Comply.Pulse

Что будет с вашим VPN: «белый список», штраф или блокировка? Поправки в КоАП РФ, запустившие настоящее колесо фортуны

На прошлой неделе приняты новые поправки в Кодекс РФ об административных правонарушениях (**КоАП**), которые вызвали широкий резонанс из-за штрафов за поиск экстремистских материалов. Менее заметной, но более значимой для бизнеса стала ответственность за корпоративные VPN. Пространства для маневра теперь все меньше, а денежных потерь — больше.
Спойлер: VPN (пока) никто не запрещал. Но неправильное развертывание VPN в вашей инфраструктуре теперь грозит новыми крупными штрафами — до 1 млн рублей.

Предыстория

Статья 15.8 ФЗ «Об информации, информационных технологиях и защите информации» уже давно устанавливает порядок ограничения доступа к VPN и другим средствам обхода блокировок Роскомнадзора (**РКН**).
В общем виде логика взаимодействия с РКН выглядит так:

1. Роскомнадзор узнает о сервисе, который позволяет получить доступ к заблокированным ресурсам и направляет владельцу сервиса требование.
2. По требованию РКН владелец ресурса обязан в течение 30 рабочих дней подключиться к федеральной государственной информационной системе с перечнем запрещенных ресурсов (**ФГИС**).
3. В течение 3 рабочих дней после подключения к ФГИС владелец ресурса обязан обеспечить невозможность использования его сервиса для доступа к заблокированным ресурсам на территории России.

Эти правила работают не только для «публичных» VPN, но и для корпоративных решений. Почему многие компании не учитывают такие правила?
Ответов здесь два:

- **Во-первых**, не было штрафов. Все-таки полмиллиона рублей за нарушение (а за повторное – целый миллион) на дороге не валяются.
- **Во-вторых**, РКН раньше мог и не узнать о вашем корпоративном VPN. А сложности — то есть обязанность соблюдать ст. 15.8 — возникают только после получения официального требования от РКН.

Явка с повинной

Все поменялось буквально за последний год, когда компании стали все чаще сталкиваться с угрозой блокировки IP-адресов VPN в рамках мероприятий властей по противодействию угрозам и защите «суверенного Интернета».

Чтобы вмиг не оказаться без доступа к корпоративным порталам и аналогичным ресурсам, многие компании, особенно локальные офисы зарубежных компаний, были вынуждены просить РКН включить их IP-адреса в «белый список». Именно такой вариант предложило и само Минцифры для бесперебойной работы корпоративных решений.

В рамках этой кампании бизнес добровольно сообщал и продолжает сообщать о своих VPN в РКН. Подход понятный: если вас и так могут заблокировать в рамках «суверенного интернета», то лучше уж попытаться войти в «белый список», чем ждать часа X и подвергать риску работу всей компании. Штрафов ведь не было — до недавнего времени.

Штрафы по новым составам

За что начнут штрафовать владельцев VPN с 1 сентября по новой ст. 13.52 КоАП:

Состав	Штраф
Нарушение порядка взаимодействия с РКН	до 500 000 руб.
Неисполнение требования подключиться к ФГИС	до 500 000 руб.
Невыполнение обязанности по «фильтрации» запрещенных в РФ ресурсов	до 500 000 руб.
Повторное нарушение любого из составов выше	до 1 000 000 руб.

Ответственность возлагается на «владельца» программно-технических средств. Кто им является – не самый простой вопрос, особенно если компания использует чужое «коробочное» решение. Здесь уместно провести аналогию с «владельцем» сайта (п. 17 ст. 2 ФЗ «Об информации...») – им является тот, кто определяет порядок использования ресурса. Поэтому, в идеале, компания не должна нести ответственность за установленные провайдером ограничения по настройке VPN. Пойдет ли по этому пути судебная практика, часто лояльная к РКН, неизвестно.

Дилемма владельца VPN

Проблема включения VPN в «белый список» РКН никуда не исчезла. И, к слову, в июле процедура включения стала еще сложнее, чем прежде. По опыту таких дел мы знаем, каким тернистым бывает путь к «обелению» IP-адресов. Но об этом как-нибудь в другой раз.

С сегодняшнего дня каждой компании нужно **предварительно** соотносить риски и решить, стоит ли:

1. Пытаться включить IP-адреса VPN в «белый список» РКН, но сообщить о себе и раскрыть карты под угрозой новых штрафов.
2. Продолжать рисковать и ничего не сообщать об IP-адресах. Риск штрафа меньше, но сам доступ к важным корпоративным решениям окажется под угрозой блокировки.

Эту дилемму нужно решать с технической командой, чтобы понять, какими решениями пользуется компания, существует ли возможность настроить решения под требования РКН, каковы шансы уложиться в 33 рабочих дня на фильтрацию запрещенных ресурсов и так далее.

Итого

Ответить на вопрос о том, как вы будете исполнять предписания регулятора, стоит до того, как вы начнёте «обелять» IP-адреса. Ниже несколько принципиальных моментов, которые важно учитывать:

- Выбирая корпоративный VPN, ориентируйтесь на то, будет ли он технически соответствовать требованиям РКН.
- Комбинируйте технические и организационные меры для соблюдения требований регулятора. Последние особенно важны, если у вас VPN от стороннего провайдера.
- Подготовьте инструкции для сотрудников. Четкое описание легальных рамок использования VPN может быть одним из вариантов митигации рисков.
- Помните, что использование VPN и других средств обхода блокировок теперь рассматривается как отягчающее обстоятельство по УК РФ.

Мы будем следить за ситуацией и держать вас в курсе. А если у вас есть вопрос по легализации VPN, напишите нам на info@comply.ru.

Про другие новости о поправках в КоАП читайте в нашем канале.

Максим Али
Партнер

maxim.ali@comply.ru
+7 981 699 60 36
t.me/maximal1st

Подписаться на Comply в Telegram