

# Wypadki bez zasad

## Co ograniczenia VPN oznaczają dla osób prywatnych i firm?

Po zablokowaniu Telegrama i innych popularnych serwisów zagranicznych, władze przeszły do kolejnego etapu: redukcji liczby użytkowników VPN. Operatorzy platform cyfrowych i mediów społecznościowych są teraz zobowiązani, pod groźbą utraty korzyści, do identyfikowania i blokowania użytkowników uzyskujących dostęp do ich platform z włączonymi VPN-ami. Władze przyznają, że stuprocentowa skuteczność wykrywania VPN-ów jest niemożliwa, ale takie środki mogłyby całkowicie uwolnić obywateli od zakazu korzystania z tej technologii. Kommiersant zbadał, jak nowe środki anti-VPN wpłyną na rosyjskie firmy IT i jak dostosują się do nich użytkownicy.

- [Odłącz to legalnie](#)
- [Zablokuj to sobie](#)
- [Dostosuj się w nowy sposób](#)
- [Odpowiedz w nowy sposób](#)
- [Ekspert ds. biznesu online w dobie lockdownów](#)

## Odłącz to legalnie

Ministerstwo Rozwoju Cyfrowego, Komunikacji i Mediów Masowych otrzymało zadanie ograniczenia korzystania z sieci VPN wśród Rosjan. Jak informował już „Kommiersant”, ministerstwo opracowało w tym celu szereg środków, mających na celu zmuszenie firm IT i platform cyfrowych do ograniczenia dostępu do swoich usług użytkownikom korzystającym z sieci VPN.

Jeśli firma zezwala użytkownikom na dostęp do swoich zasobów i aplikacji z włączoną siecią VPN, proponuje się usunięcie jej z „białych list” ( [patrz „Kommiersant”, 30 marca](#) ); jej aplikacje powinny zostać wyłączone z listy obowiązkowych preinstalacji na urządzeniach; a jej akredytacja IT, która zapewnia korzyści (ulgi podatkowe, kredyty hipoteczne na IT, odroczenia służby wojskowej dla pracowników itp.), powinna zostać cofnięta ( [patrz „Kommiersant”, 31 marca](#) ). Ponadto, jak obecnie się dyskutuje, firmy powinny być zobowiązane do samodzielnego wykrywania połączeń VPN użytkowników i zgłaszania tych danych do Roskomnadzoru, aby agencja mogła je zablokować.

Odrębnym środkiem było zwrócenie się Ministerstwa Rozwoju Cyfrowego, Komunikacji i Mediów do operatorów telekomunikacyjnych o nałożenie opłaty za korzystanie z ponad 15 GB danych międzynarodowych miesięcznie w sieciach komórkowych, donosi Forbes. Źródło w Kommiersancie bliskie rządowi wyjaśniło, że ograniczenie ruchu VPN „pozwoli nam również ograniczyć dostęp nie tylko do zakazanych serwisów społecznościowych, ale także do zasobów takich jak pirackie oprogramowanie i strony internetowe z nielegalnymi, destrukcyjnymi i ekstremistycznymi treściami”.

*VPN to technologia umożliwiająca łączenie urządzeń zdalnych w jedną prywatną sieć. Sieci VPN są często reklamowane jako sposób na ominięcie blokad. Jednak organizacje konfiguruje sieci VPN*

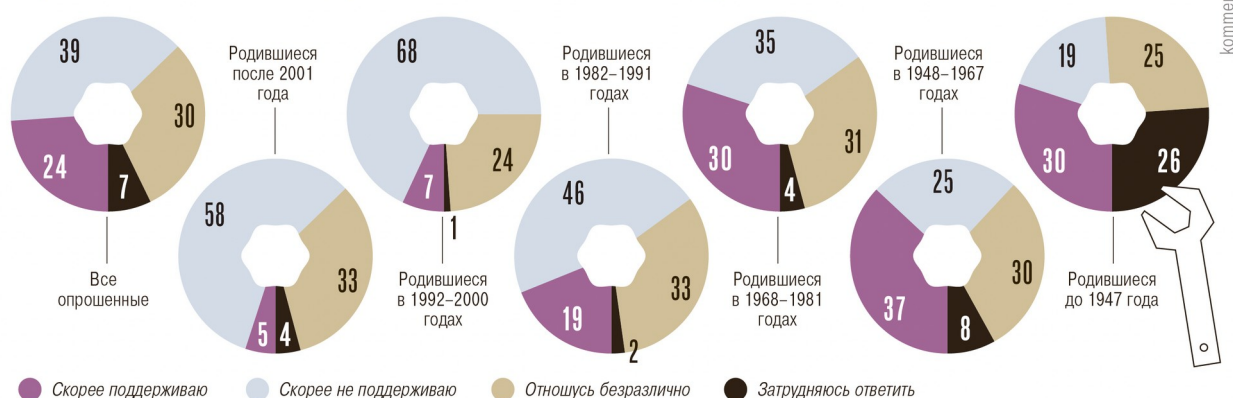
również w celu łączenia komputerów, telefonów, bankomatów i innych urządzeń znajdujących się w różnych lokalizacjach lub regionach.

**Serwer proxy** to serwer pośredniczący między użytkownikiem internetu a serwerami, z których pobierane są informacje. Serwer proxy może szyfrować ruch, buforować informacje i działać jako filtr sieciowy.

Firmy otrzymały również „metodologię identyfikacji oznak narzędzi do omijania blokad na urządzeniach klienckich” – dokument (Kommersant posiada kopię), który proponuje ujednolicone podejście do identyfikacji sieci VPN i serwerów proxy używanych do omijania zablokowanych stron internetowych i aplikacji. W dokumencie stwierdza się, że wykrywanie połączenia VPN użytkownika powinno odbywać się w trzech krokach:

- analizować sesje klientów na serwerze poprzez porównywanie adresów IP połączeń z listą zablokowanych adresów IP, a także porównywać adresy IP sesji klienta po stronie serwera z adresem IP na urządzeniu użytkownika;
- sprawdzić użycie narzędzi omijających blokady na urządzeniu, korzystając z natywnej aplikacji dla systemów operacyjnych Android i iOS;
- na „późniejszych etapach” sprawdzić urządzenia na innych systemach operacyjnych.

**КАК ВЫ ОТНОСИТЕСЬ К БЛОКИРОВКАМ МЕССЕНДЖЕРОВ И ЦИФРОВЫХ ПЛАТФОРМ? (%)** ИСТОЧНИК: ОПРОС ВЦИОМ В НОЯБРЕ 2025 ГОДА.



W dokumencie podkreślono również, że „wykrywanie stosowania narzędzi omijających blokady za pomocą jednej lub kilku metod nie gwarantuje 100% skuteczności ze względu na możliwość wystąpienia fałszywych alarmów”. Jak czytamy w dokumencie, fałszywe alarmy mogą wystąpić w wyniku korzystania z korporacyjnych sieci VPN, oprogramowania antywirusowego, narzędzi do wirtualizacji i konteneryzacji oraz technologii NAT (umożliwiającej konwersję wewnętrznych adresów IP urządzeń lokalnych na jeden lub więcej adresów zewnętrznych).

Od 2017 roku usługi VPN w Rosji mają obowiązek ograniczać dostęp do zablokowanych stron internetowych; w przeciwnym razie usługa jest blokowana. W marcu 2024 roku wszedł w życie zakaz rozpowszechniania informacji o sposobach dostępu do zablokowanych zasobów. We wrześniu 2025 roku wprowadzono ustawę zakazującą reklamowania oprogramowania do omijania blokad. Kary za reklamowanie VPN-ów wynoszą do 80 000 rubli dla osób fizycznych, do 150 000 rubli dla urzędników i do 500 000 rubli dla osób prawnych.

Podstawowym sposobem ograniczenia liczby fałszywych alarmów jest tworzenie „białych list” korporacyjnych sieci VPN i „legalnych” serwerów proxy. Taka lista już istnieje; firmy dodają do

niej swoje sieci VPN, a Roskomnadzor ją utrzymuje, według źródła w „Kommiersancie” bliskiego rządowi: „Obecnie zawiera ona około 75 000 adresów IP. Firmy przesyłają swoje dane do agencji za pośrednictwem swoich osobistych kont w Roskomnadzorze, aby wykluczyć je z filtrowania przez TSPU. Agencja wysyła również powiadomienia do właścicieli korporacyjnych sieci VPN o blokowaniu nowych usług i protokołów. Główne wymagania dla sieci VPN umieszczonych na „białej liście” to ograniczenie dostępu do zabronionych zasobów i współpraca z Roskomnadzorem”.

## **Zablokuj to sobie**

„Głównym wyzwaniem stojącym przed firmami IT będzie jak najbardziej transparentne zakomunikowanie klientom, że włączenie VPN może uniemożliwić im korzystanie z pełnej funkcjonalności produktu i zapewnienie wygodnej nawigacji” – mówi źródło w Kommiersancie bliskie dużej firmie IT. Co więcej, według tego źródła, sieci VPN wpływają na wydajność aplikacji, dlatego prawie wszyscy główni gracze i agencje rządowe już „przetwarzają logowania do aplikacji z włączonymi VPN-ami w taki czy inny sposób”.

„Z technicznego punktu widzenia spełnienie tych wymagań nie będzie trudne. Nie będzie konieczna znacząca restrukturyzacja architektury technologicznej platform” – zapewnił „Kommiersant” rosyjski portal pocztowy.

Wszelkie dodatkowe koszty będą związane z udoskonaleniem systemów bezpieczeństwa i mieszczą się w ramach bieżących planów rozwoju IT, a działanie korporacyjnych sieci VPN nie zostanie zakłócone - dodaje firma.

Koleje Rosyjskie informują, że ograniczenia techniczne w dostępie do ich usług z zagranicy zostaną wprowadzone od 2022 roku ze względu na „bezprecedensowe próby ataków komputerowych na infrastrukturę firmy z adresów należących do zagranicznych dostawców usług internetowych”. Dodają, że złożyli już wszystkie niezbędne dokumenty w celu umieszczenia korporacyjnych sieci VPN na białej liście.

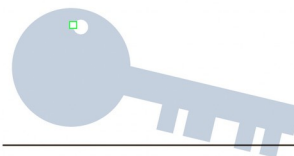
Rosatom (niektóre usługi firmy znajdują się na białej liście) wyjaśnia, że architektura jego rozwiązań „została pierwotnie zaprojektowana z uwzględnieniem wymogów odporności informacji i nie opiera się na publicznie dostępnych usługach VPN, więc nowe wymogi nie będą miały krytycznego wpływu na działanie jego zasobów”. Tymczasem niektóre zasoby niezbędne do identyfikacji użytkowników za pomocą sieci VPN – takie jak Ozon i Wildberries – już ograniczyły dostęp do swoich platform, podał portal Izwiestia.

## ЗАПРОСЫ НА ТЕМУ VPN В ПОИСКОВИКЕ «ЯНДЕКС» ИСТОЧНИК: «ЯНДЕКС ВОРДСТАТ».



>6

млн человек составляла активная база пользователей VPN в России в третьем квартале 2025 года, по данным Sensor Tower



до 500

тыс. руб. составляет штраф за рекламу VPN

kommersant.ru

Источник в Kommersancie z państwowej firmy twierdzi, że nie przewiduje spadku aktywności użytkowników w swojej aplikacji ani na swojej stronie internetowej: „Strona internetowa firmy historycznie nie działała za granicą, a co za tym idzie, z włączonym VPN”. Inne źródło w Kommersancie z rosyjskiej dużej firmy technologicznej zgadza się: „Wiele usług działa już poprawnie tylko z wyłączonym VPN – prawie wszystkie aplikacje bankowe, Gosusługi i inne”. „Jednak te środki zaradcze odnoszą się do konsekwencji, a nie przyczyn wzrostu ruchu VPN. Według badań, od jednej trzeciej do połowy rosyjskich użytkowników internetu regularnie korzysta z VPN” – mówi Siergiej Kudriaszow, partner w zespole ds. transformacji cyfrowej w Strategy Partners.

## Dostosuj się w nowy sposób

Po wprowadzeniu nowych wymogów „liczba użytkowników naturalnie spadnie” – uważa źródło w Kommersancie bliskie dużym firmom technologicznym. „Jednak jak pokazały wcześniejsze praktyki blokowania, użytkownicy dość szybko się dostosują, a same usługi VPN i proxy będą się szybko modernizować i adaptować”. Jednocześnie użytkownicy będą nadal korzystać ze swoich dotychczasowych usług, „również z powodu braku odpowiednich i pełnoprawnych alternatyw” – twierdzi.

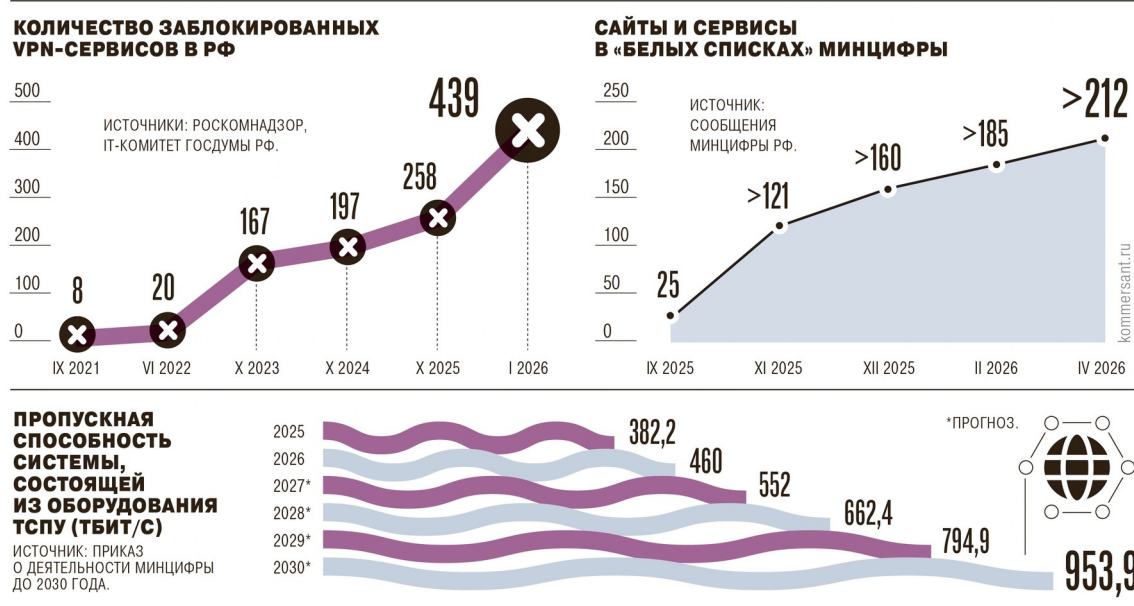
## Walka z usługami VPN w Rosji: kluczowe punkty inicjatyw Ministerstwa Rozwoju Cyfrowego

[Przeczytaj więcej](#)

To udoskonalenie technologiczne – śledzenie użytkowników z włączonymi sieciami VPN – nie byłoby uważane za skomplikowane ani kosztowne dla dużych firm IT, twierdzi źródło w Kommersancie w dużej firmie IT. Źródło w Kommersancie w firmie programistycznej wyjaśnia, że wykrywanie prostego ruchu VPN nie wymagałoby dużych inwestycji ani oddzielnego oprogramowania, takiego jak Głęboka Inspekcja Pakietów (DPI): „Na poziomie aplikacji użytkownika programiści widzą, skąd pochodzi ruch i mogą po prostu przesyłać dane IP. DPI działa

w oparciu o sygnatury ruchu, podczas gdy usługi VPN są trudne do opisanie”. Ruch VPN można zidentyfikować za pomocą DPI, choć nie w pełni, ale „jego instalacja kosztuje”.

„Trudno oszacować całkowite koszty, jakie firmy poniosą w związku z nowymi wymogami, ale struktura kosztów jest jasna. Ta dodatkowa przepustowość w zakresie klasyfikacji ruchu, modyfikacja istniejących usług w celu dostosowania ich do nowej logiki blokowania oraz czas poświęcony programistom mogą okazać się dość znaczące” – twierdzi Siergiej Kudriaszow. Źródło w Kommersancie bliskie dużym firmom technologicznym szacuje, że koszty te wyniosą dodatkowe 20% obecnych budżetów IT, „ponieważ firmy będą musiały nie tylko rekonfigurować sprzęt i kanały komunikacyjne, ale także opracować lub zakupić specjalistyczne produkty w celu wdrożenia określonych wymagań”. Pan Kudriaszow uważa jednak, że szacunki te są przesadzone: „Wyzwaniem dla platform nie jest zakup nowego sprzętu, ale modyfikacja logiki aplikacji – można to osiągnąć poprzez realokację zasobów programistycznych”.



Jednak niektórzy przedstawiciele branży są znacznie bardziej pesymistyczni. Stowarzyszenie Firm Handlu Internetowego (AKIT, do którego należą m.in. Ozon, M.Video i Avito) uważa, że nowe ograniczenia dostępu do VPN dla firm e-commerce oznaczać będą znaczny spadek ruchu: „Jeśli porównamy to do tradycyjnego handlu detalicznego i jego infrastruktury, to są to w zasadzie zakazy wejścia do sklepu i dokonywania zakupów”. Oznacza to, że niektóre usługi nadal nie znajdują się na „białej liście” – po prostu nie działają bez mobilnego internetu, a te, które są już na niej dostępne, muszą teraz działać selektywnie, wyjaśnia AKIT.

„W ostatnich latach było to największe wyzwanie i bariera dla użytkowników cyfrowych i usług cyfrowych, które opierały się na wygodzie kupowania towarów niezależnie od lokalizacji użytkownika czy sposobu korzystania z internetu. Wszelkie zmiany w tym obszarze muszą być stopniowe i konsultowane z firmami” – twierdzi stowarzyszenie.

## **Ekspert Nikołaj Metlyuk o biznesie online w erze blokowania**

Dla platform cyfrowych jako całości oznacza to zwiększone obciążenie techniczne i organizacyjne, mówi Anton Daniłow-Danilian, wiceprzewodniczący Diełowaja Rossija i szef grupy roboczej ds. agregatorów usług transportowych w Komitecie ds. Gospodarki Cyfrowej RSPP: „Będą potrzebne dodatkowe konfiguracje infrastruktury, narzędzia do wykrywania ruchu VPN i bardziej złożone procedury zgodności. Co więcej, istnieje ryzyko, że renomowane firmy będą musiały zmierzyć się nie tylko z dodatkowymi kosztami, ale także z błędami w stosowaniu takich mechanizmów”.

### **Odpowiedz w nowy sposób**

Źródło w Kommiersancie z dużej firmy technologicznej twierdzi również, że nie jest jasne, w jakim stopniu każdy aspekt nowych wymogów musi być przestrzegany: „Przygotowujemy się do wdrożenia tych wymogów, ale ich wpływ na użytkowników i firmy jest nadal niejasny. Będzie to zależeć nie tylko od naszych działań, ale także od działań innych uczestników rynku”. Źródło w Kommiersancie, znające plany Ministerstwa Rozwoju Cyfrowego, twierdzi, że nie ma jeszcze jasnego mechanizmu umożliwiającego firmom przesyłanie danych VPN do Roskomnadzoru: „Wszystko opiera się na wymogach, ale firmy nie rozumieją, jak przysyłać dane, biorąc pod uwagę, że Roskomnadzor stwierdził, że adresy IP są danymi osobowymi, a ich przesyłanie bez zgody jest ograniczone”.

Inne źródło w Kommiersancie dodaje, że kwestia indywidualnej odpowiedzialności firm, które nie dostosują się do nowych wymogów dotyczących monitorowania VPN, nie została jeszcze omówiona z przedsiębiorcami.

Anton Danilov-Danilyan dodaje, że nie ma publicznie dostępnej, szczegółowej i transparentnej procedury, która jasno wskazywałaby format, w jakim firmy muszą przysyłać dane do Roskomnadzoru: „Najprawdopodobniej będziemy mówić albo o istniejących kanałach interakcji z regulatorem, albo o dodatkowych wymogach dla usług działających w ramach specjalnych ram regulacyjnych”. „Ale obecnie nie ma ku temu podstaw prawnych, a firmy z branży nie rozumieją, dlaczego nagle oczekuje się od nich identyfikowania sieci VPN” – zauważa źródło w Kommiersancie bliskie dużej firmie IT.

Ministerstwo Rozwoju Cyfrowego omawia obecnie z branżą szereg niuansów nowych wymogów – dostępu dla deweloperów i innych kwestii – i poszukuje rozwiązań uwzględniających obowiązujące przepisy, jak donosi źródło w Kommiersancie bliskie rządowi. „Ministerstwo Rozwoju Cyfrowego chce rozwiązać ten problem, minimalizując konsekwencje i obciążenia dla użytkowników. Obecne ograniczenia i nowe środki omawiane z operatorami telekomunikacyjnymi i platformami cyfrowymi w celu ograniczenia dostępu użytkowników za pośrednictwem sieci VPN to kompromis, który pozwala uniknąć nakładania kar administracyjnych na obywateli” – twierdzi.

Avito, VimpelCom, MegaFon, MTS, T2, Yandex, VK, Ozon i Wildberries odmówiły komentarza. Ministerstwo Rozwoju Cyfrowego, Roskomnadzor, Alfa Bank, VTB, NSPK, PSB, Sber, T-Technologies, Gazprom-Media Holding, 2GIS i Okko nie odpowiedziały na prośbę Kommiersanta o komentarz.

Aleksiej Żabin, Varwara Połońska

## Opinia eksperta

### „Dotarcie do całego świata stało się trudniejsze”.

**Nikołaj Metlyuk, prezes giełdy ruchu Piter-IX, o biznesie sieciowym w erze blokowania.**

Ruch internetowy w Rosji rośnie o około 20% rocznie. Jednak jego struktura jest znacząco zaburzona przez blokowanie, ponieważ ruch jest fragmentowany z powodu korzystania z VPN. W przypadku punktów wymiany ruchu (IXP), które powstały w celu obniżenia kosztów tranzytu, sytuacja ta znacząco zwiększa koszty. **Nikołaj Metlyuk, prezes Piter-IX, jednego z IXP, rozmawiał z „Kommiersantem” o rosnącym wolumenie ruchu międzynarodowego i planach firmy w tym nowym środowisku.**

— **Jak zmieniła się struktura Twojego ruchu w ciągu ostatniego roku?**

— Całkowity wzrost ruchu w sieci Piter-IX w 2025 roku wyniósł 1,2 Tb/s, z czego około 50% stanowił ruch międzynarodowy. Udział ruchu międzynarodowego w wolumenie ruchu pozostał jednak niezmienny w ciągu roku. Ruch rosyjski dominuje w stosunku 80/20, a platformy krajowe rosną pod względem konsumpcji treści i aktywnej bazy abonentów.

— **Jak to wpływa na Twoją firmę?**

Wzrost ruchu międzynarodowego ma negatywny wpływ. Nasz ruch nie jest dzielony na krajowy i międzynarodowy; operator pobiera jedną opłatę, więc wzrost ruchu międzynarodowego zwiększa koszty. Ponadto do kosztów ruchu doliczany jest koszt utrzymania mobilnego centrum danych (TSPU).

— **Jak zmieniły się ceny kanałów i routing? Jaki jest tego powód?**

„Ceny kanałów się nie zmieniły, ale natężenie ruchu znacząco rośnie i trzeba je zwiększyć, aby zapewnić jakość. Kontrakty na kanały międzynarodowe są denominowane w walutach obcych, więc wahania kursów walut są dla nas dotkliwe. Operatorzy rosyjscy płacą w rublach, więc bardzo chcielibyśmy, aby dolar był wart 30 rubli”.

### Co ograniczenia VPN oznaczają dla osób prywatnych i firm?

Routing stał się bardziej złożony, a ruch bardziej rozdrobniony: z jednej strony wiele zagranicznych stron internetowych i platform blokuje dostęp z rosyjskich adresów IP w wyniku sankcji, z drugiej strony rosyjskie organy regulacyjne blokują zagraniczne platformy za naruszanie naszego prawa. W rezultacie dostęp do całego świata stał się trudniejszy, co kosztuje zarówno użytkowników (w przypadku sieci VPN), jak i operatorów, ponieważ zwiększone wykorzystanie sieci VPN prowadzi do wzrostu wolumenu ruchu międzynarodowego. Wzrósł również wolumen ruchu od operatorów stacjonarnego internetu szerokopasmowego z powodu regularnych przerw w dostępie do internetu mobilnego w całym kraju.

— **Jak regulacje wpływają na Ciebie?**

Wymagania regulacyjne zwiększają koszty; dotyczy to każdej branży i każdego kraju. Oprócz kosztów bezpośrednich istnieją również koszty pośrednie: do przestrzegania wymogów regulacyjnych potrzeba więcej specjalistów, podobnie jak prawników i konsultantów. Regulacje branżowe są niewątpliwie niezbędne, ale aby się rozwijać, firmy potrzebują większej swobody i,

najlepiej, autentycznych rozmów z odpowiednimi ministerstwami i agencjami na temat swoich inicjatyw.

— **Jak planują Państwo rozwijać swój biznes w obecnych warunkach?**

W 2025 roku aktywnie rozbudowaliśmy naszą sieć: zmodernizowaliśmy sprzęt w kluczowych węzłach w Moskwie, Petersburgu, Niżnym Nowogrodzie i innych miastach. Planujemy dalszy rozwój ekosystemu i współpracę z rosyjskimi sieciami CDN i platformami chmurowymi, rozszerzając geografie połączeń bezpośrednich w celu lokalizacji ruchu w regionach.

Naszym celem jest zapewnienie małym operatorom dostępu do wysokiej jakości treści na równi z dużymi graczami.

Nasze plany obejmują wdrożenie serwerów buforujących w naszych regionalnych punktach dostępu oraz zapewnienie lokalnym operatorom kompleksowej usługi: dostępu do pamięci podręcznych rosyjskiej platformy treści, naszych punktów wymiany ruchu w Rosji i za granicą oraz globalnego dostępu do internetu poprzez tranzyt IP Full View. Piter-IX postawił sobie za cel osiągnięcie 1000 połączonych systemów autonomicznych i obciążenia szczytowego na poziomie 10 Tb/s do 2027 roku. Do kwietnia 2026 roku osiągnęliśmy już 630 systemów autonomicznych i obciążenie szczytowe na poziomie 5,5 Tb/s i planujemy utrzymać to tempo.

Wywiad przeprowadził Aleksiej Żabin