Instytut Europy Środkowej

Komentarze IEŚ

Redakcja: Anton Saifullayeu (zastępca dyrektora IEŚ), Agnieszka Zajdel (sekretarz redakcji), Spasimir Domaradzki, Bartłomiej Krzysztan, Damian Szacawa, Agata Tatarenko

Nr 1592 (97/2026) | 17.04.2026

ISSN 2657-6996

Jędrzej Jander

Rosja: uderzenie w VPN jako kolejny krok w budowie „suwerennego Internetu"

W marcu i kwietniu 2026 r. władze Federacji Rosyjskiej zainicjowały nowy etap działań wymierzonych w usługi VPN[1], stanowiące kluczowe narzędzie omijania cenzury i uzyskiwania dostępu do domen internetowych zablokowanych w standardowym trybie połączenia. Dotychczasowa strategia państwa opierała się przede wszystkim na blokowaniu VPN na poziomie infrastruktury sieciowej – poprzez filtrowanie ruchu, blokowanie adresów IP oraz ograniczanie dostępu do aplikacji oferujących tego typu usługi. Obecnie władze FR przechodzą od modelu scentralizowanego do rozproszonego, w którym znaczna część odpowiedzialności za kontrolę przepływu informacji spoczywa na podmiotach komercyjnych. Jest to kolejny krok w procesie systematycznego ograniczania dostępu do globalnego Internetu oraz podporządkowania jego rosyjskiego segmentu interesom politycznym Kremla.

Skala popularności VPN i ewolucja narzędzi kontroli. W warunkach wzmożonej cenzury w Rosji VPN stał się jednym z najważniejszych narzędzi umożliwiających dostęp do treści blokowanych przez państwo, w tym mediów zagranicznych, niezależnych mediów rosyjskich, platform społecznościowych oraz komunikatorów. Dostępne dane wskazują, że korzysta z niego prawie jedna trzecia dorosłych obywateli Rosji, przy czym odsetek ten jest wyraźnie wyższy wśród młodszych użytkowników oraz osób o wyższym poziomie wykształcenia i dochodów[2]. Skala zjawiska sprawia, że jego całkowite wyeliminowanie stanowi dla władz trudne wyzwanie. W związku z tym działania regulatora (Roskomnadzor) przyjmują raczej formę stopniowego ograniczania dostępności i funkcjonalności tych usług. W tym kontekście kluczową rolę odgrywa rozwijana od kilku lat infrastruktura TSPU[3], umożliwiająca relatywnie skuteczną kontrolę ruchu sieciowego z wykorzystaniem technologii głębokiej inspekcji pakietów (DPI) (zob. Komentarze IEŚ nr 1554). System ten pozwala nie tylko blokować konkretne adresy IP, lecz także identyfikować charakterystyczne „wzorce" ruchu generowanego przez VPN i ograniczać działanie określonych protokołów. W ostatnich miesiącach odnotowano znaczący wzrost liczby blokowanych usług VPN oraz zwiększenie skuteczności filtrów, co świadczy o dalszym rozwoju zdolności państwa w tym obszarze.

Nowy model egzekwowania ograniczeń. Najważniejszą zmianą w obecnej fazie kampanii władz FR jest rozszerzenie odpowiedzialności za egzekwowanie ograniczeń na podmioty komercyjne. Ministerstwo Rozwoju Cyfrowego zobowiązało największe firmy technologiczne – w tym operatorów telekomunikacyjnych, banki oraz platformy e-commerce – do aktywnego wykrywania użytkowników korzystających z VPN oraz ograniczania im dostępu do usług. Według doniesień medialnych komunikat w tej sprawie miał zostać przekazany 30 marca 2026 r. podczas zamkniętego spotkania przez szefa resortu cyfryzacji, Maksuta Szadajewa. W praktyce oznacza to, że

[1] VPN (Virtual Private Network) to technologia umożliwiająca bezpieczne i prywatne połączenie z Internetem poprzez szyfrowanie danych oraz ukrycie rzeczywistego adresu IP użytkownika.

[2] „Problemy s mobilnym intiernietom i błokirowka inostrannych miessiendżerow: mart 2026", Lewada-Centr, https://www.levada.ru/2026/03/31/problemy-s-mobilnym-internetom-i-blokirovka-inostrannyh-messendzherov-mart-2026/ [16.04.2026]

[3] TSPU (ros. Tiechniczeskije sriedstwa protiwodiejstwija ugrozam – Techniczne Środki Przeciwdziałania Zagrożeniom) to urządzenia i oprogramowanie instalowane przez Roskomnadzor bezpośrednio w infrastrukturze rosyjskich operatorów telekomunikacyjnych, służące do zaawansowanego filtrowania, monitorowania i cenzurowania ruchu internetowego w Rosji.

dostęp do podstawowych usług cyfrowych, takich jak bankowość internetowa czy zakupy online, może być uzależniony od wyłączenia VPN. Jednocześnie firmy te mają obowiązek przekazywania regulatorowi informacji o nowych metodach omijania blokad oraz protokołach VPN, co pozwala państwu na bieżąco aktualizować listę centralnie blokowanych adresów i protokołów. Mechanizm ten opiera się w dużej mierze na presji administracyjnej – groźbie utraty preferencji podatkowych, statusu „zaufanego podmiotu" czy dostępu do wsparcia państwowego. Ważną motywacją do współpracy z państwem jest miejsce na tzw. „białej liście", czyli wśród stron internetowych, które mogą działać nawet w warunkach wyłączenia całego pozostałego ruchu w sieci na danym obszarze. Tego rodzaju lokalne odcięcia Internetu z inicjatywy organów państwa stają się coraz częstszą praktyką w Federacji Rosyjskiej. W rezultacie sektor prywatny jest włączany do systemu kontroli informacji jako jego integralna część, pełniąc w nim rolę *de facto* przedłużenia aparatu państwowego.

Rozszerzenie kontroli na poziom użytkownika. Równolegle do działań na poziomie infrastruktury sieciowej rozwijane są mechanizmy kontroli obejmujące bezpośrednio urządzenia użytkowników. Coraz większa liczba popularnych aplikacji mobilnych w Rosji posiada funkcje umożliwiające wykrywanie aktywnego połączenia VPN, a następnie przekazywanie tych informacji na serwery operatora. Według informacji opublikowanych przez rosyjski portal biznesowy The Bell, aż 22 z 30 najpopularniejszych aplikacji w systemie Android w Rosji monitoruje urządzenia użytkowników właśnie pod tym kątem. Takie rozwiązanie znacząco zwiększa skuteczność działań państwa, ponieważ umożliwia wykrywanie aplikacji VPN niezależnie od zastosowanych w nich metod maskowania ruchu sieciowego. Jednocześnie rodzi ono poważne problemy natury technicznej i prawnej. Stałe monitorowanie aktywności użytkownika może prowadzić do zwiększonego zużycia baterii i transferu danych, a brak precyzyjnych metod rozróżniania różnych typów VPN – np. korporacyjnych, do wewnętrznego użytku w firmie – zwiększa ryzyko błędnych decyzji i ograniczeń dla legalnych zastosowań. Dodatkowym wyzwaniem dla systemu cenzury pozostaje śledzenie aktywności użytkowników urządzeń z systemem iOS, który nie pozwala pojedynczym aplikacjom na tego rodzaju monitorowanie. W rezultacie system kontroli staje się bardziej inwazyjny, a jednocześnie mniej przewidywalny dla użytkowników.

Cele polityczne i kontekst strategiczny. Kampania przeciwko VPN stanowi element szerszej strategii władz rosyjskich, której celem jest budowa tzw. „suwerennego Internetu". W jej ramach państwo dąży do stworzenia środowiska cyfrowego, w którym przepływ informacji jest w pełni kontrolowany, a dostęp do zagranicznych źródeł – ograniczony i utrudniony. Działania te mają charakter długofalowy i obejmują zarówno zmiany legislacyjne, jak i rozwój infrastruktury technicznej oraz wywieranie presji na podmioty prywatne. VPN odgrywa tu kluczową rolę jako narzędzie obchodzenia ograniczeń, dlatego jego eliminacja – lub przynajmniej znaczące utrudnienie korzystania z niego – pozostaje jednym z priorytetów resortu cyfryzacji. Równolegle prowadzone są działania mające na celu promowanie krajowych alternatyw dla zagranicznych platform, co wpisuje się w strategię substytucji i centralizacji kontroli nad przestrzenią cyfrową. Przykładem takiego podejścia jest MAX, który ma integrować w sobie funkcjonalność komunikatora i platformy usług publicznych, przy jednoczesnym przechowywaniu wszystkich danych na rosyjskich serwerach (zob. Komentarze IEŚ nr 1444). W tym kontekście kampania wymierzona w VPN nie jest wyizolowanym działaniem, lecz integralną częścią szerszego projektu przebudowy rosyjskiego Internetu.

Skuteczność działań państwa. Pomimo rosnącej presji ze strony państwa całkowite wyeliminowanie VPN pozostaje mało prawdopodobnym scenariuszem. Użytkownicy adaptują się do nowych warunków, korzystając równolegle z wielu narzędzi oraz stale poszukując nowych metod omijania blokad. Na bazie zablokowanych usług VPN powstają kolejne, funkcjonujące pod zmienionymi nazwami, które pomimo krótkiej żywotności (szybkiego zablokowania) przynoszą swoim twórcom i użytkownikom korzyści z uwagi na ogromne zapotrzebowanie. W praktyce wraz z polityką państwa zmieniają się nawyki rosyjskich użytkowników: wielu z nich włącza VPN tylko w określonych sytuacjach, np. podczas korzystania z zagranicznych serwisów, a wyłącza do skorzystania z aplikacji krajowych. Strategia władz FR polega więc nie tyle na całkowitym zakazie, ile na zwiększaniu kosztów i niedogodności związanych z korzystaniem z tego typu narzędzi. Jednocześnie brak jednoznacznych regulacji penalizujących samo użycie VPN sprawia, że użytkownicy funkcjonują w stanie niepewności co do możliwych konsekwencji. Taka prawna „szara strefa" pozwala władzom na elastyczne dostosowywanie polityki do bieżącej

sytuacji, bez konieczności wprowadzania formalnych zakazów, które mogłyby wywołać większy sprzeciw społeczny.

Wnioski. Kampania władz rosyjskich przeciwko VPN to kolejny etap działań po zablokowaniu niepożądanych domen internetowych w standardowym trybie połączenia. Scentralizowany system kontroli nad ruchem w sieci uzupełniany jest przez działania o charakterze rozproszonym, z udziałem podmiotów komercyjnych. Włączenie sektora prywatnego w proces egzekwowania ograniczeń może znacząco zwiększyć skuteczność blokad. Jednocześnie działania te nie doprowadzą zapewne do pełnej eliminacji narzędzi omijania cenzury, lecz raczej do ich marginalizacji i utrudnienia dostępu, szczególnie wśród mniej zaawansowanych użytkowników. Kierunek zmian wskazuje, że Rosja konsekwentnie zmierza w stronę zamkniętego modelu Internetu na wzór chiński.