ЛАБОРАТОРИЯ ШАХУЛОВА / IT - Агенство

НАУЧНО-ТЕХНИЧЕСКОЕ ИССЛЕДОВАНИЕ / АНАЛИТИЧЕСКИЙ ПРЕПРИНТ

OLCBOX / olcRTC

WebRTC при разрешительной фильтрации: архитектура, риски нецелевой ретрансляции, авторизация и устойчивость видеоплатформ

Основания: стандарты IETF, документация Яндекса и LiveKit, GitHub-артефакты Olcbox, olcRTC, Ghostlane и snolc.

Научный статус: доказательная документальная ревизия. Лабораторные эксперименты и независимое внешнее рецензирование отсутствуют.

RESEARCH DOSSIER / REVISION 5.2 / 19.10.2026

01 / ПАСПОРТ ИССЛЕДОВАНИЯ

Аннотация и научный паспорт

Работа исследует многоуровневую архитектуру WebRTC-систем, заявленное использование легитимных видеосервисов в качестве транспортной среды сторонними клиентами, эволюцию проектов Olcbox / olcRTC и ограничения их эксплуатации в условиях разрешительной фильтрации мобильного доступа. Особое внимание уделено разграничению учётных данных, идентичности участника, разрешений конкретной комнаты, жизненному циклу JWT, медиапотокам и ретрансляции TURN.

Использована документально-аналитическая методика с проверкой официальных API, RFC и первичных GitHub-артефактов; выполнены три раунда внутренней критической ревизии. Исследование **не** включает непосредственных измерений мобильных операторов, изучения секретной конфигурации провайдеров, испытаний сторонних видеоплатформ без разрешения и внешнего независимого академического рецензирования.

ГЛАВНЫЙ РЕЗУЛЬТАТ

Идентификация пользователя, право создания комнаты, вход в неё, разрешение публикации данных и возможность продолжить активную медиасессию - разные контрольные точки. Ни одна из них по отдельности не доказывает ни полной защиты видеоплатформы, ни доступности конкретного транспортного режима в сетях с ограничениями.

Атрибут	Значение
Организация	Лаборатория Шахулова (Shahulov Lab)
Предмет	OLCBOX, olcRTC, WebRTC, Telemost, WB Stream, токены и белые списки
Тип	Научно-технический кабинетный препринт; не эмпирическое испытание
Редакция / дата	5.0 / 19.10.2026
Основа	Первоисточники + классификация уверенности + внутренняя критика
Публичность	Рабочая версия для независимой рецензии и обсуждения

Ключевые слова: WebRTC; ICE; STUN; TURN; SFU; SRTP; SCTP/DTLS; JWT; LiveKit; авторизация; room grants; токен; разрешительная фильтрация; сетевой сбой; воспроизводимость.

Структура доклада

- Исследовательские вопросы и методология
- Хронология событий и состояния проектов
- WebRTC: control plane, media plane и доверительные границы
- Идентификация, роли, JWT, реконнект и отзыв

- Политики Telemost и WB Stream; границы имеющихся свидетельств
- Модель угроз и инженерные контрмеры
- Результаты критической коллегии и лабораторный протокол
- 30 проверочных тезисов, выводы и библиография

1. Постановка задачи и гипотезы

Объект - системы коммуникаций реального времени, действующие в сетях с неодинаковыми условиями доступности. **Предмет** - юридически и технически различимые способы допуска и контроля коммуникационных каналов при нецелевом использовании. **Цель** - отделить подтверждённые архитектурные свойства от сообщений авторов проектов, сформулировать опровержимые гипотезы и определить меры уменьшения риска без ухудшения законной видеосвязи.

- **RQ1.** Какие транспортные режимы документированы в WebRTC и какие режимы заявил каждый исследуемый клиент?
- **RQ2.** В какой точке применяется доступ к аккаунту, право создания комнаты, авторизация гостя, право публикации и запрет реконнекта?
- **RQ3.** Как отличить изменение политики платформы от ошибки клиента, отказа провайдера, сетевой фильтрации и инфраструктурного сбоя?
- **RQ4.** В какой мере короткий TTL токена, revocation, MFA и серверный контроль публикаций защищают от подтверждённых сценариев злоупотребления?
- **RQ5.** Какие наблюдения можно получить из GitHub, а какие требуют специально разрешённого эксперимента?

Проверяемые гипотезы

Код	Положение	Статус
H1	Авторизация владельца комнаты ограничивает её создание, но сама не запрещает гостевой вход.	Логическая модель / нужна реализация
H2	Запрет DataChannel не тождественен запрету медиатреков.	Поддержано архитектурой и матрицей автора
H3	Истечение первоначального JWT не обязано останавливать уже открытый медиаканал.	Подтверждено для LiveKit; другие системы отдельно
H4	Совпадение по времени с отказом ЦОД не доказывает причину сбоя клиента.	Методологический принцип
H5	Проверка личности без авторизации действий недостаточна для исключения злоупотреблений.	Вывод угроз; эффект не измерен

2. Методология и качество доказательств

Для каждого утверждения задана минимальная единица проверяемости: **кто** заявил, **что именно** утверждается, **к какому ПО, версии и времени** применимо, **каким наблюдением** можно опровергнуть. Наличие опубликованного исходного кода доказывает факт присутствия соответствующей логики в данном состоянии репозитория, но не наличие настроек или эффективность контроля на серверах другой компании.

Класс	Источник	Что подтверждает
A	IETF RFC, документация производителя, официальный API	Нормативный протокол / публично задокументированное поведение заявленного продукта
B	GitHub release, merged PR, upstream README, отчёт CI	Код и утверждения разработчика об ограниченном стенде
C	GitHub issue / комментарии / независимые сообщения	Наблюдение и гипотеза автора публикации
D	Аналитическое предположение	Возможное объяснение, которое ещё требуется проверить

Для вывода о реальной доступности в мобильной сети необходимы параметры оператора, региона, даты, доступа к сигнализации, версии клиента и сервера, типа соединения, роли пользователя и размера статистической выборки. В доступных материалах таких полных наборов нет. Нельзя использовать количество совпадающих перепечаток как меру независимой подтверждённости.

Отдельный контроль: состояние репозитория, статус релиза и работоспособность конкретного сервиса на практике фиксируются как **разные переменные**. Методологическое правило не допускает переноса числа из CI release-gate непосредственно на всю генеральную совокупность российских мобильных операторов.

> **НАУЧНАЯ ГРАНИЦА**
>
> В этом документе есть технические утверждения с высокой документальной достоверностью и несколько сильных рабочих гипотез, но нет экспериментально измеренной эффективности против всех механизмов разрешительной фильтрации. Честная граница вывода - часть научной добросовестности, а не дефект исследования.

2.1. Протокол внутренней проверки источников

Проверка велась итерациями: выделение исходных утверждений, сопоставление с документом-источником, поиск несовместимых трактовок, письменное замечание, редакционная поправка и повторный контроль после внесения изменений. Для спорных фактов использованы комментарии к GitHub Issues и статус merged PR, поскольку содержание основного issue не всегда совпадает с последующими выводами сопровождающих проект. Даты публикации документа и даты самих событий в каждом случае разведены.

Важно различать **корректность источника** и **область его применимости**. Даже точный RFC не подтверждает конфигурацию коммерческого сервера. Даже настоящий merged PR не устанавливает успешное прохождение end-to-end тестов после его внедрения. Даже официальный API видеосервиса подтверждает доступность бизнес-операции при заданных правах, а не сетевую доступность через любого оператора и любую инфраструктуру.

Качество публикации также проверяется отдельно от качества научного вывода: PDF может быть визуально безупречен, но это не превращает гипотезу в измеренный факт. Поэтому итоговый вердикт разделён на издательскую готовность и экспериментальную завершённость, чтобы будущие рецензенты могли ясно отделить доказательства от планов.

3. Объекты исследования и история версий

Объект	Публичная функция	Статус, установленный по источнику
olcRTC	Движок туннелирования поверх конференций; отдельные DataChannel/видеотранспорты	Upstream архивирован 05.10.2026 [S1]
Olcbox	Kotlin Multiplatform UI и конфигуратор olcRTC	Alpha; репозиторий архивирован 05.10.2026 [S2]
Ghostlane	Самостоятельный клиент и поддерживаемый fork движка	Релиз 1.0.466 от 14.10.2026; тестовые gate [S3]
snolc	Новый модульный userspace network engine (Rust)	Иная архитектура: policy/protection/carrier [S4]

Нельзя переносить устаревший статус одного upstream-проекта на отдельные форки. Архивация olcRTC и Olcbox 05.10.2026 подтверждена на публичных страницах GitHub. Ghostlane продолжал выпускать релизы, а snolc позиционировался как самостоятельная модульная разработка. Это опровергает формулировку «все решения прекратили существование», но не доказывает работоспособность какой-либо сборки в конкретной ограниченной сети. [S1-S4]

РИС. 1 / ВРЕМЕННАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ

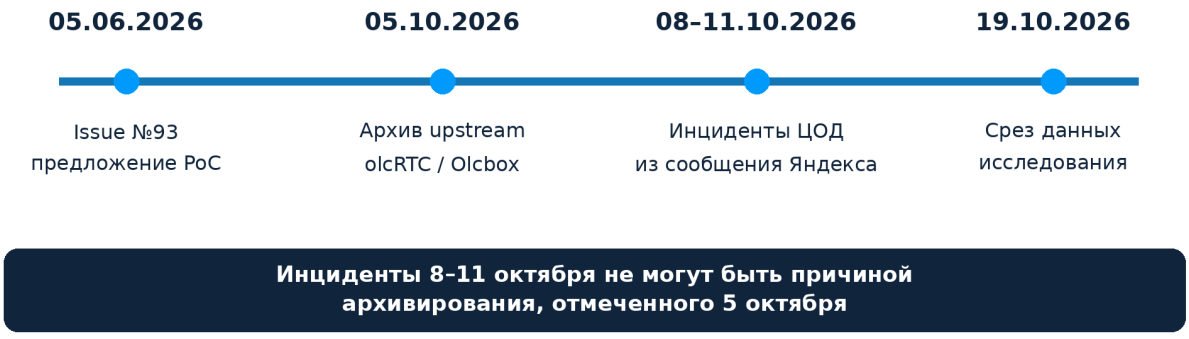


Рис. 1. Реконструкция временной последовательности. Первичное архивирование upstream предшествовало описанным инцидентам ЦОД; события разных проектов нельзя считать единой причинной цепью.

Ключевые события по первичным документам

Дата	Событие и источник	Допустимый вывод
27.03.2026	Комментарий автора vk-turn-proxy о TURN Telemost [S13]	Наблюдение сообщества, не официальное изменение политики
05.06.2026	Issue olcRTC №93 об авторизованном создании комнат [S10]	Авторский PoC; в upstream core предложение не принято
30.06.2026	Issue №114 и merged PR №115 [S11-S12]	Появилось поле account token; server-side роль не гарантирована
14.09.2026	Olcbox nightly 1.0.129 [S2]	Факт публикации сборки, не доказательство совместимости
05.10.2026	Upstream olcRTC и Olcbox архивированы [S1-S2]	Состояние конкретных репозиториев
08–11.10.2026	Заявленные инциденты ЦОД Яндекса [S14-S15]	Влияние на конкретный Telemost media path не установлено
14.10.2026	Ghostlane 1.0.466, новый release-gate [S3]	Условные self-tests новой версии и другой матрицы

4. Протокольный стек WebRTC

WebRTC включает несколько функций, которые в интерфейсе пользователя выглядят как одна видеовстреча, но технически разделены. HTTPS/WebSocket сигнализация договаривается о параметрах комнаты. ICE осуществляет проверку достижимости кандидатов, STUN помогает установить адресные параметры через NAT, TURN ретранслирует пакеты через выделенную allocation, а медиатреки используют SRTP. DataChannel является отдельной семантикой передачи сообщений поверх SCTP/DTLS. [S5-S8]



Рис. 2. Три независимые доверительные границы: identity/signaling, media control, network relay. Схема иллюстрирует типовую архитектуру, а не закрытую схему конкретного сервиса.

4.1. TURN: что предусмотрено самим стандартом

RFC 8656 заменил RFC 5766 и формализует создание relay allocations, механизм permissions для peer-адресов, ограничения времени жизни и средства борьбы со злоупотреблениями. Наличие TURN не означает безусловной пересылки пакетов куда угодно: возможности зависят от назначенных прав, сервера, пути ICE и политики провайдера. Возможность клиента создать обычную комнату никак не доказывает способность связаться с произвольным внешним адресом посредством TURN. [S6]

4.2. SFU, комнаты и публикации

SFU маршрутизирует медиатреки между участниками, основываясь на свойствах комнаты и разрешениях публикации. TURN представляет собой сетевой ретранслятор и не обязуется принимать те же решения на уровне участника конференции. Запрет отправлять DataChannel через серверный grant и отказ выдавать новый TURN allocation - принципиально разные виды отказа.

4.3. Метаданные и пределы сетевого наблюдения

Шифрование защищает содержимое от третьей стороны без ключей, но не скрывает все метаданные. Сеть может наблюдать IP/порт, продолжительность, объём, размер пакетов и интервалы. Теоретически статистический классификатор способен различать классы потоков с ненулевой ошибкой; вывод о стопроцентной неотличимости не обоснован. Для оценки такой защиты нужны контролируемые датасеты обычных видеосессий и расчёт ложноположительных блокировок.

4.4. Различие отказов

Слой	Пример наблюдения	Что нельзя из него выводить
Identity	Отказ аутентификации	Что TURN недоступен
Authorization	Нет publishData grant	Что публикация видео тоже невозможна
Signaling	Нет соединения с API	Что оператор блокирует медиатрафик
ICE/TURN	ICE failed / allocation denied	Что у клиента закрыт аккаунт
SFU/media	Нет медиатреков	Что upstream проекта закрыт
Infrastructure	Деградация ЦОД / SLO	Что это причина архивирования кода

5. Авторизация: аккаунт, комната, поток

Вместо единой переменной «доступ есть/нет» вводится пять отдельных проверок: I(u,t) для идентичности, C(u,t) для права создать комнату, J(u,r,t) для входа, P(u,r,k,t) для конкретного типа публикации k и A(u,r,t) для допуска активного соединения. Дополнительно R(u,r,t) обозначает право повторного входа после потери связи. Эти функции условно независимы: C=true не влечёт P=true, J=true не влечёт P(data)=true, а завершение срока первоначального JWT не влечёт A=false.

Это аналитическая модель, не реконструкция закрытых схем WB или Яндекса. Чтобы превратить её в утверждение о реальном сервисе, необходимы документированные правила и авторизованный эксперимент. Системы с несколькими сервисами токенов могут применять разные жизненные циклы для account access token, room token, TURN credentials и сессионных разрешений.

РИС. 3 / ЖИЗНЕННЫЙ ЦИКЛ ДОСТУПА



Рис. 3. Жизненный цикл identity и room grant. Истечение JWT, серверный отзыв прав и прекращение активного медиаканала должны проверяться раздельно.

5.1. LiveKit как публичная эталонная модель

LiveKit документирует JWT, которые кодируют идентичность участника, комнату и grants, включая возможность публиковать аудио, видео и данные. Сервер может обновлять разрешения действующих участников. Период `exp` влияет на принятие первоначального подключения, но не обязан обрывать текущую сессию. LiveKit автоматически обновляет токены для работающих клиентов. [S9]

В LiveKit Cloud механизм token revocation может использовать границу `nbf` для отзыва более старых токенов. Для self-hosted-развёртываний документация отдельно предупреждает, что серверное удаление пользователя не автоматически аннулирует его старый JWT. Документация Cloud при этом описывает нюансы уже обновлённых токенов и рекомендует явный cutoff для строгого запрета повторного входа. Это показывает, почему фраза «поставьте короткий TTL - встреча гарантированно выключится» некорректна. [S9]

5.2. Почему идентичность не равна полномочию

В issue olcRTC №114 участники обсуждали повторное использование фиксированной идентичности WB. Принятый upstream PR №115 добавил поддержку предварительно полученного аккаунтного токена, но не гарантию роли модератора. При реконнекте сервер способен выдать новый комнатный grant согласно текущей роли аккаунта; если эта роль отозвана, старый account token не должен автоматически восстанавливать права. Эмпирические детали стороннего WB Stream необходимо проверять отдельно. [S11-S12]

5.3. Защита от похищения bearer-токенов

Компрометация bearer JWT создаёт риск повторного подключения, если сервер не применяет дополнительные проверки. Инженерные меры: ограничение scope, краткий срок токенов, запрет раскрытия в логах, отдельный отзыв сессий, контроль ролей на сервере, MFA и аудит. RFC 9449 определяет DPoP для proof-of-possession в OAuth, однако это лишь применимая к ряду архитектур рекомендация; отсутствует подтверждение внедрения именно DPoP сервисами Telemost или WB. [S16]

6. Что действительно известно о видеоплатформах

6.1. Яндекс Телемост

Официальный API Яндекс Телемоста позволяет пользователю с личным Яндекс ID создать обычную публичную встречу. Для комнаты ожидания описаны режимы `PUBLIC`, `ORGANIZATION` и `ADMINS`, то есть политики приёма участников имеют разные уровни доступа. Отсюда следует, что тезис «вся система работает исключительно для сотрудников организации» не соответствует опубликованной документации. Но разрешение создать встречу не означает, что любой транспорт передачи данных доступен в мобильной сети с ограничениями. [S17]

Разработчик vk-turn-proxy 27.03.2026 в комментарии к issue №46 сообщил о запрете подключения TURN к внешним IP. Содержание комментария установлено, однако отсутствует официальное независимое подтверждение его глобальной применимости, параметров конфигурации и даты развёртывания. Следовательно, это **сообщение разработчика**, а не доказанная опубликованная политика Яндекса. [S13]

6.2. WB Stream

По матрице проекта olcRTC режим гостя WB Stream имеет ограничение `canPublishData=false`; другие транспорты в рамках self-tests авторов помечены работающими или нестабильными. Отдельное обсуждение issue №93 содержит заявленные участником опыты создания комнат с авторизованным аккаунтом, но сопровождающий проекта не принял предложенное автоматическое создание комнат непосредственно в ядро, предпочтя вынести процесс в отдельную утилиту. Эти данные не образуют официальную спецификацию сервиса WB Stream. [S10-S12]

В вопросе модерации необходимо разделить выдачу аккаунтной идентичности и динамические room grants. Возможное сохранение роли после reconnection зависит от серверной политики WB, а не от отсутствия у токена поля `exp` или от факта сохранения значения identity. Без лабораторных данных нельзя объявлять «вечную модерацию» свойством системы.

6.3. Матрица автора и её научная граница

Транспорт / сервис	Telemost	WB Stream	Jitsi
DataChannel	Не работает по self-tests	Нестабильный / ограничен guest grant	Проходит self-tests
VP8-видеоканал	Проходит self-tests	Проходит self-tests	Проходит self-tests
SEI-видеоканал	Не поддержан	Проходит self-tests	Проходит self-tests
Другой видеоканал	Проходит с оговорками	Проходит self-tests	Проходит self-tests

Табл. 5. Пересказ матрицы совместимости автора olcRTC [S18], зафиксированной в документации проекта. Не использовать как независимые лабораторные результаты и универсальное измерение доступности сетей РФ.

7. Ghostlane: сравнение выпуска без ложных корреляций

На публичной странице релизов Ghostlane для версии **1.0.456** от 05.10.2026 указан engine pin `f9edaa7f1ab5`, 48 плановых test cells, один failed case; Telemost CLI и Mobile в этой матрице прошли 1/1 и 7/7, WB Stream также присутствовал в наборе. В версии **1.0.466** от 14.10.2026 указан engine pin `bac09891b3b4`, 46 cells, семь failed; Telemost CLI 0/1 и Mobile 2/7, а WB Stream в перечне отсутствует. [S3]

Параметр	Ghostlane 1.0.456	Ghostlane 1.0.466
Дата релиза	05.10.2026	14.10.2026
Pinned engine	f9edaa7f1ab5	bac09891b3b4
Набор тестов	48 cells	46 cells
Суммарные fail	1 из 48	7 из 46
Telemost CLI	1/1 успешен	0/1 успешен
Telemost mobile	7/7 успешны	2/7 успешны
WB Stream	Включён в матрицу	Не включён в матрицу

Обе матрицы основаны на **self-tests разработчика** с различными версиями и неполным совпадением состава опытов. Их нельзя трактовать как строгий эксперимент до/после с постоянными контрольными условиями. Изменение результата может объясняться изменением transport, target, CI runner, engine, flaky test, политикой комнаты либо инфраструктурой. Отсутствие WB Stream во втором наборе означает **нет измерения**, а не «успешность равна нулю». [S3]

> ПРИНЦИП ВОСПРОИЗВОДИМОСТИ
>
> Сравнение выпусков пригодно для описания истории инженерной диагностики проекта. Для вывода о блокировках конкретного сервиса надо подтвердить сопоставимость test IDs, окружения, ролей и сети и получить независимые полевые измерения.

8. Инфраструктурные инциденты и причинность

В начале октября 2026 года появились сообщения о повреждениях дата-центров Яндекса; как минимум Reuters 13.10.2026 описывает атаки на три ЦОД и обсуждение перебоев. Корпоративное сообщение Яндекса с датами 09 и 11 октября доступно в публичном сообщении компании. При этом публичные материалы не дают достаточной топологии зависимости каждой конкретной комнаты Телемоста, её signaling backend и media relay от затронутой площадки. [S14-S15]

Нельзя выводить прямую причинность для архивирования olcRTC из инцидентов 08–11.10, если GitHub показывает архив 05.10. Для отдельного ухудшения связи после инцидента достаточно правдоподобной гипотезы, но недостаточно доказательства: нужны сопоставленные временные ряды, инфраструктурная карта, конкретные журналы отказа, альтернативные факторы и контрольный регион.

8.1. Альтернативные объяснения отказа

- Клиентская ошибка, несовместимость сетевого wire-format или изменённый codec pipeline.

- Истечение учётной сессии, изменение роли moderator, отсутствие permissions или отказ в создании комнаты.
- Отказ signaling/API, ICE negotiation, TURN allocation или медиапубликации как разные точки отказа.
- Сетевая политика доступа и зависимость от определённых IP, а не обязательно от домена в целом.
- Нагрузка и деградация дата-центра / SFU, временная изоляция зоны, fallback на другие узлы.

Только система наблюдений, способная различать эти объяснения, делает вывод об истинной причине устойчивым к критике.

9. Формальная модель угроз

Активы: доступность реальных видеовстреч, личные учётные записи, сеансы и приватность участников, ёмкость SFU/TURN, доверенные room grants и целостность аудита. **Нарушители:** анонимный автоматизированный клиент, пользователь с украденным токеном, недобросовестный авторизованный участник, ошибочно настроенный интегратор, случайно некорректное клиентское ПО. **Граница:** защита платформы от злоупотребления не должна презюмировать виновность обычного участника по одному статистическому признаку.

Риск	Основные инженерные меры	Остаточный риск
Массовое создание комнат	Отдельный grant для roomCreate, защита от автоматизации и квоты	Захваченный / легитимно зарегистрированный аккаунт
Replay bearer токена	Scope, TTL, revocation, audit; sender-binding где поддерживается	Уже действующая сессия и компрометация устройства
Нецелевая публикация	Политика типа треков, серверный контроль, квоты и аудит	Авторизованный злоумышленник / false positives
Нецелевой relay TURN	Peer permissions, allocation limits, accounting	Разрешённое соединение может использоваться не по назначению
Деградация медиаплатформы	Резервирование, зональная независимость, fallback, disaster recovery	Коррелированные отказы общих зависимостей
Ошибочное блокирование звонков	Тесты false positive, контроль нормальных сценариев, rollback	Компромисс качества детекции и доступности

9.1. Почему MFA не является окончательной контрмерой

MFA снижает угрозу компрометации учётных данных, но не заменяет проверку полномочий каждой операции. Подтверждённый аккаунт может сохранять право публикации, несмотря на нецелевое поведение. Применимость контроля оценивается не по наличию слова «верификация» в интерфейсе, а по наблюдаемому отказу запрещённой операции и минимальному ущербу нормальному сценарию.

9.2. Privacy by design

Регистрация и мониторинг могут увеличить объём чувствительных данных. Серверным журналам полезнее присваивать непрозрачные идентификаторы, ограничивать срок хранения, избегать записи исходных секретов и содержимого звонков, раздельно хранить security events и персональные сведения. В LiveKit документация отдельно предупреждает, что identity и имя комнаты попадают в логи и trace, поэтому личные данные не следует помещать в эти поля. [S9]

10. Программа научной верификации

Полноценная эмпирическая работа должна использовать собственный или явно разрешённый лабораторный стенд WebRTC/LiveKit с тестовыми аккаунтами, синтетическими безвредными потоками и закрытым контуром. Тестирование чужих сервисов без согласия в план не входит. Ни один из приведённых ниже сценариев пока не выполнен; они не представляют собой результаты измерений.

Серия	Сценарии (19)	Измеряемые реакции
AUTH / 01–05	Анонимность; зарегистрированный без права создания; только roomJoin; MFA без расширения grants; комната ожидания	Отказ, аудит, выделенные ресурсы, время допуска
PUB / 01–04	canPublishData=false; canPublish=false; только камера; viewer vs moderator	Принятие/отказ публикации, тип потока, role events
TOK / 01–06	JWT до и после exp; активная сессия; update permissions; удаление участника; Cloud/self-hosted reconnect	Enforcement latency, повторный вход, медиатрафик после revoke
NET / 01–02	Управляемый отказ TURN и SFU на стенде	Recovery time, ICE errors, доступность обычных звонков
FP / 01–02	Легитимный звонок с высоким bitrate и с плохим каналом	False positives, потеря качества, журналы

10.1. Минимальные показатели

- **Policy enforcement rate:** правильно отклонённые запрещённые операции / все запрещённые операции с известной policy oracle.
- **False-positive:** ошибочно отклонённые разрешённые действия / общее число разрешённых действий.
- **False-negative:** разрешённые нарушения установленного правила / все провоцированные нарушения.
- **Time-to-enforce:** момент фактического прекращения запрещённого поведения минус момент серверного изменения правила.
- **Quality:** задержка, потери, jitter и эффективность восстановления с указанием числа опытов, версии и окружения.

10.2. Критерии воспроизводимости

Перед тестом фиксируются релизы SDK, серверов и OS, hash контейнеров, сетевой профиль, UTC-время и монотонные timestamps, правила grant, конфигурация без секретов, безопасная нагрузка, критерии исключения, числа повторений и контрольный baseline. Для статистических выводов приводятся выборка N, доверительные интервалы, пропущенные данные и величина влияния на нормальный звонок. Иначе любая «процентная эффективность» недопустима.

10.3. Полная матрица 19 сценариев

Ниже фиксируется проверяемое условие каждого опыта. Это предрегистрация плановых испытаний, **не результаты**. Итоговые значения должны поступать из подписанного журнала стенда.

Тест	Предпосылка	Проверка результата
AUTH-01	Аноним пытается создать защищённую комнату	Отказ до создания и запись события
AUTH-02	Зарегистрированный пользователь без roomCreate	Недопуск даже после успешного login
AUTH-03	Участник с roomJoin, но не roomCreate	Вход допустим, создание отклонено
AUTH-04	MFA пройден, дополнительные grants не выданы	Не происходит скрытого расширения полномочий
AUTH-05	Guest входит в комнату ожидания	Решение о допуске выдаёт уполномоченная роль
PUB-01	canPublishData=false	Отсутствует доставленная DataChannel-публикация
PUB-02	canPublish=false; canSubscribe=true	Публикация отклонена; подписка разрешена
PUB-03	Разрешён camera, запрещён screen	Нельзя публиковать неразрешённый тип источника
PUB-04	Viewer и moderator в одной комнате	Различаются полномочия по политике роли
TOK-01	Подписанный join JWT до exp	Сервер принимает токен по своему протоколу
TOK-02	Тот же JWT после exp	Новый initial join корректно отклоняется
TOK-03	Действующая сессия в момент exp	Отдельно зафиксировано состояние медиаканала
TOK-04	Снижение grants во время звонка	Замерено время фактического прекращения права
TOK-05	Удаление участника и попытка reconnect	Зарегистрирован фактический результат повторного входа

Тест	Предпосылка	Проверка результата
TOK-06	Cloud-style revoke vs self-hosted policy	Сравнено принятие старого JWT по двум реализациям
NET-01	Плановый отказ контролируемого TURN	Проверено корректное fallback/отсутствие нарушения
NET-02	Плановый отказ контролируемого SFU	Замерены RTO и влияние на обычные звонки
FP-01	Легитимное видео с повышенным bitrate	Измерено число ошибочных блокировок
FP-02	Легитимный звонок с loss и jitter	Измерено число ошибочных квалификаций

10.4. Документирование эксперимента и защита от смещения

Процедура предрегистрации должна определять точное число повторений каждого сценария, тестовый режим, допустимые ошибки и baseline до наблюдения результатов. Оператор стенда не должен менять критерии «успеха» после того, как увидел неудачные кейсы. Для сравнений между версиями применяется парный анализ одинаковых test IDs и при необходимости стратификация по сети, OS, типу носителя и роли. Каждая пропущенная ячейка отмечается как missing, а не zero.

Участники обычных звонков составляют обязательную отрицательную контрольную группу: защита, отвергающая все подключения, будет иметь формально высокую долю блокировок, но неприемлемую практическую полезность. Поэтому безопасность оценивается вместе с доступностью, p95 media delay, качеством вызовов, false positives и организационными последствиями для пользователей.

> ВОСПРОИЗВОДИМОСТЬ
>
> Для оценки меры защиты недостаточно единичного успешного теста. Нужны заранее установленный policy oracle, независимый контроль, N, confidence interval, зафиксированные версии, анонимизированные raw logs и проверяемый хеш артефакта. Любой результат без этих условий помечается как предварительный.

11. Критическая коллегия и циклы рецензирования

Для внутренней ревизии использованы восемь **рецензионных ролей**: архитектор WebRTC, специалист по JWT/identity, исследователь GitHub-истории, инженер отказоустойчивости, рецензент эмпирики, специалист по гражданским и регуляторным последствиям, Red Team и научный редактор. Три аналитических раунда выполнялись как раздельные направления одной AI-работы, **не как независимая комиссия живых экспертов**. Методика внутренней проверки изложена в этом разделе.

Раунд	Предмет	Результат
I. Source / Architecture	RFC, API, GitHub Issues / releases, JWT и права	Исправлены смешения developer report и официальной политики
II. Adversarial review	Причинность ЦОД, активный JWT, роль, неверные обобщения	Отклонены абсолютные тезисы о «закрытии всего»

Раунд	Предмет	Результат
III. Editorial QA	Scope, термины, матрицы, табличные выводы, источники	Подготовлена редакция для внешней рецензии

11.1. Существенные исправления

- Предложение issue olcRTC №93 о создании комнат классифицировано как сторонний PoC; оно не было принято сопровождающим в core. [S10]
- Merged PR №115 подтверждает изменение исходного кода для заранее выданного токена, но не обещает постоянную роль moderator. [S12]
- Сообщение об ограничении TURN размещено именно в комментарии issue №46; независимо на серверах Яндекса не проверено. [S13]
- Изменившиеся результаты Ghostlane не выданы за показатель общей сетевой блокировки. [S3]
- Архивация репозитория и отдельные инфраструктурные инциденты разведены по времени; причинная связь исключена без доказательств. [S1, S14–S15]
- Исходный фирменный логотип не найден в доступных исходниках; используется узнаваемый знак из предыдущей редакции с раскрытием статуса.

11.2. Неустранимые редактурой ограничения

Повторение интеллектуальных циклов полезно, пока выявляются новые противоречия или недостатки источников. Но оно не производит недоступные raw logs сторонних серверов, измерения мобильных операторов, письменное разрешение на эксперимент или реальные подписи внешних научных рецензентов. Это обязательные внешние факторы; скрывать их означало бы не улучшить, а исказить научную достоверность.

12. Выводы исследования

- **01.** OLCBOX и архивный olcRTC относятся к конкретным публичным проектам. Закрытие upstream в режиме архивирования не означает исчезновения всей технологической архитектуры, что подтверждается продолжением развития других репозиториев.
- **02.** WebRTC объединяет отдельные контуры сигнализации, сетевой связности, управления идентичностью, DataChannel и медиапотоками. Ошибка одного контура не доказывает блокировку другого.
- **03.** Официальное API Яндекс Телемоста различает типы доступа; нельзя утверждать, что весь сервис требует корпоративной идентификации. В то же время API-функция публичного создания комнаты не гарантирует успешный TURN или DataChannel в любой сети.
- **04.** Матрицы olcRTC и Ghostlane имеют ценность как инженерные источники. Их авторские тесты не являются независимыми сравнительными измерениями операторов связи.
- **05.** Account bearer, room JWT, роль участника, TTL, revocation и активный медиаканал требуют раздельных контрольных решений. Упрощённая стратегия «один короткий токен решает всё» технически необоснованна.

- **06.** Практически разумная оборонительная архитектура сочетает MFA, наименьшие полномочия, server-side policy enforcement, безопасный отзыв и отключение, TURN квоты, детекцию аномалий с измерением ошибок, журнал и резервирование.

- **07.** Причина конкретного отказа должна опираться на трассировку зависимостей, согласованную временную шкалу и альтернативные гипотезы. Архивирование upstream 05.10 не могло быть вызвано атаками ЦОД 08–11.10 при принятой хронологии.

- **08.** Сильная часть настоящей работы - классификация доказательств, техническая модель угроз и воспроизводимый экспериментальный протокол. Утверждать измеренную универсальную эффективность контрмер до экспериментов нельзя.

РЕШЕНИЕ ИЗДАТЕЛЬСКОЙ РЕВИЗИИ

Текстовая и методическая часть доведена до профессиональной документальной редакции, пригодной для обсуждения с независимыми специалистами. Общий статус исследования: **аналитический препринт, не завершённая экспериментальная научная публикация**. Переход к категории «эмпирически подтверждено» потребует реальных протоколов испытаний.

Приложение A. Реестр проверочных утверждений

Ниже собраны тридцать контрольных положений. **Факт о содержании источника** не следует трактовать как факт об эксплуатационной политике другого сервиса. Полный обновляемый реестр и пояснения к нему основаны на внутренних исследованиях Лаборатории Шахулова.

Коды	Область доказательств	Класс
01–06	IETF: ICE; TURN; SCTP-over-DTLS; E2E encrypt; TURN permissions; peer authorization	A / RFC
07–12	Olcbox alpha; upstream archived; Ghostlane ongoing releases; snolc independent architecture; olcRTC transport types; author compatibility matrix	B / GitHub
13–18	WB guest data grants; account token PR115; proposed room auto-creation; Telemost comment on TURN; Telemost personal-ID public meeting; Telemost waiting room roles	A–C / scope-specific
19–24	LiveKit JWT grants; exp initial connection; refresh; Cloud revocation; self-hosted limitation; OAuth DPoP as external architecture	A / docs
25–30	Ghostlane 1.0.456 test set; Ghostlane 1.0.466 test set; WB omission; date order outages/archive; limits of SNI+IP policy inference; missing independent field evidence	B–D / methodological

Особые блокеры: независимая инфраструктурная экспериментальная база, прямые спецификации серверной политики отдельных сервисов и воспроизводимость экспериментальных результатов. Они не отменяют качества аналитической части, но ограничивают тип выводов.

Приложение A1. Протокол опровержения и независимой рецензии

Критическая гипотеза №1. «Доступ ограничен сотрудниками»

Проверяемое утверждение: невозможно создать или посещать общедоступную встречу без корпоративной учётной записи. **Контрдоказательство:** опубликованный API Телемоста прямо допускает обычные публичные встречи личного Яндекс ID. Утверждение подлежит отклонению применительно к глобальной политике создания встречи. Но оно может оставаться верным для частной комнаты с корпоративным waiting room или конкретного доступа к иной функции; нужна точная область применения. [S17]

Критическая гипотеза №2. «Верификация решает все риски»

Проверяемое утверждение: любая форма MFA блокирует передачу нецелевого контента. **Контрпример:** участник с действующей ролью и разрешением публикации проходит MFA, но остаётся способным использовать разрешённый медиаканал не по назначению. Меры защиты должны реализовывать policy enforcement на уровне комнаты и треков, и оценивать злоупотребления как отдельную задачу.

Критическая гипотеза №3. «Новые тесты означают блокировку оператора»

Проверяемое утверждение: два CI-release-gate Ghostlane образуют эквивалентные полевые замеры мобильной сети. **Контрдоказательство:** наборы отличаются по версии pin и числу ячеек, а WB отсутствует в одном из них. Для causal attribution нужны одинаковые test cases, воспроизводимая сеть и сырые артефакты. [S3]

Критическая гипотеза №4. «Инцидент ЦОД вызвал архивирование»

Проверяемое утверждение: известные инциденты 08–11.10 привели к решению владельцев репозиториев 05.10 перевести проекты в архив. **Контрдоказательство:** следствие датировано раньше предполагаемой причины. Это не исключает влияния инцидента на отдельные соединения позже, но требует новой и другой гипотезы. [S1-S2, S14-S15]

Критерии внешнего экспертного заключения

- Профиль рецензента и отсутствие конфликта интересов указаны открыто; замечания нумеруются и связываются с фрагментами текста.
- Для каждого критического замечания автор отвечает ссылкой на подтверждение, изменением текста или документированной причиной несогласия.
- Факты о чужой внутренней инфраструктуре не принимаются лишь по коду стороннего клиента.
- Эксперт проверяет воспроизводимость эксперимента, достоверность выборки, этичность доступа и ущерб обычным пользователям.
- Два независимых review согласованы только после закрытия существенных противоречий; отсутствие отзывов не моделируется искусственно.

Приложение B. Библиография и первоисточники

[S1] openlibrecommunity/olcrtc. GitHub upstream и README; архив 05.10.2026. Источник ↗

[S2] alananisimov/olcbox. GitHub README и Releases; Alpha; архив 05.10.2026. Источник ↗

[S3] ghostlane-project/ghostlane. Releases 1.0.456 и 1.0.466; CI release-gates. Источник ↗

[S4] owenewans/snolc. Документация модульной сетевой архитектуры Rust. Источник ↗

[S5] IETF RFC 8445. Interactive Connectivity Establishment (ICE). Источник ↗

[S6] IETF RFC 8656. Traversal Using Relays around NAT (TURN). Источник ↗

[S7] IETF RFC 8831. WebRTC Data Channels. Источник ↗

[S8] IETF RFC 8827. WebRTC Security Architecture. Источник ↗

[S9] LiveKit Documentation. Access tokens & grants, token lifecycle. Источник ↗

[S10] olcRTC, issue №93: proposal and discussion of automated room creation. Источник ↗

[S11] olcRTC, issue №114: account identity, WB token and reconnect. Источник ↗

[S12] olcRTC, merged pull request №115: optional pre-issued WB account token. Источник ↗

[S13] vk-turn-proxy, issue №46, сообщение в комментарии о Telemost TURN. Источник ↗

[S14] Яндекс. Корпоративное сообщение об инцидентах в ЦОД 09–11.10.2026. Доступность конкретного URL требует повторной проверки. Источник ↗

[S15] Reuters, 13.10.2026: правительственное обсуждение атак на ЦОД Яндекса. Источник ↗

[S16] IETF RFC 9449. OAuth 2.0 Demonstrating Proof of Possession (DPoP). Источник ↗

[S17] Яндекс Телемост. Официальный API создания встречи и waiting room. Источник ↗

[S18] olcRTC. Compatibility matrix в docs/settings.md. Источник ↗

[S19] IETF RFC 9700. Best Current Practice OAuth 2.0 Security. Источник ↗

[S20] GitHub Issue №109: транспортные ошибки VP8, fix и несовместимый wire format. Источник ↗

[S21] ghostlane-project/olcrtc. Форк ядра WebRTC; код и история изменений. Источник ↗

Приложение C. Редакционные ограничения и логотип

В оформлении использован **логотип «Лаборатория Шахулова / IT - Агентство»**, предоставленный непосредственно представителем лаборатории для настоящей редакции. Фирменная цветовая пара - ярко-голубой знак и тёмный текст; схемы и акценты приведены в соответствие с этим стилем. Исходное пользовательское изображение сохранено без перерисовки или замены символа.

Внутренняя аналитическая коллегия не имитирует независимую человеческую научную рецензию. Образцы тестов и архитектурные модели предназначены для надлежащим образом согласованного defensive security анализа, не для тестирования сторонних систем без разрешения.

ПАСПОРТ ВЫПУСКА

Редакция: 5.2 / 19.10.2026
Срез источников: 19.10.2026
Научный статус: аналитический препринт, ожидает независимой рецензии и экспериментальной программы
Собственные материалы: модель доверия, методология проверки и внутренние исследования.