдауны в России: что происходит с мобильным интернетом // Forbes Россия)

given: presidential press secretary Dmitry Peskov said the restrictions were being introduced "for understandable reasons," and that anything connected with ensuring citizens' safety was "justified." The logic was transparent: mobile internet is used to control drones, so during mass events it is easier to switch it off than to shield the skies over the events themselves with air-defense systems.

2. Spiderweb and the turning point (June 2025)

The turning point was the Ukrainian operation Spiderweb ("Pautina") on 1 June 2025, when drones — delivered covertly deep inside Russia in advance, in special containers on trucks with remotely opening roofs, and launched from right beside the airfields — attacked strategic aviation at several bases at once. Control of some of the craft was, according to a number of reports (though this was not proven), carried out in part over Russian cellular networks. After this, mobile-internet shutdowns ceased to be tied to holidays and turned into a routine response to any threat, or the expectation of one.[4]

It is Operation Spiderweb that explains the June surge: before it, shutdowns numbered in the dozens per month; immediately afterward, in the hundreds. On 8 July 2025, an anti-record for coverage was set: mobile internet was shut down in one form or another in 77 of the 89 federal subjects.[5] On the chart this turning point appears as an almost sheer rise of the curve in the first days of June, and the 8 July anti-record sits on the upper boundary — around 75 regions per day.

The counting methodology used by independent observers is conservative: it counts user complaints confirmed by technical checks across at least two operators, as well as official statements by the authorities.[6] This means the real scale is most likely higher than what is recorded.

3. Moscow and the question of effectiveness (2025–2026)

By the spring of 2026 the shutdowns reached the capital in a new form. From 6 March 2026, mobile internet in central Moscow was shut down for more than a week straight — according to

[4] A map of the shutdowns: how mobile internet is switched off in Russia // Meduza. URL: https://meduza.io/feature/2025/07/07/karta-shatdaunov (Карта шатдаунов: как в России отключают мобильный интернет // Meduza)
[5] Mobile-internet shutdowns in Russia // Ruwiki. URL: https://ru.ruwiki.ru/wiki/Отключения_мобильного_интернета_в_России (Отключения мобильного интернета в России // Рувики)
[6] How the internet dies: a map of the shutdowns // Meduza. URL: https://meduza.io/feature/2025/10/16/kak-umiraet-internet-karta-shatdaunov (Как умирает интернет: карта шатдаунов // Meduza)

industry sources, this was linked to the final testing of the "whitelist" regime in the capital.[7] For Muscovites it came as a surprise: shutdowns on Moscow's territory had happened before, but never on such a scale or for so long. The capital, accustomed to living in a special regime, learned from its own experience that it, too, is in Russia.

At the same time, the effectiveness of shutdowns as a counter-drone measure raises more and more questions. In March 2026, data journalists at Novaya Gazeta Europe, comparing the geography of shutdowns with reports of actual attacks, concluded that around 85% of shutdown cases fell on days when no strikes were reported in the regions concerned. In Novosibirsk Oblast and Krasnoyarsk and Khabarovsk Krais — regions beyond the reach of Ukrainian drones — the internet was shut down on more than 98% of the days observed.[8] The shape of the chart confirms this: in the autumn the curve does not decline but stays high through the end of the year. Mobile shutdowns have turned from a situational security measure into a permanent operating regime that itself becomes an instrument for restricting communications.

4. The cost

Economic estimates diverge depending on methodology, but all point to a colossal scale of damage. The Internet Protection Society, using the Brookings Institution methodology, estimated a single hour of a full shutdown at roughly 46 billion rubles nationwide (for Moscow alone, about 9.6 billion rubles per hour).[9] The international service Top10VPN, in its year-end review, named Russia the world leader of 2025 for the duration of internet restrictions: 37,166 hours, around 146 million users affected, and $11.9 billion in damage — more than 60% of all shutdown-related damage worldwide.[10]

The market's reaction was telling: demand shifted toward wired access and satellite internet. Kommersant, citing data from Tricolor, reported that sales of the "Tricolor Internet" service grew 2.4 times year-on-year in the second quarter of 2025.[11] The impossibility of relying on mobile communications became not a temporary inconvenience but a factor reshaping consumer

---

[7] "Whitelists" of sites in Russia // Wikipedia. URL: https://ru.wikipedia.org/wiki/%C2%AB%D0%91%D0%B5%D0%BB%D1%8B%D0%B5_%D1%81%D0%BF%D0%B8%D1%81%D0%BA%D0%B8%C2%BB_%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8 ("Белые списки" сайтов в России // Википедия)

[8] No reply, no strike // Novaya Gazeta Europe. URL: https://novayagazeta.eu/articles/2026/03/26/ni-otveta-ni-prileta (Ни ответа, ни прилета // Новая газета Европа)

[9] The shutdowns continue: how to live in the era of the internet shutdown // Yamal-Media. URL: https://yamal-media.ru/narrative/otkljuchenija-prodolzhajutsja-kak-zhit-v-epohu-internet-shatdauna (Отключения продолжаются: как жить в эпоху интернет-шатдауна // Ямал-Медиа)

[10] The Global Cost of Internet Shutdowns // Top10VPN. URL: https://www.top10vpn.com/research/cost-of-internet-shutdowns/ (The Global Cost of Internet Shutdowns // Top10VPN)

[11] Demand for satellite and wired internet grew against the backdrop of shutdowns // Kommersant. URL: https://www.kommersant.ru/doc/7908736 (Спрос на спутниковый и проводной интернет вырос на фоне отключений // Коммерсантъ)

behavior.

5. The administrative logic of the shutdowns

To understand why the shutdowns became exactly what they are — chaotic and ubiquitous — one has to look not at the technology but at the bureaucracy. Behind the rolling shutdowns lies not a single state strategy but the logic of departmental reporting.

The public justification is unchanging: authorities at various levels have repeatedly said they shut down mobile internet for safety, since Ukrainian drones use cellular networks to communicate with control centers. The problem is that regional authorities have no real means of countering drones. Not even the military and air-defense systems have that capability, and it is even less clear what the administration of a small federal subject could set against a drone threat. In a situation where a region is by default held responsible for preventing damage but given no tools to do so, the idea was born of shutting down the internet — not so much for the result as for the sake of reporting up to the federal center.

Organizationally, this is arranged outside the legal field. As far as is known, shutdown decisions are made by regional working groups that include the regional administration, the medical service, the Emergencies Ministry, the Interior Ministry, and the regional FSB units; it is they who give telecom operators the command to shut down. Since no law or other normative act regulating this procedure exists, the regions act haphazardly: each shuts down the internet in its own way, within its own borders, and on its own grounds. Hence both the patchwork on the shutdown map and the impossibility of predicting in advance where and when the connection will drop.

The geography of the first months confirms that the practice spread not from the top down but sideways, from the pioneer regions. The largest number of shutdowns in the first two months fell on Nizhny Novgorod Oblast (21 cases) and Omsk Oblast (20 cases); the top five also included Rostov, Pskov, Saratov, and Tula Oblasts — 19 cases each. Apparently the technique was worked out in one of these subjects and then adopted by the rest.

A kind of reverse cargo cult helped the practice take hold. The regional authorities' logic runs like this: the internet was shut down — the drone did not come — therefore the shutdown worked. The absence of an attack is credited to the shutdown, even though there is no causal link between them, and the correlation is explained by the fact that the overwhelming majority of shutdowns occur in regions beyond drones' reach anyway. Thus a self-confirming conclusion turns a one-off measure into a permanent one: reporting requires it to continue, and the illusory effectiveness provides grounds not to stop.

Chapter 3. Whitelists: the underside of the shutdowns

The most significant consequence of the shutdowns was what had been forecast as a distant

scenario: the move from a "blacklist" model to a "whitelist" model. And it happened not as a separate ideological decision but as a forced technical reaction to the chaos of the shutdowns.

In the terms of the "blocking ladder," this is precisely that inversion of logic which the first part had assigned to the distant future: not "what is on the list is forbidden," but "only what is on the list is allowed." The difference is fundamental — under a "whitelist" model, everything is inaccessible by default except what is explicitly permitted.

1. How they came about

A total shutdown of mobile internet hits not so much drones as the economy and citizens' loyalty: banking apps, payments, taxis, government services, and maps all stop working. The losses fall on everyone — from the retailer whose payment terminals go down to the telecom operators, for whom a shut-down network means direct lost revenue while all the costs of maintaining it remain. It was the operators and the "digital economy" segment tied to mobile internet that became the side for whom the shutdowns turned out to be not an abstract inconvenience but measurable financial losses.

For that reason, "whitelists" should be seen not as a bureaucratic design but as a forced compromise into which the authorities were pushed by the industry itself. The regulator needed a way to keep shutting down the network under the pretext of fighting drones while at the same time relieving the pressure from a business that demanded at least the vital services be preserved. "Whitelists" became that mechanism: a list of resources access to which is preserved during a shutdown, while everything else is cut off.

The idea was voiced publicly by Minister of Digital Development Maksut Shadaev at the "Digital Evolution" forum on 7 August 2025; the technical scheme was agreed with the operators, and access to the permitted resources was to be protected by a captcha so they could not be used to control drones.[12]

2. Rollout (from September 2025)

The first list appeared on 5 September 2025. It included Gosuslugi, VKontakte, Odnoklassniki, Mail.ru, the Max messenger, Yandex's services, and government websites.[13] The list then expanded — in November, twice in December 2025, and in February and April 2026; by May 2026 it included more than 500 Russian services. The key condition for inclusion is stated plainly: all of a resource's computing capacity must be located in Russia.[14]

---

[12] The Ministry of Digital Development prepared a scheme for accessing mobile internet under restrictions // TASS. URL: https://tass.ru/ekonomika/24732149 (Минцифры подготовило схему доступа к мобильному интернету в условиях ограничений // ТАСС)
[13] The whitelist of sites in Russia: what is available during shutdowns // GoGov. URL: https://gogov.ru/articles/site-white-list (Белый список сайтов в России: что доступно при шатдаунах // GoGov)
[14] Internet whitelists in Russia // Forbes Russia. URL: https://www.forbes.ru/tekhnologii/559771 (Белые списки интернета в России // Forbes Россия)

The geography of the regime grew in parallel with the geography of the shutdowns: by mid-October 2025 "whitelists" were applied in roughly 48 regions, by March 2026 in 68–71 regions.[15] The timeline of the first weeks, where the exact date each region was connected is known, not only confirms this estimate but also shows how unevenly the process went.

Table 1. Timeline of regions joining the whitelist regime (16 September – 16 November 2025)

Date	Added	Regions	Total
16.09.2025	9	Vladimir Oblast, Volgograd Oblast, Kamchatka Krai, Republic of Bashkortostan, Republic of Dagestan, Rostov Oblast, Samara Oblast, Saratov Oblast, Yaroslavl Oblast	9
17.09.2025	5	Voronezh Oblast, Krasnodar Krai, Nizhny Novgorod Oblast, Omsk Oblast, Primorsky Krai	14
18.09.2025	3	Krasnoyarsk Krai, Moscow, Oryol Oblast	17
19.09.2025	6	Murmansk Oblast, Novgorod Oblast, Penza Oblast, Udmurt Republic, Tomsk Oblast, Chelyabinsk Oblast	23
20.09.2025	3	Kaluga Oblast, Republic of Tatarstan, Sverdlovsk Oblast	26
21.09.2025	4	Amur Oblast, Mari El Republic, Sakha Republic (Yakutia), Tambov Oblast	30
22.09.2025	1	Irkutsk Oblast	31
24.09.2025	1	Pskov Oblast	32
25.09.2025	3	Kirov Oblast, Kostroma Oblast, Tula Oblast	35
26.09.2025	6	Altai Krai, Kursk Oblast, Saint Petersburg, Sakhalin Oblast, Tver Oblast, Khanty-Mansi Autonomous Okrug	41
29.09.2025	1	Bryansk Oblast	42

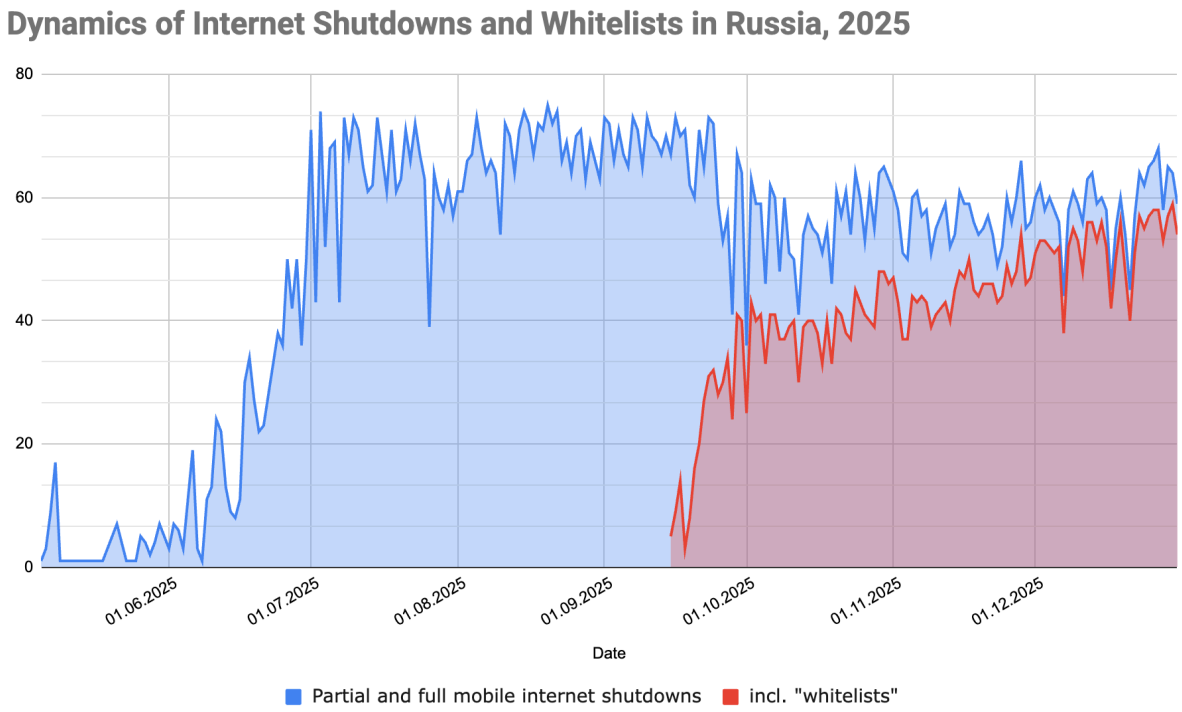
[15] How the internet dies: a map of the shutdowns // Meduza. URL: https://meduza.io/feature/2025/10/16/kak-umiraet-internet-karta-shatdaunov (Как умирает интернет: карта шатдаунов // Meduza)

Date	Added	Regions	Total
30.09.2025	3	Astrakhan Oblast, Ivanovo Oblast, Tyumen Oblast	45
01.10.2025	1	Smolensk Oblast	46
02.10.2025	1	Ulyanovsk Oblast	47
15.10.2025	1	Komi Republic	48
24.10.2025	1	Vologda Oblast	49
26.10.2025	1	Republic of Adygea	50
28.10.2025	1	Ryazan Oblast	51
01.11.2025	1	Khabarovsk Krai	52
13.11.2025	3	Orenburg Oblast, Arkhangelsk Oblast, Perm Krai	55
14.11.2025	1	Kemerovo Oblast	56
16.11.2025	1	Moscow Oblast	57

The timeline breaks into two phases with different dynamics. In the first fifteen days, from 16 to 30 September, the regime was switched on in 45 of the 57 regions in this sample (79%); of those, 30 (53%) in the first six days, 16–21 September, when 3 to 9 regions were added simultaneously each day. This is not a gradual spread of the practice but effectively a synchronous nationwide launch, stretched over several days by a technical rotation of regions. After 30 September the pace drops by an order of magnitude: over the month and a half from 1 October to 16 November, only 12 regions were added — on average once every four days, against three a day in September. The remaining regions were connected on a residual basis: either the shutdowns there were less intense, or delays with the TSPU equipment took their toll.

Moscow's case stands out sharply: the city gained access to the regime as early as the third day of the campaign, 18 September, whereas Moscow Oblast came only on 16 November, the last entry in this timeline. The two-month gap between the capital and its immediate surroundings is visible even against the general unevenness of the process.

Chart 2. Mobile-internet shutdowns and whitelist coverage, 2025



The chart shows the same dynamics of rolling shutdowns (blue area, see Chart 1), but overlaid with the share of cases where the shutdown was accompanied by an active whitelist (red area). Until early September the red area equals zero: the mechanism did not yet exist. With the launch of the first list on 5 September it begins to grow, and the sharp acceleration falls on 16–30 September — the same dates as the mass entry of regions in the table above; during this time the red area rises from zero to 30–40. After the brief dip at the turn of September and October, synchronous with the dip in the blue curve, growth resumes and continues through the whole fourth quarter: by the end of December the red area reaches 55–58 against the blue's 60–68. The gap between the curves, 20–25 in October, narrows to 5–10 by the end of the year.

Here it is important to distinguish two dimensions of one process. The table records the geography of availability — when the regime became technically possible in each region; this is almost entirely a September story, in fifteen days of which 79% of the final list was covered. The chart shows the intensity of application — the share of daily shutdowns that actually run with a whitelist rather than as a total blackout; here the main growth comes already in October–December, that is, in the months when the addition of new regions had almost stopped. The infrastructure was deployed almost everywhere by the end of September, but the transition from technical possibility to application by default took another quarter. This confirms the thesis stated at the start of the chapter: the move from blacklists to whitelists is not a one-off decision but a process with two different speeds — technical deployment and subsequent

entrenchment in everyday practice.

3. The mechanics of whitelists

Technically the regime is implemented through filtering by DNS, IP addresses, and subnets: anything not on the list does not open. It is implemented by the operators themselves — on a combination of the TSPU equipment installed at RKN's demand and their own DPI systems, which operators buy on the open market. Thus, in early September 2025, Beeline announced a tender to upgrade its DPI platform, asking the supplier to add to the blocking of specific addresses the ability to classify subscriber traffic by thematic categories.[16] It is fundamentally important that changing an IP address or using a VPN does not help here — foreign addresses are blocked as a class, and the VPN server itself is not on the list.[17] The regime applies to mobile internet; rumors of its extension to wired access were refuted by the Ministry of Digital Development in March 2026.[18]

Circumventing these restrictions is built on "transport camouflage" based on the V2Ray/Xray family of protocols (in particular, VLESS with the Reality technology), where forbidden proxy traffic is packed inside legitimate TLS sessions directed at IP addresses that are on the whitelists — for example, Yandex or VK servers. Tuned to imitate a connection to a permitted resource from the list, the technology copies its TLS handshake and encryption parameters, so that DPI systems see what is happening as a standard request from a local user to an approved site.

It is important to understand that any of these technologies works only with a certain probability. The same method does not work identically across different operators, in different regions, or even within one operator in one region: the result depends on the specific firmware of the equipment, the version of the signatures, and the current wave of restrictions. Over time the share of successful connections under the whitelist regime declined, and by the available estimates does not exceed ten percent by mid-2026.

The reason is that operators and RKN are deliberately fighting circumvention. Filtering is supplemented by behavioral analysis: the system tracks traffic anomalies — for example, several parallel attempts to establish a TLS connection to the same SNI within a short interval

---

[16] Beeline announced a DPI-upgrade tender; the system will have to classify traffic not only by individual addresses but by categories. Mediazona, 3 September 2025. https://zona.media/news/2025/09/03/dpiline (Билайн объявил тендер на обновление DPI; система должна будет классифицировать трафик не только по отдельным адресам, но и по категориям. Медиазона, 3 сентября 2025.)

[17] The whitelist: what it is and how it works // Kod.ru. URL: https://kod.ru/bely-spisok (Белый список: что это и как работает // Kod.ru)

[18] "Whitelists" of sites in Russia // Wikipedia. URL: https://ru.wikipedia.org/wiki/%C2%AB%D0%91%D0%B5%D0%BB%D1%8B%D0%B5_%D1%81%D0%BF%D0%B8%D1%81%D0%BA%D0%B8%C2%BB_%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8 ("Белые списки" сайтов в России // Википедия)

freeze further connections.[19] In addition, the cloud platforms through which the camouflage is built have themselves come under surveillance and restriction. Providers whose addresses are on the whitelists — Yandex Cloud and VK Cloud (and also Selectel and Cloud.ru) — have ceased to be a guarantee of availability: RKN has begun restricting entire subnets and autonomous systems of Russian data centers that were previously considered safe.[20]

4. The "cooling-off" of SIM cards

As part of introducing "whitelists" and restricting access to the network, one of the key measures for "preventing enemy drones from connecting to public networks" was tight regulation of SIM cards. Under special control are devices that register on the network after a long absence or return from international roaming. For these a mechanism called the "cooling-off period" is applied: as soon as such a SIM card is reactivated on Russian territory, operators automatically block its access to mobile internet and to sending/receiving SMS for exactly 24 hours.[21] To lift this restriction once the day is over and confirm that the card is used by a real person and not an automated drone navigation system, the subscriber must pass a captcha (CAPTCHA) verification.[22] For SIM cards of foreign operators, a similar restriction regime came into effect in October 2025. Officially the procedure is positioned as protecting infrastructure from drone control via cellular networks, but in practice it lets the state instantly isolate and manually control the connection of any mobile subscriber.

5. Under FSB control

Formally the whitelists are drawn up by the Ministry of Digital Development, but the list is approved only after coordination with the agencies responsible for security — above all the FSB; this was confirmed by the ministry itself.[23] The distribution of roles alone once again proves that the whitelists arose not as an element of a strategy to disconnect the country from the global internet, but as a reaction to full shutdowns already underway: they were introduced

---

[19] On RKN's restriction scheme in June 2026 (reverse-engineering of the mechanism freezing TLS connections by SNI). Habr, June 2026. https://habr.com/ru/articles/1044396/ (О схеме ограничений РКН в июне 2026-го (реверс-инжиниринг механизма заморозки TLS-соединений по SNI). Хабр, июнь 2026.)

[20] The end of the whitelist era: RKN affected the operation of cloud providers. Habr, January 2026. https://habr.com/ru/articles/988862/ (Конец эпохи белых списков: РКН повлиял на работу облачных провайдеров. Хабр, январь 2026.)

[21] The SIM-card limit and the access regime // Rossiyskaya Gazeta. URL: https://rg.ru/2025/11/11/rezhim-dostupa.html (Лимит SIM-карт и режим доступа // Российская газета)

[22] Russians returning from abroad faced SIM blocking // CNews. URL: https://www.cnews.ru/news/top/2025-11-11_rossiyanevernuvshiesya_iz-za (Россияне, вернувшиеся из-за границы, столкнулись с блокировкой SIM // CNews)

[23] Ministry of Digital Development: services are added to the whitelist after coordination with the interested agencies and the bodies responsible for security, including the FSB. Anti-Malware, 2 February 2026. https://www.anti-malware.ru/news/2026-02-02-114534/48900 (Минцифры: сервисы вносятся в белый список после согласования с заинтересованными ведомствами и органами, отвечающими за безопасность, в том числе с ФСБ. Anti-Malware, 2 февраля 2026.)

not to cut something off, but to keep at least a vital minimum available. Yet it was precisely this compromise mechanism that the security bloc quickly seized and re-tooled for its own purposes: over a few months control of the list's contents effectively passed to it, and the inclusion criterion shifted from technical to political.

Whereas in the autumn of 2025 placing a service's infrastructure on Russian territory was enough to get onto the list, in early February 2026 the FSB forbade adding to the whitelists the apps of banks that had not installed SORM equipment.[24] Because of a failure to meet this requirement, the lists lack the apps of Sberbank, T-Bank, and Gazprombank — that is, services used by tens of millions of people.[25]

The logic of the requirement is built through the status of "organizer of information dissemination" (ORI). Back in October 2025 the FSB notified major banks that their apps fall under ORI, since they contain a messaging function — correspondence with support and between users — and required them to install SORM by 2027.[26] ORI status entails compliance with the requirements of the Yarovaya package: storing metadata and the content of correspondence on Russian territory and handing this data over, together with encryption keys, at the request of law enforcement. From January 2026 the mandatory storage period for such information was raised to three years, with fines and even blocking of the resource for non-compliance.[27]

Thus the construction closed on itself: the availability of a banking app to citizens during an internet shutdown is placed in direct dependence on the bank's readiness to enable surveillance of its own clients. The whitelist turned from an instrument for preserving vital services into a lever of compulsion — a mechanism that forces businesses to deploy surveillance infrastructure under threat of being shut off.

A side effect was distortion of competition. In March 2026 the head of the Bank of Russia, Elvira

---

[24] The whitelist of digital platforms // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Белый_список_цифровых_платформ (Белый список цифровых платформ // TAdviser)

[25] RBC: the apps of Sberbank, T-Bank, and Gazprombank are absent from the whitelists (as reported by Meduza). 2 February 2026. https://meduza.io/news/2026/02/02/rbk-fsb-zapretila-vnosit-v-belyy-spisok-prilozheniya-bankov-ne-ustanovivshih-sistemu-dlya-otslezhivaniya-i-hraneniya-perepiski-polzovateley (РБК: в белых списках отсутствуют приложения Сбербанка, Т-Банка и Газпромбанка (изложение по Meduza). 2 февраля 2026.)

[26] In October 2025 the FSB demanded that major banks install SORM by 2027 in connection with their ORI status. Forbes, 2 February 2026. https://www.forbes.ru/finansy/554634-fsb-zapretila-vnosit-v-belyj-spisok-prilozenia-bankov-bez-sistemy-hranenia-dannyh (ФСБ в октябре 2025 года потребовала от крупных банков установить СОРМ до 2027 года в связи со статусом ОРИ. Forbes, 2 февраля 2026.)

[27] Yarovaya-package requirements for ORI: storage of correspondence and encryption keys, transfer on request; from January 2026 the storage period is increased to three years. SecurityLab, 2 February 2026. https://www.securitylab.ru/news/568856.php (Требования пакета Яровой к ОРИ: хранение переписки и ключей шифрования, передача по запросу; с января 2026 года срок хранения увеличен до трех лет. SecurityLab, 2 февраля 2026.)

Nabiullina, publicly criticized the selective inclusion of banks on the list, calling it a violation of the rules of fair competition, and stated that all licensed banks should be on it.[28] The banks themselves, according to market participants, are dragging their feet on installing SORM for fear of losing clients; the dispute, however, is not about the surveillance itself but about who will be the first to agree to announce it.

Chapter 4. The state messenger MAX

Alongside the blocking and restriction of access to familiar foreign services, the state was building the "positive" part of its strategy. It consisted of the forced creation and promotion of fully controlled Russian platforms (such as VK, Rutube, Dzen), to which, the authorities intended, users deprived of alternatives were to migrate by force.

1. From announcement to law

On 25 March 2025 the VK holding (CEO Vladimir Kiriyenko) announced the Max messenger, describing it outright as an analog of China's WeChat: communication, payments, government services, and mini-apps in one window.[29] Already on 4 June, at a meeting chaired by the president, the head of the Ministry of Digital Development, Maksut Shadaev, announced the development of a national messenger based on Max, and in June the platform was entered into the registry of domestic software.

On 24 June 2025 Vladimir Putin signed Federal Law No. 156-FZ on the creation of a "multifunctional information-exchange service" — the legal basis for the national messenger.[30] On 12 July 2025, by government order No. 1880-r, LLC MAX was designated the operator of the service.[31]

2. Ownership structure and the Kremlin's personal control

---

[28] Nabiullina: including only some banks on the whitelist violates the rules of fair competition; all licensed banks should be on the list. Forbes, March 2026. https://www.forbes.ru/finansy/557633-nabiullina-raskritikovala-vklucenie-v-belyj-spisok-mincifry-tol-ko-nekotoryh-bankov (Набиуллина: включение только части банков в белый список нарушает правила равной конкуренции; в перечне должны быть все лицензированные банки. Forbes, март 2026.)

[29] Max (messenger) // Wikipedia. URL: https://ru.wikipedia.org/wiki/Max_(мессенджер) (Max (мессенджер) // Википедия)

[30] On the creation of a multifunctional information-exchange service (Federal Law No. 156-FZ of 24.06.2025) // Official Publication of Legal Acts. URL: http://publication.pravo.gov.ru/document/0001202506240021 (О создании многофункционального сервиса обмена информацией (ФЗ № 156-ФЗ от 24.06.2025) // Официальное опубликование правовых актов)

[31] The MAX messenger: the service operator // Gosuslugi (regional portal). URL: https://co44-cherepovec-r19.gosweb.gosuslugi.ru/glavnoe/messendzher-mah/ (Мессенджер MAX: оператор сервиса // Госуслуги (региональный портал))

The official operator of the national messenger was designated by government order as LLC MAX (until 24 June 2025 named LLC Communication Platforms). The company was registered on 4 September 2024 at the legal address: Moscow, Leningradsky Prospekt, 39, bld. 79. The post of CEO is held by Farit Faritovich Khusnoyarov, and the managing organization's functions are performed by LLC Communication Platform — a direct subsidiary of the VK holding.

Through this chain of legal entities, the Max messenger belongs entirely to the international public joint-stock company VK (formerly Mail.ru Group), whose management and ownership vividly demonstrate that the country's main digital platform is controlled by Vladimir Putin personally and his closest circle:

- **The holding's leadership:** VK's CEO is Vladimir Kiriyenko, son of the first deputy head of the Presidential Administration, Sergei Kiriyenko, who in the Kremlin is directly responsible for domestic policy, ideology, and censorship in the Russian internet segment.
- **Shareholders and beneficiaries:** A controlling stake of VK's voting shares (through the company MF Technologies) belongs to a consortium of structures inseparably linked to Putin's inner circle. The main shareholders are JSC SOGAZ and Gazprombank. The largest co-owners of SOGAZ are the president's longtime personal friend Yuri Kovalchuk, his family, and Putin's own relatives (in particular, his nephew Mikhail Shelomov).

Thus the creation of the Max messenger is not a commercial project of the private market but a strategic state initiative, whose operator is a digital holding under direct family-nomenklatura management by the Presidential Administration and financed by the "wallets" of the ruling clan.

3. Coercing the migration

Further steps turned the "national messenger" into a mandatory one. From September 2025, Max began to be pre-installed on all new smartphones and tablets sold in Russia, and school chats and "Sferum" profiles began to be moved to Max.[32] In November 2025 the Ministry of Digital Development ordered, by letter, state organizations to move to Max by 1 January 2026, and budget-funded institutions by 1 February 2026, with reporting on the transition.[33] In March 2026 Max received the official status of a social network, and RKN began registering channels in it.[34]

On 29 December 2025 a law was signed obliging the "building chats" of management companies, utility-supply organizations, and capital-repair funds to be run specifically in Max (an

[32] The new Russian messenger MAX // Obrazovanie (regional portal). URL: https://xn--h1alcedd.xn--d1aqf.xn--p1ai/instructions/novyy-rossiyskiy-messendzher-makh/ (Новый российский мессенджер MAX // Образование (региональный портал))
[33] State organizations to be obliged to move to Max // GoGov. URL: https://gogov.ru/news/924335 (Госорганизации обяжут перейти на Max // GoGov)
[34] Max received the status of a social network // Garant. URL: https://www.garant.ru/news/2024987/ (Max получил статус социальной сети // Гарант)

exception was made only for Moscow, which was allowed to use regional systems).[35] In this way the user was pushed into the messenger from several directions at once: through school, through work in the public sector, through utility services.

By March 2026 the platform reported 100 million registered users and a daily audience of more than 55 million.[36] These figures must be read with an allowance for the coercive nature of registration, but the sheer scale of coverage is beyond doubt.

4. Privacy and surveillance

Criticism of the Max messenger centers on threats to users' privacy. The app entirely lacks end-to-end encryption, and its rules directly provide for handing over data at the request of government bodies. Independent researchers found that Max collects IP addresses and checks whether the user has a VPN enabled, and reverse-engineering of the code revealed hidden third-party libraries inside the app.[37] Roskomsvoboda lawyer Sarkis Darbinyan characterized the project as a large-scale experiment on citizens that creates risks of building a social-credit system in Russia on the Chinese model.[38]

The link between the forced introduction of Max and the artificial strangling of its competitors was stated openly by experts. Back in August 2025, the analyst Eldar Murtazin — who broadly supports the war and the current government — commenting on the then-beginning blocking of calls in WhatsApp and Telegram, directly suggested that these messengers would be deliberately "broken" in Russia to force people to switch to Max.[39] Subsequent events fully confirmed this logic.

5. MAX and VK out of the App Store: a sanctions paradox

In the summer of 2026, the VK ecosystem, including the state-promoted MAX, lost access to the App Store. On 3 June, Apple removed MAX itself, citing compliance with export-control rules and sanctions restrictions; the app stopped sending push notifications to iPhones. On 25 June, the rest of the holding's services also disappeared from the store — about two dozen apps: VKontakte, Odnoklassniki, Dzen, Mail.ru, VK Video, VK Music, VK Messenger, VK Dating, VK

---

[35] Building chats to be moved to the Max messenger // Forbes Russia. URL: https://www.forbes.ru/society/553066 (Домовые чаты переведут в мессенджер Max // Forbes Россия)
[36] Max: user statistics // GoGov. URL: https://gogov.ru/news/927214 (Max: статистика пользователей // GoGov)
[37] The Max messenger checks users' IP addresses and VPN activity: a study // Skillbox. URL: https://skillbox.ru/media/code/messendzher-max-proveryaet-ip-polzovateley-i-aktivnost-vpn-issledovanie/ (Мессенджер Max проверяет IP пользователей и активность VPN: исследование // Skillbox)
[38] The "secure" Max messenger came under fire // Tproger. URL: https://tproger.ru/news/-bezopasnyj--messendzher-max-okazalsya-pod-ognem-kritiki ("Безопасный" мессенджер Max оказался под огнем критики // Tproger)
[39] An expert warned of a possible blocking of WhatsApp // Moskovsky Komsomolets. URL: https://www.mk.ru/social/2025/08/12/ (Эксперт предупредил о возможной блокировке WhatsApp // Московский комсомолец)

Play, and others. Apple invoked sanctions legislation without specifying particular grounds; VK called the actions unilateral and stated that it had never appeared on any sanctions lists, while the Ministry of Digital Development complained to the Federal Antimonopoly Service about unfair competition.[40]

Formally, VK is right: the company itself is not on the OFAC, EU, or UK lists. But sanctions regimes work not only through direct inclusion on a list but also through the principles of ownership and control — OFAC's 50 percent rule and its British analog, under which a structure controlled by sanctioned persons is itself subject to sanctions. By these principles, VK's position is different. The holding's CEO, Vladimir Kiriyenko (son of the deputy head of the Presidential Administration, Sergei Kiriyenko), has been under US personal sanctions since February 2022. A majority of the votes in VK are controlled through JSC MF Technologies: in 2021 Gazprombank bought Sber's stake in this structure and handed it to Gazprom-Media. That is, VK is controlled by a chain closing on sanctioned parties — and by the letter of the control principles, Western corporations should have ceased all cooperation with it.

That is exactly what once happened. In late September 2022, after the UK imposed sanctions on Gazprombank's executives, Apple removed VK's apps from the App Store, and a company representative directly explained that the services are distributed by developers, most of which belong to or are controlled by sanctioned parties. But already in October 2022, Apple returned the apps, and cooperation resumed.[41] The current removal is in essence a return to the consistent application of the same principles, from which they had retreated four years earlier.

The removal, however, remained half-hearted. On the Android side, the VK and MAX apps remain available in Google Play: Google, unlike Apple, did not end its cooperation with the

---

[40] Apple removed VK's apps from the App Store on 25 June 2026, citing sanctions rules; the MAX messenger was removed on 3 June; VK denies being under sanctions, the Ministry of Digital Development complained to the Federal Antimonopoly Service; VK's CEO Vladimir Kiriyenko has been under US sanctions since February 2022. Kommersant, 26 June 2026. https://www.kommersant.ru/doc/8765165 (Apple удалила приложения VK из App Store 25 июня 2026 года, сославшись на санкционные правила; мессенджер MAX удален 3 июня; VK отрицает нахождение под санкциями, Минцифры пожаловалось в ФАС; гендиректор VK Владимир Кириенко под санкциями США с февраля 2022 года. Коммерсантъ, 26 июня 2026.)

[41] Control over the majority of votes in VK through JSC MF Technologies (Gazprombank bought Sber's stake in 2021 and handed it to Gazprom-Media); the removal of VK's apps in September 2022 due to UK sanctions against Gazprombank executives and their restoration in October 2022; the Apple representative's explanation about services being distributed by sanctioned parties. Forbes, 14 October 2022. https://www.forbes.ru/tekhnologii/479753-apple-vernula-zablokirovannoe-v-konce-sentabra-prilozenie-soc seti-vk-v-v-app-store (Контроль над большинством голосов в VK через АО МФ Технологии (Газпромбанк выкупил долю Сбера в 2021 году и передал Газпром-медиа); удаление приложений VK в сентябре 2022 года из-за санкций Великобритании против руководителей Газпромбанка и их восстановление в октябре 2022 года; пояснение представителя Apple о распространении сервисов подсанкционными сторонами. Forbes, 14 октября 2022.)

holding.[42] The same set of facts about ownership and control is interpreted in opposite ways by two American corporations — which only underscores how the application of sanctions principles to VK remains a matter of corporate decision rather than an automatic consequence of the law.

Hidden here, too, is the reverse causal link that explains the entire campaign against messengers in the next chapter. Had Apple and Google from the outset consistently applied the control principles and removed MAX and VK from their stores, the state would have been left with no national messenger for whose sake it was worth clearing the market. There would simply be nothing to promote — and then blocking WhatsApp and Telegram would lose its point: there is no reason to herd an audience by force into a service that is not in the stores. It was precisely the corporations' willingness (above all Google, and until June 2026 Apple as well) to keep hosting and updating MAX that made betting on it realistic — and therefore made the very blocking of its competitors meaningful. In other words, the blocking of WhatsApp and Telegram became possible not despite but because Western platforms kept MAX and VK in their stores all those months.

Chapter 5. The strangling of WhatsApp and Telegram

The campaign against Telegram and WhatsApp — the last two mass independent messengers in Russia — unfolded in stages, moving from the targeted degradation of individual functions (for example, blocking calls) to effectively closing off access to the apps. Officially these restrictions were justified by rhetoric about fighting phone fraud and spam. But behind that screen lay the Kremlin's obvious desire to fully clear the information field of uncontrolled communication channels and to forcibly move the Russian audience to the state-approved Max messenger.

1. The assault on calls (August 2025)

In August 2025, mass failures of voice and video calls began. On 13 August, RKN officially confirmed the "partial restriction" of calls in Telegram and WhatsApp, explaining it as a fight against fraud and against drawing citizens into "sabotage and terrorist activity."[43] Technically the restriction was implemented primarily through the TSPU infrastructure, aimed at VoIP traffic.[44]

---

[42] At the time of the removal of VK's apps from the App Store, they remained available for Android in Google Play, RuStore, Huawei AppGallery, and other stores. CNews, 25 June 2026. https://zoom.cnews.ru/news/item/694702 (На момент удаления приложений VK из App Store они оставались доступны для Android в Google Play, RuStore, Huawei AppGallery и других магазинах. CNews, 25 июня 2026.)

[43] RKN confirmed the restriction of calls in Telegram and WhatsApp // RBC. URL: https://www.rbc.ru/politics/13/08/2025/689c8c7c9a79479b1087586d (РКН подтвердил ограничение звонков в Telegram и WhatsApp // РБК)

[44] How RKN restricts calls in messengers // RBC. URL: https://www.rbc.ru/technology_and_media/13/08/2025/689cab709a7947a32eb24afb (Как РКН

The blow aimed specifically at calls looked calculated: voice communication in messengers was in massive demand and considered secure. By undermining it, the authorities simultaneously reduced the value of the services and created demand for a domestic alternative.

2. Blocking WhatsApp

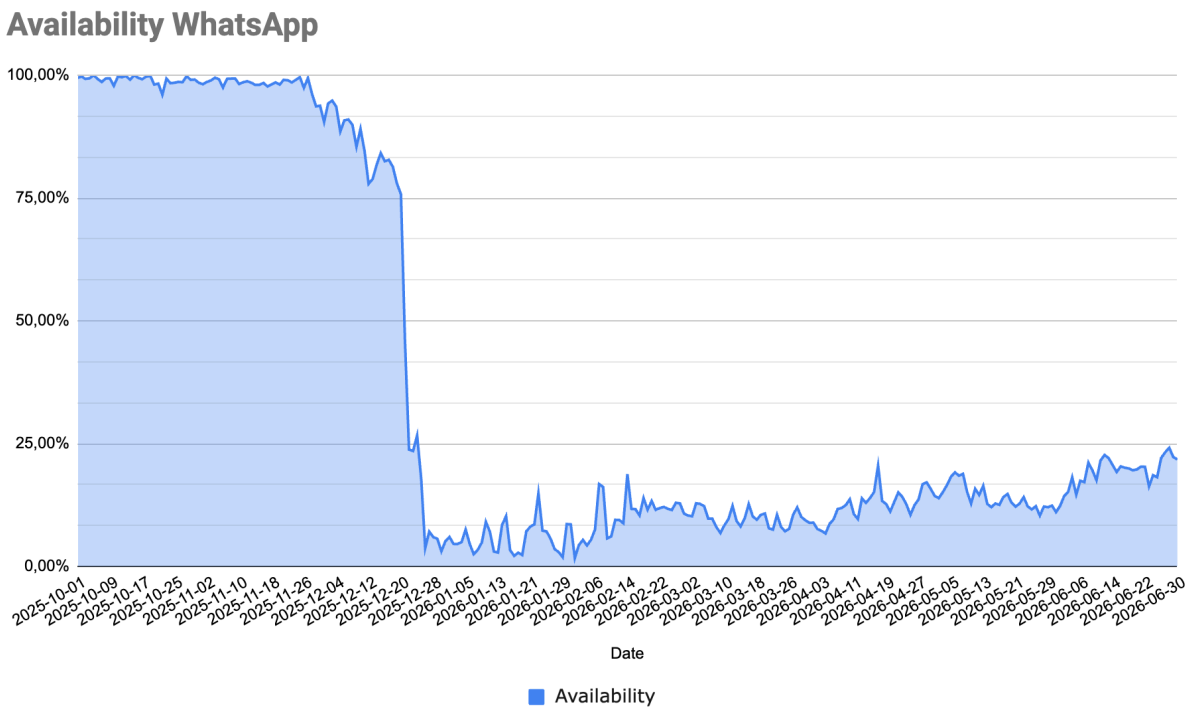
The restrictions that began in August 2025 with the blocking of calls in WhatsApp and Telegram grew by autumn into problems accessing the messengers themselves. The failures began on 20–21 October in southern regions, and by 22 October had spread to dozens of regions, including Moscow and Saint Petersburg; on the same day, RKN again acknowledged a "partial restriction" of WhatsApp and Telegram. Many observers agreed that the true goal was to move the audience to Max.[45]

In December 2025 the pressure intensified: according to RBC, WhatsApp's speed was reduced by 70–80%, and RKN allowed for the possibility of a full block of the service.[46] Also in December, Snapchat, FaceTime, and the gaming platform Roblox came under restriction.[47]

The chronology of this transition is vividly captured by the WhatsApp availability chart (OONI data). Until the end of November 2025 the figure held at 100%, fluctuating within the usual statistical noise. On 1 December, availability dropped below 90% for the first time — that is, it went beyond those fluctuations — the first measurable sign of deliberate degradation rather than random failures. Then, over three weeks, came a steady decline — that same 70–80% throttling phase: on 21 December availability fell below 50%, and on 25 December the service was effectively blocked, the figure collapsing below 10%.

Chart 3. Blocking of WhatsApp, availability chart

ограничивает звонки в мессенджерах // РБК)
[45] Partial blocking of Telegram and WhatsApp in Russia // Wikipedia. URL: https://ru.wikipedia.org/wiki/Частичная_блокировка_Telegram_и_WhatsApp_в_России (Частичная блокировка Telegram и WhatsApp в России // Википедия)
[46] WhatsApp throttled by 70–80% in Russia // E1. URL: https://www.e1.ru/text/world/2025/12/24/76185979/ (В России замедлили WhatsApp на 70–80% // E1)
[47] What was blocked in Russia in December 2025 // Novaya Gazeta Europe. URL: https://novayagazeta.eu/articles/2025/12/29/ (Что заблокировали в России в декабре 2025 // Новая газета Европа)



The very shape of the curve is characteristic: this is not an instant shutdown but a controlled descent from throttling to blocking, stretched over almost a month. Such a drawn-out course is explained by the design of the filtering system. TSPU equipment is installed at operators across the whole country, in different regions, and cannot be switched over all at once — the rollout of any new block goes gradually, node by node. Moreover, shutting off a service with an audience of about 97 million users[48] risks unpredictable consequences, so an abrupt cutoff is dangerous. RKN and its subdivision TsMU SSOP worked out a cautious tactic back during the throttling of YouTube: a block is rolled out in stages, starting, apparently, with segments carrying the least traffic and gradually spreading to the rest.

After 25 December, availability did not fall to zero but settled below 10%. Bringing the block all the way down to zero cannot be done for a structural reason: Russia has "too many" telecom operators, and TsMU SSOP does not control every node with equal density. Part of the traffic continues to pass through circumvention tools, part through routing incidents, when routes leak around the TSPU by mistake or on purpose. From early June 2026 a gradual rise is noticeable on the chart: by the end of the month availability climbed to roughly 20–25%. This reflects not a softening of policy but an adaptation of circumvention tools, which by the summer of 2026

[48] Per Mediascope (Group4Media study), in August 2025 WhatsApp's monthly reach in Russia exceeded 97 million unique users. Kommersant, 22 September 2025. https://www.kommersant.ru/doc/8058240 (По данным Mediascope (исследование Group4Media), в августе 2025 года месячный охват WhatsApp в России превысил 97 млн уникальных пользователей. Коммерсантъ, 22 сентября 2025.)

managed to partially restore the connection.

3. Blocking Telegram

On 10 February 2026, RKN officially announced the throttling of Telegram nationwide, citing non-compliance with Russian legislation.[49] On 16 March, the Tagansky Court in Moscow fined Telegram 35 million rubles for refusing to remove prohibited content.[50]

About two months passed between the official statement on 10 February and the actual blocking in April — and this was not a technical pause but a time of open dispute within the loyalist milieu itself. The throttling of Telegram provoked an unusually broad wave of criticism: those who spoke out against it included servicemen and Z-war-correspondents, State Duma deputies, pro-government propagandists, and members of the clergy. The leader of A Just Russia, Sergei Mironov, called the initiative's authors "idiots," and the military argued that the restrictions hit frontline communications, for which Telegram remained a key channel.[51] Displeasure was also voiced by Vladimir Solovyov, who lost part of his audience after the throttling; analysts called what was happening the first noticeable split in pro-Kremlin communities.[52] The authorities' reaction was half-hearted: the Kremlin publicly downplayed the concerns, and the Ministry of Digital Development promised not to throttle the messenger "in the special-operation zone."[53]

Chart 4. Blocking of Telegram, availability chart

---

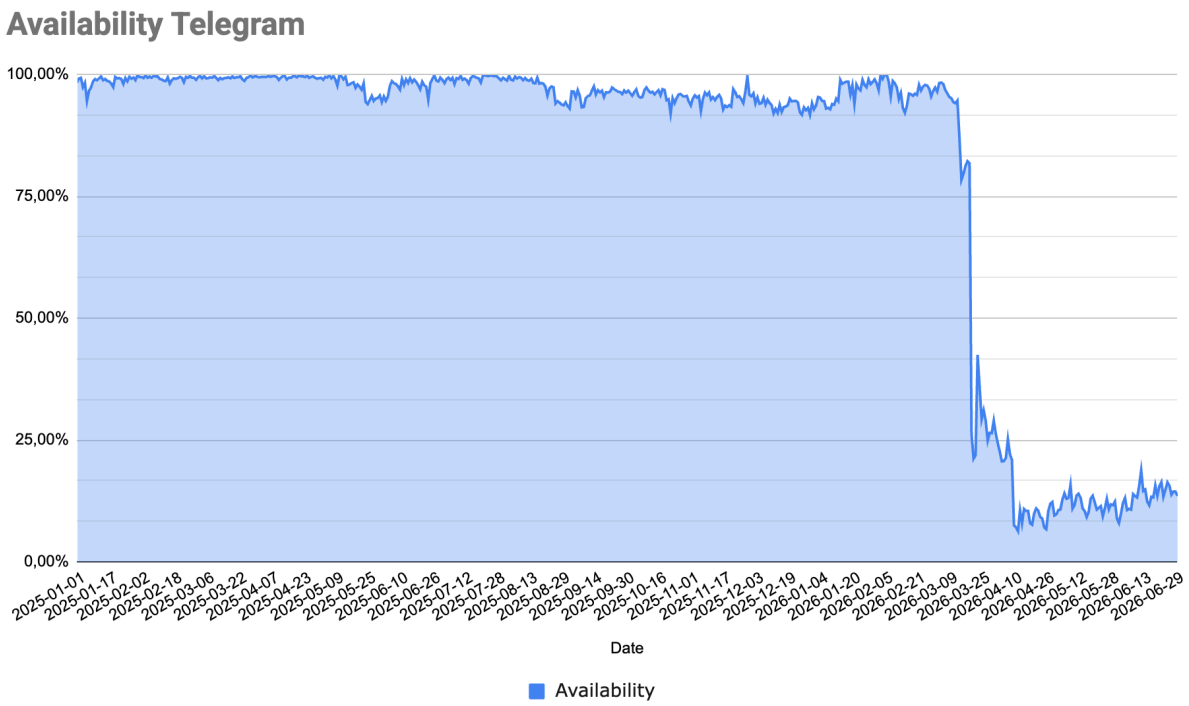
[49] RKN began throttling Telegram across Russia // RBC. URL: https://www.rbc.ru/technology_and_media/10/02/2026/698afe729a79470c08a17b91 (РКН начал замедлять Telegram по всей России // РБК)

[50] The Tagansky Court in Moscow fined Telegram 35 million rubles (five episodes under Part 4 of Art. 13.41 of the Administrative Offenses Code) for refusing to remove prohibited content, 16 March 2026 // Forbes. URL: https://www.forbes.ru/society/557296-sud-v-moskve-ostrafoval-telegram-ese-na-35-mln-rublej (Таганский суд Москвы оштрафовал Telegram на 35 млн рублей (пять эпизодов по ч. 4 ст. 13.41 КоАП) за отказ удалять запрещённый контент, 16 марта 2026 // Forbes)

[51] The Russian authorities keep breaking Telegram and WhatsApp: criticism from Z-bloggers and State Duma deputies, Mironov called RKN "idiots." Meduza, 14 February 2026. https://meduza.io/feature/2026/02/14/rossiyskie-vlasti-prodolzhayut-lomat-telegram-i-votsap (Российские власти продолжают ломать телеграм и вотсап: критика Z-блогеров и депутатов Госдумы, Миронов назвал РКН "идиотами". Meduza, 14 февраля 2026.)

[52] The blocking of Telegram caused the largest split in the camp of pro-Kremlin propagandists (Solovyov; assessment by Tatiana Stanovaya). The Moscow Times, 17 February 2026. https://ru.themoscowtimes.com/2026/02/17/kreml-shokiroval-provoennih-propagandistov-blokirovkoi-telegram-a187503 (Блокировка Telegram вызвала крупнейший раскол в лагере прокремлевских пропагандистов (Соловьев; оценка Татьяны Становой). The Moscow Times, 17 февраля 2026.)

[53] The authorities promised not to throttle Telegram in the "special-operation zone" after criticism from the military and Z-war-correspondents; Peskov downplayed the concerns. The Moscow Times, 18 February 2026. https://ru.themoscowtimes.com/2026/02/18/vlasti-poobeschali-nezamedlyat-telegram-vzone-svo-posle-kritiki-voennih-iz-voenkorov-a187582 (Власти пообещали не замедлять Telegram в "зоне СВО" после критики военных и Z-военкоров; Песков преуменьшил опасения. The Moscow Times, 18 февраля 2026.)



How that discussion ended is shown by the very fact of the block. Neither the military's objections, nor the propagandists' complaints, nor the arguments about frontline communications outweighed the outcome — Telegram was blocked anyway. That means the dispute was once again won by the security bloc, apparently by the FSB's Second Service, responsible for protecting the constitutional order, for which control over a channel of mass communication proved more important than the costs the loyalists pointed to.

Independent measurements not only confirm the degradation but also make it possible to date its phases. Throughout 2025 and in the first weeks of March 2026, Telegram's availability held near the 100% mark, staying within ordinary statistical fluctuations. On 15 March the figure fell below 80% for the first time — the first move beyond the noise; that same day OONI recorded an anomaly share of about 21%, and by 16 March the share of failed requests to the messenger's domains averaged almost 80%.[54] On 20 March availability collapsed to roughly 26%, after which came a partial rollback — a brief softening characteristic of a stepwise and reversible rollout of restrictions. The decisive collapse came on 10 April: availability fell below 10%, the share of failed requests approached 100%, and OONI anomalies reached 95% — higher than for WhatsApp and Signal.[55] For comparison: WhatsApp had been unavailable in

[54] A sharp deterioration in Telegram's availability in Russia // Verstka. URL: https://verstka.media/rezkoe-uhudshenie-dostupnosti-telegram-v-rossii (Резкое ухудшение доступности Telegram в России // Верстка)
[55] Chronicle of the Telegram block // Xakep. URL: https://xakep.ru/2026/05/04/telegram-chronicle/ (Хроника блокировки Telegram // Xakep)

more than 85% of measurements since at least 17 February.

After 10 April, availability did not fall to zero but settled below 10% with a subsequent slow rise — the chart shows a gradual recovery by the summer of 2026 thanks to the adaptation of circumvention tools. The scale of this adaptation was acknowledged by Telegram itself: according to Pavel Durov, by April 2026 about 65 million Russians used the messenger daily via VPN, and more than 50 million sent messages every day.[56]

Precision of wording matters here. Officially RKN nowhere announced a "full block" of Telegram — only "throttling" and "partial restriction" due to a violation of the law. Reports of an imminent full block "in early April" came from anonymous sources in the agencies, cited by RBC, and not from any published normative act.[57] Yet the actual result — the impossibility of using the service normally — was achieved by technical means, as with YouTube two years earlier. The shape of the curve confirms this: not a one-off shutdown by order, but a controlled degradation with a throttling phase, a collapse, a rollback, and settlement at a low level. To grasp the scale: over 2025 Telegram itself blocked 44 million channels and groups, 2.7 times more than a year earlier.[58]

Chapter 6. Blocking the circumvention protocols

While the campaign against messengers was underway, a new phase of the fight against VPNs was unfolding on the technical front. If in 2023 the TSPU learned to recognize the classic protocols (OpenVPN, WireGuard, IPsec), then in 2025–2026 the next-generation protocols, specially designed to disguise themselves as ordinary traffic, came under fire.

1. The end of the "invisible" protocols

By the end of 2025 the TSPU had achieved practically full network coverage, and the total load on the system was estimated at tens of terabits per second.[59] On this base RKN moved to detecting the VLESS, REALITY, XTLS, and Shadowsocks protocols, which had previously been considered resistant to blocking.

---

[56] According to Pavel Durov (April 2026), about 65 million Russians use Telegram daily via VPN, more than 50 million send messages every day // The Insider. URL: https://theins.ru/news/291084 (По заявлению Павла Дурова (апрель 2026), около 65 млн россиян ежедневно используют Telegram через VPN, более 50 млн отправляют сообщения каждый день // The Insider)
[57] The blocking of Telegram and WhatsApp in Russia // Wikipedia. URL: https://ru.wikipedia.org/wiki/Блокирование_Telegram_и_WhatsApp_в_России (Блокирование Telegram и WhatsApp в России // Википедия)
[58] In 2025 Telegram blocked 44.085 million channels and groups — almost 2.7 times more than in 2024 // TASS. URL: https://tass.ru/ekonomika/26125941 (Telegram за 2025 год заблокировал 44,085 млн каналов и групп — почти в 2,7 раза больше, чем в 2024 году // ТАСС)
[59] How RKN blocks VLESS and other protocols // Habr. URL: https://habr.com/ru/news/973082/ (Как РКН блокирует VLESS и другие протоколы // Habr)

On 24 November 2025 the first reports appeared of testing the blocking of VLESS and the XRay toolkit — complaints came from Krasnoyarsk, Novosibirsk, Yekaterinburg, Kazan, Volgograd. The blow fell on the transport layer, which is why legitimate services on ordinary TLS suffered too.[60] By the end of November the complaints spanned more than a dozen regions, and in December RKN, having updated the TSPU, began blocking SOCKS5, VLESS, and L2TP. This was confirmed by independent specialists, including Igor Bederov and Alexei Uchakin.[61]

2. How the detection works

The fundamental difference of the new phase is that the system stopped relying on signatures alone. According to specialists' analyses, the detection is built in several layers working simultaneously:

1. Signature analysis of the connection's first bytes. The simplest layer: characteristic sequences at the start of a session make it possible to recognize and immediately cut off plain Shadowsocks, OpenVPN, and other protocols with a recognizable handshake.[62]
2. Fingerprinting of the TLS handshake (JA3/JA4). The system takes a fingerprint of the TLS parameters and distinguishes a non-standard client from an ordinary browser's handshake, even if the content is encrypted.
3. Active probing. RKN's servers (or those of its contractors) connect to a suspicious server and check whether it behaves like a real website or like a proxy that answers only to the correct key.
4. Analysis by IP, subnet, and reputation. Connections to the subnets of known foreign hosting providers (Hetzner, DigitalOcean, OVH) are considered suspicious; with a poor reputation, entire data-center subnets are blocked rather than individual addresses.
5. Behavioral (statistical) traffic analysis. By content, VLESS is indistinguishable from ordinary HTTPS, so it is worked out from indirect markers: requests to foreign data-center IP addresses, a mismatch between SNI and the real source, and atypical patterns in the volume, direction, and rhythm of traffic.
6. The "16 KB veil." A connection is dropped after the first 15–20 kilobytes if it is established with the subnet of a known foreign hosting provider.[63]

This is precisely the implementation of that very "statistical method" the first part described as a hypothesis: the system does not break the encryption but works out the VPN user from the shape of their network behavior.

---

[60] RKN began testing the blocking of VLESS // Meduza. URL: https://meduza.io/news/2025/11/24/ (РКН начал тестировать блокировку VLESS // Meduza)
[61] RKN blocks VLESS, SOCKS5, and L2TP // Xakep. URL: https://xakep.ru/2025/12/05/rnk-vless/ (РКН блокирует VLESS, SOCKS5 и L2TP // Xakep)
[62] How the TSPU detect circumvention protocols // Habr. URL: https://habr.com/ru/articles/1009542/ (Как ТСПУ детектируют протоколы обхода // Habr)
[63] A memo on the blocks // Dept.one. URL: https://dept.one/memo/blokirovky/ (Памятка по блокировкам // Dept.one)

3. The blocking industry: procurement and capacity

Behind the technical escalation stands not an abstract "Roskomnadzor" but a built-out industry with its own contractor and budgets. The key integrator of sovereign-internet systems and supplier of TSPU is JSC DTsOA (Data — Center for Processing and Automation), created in 2019 under the sovereign-Runet law and controlled by Rostelecom through the special company Gradient. The same structure also owns JSC RDP.RU, a key developer of blocking systems, and received about 12 billion rubles in recapitalization and loans.[64]

In June 2026 DTsOA announced the procurement of at least 154 Russian servers for 1.31 billion rubles. Their specifications show the direction of development: two Intel Xeon Gold processors of the Emerald Rapids generation per server, at least 1 TB of DDR5 memory, PCIe 5.0 with enough lanes to install a GPU. The latter points directly to preparation for filtering traffic by machine-learning means. At the same time, the servers are required to be Russian-made per the Ministry of Industry and Trade registry — but assembled on imported Intel processors, since there is nothing in domestic components to set against them in performance.

This procurement also explains the flip side of the system — why the blocks do not reach 100%. Deep-filtering capacity is chronically insufficient: traffic volume grows, circumvention methods grow more complex, and when the TSPU cannot cope, bypass mode kicks in — traffic goes straight through, past the filter. That is precisely why in mid-March 2026 some blocked resources temporarily started working again. In response, RKN intensified pressure on operators: from late 2025 to spring 2026 dozens of companies received large fines for letting part of their traffic bypass the TSPU. The agency itself, meanwhile, denied any capacity problems.

The scale of the plan is visible from the financing plans. TSPU capacity is to grow 2.5 times by 2030, with about 84 billion rubles earmarked for the federal project, and the system's target throughput is 954 Tbit/s (for comparison: the average traffic of the entire Runet in 2024 was estimated at roughly 30 Tbit/s). By the end of 2026 the plan is to pass all Russian users' traffic through the system. Separately, about 40 billion rubles is allocated to RKN structures, including for the fight against VPNs, and a filtering system based on machine learning is supposed to help detect both prohibited content and circumvention tools.

4. Purging the app stores

In parallel came an assault on the very channel for distributing circumvention tools. Demand,

[64] The company responsible for Runet blocking is preparing to expand: DTsOA (Rostelecom) is procuring at least 154 servers for 1.31 billion rubles based on Intel Xeon Gold; ownership structure (Gradient, RDP.RU); capacity shortage, bypass mode, fines to operators for bypassing the TSPU. CNews, 9 June 2026. https://www.cnews.ru/news/top/2026-06-09_glavnyj_integrator_filtratsii (Компания, отвечающая за блокировки Рунета, готовится к расширению: ДЦОА (Ростелеком) закупает не менее 154 серверов на 1,31 млрд рублей на базе Intel Xeon Gold; структура собственности (Градиент, РДП.РУ); дефицит мощностей, режим bypass, штрафы операторам за обход ТСПУ. CNews, 9 июня 2026.)

meanwhile, only grew: as of March 2026 the number of downloads of the top-5 VPN services in Google Play had grown 14 times in a year, to 9.2 million, and over March 2025 – March 2026 a total of 35.7 million downloads were recorded.[65] Pressure on the app stores mounted throughout the period. Over 2025, Apple removed more than 1,200 apps from the Russian App Store at the demand of the Russian authorities, predominantly VPN services.[66] By mid-January 2026, RKN had restricted access to 439 VPN services — 70% more than in October 2025.[67] On 28 March 2026, more than two dozen popular VPN clients (v2RayTun, Streisand, Happ, and others) were removed from the App Store at once, which Pavel Durov publicly criticized.[68]

5. The race goes on

On 17 February 2026 the blocking of VLESS sharply intensified and covered more regions and providers. The circumvention community responded by moving to new transports — VLESS over XHTTP and gRPC, and the Hysteria2 and AmneziaWG protocols.[69] The "block — circumvent — block the circumvention" cycle described in the first part reached a new turn: it now runs not at the level of individual services but at the level of fundamental transport protocols.

6. VPN penetration: model and data

The exact number of VPN users in Russia is unknown — it cannot be judged from the number of downloads, since one person installs several apps and an install does not equal use.

---

[65] Plans to build up TSPU capacity (2.5-fold growth by 2030, about 84 billion rubles, target of 954 Tbit/s), allocation of about 40 billion rubles to RKN structures for the fight against VPNs, a machine-learning-based filtering system; a 14-fold year-on-year rise in VPN downloads (Digital Budget data). CNews, 9 June 2026. https://www.cnews.ru/news/top/2026-06-09_glavnyj_integrator_filtratsii (Планы по наращиванию мощности ТСПУ (рост в 2,5 раза к 2030 году, около 84 млрд рублей, целевые 954 Тбит/с), выделение около 40 млрд рублей структурам РКН на борьбу с VPN, система фильтрации на базе машинного обучения; рост числа скачиваний VPN в 14 раз год к году (данные Digital Budget). CNews, 9 июня 2026.)

[66] Apple removed more than 1,200 apps from the Russian App Store // Meduza. URL: https://meduza.io/video/2026/05/26/ (Apple удалила более 1200 приложений из российского App Store // Meduza)

[67] Pavel Durov criticized Apple for blocking VPNs // Expert. URL: https://expert.ru/news/pavel-durov-raskritikoval-apple-za-blokirovku-vpn (Павел Дуров раскритиковал Apple за блокировку VPN // Эксперт)

[68] Apple removed popular VPN apps at RKN's demand // Forbes Russia. URL: https://www.forbes.ru/tekhnologii/558320 (Apple удалила популярные VPN-приложения по требованию РКН // Forbes Россия)

[69] Roskomnadzor intensified the blocking of VLESS on 17 February 2026 (coverage of regions and providers grew); the community moved to XHTTP/gRPC, Hysteria2, and AmneziaWG // The Moscow Times. URL: https://ru.themoscowtimes.com/2026/02/17/roskomnadzor-usilil-blokirovku-odnogo-iz-populyarnih-vpn-protokolov-a187470 (Роскомнадзор усилил блокировку VLESS 17 февраля 2026 (охват регионов и провайдеров вырос); сообщество перешло на XHTTP/gRPC, Hysteria2 и AmneziaWG // The Moscow Times)

Therefore the chart below is built as an estimative model: the dynamics of search interest by Google Trends and Yandex Wordstat serve as a leading indicator, calibrated against survey data. The chart has three series: search interest (Google Trends, blue line, normalized so that 100 points is the maximum over the whole period), the estimated number of users in millions (red line), and the penetration level in percent (yellow bars).

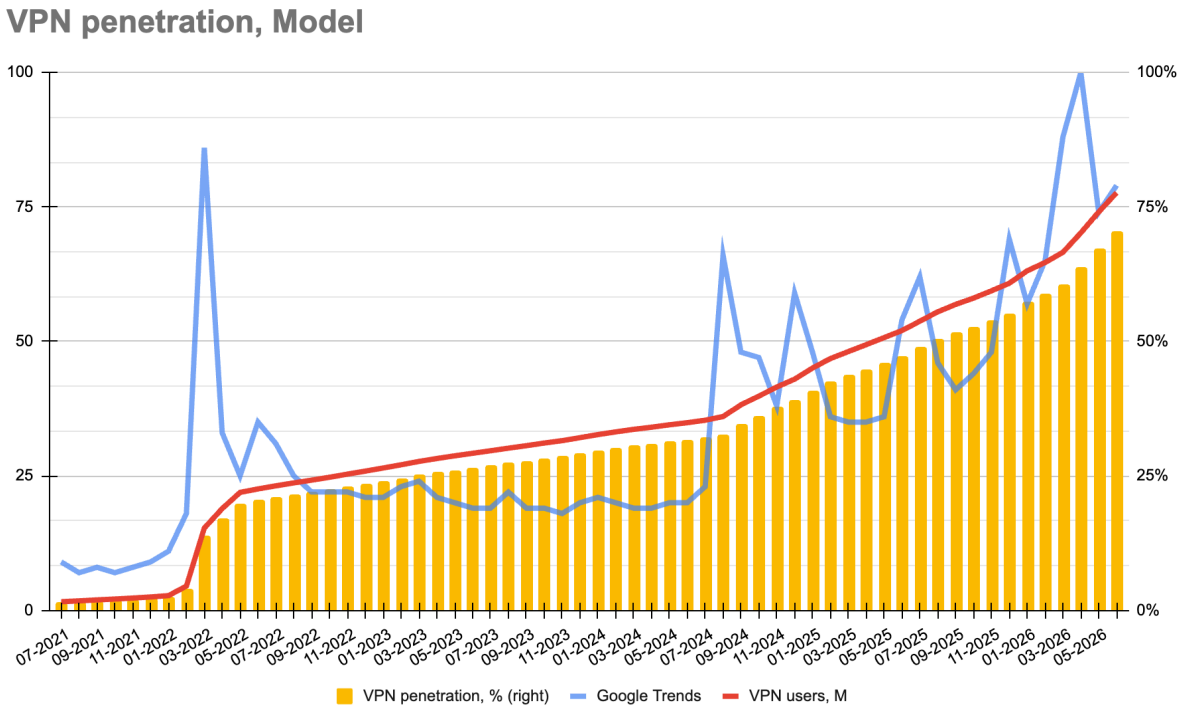
The methodology of the calculations: the starting point is the estimate of the number of VPN users before the war — on the order of 1.6 million people in February 2022; after the blocking of social networks this figure grew about fifteenfold within a few months, to 24 million by May 2022.[70] From there the base is built up month by month: the increment for each month is computed from the dynamics of search queries (Google Trends and Yandex Wordstat) multiplied by an empirically fitted coefficient. Direct addition is inadmissible here — one cannot simply add the number of queries to the number of users, because the same person searches for a circumvention method many times, and a surge in queries only partly converts into new users. The coefficient is calibrated against independent audience estimates on various dates: besides the 2022 points, it uses Levada Center data for March 2024, according to which roughly a quarter of Russians used a VPN at least occasionally,[71] and a Russian Field survey for April 2026 with 40% active users.[72] Between these anchor points the curve is interpolated from the search signal.

[70] Before the war, about 1.6 million Russians used a VPN (February 2022); after the blocking of social networks the number grew about 15-fold, to 24 million by May 2022. Radio Svoboda, 7 June 2022. https://www.svoboda.org/a/chislo-poljzovateley-vpn-vyroslo-v-15-raz-s-nachala-voyny/31886155.html (До начала войны VPN пользовались около 1,6 млн россиян (февраль 2022); после блокировки соцсетей число выросло примерно в 15 раз, до 24 млн к маю 2022 года. Радио Свобода, 7 июня 2022.)

[71] Per Levada Center data (March 2024), about a quarter of Russians use a VPN at least occasionally. Levada Center, 14 June 2024. https://www.levada.ru/en/2024/06/14/the-audience-of-internet-users-social-networks-messengers-and-vpn-services/ (По данным Левада-центра (март 2024), VPN хотя бы иногда пользуется около четверти россиян. Левада-центр, 14 июня 2024.)

[72] Russian Field survey (15–22 April 2026, 1,600 respondents): 40% of Russians actively use a VPN, 74% are aware of the technology, in Moscow 62%, in Saint Petersburg 58%. SecurityLab, 6 May 2026. https://www.securitylab.ru/news/572416.php (Опрос Russian Field (15–22 апреля 2026, 1600 респондентов): 40% россиян активно пользуются VPN, 74% осведомлены о технологии, в Москве — 62%, в Санкт-Петербурге — 58%. SecurityLab, 6 мая 2026.)

Chart 5. Google Trends and VPN penetration



The chart divides into three characteristic periods, and each coincides with a major wave of blocking.

The first sharp spike is March 2022, the blocking of social networks after the start of the war, primarily Instagram. Search interest soars to nearly 90 points. It is from this moment that the previously gentle red line changes its angle and begins to rise confidently, dragging the penetration percentages along with it. After the peak, search interest subsides, but the user base does not roll back: it holds a plateau until mid-2024.

The second series of waves is July 2024 – July 2025, the throttling and blocking of YouTube. In the summer of 2024 the blue line rises again (to about 68 points), followed by new spikes in the autumn of 2024 and early 2025. Against this backdrop, the growth of the real base accelerates: the red line crosses the 50-million mark, and penetration passes 50%.

The third period is spring 2026, the blocking of Telegram. Search interest reaches 100 points, the maximum of the whole scale, after which it rolls back to about 80 by summer. This spike takes consumption to a new level: by June 2026 the estimated number of users approaches 70 million, and penetration approaches 65–68%.

The model is confirmed by independent data. According to a Russian Field survey (April 2026), 40% of Russians actively use a VPN, 74% are aware of the technology, and in Moscow the

share of users reaches 62%; among citizens aged 18–45, more than half reported regular use.[73] Earlier measurements give the same order of magnitude and the same unidirectional dynamics: about a third per Levada Center data and 46% per the Institute of Social Marketing acknowledged having used a VPN at least once. The model's leading indicator is verified too: in March 2026 the number of VPN search queries grew about 3.3 times year-on-year, with Yandex Wordstat and Google Trends showing a consistent picture, and peak values comparable to the level of spring 2022.[74]

The model's general conclusion is simple: short-term triggers form a long-term habit. As soon as the media noise around each new wave of blocking dies down and the blue line goes down, the red line and the yellow bars do not return to their former values — they move only upward. Each new block does not shrink the circumvention audience but expands it, entrenching the VPN as an everyday tool for the majority of users. Herein lies the structural paradox of the policy: the fight against circumventing blocks itself acts as the main driver of its spread.

Chapter 7. Controlling the perimeter

The technical measures against VPNs were supplemented by legal and administrative ones — and the state shifted part of the censorship work onto users themselves, onto business, and onto infrastructure. In parallel, control was extended over the entire chain: who publishes, who advertises, where content is hosted, and who even goes online at all.

1. Punishment for searching for extremism (281-FZ)

On 31 July 2025, Federal Law No. 281-FZ was signed, coming into force on 1 September 2025.[75] It introduced into the Administrative Offenses Code an article on fines for deliberately searching for "knowingly extremist materials" from the Justice Ministry's registry, including with

---

[73] The country of the victorious VPN: per Russian Field for April 2026, more than 50% of Russians aged 18–45 use a VPN; a review of estimates (Levada Center, Institute of Social Marketing) and RKN's targets for blocking effectiveness. Carnegie, 28 May 2026. https://carnegieendowment.org/ru/russia-eurasia/politika/2026/05/russia-vpn-usage-political (Страна победившего VPN: по данным Russian Field на апрель 2026 года более 50% россиян 18–45 лет пользуются VPN; обзор оценок (Левада-центр, Институт социального маркетинга) и цели РКН по эффективности блокировок. Carnegie, 28 мая 2026.)

[74] In March 2026 search interest in VPNs reached a five-year record (Google Trends — 100 points); Yandex Wordstat data is consistent with Google Trends, comment by M. Klimarev // The Moscow Times. URL: https://ru.themoscowtimes.com/2026/03/30/rossiyane-postavili-rekord-po-zaprosam-o-vpn-v-google-a191239 (В марте 2026 года поисковый интерес к VPN достиг пятилетнего рекорда (Google Trends — 100 баллов); данные Яндекс Вордстат согласуются с Google Trends, комментарий М. Климарёва // The Moscow Times)

[75] A law on fines for searching for extremist materials was signed // Pravo.ru. URL: https://pravo.ru/news/259848/ (Подписан закон о штрафах за поиск экстремистских материалов // Pravo.ru)

the use of a VPN: for citizens, from 3,000 to 5,000 rubles. By the time the law came into force, the registry held over 5,400 entries; the head of the Ministry of Digital Development stressed that punishment would apply only to deliberate viewing, and that proving intent was a task for law enforcement.[76]

The same package sharply tightened liability for advertising circumvention tools: fines for advertising VPNs came to between 50,000 and 80,000 rubles for citizens, up to 150,000 for officials, and up to 500,000 for legal entities (up to a million for a repeat offense).[77] A separate law made the use of a VPN in the commission of a crime an aggravating circumstance.

The fundamental novelty here is the shift in the object of repression: it became punishable not only to distribute the prohibited but the very act of a user searching for information — for the first time, liability is transferred to the end consumer of content.

In practice, however, the article did not see mass application. Despite the law being in force since 1 September 2025 and the Justice Ministry's registry holding over 5,400 entries, in all that time there is essentially only one known case of actual punishment. In December 2025 a justice-of-the-peace court in Kamensk-Uralsky fined 20-year-old Sergei Glukhikh 3,000 rubles — according to the investigation, he had searched in his browser for an image of the Azov battalion's chevron.[78]

The circumstances of this sole case are telling. The initiator was not an automated system but the FSB: the accused, by a security officer's own admission, had long been "on the radar," and the protocol was drawn up on the basis of a report by an unidentified person.[79] The defense pointed out that the Azov chevron stands at number 3,269 on the list of extremist materials — it

---

[76] Fines for searching for extremist materials came into force // RBC. URL: https://www.rbc.ru/society/01/09/2025/68b03edf9a79470b449c7b8e (Штрафы за поиск экстремистских материалов вступили в силу // РБК)

[77] Putin signed a law on fines for advertising VPNs (for citizens, 50–80 thousand rubles) and on recognizing the use of a VPN in the commission of a crime as an aggravating circumstance (Art. 63 of the Criminal Code); both laws dated 31.07.2025, in force from 01.09.2025 // Forbes. URL: https://www.forbes.ru/society/543070-putin-podpisal-zakon-o-strafah-za-poisk-ekstremistskih-materialov-i-reklamu-vpn (Путин подписал закон о штрафах за рекламу VPN (для граждан 50–80 тыс. руб.) и о признании использования VPN при совершении преступления отягчающим обстоятельством (ст. 63 УК); оба закона от 31.07.2025, вступление 01.09.2025 // Forbes)

[78] For the first time in Russia, someone was fined for searching for extremist materials: the justice-of-the-peace court in Kamensk-Uralsky imposed 3,000 rubles on 20-year-old Sergei Glukhikh (Art. 13.53 of the Administrative Offenses Code). RBC, 10 December 2025. https://www.rbc.ru/politics/10/12/2025/6939684f9a7947ac893c161e (В России впервые оштрафовали за поиск экстремистских материалов: мировой суд Каменска-Уральского назначил 3 тысячи рублей 20-летнему Сергею Глухих (ст. 13.53 КоАП). РБК, 10 декабря 2025.)

[79] Case circumstances: the FSB's initiative, the accused had long been "on the radar," a protocol based on a report by an unidentified person; the defense's arguments about the impossibility of establishing intent. Radio Svoboda, 10 December 2025. https://www.svoboda.org/a/v-rf-naznachen-pervyy-shtraf-za-poisk-ekstremistskih-materialov-/33619184.html (Обстоятельства дела: инициатива ФСБ, фигурант давно был "в поле зрения", протокол по обращению неустановленного лица; аргументы защиты о невозможности установить умысел. Радио Свобода, 10 декабря 2025.)

is impossible to remember exactly what is forbidden to search for, and a four-letter query returns both the Sea of Azov and cities. This exposes the norm's built-in contradiction: neither the telecom operator nor RKN technically sees the content of search queries — the TSPU can only block traffic types. Establishing intent, and even learning of the query at all, is possible only through seizing the device and the security services' operational work. Therefore the article works not as an instrument of blanket control but as a selective, demonstrative weapon of pinpoint pressure — a threat addressed to everyone but applied selectively.

2. The Apple tax

To grasp the meaning of this measure, one has to recall how payment in the Apple ecosystem works in Russia. Before 2022, users paid for apps, subscriptions, and iCloud storage with ordinary bank cards. In April 2022, after Visa and Mastercard left, Apple stopped accepting the cards of Russian banks, including Mir — direct card payment became impossible. For the next four years the main channel remained topping up an Apple ID balance from a mobile-phone account: the user went into the App Store profile, specified an amount, and the money was debited from the balance. MTS and Beeline provided this service directly, MegaFon and T2 through partners. Requiring neither foreign cards nor third-party services, this method became widespread.[80]

It was this that was struck. Directly removing VPN apps from the stores, described in the previous chapter, did not stop users definitively, so the authorities came at it from the financial side. Following Shadaev's meeting with telecom operators in late March, from 1 April 2026 MTS, Beeline, MegaFon, and T2 disabled the option to top up an Apple ID balance from a mobile-phone account. The goal was stated outright — to force Apple to return the removed apps by cutting off the company's payment channel in Russia.[81] After the disabling, users were left mainly with Apple gift cards for the Russian region and workarounds involving a change of region and foreign cards.

3. Censorship by corporate hands

The most telling novelty was compelling Russian IT companies to detect and restrict VPN users themselves. In late March – early April 2026, the Ministry of Digital Development held meetings

[80] Since April 2022, after Apple stopped accepting Russian bank cards, topping up from a mobile-phone account became the main way to fund an Apple ID; MTS and VimpelCom (Beeline) provided the service directly, T2 and MegaFon through partners. Forbes, 1 April 2026. https://www.forbes.ru/tekhnologii/558358-kartocnaa-sistema-kak-popolnit-balans-apple-id-bez-ucastia-operatorov-svazi (С апреля 2022 года, после отказа Apple принимать карты российских банков, оплата со счета мобильного телефона стала основным способом пополнения Apple ID; МТС и Вымпелком (Билайн) предоставляли услугу напрямую, Т2 и МегаФон — через партнеров. Forbes, 1 апреля 2026.)

[81] Russians to be banned from paying for Apple services from a phone balance // Meduza. URL: https://meduza.io/cards/rossiyanam-hotyat-zapretit-oplachivat-servisy-apple (Россиянам запретят оплачивать сервисы Apple с баланса телефона // Meduza)

with more than twenty platforms (Sber, Yandex, VK, Wildberries, Ozon, Avito, 2GIS, ivi, and others), distributed a guide on detecting VPNs, and set a deadline for implementing the restrictions — 15 April.[82]

On 15 April 2026, Ozon, Wildberries, Kinopoisk, ivi, Yandex Pay, and a number of other services stopped fully working with a VPN enabled.[83] The mechanism is simple: the app sends the client's IP address to the server and checks it against VPN and proxy databases. A study by the RKS Global project showed that 22 of 30 popular Android apps track VPN use, and most of them transmit this status to their servers.[84]

This is a new turn in the war on VPNs — and probably the most alarming in the entire history of censorship technologies. Before, the state blocked traffic with its own hands, through the TSPU and RKN managers. Now it has delegated the detection to those who are demonstrably better at it: the engineers of Sber, Yandex, or Ozon surpass the operators of the state system in skill, their apps are installed on tens of millions of devices, and they already collect data on clients. The state no longer needs to chase circumvention technologies — it is enough to force those who understand these technologies to work for censorship.

The coercion, moreover, is built on a lever without analog in the history of censorship. For refusing to implement VPN detection, a company faces removal from the whitelists and loss of its IT accreditation.[85] But accreditation is not only tax breaks: it is precisely what gives employees deferral from conscription and a reservation from mobilization, and with its loss the deferral is annulled for all employees at once.[86] That is, failure to meet RKN's requirements turns into a direct threat of sending the company's entire male draft-age staff to war. For the first time, censorship is enforced not by a fine and not by blocking, but by the risk of employees' mobilization: the state coerces business into complicity, staking not profit but the lives of its workers.

---

[82] The Ministry of Digital Development obliged IT companies to detect VPN users // Habr. URL: https://habr.com/ru/news/1018576/ (Минцифры обязало IT-компании выявлять пользователей VPN // Habr)

[83] From 15 April 2026, Ozon, Wildberries, Kinopoisk, ivi, Yandex Pay, and other services stopped working with a VPN enabled at the Ministry of Digital Development's demand // Meduza. URL: https://meduza.io/feature/2026/04/15/krupneyshie-rossiyskie-servisy-perestayut-rabotat-pri-vklyuchennom-vpn-kak-i-trebovalo-mintsifry (С 15 апреля 2026 года Ozon, Wildberries, Кинопоиск, ivi, Яндекс Пэй и другие сервисы перестали работать при включённом VPN по требованию Минцифры // Meduza)

[84] 22 of 30 apps track VPNs: a study // Habr. URL: https://habr.com/ru/articles/1021392/ (22 из 30 приложений отслеживают VPN: исследование // Habr)

[85] The Ministry of Digital Development obliged IT companies to detect VPN users // Habr. URL: https://habr.com/ru/news/1018576/ (Минцифры обязало IT-компании выявлять пользователей VPN // Habr)

[86] State accreditation of an IT company gives employees the right to conscription deferral (Presidential Decree No. 83 of 02.03.2022; rules — Government Resolution No. 490 of 28.03.2022); when accreditation is withdrawn, the right is annulled // GARANT. URL: https://www.garant.ru/consult/military/1717264/ (Государственная аккредитация IT-компании даёт сотрудникам право на отсрочку от призыва (Указ Президента № 83 от 02.03.2022; правила — ПП № 490 от 28.03.2022); при отзыве аккредитации право аннулируется // ГАРАНТ)

For the companies themselves, this also entails direct costs. According to industry analysts, marketplaces' losses from restricting VPN users ran into billions of rubles, and app traffic dipped by a few percent.[87]

4. The ban on advertising on banned platforms

On 7 April 2025, Federal Law No. 72-FZ was signed, coming into force on 1 September 2025: it supplemented Article 5 of the "On Advertising" law with a new Part 10.7 and banned advertising on the resources of undesirable, extremist, and terrorist organizations, as well as on any platforms to which access is restricted in Russia — primarily Instagram and Facebook (Meta is recognized as extremist in Russia), and also X (formerly Twitter). The criteria for what counts as advertising on such resources were fixed by the government in resolution No. 1087 of 24 July 2025.[88]

The ban covers not only direct integrations but any posts with an advertising subtext — posts, stories, reels, reviews, and unboxings, if they show signs of promoting a product; barter and free placement are equated with paid advertising. Liability falls on both the advertiser and the advertising distributor simultaneously. Fines are set under Article 14.3 of the Administrative Offenses Code: for citizens, from 2,000 to 2,500 rubles; for officials and sole proprietors, from 4,000 to 20,000; for legal entities, from 100,000 to 500,000 rubles for each placement.[89] Separately, lawyers point to the risk of criminal prosecution under Article 282.3 of the Criminal Code (financing extremism) if payment for the advertising passes through Meta's structures.[90]

Old posts do not need to be deleted, but actions to redistribute them — reposting, pinning, adding links — are punished on a par with new advertising. This was confirmed by both Roskomnadzor and the Federal Antimonopoly Service.[91]

---

[87] Business losses from restricting VPN users // Forbes Russia. URL: https://www.forbes.ru/biznes/560978 (Потери бизнеса от ограничения VPN-пользователей // Forbes Россия)

[88] The ban on advertising on banned resources (Federal Law No. 72-FZ, Part 10.7 of Art. 5 of the "On Advertising" law, in force from 1 September 2025; criteria — Government Resolution No. 1087 of 24.07.2025) // Garant.ru. URL: https://www.garant.ru/article/1845542/ (Запрет рекламы на запрещенных ресурсах (ФЗ № 72-ФЗ, ч. 10.7 ст. 5 закона "О рекламе", вступление 1 сентября 2025; критерии — ПП № 1087 от 24.07.2025) // Гарант.ру)

[89] Fines for advertising on Instagram and the liability of the advertiser and advertising distributor (Art. 14.3 of the Administrative Offenses Code) // RBC. URL: https://www.rbc.ru/life/news/67e2964c9a794762d0a5ffe3 (Штрафы за рекламу в Instagram и ответственность рекламодателя и рекламораспространителя (ст. 14.3 КоАП) // РБК)

[90] The risk of criminal liability under Art. 282.3 of the Criminal Code when paying for advertising through Meta // Contra Legal Firm. URL: https://contralegal.ru/ru/articles/analitika/instagram-pod-zapretom-kakie-shtrafy-groziat-biznesu-i-kak-minimizirovat-riski (Риск уголовной ответственности по ст. 282.3 УК при оплате рекламы через Meta // Contra Legal Firm)

[91] Advertising posted before 1 September: deletion is not required, but redistribution is a violation // Garant.ru. URL: https://www.garant.ru/article/1845542/ (Реклама, размещенная до 1 сентября: удаление необязательно, но повторное распространение — нарушение // Гарант.ру)

From the first weeks, enforcement became telling — familiar from the norm on searching for extremism: the blow fell not on major advertisers but on individual bloggers, and the charges turned out to be contentious. The first known fine — 30,000 rubles — went to lawyer-blogger Evgenia Tutushkina from Krasnodar for a reel about a hotel with a promo code, posted back in the summer of 2025; formally she was punished for the absence of labeling, but publicly it became a precedent of punishment for advertising on a banned network.[92] The first case under the new ban itself was opened by the Omsk antimonopoly office on 22 October 2025 against influencer-producer Asya Sivokoneva (21,000 subscribers): the pretext was an ironic clip of a cosmetics unboxing titled "All bloggers after 1 September," in which brands were mentioned without being named directly. They decided to fine her twice — both as advertiser and as advertising distributor.[93]

The economic sense of the ban is transparent: it hits the revenue base of uncontrolled platforms and redirects advertising budgets to domestic services — VK, Rutube, Dzen. As new services were blocked, the restriction extended to them as well. On 5 March 2026, the antimonopoly service recognized advertising on Telegram and YouTube as a violation, citing the access restrictions introduced by Roskomnadzor. However, already on 25 March, after a negative market reaction, the agency announced a transition period for these two platforms: until the end of 2026, liability measures for advertising on them would not be applied. The reprieve does not extend to Instagram, Facebook, and VPN services — there the ban is in full force.[94]

5. Regulation of hosting providers

The registry of hosting providers, inclusion in which is required to provide services in Russia, has been in effect since 1 February 2024; Roskomnadzor began compiling it in December 2023.[95] By April 2026 it listed about 566 organizations.[96] The conditions for staying in the registry are strict: client identification, connection to the state GosSOPKA system, installation of

---

[92] The first fine for advertising on Instagram — blogger Evgenia Tutushkina, 30 thousand rubles // Forbes. URL: https://www.forbes.ru/forbeslife/548314-v-rossii-vpervye-naznacili-straf-za-reklamu-v-instagram (Первый штраф за рекламу в Instagram — блогер Евгения Тутушкина, 30 тыс. рублей // Forbes)
[93] The first FAS case under the new ban — blogger Asya Sivokoneva, Omsk FAS office, case No. 055/05/18.1-1292/2025 // ADPASS. URL: https://adpass.ru/pervoe-delo-za-reklamu-v-instagram-2025/ (Первое дело ФАС по новому запрету — блогер Ася Сивоконева, Омское УФАС, дело № 055/05/18.1-1292/2025 // ADPASS)
[94] FAS on advertising on Telegram and YouTube: recognition as a violation (5 March) and a transition period until the end of 2026 // Forbes. URL: https://www.forbes.ru/tekhnologii/557924-fas-ob-avila-perehodnyj-period-dla-reklamy-v-telegram-i-youtube (ФАС о рекламе в Telegram и на YouTube: признание нарушением (5 марта) и переходный период до конца 2026 года // Forbes)
[95] The registry of hosting providers: operating outside the registry is prohibited from 1 February 2024 // Roskomnadzor. URL: https://rkn.gov.ru/press/news/news74803.htm (Реестр провайдеров хостинга: работа вне реестра запрещена с 1 февраля 2024 года // Роскомнадзор)
[96] The registry has about 566 organizations (April 2026) // Forbes. URL: https://www.forbes.ru/tekhnologii/559360-uznal-o-vozmoznom-uzestocenii-trebovanij-k-hosting-provajderam-dla-bor-by-s-vpn (В реестре около 566 организаций (апрель 2026) // Forbes)

SORM equipment (without which exclusion follows), use of traffic-exchange points from the official registry, and hosting of infrastructure in Russia.[97]

From 1 January 2026 these requirements were backed by administrative liability: Federal Law No. 508-FZ of 28 December 2025 introduced fines of up to one million rubles for providing hosting outside the registry and forbade state and municipal bodies from placing their systems with non-registry providers.[98] The costs of regulation fall on the market and ultimately on clients: according to RUVDS head Nikita Tsaplin, more expensive equipment, higher VAT, and the introduction of SORM at the hosters' own expense have already raised service costs by more than 30 percent, while integration with Roskomnadzor's databases will lead to a new price increase and the squeezing-out of small players.[99]

Worth highlighting separately is the transformation of hosters into an "anti-fraud" instrument. The practice was worked out manually even before the law was passed: from late 2025, Roskomnadzor sent providers lists of IP addresses from their own networks with a demand to remove the VPN servers hosted there within 24 hours — otherwise the entire subnet was subject to blocking. Tellingly, the system learned to find even obfuscated protocols (Xray, VLESS) in "clean" subnets where the easily detectable OpenVPN and WireGuard had not previously been run. In the spring of 2026 this practice was enshrined in law: the amendments known as "Anti-Fraud 2.0" extended to all registry participants the obligation to independently detect and disconnect clients whose capacity is used to circumvent blocks. This changes the very model of a hoster's liability — from reacting to a complaint to a preemptive check: the provider can no longer invoke the neutral status of a technical platform.[100]

In parallel, control over the infrastructure level as a whole tightened. In the summer of 2026, Roskomnadzor moved from blocking individual addresses to the rolling restriction of entire subnets and autonomous systems of data centers — the filter caught platforms of both foreign (Leaseweb) and Russian providers (Selectel, Yandex Cloud, Cloud.ru, Beget) previously

---

[97] Requirements for registry hosters: identification, GosSOPKA, SORM, traffic-exchange points, location in Russia // Habr (ispmanager). URL: https://habr.com/ru/companies/ispmanager/articles/818525/ (Требования к реестровым хостерам: идентификация, ГосСОПКА, СОРМ, точки обмена трафиком, локация в РФ // Хабр (ispmanager))

[98] Fines of up to 1 million rubles for hosting outside the registry and a ban for state bodies (Federal Law No. 508-FZ of 28.12.2025) // Law.ru. URL: https://www.law.ru/news/44280-vstupil-v-silu-zakon-o-shtrafah-do-1-mln-rubley-dlya-hosting-provayderov-ne-iz-reestra-rkn (Штрафы до 1 млн рублей за хостинг вне реестра и запрет госорганам (ФЗ № 508-ФЗ от 28.12.2025) // Law.ru)

[99] Hosting-service prices rose by more than 30% due to SORM, VAT, and integration with RKN databases (N. Tsaplin, RUVDS) // The Insider. URL: https://theins.ru/news/291587 (Рост цен на услуги хостинга более чем на 30% из-за СОРМ, НДС и интеграции с базами РКН (Н. Цаплин, RUVDS) // The Insider)

[100] The obligation of registry hosters to detect and disconnect VPN clients ("Anti-Fraud 2.0"); RKN's manual orders with a 24-hour deadline; detection of obfuscated protocols // te-st.org. URL: https://te-st.org/2026/05/12/hostingrules/ (Обязанность реестровых хостеров выявлять и отключать VPN-клиентов ("Антифрод 2.0"); ручные предписания РКН с 24-часовым сроком; обнаружение обфусцированных протоколов // te-st.org)

considered safe.[101]

As a result, the hosting layer turned from a neutral technical stratum into a full-fledged instrument of control, operating in three dimensions at once. The registry decides who is even entitled to provide services; SORM and GosSOPKA embed a surveillance point in every provider; the obligation to seek out and disconnect VPNs makes the hoster a party to censorship. This is the same technique as with the marketplaces and banks in the previous sections: the state offloads the filtering work itself onto business, keeping for itself the role of overseer. The side effect is predictable — market consolidation, rising prices, and the departure of small providers, that is, the cost of control passed on to the infrastructure and its clients.

6. The ban on authorization through "foreign services"

In July 2023, Russia passed Federal Law No. 406-FZ, banning registration on Russian sites using foreign authorization systems, including foreign mail services such as Gmail or Apple ID. The restriction initially came into force on 1 December 2023. Under the established rules, the only legal ways to register and log in for Runet users are a Russian phone number, the Gosuslugi portal, the Unified Biometric System, or another information system controlled by a Russian citizen or a Russian legal entity.[102]

In June 2026 the regulation moved into practice: Federal Law No. 199-FZ was signed, introducing administrative liability for non-compliance with these requirements.[103] The punishment is imposed directly on the owners of internet resources who continue to offer authorization through the banned foreign services. Fines for legal entities are between 500,000 and 700,000 rubles, for officials between 30,000 and 50,000 rubles, and for individuals (site owners) between 10,000 and 20,000 rubles.[104]

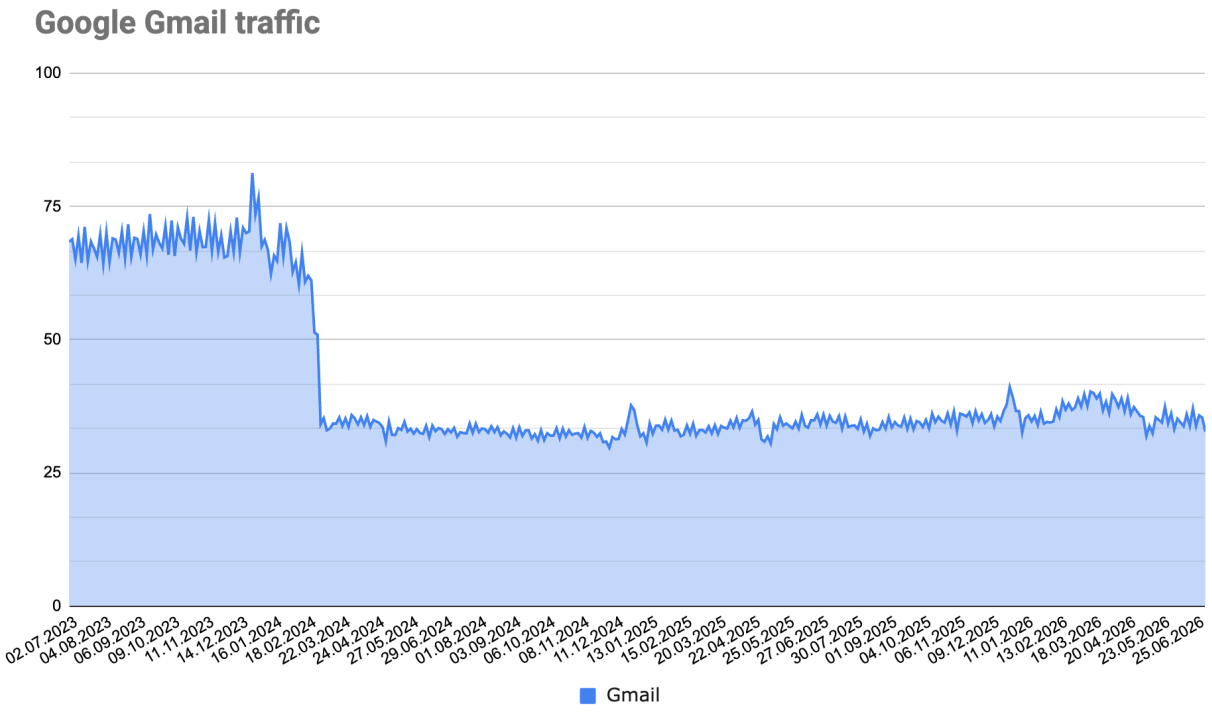
For ordinary citizens, the law provides no direct fines for using foreign mailboxes.[105]

---

[101] Rolling blocking of subnets and autonomous systems of data centers, June 2026 // Habr. URL: https://habr.com/ru/articles/1044396/ (Веерная блокировка подсетей и автономных систем дата-центров, июнь 2026 // Хабр)
[102] Requirements for user authorization on Russian sites (Federal Law No. 406-FZ of 31.07.2023, in force from 1 December 2023) // ConsultantPlus. URL: https://www.consultant.ru/law/hotdocs/81325.html (Требования к авторизации пользователей на российских сайтах (ФЗ № 406-ФЗ от 31.07.2023, вступление в силу 1 декабря 2023) // КонсультантПлюс)
[103] Administrative liability for violating the authorization rules (Federal Law No. 199-FZ of 26.06.2026, Art. 13.55 of the Administrative Offenses Code, in force from 7 July 2026) // Garant.ru. URL: https://www.garant.ru/article/2136195/ (Административная ответственность за нарушение правил авторизации (ФЗ № 199-ФЗ от 26.06.2026, ст. 13.55 КоАП, вступление в силу 7 июля 2026) // Гарант.ру)
[104] The amounts of fines for authorization through foreign services // Vedomosti. URL: https://www.vedomosti.ru/society/news/2026/06/09/1204637-shtrafi-za-avtorizatsiyu (Размеры штрафов за авторизацию через иностранные сервисы // Ведомости)
[105] The fines concern site owners, not users of foreign mail // 360.ru. URL: https://360.ru/tekst/obschestvo/fejk-v-rossii-vvodjat-shtrafy-za-avtorizatsiju-na-sajtah-cherez-inostrannuju-pochtu/ (Штрафы касаются владельцев сайтов, а не пользователей иностранной почты // 360.ru)

Nevertheless, the harsh sanctions for business force Russian platforms, online stores, and government portals to mass-disable login buttons through Google ID or Apple ID and to require users to re-link accounts to domestic email addresses (Mail.ru, Yandex) or phone numbers, which methodically isolates foreign mail services from Russia's digital infrastructure.

Chart 6. Gmail traffic in Russia, 2023–2026



The chart shows the dynamics of Gmail traffic in Russia, normalized to 100. Three conclusions follow from it. First: there were no problems with mail either before the war or in its first years — throughout 2023 Gmail and other foreign mailboxes worked freely, and the curve holds high, in the 65–75 point corridor. Second: the decisive factor was the 2023 ban — as it was applied in practice, traffic in early 2024 fell almost by half, from about 62 to 33 points, and settled at that level. Third: the introduction of fines in 2026 had no effect on Gmail use — after the 2024 collapse the line runs on an even plateau until mid-2026, with no new decline.

7. Anti-fraud packages and paying for circumvention

Alongside the technical and legal pressure on VPNs, the state built a third contour — a financial one. Formally it is framed as a fight against fraud: over 2025–2026 two large packages of measures against phone and cyber fraud were adopted. The first (April 2025) introduced mandatory call verification, a limit on the number of SIM cards per person, and a ban on using foreign messengers for communication between government bodies and banks and their clients.

The second, known as "Anti-Fraud 2.0," went further.[106] It limited the number of bank cards to twenty per person across all banks at once, introduced a unified system for tracking them, and a "cooling-off period" — the bank's right to delay a suspicious transfer for six hours.[107] The same package included a ban on terminating a communications contract earlier than 90 days, an IMEI database for blocking devices "by hardware," and a "red button" for complaints through Gosuslugi and the MAX messenger.[108]

The official logic is clear: limits on SIM cards and bank cards hit the "dropper" schemes, where fraudsters use dozens of front numbers and accounts to cash out stolen money and cover their tracks. But that very same infrastructure — a multitude of anonymous SIM cards, dozens of cards, fast transfers between people — became, after 2022, the main way of paying for foreign services unavailable for direct payment with a Russian card. After Visa and Mastercard left, payments for foreign subscriptions, server rental, and VPNs run precisely on "grey" rails: topping up from a phone balance, pools of cards, transfers through intermediaries, and cryptocurrency. By limiting the number of SIM cards and bank cards, de-anonymizing every payment, and obtaining the right to freeze transfers, the state cuts off not so much the channel for laundering stolen money as the channel for paying for circumvention.

That circumvention, and not just fraud, is the target is shown by the composition of the package itself. "Anti-Fraud 2.0" directly includes a ban on hosting providers offering resources for hosting VPN services — a measure with no relation to phone scams but fitting entirely within the anti-VPN campaign of the previous chapters.[109] The anti-fraud law thus serves as a carrier for a norm that in essence belongs not to the financial but to the censorship contour.

The precedent was worked out in advance and described above — in the section on the "Apple tax," when operators, at the authorities' demand, disabled topping up an Apple ID from a phone balance in order to cut off the payment channel and force Apple to return the removed VPN apps. The anti-fraud packages generalize this technique: if a VPN cannot be blocked technically, and prosecuting the user is legally difficult, what remains is to make paying for circumvention expensive, rare, and traceable.

---

[106] The second anti-fraud package "Anti-Fraud 2.0": composition, adoption by the State Duma on 9 June and signing on 26 June 2026 // Kommersant. URL: https://www.kommersant.ru/doc/8728414 (Второй антифрод-пакет "Антифрод 2.0": состав, принятие Госдумой 9 июня и подписание 26 июня 2026 года // Коммерсантъ)

[107] A limit of 20 bank cards per person across all banks and a "cooling-off period" of 6 hours // RIA Novosti. URL: https://ria.ru/20260609/gosduma-2097923590.html (Лимит 20 банковских карт на человека во всех банках и "период охлаждения" 6 часов // РИА Новости)

[108] An IMEI database, a "red button" via Gosuslugi and MAX, a ban on terminating a communications contract earlier than 90 days // SecurityLab. URL: https://www.securitylab.ru/news/574218.php (База IMEI, "красная кнопка" через Госуслуги и MAX, запрет расторгать договор связи ранее 90 дней // SecurityLab)

[109] A ban on hosting providers offering resources for hosting VPN services as part of the anti-fraud package // Kommersant. URL: https://www.kommersant.ru/doc/8728414 (Запрет хостинг-провайдерам предоставлять ресурсы для размещения VPN-сервисов в составе антифрод-пакета // Коммерсантъ)

Yet the measures poorly achieve their stated goal. They do not destroy the fraud market but merely raise the cost of consumables — SIM cards and drop accounts — and drive the schemes deeper into the shadows. Meanwhile, the law-abiding user gets de-anonymized payments, delayed transfers, and limits on familiar services. The upshot is the same as throughout the chapter: under the banner of security, an infrastructure of control is built, while the real burden falls not on the criminal but on the ordinary person and on their ability to pay for access to a free internet.

Chapter 8. Splitting the internet

The most strategically significant direction of 2026 was the attempt to split traffic into domestic and international — that is, to approach the very isolation the first part described as the final stage of the ladder. At the heart of the plan lies an admission of a technical limit: a VPN cannot be blocked by filtering, since blanket detection requires ever-greater computing power, and the probability of DPI false positives as the rules tighten approaches one. Hence the change of approach — from technical suppression to economic containment. The task is formulated as follows: make circumvention knowingly expensive without cutting off foreign traffic entirely, since it is needed for access to business and technology services, software updates, and foreign trade. Hence two parallel mechanisms — a limit on international traffic in mobile networks and a moratorium on expanding cross-border channels.

1. Charging for international traffic on mobile networks

On 28 March 2026, at a meeting with telecom operators, Maksut Shadaev proposed introducing a charge for international traffic in mobile networks above a limit of 15 GB per month, to start by 1 May 2026.[110] The logic is directly tied to the fight against circumvention: VPN traffic is technically indistinguishable from ordinary foreign traffic, so the measure hits all international traffic at once. The size of the limit was justified by a Ministry of Digital Development calculation, according to which the average subscriber consumes about 10 GB of international traffic a month, while the cost of exceeding it was estimated at roughly 150 rubles per gigabyte.[111]

The original deadline fell through because of the specifics of contractual regulation. An operator sets and changes tariffs for communications services on its own, but the law distinguishes changing a price from changing a tariff plan as a set of services. Under Article 28 of Federal Law No. 126-FZ "On Communications" and the Rules for Providing Telephone Communications Services, an operator has the right to unilaterally change the price of an existing tariff, notifying

[110] The Ministry of Digital Development proposed a charge for foreign traffic above 15 GB // Fontanka. URL: https://www.fontanka.ru/2026/03/30/76339405/ (Минцифры предложило плату за зарубежный трафик свыше 15 ГБ // Фонтанка)
[111] Russians may be charged for foreign internet from autumn // The Moscow Times. URL: https://ru.themoscowtimes.com/2026/06/25/rossiyanam-s-oseni-mogut-vvesti-platu-za-zarubezhnii-internet-a199232 (Россиянам с осени могут ввести плату за зарубежный интернет // The Moscow Times)

the subscriber at least 10 calendar days in advance through the website and by SMS.[112] However, separate tariffication of domestic and international traffic is not a price increase but the introduction of a new tariffication parameter, that is, a change of the essential terms of the contract, which affects the set and structure of services.[113] Such a change requires reworking billing systems capable of separating foreign traffic from domestic in real time, and re-executing contractual terms with subscribers.

On 22 April 2026, the operators requested a delay, citing the unpreparedness of their billing systems, and the decision was postponed to the period after the autumn State Duma elections.[114] On 27 April the Ministry of Digital Development confirmed that separate tariffication of international traffic was under development.[115] The postponement is explained by a combination of reasons. Technically, separate tariffication requires reworking the billing. Legally, introducing a charge runs into the absence of a normative basis: the Ministry of Digital Development has no direct authority, which means amendments to legislation are required. Politically, the launch of a mechanism that directly raises the cost of internet access for the mass subscriber was deferred so as not to create an irritant on the eve of the vote.

By the end of the second quarter of 2026 the mechanism is not enshrined in law, but the direction is fixed by official documents and meetings. The ultimate goal remains twofold: to economically restrain the circumvention of blocks and to force foreign services to place infrastructure within Russian jurisdiction, under SORM.

2. The moratorium on international channels

On 16 April 2026 it emerged that about twenty companies — owners of communications channels running from Russia to Europe — had signed an agreement with the Ministry of Digital Development to suspend their expansion.[116] According to sources in the telecom market, the document was signed at one of the meetings with Maksut Shadaev devoted to restricting VPNs. Among the participants named were MSK-IX (MMTS-9), TransTeleCom, MTS, VimpelCom

---

[112] Ministry of Digital Development / Government Resolution No. 59 of 24.01.2024, the operator's right to change a tariff with 10 days' notice, Art. 28 of Federal Law 126-FZ — https://digital.gov.ru/ru/appeals/faq/374/ (Минцифры / ПП № 59 от 24.01.2024, право оператора изменять тариф с уведомлением за 10 дней, ст. 28 ФЗ-126)

[113] Rospotrebnadzor, distinguishing a change in a tariff's price from a change in the tariff plan (a set of services) as an essential term of the contract — https://zpp.rospotrebnadzor.ru/handbook/svyaz/memos/207553 (Роспотребнадзор, разграничение изменения цены тарифа и тарифного плана (набора услуг) как существенного условия договора)

[114] Operators requested a delay on tariffing foreign traffic // Vedomosti. URL: https://www.vedomosti.ru/technology/articles/2026/04/22/1192083 (Операторы попросили отсрочку по тарификации зарубежного трафика // Ведомости)

[115] The Ministry of Digital Development on tariffing international traffic // Habr. URL: https://habr.com/ru/news/1029090/ (Минцифры о тарификации международного трафика // Habr)

[116] Operators signed a moratorium on expanding international channels // GoGov. URL: https://gogov.ru/news/927744 (Операторы подписали мораторий на расширение международных каналов // GoGov)

(Beeline), T2 Mobile, and Ufanet.[117] The operators were not told the duration of the restriction.

The reason for the measure is directly linked to VPNs. To an operator, circumvention-service traffic looks like ordinary foreign traffic, and the more actively VPN use grows, the faster the bands for passing cross-border traffic fill up. The regulator's logic is that the reserves of these bands are limited, and natural traffic growth will lead to their exhaustion. Besides suspending expansion, market participants were obliged to report monthly on cross-border traffic: its volume, the source resources, and the communication nodes through which it passes.[118] Sources name a second stated goal: to force foreign services wishing to keep operating in Russia to place infrastructure inside the country — so that access speed for Russian users does not fall as the channels fill up.

Formally, this is not a ban but a permit-based procedure, introduced back in March 2026: an operator wishing to expand foreign channels must obtain permission.[119] As of the publication of these materials, not a single operator had passed the permit procedure, and the criteria for issuing permissions were not communicated to market participants. Moreover, the Ministry of Digital Development lacks the authority for such additional approval: for the procedure to become lawful, amendments to the law or a government resolution are required.[120]

3. Consequences for the market

The forecast of consequences has already been voiced publicly by industry participants. Ilya Gudenko, head of telecom-business development at TransTeleCom, at the Night Telecom Forum in Saint Petersburg in June 2026, described the scenario: by the autumn of 2026 the existing channels may be fully utilized, and new ones will not receive permission for full

---

[117] Meduza, the composition of the meeting's participants and the moratorium's signatories, the term not named — https://meduza.io/news/2026/04/16/rbk-operatory-svyazi-soglasilis-zamorozit-rasshirenie-kanalov-svyazi-v-evropu-chtoby-borotsya-s-ispolzovaniem-vpn (Meduza, состав участников совещания и подписантов моратория, срок не назван)

[118] Forbes, monthly reporting on cross-border traffic and the aim to force services to place servers in Russia — https://www.forbes.ru/tekhnologii/559280-rbk-uznal-o-moratorii-na-rassirenie-kanalov-svazi-v-evropu-radi-bor-by-s-vpn (Forbes, ежемесячная отчетность о трансграничном трафике и цель принудить сервисы размещать серверы в РФ)

[119] Habr, the permit-based procedure since March 2026, no one passed it, criteria not disclosed — https://habr.com/ru/news/1052072/ (Хабр, согласительный порядок с марта 2026, никто не прошел, критерии не сообщены)

[120] Meduza, for additional approval the Ministry of Digital Development needs amendments to the law or a government resolution — https://meduza.io/news/2026/04/16/rbk-operatory-svyazi-soglasilis-zamorozit-rasshirenie-kanalov-svyazi-v-evropu-chtoby-borotsya-s-ispolzovaniem-vpn (Meduza, для дополнительного согласования Минцифры нужны поправки в закон или постановление правительства)

expansion.[121] In that case, providers will begin to squeeze out less profitable clients, clear the band, and introduce differentiated tariffs, splitting access into two kinds — cheaper or at the current price with the Russian internet, and more expensive with the foreign one. The burden of restraining VPNs is thereby shifted onto the operators themselves: with the channels full and their expansion banned, business is forced either to filter circumvention traffic or to set an economic barrier by raising the cost of foreign access.[122]

A separate difficulty concerns the mechanism for distinguishing Russian from foreign traffic. The most likely markup tool becomes RANR — the Registry of Address and Number Resources of the Russian segment of the internet, which TsMU SSOP under GRChTs launched in public access in April 2024 as a national analog of whois and the RIPE database.[123] For failure to connect to RANR, Article 13.44 of the Administrative Offenses Code already provides for fines of up to fifty thousand rubles for legal entities.[124] The registry in theory makes it possible to mark up which IP addresses and autonomous systems count as Russian, and to build separate routing and tariffication on this basis. However, a significant part of Russian companies' resources is physically hosted on foreign hosting — including because of a shortage of domestic capacity, especially in the field of artificial intelligence. This creates the risk that separate tariffication will affect legal business traffic, while circumvention through reverse proxies and VPNs will retain its fundamental possibility.

The extreme form of this regulation is shown by the experience of Iran. After restoring internet access in the summer of 2025, the Iranian authorities first brought data centers back into operation but, within a few days, restricted them again, having encountered a mass deployment of VPNs on rented servers. The rules were tightened: to buy any data-center service, a verified profile in the state subscriber-verification system "Shahkar" is now mandatory, with the phone number and national identifier having to belong to one person, and information about connected digital services displayed in a citizen's personal account on the state portal. Responsibility for identifying end users is placed either on the data center itself or on the intermediary hosting

---

[121] Habr, the forecast of Ilya Gudenko (TTK) at the Night Telecom Forum on differentiated tariffs by autumn 2026 — https://habr.com/ru/news/1052072/ (Хабр, прогноз Ильи Гуденко (ТТК) на Night Telecom Forum о дифференцированных тарифах к осени 2026)

[122] Expert, the economic filter — operators themselves will either filter VPNs or raise the price for foreign traffic — https://expert.ru/news/rbk-uznal-o-moratorii-operatorov-na-rasshirenie-kanalov-svyazi-v-evropu-radi-borby-s-vpn/ (Эксперт, экономический фильтр — операторы сами будут фильтровать VPN или поднимать цену на зарубеж)

[123] The launch of the public RANR service (Registry of Address and Number Resources) and a whois analog by GRChTs/TsMU SSOP, April 2024, an analog of the RIPE database // Habr. URL: https://habr.com/ru/news/806591/ ; RoskomSvoboda URL: https://roskomsvoboda.org/ru/post/suveren-whois-ranr/ (Запуск публичного сервиса РАНР (реестр адресно-номерных ресурсов) и whois-аналога ГРЧЦ/ЦМУ ССОП, апрель 2024, аналог базы RIPE // Хабр ; RoskomSvoboda)

[124] OrderCom, fines under Art. 13.44 of the Administrative Offenses Code for failure to connect to RANR, up to 50 thousand rubles for legal entities — https://www.ordercom.ru/analitika/suvenirans (ОрдерКом, штрафы по ст. 13.44 КоАП за неподключение к РАНР до 50 тыс. руб. для юрлиц)

company to which a pool of addresses is allocated. The Shahkar system, originally created for telecom operators and then extended to banking and government services, and now to hosting, is — according to documents analyzed by Citizen Lab — part of Iran's lawful-intercept system and enforces a strict one user — one profile binding.[125] Russia's RANR so far solves the narrower task of marking up the address space, but the vector coincides: binding every network resource to a verified owner while offloading responsibility for identification onto business.

Chapter 9. The new overseer: the FSB takes control

The institutional upshot of the period was the shift of the censorship control center from Roskomnadzor to the security bloc.

Government resolution No. 1667 of 27 October 2025 approved new rules for the centralized management of the public communications network, which came into force on 1 March 2026. Management of the TSPU infrastructure was assigned jointly to Roskomnadzor, the FSB, and the Ministry of Digital Development, and the decision to introduce a centralized-management regime (filtering, blocking of directions, isolation of a network segment) was handed to an interagency commission.[126]

A separate law went even further (draft law No. 1069501-8, passed by the State Duma in third reading on 17 February 2026 and approved by the Federation Council on 18 February): it obliged telecom operators to suspend any services at the FSB's motivated demand. The new grounds — "threats to the security of citizens and the state," the content of which is defined by classified acts — while operators are released from liability to subscribers for such shutdowns.[127] In January 2026 the State Duma separately considered amendments giving the FSB the right to shut down not only mobile but also fixed-line communications and telephony.[128]

---

[125] Citizen Lab, "Shahkar" as a component of the lawful-intercept system, the one user — one profile binding — https://citizenlab.ca/research/uncovering-irans-mobile-legal-intercept-system/ (Citizen Lab, "Шахкар" как компонент системы законного перехвата, связка один пользователь — один профиль)
[126] Rules for the centralized management of the public communications network (Government Resolution No. 1667 of 27.10.2025, in force from 1 March 2026) // ConsultantPlus. URL: https://www.consultant.ru/law/hotdocs/91389.html (Правила централизованного управления сетью связи общего пользования (ПП № 1667 от 27.10.2025, вступление 1 марта 2026) // КонсультантПлюс)
[127] The law on operators' obligation to suspend communications services at the FSB's demand (draft law No. 1069501-8, passed by the State Duma on 17 February 2026, approved by the Federation Council on 18 February) // Pravo.ru. URL: https://pravo.ru/news/262459/ (Закон об обязанности операторов приостанавливать услуги связи по требованию ФСБ (законопроект № 1069501-8, принят Госдумой 17 февраля 2026, одобрен Совфедом 18 февраля) // Право.ру)
[128] The State Duma in the first reading (27 January 2026) — on the FSB's right to demand the shutdown of not only mobile but also fixed-line communications and telephony (draft law No. 1069501-8) // ComNews. URL: https://www.comnews.ru/content/243470/2026-01-28/2026-w05/1008/otklyuchenie-interneta-pereydet-pod-kontrol-fsb (Госдума в первом чтении (27 января 2026) — о праве ФСБ требовать отключения не только мобильной, но и стационарной связи и телефонии (законопроект № 1069501-8) // ComNews)

Behind the impersonal formulation "FSB" stands a specific unit. Judging by the totality of indicators — above all by who won the bureaucratic dispute around the blocking of Telegram (see Chapter 5) — the management of internet censorship, from February 2026, was concentrated in the FSB's Second Service, the Service for the Protection of the Constitutional Order and the Fight Against Terrorism (in internal jargon, the "deuce"). This unit is considered a direct heir of the KGB's Fifth Directorate, which was responsible for combating "ideological subversion," and historically specializes in threats in the socio-political sphere, that is, in internal dissent. Handing it control over the blocks means that internet censorship in Russia has finally ceased to be regarded as a technical or sectoral task and has been assigned to the same category as political policing.[129]

Since March 2006 the service has been permanently headed by Colonel-General Alexei Semyonovich Sedov (b. 1954, Sochi). A product of the Leningrad KGB directorate, in the 1990s he worked in the tax police, then was deputy director of the State Drug Control Service, and in 2006 returned to the FSB, now to the post of head of the "deuce." In 2021 Sedov came under sanctions from the UK, the US, Canada, and Ukraine as the head of the service that coordinated the actions of the unit implicated in the poisoning of Alexei Navalny.[130] The relevant directorate within the service — the Directorate for the Protection of the Constitutional Order (UZKS) — is headed by Lieutenant-General Alexei Zhalo. Both figures remain almost publicly invisible, which is typical for this unit: its contacts with the press and with the FSB's other departments are deliberately restricted.

The meaning of the shift is that Roskomnadzor's role is changing. From an agency that defined threats and made blocking decisions, it is turning into a technical executor under a security overseer. The management of access to information in Russia has finally moved from the administrative plane into the plane of security — with all the attendant secrecy of procedures and grounds.

The practical consequences of this transition are twofold. First, the blocks have become markedly harsher. A service whose task is the suppression of threats in the socio-political sphere, not the balancing of economic costs, is ready to pay the price before which the Ministry of Digital Development and the operators had previously stopped: that is precisely why Telegram was blocked after all, despite the protests of war correspondents, deputies, and pro-government bloggers. Second, having found that the technical race with VPNs cannot be won, the security overseer changed the tactics themselves. Instead of continuing to chase

[129] The Service for the Protection of the Constitutional Order and the Fight Against Terrorism (the Second Service, the "deuce"): area of responsibility, structure, deputy head A. Zhalo (UZKS) // Dossier Center. URL: https://fsb.dossier.center/2s/ (Служба по защите конституционного строя и борьбе с терроризмом (Вторая служба, "двойка"): сфера ответственности, структура, заместитель руководителя А. Жало (УЗКС) // Центр Досье)

[130] Alexei Sedov — head of the FSB's Second Service since March 2006, colonel-general; biography and sanctions over the poisoning of A. Navalny (2021) // Wikipedia. URL: https://ru.wikipedia.org/wiki/Седов,_Алексей_Семёнович (Алексей Седов — руководитель Второй службы ФСБ с марта 2006 года, генерал-полковник; биография и санкции по делу об отравлении А. Навального (2021) // Википедия)

circumvention tools with its own hands, the state devised the move that runs like a red thread through this whole chapter — offloading the fight against VPNs onto business. Marketplaces, banks, and hosters are forced to detect and disconnect circumvention users themselves under threat of exclusion from the whitelists, loss of accreditation, and the mobilization of employees, while the anti-fraud packages cut off the very payment for circumvention. Thus the censorship function is finally distributed among those who, by skill and reach, are able to perform it better than the state system — under the control and on the orders of the security overseer.

Conclusion: which steps have been taken

A comparison with the first part's forecast gives a vivid picture. Of the six probable future steps listed in the spring of 2025, by mid-2026 almost all have been taken or are actively being taken. Telegram is effectively blocked, though formally this has not been announced. Statistical methods for detecting VPNs have been introduced — VLESS and REALITY are detected precisely by traffic behavior. Blocking large blocks of IP addresses has become routine: it caught both Cloudflare and the subnets of foreign hosters. The tactics of "grey lists" and deliberate degradation of connection quality are the main instrument against messengers. The move to "whitelists," described as a distant scenario, has been implemented and deployed in most regions on mobile networks. And even the drive toward full isolation — through a limit on international traffic and a moratorium on expanding channels — has ceased to be a hypothesis.

To this predictable set, the period added what the earlier analysis did not consider central: everyday rolling shutdowns and the coercion of tens of millions of users into a state messenger. The logic of the "ladder," meanwhile, has been fully preserved — every new measure passes through the same four stages (political decision, legal formalization, technical implementation, resource provision) that were described in the first part. Only the scale and the speed have changed.

Nor has the fundamental dilemma changed. Rolling shutdowns and "whitelists" deal a direct blow to the economy, estimated in billions of dollars; shifting censorship functions onto business turns into direct costs for companies; the splitting of traffic threatens isolation from the global infrastructure on which, among other things, the export economy rests. The authorities still choose "surgical" and "quiet" methods so as not to pay the full price of isolation all at once — hence throttling instead of blocking, a "cooling-off period" instead of a shutdown, a traffic limit instead of severing channels.

Nor has the balance of forces in the main confrontation changed. Despite all the measures listed, VPN penetration among Russian users holds, by various estimates, at around 40%, and by some studies exceeds 60% in the capitals.[131] This means the scenario in which a significant

[131] The share of Russians using a VPN grew to 39% // NSN. URL: https://nsn.fm/society/smi-dolya-ispolzuuschih-vpn-rossiyan-vyrosla-do-39 (Доля использующих VPN россиян выросла до 39% // НСН)

part of the population retains access to independent information remains real. The "blocking ladder" continues to be built upward — but the counter-movement of those who circumvent that ladder does not cease either. The outcome of this struggle is still not predetermined.

Conclusions

1. The forecast became a chronicle. Of the six steps named probable in the spring of 2025, by mid-2026 almost all have been taken or are actively being taken: the effective blocking of Telegram, statistical detection of VPNs, blocking of large IP blocks, deliberate degradation of communications, the move to "whitelists," and the first steps toward splitting traffic. To this set the period added what the earlier analysis did not consider central — everyday rolling shutdowns and the coercion of tens of millions of users into a state messenger.
2. The very logic of censorship changed. The model "what is on the list is forbidden" gave way to the model "only what is on the list is allowed." At the same time, "whitelists" arose not as an ideological design but as a forced reaction to the chaos of shutdowns — and the security bloc quickly seized this mechanism, turning it from a way to preserve vital services into a lever of compulsion: the availability of a banking app was made dependent on installing SORM.
3. Censorship was offloaded onto business and users. Companies are forced to detect VPNs themselves under threat of exclusion from the "whitelists," loss of IT accreditation, and, as a consequence, mobilization of employees; for the first time liability also shifted onto the end user — up to punishment for the very search for information. The state no longer needs to chase circumvention technologies — it is enough to make those who understand them best work for censorship.
4. The logic of the "ladder" was preserved; the scale and speed changed. Every new measure passes through the same four stages — political decision, legal formalization, technical implementation, resource provision. Behind the technology stands a built-out industry with its own contractor, budgets in the tens of billions of rubles, and a move to machine-learning-based filtering.
5. The control center shifted from Roskomnadzor to the FSB. RKN, from an agency that defined threats and made decisions, turned into a technical executor under a security overseer. The management of access to information finally moved from the administrative plane into the plane of security — with classified procedures and grounds.
6. The outcome is not predetermined. Despite all the measures, VPN penetration holds at around 40%, and in the capitals exceeds 60%, and each new wave of blocking expands the circumvention audience rather than shrinking it. The authorities still choose "quiet" methods — throttling instead of blocking, a traffic limit instead of severing channels — so as not to pay the full price of isolation all at once. The blocking ladder continues to be built upward, but the counter-movement of those who circumvent it does not cease.