**Руководство по безопасной коммуникации**

В этом документе, к которому могут обращаться сотрудники RFE/RL, собраны все инструменты, которые мы рекомендуем использовать для безопасного общения как между коллегами, так и с источниками и аудиторией. Внутренняя коммуникация в RFE/RL должна осуществляться через платформу Microsoft (например, Outlook, Teams). Однако в некоторых случаях, описанных ниже, допустимо и необходимо использовать другие инструменты. Не включенные в этот список мессенджеры, такие как Facebook Messenger, не считаются безопасными и не подходят для рабочей коммуникации. Если у вас есть вопросы по этому руководству или вам нужна дополнительная помощь для обеспечения безопасности ваших коммуникаций, свяжитесь с Carter Boone через Teams или по электронной почте: boonec@rferl.org.

**Signal**

Signal — это универсальное средство обмена зашифрованными сообщениями, рекомендуемое для обмена сообщениями между коллегами и общения с источниками. Signal использует надежные протоколы шифрования и не передает пользовательские данные властям или рекламодателям. Приложение широко используется и доступно в надежных магазинах приложений. Signal относительно прост в использовании и не требует длительной настройки для обеспечения безопасности, однако в разделе настроек приложения можно внести некоторые изменения, чтобы обеспечить еще большую безопасность.

Рекомендации:

* Настроить исчезновение сообщений: это можно сделать через «Настройки приложения» → «Приватность» → «Исчезающие сообщения» → выберите время (рекомендуем не более 1 часа). **Исчезающие сообщения особенно важны** для общения с источниками или фрилансерами в зонах повышенного риска.
* Скрытие вашего телефонного номера: В последней версии Signal номера телефонов скрываются по умолчанию. Если вы используете устаревшую версию, измените настройки в «Приватность» → «Номер телефона» → «Кто может видеть мой номер» → **«Никто»**.
* Ограничьте личную информацию: избегайте использования фотографий в профиле, предпочтительно использовать аватар или инициалы. Не указывайте личную информацию (email, адрес и т.д.) в био. Если вы относитесь к группе повышенного риска или общаетесь с человеком, находящимся в зоне повышенного риска, используйте в своем профиле инициалы, а не полное имя.
* Удаляйте старые чаты: если у вас есть старые чаты без настройки исчезающих сообщений, удалите их и начните новый чат с включенной этой функцией. Включение функции "исчезающие сообщения" в существующем диалоге не будет применяться к сообщениям, отправленным ранее.
* Используйте VPN или прокси: для дополнительной защиты рекомендуется использовать VPN для сокрытия IP-адреса и браузера. Однако важно помнить, что в некоторых юрисдикциях использование VPN может быть ограничено или запрещено.
* **Для фрилансеров в России и Беларуси:** отключите автоматическое резервное копирование. Фрилансеры, работающие в России или Беларуси, должны принимать дополнительные меры предосторожности для снижения риска. Для отключения автоматического резервного копирование сообщений в зашифрованном виде зайдите в «Настройки» → «Чаты» → «Резервные копии» и выберите «Выключить».
* Обмен файлами: Signal не считается оптимальным инструментом для передачи файлов из-за ограничений на размер файлов. Для получения больших файлов или утечек лучше использовать другую платформу, например, Globaleaks.

**WhatsApp**

WhatsApp также является хорошим инструментом для зашифрованного обмена сообщениями с источниками и фрилансерами, если использование Signal затруднено. В некоторых регионах использование Signal не распространено и может привлекать внимание властей, в таких случаях WhatsApp является допустимой альтернативой. Основное различие между Signal и WhatsApp заключается в объёме собираемых данных пользователей и их управлении. В прошлом у Meta были проблемы со сбором большого количества персональных данных от своих пользователей, поэтому WhatsApp требует от пользователя большего участия для настройки безопасности.

Рекомендации:

* Удаление данных о местоположении: если геолокация включена в настройках, эти данные собираются. Чтобы отключить это, перейдите в «Настройки» → «Конфиденциальность» → «Местоположение в реальном времени» → «Нет».
* Двухфакторная аутентификация: Включите двухфакторную аутентификацию для дополнительной защиты аккаунта. Перейдите в «Настройки» → «Аккаунт» → «Двухэтапная проверка» → «Включить» → Установите PIN-код.
* Исчезающие сообщения: Как и в Signal, функция исчезающих сообщений является важной. Перейдите в «Настройки» → «Конфиденциальность» → «Таймер сообщений по умолчанию» → «24 часа».
* Фотографии и видео «Просмотреть один раз»: При отправке фото или видео нажмите на круг с числом «1», чтобы активировать функцию «Просмотреть один раз».
* Защита IP-адреса для звонков: Эта настройка затрудняет определение вашего местоположения на основе использования приложения. Перейдите в «Настройки» → «Конфиденциальность» → «Расширенные» → «Защита IP-адреса для звонков» → «Включить».
* Шифрование резервных копий: WhatsApp автоматически сохраняет резервные копии ваших чатов и медиафайлов, но эти резервные копии не зашифрованы. Для изменения этой настройки перейдите в «Настройки» → «Чаты» → «Резервные копии с сквозным шифрованием» → «Включить». Храните ключ шифрования в безопасном месте, например, в [менеджере паролей](https://rferl.sharepoint.com/%3Aw%3A/s/DigitalStrategy/ESPDbgRo3QxJoWs4gTQmLJcBvmGC1NYm0nIyLByzz8sOiQ?e=IPx3x4).

**CDR Link**

CDR Link — это хелпдеск-платформа, созданная для правозащитных организаций Center for Digital Resilience. Это безопасная платформа, которая может использоваться редакциями для сбора информации и общения со своей аудиторией. Это особенно полезно для служб в странах, где открытое взаимодействие с контентом RFE/RL запрещено или может быть опасным, таких как Россия и Беларусь. Различные каналы связи (Telegram, Signal, WhatsApp, электронная почта, формы и т.д.) подключены к одной платформе CDR Link, что позволяет вам получать все сообщения в одном удобном месте. Вы можете получать текстовые сообщения и вложения, такие как фотографии, скриншоты, аудио и видео. Для анонимного и безопасного обмена файлами предпочтительнее использовать Globaleaks.

Рекомендации:

* Получение доступа: В настоящее время эта платформа успешно тестируется несколькими командами. Если ваша редакция хочет использовать CDR Link, отправьте запрос на почту cdrlink@rferl.org.
* Используйте KASM: Подключайтесь к платформе только через KASM, используя браузер EU (не используйте RU/BY). Это обеспечит безопасность вашего соединения и коммуникаций. После завершения работы не забудьте завершить сессию KASM.

**LetsConvene.im**

Для чего использовать: Convene — это удобная веб-платформа для безопасного общения, разработанная Guardian Project. Платформа особенно удобна тем, что для создания чата не требуется профиль, номер телефона или любая личная информация. Для доступа к чату нужен только браузер и подключение к интернету. Комнаты чатов создаются на сайте [LetsConvene.im](https://letsconvene.im/), а ссылка на чат может быть передана источнику или фрилансеру, работающему в зоне высокого риска, предпочтительно через Signal или WhatsApp с включенными исчезающими сообщениями. Участники чата идентифицируются псевдонимами, такими как «Guest Shark». Платформа поддерживает широкий спектр типов файлов, включая zip, PDF, видео, аудио и изображения.

Рекомендации:

* Модераторы: Модераторы создают комнаты чатов и делятся ссылкой с пользователями. Они могут видеть историю чатов, создавать опросы и отправлять/получать голосовые заметки или файлы. Модераторы **обязаны удалять комнату** после завершения общения. Если злоумышленник получит ссылку на уже удалённый чат, она не будет работать.
* Режим отправки файлов: Функция работает как «дропбокс», где модератор переводит чат в режим отправки файлов, и участники могут загружать файлы.
* Автоматическое удаление комнат: В настоящее время функция автоматического удаления комнат находится в разработке. Пока она недоступна, **модераторы несут ответственность за своевременное удаление комнат**.
* Создание комнаты: Зайдите на <https://letsconvene.im/> → выберите «Open a Private Room» → задайте название комнаты (рекомендуется использовать нейтральное название) → комната будет создана.
* Распространение ссылки на комнату: В комнате нажмите на три точки рядом с аватаром → выберите «Copy Invite Link» для копирования ссылки. Вы также можете перейти в «Room Details» для получения общей информации о комнате или создания QR-кода для обмена ссылкой.
* Управление комнатой: В разделе **«Room Details» модератор может управлять комнатой,** видеть список участников (только псевдонимы), изменять права доступа и тип комнаты (например, «Голосовой режим» или «Режим отправки файлов»). Здесь же можно экспортировать чат для архивирования переписки.

Для визуальной инструкции по использованию LetsConvene.im обратитесь к руководству Scribe: <https://scribehow.com/shared/Create_private_room_and_export_chat_guide__GazImdteTvqiwzMcMti04A>

**Globaleaks**

Globaleaks — это платформа для безопасной передачи файлов RFE/RL. Она предназначена для информаторов, чтобы анонимно и безопасно передавать большие объёмы данных или утечки. Платформа не подходит для постоянной коммуникации с аудиторией. Если источник или информатор связывается с вами через Telegram, WhatsApp или Signal для передачи файлов, лучше направить его к Globaleaks для отправки этой информации. Использование Globaleaks наиболее безопасно в сочетании с браузером Tor. Однако в некоторых юрисдикциях использование Tor может привлечь внимание властей (например, в России, Беларуси, Турции, Иране).

Рекомендации: Globaleaks в настоящее время управляется boonec@rferl.org. Если ваша служба хочет использовать Globaleaks, свяжитесь с Carter Boone через Teams или email, чтобы начать процесс создания платформы для вас.

**Telegram**

Telegram является одним из самых популярных инструментов коммуникации в нескольких наших регионах. Однако Telegram **не считается полностью безопасным**, и в большинстве ситуаций **не рекомендуется для использования**. Общение с источниками или фрилансерами через Telegram не рекомендуется. Если вы всё же контактируете с источником через Telegram, настоятельно рекомендуется как можно быстрее перейти в Signal или WhatsApp и продолжить коммуникацию там. Если вы используете Telegram в личных целях, настройте его для повышения безопасности.

Рекомендации:

* Скачивайте приложение только из проверенных магазинов приложений (**эта рекомендация касается всех приложений):** проверенные магазины, такие как Apple App Store, Google Play или Samsung Galaxy Store, обеспечивают дополнительный уровень безопасности. В случае с Telegram были зафиксированы случаи появления вредоносных или поддельных версий приложения, содержащих вредоносное ПО.
* Включите двухэтапную аутентификацию: Двухфакторная аутентификация должна быть включена всегда, когда это возможно. В Telegram перейдите в «Настройки» → «Конфиденциальность и безопасность» → «Двухэтапная аутентификация» → «Включить».
* Управляйте настройками конфиденциальности: как и в WhatsApp и Signal, минимизируйте личную информацию в Telegram. В разделе «Настройки» → «Конфиденциальность и безопасность» вы можете скрыть номер телефона, статус «был в сети» и фотографию профиля. Рекомендуется ограничить доступ к номеру телефона и статусу «был в сети» только для вас. Для людей в зоне высокого риска предпочтительно использовать аватар или инициалы вместо фотографии.
* Используйте «Секретные чаты»: В отличие от Signal и WhatsApp, чаты в Telegram не шифруются по умолчанию. Обязательно используйте секретные чаты с исчезающими сообщениями. Для создания нового секретного чата нажмите на значок карандаша в разделе чатов и выберите «Новый секретный чат».
* Используйте KASM для работы с Telegram: Telegram доступен через KASM, что снижает риски безопасности, так как KASM обеспечивает амнезию и изолированность браузерного окна. Однако загрузка вложений через KASM на ваш компьютер может привести к распространению вредоносного ПО. Решением является использование скриншотов или записей экрана внутри KASM.