OpenVPN ГОСТ

Введение

В НАЙС.ОС ГОСТ-криптография доступна «из коробки»: достаточно установить пакет `openvpn` и запустить мастер `vpn-admin`, который ставится вместе с `openvpn.rpm`. В этом разделе — зачем ГОСТ, что рекомендует РКН, и каких целей мы добьёмся в статье.

Что такое ГОСТ-криптография

ГОСТ-криптография — это семейство отечественных криптографических алгоритмов и стандартов, разработанных в России и утверждённых регуляторами (ФСТЭК, ФСБ). В контексте VPN нас интересуют две группы алгоритмов:

Шифрование (data-channel)

- Кузнечик (GOST R 34.12-2015) — блочный шифр 128-битного блока, ключ 256 бит: `kuznyechik-cbc`, `kuznyechik-cfb`, `kuznyechik-ofb`.
- Магма / GOST 28147-89 — 64-битный блок (варианты `magma-cbc`, `gost89-*` используются для совместимости и считаются устаревающими).

Хеш / HMAC (auth)

- Стрибог (GOST R 34.11-2012) — `id-tc26-gost3411-12-256` и `id-tc26-gost3411-12-512` (рекомендуемые значения параметра `auth`).
- GOST R 34.11-94 — устаревший вариант (`id-GostR3411-94`), оставлен для совместимости.

Использование ГОСТ-алгоритмов позволяет строить защищённые каналы связи в соответствии с российскими требованиями, исключая «иностранные» криптопротоколы на уровне канала данных VPN.

10.04.2025

Уведомление РКН: отказ от иностранных протоколов шифрования

РКН рекомендует при передаче данных **отказаться от иностранных протоколов шифрования**, используемых в том числе приложениями, предоставляющими доступ к запрещённой информации.

- Техническая необходимость допускается — направьте заявление с обоснованием и перечнем IP-адресов в ЦМУ ССОП: white_list@cmu.gov.ru.
- Укажите: наименование организации и ИНН; используемый протокол подключения; IP источника (если возможно) и назначения; цель использования; контакты ответственного; дополнительные комментарии (при необходимости).

Официальное уведомление РКН от 10.04.2025

Время публикации: 10.04.2025 18:06; последнее изменение: 10.04.2025 18:09.

Цель статьи

1

Быстрый запуск OpenVPN с ГОСТ в НАЙС.ОС

В НАЙС.ОС всё готово: OpenSSL+ГОСТ и OpenVPN уже поддерживают необходимые алгоритмы. После установки пакета `openvpn` доступен мастер `vpn-admin` (поставляется вместе с `openvpn.rpm`), который развернёт сервер и клиентов.

2

Полный перечень ГОСТ-алгоритмов

Покажем все доступные в OpenVPN ГОСТ-шифры (`kuznyechik-*`, `magma`, `gost89`) и HMAC-дайджесты (`id-tc26-gost3411-12-256/512`), объясним отличия и безопасные варианты.

3

Практика и готовые конфигурации

Приведём готовые конфиги сервера/клиента с `cipher kuznyechik-cbc` и `auth id-tc26-gost3411-12-256`, плюс рекомендации по безопасности (CRL, `tls-crypt`, NAT/маршрутизация) и процедуру взаимодействия с ЦМУ ССОП.

Что вы получите

- Рабочий OpenVPN-сервер с ГОСТ-шифрованием;
- Готовые `.ovpn`-профили клиентов;
- Понимание доступных ГОСТ-алгоритмов и их применения.

Что потребуется

- НАЙС.ОС с установленным пакетом `openvpn`;
- Права `root` и сетевой доступ;
- Мастер `vpn-admin` (устанавливается вместе с `openvpn.rpm`).

Быстрый старт: `dnf install openvpn` → `vpn-admin` → выбрать «kuznyechik-cbc + id-tc26-gost3411-12-256» при создании сервера/клиента.

Где взять инструменты

- `openvpn` — устанавливается командой `dnf install openvpn`.
- `vpn-admin` — мастер настройки, ставится автоматически вместе с пакетом `openvpn.rpm`; запускается командой `vpn-admin` от root.

Почему именно НАЙС.ОС

Выбор дистрибутива для безопасного VPN — ключевой момент. НАЙС.ОС уже содержит всё необходимое для развёртывания OpenVPN с ГОСТ-алгоритмами прямо «из коробки», без сложной подготовки и дополнительной установки криптопровайдеров.

1 OpenSSL с ГОСТ уже установлен

В НАЙС.ОС по умолчанию поставляется `OpenSSL`, собранный с поддержкой ГОСТ-алгоритмов (`kuznyechik`, `magma`, `stribog`). Это означает, что все утилиты и сервисы могут использовать ГОСТ без установки сторонних модулей или патчей.

2 OpenVPN собран с поддержкой ГОСТ

Пакет `openvpn` в НАЙС.ОС собран с прямой поддержкой ГОСТ-шифров и HMAC-добавок. Вам доступны все алгоритмы из `--show-ciphers` и `--show-digests`, включая `kuznyechik-cbc` и `id-tc26-gost3411-12-256`, без необходимости подгрузки дополнительных модулей или криптопровайдеров.

3 Без дополнительной настройки криптопровайдеров

Вам не нужно вручную прописывать пути до движков, менять `openssl.cnf` или подключать проприетарные криптобиблиотеки. Всё готово для работы сразу после установки пакета `openvpn`.

4 Встроенная автоматизация через `vpn-admin`

Вместе с пакетом `openvpn.rpm` устанавливается мастер `vpn-admin` — это интерактивный скрипт на Bash, который автоматизирует развёртывание сервера и генерацию профилей клиентов. С его помощью можно развернуть полностью готовый ГОСТ-VPN за считанные минуты.

Как это работает на практике

1. Установите OpenVPN: `dnf install openvpn`
2. Запустите мастер: `vpn-admin`
3. Выберите **cipher**: `kuznyechik-cbc`
4. Выберите **auth**: `id-tc26-gost3411-12-256`
5. Следуйте инструкциям для генерации сервера и клиентов.

Итог: готовый OpenVPN-сервер с ГОСТ-алгоритмами, профили клиентов `.ovpn` и

полная совместимость с политиками отказа от иностранных протоколов.

ГОСТ-алгоритмы в OpenVPN (НАЙС.ОС)

В дистрибутиве НАЙС.ОС OpenVPN уже собран с поддержкой российских криптографических алгоритмов, что позволяет использовать их без дополнительной настройки. Ниже приведены доступные ГОСТ-шифры, которые можно выбрать с помощью параметра `--data-ciphers` или `--cipher`.

4.1Шифры (`--show-ciphers`)

Алгоритм	Стандарт	Режим	Параметры	Описание и рекомендации
`kuznyechik-cbc`	ГОСТ Р 34.12-2015	CBC	256-бит ключ, 128-бит блок	**Основной рекомендуемый ГОСТ-шифр**. Обеспечивает высокую стойкость, поддержан ФСБ и ФСТЭК. Используется в большинстве современных конфигураций.
`kuznyechik-cfb`	ГОСТ Р 34.12-2015	CFB (TLS only)	256-бит ключ, 128-бит блок	Потоковый режим шифрования, удобен в TLS-сценариях, где CBC невозможен (например, для совместимости с некоторыми клиентами).

Алгоритм	Стандарт	Режим	Параметры	Описание и рекомендации
kuznyechik-ofb	ГОСТ Р 34.12-2015	OFB (TLS only)	256-бит ключ, 128-бит блок	Потоковый режим без обратной связи по шифротексту, снижает риск некоторых атак на CBC, но используется реже.
magma-cbc	ГОСТ 28147-89	CBC	256-бит ключ, 64-бит блок	Старый стандарт («Магма»). Формально поддерживается, но блок 64 бит делает его менее стойким против современных атак. Использовать только для совместимости.
gost89-cbc	ГОСТ 28147-89	CBC	256-бит ключ, 64-бит блок	Устаревшая реализация ГОСТ 28147-89. Совместимость со старыми системами.
gost89-cnt	ГОСТ 28147-89	Counter (TLS only)	256-бит ключ, 64-бит блок	Режим счётчика, используется только в TLS client/server. Поддержка ради обратной совместимости.

Алгоритм	Стандарт	Режим	Параметры	Описание и рекомендации
gost89-cnt-12	ГОСТ 28147-89 (2012)	Counter (TLS only)	256-бит ключ, 64-бит блок	Вариант счётчика с поправками 2012 года. Всё ещё 64-бит блок — использовать с осторожностью.

Замечание: Алгоритмы magma и gost89 имеют длину блока 64 бита, что снижает стойкость при большом объёме передаваемых данных. Рекомендуется использовать kuznyechik-cbc как основной шифр в новых конфигурациях.

4.2Аутентификация / HMAC (--show-digests)

В OpenVPN функция аутентификации пакетов реализуется с использованием HMAC (Keyed-Hash Message Authentication Code). Алгоритм хэширования задаётся через параметр auth в конфигурации. В НАЙС.ОС доступны следующие ГОСТ-хэш-функции, уже интегрированные в OpenSSL и OpenVPN.

Алгоритм	Стандарт	Длина хэша	Описание и рекомендации
id-tc26-gost3411-12-256	ГОСТ Р 34.11-2012	256 бит	**Основной рекомендуемый алгоритм** («Стрибог»). Оптимальный выбор для HMAC в сочетании с kuznyechik-cbc. Обеспечивает высокую скорость и соответствие актуальным требованиям ФСБ и ФСТЭК.

Алгоритм	Стандарт	Длина хэша	Описание и рекомендации
`id-tc26-gost3411-12-512`	ГОСТ Р 34.11-2012	512 бит	Усиленный вариант «Стрибог» с увеличенной длиной хэша. Рекомендуется, если требуется максимальный уровень стойкости (например, для особо важных данных), но будет чуть медленнее.
`id-GostR3411-94`	ГОСТ Р 34.11-94	256 бит	Устаревший алгоритм ГОСТ-хэширования (1994 г.). Оставлен только для совместимости со старыми системами и оборудованием. Не рекомендуется для новых проектов.

Пример использования в конфигурации OpenVPN:

```
auth id-tc26-gost3411-12-256
cipher kuznyechik-cbc
```

Такой набор обеспечивает полное использование современных ГОСТ-алгоритмов шифрования и хэширования.

5Рекомендации по выбору параметров

Ниже — практические профили настроек для OpenVPN в НАЙС.ОС. Базовый вариант ориентирован на актуальные требования и использует современную связку «Кузнечик + Стрибог-256». Отдельно приведены профили совместимости и примечания по TLS.

5.1. Базовый профиль (соответствие современным требованиям ФСТЭК)

Рекомендуемый набор параметров для канала данных (data-channel) и HMAC-аутентификации. Он же — «профиль по умолчанию» для новых развёртываний.

Фрагмент конфига (сервер)

```
data-ciphers kuznyechik-cbc
data-ciphers-fallback kuznyechik-cbc
cipher kuznyechik-cbc
auth id-tc26-gost3411-12-256
```

Фрагмент конфига (клиент)

```
data-ciphers kuznyechik-cbc
data-ciphers-fallback kuznyechik-cbc
cipher kuznyechik-cbc
auth id-tc26-gost3411-12-256
```

Почему так: начиная с OpenVPN 2.5/2.6 основное согласование шифров идёт через `data-ciphers` (а `cipher` оставлен для совместимости со старыми клиентами). Явный `data-ciphers-fallback` гарантирует подключение в смешанных парках.

5.2. Совместимость: `magma-cbc` / `gost89-cbc`

Для старых клиентских устройств/ПО иногда требуется ГОСТ 28147-89 (64-битный блок). Используйте эти профили только при реальной необходимости и ограничивайте объём передаваемых данных.

Профиль	Назначение	Фрагмент конфигурации	Комментарий

`magma-cbc + stribog-256`	Совместимость с системами, поддерживающими «Магму»	`data-ciphers magma-cbc`
		`data-ciphers-fallback magma-cbc`
		`cipher magma-cbc`
		`auth id-tc26-gost3411-12-256`
			64-битный блок снижает стойкость при больших объёмах трафика.

`gost89-cbc + stribog-256`	Наиболее старые реализации ГОСТ 28147-89	`data-ciphers gost89-cbc`
		`data-ciphers-fallback gost89-cbc`
		`cipher gost89-cbc`
		`auth id-tc26-gost3411-12-256`
			Только для крайней совместимости; переводите парк на «Кузнечик».

Важно: алгоритмы с блоком 64 бита (`magma`, `gost89`) повышают риск коллизий при шифровании больших объёмов данных (эффект «birthday bound»). Планируйте миграцию на `kuznyechik-cbc`.

5.3. TLS-поток с ГОСТ-шифрами: `kuznyechik-cfb` / `kuznyechik-ofb`

Для некоторых сценариев (например, при ограничениях на CBC) в TLS-потоке доступны потоковые режимы «Кузнечика». Они применяются только в контексте TLS client/server и не используются как основной data-channel.

Сервер

```
# Основной data-channel остаётся на CBC:
data-ciphers kuznyechik-cbc
cipher kuznyechik-cbc
auth id-tc26-gost3411-12-256

# Для TLS-контроля при необходимости:
# (зависит от доступности соответствующих шифросьютов на вашей сборке)
# tls-cipher ...
```

Клиент

```
data-ciphers kuznyechik-cbc
cipher kuznyechik-cbc
auth id-tc26-gost3411-12-256
# При необходимости для TLS:
# (клиент подхватит разрешённые сервером шифросьюиты)
```

Примечание: список реально доступных TLS-шифросьютов зависит от сборки OpenVPN/OpenSSL. В любом случае канал данных (data-channel) можно и нужно держать на `kuznyechik-cbc` + `id-tc26-gost3411-12-256`.

5.4. Дополнительные рекомендации по безопасности

- **Используйте `tls-crypt` вместо `tls-auth`** — это скрывает сигнатуру TLS и усложняет сканирование порта.
- **Ограничивайте `data-ciphers` минимально необходимым набором** (желательно

одним значением) для исключения даунгрейдов.
- **Регулярно обновляйте CRL** и следите за сроками действия сертификатов.
- **Ограничьте доступ к management-сокету** (права на файловый сокет, недоступность извне).
- **Логируйте и мониторьте** подключённые сессии; при необходимости экспортируйте метрики в Prometheus.

5.5. Мини-чеклист

- Новые установки: **kuznyechik-cbc** + **id-tc26-gost3411-12-256**.
- Смешанный парк: добавьте `data-ciphers-fallback` (но минимизируйте список шифров).
- Совместимость со старыми системами: временно `magma-cbc` или `gost89-cbc`; планируйте миграцию.
- TLS-поток с ограничениями на CBC: рассматривайте `kuznyechik-cfb` / `kuznyechik-ofb` (если поддерживается).

6Настройка сервера

В НАЙС.ОС мастер `vpn-admin` устанавливается вместе с пакетом `openvpn.rpm`. Он автоматизирует генерацию PKI, создание конфигурации OpenVPN и systemd-юнита. Ниже — пошаговая процедура и готовый пример конфигурации с ГОСТ-алгоритмами.

6.1. Запуск скрипта `vpn-admin`

1. Откройте консоль под `root` и запустите мастер:

   ```
   vpn-admin
   ```

2. В главном меню выберите пункт **«Создать серверный инстанс»**.
3. Укажите шифр и HMAC из списка (см. разделы 4.1 и 4.2). Рекомендуемая связка: cipher: kuznyechik-cbc auth: id-tc26-gost3411-12-256.
4. Мастер автоматически:
   - сгенерирует инфраструктуру ключей (CA + серверный сертификат);
   - создаст конфигурацию OpenVPN с ГОСТ-параметрами;
   - развернёт systemd-юнит `openvpn-server@<имя>.service` для автозапуска.

6.2. Пример конфигурации сервера (ГОСТ)

фрагмент `*.conf`

```
port 1194
proto udp
dev tun

# ГОСТ: канал данных
data-ciphers kuznyechik-cbc
data-ciphers-fallback kuznyechik-cbc
cipher kuznyechik-cbc
auth id-tc26-gost3411-12-256

# TLS-режим сервера
tls-server

# PKI
ca   ca.crt
cert server.crt
key  server.key

# Диффи-Хеллман
dh none
```

Пояснения

- `data-ciphers` — основной механизм согласования шифров в OpenVPN 2.5+;
- `cipher` — оставлен для совместимости со старыми клиентами;
- `auth` — HMAC/хеш (Стрибог-256);
- `dh none` — для современных профилей ECDH/TLS; если ваша инфраструктура создаёт `dh.pem`, укажите его явно: `dh dh.pem`.

Совет по безопасности: при возможности используйте `tls-crypt` вместо `tls-auth`, чтобы скрыть сигнатуру TLS и усложнить сканирование порта.

6.3. Запуск сервиса и автозагрузка (systemd)

После генерации конфигурации запустите серверный инстанс и включите его автозапуск:

```
systemctl enable --now openvpn-server@myvpn
```

Проверка статуса

```
systemctl status openvpn-server@myvpn
journalctl -u openvpn-server@myvpn -b
```

Быстрая диагностика

- порт/протокол открыты в фаерволе;
- включён `net.ipv4.ip_forward=1` (мастер настраивает автоматически);
- CRL подключён, сертификаты не просрочены.

Готово: сервер с ГОСТ-алгоритмами запущен. Перейдите к созданию клиентских профилей в мастере («Создать клиента») и раздайте `.ovpn` сотрудникам.

7Настройка клиента

Мастер `vpn-admin` в НАЙС.ОС автоматизирует создание клиентских профилей. Профиль `.ovpn` включает все необходимые ключи, сертификаты и параметры ГОСТ-шифрования, чтобы клиент мог подключиться к серверу без ручной донастройки.

7.1. Создание клиентского профиля

1. Запустите мастер `vpn-admin`:

   ```
   vpn-admin
   ```

2. В меню выберите **«Создать клиента»**.
3. Введите имя клиента (например, `user01`).
4. Мастер сгенерирует `.ovpn`-файл, в который будут встроены:
   - ключ клиента (`inline`);
   - сертификат клиента (`inline`);
   - сертификат CA (`inline`);
   - настройки шифрования и HMAC ГОСТ.

7.2. Пример содержимого .ovpn

фрагмент

```
client
dev tun
proto udp
remote vpn.example.ru 1194

# ГОСТ-шифрование
cipher kuznyechik-cbc
auth id-tc26-gost3411-12-256

resolv-retry infinite
nobind
persist-key
persist-tun

# Сертификаты и ключи встроены ниже
<ca>...</ca>
<cert>...</cert>
<key>...</key>
```

7.3. Подключение к серверу

Готовый `.ovpn`-профиль можно использовать:

Через OpenVPN GUI

- Откройте GUI-клиент OpenVPN;
- Импортируйте `.ovpn`-файл;
- Выберите профиль и нажмите **Connect**.

Через командную строку

```
openvpn --config client.ovpn
```

Готово: клиент подключён к серверу с ГОСТ-алгоритмами, канал зашифрован по стандартам ФСТЭК.

8Проверка работы

После настройки сервера и клиента необходимо убедиться, что соединение установлено корректно и используется именно ГОСТ-шифрование.

8.1. Просмотр логов OpenVPN

Логи можно просмотреть с помощью `journalctl`:

```
journalctl -u openvpn-server@myvpn
```

Замените `myvpn` на имя вашего серверного инстанса.

8.2. Проверка используемого шифра и HMAC

В логе успешного подключения клиента должна появиться строка, подтверждающая использование ГОСТ-алгоритмов:

```
Data Channel: cipher 'kuznyechik-cbc' authenticated with 'id-tc26-gost3411-12-256'
```

Важно: если в этой строке указан другой шифр или HMAC, значит, используется не ГОСТ-алгоритм. Проверьте настройки `cipher` и `auth` на сервере и клиенте.

9Мониторинг и управление

НАЙС.ОС с установленным OpenVPN и скриптом `vpn-admin.sh` позволяет удобно контролировать работу VPN-сервера и управлять подключёнными клиентами.

9.1. Просмотр подключённых пользователей

Для получения списка активных VPN-подключений запустите `vpn-admin.sh` и выберите соответствующий пункт меню:

```
./vpn-admin.sh
```

В интерфейсе будут отображены IP-адреса, время подключения и используемые алгоритмы.

9.2. Отключение клиента (CRL)

Если необходимо заблокировать доступ конкретного клиента, используйте функцию создания списка отозванных сертификатов (CRL) в `vpn-admin.sh`.

1. Запустите `vpn-admin.sh`.
2. Выберите пункт **«Отозвать сертификат клиента»**.
3. Введите имя клиента.

После отзыва сертификата клиент больше не сможет подключаться к серверу, даже если у него сохранён старый профиль.

9.3. Ротация ключей

Для повышения безопасности рекомендуется периодически менять ключи шифрования и сертификаты.

- Запустите `vpn-admin.sh` и создайте новый серверный сертификат.
- Пересоздайте клиентские сертификаты и выдайте новые профили пользователям.

Оптимальный срок ротации ключей — каждые 6–12 месяцев, в зависимости от политики информационной безопасности вашей организации.

10Взаимодействие с ЦМУ ССОП по уведомлению РКН

В соответствии с уведомлением РКН от **10.04.2025**, использование иностранных протоколов или шифров, не соответствующих ГОСТ, требует согласования с Центром мониторинга и управления сетью связи общего пользования (ЦМУ ССОП).

10.1. Когда требуется согласование

Согласование необходимо в случаях, когда:

- Используются иностранные алгоритмы шифрования или аутентификации (например, AES, CHACHA20, SHA256 и др.) вместо ГОСТ.
- Организация не может перейти на ГОСТ по техническим причинам и вынуждена использовать зарубежные криптографические протоколы.
- Требуется обеспечение совместимости с зарубежными партнёрами или поставщиками.

Если вы используете **только ГОСТ-алгоритмы** (например, `kuznyechik-cbc` и `id-tc26-gost3411-12-256`), согласование **не требуется**.

10.2. Шаблон письма

Для согласования необходимо направить письмо в ЦМУ ССОП по установленной форме. Пример структуры письма:

```
Наименование организации: ООО "Пример"
ИНН: 7700000000
Протокол подключения: OpenVPN с использованием AES-256-GCM
IP-адрес источника: 203.0.113.10
IP-адрес назначения: 198.51.100.25
Цель подключения: Обмен данными с зарубежным филиалом
Контактное лицо: Иванов Иван Иванович, +7 (999) 123-45-67, ivanov@example.com
```

Формат письма может быть как в электронном виде (с ЭЦП), так и на бумажном носителе.

10.3. Пример заполнения при использовании западных шифров

Ниже приведён пример письма, если организация использует OpenVPN с зарубежными шифрами:

```
Наименование организации: АО "ТехСвязь"
ИНН: 7800000000
```

```
Протокол подключения: OpenVPN с использованием AES-256-GCM и SHA256
IP-адрес источника: 192.0.2.50
IP-адрес назначения: 203.0.113.77
Цель подключения: Передача данных между офисами в России и ЕС
Причина использования иностранных алгоритмов: Требования совместимости с зарубежными партнёрами
Контактное лицо: Петров Пётр Петрович, +7 (495) 555-55-55, petrov@techsvyaz.ru
```

В таком случае организация должна дождаться положительного ответа ЦМУ ССОП, прежде чем эксплуатировать подключение.

11Рекомендации по безопасности

Следующие меры помогут повысить криптостойкость и надёжность VPN-соединений в НАЙС.ОС при использовании ГОСТ-алгоритмов.

11.1. Избегайте устаревших алгоритмов

Алгоритмы `GOST R 34.11-94`, `gost89-cbc` и их варианты с 64-битным блоком считаются устаревшими и менее устойчивыми к атакам.

Используйте их только при необходимости совместимости со старыми системами.

11.2. Регулярно обновляйте CRL

Список отозванных сертификатов (CRL) необходимо пересоздавать до истечения его срока действия, чтобы исключить подключение скомпрометированных клиентов.

```
vpn-admin.sh # Пункт: Обновить CRL
```

Если CRL истечёт, сервер OpenVPN отклонит все новые подключения до обновления файла.

11.3. Минимизируйте набор доступных шифров

Указывайте только необходимые алгоритмы в параметре `data-ciphers`, чтобы исключить возможность использования слабых шифров.

```
data-ciphers kuznyechik-cbc
cipher kuznyechik-cbc
auth id-tc26-gost3411-12-256
```

Чёткое определение списка шифров предотвращает «даунгрейд»-атаки и повышает безопасность канала.

12Заключение

ГОСТ-криптография в **НАЙС.ОС** доступна «из коробки» — без сложных манипуляций, дополнительных модулей или настройки криптопровайдеров. OpenVPN, собранный с поддержкой ГОСТ-алгоритмов, позволяет быстро и безопасно развернуть VPN, соответствующий требованиям РКН и ФСТЭК.

Мы призываем системных администраторов и IT-отделы протестировать и внедрить данное решение в корпоративной инфраструктуре, чтобы обеспечить надёжную защиту передаваемых данных и соответствие нормативным требованиям.

⚠ ВАЖНОЕ ПРЕДУПРЕЖДЕНИЕ

VPN с ГОСТ-шифрованием предназначен **только** для обеспечения защищённого доступа к корпоративным ресурсам и взаимодействия с доверенными сетями.

- Категорически **запрещается** использовать данное решение для обхода блокировок, получения доступа к запрещённой информации или любых противоправных действий.
- Запрещено рекламировать, распространять или предлагать данную настройку как средство для действий, нарушающих законодательство РФ.
- Администратор, настраивающий VPN, несёт **полную ответственность** за его использование.
- В случае выявления нарушений ответственность наступает в соответствии с действующим законодательством, включая административную и уголовную.

Используйте VPN с ГОСТ только по назначению, в рамках закона и внутренних политик вашей организации.