

ВЕРСИЯ 1.9 · 28 ОКТЯБРЯ 2026 Г.

Colitu: технический документ по безопасности

Архитектура безопасности, модель угроз и защита приватности

Чему вам приходится доверять при использовании Colitu, кто и что может видеть, от каких атак Colitu защищает, а от каких нет, и как вы можете проверить наши утверждения. Каждое утверждение описывает то, что работает в выпущенных версиях на сегодняшний день. Там, где чего-то не хватает или защита слабее, чем должна быть, мы говорим об этом прямо.

ВЕРСИЯ	ОБНОВЛЕНО	КОНТАКТ ПО БЕЗОПАСНОСТИ
1.9	28 октября 2026 г.	security@colitu.com

ОТНОСИТСЯ К ВЕРСИЯМ

Android 2.9.9 · Windows 3.0.5 · Linux 1.6.2 (бета) · iOS 5.9.7 (TestFlight) · управляющий контур по состоянию на 16 октября 2026 г., агент узла по состоянию на 7 октября 2026 г.

ИСХОДНЫЙ КОД

Приложения для Android, Windows и Linux: github.com/colitu; приложение для iOS: github.com/colitu/ios (все под GPL-3.0). Серверное ПО: исходный код закрыт.

Безопасность Colitu в одной таблице

Краткая сводка разделов ниже. Зелёный: работает так, как описано, на всех указанных платфор
Жёлтый: частично или с описанными ограничениями. Красный: пока нет.

Приложения с открытым исходным кодом	● Приложения для Android, iOS, Windows и Linux открыты (GP 3.0). Исходный код серверного ПО закрыт.
Зашифрованный туннель	● Hysteria2, VLESS Reality, VLESS XHTTP, Trojan и Shadowsock 2022 на основе проверенных реализаций (Xray-core, sing-box Hysteria).
Содержимое трафика и история посещений	● Не записываются. VPN-серверы не ведут журналы отдельн подключений.
Объём трафика по пользователям	● Записывается по каждому серверу интервалами примерно 15 секунд и хранится 90 дней для учёта квот, после чего остан только итоги за период.
DNS через туннель	● Да в приложениях для Android и iOS и в режиме TUN. В реж системного прокси — нет для приложений, работающих в обх прокси (на Linux он по умолчанию; новые установки Windows начинают с режима TUN).
Защита от утечек IPv6	● Блокируется на Android и iOS, а также на Windows и Linux в режиме TUN при включённом kill switch. В режиме системног прокси не охватывается.
Kill switch (аварийное отключение)	● Windows: собственная служба с постоянными правилами брандмауэра; Linux (режим TUN): правила nftables; оба продолжают блокировку при аварийном завершении приложения. Android полагается на системную настройку «Постоянная VPN»; на iOS есть необязательный переключател «Блокировать интернет без VPN» (по умолчанию выключен).
Региональные сайты в обход VPN	● В новых установках по умолчанию выключено (режим приватности включён) начиная с Windows и Android 2.7.0, iOS 5.6.0 и Linux 1.3.0; установки, сделанные раньше, сохраняют прежнюю настройку. Если режим приватности выключить, са из встроенного списка идут в обход VPN во всех четырёх приложениях, кроме случаев, когда вы подключены к серверу этом регионе. Описано в §9.

Двухэтапная проверка для пользователей	● Необязательна для любого аккаунта (настраивается на сай все четыре приложения запрашивают код при входе. Для аккаунтов администраторов обязательна.
Passkey и управление сеансами	● Passkey для сайта (до 10 на аккаунт); страница безопасност показывает и завершает сеансы в браузерах; при смене паро все остальные сеансы завершаются. Приложения входят по паролю, как раньше.
Закреплённое соединение с API в приложениях	● Начиная с релизов приложений от 10 октября 2026 г. все четыре приложения закрепляют (pinning) корневые центры сертификации Let's Encrypt (ISRG) и Google Trust Services для API. Ограничения: §12.
Раздельное туннелирование	● Приложения, сайты и IP-адреса на Windows, Android и Linu (приложения на Windows и Linux только в режиме TUN); на iO только сайты и IP-адреса, так как iOS разрешает VPN для отдельных приложений только в управляемых профилях.
Colitu Shield (защита на уровне DNS)	● Необязательно. Блокирует домены рекламы, трекеров, вредоносного ПО, фишинга, мошенничества и криптомайнинг (около 380 тысяч правил). На его резолверах нет журнала запросов и статистики.
Сторонняя аналитика	● Отсутствует во всех приложениях (Android, iOS, Windows, Linux). Из приложения для iOS удалена в версии 5.4.1.
Подписанные обновления	● Подписанный манифест обновлений (ECDSA P-256) и SHA-2 на Android, Windows и Linux; подпись App Store на iOS.
Подпись кода Windows (Authenticode)	● Пока нет.
Воспроизводимые сборки	● Android начиная с 2.9.3 и Windows начиная с 2.9.8: исходны код с тегом даёт побайтово идентичный файл. iOS и Linux пока нет.
Спецификация компонентов ПО (SBOM)	● SPDX для каждого выпуска Android и Windows на GitHub; д Linux пока нет.
Независимый аудит безопасности	● Пока не проводился.

Сообщение об уязвимостях	🟢 security@colitu.com, правила — в §18 и в security.txt.
Размещение на собственных серверах	🔴 Не предлагается. Все серверы Colitu эксплуатирует самостоятельно.

1 Краткое изложение

Colitu — это VPN-сервис с приложениями для Android, Windows, Linux и iOS. Он рассчитан на недоверенные или нестабильные сети: каждый сервер поддерживает несколько транспортов, и приложение выбирает тот, который работает в сети пользователя.

Цель архитектуры — свести к минимуму объём чувствительных данных в каждом отдельном ме Аккаунты и платежи находятся в управляющем контуре, через который никогда не проходит VP трафик. VPN-серверы передают трафик, но не хранят адреса электронной почты и платёжные данные. Приложения хранят свои учётные данные в защищённом хранилище каждой платформ

В этом документе описаны архитектура, модель угроз, протоколы, обращение с ключами и аккаунтами, что записывается в журналы, как защищены обновления, известные ограничения и оставшаяся работа. Он написан для читателей, которые хотят проверить наши утверждения, а н принимать их на веру.

Принципы

- Собирать как можно меньше и точно сообщать, что именно мы собираем.
- Шифровать трафик между приложением и VPN-сервером с помощью проверенных протокол Собственной криптографии у Colitu нет.
- Держать аккаунты и платежи отдельно от серверов, передающих трафик.
- Предпочитать задокументированные ограничения широким обещаниям.
- Делать поведение приложений проверяемым: публиковать исходный код приложений для An Windows, Linux и iOS.

> VPN не делает вас анонимным. Он переносит доверие с вашей локальной сети и интернет-провайдера на оператора VPN. В этом документе объясняется, что именно охватывает это доверие.

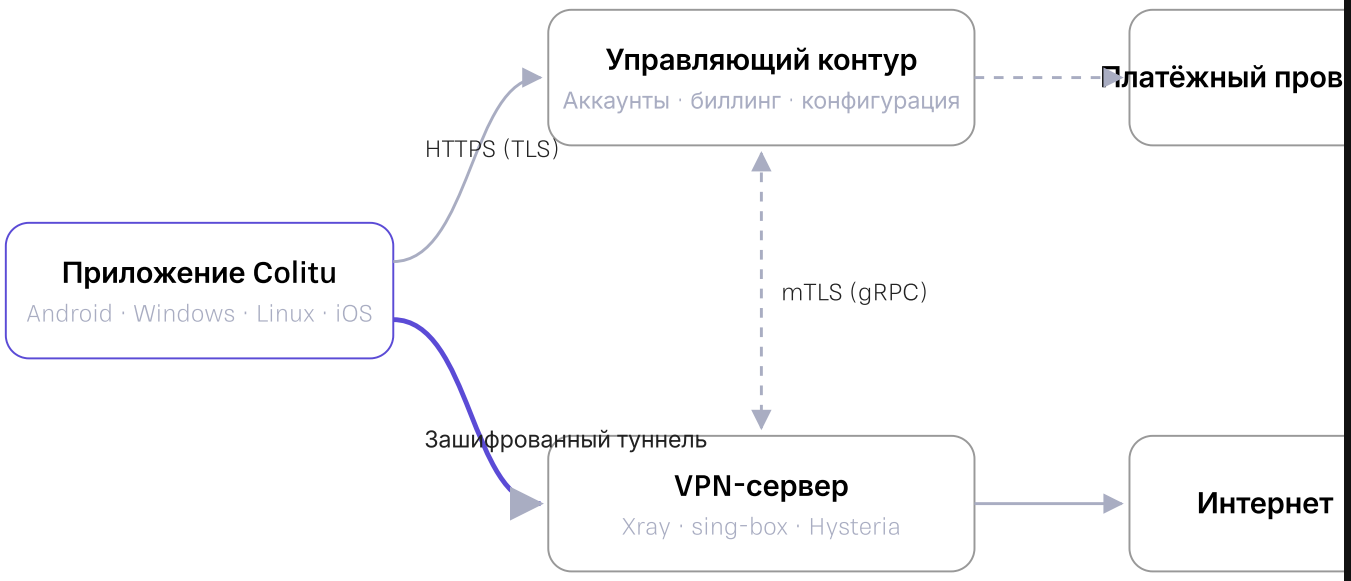
2 Область применения

Охватывается: приложения Colitu для Android, Windows, Linux и iOS; управляющий контур (API аккаунтов, биллинг, конфигурация, панель администратора); VPN-серверы и агент узла, который настраивает; DNS-серверы Colitu Shield; доставка обновлений; colitu.com и его поддомены.

Не охватывается: безопасность операционной системы и устройства пользователя, расширения браузера и другое ПО на устройстве, внутренняя безопасность платёжного провайдера и других третьих сторон, перечисленных в §11, а также сайты, которые посещает пользователь.

3 Архитектура

Colitu разделяет управляющий контур (control plane), которому известно, кто пользователи, и контур передачи данных (data plane), по которому идёт их трафик.



Управляющий контур и контур передачи данных. Через управляющий контур никогда не проходит VPN-трафик; VPN-серверы не хранят адреса электронной почты и платёжные данные.

Компоненты

Компонент	Функции	Хранит
Приложение	Вход, выбор сервера, выбор протокола и переключение на резервный, установка туннеля, настройки маршрутизации и DNS, kill switch там, где он есть, проверка обновлений.	Токены сессии и текущие параметры подключения (§12).
Управляющий контур	Аккаунты, вход, подписки и платежи, регистрация устройств, формирование конфигурации каждого сервера, панель администратора, поддержка.	Данные аккаунтов и билли (§10). Работает на одном сервере; база данных недоступна из интернета.

Компонент	Функции	Хранит
Агент узла	Работает на каждом VPN-сервере. Получает свою конфигурацию по TLS с взаимной аутентификацией, запускает VPN-ядра, передаёт счётчики трафика по пользователям и данные о состоянии.	Ключи протоколов этого сервера и учётные данные подключения пользовател которые им пользуются, с привязкой к внутреннему идентификатору пользоват Адресов электронной почт нет.
VPN-сервер (контур передачи данных)	Завершает зашифрованный туннель и передаёт трафик в интернет.	Ничего сверх данных аген Журналов трафика и подключений нет (§10).
Colitu Shield DNS	Необязательный DNS-over-HTTPS-резолвер (AdGuard Home) на трёх VPN-серверах, доступный изнутри туннеля, который блокирует домены рекламы, трекеров, вредоносного ПО, фишинга, мошенничества и криптомайнинга: около 380 тысяч правил, списки обновляются каждые 24 часа. Вышестоящие резолверы — Cloudflare и Quad9 по DoH, ECS отключён.	Журнала запросов нет, статистики нет.

Как устанавливается подключение

1. Приложение выполняет вход по HTTPS и получает короткоживущие токены.
2. Оно запрашивает у управляющего контура список серверов и параметры подключения к выбранному.
3. Оно перебирает транспорты по порядку и оставляет первый, который прошёл проверку связи
4. Далее трафик идёт по пути приложение → VPN-сервер → интернет. Управляющий контур на э пути не находится.

4 Модель доверия

Пользуясь Colitu, вы должны доверять:

- установленному вами приложению Colitu, а также устройству и операционной системе, на ко оно работает;
- VPN-серверу, к которому вы подключаетесь, и хостинг-провайдеру, который его обслуживае (VPN-серверы — арендованные виртуальные машины без шифрования дисков, поэтому у

провайдера есть к ним технический доступ);
- управляющему контуру Colitu и людям, которые его эксплуатируют;
- реализациям протоколов, которые использует Colitu (Xray-core, sing-box, Hysteria), и криптографическим библиотекам, на которых они построены.

Вам не нужно доверять локальной сети или интернет-провайдеру содержимое и адресатов туннелируемого трафика. Тем не менее они могут видеть:

- что вы подключаетесь к серверу Colitu, его IP-адрес и порт;
- когда вы подключены и примерно сколько данных вы отправляете и получаете;
- возможно, что это VPN-трафик — в зависимости от протокола и средств анализа трафика в се
- трафик, который приложение намеренно отправляет в обход туннеля: некоторые региональн сайты (§9), трафик локальной сети, проверки обновлений и измерения задержки.

Вы	**Локальная сеть / провайдер**	**VPN-сервер**	**Сайт**
	Видит ваш IP, IP сервера, время и объём	Видит ваш IP, адресатов и время; не видит содержимое HTTPS	Видит IP VPN-сер

Кто что видит для трафика, идущего через туннель.

5 Модель угроз

Colitu предназначен для защиты трафика от враждебных или недоверенных локальных сетей, о интернет-провайдеров, которые читают или записывают ваши действия, и от многих видов сете фильтрации. Он не рассчитан на обеспечение анонимности против противника, способного одновременно наблюдать трафик на входе в VPN и на выходе из него.

Угроза	Защищено?	Пояснение
Прослушивание в общедоступной сети Wi-Fi	● Да	Туннелируемый трафик зашифрован между приложением и VPN-сервером.
Чтение интернет-провайдером содержимого или адресатов трафика	● Да, для туннелируемого трафика	Кроме трафика, намеренно направляемого в обход туннеля (§9).

Угроза	Защищено?	Пояснение
Обнаружение интернет-провайдером использования VPN	🟡 Иногда	Reality, XHTTP и Hysteria2 спроектированы та чтобы выглядеть как обычный TLS или QUIC, необнаружимых транспортов не бывает.
Утечки DNS	🟡 В основном	Android, iOS и режим TUN на Windows разрешают имена через туннель. Режим про на Windows не охватывает системный резол
Утечки IPv6	🟡 Частично	См. §9.
Утечка при обрыве туннеля	🟡 Частично	На Windows и Linux есть kill switch, который продолжает блокировку при аварийном завершении приложения (пробелы описаны ниже); на Android нужна системная настройк на iOS есть необязательный переключатель «Блокировать интернет без VPN», по умолча выключенный.
Атака «человек посередине» на API аккаунтов	🟢 Да	TLS с системной проверкой сертификатов; начиная с релизов приложений от 10 октября 2026 г. все четыре приложения дополнитель закрепляют (pinning) корневые центры сертификации Let's Encrypt (ISRG) и Google T Services, поэтому установленный на устройс чужой корневой сертификат нельзя использовать для чтения трафика API.
Вредоносный или скомпрометированный VPN-сервер	🔴 Нет	Сервер видит ваш IP-адрес и адресатов ваш трафика, но не содержимое HTTPS-соединен
Компрометация управляющего контура	🟡 Частично	Злоумышленник получит данные аккаунтов и биллинга и сможет отправлять конфигурации серверы. Содержимого трафика там нет ник

Угроза	Защищено?	Пояснение
Кража пароля от аккаунта	● Частично	Ограничения частоты запросов замедляют подбор, а сеансы на устройствах можно завершить. Необязательная двухэтапная проверка (приложение-аутентификатор) означает, что один украденный пароль уже н даёт войти, но она выключена, пока вы её не включите. Passkey — альтернативный способ входа на сайте; смена пароля завершает все остальные сеансы, а сброс пароля на 24 часа блокирует удаление аккаунта и отключение двухэтапной проверки.

Рассматриваемые противники

Класс	Пример	Защита Colitu
A1 Злоумышленник в локальной сети	Человек в той же сети Wi-Fi в кафе	Надёжная для туннелируемого трафика.
A2 Интернет-провайдер	Провайдер или оператор мобильной связи пользователя	Надёжная для содержимого и адресатов; время и объём остаю видимыми.
A3 Цензор	Фильтрация в масштабах сети с DPI и активным зондированием	Несколько транспортов и автоматическое переключение н резервный; гарантий нет (§14).
A4 Вредоносный VPN-сервер или хостинг	Скомпрометированный сервер или враждебный хостинг-провайдер	Ограниченная: видит те же метаданные, что и сервер. Учётн данные у каждого сервера свои поэтому один сервер нельзя использовать для доступа к остальным.
A5 Скомпрометированный управляющий контур	Злоумышленник с доступом к панели	Ограниченная: данные аккаунто раскрыты; содержимого трафик истории посещений, которые мо было бы похитить, нет.
A6 Злоумышленник на конечном устройстве	Вредоносное ПО на устройстве пользователя	Нет.
A7 Глобальный пассивный противник	Наблюдатель за обоими концами туннеля	Нет.

6 Протоколы

Каждый сервер поддерживает один и тот же набор транспортов. Colitu не изобретает криптогра шифрование, аутентификацию и обмен ключами обеспечивают Xray-core, sing-box и Hysteria и используемые ими библиотеки.

Транспорт	Принцип работы	Аутентификация сервера	Примечания и ограничени
Hysteria2	QUIC (UDP) с TLS 1.3	Сертификат, выданный серверу Let's Encrypt (ACME)	Быстрый в сетях с потеря Не работает там, где UDP блокируется или замедляется.
VLESS Reality	TCP; Reality выполняет рукопожатие TLS 1.3, имитирующее реальный сайт, с ключами X25519	Открытый ключ Reality сервера, передаваемый вместе с конфигурацией	Создан для противодейст DPI и активному зондированию. Не гарантирует защиту от блокировки по IP.
VLESS XHTTP	Reality плюс HTTP-подобный поток	Как у Reality, с собственными ключами	Для сетей, которые обрывают долгоживущие TCP-соединения.
Trojan	TCP с TLS (версии 1.2 или 1.3; сервер пока не требует 1.3 принудительно)	Тот же сертификат, что и у Hysteria2	Резервный вариант на TL там, где UDP заблокиров
Shadowsocks 2022	2022-blake3-aes-256-gcm (AEAD), новый ключ для каждой сессии	Предварительно согласованный ключ	Лёгкий и быстрый. Нет прямой секретности (for secrecy): утечка ключа позволила бы расшифров записанные сессии.

Какое ядро обслуживает транспорт, зависит от платформы. Android и iOS используют Xray-core всех транспортов, включая Hysteria2. Windows и Linux используют Xray-core для VLESS, Trojan и Shadowsocks и sing-box для Hysteria2. На серверах Xray обслуживает VLESS, sing-box — Trojan Shadowsocks, а официальный сервер Hysteria — Hysteria2.

Переключение транспортов происходит автоматически, но не бесшовно: при переходе приложе на другой транспорт туннель разрывается и строится заново, что занимает около секунды или

больше.

7 Криптография и управление ключами

Назначение	Механизм
Приложение и сайт → API	TLS 1.2/1.3 с системной проверкой сертификатов. Начиная с релизов приложений от 10 октября 2026 г. приложения для Windows, Android, L и iOS дополнительно закрепляют корневые ключи Let's Encrypt (ISRG) Google Trust Services для API. Закрепление перестаёт применяться 31 декабря 2027 г., поэтому старые версии приложений никогда не окажу заблокированными.
Хранение паролей	Argon2id: 64 МиБ памяти, 3 прохода, 2 потока, случайная соль 16 байт, 32 байта. Пароли никогда не хранятся в открытом виде.
Токены доступа	JWT, подписанные HMAC-SHA256 ключом из ротируемого набора клю срок действия 15 минут.
Токены обновления	32 случайных байта, хранятся только в виде хеша SHA-256, действуют дней, заменяются при каждом использовании. Повторное использова старого токена отзывает всё семейство токенов.
Управляющий контур ↔ VPN-серверы	Взаимный TLS 1.3 (gRPC). Удостоверяющий центр на ECDSA P-256; сертификаты серверов действуют 30 дней и обновляются автоматиче отзыв — через список разрешённых отпечатков.
Ключи Reality	Пара ключей X25519 для каждого транспорта на каждом сервере, генерируется в управляющем контуре.
TLS-сертификаты серверов	Let's Encrypt, выпускаются на каждом сервере; закрытый ключ остаёт на этом сервере.
Секреты в базе данных	Учётные данные платёжного, почтового и ИИ-провайдеров зашифрова AES-256-GCM.
Манифесты обновлений	Подписи ECDSA P-256, которые приложения проверяют по встроенно открытому ключу.
Резервные копии	Зашифрованы с помощью age на открытый ключ; для создания копии нужен только этот ключ. Ключ расшифровки хранится офлайн, не на каком-либо сервере.

Назначение	Механизм
Отпечатки для проверок злоупотреблений и переносов	HMAC-SHA256 с ключом, производным от ключа шифрования настрое который не хранится в базе данных.

Где хранятся ключи и что будет при утечке

- Закрытый ключ удостоверяющего центра хранится в файле в управляющем контуре. Получив его мог бы выпускать удостоверения серверов, поэтому это самый чувствительный ключ из что у нас есть.
- Каждый VPN-сервер хранит собственные закрытые ключи Reality, ключ своего TLS-сертифик учётные данные подключения пользователей, которые к нему подключались. Эти учётные да случайны и различаются на каждом сервере, поэтому компрометация одного сервера не раскрывает учётные данные, действующие на других.
- Закрытые ключи Reality и учётные данные подключения пользователей хранятся в базе данн управляющего контура в незашифрованном виде. Шифрование этих значений на уровне базы данных включено в план работ.
- Плановой ротации ключей Reality пока нет. Если есть подозрение на компрометацию сервер убирают из приложений, а его ключи и учётные данные заменяют.
- Управляющий контур каждый день делает зашифрованную резервную копию и хранит её 3 д Копия отправляется в Backblaze B2 (EU Central, Амстердам) с Object Lock: в течение 30 дней включая Colitu, не может её удалить или изменить, а автоматически она удаляется не поздне через 36 дней. Ключ расшифровки хранится офлайн с 16 октября 2026 г., поэтому копии не мо прочитать ни сервер, ни Backblaze. Восстановление из внешней копии проверено 16 октября г. Снимки базы данных, сделанные перед развёртыванием, не шифруются и остаются на серв управляющего контура не более 7 дней.

8 Аккаунты и сессии

- Вход выполняется по адресу электронной почты и паролю. Телевизор может выполнить вход показав QR-код, который подтверждается на телефоне с выполненным входом (8-символьны действует 10 минут). Входа через Google, Telegram или другие сторонние сервисы нет.
- Пароль должен содержать не менее 10 символов. Новый аккаунт получает доступ к VPN толь после подтверждения 6-значного кода, отправленного по электронной почте.
- Для сброса пароля используется 6-значный код, действующий 15 минут, одноразовый, с ограничением в 5 попыток. Ответ одинаков независимо от того, существует ли аккаунт с этим адресом. Сброс пароля завершает сеансы на всех устройствах и все веб-сессии. После сбро коду из письма удаление аккаунта и отключение двухэтапной проверки блокируются на 24 ча (ошибка RECOVERY_LOCKED).

- Вход, регистрация, сброс пароля и промокоды ограничены по частоте для каждого IP-адреса сайте вход и сброс пароля дополнительно ограничены для каждого адреса электронной почт приложениях вход ограничен только по IP. Блокировки пользовательских аккаунтов нет.
- Выход из аккаунта отзывает токен обновления этого устройства. Его токен доступа остаётся действительным до истечения срока (не более 15 минут).
- Устройства можно удалять на странице аккаунта. Страница безопасности показывает сеансы браузерах с названием устройства (браузер и операционная система), страной, способом вх IP-адресом; можно завершить один сеанс, все остальные (текущий останется) или выйти вез
- Смена пароля на сайте сохраняет сеанс браузера, в котором вы находитесь, и завершает все остальные веб-сессии и все токены обновления приложений. Токены доступа приложений, выданные до смены, перестают работать сразу (ошибка AUTH_SESSION_REVOKED).
- Действия, которые повторно запрашивают пароль (смена пароля, удаление аккаунта, измене двухэтапной проверки, passkey), ограничены 10 попытками за 15 минут на аккаунт.
- Двухэтапная проверка (TOTP) необязательна для любого аккаунта. Вы включаете её на colitu.com/account/security с помощью приложения-аутентификатора и получаете 10 однора кодов восстановления; после этого приложения запрашивают код после пароля (поддержива начиная с версий Windows 2.6.0, Android 2.6.0, Linux 1.2.0 и iOS 5.5.0; старое приложение поп обновиться). Настраивается только на сайте.
- Passkey: на colitu.com в разделе «Аккаунт → Безопасность» (нужен пароль) можно добавить passkey, назвать каждый и удалить его с помощью пароля, а затем входить через «Войти с passkey» на странице входа. Passkey с проверкой пользователя считается двумя факторами, поэтому код двухэтапной проверки не запрашивается; вход из страны, которую не видели последние 90 дней, по-прежнему требует код из письма. Passkey не работают на зеркальных доменах. Приложения входят как раньше или через подтверждение QR-кода привязки устрой в браузере, где выполнен вход с passkey.
- Colitu отправляет письмо о безопасности в случаях: новое устройство в приложении (кроме первого), вход из новой страны (не встречавшейся 90 дней), включение или отключение двухэтапной проверки, повторное создание кодов восстановления, добавление или удаление passkey и смена пароля.
- Ссылки подписки: помимо основной ссылки можно создать до 5 дополнительных именованн ссылок с необязательным сроком действия 7, 30 или 90 дней и отзывать их по одной. Если со за короткое время использовали из множества разных сетей, появляется предупреждение. I адреса для этого Colitu не хранит: только анонимный дневной счётчик различных сетей, кото хранится 48 часов.

Учётные данные подключения выдаются на каждое устройство (и ссылку подписки) и на сервер. Удаление устройства или обновление ссылки подписки удаляет его данные со всех серверов: новые подключения с него отклоняются примерно через 15 секунд, а уже открыт соединения завершаются, когда закрываются. Устройство, приостановленное из-за того, чт тариф разрешает меньше устройств, точно так же исключается, пока вы снова не сделаете активным. Если устройство потеряно, также смените пароль.

Доступ администраторов

Colitu обслуживает очень небольшая команда. Панель администратора находится на отдельном адресе и использует ролевые права доступа, административные эндпоинты закрыты в публичн API, аккаунты администраторов блокируются на 15 минут после 5 неудачных попыток, а действи администраторов записываются в журнал аудита. Двухэтапная проверка (TOTP) для аккаунтов администраторов обязательна: администратор без неё после входа может только настроить её, каждый следующий вход требует кода или одноразового кода восстановления (число попыток ограничено). Администратор также может зарегистрировать аппаратный ключ безопасности (WebAuthn); после этого вход требует пароля и ключа вместо TOTP, а одноразовый код восстановления остаётся записываемым в журнал аварийным способом. Утерянный ключ заменяется кодом восстановления или, после проверки личности по независимому каналу, записываемой в журнал командой сброса на сервере. Доступ отзывается отключением аккаунт прекращается со следующего запроса. Сеансы администраторов привязаны к браузеру и сети, которых они открыты.

9 Трафик, DNS, IPv6 и kill switch

Что видит VPN-сервер

VPN-сервер должен знать, куда отправлять ваш трафик, поэтому технически он видит ваш IP-ад IP-адреса и зачастую имена хостов (TLS SNI) сайтов, к которым вы подключаетесь, а также вре объём вашего трафика. Он не может прочитать содержимое HTTPS-соединений, которое остаёт зашифрованным между вашим устройством и сайтом. Colitu не расшифровывает и не анализир HTTPS-трафик.

Маршрутизация по умолчанию

	Android	Windows	iOS	Linux (бе
Как перехватывается трафик	Системный VPN (все приложения)	Режим TUN (весь трафик) для новых установок; установки, использовавшие системный прокси, его сохраняют	Системный VPN (все приложения)	По умолчан системн прокси; режим T по выбор
Не охватывается по умолчанию	Локальная сеть	В режиме системного прокси: приложения, игнорирующие системный прокси, DNS-резолвер Windows, UDP-трафик браузера (QUIC/WebRTC), IPv6. Режим TUN охватывает их.	Локальная сеть	Как на Windows режиме системн прокси

	Android	Windows	iOS	Linux (бе
Региональные сайты и IP-адреса (встроенный список)	В обход VPN, только если режим приватности выключен и сервер не в этом регионе	В обход VPN, только если режим приватности выключен и сервер не в этом регионе	В обход VPN, только если режим приватности выключен и сервер не в этом регионе	В обход V только е режим приватно выключе сервер н этом регионе
DNS	Через туннель на 1.1.1.1	TUN: через туннель на DNS-over-HTTPS Cloudflare. Режим прокси: только для трафика, который доходит до прокси.	Через туннель (8.8.8.8 → Xray → 1.1.1.1)	Как на Windows
IPv6	● Блокируется	● Блокируется в режиме TUN при включённом kill switch; в режиме системного прокси не охватывается	● Не утекает: направляется в туннель и отбрасывается там	● Как на Windows
Kill switch	● Использует настройки Android «Постоянная VPN» и «Блокировать подключения без VPN», которые пользователь должен включить сам	● Собственная служба Windows с постоянными правилами Windows Filtering Platform, включён по умолчанию (см. ниже)	● «Блокировать интернет без VPN» (iOS includeAllNetworks), по умолчанию выключено; пока включено, страницы входа в Wi-Fi не открываются. «Always-on» только переподключает	● Прави nftables, остающи при сбое приложе только режим T

Региональные сайты в обход VPN

Некоторые региональные сайты (домены и диапазоны IP-адресов из встроенного списка) открываются напрямую, в обход туннеля, чтобы продолжали работать сервисы, которые не принимают иностранные IP-адреса. При подключении к серверу в этом регионе это не примен
Для этого трафика сайт и ваш интернет-провайдер видят ваш реальный IP-адрес. Правило дейс
только при выключенном режиме приватности. В новых установках режим приватности включё
умолчанию (Windows и Android 2.7.0, iOS 5.6.0, Linux 1.3.0 и новее), поэтому по умолчанию весь
трафик идёт через VPN; установки, сделанные раньше, сохраняют прежнюю настройку. При пер
подключении с активным правилом приложение показывает одноразовое уведомление с
объяснением. Можно также выбрать сервер в этом регионе.

	Android	Windows	iOS	Linux (бет
Раздельное туннелирование	● Приложения, сайты и IP-адреса	● Приложения (только режим TUN), сайты и IP-адреса	● Только сайты и IP-адреса (iOS разрешает VPN для отдельных приложений только в управляемых профилях)	● Приложе (только режим T
Multihop и сменяющийся IP	● Только VLESS	● Только VLESS	● Только VLESS	● Только VLESS

Kill switch на Windows подробно

- Он блокирует весь трафик IPv4 и IPv6, кроме loopback, локальной сети (это настройка, по умолчанию включена), DHCP, VPN-ядер, адаптера TUN и самого приложения Colitu.
- Он активен в течение всей сессии, и в режиме TUN, и в режиме системного прокси. В режим прокси приложения, не использующие прокси, остаются без интернета, пока вы подключены
- Правила держит отдельная служба Windows (ColituKillSwitch, LocalSystem, автоматический запуск) в виде постоянных правил Windows Filtering Platform. Если приложение или VPN-ядр аварийно завершается либо служба перезапускается, правила остаются, и интернет блокиру пока Colitu не подключится заново (fail-closed).
- Обычная перезагрузка или выключение Windows снимает блокировку. Это сделано намерен некому было бы объяснить, почему нет интернета. Исключение — когда включены и автоподключение, и запуск вместе с Windows: тогда блокировка держится, пока Colitu не подключится заново. Если вы сами нажали «Отключить», блокировка снимается, а при удале приложения все правила удаляются.
- Если службы нет (например, после повреждённой установки), приложение предупреждает в переключается на прежний kill switch внутри приложения. Его фильтры принадлежат процес приложения: если приложение аварийно завершается или принудительно закрыто, Windows удаляет их, и трафик идёт без защиты (fail-open).
- Трафик, который приложение направляет напрямую, например региональные сайты из встроенного списка, намеренно не блокируется.

Трафик, который приложения отправляют в обход туннеля

- Проверка и загрузка обновлений (colitu.com).
- Измерение задержки до серверов.
- На Windows — разрешение имён хостов серверов через DNS-over-HTTPS Cloudflare или Goo

Проверки связи (например, адрес generate_204 от Google) отправляются через туннель.

10 Журналирование и перечень данных

Это полный перечень того, что хранит Colitu. Политика конфиденциальности содержит тот же перечень в юридической форме.

VPN-сервис

Данные	Хранятся?	Срок хранения и назначение
Содержимое вашего трафика	● Никогда	—
Сайты и IP-адреса, которые вы посещаете	● Не хранятся	Не записываются.
Ваши DNS-запросы	● Не хранятся	На резолверах Colitu Shield журналирование запросов и статистика отключены. По умолчанию приложения использ публичные резолверы (Cloudflare, Google), которые получа запросы с IP-адреса VPN-сервера, а не с вашего.
Ваш IP-адрес на VPN-серверах	● Не хранится	Используется в памяти только на время подключения.
Объём трафика по пользователям	● Хранится	Число байт на пользователя на сервере интервалами около секунд, хранится 90 дней для учёта квот и честного использования; после этого — только итоги за расчётный период. По этим данным видно, когда аккаунт был активен сколько трафика он использовал, но не куда этот трафик ш

Аккаунт и сайт

Passkey, веб-сессии и ссылки подписки включены в таблицу ниже. Для ссылок подписки IP-ад не хранятся: по каждой ссылке хранится только анонимный дневной счётчик различных сетей, часов.

Данные	Срок хранения	Назначение
Адрес электронной почты, хеш пароля (Argon2id), язык, даты аккаунта	До удаления аккаунта; при удалении адрес заменяется заглушкой, а пароль становится непригодным	Аккаунт и вход
Коды подтверждения e-mail и сброса пароля (адрес, хеш кода, IP-адрес)	7 дней	Подтверждение адреса, сброс паро
События входа (IP-адрес, страна, браузер или приложение)	180 дней	Безопасность аккау предотвращение злоупотреблений
IP-адрес и страна при регистрации и при последнем входе	Регистрация: 180 дней. Последний вход: стирается, если 180 дней не было входа	Безопасность аккау региональные прав
Регистрации и входы, отклонённые по региональным правилам (IP-адрес, страна)	90 дней	Применение региональных прав
Веб-сессии (IP-адрес, страна, браузер, способ входа)	Удаляются через 30 дней после окончания сессии (выход, истечение срока или отзыв)	Вход, список сесси странице аккаунта
Токены входа приложений (хранятся только в виде хешей, привязаны к устройству)	Удаляются через 30 дней после истечения срока или отзыва	Сохранение входа в приложениях
Двухэтапная проверка (зашифрованный секрет аутентификатора, хеши одноразовых кодов восстановления, 5-минутные шаги входа)	Секрет и коды восстановления — пока вы её не отключите или аккаунт не будет удалён; шаги входа удаляются через 1 день после истечения	Безопасность аккау

Данные	Срок хранения	Назначение
Passkey (открытый ключ, идентификатор учётных данных, указанное вами название, счётчик подписей, даты создания и последнего использования; закрытый ключ и биометрические данные никогда не покидают ваше устройство; одноразовые запросы проверки на 5 минут)	Пока вы не удалите passkey или аккаунт; запросы проверки удаляются сами через 5 минут	Вход без пароля и безопасность аккау
Учётные данные VPN-подключения (случайные секреты для каждого сервера, привязанные к устройству или ссылке подписки)	Пока устройство или ссылка используются; удаляются через 30 дней после удаления или замены	Доступ к VPN
Ссылки подписки (указанное вами название, даты создания, последнего использования и окончания, пометка «возможно, ссылкой делятся»; сама ссылка хранится только в виде хеша). IP-адреса, с которых используется ссылка, не сохраняются; на 48 часов остаётся лишь ежедневный анонимный приблизительный счётчик числа разных сетей на каждую ссылку	Пока вы не отзовёте ссылку или не удалите аккаунт (истёкшая ссылка отзывается автоматически); счётчик сетей удаляется сам через 48 часов	Отдельная ссылка д каждого устройства предупреждение об общей ссылке
Запросы входа с ТВ (имя устройства, IP-адрес, страна)	Удаляются через 1 день после истечения 10-минутного кода	Вход по QR-коду
Устройства (имя, платформа, версия приложения и ОС, последний IP-адрес и страна, ключевой хеш идентификатора оборудования)	Хранятся, пока устройство привязано к аккаунту. Имя, IP-адрес, страна и хеш оборудования удалённого устройства стираются через 30 дней; IP-адрес и страна устройства, не появлявшегося 180 дней, стираются	Ограничение числа устройств, безопасность аккау

Данные	Срок хранения	Назначение
Отклонённые попытки добавить устройство или получить пробный период (IP-адрес, данные устройства)	180 дней	Ограничение числа устройств, защита с злоупотреблений
Проверки злоупотреблений бесплатным тарифом и пробным периодом (ключевые хеши HMAC-SHA256 адреса электронной почты, идентификатора оборудования и сети; ключ не хранится в базе данных)	Сеть: 30 дней. Адрес и идентификатор оборудования: пока существует аккаунт и 180 дней после его удаления. Хеши SHA-256 без ключа, записанные до этого изменения, удаляются не позднее чем через 180 дней после записи	Предотвращение повторного создани бесплатных аккаунт
Автоматическая проверка на ботов и злоупотребления: для задержанных или заблокированных аккаунтов — оценка, сработавшие признаки, IP-адрес, страна, сеть (ASN) и user agent; для регистраций, отклонённых до создания аккаунта, также адрес электронной почты	Задержанные или заблокированные аккаунты: пока существует аккаунт, удаляются вместе с ним. Отклонённые регистрации: 30 дней	Защита от ботов, автоматической регистрации и сбор адресов серверов
Проверки злоупотреблений пробными промокодами (ключевые хеши HMAC-SHA256 нормализованного адреса электронной почты, идентификатора оборудования устройства и сети — IPv4 /32 и /24 или IPv6 /64 и /48; ключ не хранится в базе данных)	Сеть: 35 дней. Адрес и идентификатор оборудования: 365 дней, в том числе после удаления аккаунта	Один пробный промокод на челов
Заявки на перенос из прежнего сервиса (Telegram ID и имя, заметки, IP-адрес)	Удаляются через 30 дней после последнего изменения. От одобренной заявки остаётся только ключевой хеш Telegram ID на 2 года	Перенос старых подписок; защита о повторного перено одной подписки

Данные	Срок хранения	Назначение
Метка источника регистрации (например, «github», «app:android») из utm/ref-метки ссылки на сайт, имени сайта, с которого вы пришли (например, github.com), или из приложения; cookie, пиксели и адреса не сохраняются. Время первого VPN-подключения.	Удаляется вместе с аккаунтом	Сводная оценка тог какие каналы приво реальных пользователей и сколько длится пер подключение
Ваш код приглашения; связь между аккаунтом, созданным по ссылке-приглашению, и аккаунтом пригласившего, статус приглашения (ожидает, засчитано, недействительно и причина) и начисленные дни Premium. Пригласившему не показываются имя и e-mail приглашённого.	Удаляется при удалении любого из двух аккаунтов	Начисление наград приглашения; защит злоупотреблений (т же IP-адрес или устройство, времен e-mail); сводный уч регистраций по приглашениям
Анонимная статистика приложений: результаты подключений и тип ошибки, время подключения и восстановления (в виде счётчиков по диапазонам), неожиданные разрывы, переключения протоколов Adaptive Connect, измеренная задержка до серверов и выбор сервера в автоматическом режиме, используемые функции и состояние kill switch; тип сети, страна и номер интернет-провайдера (ASN) текущей сети (из подписанной метки, полученной при выключенном VPN). На сервере хранятся только суммы за день, причём сети (страна + ASN) и серверы — в отдельных таблицах; аккаунт, устройство, IP-адрес и посещённые сайты не сохраняются. Отключается в настройках приложения.	Суммы хранятся бессрочно (без связи с человеком)	Оценка и улучшени качества подключе работы Adaptive Connect и использования фун

Данные	Срок хранения	Назначение
Colitu Passport сохраняется в вашем аккаунте и следует за вами на каждое устройство, где вы входите. По каждой стране марки: время открытия и число частей; достижения, коллекции, прогресс еженедельных экспедиций, псевдоним, звание, обложка, смещение часового пояса и номер коллекционера; итоги по дням (минуты использования, части, ночные и ранние минуты, список стран, использованных в этот день); текущая серия (страна, её длина и последняя засчитанная минута); события наград для анимаций в приложениях. Минуты считают наши серверы по времени подключения: минута засчитывается, если один из наших серверов сообщил о трафике вашего аккаунта в эту минуту (каждая минута не более одного раза, сколько бы ни было устройств), а страна — это страна сервера; приложения не могут добавлять минуты. Хранятся только итоги по дням и странам; журнала по минутам или сессиям, сайтов и IP-адресов нет. Прогресс, уже имевшийся на устройстве в старой версии, импортируется один раз для каждого устройства (в правдоподобных пределах, берётся большее значение).	Итоги по дням — 400 дней, события наград — 30 дней, остальное — до удаления аккаунта	Сохранение паспор аккаунте, показ на каждом устройстве расчёт наград и еженедельных экспедиций

Данные	Срок хранения	Назначение
Необязательные анонимные счётчики Colitu Passport, не больше одного отчёта в день: число открытых марок, самая высокая открытая глава, число марок по уровням, завершённые еженедельные экспедиции, части, полученные за день, и открывался ли паспорт в этот день. Отправляются без аутентификации; сервер лишь добавляет каждый отчёт к суммам за день и не хранит ни строки отчёта, ни аккаунта, ни устройства, ни IP-адреса. Из каких стран и когда получены марки, не передаётся. Отправляют только старые версии приложений; новые не отправляют, так как паспорт теперь хранится в аккаунте (см. строку «Colitu Passport»). Настройка по умолчанию выключена и отключается в приложении.	Суммы хранятся бессрочно (без связи с человеком)	Сводная оценка тог насколько используется паспо сбалансированы ли правила (темп уров и частей)
Ваши ответы на опросы в приложении: оценка рекомендации (0–10), что вы почувствуете без Colitu, причина отказа от продления Premium, необязательный комментарий и платформа; закрытые опросы (не чаще одного опроса в 30 дней)	При удалении аккаунта связь с ним и комментарий удаляются; остаётся только анонимная оценка	Сводная оценка удовлетворённости (NPS), соответствия продукта рынку и причин ухода
Оценка 1–5 и необязательный комментарий к решённому обращению; время первого ответа и решения	Удаляется вместе с обращением	Сводная оценка качества поддержк (удовлетворённост время ответа и решения)
Какие транспорты сработали для устройства, на каком сервере и с какой скоростью (без IP-адреса)	Перезаписывается при каждом отчёте; удаляется через 35 дней после последнего отчёта	Выбор работающих транспортов в перв очередь

Данные	Срок хранения	Назначение
Тариф, платежи и заказы (сумма, тип способа оплаты, идентификатор транзакции у провайдера, уведомление провайдера; для оплат через Rialit — постоянный номер плательщика, привязанный к аккаунту)	Столько, сколько требует бухгалтерское и налоговое законодательство, в том числе после удаления аккаунта; автоматического удаления по окончании этого срока пока нет	Биллинг, возвраты, требования закона
Корпоративный аккаунт Colitu Business: название компании, адрес для счетов, страна, налоговый номер, число мест и срок их действия; членство (роль, даты приглашения, вступления и выхода, кто добавил участника); счета компании и журнал действий компании. Владелец и администраторы компании видят адрес электронной почты и роль каждого участника, а также название, платформу, версию приложения и время последней активности его устройств; трафик и посещённые сайты им не видны	Пока Colitu не закроет корпоративный аккаунт; счета компании — столько, сколько требует бухгалтерское и налоговое законодательство; ссылки для создания пароля действуют 7 дней. Если участник удаляет свой аккаунт, его членство закрывается, а место возвращается компании	Управление местам компании, выставле счетов компании, напоминания о продлении
Компании и авторы контента, которым мы отправляем предложения о партнёрстве Colitu Business: название компании или канала, адрес электронной почты, опубликованный ими для деловых контактов на сайте или в описании канала, страна и язык; отправленные письма и их даты; тема и первые 300 символов ответов, недоставленные письма	Записи об отправке и ответах в панели удаляются через 12 месяцев. Список контактов хранится, пока контакт не попросит больше не писать или адрес не перестанет быть нужен; на адрес, ответивший «не пишите	Предложение партнёрства Colitu Business: расселлин white label (законны интерес; в каждом письме указано, ка отказаться, и ссылк эту политику)

Автоматическая задача ежечасно применяет эти сроки, а удаление аккаунта сразу стирает что перечислено в политике конфиденциальности. Оставшиеся пробелы: для записей о тарифах, платежах и заказах и для журнала аудита автоматического удаления пока нет, а зашифрованные резервные копии, сделанные до удаления, хранят данные не более 36 дней незашифрованные снимки, сделанные перед развёртыванием, — не более 7 дней. Хеши проверок злоупотреблений вычисляются с серверным ключом; хеши SHA-256 без ключа, записанные до этого изменения, сопоставимы, пока не будут удалены, — не позднее чем че

180 дней после записи.		
Сообщения о безопасности: текст сообщения об уязвимости (заголовок, описание, шаги, влияние) и переписка с командой; если вы хотите быть упомянуты в Зале славы, выбранное вами имя (публикуется открыто вместе с месяцем и уровнем серьёзности)	До удаления аккаунта; при удалении удаляются сообщения, переписка и запись в Зале славы	Исправление уязвимостей и выпл вознаграждений (п желанию: упоминан Зале славы)
Отчёт о подключении: когда поддержка разбирается с проблемой подключения, приложение при следующем запуске отправляет данные о приложении и устройстве, события подключения и журналы приложения; названия сайтов и адреса маскируются на устройстве и на сервере, посещённые сайты не отправляются	Удаляется через 90 дней	Устранение пробле подключением (поддержка)
Переписка с Colitu Bot (текст, IP-адрес, отзыв «помог ли ответ»)	180 дней	Ответы на вопросы
Записи о доставке электронной почты (адрес получателя, тип письма)	90 дней	Решение проблем с доставкой
Подписка на рассылку (адрес электронной почты, язык, время подтверждения); только если вы подтвердили её по ссылке из письма	До отписки; неподтверждённые заявки удаляются через 7 дней	Письма с анонсами заметками о выпус и предложениями (вашего согласия)
Журналы доступа к сайту и API (IP-адрес, запрошенный адрес, браузер)	14 дней	Эксплуатация и защ Сервиса
Тест на утечку DNS на нашем сайте	10 минут, только в памяти	Отображение результата теста
Журнал аудита (действия администраторов и некоторые действия с аккаунтом, например его удаление, по ID аккаунта)	Бессрочно; необязательная причина, указанная при удалении аккаунта: 180 дней	Подотчётность действий

11 Телеметрия и третьи стороны

Телеметрия в приложениях

- Ни одно приложение Colitu (Android, iOS, Windows, Linux) не содержит библиотек аналитики, рекламы или отчётов о сбоях; в приложении для iOS их нет начиная с версии 5.4.1.
- Все приложения сообщают Colitu, какие транспорты сработали на каком сервере и с какой скоростью, с привязкой к устройству, чтобы работающие транспорты выбирались в первую очередь.
- К обращениям в поддержку прикладываются последние журналы приложения, в которых адр секреты замаскированы.

Третьи стороны, получающие данные

Сторона	Что получает
Платёжный провайдер (только для клиентов, купивших платный тариф)	Номер заказа, сумму, валюту, описание тарифа и способ оплат данные карты или банковские реквизиты вводятся на странице провайдера. Colitu не передаёт ваш адрес электронной почты и IP-адрес.
Resend (электронная почта)	Ваш адрес электронной почты и содержимое писем, связанных аккаунтом (коды, квитанции).
Brevo (почтовый ретранслятор)	Ответы, отправленные из нашего ящика поддержки.
DeepSeek (Colitu Bot)	Вопрос и несколько последних сообщений переписки с ботом. Данные аккаунта не передаются, но всё, что вы вводите, передаётся.
Have I Been Pwned (Pwned Passwords)	При регистрации и смене пароля: первые 5 символов SHA-1-хе пароля для сверки с известными утечками. Сам пароль, полный хеш, e-mail и IP-адрес не передаются.
Cloudflare	Обслуживает DNS-записи и проксирует docs.colitu.com и map.colitu.com. Также предоставляет DNS-резолверы, используемые в приложениях по умолчанию, и точку выхода дл нескольких доменов на двух серверах (§17).
Backblaze B2 (EU Central, Амстердам)	Зашифрованные копии ежедневной резервной копии. Прочитат Backblaze не может: ключ расшифровки хранится офлайн.

Сторона	Что получает
Хостинг-провайдеры	Обслуживают серверы и имеют к ним технический доступ.

Сайт не загружает сторонние скрипты, шрифты или трекеры.

12 Безопасность приложений

	Android	Windows	iOS	Linux (бета)
Токены сессии	AES-256-GCM с ключом Android Keystore (программный ключ, если Keystore не работает)	DPAPI (текущий пользователь)	Keychain (доступен после первой разблокировки)	AES-GCM с ключом, производны данных компьютера пользовател
Учётные данные подключения	Зашифрованы (AES-GCM)	В открытом виде в базе данных, доступной для чтения только администраторам и SYSTEM	Файл в открытом виде в закрытом контейнере приложения	Защищённы файлы (0600
Закрепление сертификатов для API	● Да	● Да (с 10 октября 2026 г.)	● Да (с 10 октября 2026 г.)	● Да (с 10 октября 202
Привилегии	Обычное приложение с разрешением на VPN	Всегда запускается от имени администратора; правила kill switch держит отдельная фоновая служба (ColituKillSwitch, LocalSystem)	Network extension	Запрашивае sudo; парол хранится в памяти

	Android	Windows	iOS	Linux (бета)
Локальные журналы VPN	Только предупреждения; журнала доступа нет	Только предупреждения; адреса замаскированы; удаляются через 7 дней	Только предупреждения; журнала доступа нет	Только предупрежд

Закрепление означает, что корневой сертификат, установленный на устройстве кем-то посторонним, нельзя использовать для чтения трафика приложений к API. Поэтому защитн ПО, проверяющее HTTPS с подстановкой собственного корневого сертификата, блокирует соединение приложений с API; в таком ПО добавьте Colitu в исключения.

13 Обновления и цепочка поставок

Платформа	Как проверяется обновление
Android (версия для загрузки с сайта)	Манифест подписан ECDSA P-256 и проверяется по ключу, встроенному приложение. APK должен быть получен по HTTPS с colitu.com, совпадать SHA-256 из манифеста и быть подписан тем же сертификатом, что и установленное приложение. Более старые версии отклоняются.
Android (Google Play)	Обновляется через Google Play.
Windows	Тот же подписанный манифест, загрузка по HTTPS с colitu.com, проверка SHA-256, повторная проверка на этапе установки с повышенными права Установщик пока не подписан Authenticode, поэтому Windows SmartScre может выдавать предупреждение.
Linux	Подписанный манифест и SHA-256 пакета.
iOS	Распространяется через Apple TestFlight; Apple подписывает и доставляе обновления.

Сборка и исходный код

- Каждый выпуск приложений с открытым исходным кодом помечается тегом на GitHub. На странице выпуска указаны контрольные суммы SHA-256 и спецификация компонентов ПО в формате SPDX (Android и Windows).
- В репозиториях Android и Windows работают сканирование кода CodeQL и обновление зависимостей Dependabot; GitHub Actions закреплены по хешам коммитов.
- Выпуск для Android собирается в CI; установщик для Windows собирается на компьютере разработчика; пакеты для Linux собираются в CI; сборки для iOS в TestFlight собираются в Codemagic.
- Сборки Android (начиная с 2.9.3) и Windows (начиная с 2.9.8) воспроизводимы, поэтому любо может заново собрать исходный код с соответствующим тегом и сравнить результат с опубликованным файлом. На iOS и Linux контрольная сумма по-прежнему доказывает лишь т у вас тот файл, который мы опубликовали, но не то, что он собран из исходного кода с соответствующим тегом. Библиотека ядра Xray для Android — это официальный бинарный фа основного репозитория (upstream), закреплённый по SHA-256, а не пересобираемый из исхо кода.

Что открыто, а что закрыто

Компонент	Исходный код
Приложение для Android	Открыт (GPL-3.0)
Приложение для Windows	Открыт (GPL-3.0)
Приложение для Linux	Открыт (GPL-3.0)
Приложение для iOS	Открыт (GPL-3.0)
Управляющий контур и агент узла	Закрыт
Сайт	Закрыт

14 Устойчивость к цензуре

Ни один транспорт не может гарантированно работать против любой системы цензуры. Подход — предлагать несколько транспортов с разными свойствами и позволять приложению автомати переключаться на резервный.

Метод блокировки	Ответ Colitu
Блокировка IP-адресов серверов	Несколько серверов в разных сетях, а также ретранслятор (§17 Заблокированный IP остаётся заблокированным, пока сервер н сменится.
Блокировка портов или UDP	TCP-транспорты (Reality, XHTTP, Trojan), когда заблокирован U Hysteria2, когда нарушена работа TCP.
Подмена DNS	Приложения получают адреса серверов от API и при необходимости разрешают их через зашифрованный DNS.
Анализ отпечатков TLS и активное зондирование	Reality отвечает на зондирующие запросы как настоящий сайт, который он имитирует.
Анализ отпечатков протоколов (DPI)	Reality и XHTTP похожи на обычный HTTPS; Hysteria2 похож на QUIC.
Замедление и сброс соединений	Автоматическое переключение на другой транспорт; XHTTP дл сетей, обрывающих долгие соединения.

15 Ограничения приватности

VPN скрывает ваш трафик от сети, в которой вы находитесь. Скрыть всё он не может:

- Размеры пакетов, время и общий объём трафика остаются видимыми, и наблюдатель, видящ конца, может их сопоставить.
- Сайты по-прежнему могут идентифицировать вас по cookie, отпечатку браузера и аккаунтам которые вы вошли.
- VPN не защищает от вредоносного ПО, фишинга или скомпрометированного браузера.
- Трафик, направляемый в обход туннеля (§9), не защищён.

16 Реагирование на инциденты и журнал инцидентов

Если мы подозреваем компрометацию VPN-сервера, мы скрываем его из приложений, заменяе ключи и учётные данные подключения и пересобираем его. Если утечка затрагивает персональ данные, мы без неоправданных задержек сообщаем об этом затронутым пользователям по электронной почте и публикуем описание произошедшего в этом разделе и в Центре доверия. Состояние сервиса публикуется на status.colitu.com.

17 Инфраструктура

- Все серверы — арендованные виртуальные машины у нескольких независимых хостинг-провайдеров. VPN-серверы распределены по ряду стран; актуальный список — на странице серверов. Управляющий контур, в котором находится база данных аккаунтов, работает на се в Турции.
- Диски не зашифрованы. Хостинг-провайдеры имеют технический доступ к своим машинам.
- Административный доступ осуществляется только по SSH с ключами; вход по паролю отклю Ключи есть только у команды Colitu.
- Автоматические обновления безопасности включены на большинстве серверов; их включен везде включено в план работ.
- Управляющий контур и часть VPN-серверов используют межсетевой экран с запретом по умолчанию. На остальных VPN-серверах входящие подключения принимают только VPN-сер SSH и эндпоинт измерений; межсетевой экран с запретом по умолчанию на всех серверах включён в план работ.
- База данных управляющего контура недоступна из интернета. У VPN-серверов нет к ней дост
- Два сервера направляют небольшой фиксированный набор доменов (сервисы Google на одн ИИ-сервисы Google на другом) через Cloudflare WARP, чтобы эти сервисы видели европейск местоположение. Для этих доменов точкой выхода является Cloudflare, и он видит те же метаданные, что видел бы VPN-сервер.
- Один входной сервер-ретранслятор пересылает зашифрованные пакеты без изменений на выходной сервер в Латвии. Входной сервер не может расшифровать трафик; он видит ваш IP адрес, как и любая сеть.

18 Сообщение об уязвимостях

Сообщайте о проблемах безопасности конфиденциально на security@colitu.com (адрес также у в /.well-known/security.txt). Пожалуйста, приложите шаги для воспроизведения и затронутую в Полная политика — на colitu.com/responsible-disclosure.

- Мы подтверждаем получение сообщений в течение 3 рабочих дней и даём первичную оценк течение 10 рабочих дней.
- Пожалуйста, дайте нам разумное время на исправление проблемы, прежде чем публиковать подробности.
- Мы не будем предпринимать юридических действий в отношении добросовестных исследов которые не затрагивают данные других пользователей, не нарушают работу сервиса и о результатах которых сообщено конфиденциально.
- Мы указываем имена исследователей, которые этого хотят. В рамках программы вознагражд (colitu.com/bug-bounty) подтверждённые сообщения, отправленные из аккаунта, вознаграждаются подпиской Plus на срок от 1 до 12 месяцев в зависимости от серьёзности, а критические уязвимости — денежным вознаграждением.

- В рамках программы: приложения, colitu.com и его поддомены, API и VPN-серверы. Вне рам программы: отказ в обслуживании, спам, социальная инженерия и третьи стороны из §11.

19 Статус аудита

Colitu пока не проходил независимый аудит безопасности или тест на проникновение третьей стороной. В настоящее время гарантии обеспечиваются следующим:

- открытый исходный код приложений для Android, Windows, Linux и iOS;
- автоматическое сканирование кода (CodeQL) и обновление зависимостей (Dependabot);
- внутренние проверки безопасности приложений (октябрь 2026 г.) и проверка, лежащая в осн этого документа;
- публичный процесс сообщения об уязвимостях.

Независимый аудит запланирован, но сроки пока не назначены.

20 Известные ограничения

- Независимого аудита безопасности пока не было.
- VPN-серверы и их хостинг-провайдеры входят в число тех, кому вы должны доверять; диски серверов не зашифрованы.
- Если режим приватности выключить, некоторые региональные сайты из встроенного списка обход VPN в приложениях для Windows, Android, iOS и Linux. В новых установках режим приватности включён по умолчанию начиная с Windows и Android 2.7.0, iOS 5.6.0 и Linux 1.3.0 установки, сделанные раньше, сохраняют прежнюю настройку.
- Новые установки Windows начинают с режима TUN, но установки, использовавшие системны прокси, его сохраняют, а режим прокси охватывает не все приложения, не охватывает систем DNS-резолвер и IPv6. Обычная перезагрузка Windows снимает блокировку kill switch, если C не настроен на повторное подключение при входе в систему.
- На Android нет собственного kill switch, и нужны две системные настройки, по умолчанию выключенные; переключатель iOS «Блокировать интернет без VPN» по умолчанию выключен пока он включён, страницы входа в Wi-Fi не открываются.
- Двухэтапная проверка обязательна для аккаунтов администраторов и только необязательна пользователей.
- Для записей биллинга и журнала аудита пока нет автоматического удаления (§10).
- Защитное ПО, проверяющее HTTPS с собственным корневым сертификатом, из-за закреплен сертификатов блокирует соединение приложений с API; в нём нужно добавить Colitu в исключения. Passkey работают только на colitu.com: не на зеркальных доменах и не внутри приложений.

- Приложение для Windows не подписано Authenticode, а сборки для iOS и Linux пока не воспроизводимы.
- У Shadowsocks 2022 нет прямой секретности; Trojan принимает TLS 1.2.

21 Изменения в версиях с 1.4 по 1.9

Версия 1.3 описывала приложения такими, какими они были до последних релизов приложений версия описывает то, что работает сегодня.

- Двухэтапная проверка (TOTP) доступна для любого пользовательского аккаунта, а не только администраторов. Приложения запрашивают код при входе.
- Windows: kill switch теперь отдельная служба Windows с постоянными правилами брандмауэ Она продолжает блокировку, если приложение или VPN-ядро аварийно завершается (больше fail-open). Обычная перезагрузка Windows по-прежнему снимает блокировку, если Colitu не настроен на повторное подключение при входе в систему. Новые установки начинают с режи TUN.
- Раздельное туннелирование есть во всех четырёх приложениях: приложения, сайты и IP-адр Windows, Android и Linux; сайты и IP-адреса на iOS.
- iOS: IPv6 больше не утекает, а необязательный переключатель «Блокировать интернет без VP (по умолчанию выключен) блокирует трафик вне туннеля.
- Режим приватности (в новых установках включён по умолчанию) позволяет пользователям приложений для Windows, Android, iOS и Linux решать, действует ли встроенное правило, по которому некоторые региональные сайты идут в обход VPN.
- Multihop (двойной VPN) и сменяющийся IP доступны на серверах VLESS.
- Блокировщик рекламы стал Colitu Shield — необязательной защитой на уровне DNS с пятью категориями (реклама и трекеры, вредоносное ПО, фишинг, мошенничество, криптомайнинг) октября 2026 г. На его резолверах нет журнала запросов и статистики, новые данные не собираются. Необязательный фильтр контента для взрослых, личные списки, счётчик на устройстве и переключатели по категориям — в плане развития, пока не работают.
- Версии, даты и контрольные суммы в этом документе, на страницах загрузки и на странице открытого исходного кода теперь берутся из одного манифеста релизов.
- Версия 1.5 (9 октября 2026 г.): платные тарифы («Личный», Plus и «Семейный») в продаже; оп проходит на странице платёжного провайдера, данные карты в Colitu не попадают. Утвержде том, что платные тарифы не продаются, удалено. Другие описанные в документе практики не менялись.
- Версия 1.6 (10 октября 2026 г.): passkey для сайта, список сеансов с управлением ими, письм безопасности, 24-часовая блокировка удаления аккаунта и отключения двухэтапной проверк после сброса пароля, ограничение числа попыток повторной проверки пароля, дополнительн именованные ссылки подписки со сроком действия, необязательные аппаратные ключи безопасности для аккаунтов администраторов и закрепление соединения с API за корневым

центрами сертификации Let's Encrypt (ISRG) и Google Trust Services во всех четырёх прилож
Другие описанные в документе практики не менялись.

- Версия 1.7 (16 октября 2026 г.): резервные копии. Ключ расшифровки перенесён в офлайн и б
не хранится на сервере. Ежедневная зашифрованная копия хранится вне сервера в Backblaz
(EU Central) с 30-дневной защитой от удаления и удаляется не позднее чем через 36 дней.
Незашифрованные снимки, сделанные перед развёртыванием, удаляются через 7 дней. Back
добавлен в список третьих сторон. Другие описанные в документе практики не менялись.
- Версия 1.8 (20 октября 2026 г.): воспроизводимые сборки для Android (начиная с 2.9.3) и Win
(начиная с 2.9.8). Другие описанные в документе практики не менялись.
- Версия 1.9 (28 октября 2026 г.): добавлено описание программы вознаграждений (Plus на сро
до 12 месяцев, денежное вознаграждение за критические уязвимости), удалено утверждение
отсутствии денежных вознаграждений. Отчёт о внутренней оценке безопасности опубликова
colitu.com/security-assessment. Другие описанные в документе практики не менялись.

22 План работ по безопасности

Ближайшее (IV квартал 2026 г.)

- Автоматическое удаление записей биллинга по окончании установленного законом срока хранения.
- Более короткий срок хранения журналов доступа к сайту и запись без полных IP-адресов.
- Межсетевой экран с запретом по умолчанию и автоматические обновления безопасности на серверах.
- Обязательный TLS 1.3 для Trojan.

Позже

- Подпись Authenticode для Windows.
- Воспроизводимые сборки для iOS и Linux и SBOM для всех платформ.
- Внешний тест на проникновение и независимый аудит.
- PGP-ключ для сообщений о безопасности и ежеквартальные отчёты о прозрачности.

23 Юрисдикция

Colitu управляет компания COLITU LIMITED, зарегистрированная в Англии и Уэльсе (юридичес
адрес: 128 City Road, London, Великобритания, EC1V 2NX; регистрационный номер компании
17520342); она подчиняется праву Англии и Уэльса. База данных аккаунтов находится на сервер
Турции; VPN-серверы расположены в странах, указанных на странице серверов, и подчиняются
местному законодательству по месту нахождения. Мы можем передать только те данные, котор
нас есть; все они перечислены в §10. Полученные запросы учитываются в отчётах о прозрачнос
Центре доверия.

24 Ссылки

- **Протокол** Hysteria 2: v2.hysteria.network
- Xray-core **и** REALITY: github.com/XTLS
- sing-box: sing-box.sagernet.org
- TLS 1.3: RFC 8446 · QUIC: RFC 9000 · security.txt: RFC 9116
- Argon2: RFC 9106
- OWASP ASVS **и** MASVS
- **Документация** Android VpnService, Apple Network Extension **и** Windows Filtering Platform

Colitu: **технический документ по безопасности** · **Версия** 1.9 · 28 **октября** 2026 **г.** · security@colitu.com · colitu.com/security