



TSPU and You

**Architecture, Blocking Behaviours, and
Implications for Tool Development**

Dmitry Kuznetsov
September 2026

critical
Infrastructure
lab

The logo graphic for critical Infrastructure lab, featuring a stylized, jagged line that forms a shape resembling a lightning bolt or a series of connected triangles.

TSPU and You: Architecture, Blocking Behaviours, and Implications for Tool Development

Research Report

Published by the critical infrastructure lab, Amsterdam, September 2026.

“TSPU and You: Architecture, Blocking Behaviours, and Implications for Tool Development” is marked with CC0 1.0 Universal.

Set in Source Sans, Source Serif, and Source Code.

Design and visual identity by Ulrike Uhlig.

The publication pipeline is made with free software from plain text:
<https://codeberg.org/criticalinfralab/publication-pipeline>

Originally developed by Ulrike Uhlig, currently maintained by Anders Aarvik and maxigas.

critical infrastructure lab document series
CIL#018

DOI 10.5281/zenodo.22902263

This work was supported by the Open Technology Fund.

The author thanks everyone who contributed to this report through discussions, careful reading, and helpful feedback.

Table of Contents

Overview	1
1. System Architecture	2
1.1 In-path deployment	2
1.2 Hardware and software stack	3
1.3 Filtering architecture	5
2. Ownership & Operation	10
2.1 State ownership and centralised management	10
2.2 Operational modes	11
3. Blocking in Practice	12
3.1 VPN blocking	12
3.2 Escalation, collateral damage, and the ECH decision	14
3.3 Transit censorship and DPI extraterritorial effects	16
4. Implications for Tool Development	17
4.1 Market consolidation and regulatory compliance	17
4.2 Network security and system entrenchment	18
4.3 Protocol detection and evasion	19
4.4 Comprehensive data collection and coordination	21
Notes	24

Overview

Russia's TSPU (Technical Means of Countering Threats) is a state-owned deep packet inspection system installed inline across Russia's licensed networks. Where traffic volumes warrant dedicated equipment, it is installed at the operator's premises. Otherwise, the operator's traffic passes through an upstream provider's TSPU device. The system is actively managed and operated by the General Radio Frequency Centre (GRFC), the technical arm of Roskomnadzor (RKN), through its Centre for Monitoring and Management of the Public Communications Network (CMU SSOP). The state allocated 58.97 billion roubles to TSPU modernisation across 2025–2030⁰¹. The total Cybersecurity Infrastructure federal project, of which this forms the bulk, rose to 83.7 billion roubles in March 2026⁰². This is not a static blocklist but an evolving filtering infrastructure. This advisory is written for circumvention tool developers, network measurement researchers, and digital security trainers. It assumes technical familiarity with DPI, traffic engineering, and the internet landscape in Russia.

1. System Architecture

1.1 In-path deployment

TSPU devices are deployed inline at ISP premises, and traffic on a covered path transits them before reaching its destination. Independent measurement research identified approximately 6,871 in-path TSPU “links” (network paths inferred from traceroute clustering) as of 2022, with affected endpoints across 650 ASes. The authors flag the figure as a gross underestimate of installed devices because TSPU behind NAT is invisible to their method⁰³. By October 2025, Roskomnadzor reported 1,406 communications nodes (the regulatory unit of installation under Government Decree No. 126) with 132.3 Tbit/s of traffic passing through⁰⁴. The Ministry of Digital Development’s stated target is 954 Tbit/s by 2030⁰².

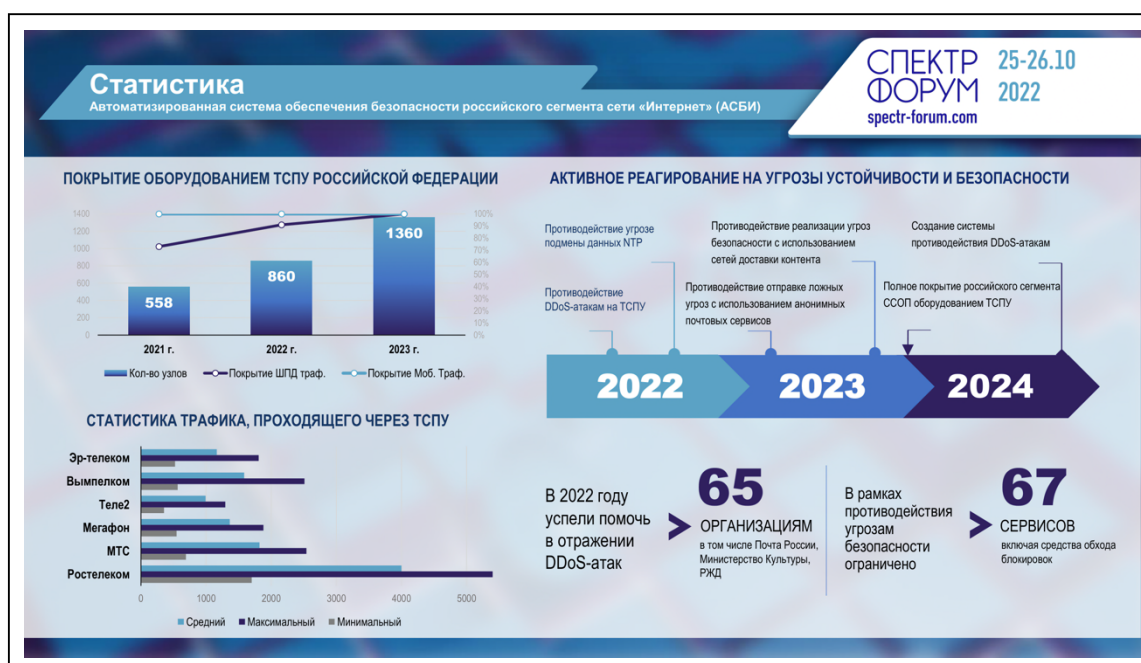


Figure 1: TSPU node deployment, 2021–2023: 558 → 860 → 1,360 nodes, with coverage approaching 100%.

Source: Sergei Khutortsev, head of the Centre for Monitoring and Management of the Public Communications Network (CMU SSOP; Russian: ЦМУ ССОП), Spektr Forum, October 2022 (2023 value as then planned).⁰⁵

All nodes handling traffic above 10 Gbps are in scope⁰⁶. Smaller ISPs are typically filtered at their upstream provider’s TSPU device rather than receiving dedicated hardware. In October 2023, Roskomnadzor’s head told journalists that mobile, broadband and cross-border nodes were “closed 100 per cent”, a level he said had been reached that August, while noting that installed equipment needs continual modernisation as operator traffic grows⁰⁷. Node counts have

continued to rise since. From July 2026, traffic from 5G handsets used in satellite mode must also pass through TSPU, at the domestic gateway station that receives it — though a satellite-industry source calls near-term enforcement against existing foreign operators such as Starlink unlikely, and reads the requirement instead as preparation for Russian mobile operators building or leasing satellite networks of their own⁰⁸.

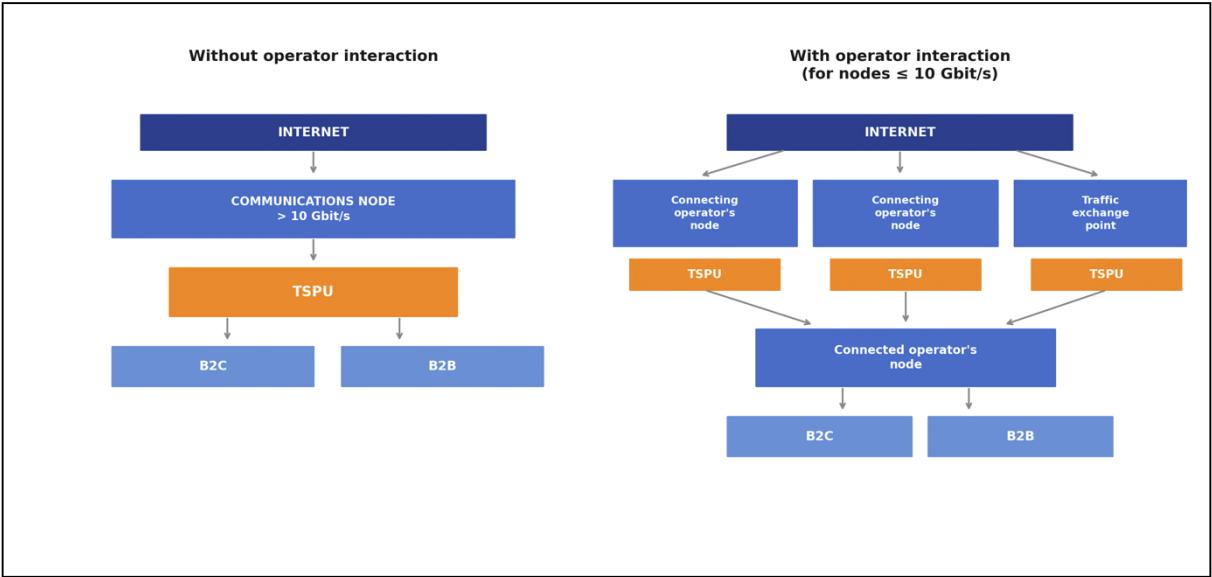


Figure 2: Two TSPU deployment configurations: (1) for links above 10 Gbit/s, a single TSPU device installed inline without operator interaction; (2) for links up to 10 Gbit/s, three placement options requiring operator coordination. Source: GRFC.⁰⁶

1.2 Hardware and software stack

The TSPU stack is assembled through a coordinated chain of state bodies, vendors and operators. GRFC owns the equipment and commissions the system. DCOA (Data Centre for Data Processing and Automation) handles procurement, logistics, and on-site installation at ISP premises. It was created in 2019 to implement Federal Law No. 90-FZ, the amendments conventionally known as the Sovereign Internet Law⁰¹. RDP.RU, a wholly owned Rostelecom subsidiary⁰⁹, supplies the DPI platform and develops its software¹⁰. Its core product line is EcoFilter/EcoSGE, DPI appliances operating at wire speed across models from 24 to 200 Gbps¹¹. Traffic distribution to DPI, DDoS, SORM (System of Operative-Investigative Measures), and Quality of Experience (QoE) analysers simultaneously is handled by EcoBalancer¹², a P4-programmable network packet broker rated at 2.0–6.4 Tbit/s¹³.

Component suppliers in the 2021 configuration included Eltex switches, Silicom bypass devices, and Fiber Trade optical modules⁰⁹. The optical bypass switch was subsequently redeveloped to Roskomnadzor’s specification and, ac-

—

cording to GRFC's 2024 account, had been supplied since 2023 to several hundred nodes¹⁴. Reporting identifies Bulat as its developer, with RDP.RU software and Signaltek hardware¹⁰. A domestic traffic balancer from Vizir was under testing in 2024¹⁰. GRFC attributed the replacement of foreign equipment to unreliable delivery and the loss of technical support following vendors' withdrawal¹⁴.

Localisation proceeded at different rates across software, equipment, and components. Russian-developed DPI software initially ran on a foreign hardware platform, which was replaced by a domestic platform from 2022¹⁴. July 2024 reporting identified Yadro as the platform supplier and a further Signaltek platform as under testing¹⁰. GRFC said it had ended foreign equipment purchases for its sites in 2024, while some replacement products were still being tested¹⁴. This procurement claim does not establish that every component in the installed fleet was domestic. In the same account, domestic optical-module supplies remained conditional on testing, and replacement of the foreign communications processor was a target for 2027^{14, 15}.

GRFC also described how it supported production: it specified requirements and guaranteed manufacturers a minimum order volume¹⁴. The state sets the regulatory mandate and controls the principal DPI supplier through Rostelecom's stake in RDP.RU, while equipment and components come from several vendors. This arrangement provides a coordinated route from state requirements to procurement and deployment. It does not eliminate supply constraints or the need to coordinate installation and maintenance with operators. The 2.27 billion roubles allocated for machine learning enters this existing procurement and deployment structure¹⁶. The allocation establishes a funded programme, rather than demonstrating that the intended capability is already operational.



Figure 3: Deployed TSPU rack with labelled components (left), EcoSGE DPI platform interface (centre), completed installation at ISP premises (right). Source: CNews, 10 July 2024 (left); RDP.RU (centre); ISP practitioner documentation (right).^{10, 11, 17}

1.3 Filtering architecture

Inline TSPU controls multiple network layers. Russia’s National System of Domain Names (NSDI) supplies a parallel DNS layer. DNS control also concerns whether users can reach alternative resolvers. Restrictions on those connections can obstruct attempts to bypass NSDI, although their implementation varies by network and transport^{18, 19}. Defeating one mechanism is insufficient when several apply in sequence or simultaneously.

YouTube illustrates the pattern. Server Name Indication (SNI)-based DPI throttling of `googlevideo.com` began in August 2024²⁰. In February 2026, `youtube.com` was deleted from NSDI, adding a DNS-layer restriction^{21, 22}. The independent telecom analyst Alexey Uchakin read the move as resource economy, on the view that TSPU capacity may not stretch to throttling two large services at once²¹. WhatsApp followed the same sequence, its principal domains disappearing from the NSDI in February 2026²². Telegram has not: its calls have been blocked and media transfer throttled since August 2025²³ — the competing load Uchakin points to²¹. A tool that defeats DPI is not the same as a tool that defeats the system. Each layer requires a different circumvention strategy.

In-path placement: the transparent bridge

TSPU operates at L2, sits in-line rather than on a mirror, and adds no extra hop to traceroute. A transit operator’s account is that its installation cannot be detected with standard diagnostic tools until it intercepts traffic²⁴. The device sits inline between the ISP’s border router and access network, processing Ethernet frames while inspecting payload contents at higher layers. A packet’s TTL,

source routing, and hop count appear identical whether or not it has transited a TSPU device. ISPs themselves have limited visibility into what the device is doing to their traffic.

As one ISP operator documented: “TSPU in your network is designed by RKN’s contractor, installed by RKN’s contractor, filters by RKN’s lists, checked by RKN’s equipment (Revisor²⁵), but YOU are liable for filtering bypasses”²⁶. The promised failover, in which “TSPU swings the physical mirrors in 3 milliseconds and the traffic goes past”, took 3 seconds when one operator timed it²⁶. These practitioner reports consistently characterise TSPU as a “black box”.

Because an inline device need not appear as a separate traceroute hop, Xue et al. (2022) inferred TSPU presence from behavioural artefacts: injected RST packets, consistent throttling thresholds across geographically distributed vantage points, and timing signatures of blocking responses relative to legitimate server responses (categorised as “SNI-I”, “SNI-II”, and “SNI-III” in their taxonomy)³. Successful ping or route tests do not rule out application-level interference. Selectel’s troubleshooting guidance combines basic reachability checks with protocol-specific tests and packet captures, including tests in both directions where possible²⁷. Such symptoms can guide investigation, but do not uniquely identify TSPU as the cause.

The Yarnet incident (Yaroslavl, November 2023) provided direct operational confirmation²⁸. After a power failure the ISP’s TSPU device came up in bypass mode, where by design it stays until Roskomnadzor manually returns it to filtering. Roskomnadzor emailed the operator asking it to agree to a night-time switch back, sent the request to the wrong address, got no reply, and switched at around 1 a.m. regardless. The device then held back roughly 90% of the operator’s traffic for hours. Roskomnadzor did not notice, and filtering was lifted only after the operator’s engineers traced the fault themselves and telephoned its support line.

The operator’s traffic genuinely transits the device, and the operator controls neither its mode nor the timing of a change. A malfunction after the return to filtering can severely disrupt a live network. Because the devices sit inline, traffic that merely transits a Russian network can be filtered as domestic traffic is, with documented consequences for neighbouring states²⁹.

Table 1. Cross-layer control architecture — functions and circumvention responses by layer. DNS control includes both resolver-side responses and interference with connections to external resolvers. The latter can involve in-path filtering. Sources: Xue et al. 2022 and later evidence cited in the table.⁰³

Layer	System function	Circumvention response
DNS — Resolver responses and reachability	NSDI domain removal (NXDO-MAIN); mandatory resolver use; approximately 13 bn queries/day. YouTube removal observed in February 2026. ^{21, 22} External resolver access also faces restrictions that vary by network and transport. ^{18, 19}	Alternative resolvers, including encrypted DNS (DoH, DoT), where reachable. Tunnelled queries via VPN/proxy.
L5-L7 — Deep Packet Inspection	TLS SNI inspection leading to L4 throttling or blocking. QUIC Initial-packet and crypto-frame inspection. VPN protocol and traffic fingerprinting. Machine-learning traffic analysis is funded as planned development, not established here as an active inline capability. ^{16, 20}	Encrypted Client Hello (ECH) conceals the inner SNI. Specific Cloudflare-related ECH blocking and ways around it were measured in March 2025. ³⁰ Protocol mimicry and obfuscation.
L4 — TCP Manipulation	RST/ACK response modification (SNI-I). Symmetric packet dropping after several further packets (SNI-II). Traffic policing by dropping packets above a rate limit (SNI-III).	TCP segmentation strategies.
L3 — IP Inspection and Reassembly	Fragment reassembly (up to 45 fragments, ~5s timeout). RFC 5722 strict discard, all IP versions. IP blocklisting of known VPN server addresses.	Server rotation, IP cycling, CDN fronting. Fragment overlap evasion ineffective.
L2 — Transparent Bridge	No IP address on the data path. Sits in-path, not on a mirror, and adds no extra traceroute hop. Injected packets preserve the flow's original TTL, though TSPU rewrites TTL when forwarding IP fragments. All traffic on the covered path transits the device. Detection by behavioural inference (Xue et al. 2022).	In-path by design. Evasion applies at the layers above, not at L2. Detection: injected packet timing analysis.

—

Network and transport: packet inspection and manipulation

At L3, TSPU reassembles up to 45 IP fragments before inspection, with an approximately five-second timeout⁰³. It drops the entire queue when fragments overlap or are duplicated. RFC 5722 requires the same strict discard for IPv6, but many IPv4 implementations tolerate overlapping fragments. TSPU applies the strict policy to both versions, so fragmentation-based evasion relying on overlaps does not bypass it⁰³. It also blocks known VPN server addresses at the IP layer.

At L4, Xue et al. distinguish multiple SNI-triggered behaviours. In SNI-I, TSPU modifies remote-to-local packets by truncating their payload and changing their TCP flags to RST/ACK. In SNI-II, an additional five to eight packets may pass after the ClientHello before symmetric packet dropping begins. SNI-III instead uses traffic policing, dropping packets that exceed a rate limit.⁰³ Practitioner analysis of the 2024 YouTube throttling likewise identified SNI-triggered packet loss.²⁰

Application-layer filtering: DPI, SNI, and ECH

This is where the core filtering decisions are made. TSPU inspects TLS ClientHello messages for the SNI field, the plaintext domain name that identifies which service a connection is destined for. SNI visibility is the primary detection mechanism for selective blocking and throttling. The YouTube throttling targeted the `googlevideo.com` SNI value. ECH encrypts the inner ClientHello, concealing that destination name. Russian authorities urged website operators to disable it in November 2024³¹. Measurements from one Moscow vantage point in March 2025 found blocking under specific conditions involving Cloudflare's outer SNI and advertised IP ranges, alongside ways around that blocking³⁰. These findings do not establish that every ECH-enabled connection is blocked. QUIC v1 traffic is fingerprinted by its Initial packet headers. Connections carrying prohibited SNI values in the QUIC crypto frame are blocked or throttled using the same mechanisms. VPN protocol signatures (OpenVPN, WireGuard, Shadowsocks/VLESS variants) are identified by traffic patterns, which is why protocol mimicry is a current evasion approach³².

DNS control: NSDI and access to alternative resolvers

NSDI was established under FZ-90 (2019), operationalised through RKN Order No. 229. By 2022, NSDI was processing approximately 13 billion DNS queries per day, according to GRFC figures²². Removal from the NSDI is an operationally simpler and computationally cheaper means of information control. As of early 2026, services fully removed from NSDI include: YouTube (10 February 2026),

WhatsApp (principal domains, February 2026), Facebook, Instagram, Messenger, Tor, Discord (October 2024), and Signal (October 2024)^{20, 22}.

Use of NSDI is *mandatory*: all companies with technological networks and autonomous system numbers must connect²². ISPs must route subscriber DNS queries through NSDI resolvers. A court may fine non-compliant companies 60,000–100,000 roubles³³.

A September 2021 technical discussion reported inconsistent blocking of Google, Cloudflare, and OpenDNS resolvers and reproduced circulating correspondence about planned restrictions. The discussion also records uncertainty about the correspondence’s authenticity¹⁸. Resolver-selection requirements and interference with connections to public external resolvers are distinct mechanisms. Access to external resolvers cannot be assumed to remain available through every transport. Teplitsa’s August 2026 investigation found UDP/53 queries to Google, Cloudflare, and OpenDNS failing from one residential St Petersburg connection on 29 August, while TCP DNS, DoH, and DoT remained available there. Two Russian VPS vantage points did not show the same change. The investigators did not reproduce reported redirection to NSDI, and their route measurements did not identify the filtering device¹⁹.



```
копировать
phil@wtvlab:~/$ host -t A youtube.com a.res-nsdi.ru
Using domain server:
Name: a.res-nsdi.ru
Address: 195.208.4.1#53
Aliases:

Host youtube.com not found: 3(NXDOMAIN)
phil@wtvlab:~/$ host -t A youtube.com b.res-nsdi.ru
Using domain server:
Name: b.res-nsdi.ru
Address: 195.208.5.1#53
Aliases:

Host youtube.com not found: 3(NXDOMAIN)
```

Figure 4: Resolving youtube.com against the two NSDI resolvers, February 2026: both answer NXDOMAIN. Source: Habr, “Эксперты: Роскомнадзору может не хватать мощности ТСПУ”²¹

2. Ownership & Operation

2.1 State ownership and centralised management

TSPU equipment is state property, supplied to the operator free of charge and recoverable on demand. ISPs must give GRFC remote access to the device and must not obstruct its remote management³⁴. Physical access to the device and to the node must be given within 48 hours, a deadline written into the rules because large operators' internal approval procedures were delaying maintenance⁰⁶.

All devices are managed remotely by GRFC via a centralised system. ISPs have no access to device configuration, filtering rules, or operational status. GRFC deploys filter-rule changes without notifying operators¹⁷. ISP practitioner accounts describe regular false positives (services breaking with SSL timeouts, sites becoming inaccessible because their CDN host was added to filter lists) that are difficult to diagnose because there is no alerting system and no published changelog¹⁷. Filtering rules are not uniform across installations: a resource blocked through one ISP may be accessible through another¹⁷. Multiple agencies beyond RKN can add blocks via TSPU, including NKCCI (the National Coordination Centre for Computer Incidents) for security vulnerabilities, and these additional blocks are not published on RKN's registry¹⁷.

№ п/п	Перечень ключевых мероприятий по установке и обеспечению функционирования ТСПУ
I.	Утверждение радиочастотной службой (далее - РЧС) инструкции по взаимодействию уполномоченных лиц оператора связи с РЧС
II.	Оценка пропускной способности канала передачи данных, к которому подключается ТСПУ
III.	Разработка проектной документации на установку и функционирование ТСПУ
IV.	Представление и согласование перечня лиц, допущенных к установке ТСПУ
V.	Выполнение работ по организации технологического канала связи, к которому подключается ТСПУ
VI.	Проведение пусконаладочных работ ТСПУ
VII.	Подключение оператором связи ТСПУ к своей сети связи
VIII.	Проведение приемо-сдаточных испытаний ТСПУ
IX.	Представление и согласование перечня лиц, допущенных к обслуживанию ТСПУ
X.	Опытная эксплуатация ТСПУ, в том числе устранение недостатков, выявленных при их опытной эксплуатации
XI.	Сдача в эксплуатацию ТСПУ
XII.	Модернизация ТСПУ**
XIII.	Порядок возврата ТСПУ**

Figure 5: Key activities for the installation and operation of TSPU equipment per Government Decree No. 126. Source: OrderKom.³⁴

ISP practitioner accounts confirm that operators must coordinate every infrastructure change through the state agency, creating friction around network architecture changes²⁶. Any changes to network topology must be reported to GRFC within 7 working days. All planned modernisation or liquidation of TSPU-

equipped nodes must be reported annually by 1 November, while the reconstruction or liquidation affecting TSPU locations requires 90 days' advance notice³⁴.

Because those reporting duties are continuous, the state holds a running map of licensed network architecture. Network-level obfuscation strategies that depend on ISP topology remaining opaque to the state should be treated as unreliable.

Beyond mapping, the system is regularly used for disconnection exercises. Sergei Khutortsev, then head of CMU SSOP, confirmed at the 2022 Spektr Forum that exercises are conducted annually³⁵. The capability to disable international connectivity at scale has reportedly been present since 2023³⁵.

The compliance perimeter extends beyond ISPs. Cloud and hosting operators face parallel obligations with client identification requirements (legal entity in a Russian region, user identification via the Unified System of Identification and Authentication (ESIA) or passport) and GosSOPKA (the state cyber-incident reporting system) integration, which mandates a certified GOST VPN device. One cloud provider's account of its own registration describes a four-month wait for that device, a supplier field it puts at "roughly two and a half vendors" oriented to large state buyers, and a first quote above 10 million roubles³⁶. Cloudflare's forced registration as an Organiser of Dissemination of Information (ORI) in February 2025 extended the same logic to CDN providers: any infrastructure serving Russian users is pulled into the licensing and reporting framework³⁷. CDN-fronted distribution and Russian-hosted infrastructure are subject to the same identification and reporting regime that binds ISPs.

2.2 Operational modes

In **blocklist mode**, TSPU executes centrally-managed filter rules to block, throttle, or degrade access to resources. In **allowlist mode**, ordinary access is restricted to pre-approved services. Circumvention may still exploit reachable infrastructure, but its availability and cost depend on the network and the service³². The allowlist mode is deployed in conflict-adjacent regions, areas under permanent restriction³⁸, and strategic military regions³⁹.

The first tier of the list, managed by the Ministry of Digital Development, covers commercial and public services, which are selected by popularity. The second is gated by the security bureaus (e.g. FSB), where admission turns on interception capability: in early 2026 the FSB barred the apps of banks that had not installed SORM, leaving Sberbank, T-Bank and Gazprombank outside the

list while VTB and Promsvyazbank were admitted. Full implementation becomes mandatory for banks in 2027⁴⁰. The list is therefore a compliance-gating mechanism in itself, not just a way to maintain essential access during shutdowns⁴⁰.

In June 2025 alone, 655 mobile internet shutdowns were documented³⁹. Mobile and fixed-line networks have operated differently, with the latter rarely entering allowlist mode. The distinction may be eroding. In March 2026, users in Rostov-on-Don reported restrictions limiting home-internet access to approved services, with Telegram blocked and VPNs non-functional on fixed broadband. The operator disputes the account⁴¹.

3. Blocking in Practice

3.1 VPN blocking

TSPU performs network-level blocking, but Russia's controls extend beyond DPI⁴². The state combines several mechanisms:

Domain blocking. VPN provider websites are removed from NSDI or blocked at the DNS layer, preventing sign-up and download.

IP blocking. Known server addresses are blocked.

Protocol blocking. DPI-based traffic shaping of VPN protocols (OpenVPN, WireGuard, Shadowsocks/VLESS variants), regardless of destination server. This is the most operationally consequential capability: it targets how circumvention tools communicate, not just where they connect.

App store removal. Apple continues removing VPN clients from the Russian App Store on RKN request, without requiring a court order⁴³.

Advertising and information bans. From March 2024, publishing articles about how to use VPN or Tor is illegal⁴⁴.

Evading protocol detection is only one condition of usable access. Users must also discover a trustworthy service, obtain its client, pay where necessary, complete setup, and keep the connection working as blocking changes³². App-store removals and information bans obstruct some of these steps. Payment barriers, misleading offerings, and repeated configuration changes obstruct others. Socket's August 2026 investigation documented VPN-brand impersonation tar-

getting Russian-speaking users seeking access to blocked services⁴⁵. Technical support and accessible onboarding therefore matter alongside protocol resilience.

The cumulative number of targeted services nearly tripled, from 167 in October 2023 to 469 by February 2026^{46, 47, 42}. Regional protocol blocking was already being tested in January 2023, when providers reported access failures in Altai, Biysk, Omsk and Novosibirsk while their server addresses remained unblocked⁴⁸. Later that year, a Roskomsvoboda survey found access problems affecting at least 6 of 15 popular services after OpenVPN and WireGuard were blocked. Collectively, the services used OpenVPN, WireGuard, Shadowsocks, IKEv2 and V2Ray⁴⁹.

RKN's December 2025 digitalisation plan allocated 2.27 billion roubles to machine-learning traffic analysis but did not specify its targets. Analysts infer encrypted and obfuscated traffic that defeats classical DPI signatures¹⁶. VPN developers separately report an ML system analysing copied traffic dumps post-hoc alongside DPI³². This does not show that the funded system is operational. RKN also monitors high-traffic servers and buys VPN access keys to identify and block them³². One developer describes that purchasing as automated: a test rig built from the service's own client, loaded with freshly issued configuration files, from which an aggregate protocol fingerprint is derived and used to block servers⁵⁰.

When technical circumvention succeeds, the state raises the cost of sustaining it. VPN providers with large user bases estimate that fully countering active blocking would cost tens of thousands of dollars per hour, resources they report not having. Smaller services face financial unviability from continuous server replacement costs³². The resulting cost may drive providers to withdraw rather than adapt.

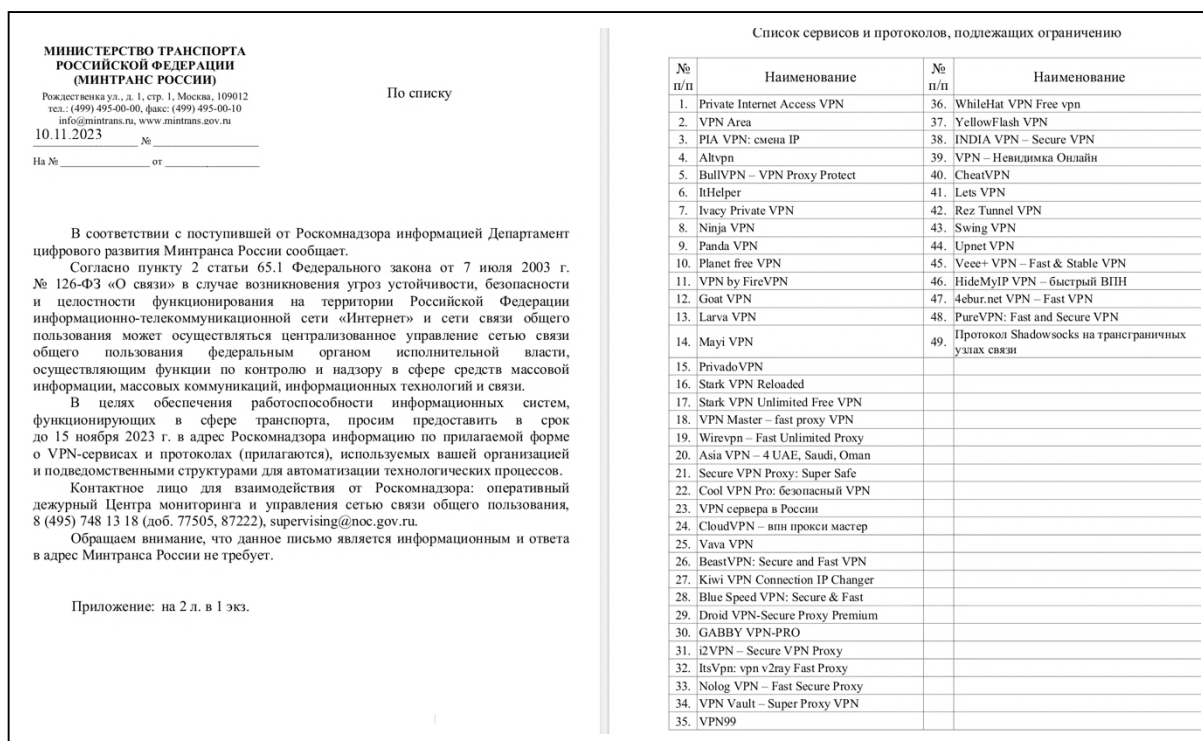


Figure 6: Ministry of Transportation letter forwarding RKN VPN blocklist to operators — ~70 services with protocol identifiers, October 2023. Source: Russian Ministry of Transport (October 2023, via Roskomsvoboda).⁴⁹

3.2 Escalation, collateral damage, and the ECH decision

An RKN order drafted in October 2024 would authorise the regulator to restrict any service for Russian users at the request of the Prosecutor General or a deputy prosecutor, implemented through TSPU throttling or binding mandatory instructions to operators⁵¹. YouTube²⁰ and WhatsApp²² have both followed the DPI throttling → DNS removal sequence. Telegram remains at the throttling stage²³. When Beeline briefly offered a “YouTube without VPN” service in January 2026, effectively routing around the throttling for subscribers, it was shut down within days under regulatory pressure⁵².

SNI visibility is central to application-layer filtering, and CDN operators are required to preserve it upstream. When Cloudflare enabled ECH by default in October 2024, it encrypted the field TSPU uses for selective blocking. On 7 November, GRFC’s operational arm urged Russian website operators to disable ECH or migrate to domestic CDNs, saying the extension was restricted by TSPU and violated Russian law³¹. RKN repeated the recommendation in April 2025³¹. Between those interventions, RKN entered Cloudflare in the register of organisers of dissemination of information, requiring it to store user data in Russia and provide FSB access³⁷. The March 2025 measurements found selective ECH blocking under Cloudflare-related conditions, while also demonstrating circumvention. They do not establish uniform ECH blocking across Russian net-

works³⁰. Because ISPs cannot inspect TSPU rules, they could neither exempt affected services nor mitigate the effects for business customers.

Blocking OpenVPN and WireGuard signatures affects Twitch streams, BitTorrent traffic, and online gaming³². It also disrupts legitimate corporate VPN traffic: Roskomsvoboda documented that Russian banks and commercial companies rely on OpenVPN for secure internal communications⁴⁹. The protocol-exemption list is administered by CMU SSOP: applications to `white_list@cmu.gov.ru` must declare organisation and tax number, protocol, source and destination IP, and the purpose of the connection. RKN head Andrei Lipov put it at 12,000 corporate IP addresses in October 2023. RKN reported 75,000 entries as of 16 April 2025⁵³. An exemption requires a declaration of what the network runs and why. That route is unavailable to circumvention infrastructure.

In January 2025, a TSPU misconfiguration cascaded across ISPs, causing an 11% dip in MSK-IX traffic before rollback within twenty minutes⁵⁴. Operators could not bypass the broken filtering path or exempt their customers.

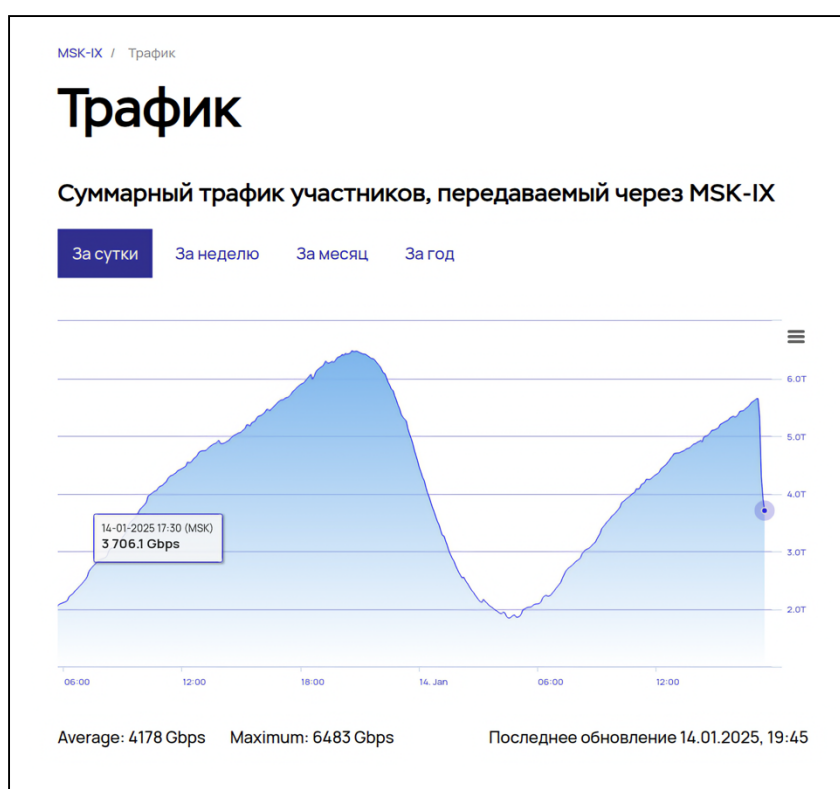


Figure 7: MSK-IX traffic during the 14 January 2025 TSPU outage. The ~11% dip (4,178 → 3,706 Gbps) marks the degraded-bypass window. Source: MSK-IX traffic graph.⁵⁴

3.3 Transit censorship and DPI extraterritorial effects

Filtering effects extend beyond Russia wherever traffic transits a Russian AS using state-owned TSPU or ISP-purchased commercial equipment. Ortwein et al. (2023) scanned address space in 18 countries surrounding Russia and found Russian censorship blockpages returned to traffic destined for at least 8: Afghanistan, Azerbaijan, Kazakhstan, Kyrgyzstan, Lithuania, South Korea, Tajikistan and Ukraine²⁹. At least 6 Russian ASes were responsible. The authors treat this as a lower bound determined by their vantage points, not as evidence about every transit link in the region²⁹.

AS3216 (PJSC Vimpelcom) produced the widest geographic reach, returning Russian blockpages to destinations across Central Asia and Eastern Europe. Two other identified networks, AS60299 and AS201776 (Miranda-Media), use VAS Experts' commercial SKAT/Stingray DPI platform²⁹, ⁵⁵. VAS Experts reports more than 2,000 installations of that platform globally since 2013⁵⁶.



Figure 8: Fibre routes from Russia through the Urals to Kazakhstan, Kyrgyzstan, Tajikistan, and Afghanistan. Traffic transiting these routes crosses Russian networks subject to TSPU and to operator-purchased commercial DPI, exposing neighbouring states to Russian filtering rules. Source: Habr, “Пытаюсь представить жизнь при суверенном интернете в России.”²⁹

For ISPs in neighbouring states whose upstream transit paths cross Russian backbone infrastructure, traceroute alone does not reveal an inline filtering device as a separate hop. Identifying interference requires evidence of how traffic is treated²⁹. Ukraine is subject to the most extensive transit censorship, likely due to re-routing of Ukrainian internet traffic through Russian telecommunications infrastructure in occupied territories. Fontugne, Ermoshina and Aben (2020) documented this post-annexation rerouting pattern for Crimea

after 2014⁵⁷. Limonier et al. (2021) mapped the same pattern in eastern Ukraine⁵⁸, but the technical dynamic is now reproduced at a larger scale across the post-2022 occupied territories²⁹.

Any network measurement study of internet freedom in Central Asia, the Caucasus, or Eastern Europe must account for the possibility that observed blocking originates not from local censorship infrastructure but from Russian transit filtering. Changes to TSPU configuration, including blocking errors and false positives, could propagate beyond Russia's borders.

4. Implications for Tool Development

4.1 Market consolidation and regulatory compliance

The number of valid telecom licences halved from 53,538 to 26,229 between May 2016 and April 2025, though that count covers radio, satellite and television broadcasting alongside internet services and so does not on its own measure ISP attrition⁵⁹. Entry costs also rose: since January 2024 a new licence carrying lawful-interception obligations costs 1,000,000 roubles per service type against 7,500 before, though renewals were untouched⁵⁹. In January 2026, Roskomnadzor reported violations at 33 telecom operators in the installation and operation of traffic-filtering equipment⁶⁰. A single order in December 2025 cancelled 943 licences, about 4% of the register, on the ground of non-provision of services rather than any filtering obligation⁶¹.

If consolidation produces fewer, larger operators, tool distribution will face fewer network paths, more uniform filtering, and less variation in TSPU implementation to exploit. SORM remains mandatory alongside TSPU, and its current generation integrates the earlier ones: SORM-3 brings together interception and traffic storage and adds control of some VPN servers, Skype interception, communications data from encrypted messengers, and satellite links, with end-to-end encrypted services yielding metadata only⁶². A telecom licence now carries both obligations: compliance with network requirements, including TSPU, as a licensing condition under Federal Law No. 473-FZ in force from December 2024⁵⁹, and SORM compliance verified by the FSB⁶³. The two obligations differ in who carries them: TSPU equipment is supplied by the state and operated remotely from it, while SORM is operator-funded and operator-implemented⁶⁴, under regional FSB curators⁶⁵.

—

App-store removals, information bans, and server blocking mean technical capability alone is insufficient. Awareness, trust, usable payment methods, and help with setup and configuration changes also shape whether users can obtain and sustain access^{32, 45}. Under allowlist mode, circumvention tools may be unreachable on mobile even where they work on fixed broadband. CDN-based distribution and domain fronting face the same pressure as the compliance perimeter expands beyond ISPs to providers serving Russian users³⁶. The cost of continuous evasion can itself restrict access.

4.2 Network security and system entrenchment

TSPU's expansion into network security creates structural lock-in because removing it would also mean losing DDoS defence and vulnerability monitoring. As the system's operational rationale diversifies, challenging the content-control function in isolation underestimates what sustains the infrastructure.

The National Anti-DDoS System (NSPA), operational since March 2024, uses 88 TSPU devices handling cross-border traffic—the 'transborder' segment—as its first echelon of volumetric attack filtering⁶⁶. The segment covers nodes where traffic enters or leaves Russia, within an operator's network or at its interconnection with international infrastructure²⁷. In 2025, RKN recorded over 21,000 DDoS incidents, more than double the previous year⁶⁷. A "Security Scanner", built for GRFC under a contract let in 2023 at 465 million roubles, was still undergoing trial operation when it was reported to have found 26,000 critical vulnerabilities across more than 300 Russian companies in 2024. Roskomnadzor says exposed services can be blocked at the TSPU level, temporarily or permanently, where the owner does not act on its warnings⁶⁸.

During the 2024 Conference of Russian Telecom Operators (KROS), GRFC representatives shared the current status of NSPA and its development roadmap. The speaker highlighted a new TSPU API that enables DDoS protection providers and large infrastructure owners to apply TSPU countermeasures on their own declared IP ranges, commercially and only across the transborder segment. No mechanism yet exists for applying TSPU countermeasures on the intra-Russian segment, he said, and building one is harder⁶⁹. Operators used the Q&A to raise concerns about service failures, filtering transparency, and notification. The speaker acknowledged that closer coordination would be needed. TSPU is therefore becoming part of routine network-security operations as well as content control.

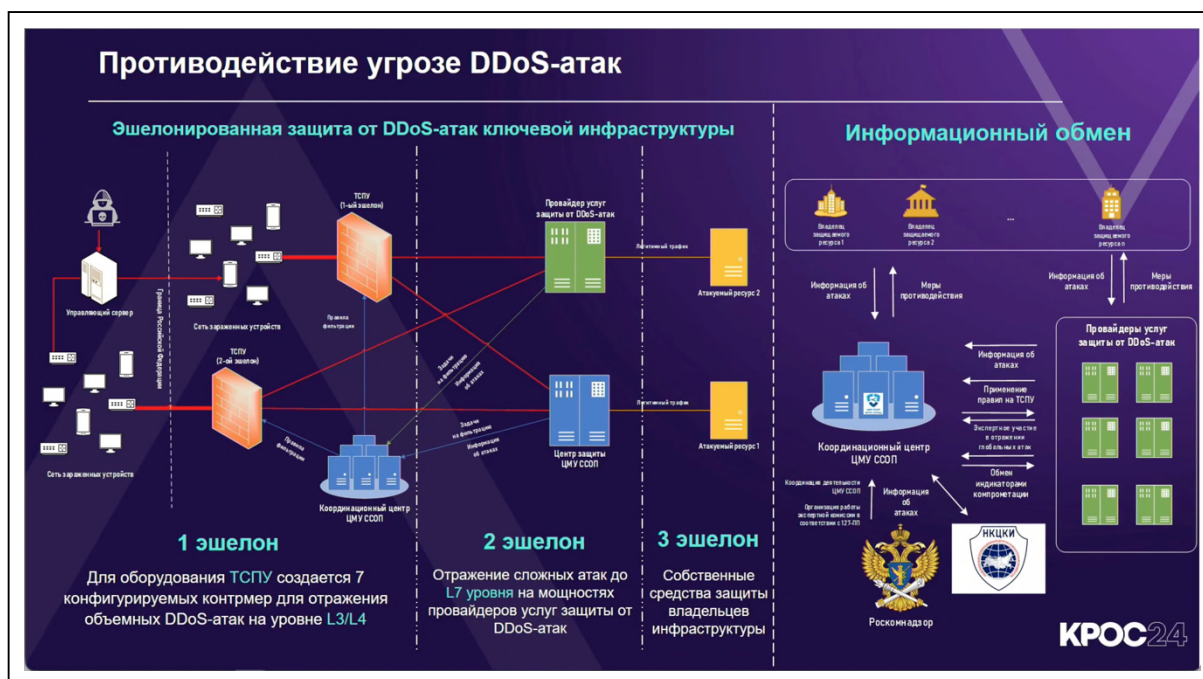


Figure 9: NSPA echeloned DDoS defence architecture: TSPU as first echelon (L3/L4, 7 configurable countermeasures), cloud anti-DDoS providers as second echelon, resource owner infrastructure as third. Source: GRFC, KROS 2024.⁶⁹

4.3 Protocol detection and evasion

Tools with stable, identifiable traffic signatures will be detected over time. The first protocol-level blocking was reported in 2021. Regional waves followed through 2022 and early 2023, and sustained nationwide blocking of OpenVPN and WireGuard dates from the second half of 2023^{48, 49}. TSPU uses two principal detection approaches, which tools seek to evade through mimicry:

- ◆ Signature-based detection matches known protocol fingerprints and is effective against standard VPN protocols.
- ◆ Traffic fingerprinting identifies encrypted protocols by packet-size patterns and session behaviour, even without a protocol signature.

Protocol mimicry makes VPN traffic resemble permitted traffic types, but the advantage is temporary. AmneziaWG 1.0, a WireGuard fork built for mimicry, was blocked in summer 2025. A developer of the service reports that AmneziaWG 2.0 was then blocked in waves during June and July 2026, after roughly a year of signature collection⁵⁰. The same account describes a shift from detecting the protocol to identifying the servers carrying it: scoring rules combine multiple weak indicators, especially traffic volume, and trigger blocking at address and subnet level even where the protocol continues to negotiate⁵⁰. Pressure on UDP traffic rose alongside it, with online games reported as collateral⁵⁰.

Tool developers must treat protocol viability and service viability as separate problems. Obfuscation alone does not address exposure associated with traffic volume and the concentration of users on identifiable infrastructure⁵⁰. Distribution through smaller brands or channels may change a service’s visibility and reach, but whether it reduces detection depends on the infrastructure behind those offerings. Several brands can still share the same servers.

Changes that require a new client release can be delayed by app-store review. An Amnezia developer reported a three-to-four-day turnaround during the 2026 blocking waves⁵⁰. Where the installed client already supports the required functionality, remotely updated connection settings can allow adaptation without a new release. Outline’s dynamic access keys, for example, point to remotely hosted connection settings that can be changed without issuing new keys⁷⁰. This still depends on users being able to reach the configuration service. ISP practitioners periodically report operational incidents from over-blocking, caused by filtering rules that cannot distinguish all traffic types²⁶. Tools need protocol diversity and the ability to adapt as detection changes.

9. Формат передаваемой информации, предусмотренной подпунктом «г» пункта 2 настоящего Порядка, должен соответствовать следующим требованиям:

а) поле данных выделяется следующими символами «{ }» (фигурные скобки и запятая);

б) информация предоставляется при помощи программного приложения и имеет вид «{ID}, {TTL}, {xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xx}, {xxx.xxx.xxx.xxx}, {Operation}, {Timestamp}, {x...x}», где:

ID – уникальный идентификатор пользовательского оборудования (оконечного оборудования);

TTL – срок использования протоколов в формате IPv4 и IPv6 (количество знаков определяется оператором связи в зависимости от срока использования протоколов в формате IPv4 и IPv6, измеряемого в минутах и состоящего из положительных целых чисел);

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xx – выделенный сетевой адрес в соответствии с протоколом в формате IPv6;

xxx.xxx.xxx.xxx/xx – выделенный сетевой адрес в соответствии с протоколом в формате IPv4;

Operation – операция, положительное целое число, где:

0 – окончание использования протоколов в формате IPv4 и IPv6;

1 – начало использования протоколов в формате IPv4 и IPv6;

2 – продление использования протоколов в формате IPv4 и IPv6;

Timestamp – время создания записи оператором связи (количество миллисекунд, прошедших с полуночи 1 января 1970 года), целое число.

x...x – целые положительные числа, обозначающие уникальные номера технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети «Интернет» и сети связи общего пользования, на которые осуществляется пропуск трафика пользователя услугами связи.

Figure 10: The reporting format proposed in Roskomnadzor’s December 2024 draft: user-equipment identifier, TTL, IPv6 and IPv4 addresses, operation code, timestamp and TSPU serial numbers. The final Order No. 51 does not include the user-equipment identifier. Source: RKN.⁷¹

4.4 Comprehensive data collection and coordination

Tools should assume that unencrypted HTTP requests can be logged, and that subscriber identity is obtainable within 24 hours. RDP.RU's EcoFilter product line, from which TSPU hardware is drawn, advertises the logging of every subscriber HTTP GET request to an external server. Which functions are enabled on a given TSPU deployment is not published⁷².

In November 2022, Roskomnadzor and the Ministry of Digital Development announced a traffic-route monitoring system budgeted at 1.2 billion roubles for 2023 and 2024, to be built by CMU SSOP. As announced, it would map how traffic moves between networks at the level of BGP routing and interconnection and let Roskomnadzor identify operators not meeting its requirements. We found no later public account confirming whether it was completed or became operational⁷³.

Under Roskomnadzor Order No. 51, in force since 12 April 2025, ISPs must report the network addresses allocated to users, the municipality where they are used, and the unique numbers of the TSPU through which that traffic passes — including TSPU belonging to upstream operators — filing changes through the Roskomnadzor portal within one calendar day. Where an operator issues dual-stack IPv4/IPv6 addresses, the paired addresses and TSPU numbers pass to CMU SSOP automatically over a secured channel, GOST-encrypted, within one hour of any change. Operators licensed before commencement had six months to comply, new entrants fifteen working days⁷⁴.

From September 2025, new anti-fraud amendments give the Ministry of Internal Affairs and the FSB warrantless access to the subscriber identity data collected by ISPs. A request must be fulfilled within 24 hours via the Interagency Electronic Interaction data exchange system⁷⁴. The scope includes full name, passport details, contract dates, IMSI, and SIM-card identifiers.

Tracking the system. Much of this system's architecture and operation is documented in publicly available Russian-language sources. GRFC publishes monthly and annual operational reports covering domain-system availability, autonomous-system connectivity, traffic distribution by federal district, and the Antifraud caller-verification system⁷⁵.

RKN's own legislative monitoring digests tracked the regulatory pipeline from concept to law: the May 2019 digest documented FZ-90's passage⁷⁶; the September 2019 digest recorded Order No. 228 (TSPU technical specifications, 100 Mbps minimum channel requirement)⁷⁷; the February 2020 digest documented Gov-

ernment Decrees No. 126 and 127 (state ownership and centralised management rules)⁷⁸. The RANR (Registry of Address and Number Resources), whose public service launched in April 2024, provides Russia’s domestic IP and AS address allocation data, independent of RIPE NCC. Its development left an extensive public record. The principal barrier is that much of it is in Russian.

The system documented here is a moving target. Continued investment in traffic analysis, NSPA expansion, and the expansion of approved-access restrictions from mobile to fixed broadband all signal continued development. Tool design should assume that the configuration documented here will change and should account for controls across network layers, TSPU’s growing security role, and consolidation among operators.

Table 2. Protocol status and observed blocking approaches as of August 2026 (likely to change).

Protocol / approach	Blocking mode	Status	First observed	Notes
OpenVPN	Signature-based	Blocked	Jan 2023	85% fingerprinted in controlled testing ⁴⁹ . Session terminated after DATA packets ⁴⁹
WireGuard (standard)	Signature-based	Blocked	Sep 2021	UDP blocked after 1–5 Transport Data packets from server ⁴⁹
IKEv2 / IPsec	Signature-based	Blocked	Jan 2023	Widely used for corporate VPNs. Blocked during session establishment ⁴⁹ . Protocol exemptions grew to 75,000 entries by April 2025 ⁵³
L2TP	Signature-based	Blocked	Aug 2023	Control Message packets blocked before reaching server ⁴⁹
SOCKS5 (unobfuscated)	Signature-based	Blocked	Nov 2025	Per industry reporting, corroborated by named telecom and infosec experts ⁷⁹
Shadowsocks / VMess	Traffic fingerprinting	Blocked	Apr–May 2024	No protocol signature. Detected by packet size patterns during TLS handshake (client sends 3 packets of 411+ bytes → blocked) ⁸⁰ . Different detection approach than standard VPNs
VLESS (basic)	Heuristic + partial signature	Partially blocked	2024–2026	RKN began filtering VLESS via heuristics (foreign IPs, domain mismatch) in November 2025 ⁷⁹ . By Feb 2026, a VPN developer reported <5% detection for well-configured VLESS, versus 100% for OpenVPN/WireGuard, 95% Shadowsocks and 80% VMess ⁸¹
AmneziaWG 1.0	Signature-based	Blocked	Summer 2025	First blocking of the fork's own signature rather than WireGuard's. The developer treats it as evidence of dedicated analytic effort against a single protocol ⁵⁰
AmneziaWG 2.0	Signature-based	Blocked	Jun 2026	The developer reports signatures collected over roughly a year and deployed on 1 June, 7 July and 25 July 2026, with the later waves answering client fixes ⁵⁰
AmneziaWG 3.0	Mimicry evasion	Reported viable	—	Added to AmneziaVPN v5.0 after the June–July 2026 wave. The developer reports access restored for updated clients ⁵⁰ . The protocol adds junk data and can mimic permitted traffic types ^{32, 80}
XRay VLESS (Reality)	Mimicry evasion	Reported viable	—	TLS-based obfuscation with real server certificates. Services on VLESS/Xray were less affected by the June 2026 wave ^{32, 50}

Notes

- 01** Gavriluk, A., ‘RKN casts a new net: 59 billion roubles to overhaul the site-blocking system’ (in Russian), Forbes Russia, 10 September 2024. <https://www.forbes.ru/tekhnologii/520876-rkn-pletet-novye-seti-sluzba-obnovit-sistemu-blokirovki-sajtov-za-59-mlrd-rublej> (archived)
- 02** Habr, ‘Ministry of Digital Development plans to raise TSPU capacity to 954 Tbit/s by 2030’ (in Russian), 25 March 2026, relaying Kommersant. <https://habr.com/ru/news/1014590/> (archived)
- 03** Xue, D., et al. (2022). ‘TSPU: Russia’s decentralized censorship system’. Proceedings of the 22nd ACM Internet Measurement Conference (IMC ’22). <https://dl.acm.org/doi/10.1145/3517745.3561461> (archived)
- 04** Cableman.ru, ‘Roskomnadzor blocked 50% more resources in 2025’ (in Russian), 24 October 2025. <https://www.cableman.ru/content/kolichestvo-zablokirovannykh-roskomnadzorom-resursov-vyroslo-na-50-v-2025-godu> (archived)
- 05** GRFC portal, ‘Address by ЦМУ ССОП director Sergei Khutortsev to the Spektr-2022 forum’ (in Russian), 26 October 2022. <https://portal.noc.gov.ru/ru/news/2022/10/26/vystuplenie-direktora-cmu-ssop-sergeya-hutorceva-na-forume-spektr2022/> (archived)
- 06** Tyomny, S., ‘Telecom Operators’ Obligations to Install TSPU and Pass Network Traffic’ (in Russian), MUSE 2022. Video, <https://www.youtube.com/watch?v=7aJE80KTVHM> (archived)
- 07** Interfax, ‘All communications nodes in Russia are 100% equipped with threat-counteracting means’ (in Russian), 24 October 2023. <https://www.interfax.ru/russia/927357> (archived)
- 08** Order of the Ministry of Digital Development No. 219, 16 March 2026, in force 6 July 2026, scoped to 5G/IMT-2020 subscriber terminals in satellite mode. Draft reported at Forbes Russia (in Russian), 11 August 2025. <https://www.forbes.ru/tekhnologii/543650-mincifry-obazet-sputnikovyh-operatorov-oborudovat-nazemnye-stancii-sorm-i-tpsru> (archived)
- 09** Melnikova, Yu., ‘ТСПУ по правилам и без’ (in Russian), ComNews, 31 March 2021. <https://www.comnews.ru/content/213851/2021-03-31/2021-w13/tspu-pravilam-i-bez> (archived) For the 2025 intra-group restructuring and consolidation under Gradient: CNews, ‘У создателя решений для блокировок в Рунете новый хозяин’ (in Russian), 30 September 2025. https://www.cnews.ru/news/top/2025-09-30_u-sozdatelejreshenij_dlya (archived)
- 10** CNews, ‘Authorities begin managing Runet blocking with domestically produced equipment’ (in Russian), 10 July 2024. https://www.cnews.ru/news/top/2024-07-10_vlasti_nachali_upravlyat (archived)
- 11** RDP.RU, ‘EcoFilter: Functional URL-Filtering’, datasheet (in Russian), 2 pp., 1 February 2024, revised 28 March 2025. The 24–200 Gbps range is the model table, p. 2 (EcoSGE 2020–5200). The sheet’s prose and the English sheet still state 160 Gbit/s.
- 12** RDP.RU, ‘EcoBalancer: Network Packet Broker and Load Balancer’, datasheet (in Russian), 2 pp., 6 October 2021, p. 1.
- 13** The throughput figures and the P4 description are from the EcoBalancer datasheet (RDP.RU, 6 October 2021), which rates the EcoSwitch 1020, 1032 and 2065 platforms at up to 2.0, 3.2 and 6.4 Tbit/s. Platform context: RDP.RU, ‘EcoSGE Service Platforms’ webinar annotation (in Russian), NAG, 2021. <https://nag.ru/material/41081> (archived)
- 14** Tyomny, S. (GRFC), interviewed in ‘Roskomnadzor reports full import substitution of TSPU equipment’ (in Russian), Rossiyskaya Gazeta, 3 June 2024. <https://rg.ru/2024/05/31/v-roskomnadzore-rasskazali-o-polnom-importozameshchenii-oborudovaniia-tpsru.html> (archived)
- 15** GRFC, ‘TSPU: Hardware Localisation’ (S. Tyomny) (in Russian), video clip, 2024. https://vkvideo.ru/@grfc_ru/clips?z=clip-223065867_456239070%2Fclub223065867 (archived)
- 16** ComNews, ‘Algorithmic exercises: RKN to filter traffic using machine learning’ (in Russian), 19 January 2026. <https://www.comnews.ru/content/243319/2026-01-19/2026-w04/1009/algorit>

micheskie-uprazhneniya-rkn-budet-filtrovat-trafik-pomoschyu-mashinnogo-obucheniya
(archived)

- 17** Vasiliev, P., 'TSPU: A Year in Operation' (in Russian), pavel.su blog, 18 August 2023. <https://pavel.su/internet/tspu-1-year/> (archived)
- 18** wkrp, 'Blocking of DNS, DoH, DoT servers (Google, Cloudflare, OpenDNS) in Russia', net4people/bbs, GitHub issue 81, opened 8 September 2021. <https://github.com/net4people/bbs/issues/81> (archived)
- 19** Teplitsa of Social Technologies, 'What is happening with DNS in Russia? We may have found signs of censorship. Analysis no. 26' (in Russian), 7 August 2026, updated 31 August 2026. <https://test.org/2026/08/07/dnsdnsdns/> (archived)
- 20** Habr, 'YouTube throttling from the technical side: restriction and circumvention' (in Russian), 31 July 2024. <https://habr.com/ru/articles/832678/> (archived)
- 21** Habr, 'Experts: Roskomnadzor may lack the TSPU capacity to throttle two large resources at once — YouTube and Telegram' (in Russian), 10 February 2026. <https://habr.com/ru/news/995016/> (archived)
- 22** Habr, 'Missing from RKN's DNS servers: YouTube, WhatsApp, Facebook, Instagram, Messenger, Tor-project and others' (in Russian), 11 February 2026. <https://habr.com/ru/news/995512/> (archived)
- 23** Habr, 'Senator Sheikin: restrictions on Telegram are being introduced step by step, hence the trouble loading video' (in Russian), 21 January 2026. <https://habr.com/ru/news/987526/> (archived)
- 24** Vasiliev, P., 'TSPU as a Threat to the Russian Internet-Transit Business' (in Russian), pavel.su blog, 20 December 2022. <https://pavel.su/internet/tspu-as-a-threat/> (archived)
- 25** Revizor is RKN's compliance-monitoring system, distinct from TSPU itself. Revizor checks that ISPs are correctly blocking resources on the federal blocklist. TSPU performs the actual filtering. The operator's complaint is that RKN controls both the blocking and the monitoring of that blocking, while the ISP bears legal liability.
- 26** Vasiliev, P., 'Installing TSPU' (in Russian), pavel.su blog, 12 December 2022. <https://pavel.su/internet/setting-up-tspu/> (archived)
- 27** Selectel, 'Diagnosing TSPU interference' (in Russian), documentation, updated 27 August 2026, consulted 22 September 2026. <https://docs.selectel.ru/dedicated/troubleshooting/tspu/> (archived, earlier version)
- 28** Habr, 'Yaroslavl provider Yarnet reveals how RKN's TSPU behaves during an outage on the operator's network' (in Russian), 17 November 2023. <https://habr.com/ru/news/774734/> (archived)
- 29** Ortwein, A., Bock, K. and Levin, D. (2023). 'Towards a Comprehensive Understanding of Russian Transit Censorship'. Free and Open Communications on the Internet (FOCI 2023). <https://www.petsymposium.org/foci/2023/foci-2023-0012.php> (archived)
- 30** Niere, N., Lange, F., Heitmann, N., and Somorovsky, J. (2025). 'Encrypted Client Hello (ECH) in Censorship Circumvention'. Free and Open Communications on the Internet, 2025(2), 64–73, especially §5 and Appendix A. <https://petsymposium.org/foci/2025/foci-2025-0016.pdf> (archived)
- 31** The recommendation was issued by ЦМЯ ССОП on 7 November 2024 and published at portal.noc.gov.ru; reported the same day by RBC (in Russian). https://www.rbc.ru/technology_and_media/07/11/2024/672cc8079a7947318949ba7d (archived) Reissued by RKN under its own name: Habr (in Russian), 2 April 2025. <https://habr.com/ru/news/896920/> (archived)
- 32** Meduza, 'Can all VPNs really be blocked? Meduza asked the biggest VPN services how they hold out against Roskomnadzor' (in Russian), 3 April 2026. <https://meduza.io/feature/2026/04/03/mozhno-li-deystvitelno-zablokirovat-vse-vpn> (archived)
- 33** Habr, 'Roskomnadzor begins drawing up charges under the "sovereign Runet" law' (in Russian), 1 September 2021, relaying Kommersant. <https://habr.com/ru/news/575732/> (archived)
- 34** Federal Law No. 126-FZ art. 65.1(3), under which the equipment is provided free of charge, with Government Decree No. 126 (in Russian), 12 February 2020, for transfer, return and the reporting

- deadlines. <https://portal.noc.gov.ru/documents/49/>
Постановление_Правительства_РФ_от_12_02_2020_N_126_p2W1A4X.docx (archived)
- 35** Habr, 'RKN, GRFC and telecom operators "switched off the international internet" on the night of 4–5 July' (in Russian), 5 July 2023. <https://habr.com/ru/news/746120/> (archived)
- 36** Habr (H3LLO.CLOUD corporate blog), 'The bureaucracy we went through to open a public cloud in Russia under the new laws' (in Russian), 4 February 2025. One provider's first-person account. https://habr.com/ru/companies/h3llo_cloud/articles/879236/ (archived)
- 37** Habr, 'Roskomnadzor forcibly enters Cloudflare in the register of organisers of dissemination of information' (in Russian), 20 February 2025. <https://habr.com/ru/news/884710/> (archived)
- 38** ComNews, 'A forced measure: what is happening with mobile-internet shutdowns' (in Russian), 12 November 2025. <https://www.comnews.ru/content/242284/2025-11-12/2025-w46/1009/vynuzhdennaya-mera-chto-proiskhodit-otklyucheniem-mobilnogo-interneta> (archived)
- 39** Belkova, E. and Rozhkov, R., 'Russia to get a list of services available during mobile-internet blocks' (in Russian), Forbes Russia, 7 August 2025. <https://www.forbes.ru/tekhnologii/543521-v-rossii-poavitsa-spisok-servisov-dostupnyh-v-period-blokirovki-mobil-nogo-interneta> (archived)
- 40** Cableman.ru, 'The Ministry of Digital Development expands the list of sites available during internet shutdowns' (in Russian), 17 November 2025, on the second stage of the list. <https://www.cableman.ru/content/mintsifry-rasshirilo-spisok-saitov-dostupnykh-pri-otklyucheniiyakh-interneta> (archived) The FSB veto over bank apps without SORM: Anti-Malware.ru, 4 February 2026, <https://www.anti-malware.ru/news/2026-02-04-111332/48928> (archived) The requirement set and the 2027 deadline: Frank Media, 26 February 2026, relaying Izvestia. <https://frankmedia.ru/263929>
- 41** Meduza, "'Durov's Code": Rostov-on-Don is testing a "white list" on home internet' (in Russian), 31 March 2026. <https://meduza.io/news/2026/03/31/kod-durova-v-rostove-na-donu-testiruyut-belyy-spisok-na-domashnem-internete> (archived)
- 42** Cableman.ru, 'Roskomnadzor has restricted access to 469 VPN services' (in Russian), 26 February 2026. <https://www.cableman.ru/content/roskomnadzor-ogranichil-dostup-k-469-vpn-servisam> (archived) On the wider environment: Roskomsvoboda, 'State of Surveillance' (2024).
- 43** Habr, "'Durov's Code": Apple continues removing VPN clients from the Russian App Store at RKN's demand' (in Russian), 28 March 2026. <https://habr.com/ru/news/1016186/> (archived)
- 44** Habr (Xeovo corporate blog), 'The ban on articles about Tor and VPN takes effect' (in Russian), March 2024. <https://habr.com/ru/companies/xevo/articles/797463/> (archived)
- 45** Pandya, K., '737 Chrome VPN Extensions Linked to Brand Impersonation and Browser Traffic Redirection', Socket, 11 August 2026. <https://socket.dev/blog/chrome-vpn-extension-impersonation> (archived)
- 46** For the 167: Habr, 'RKN: 167 VPN services and over 200 email services blocked in Russia since 2021' (in Russian), 25 October 2023. <https://habr.com/ru/news/769810/> (archived) For the 197: Human Rights Watch, 'Disrupted, Throttled, and Blocked', 30 July 2025, p. 21. <https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation> (archived)
- 47** Habr, 'RKN: 258 VPN services blocked in Russia in 2025' (in Russian), 24 October 2025. <https://habr.com/ru/news/959718/> (archived)
- 48** Roskomsvoboda, 'VPN-protocol blocking tests continue in Russia' (in Russian), January 2023. <https://roskomsvoboda.org/ru/post/blok-protokol-vpn-01-2023/> (archived)
- 49** Roskomsvoboda, 'VPN in Russia: from blocking services to blocking protocols' (in English), October 2023. <https://roskomsvoboda.org/ru/analysis/vpn-russia-2023-eng/> (archived) Carries the 6-of-15 finding and the protocol set tested.
- 50** Meduza, "'Theoretically they can block any service entirely": an interview with a developer of Amnezia VPN' (in Russian), 3 August 2026. <https://meduza.io/feature/2026/08/03/teoreticheski-oni-mogut-zablokirovat-lyuboy-servis-tselikom> (archived) See also Amnezia, 'How VPNs are blocked in Russia and what to do if Amnezia VPN won't connect' (in Russian), 16 July 2026. <https://amnezia.org/ru/blog/amnezia-vpn-no-connection-what-to-do> (archived)

- 51 Habr, 'Roskomnadzor drafts an order letting the regulator throttle any service as part of communications-network management' (in Russian), 12 October 2024. <https://habr.com/ru/news/850140/> (archived)
- 52 ComNews, 'Beeline adds the option of watching YouTube without a VPN for its subscribers' (in Russian), 21 January 2026. <https://www.comnews.ru/content/243370/2026-01-21/2026-w04/1009/bilayn-dobavil-vozmozhnost-smotret-youtube-bez-vpn-dlya-svoikh-abonentov> (archived)
- 53 Habr, '75,000 entries added to the "white list" of IP addresses using foreign encryption protocols' (in Russian), 17 April 2025. <https://habr.com/ru/news/901584/> (archived) The 12,000 is RKN head Andrei Lipov's figure of October 2023, the 75,000 RKN's own, of 16 April 2025. The application requirements are given there too.
- 54 Habr (X-Com corporate blog), 'When Runet goes down: causes of the large-scale internet outages in Russia, 2024–2025' (in Russian), 7 March 2025. <https://habr.com/ru/companies/x-com/articles/888840/> (archived) The ~11% is read from MSK-IX's published traffic graph, <https://www.msk-ix.ru/traffic/> (archived), as reproduced by Habr on 14 January 2025, <https://habr.com/ru/news/873606/> (archived) and <https://habr.com/ru/news/873630/> (archived). MSK-IX is a Moscow exchange-point measure.
- 55 VAS Experts, 'Stingray DPI and QoE Overview', product brochure, 41pp; copy consulted dated 21 October 2025. Listed at <https://vasexperts.com/resources/brochures/> (archived); product page <https://vasexperts.com/products/stingray/> (archived) The brochure is revised in place, so figures in the current revision may differ from the copy cited here.
- 56 VAS Experts, 'Stingray Service Gateway: DPI and QoE' product documentation: more than 2,000 installations since 2013. For the market chronology: Habr, 'A chronology of DPI development in Russia and the CIS' (in Russian), April 2022. <https://habr.com/ru/articles/663304/> (archived)
- 57 Fontugne, R., Ermoshina, K. and Aben, E. (2020). 'The Internet in Crimea: A case study on routing interregnum'. IFIP Networking Conference 2020. <https://ieeexplore.ieee.org/document/9142776> (archived)
- 58 Limonier, K., et al. (2021). 'Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine'. First Monday, 26(5). <https://firstmonday.org/ojs/index.php/fm/article/view/11700> (archived)
- 59 Two instruments. Federal Law No. 497-FZ, 28 September 2023, effective 1 January 2024, sets the 1,000,000-ruble duty on the *grant* of a licence. Renewals remain 7,500. <http://publication.pravo.gov.ru/Document/View/0001202309280013> (archived) The licensing condition and revocation grounds come from Federal Law No. 473-FZ, 4 August 2023, in force 1 December 2024. Licence figures: Human Rights Watch, 'Disrupted, Throttled, and Blocked', 30 July 2025, pp. 26–27.
- 60 SecurityMedia, 'Roskomnadzor found violations at 33 telecom operators in the installation of traffic-filtering equipment' (in Russian), January 2026. <https://securitymedia.org/news/roskomnadzor-vyyavil-narusheniya-u-33-operatorov-svyazi-pri-ustanovke-sredstv-filtratsii-trafika.html> (archived)
- 61 Roskomnadzor order No. 1146-rchs, 5 December 2025; reported by ComNews, 10 December 2025, <https://www.comnews.ru/content/242834/2025-12-10/2025-w50/1007/roskomnadzor-provel-massovyy-otstrel-licenziy> (archived) and Cableman.ru, <https://www.cableman.ru/content/roskomnadzor-annuliroval-pochti-tysyachu-litsenzii-operatorov-svyazi> (archived)
- 62 Roskomsvoboda, 'State of Surveillance' (2024), p. 29. Technical requirements are set by Order No. 573 of the Ministry of Communications, 29 October 2018, extended in September 2023 to VoWiFi and WiFi Calling. For the operator-side view: Galushko, D., 'Regulatory Risks for Telecom Operators' (in Russian), KROS 2017. Video, https://www.youtube.com/watch?v=NB-TvImn_cQ (archived)
- 63 Shakhmetova, O., 'Overview of Legislative Changes' (in Russian), MUSE 2023. Video, <https://www.youtube.com/watch?v=cZQob6Yw3vo> (archived)
- 64 Ermoshina, K., Loveluck, B. and Musiani, F. (2022). 'A market of black boxes: The political economy of Internet surveillance and censorship in Russia'. Journal of Information Technology & Politics, 19(1). <https://doi.org/10.1080/19331681.2021.1905972> (archived)

- 65** KROS 2019 roundtable, 'The Nuances of Implementing SORM and the Yarovaya Package in Practice' (in Russian). Video, <https://www.youtube.com/watch?v=HMG2tic5dTQ> (archived)
- 66** Cableman.ru, 'Roskomnadzor plans to scale up the National Anti-DDoS System to defend against internal threats' (in Russian), 28 October 2025, relaying Kommersant (kommersant.ru/doc/8159639). <https://www.cableman.ru/content/roskomnadzor-planiruet-masshtabirovat-natsionalnuyu-sistemu-protivodeistviya-ddos-atakam> (archived) The 88 transborder devices are Oleg Diyansky, head of GRFC's cyberthreat-protection centre, at the Spektr-2025 forum.
- 67** Cableman.ru, 'Roskomnadzor: DDoS attacks more than doubled in 2025' (in Russian), 19 January 2026, relaying Kommersant. <https://www.cableman.ru/content/roskomnadzor-v-2025-godu-chislo-ddos-atak-velichilos-bolee-chem-vdvoe> (archived)
- 68** Habr, 'RKN's "Security Scanner" found 26,000 critical vulnerabilities in the networks of 300 Russian companies in 2024' (in Russian), 25 October 2024, reporting Khutortsev at the Spektr-2024 forum the previous day. <https://habr.com/ru/news/853330/> (archived)
- 69** Smirnov, V. (GRFC), 'Developing Measures to Counter Threats to Communications-Network Security' (in Russian), KROS 2024. Video, <https://www.youtube.com/playlist?list=PLKzXMzX502jECS-BeePir4NsegcDnb6Bow> (archived)
- 70** Outline, 'Dynamic Access Keys', Outline Developer Documentation, undated, consulted 22 September 2026. <https://developer.getoutline.org/vpn/management/dynamic-access-keys/> (archived)
- 71** Roskomnadzor Order No. 51 of 28 February 2025, made under Federal Law No. 126-FZ art. 46, cl. 5.2-1 (inserted by Federal Law No. 216-FZ, 8 August 2024); registered with the Ministry of Justice 31 March 2025, reg. no. 81700, in force 12 April 2025. Draft consultation record (in Russian): <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=153276> (archived) Official publication (in Russian): <https://rg.ru/documents/2025/04/02/roskomnadzor-prikaz51-site-dok.html> (archived) Approved procedure, paras 1–7 and 12: https://www.consultant.ru/document/cons_doc_LAW_502246/3d5e08a9395f55c7d31c51fbd8265c1dde64cb86/ (archived)
- 72** RDP.RU, 'EcoFILTER: Functional URL-Filtering', product sheet (in English), 2 pp., undated; file creation date 30 May 2017. Company document. On p. 2: 'EcoFilter allows the extraction of all GET-requests of subscribers with a recording them to an external server (BIG data collection).'
- 73** Habr, 'Roskomnadzor and the Ministry of Digital Development to launch a 1.2-billion-rouble traffic-route monitoring system within two years' (in Russian), 7 November 2022, relaying Vedomosti of the same date. <https://habr.com/ru/news/697736/> (archived)
- 74** Gavriluk, A., 'Handing over the data: what subscriber information operators will give police directly' (in Russian), Forbes Russia, 6 May 2025. <https://www.forbes.ru/tekhnologii/536706-dannye-nasdacu-kakuu-informaciu-ob-abonentah-operatory-peredadut-policii-napramuu> (archived)
- 75** GRFC monthly reports, 22 issues from April 2023 to January 2025, plus an annual report for 2023 (in Russian); individual issues at <https://portal.noc.gov.ru/documents/> (archived)
- 76** Roskomnadzor, 'Monitoring of Sectoral Legislation' (in Russian), May 2019 digest. https://rkn.gov.ru/docs/docD_8710.docx (archived)
- 77** Roskomnadzor, 'Monitoring of Sectoral Legislation' (in Russian), September 2019 digest. https://rkn.gov.ru/docs/Monitoring_otraslevogo_zakonodatel6stva_sentjabr6__2019.docx (archived)
- 78** Roskomnadzor, 'Monitoring of Sectoral Legislation' (in Russian), February 2020 digest. https://rkn.gov.ru/docs/1_Monitoring_otraslevogo_zakonodatel6stva_fevral6_2020.docx (archived)
- 79** RBC, 'Roskomnadzor begins changing its approach to blocking prohibited content' (in Russian), 4 December 2025. https://www.rbc.ru/technology_and_media/04/12/2025/692edb139a79470afc90db77 (archived) Also reported at Habr, same date. <https://habr.com/ru/news/973082/> (archived)
- 80** Habr, 'What's new in the world of internet-censorship circumvention in mid-2024' (in Russian), 13 July 2024. <https://habr.com/ru/articles/828598/> (archived)
- 81** Habr, 'The VLESS Protocol: How It Bypasses Censorship in Russia and Why It Works' (in English), 17 February 2026. <https://habr.com/en/articles/990144/> (archived)

