# СХЕМЫ СОХРАНЕНИЯ АНОНИМНОСТИ В СЕТИ

от VEKTOR T13

www.VektorT13.pro

*Все представленные в данной брошюре связки предполагают сокрытие подлинного IP-адреса и надежное шифрование трафика. Отличаются связки ценой, скоростью работы и защитой от активных способов деанонимизации. Подробно о каждом способе активной деанонимизации будет рассказано в процессе обучения, здесь будет приведена только краткая справка.*

**ДЕАНОНИМИЗАЦИЯ АДМИНИСТРАТИВНЫМИ МЕТОДАМИ** предполагает отправку запроса хостинг-провайдеру с просьбой предоставить данные о подключениях к серверу. В случае, если используется несколько звеньев, например, несколько VPN, запросы отправляются последовательно каждому хостинг-провайдеру, начиная с последнего. В итоге удается выйти на первое звено в связке, к которому пользователь подключается со своего IP-адреса.

**ДЕАНОНИМИЗАЦИЯ ВРЕДОНОСНЫМ ПО** предполагает отправку вредоносной программы, которая, попав на компьютер жертвы, передает информацию о нем на управляющий сервер. Передаваемая информация включает и подлинный IP-адрес жертвы. Вредоносная программа может быть замаскирована под программу, картинку, документ или иной файл. Данное программное обеспечение активно закупают как правоохранительные органы, так и спецслужбы различных стран, его же активно используют и злоумышленники для сбора данных о жертве.

**ТАЙМИНГ-АТАКИ.** Тайминг-атаки имеют массу разновидностей. Чтобы было проще понять, что такое тайминг-атака, представьте себе множество перепутанных шлангов, из которых льется вода, и один выключатель. Как понять, к какому шлангу относится этот выключатель? Вы просто на пару секунд отключаете им воду, где струя ненадолго ослабнет, тот шланг и ведет к выключателю.

**ДЕАНОНИМИЗАЦИЯ ПУТЕМ ЭКСПЛУАТИРОВАНИЯ УЯЗВИМОСТЕЙ** предполагает обнаружение уязвимости в одном из элементов связки. Например, некоторое время назад ФБР успешно проэксплуатировала уязвимость Tor, деанонимизировав множество пользователей луковой сети. В некоторых связках уязвимость одного элемента непременно приведет к деанонимизации пользователя, другие связки устойчивы к данному способу.

**ДЕАНОНИМИЗАЦИЯ ПУТЕМ ЭКСЛУАТИРОВАНИЯ УЯЗВИМОСТИ ВЕБ-БРАУЗЕРА** предполагает переход пользователя по ссылке. Обычный сайт увидит IP-адрес конечного звена цепочки, обеспечивающей анонимность. Однако в этом случае в результате перехода владельцу ресурса станет известен подлинный IP-адрес жертвы. Это возможно из-за уязвимостей веб-браузеров, которые постоянно обнаруживают и закрывают. Мы разместили этот путь деанонимизации последним, хотя на сегодняшний день именно он остается самым распространенным. Популярность его обусловлена высокой эффективностью и простотой реализации, ведь заставить жертву перейти по ссылке гораздо проще, нежели убедить открыть файл.

## БАЗОВАЯ АНОНИМНОСТЬ (DOUBLE/TRIPPLE/QUADRO VPN)


Стоимость: средняя  Скорость: высокая

Защита от деанонимизации административными методами: средняя

Защита от активной деанонимизации вредоносным ПО: отсутствует

Защита от деанонимизации тайминг-атаками: низкая

Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: отсутствует

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: отсутствует

Экономичное решение без потери скорости интернет-соединения. Ваш трафик будет надежно зашифрован, а подлинный IP-адрес скрыт от веб-сайтов. Вас не сможет прослушивать не только ваш провайдер, но и спецслужбы вашей страны. Однако, если вас очень захотят найти при наличии административного ресурса и запросов к хостинг-провайдерам, это не составит труда. Кроме того, данная связка практически никак не защищает от активных способов деанонимизации.

## TOR


Стоимость: бесплатно  Скорость: средняя

Защита от деанонимизации административными методами: высокая

Защита от активной деанонимизации вредоносным ПО: отсутствует

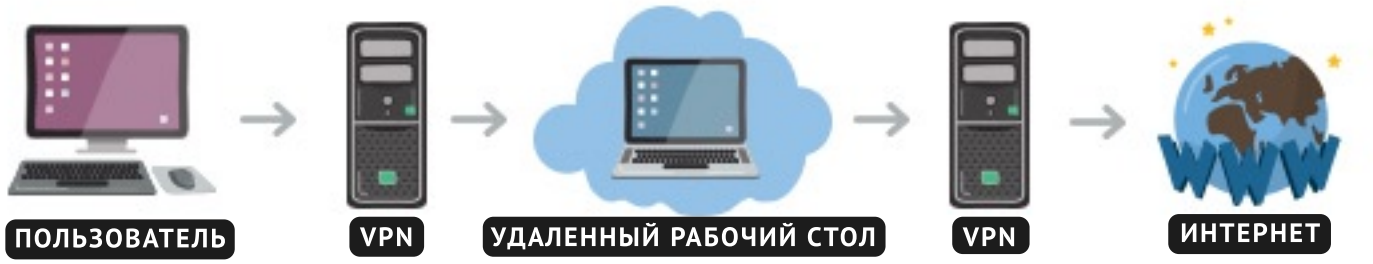
Защита от деанонимизации тайминг-атаками: средняя

Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: отсутствует

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: отсутствует

Использование Tor заметно замедляет скорость интернета. При этом Tor бесплатен, Tor повышает защиту от тайминг-атак и делает почти невозможной деанонимизацию путем использования административного ресурса. Но Tor имеет один критический недостаток: трафик на выходных нодах нередко перехватывается злоумышленниками, которые разворачивают выходные ноды исключительно для этой цели. Потому использовать можно только персональную выходную ноду, к которой мошенники не будут иметь доступа.

## VPN-УДАЛЕННЫЙ РАБОЧИЙ СТОЛ-VPN




Стоимость: высокая  Скорость: высокая

Защита от деанонимизации административными методами: средняя

Защита от активной деанонимизации вредоносным ПО: высокая

Защита от деанонимизации тайминг-атаками: высокая

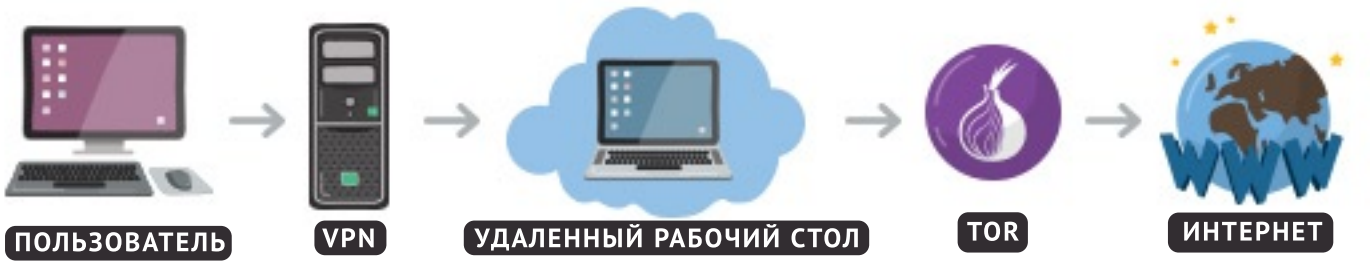
Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: средняя

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: высокая

Полноценная анонимность практически недостижима без использования удаленного рабочего стола. Удаленный рабочий стол служит надежным барьером против

активных способов деанонимизации. Данная связка обеспечивает отличную скорость, однако уязвима к деанонимизации административными методами. Как правило, ее берут вместе с Tor, но Tor отключают, когда высокая скорость нужна больше высокой анонимности.

## VPN-УДАЛЕННЫЙ РАБОЧИЙ СТОЛ-TOP




Стоимость: высокая  Скорость: средняя

Защита от деанонимизации административными методами: высокая

Защита от активной деанонимизации вредоносным ПО: высокая

Защита от деанонимизации тайминг-атаками: высокая

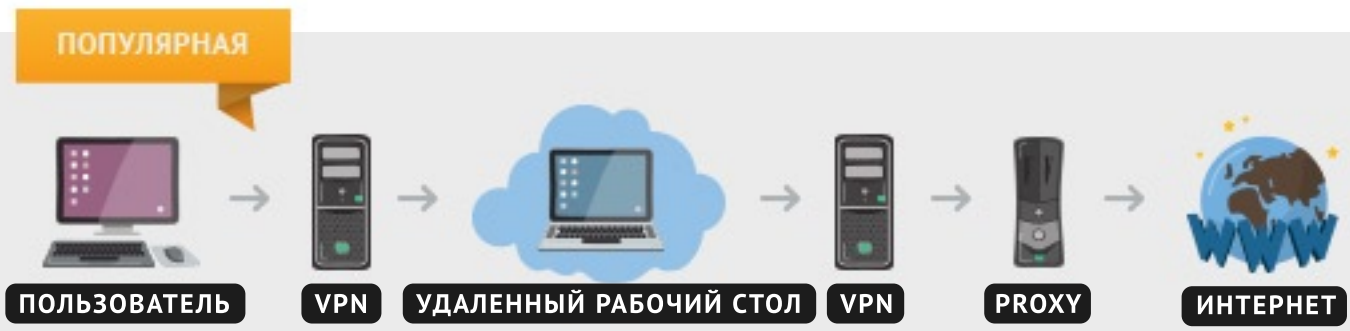
Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: высокая

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: высокая

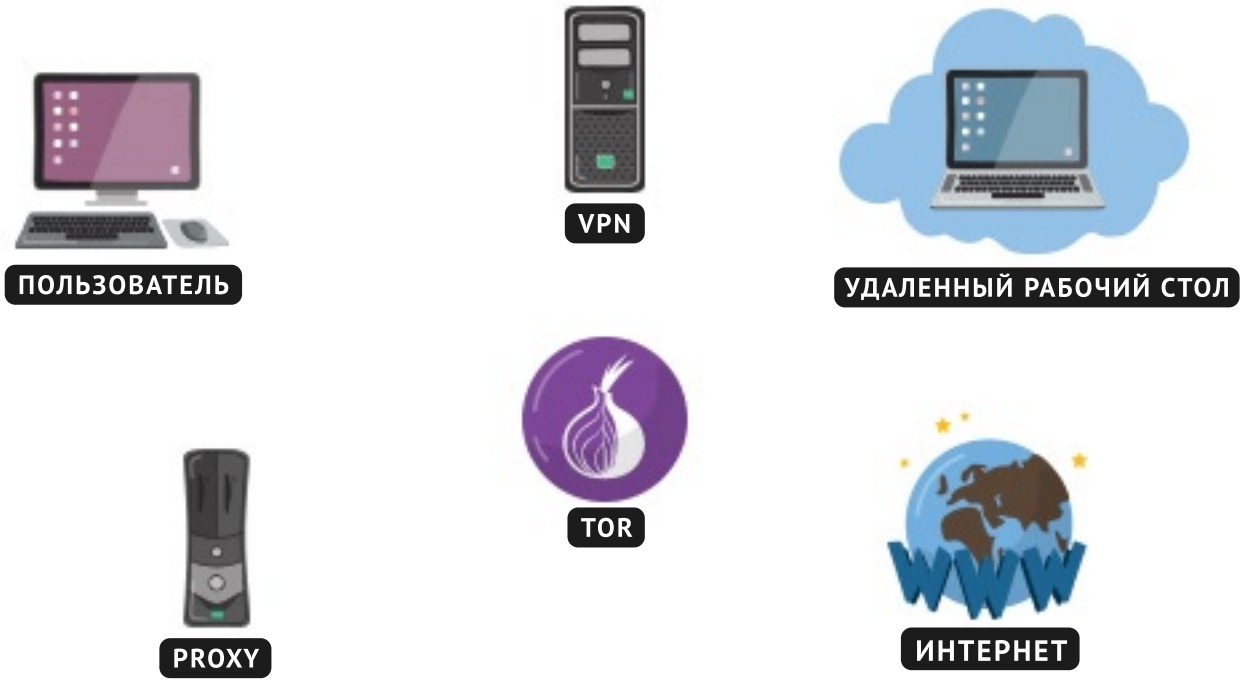
Это самая надежная связка, которую мы предлагаем нашим клиентам. Она устойчива как к активным способам деанонимизации, так и к деанонимизации путем использования административного ресурса. Главный недостаток этой связки — скорость, на которую влияет использование Tor.

Вы можете настроить себе две связки и чередовать их в зависимости от требуемого уровня анонимности. К любой схеме в конце можно добавить  proxy для регулярной смены IP-адреса.

Самая популярная среди наших клиентов связка выглядит так




Вы можете самостоятельно придумать связку, используя VPN-сервера, Tor, удаленный рабочий стол и proxy. А мы поможем вам реализовать ее на практике.



## КОНТАКТЫ ДЛЯ ЗАПИСИ НА ОБУЧЕНИЕ

help@VektorT13.pro

help@VektorT13.pro