Информационная безопасность

Перечень рекомендаций по использованию телефонов, подготовке их для служебной деятельности. Также представлен небольшой список программного обеспечения для безопасного использования компьютеров ОС Microsoft Windows и телефонов на ОС Android.

Кто собирает данные?

1. **Вендоры** — это компании или лица, которые поставляют товары или услуги другим организациям или конечным пользователям. Они занимаются производством, дистрибуцией или продажей продукции. Вендоры могут быть как крупными корпорациями, так и малым бизнесом, и играют ключевую роль в цепочке поставок.
2. **Технологические компании**: например, производители телефонов и операционные системы собирают данные для улучшения своих продуктов и персонализации услуг.
3. **Интернет-компании**: Социальные сети и поисковые системы собирают информацию для предоставления таргетированной рекламы и улучшения персонализированного контента.
4. **Рекламодатели**: собирают данные для анализа поведения пользователей и повышения эффективности рекламных кампаний.
5. **Аналитические компании**: используют данные для проведения маркетинговых исследований и анализа рыночных тенденций.
6. **Провайдеры** — это компании, которые предоставляют доступ к различным услугам, таким как интернет, телефонная связь или телевидение. Интернет-провайдеры (ISP), например, обеспечивают подключение пользователей к глобальной сети. Провайдеры могут также предлагать облачные сервисы, хостинг и другие технологические услуги.
7. **Государственные структуры**, которые могут собирать данные о пользователях, включают:

- Агентства национальной безопасности: например, Агентство национальной безопасности (NSA) в США.
- Правоохранительные органы: Такие как полиция или федеральные службы, отслеживающие преступную деятельность.
- Иммиграционные службы: Сбор данных для управления пересечением границ и визами.

Эти структуры собирают данные в целях безопасности, обеспечения правопорядка и управления государственными функциями.

Основные понятия

Прокси-сервер — это промежуточный сервер, который действует как посредник между клиентом и целевым сервером. Он получает запросы от клиента, пересылает их на нужный сервер, а затем возвращает ответ обратно клиенту.

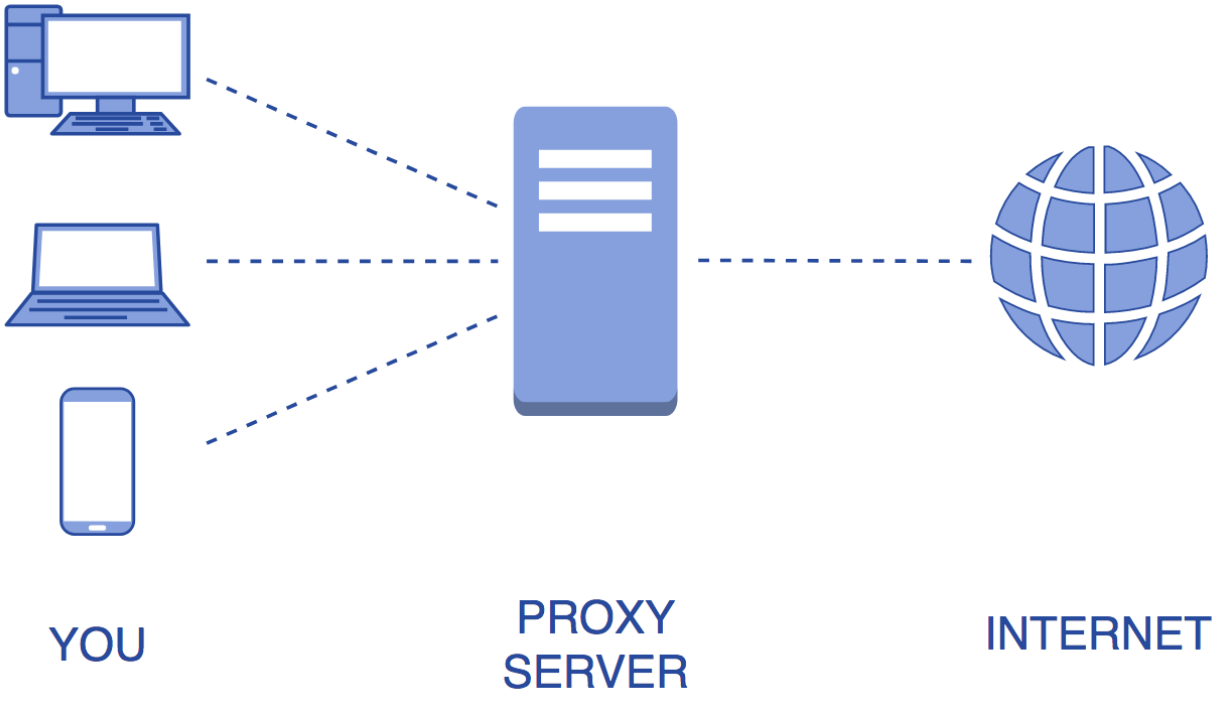
Принципы работы:

- Клиент отправляет запрос на прокси-сервер.
- Прокси обрабатывает запрос и перенаправляет его на целевой сервер.
- Целевой сервер отправляет ответ на прокси.
- Прокси передаёт этот ответ клиенту.

Недостатки:

- Прокси трафик никак не шифруется.
- Владелец сервера при первом звоночке расскажет все что о вас знает

Пример использования: когда вы используете публичный Wi-Fi, можно настроить подключение через прокси-сервер для анонимности и защиты данных. Прокси скрывает ваш IP-адрес и может кэшировать запрашиваемые ресурсы для ускорения доступа.



VPN (Virtual Private Network) — это технология, создающая защищённое и зашифрованное соединение поверх публичных сетей (например, интернет).

Принципы работы:

- Клиентский компьютер устанавливает защищённое соединение с VPN-сервером.
- Данные, отправляемые через это соединение, шифруются.
- VPN-сервер передаёт данные в интернет, используя свой IP-адрес.
- Ответы возвращаются обратно через сервер, шифруются, и расшифровываются на клиенте.

Пример использования: Использование VPN для доступа к ресурсам, заблокированным в вашем регионе, таких как стриминговые сервисы.

Преимущества:

- Безопасность: Шифрование защищает ваши данные от перехвата.
- Анонимность: Меняет ваш IP-адрес, скрывая ваше местоположение.
- Доступ к заблокированным ресурсам: Позволяет обходить региональные ограничения.

Недостатки:

- Скорость: Может снизить скорость интернета из-за шифрования данных.
- Стоимость: Хорошие VPN-услуги обычно платные.
- Необходимость доверять: Нужно доверять провайдеру, что он не будет хранить вашу активность.

Tor (The Onion Router) — это сеть и программное обеспечение для анонимного использования интернета. Она скрывает действия пользователя путем многослойного шифрования данных и передачи их через множество случайно выбранных узлов.

Принципы работы:

- Пользовательский трафик многократно шифруется.
- Данные проходят через последовательность случайно выбранных узлов (ретрансляторов) в сети Tor.
- Каждый узел расшифровывает один слой, узнаёт адрес следующего узла, и передаёт данные дальше.
- Последний узел sendтрафик в открытый интернет.

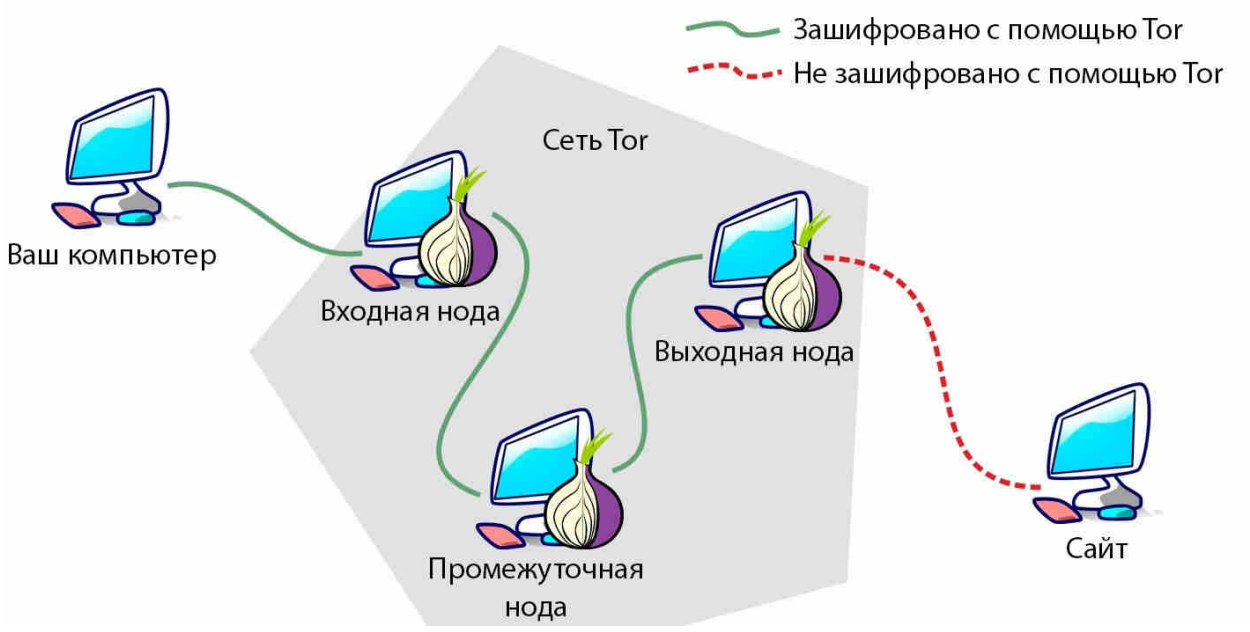
Пример использования: Использование Tor для доступа к сайтам, с которых вы хотите оставаться анонимным, или для захода на ресурсы в "темной" сети.

Преимущества:

- Высокая степень анонимности: Защита от отслеживания и наблюдения.
- Доступ к заблокированным ресурсам: Позволяет обходить цензуру.

Недостатки:

- Скорость: Зачастую значительно ниже из-за многократной передачи через узлы.
- Не все сайты поддерживают: Некоторые сайты блокируют доступ из Tor.
- Небезопасные узлы: Выходные узлы могут перехватить незашифрованный трафик.



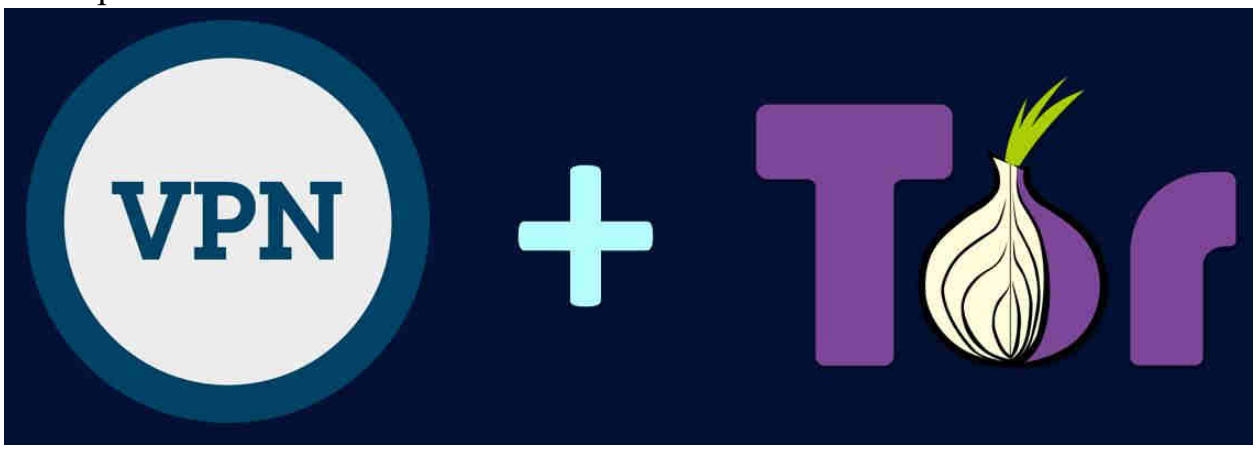
Использование Tor вместе с VPN может обеспечить дополнительный уровень безопасности и анонимности, но имеет свои плюсы и минусы.

Преимущества:

- Увеличенная анонимность: VPN скрывает ваш IP-адрес от узлов Tor, а Tor защищает вас от отслеживания самим VPN-провайдером.
- Защита от компрометации узлов Tor: VPN защищает ваше соединение от потенциально вредоносных выходных узлов Tor.
- Обход блокировок Tor: Некоторые сети блокируют доступ к Tor, но VPN может обойти эти ограничения.

Недостатки:

- Снижение скорости: Объединение VPN и Tor может значительно замедлить соединение из-за сочетания шифрования и маршрутизации через несколько узлов.
- Сложность настройки: Корректная конфигурация может быть сложной для неподготовленных пользователей.
- Нужно доверять VPN-провайдеру: Хотя VPN может защитить вас от узлов Tor, он сам может вести логи.
- Совместимость: Некоторые VPN не поддерживают работу с Tor или наоборот.



Использование браузера

Самым безопасным браузером для анонимного серфинга считается Tor Browser. Он обеспечивает высокий уровень конфиденциальности, так как маршрутизирует трафик через сеть Tor, скрывая ваш IP-адрес и защищая от отслеживания.

Tor Browser

Tor Browser — это браузер, специально разработанный для безопасного и анонимного серфинга в интернете через сеть Tor.

Как работает:

- Многослойное шифрование: Трафик шифруется и передаётся через несколько узлов (ретрансляторов) в сети Tor.
- Маршрутизация: Каждый узел расшифровывает один слой, узнаёт только адрес следующего узла, и данные передаются дальше.
- Выходной узел: Последний узел расшифровывает и отправляет трафик в открытый интернет.

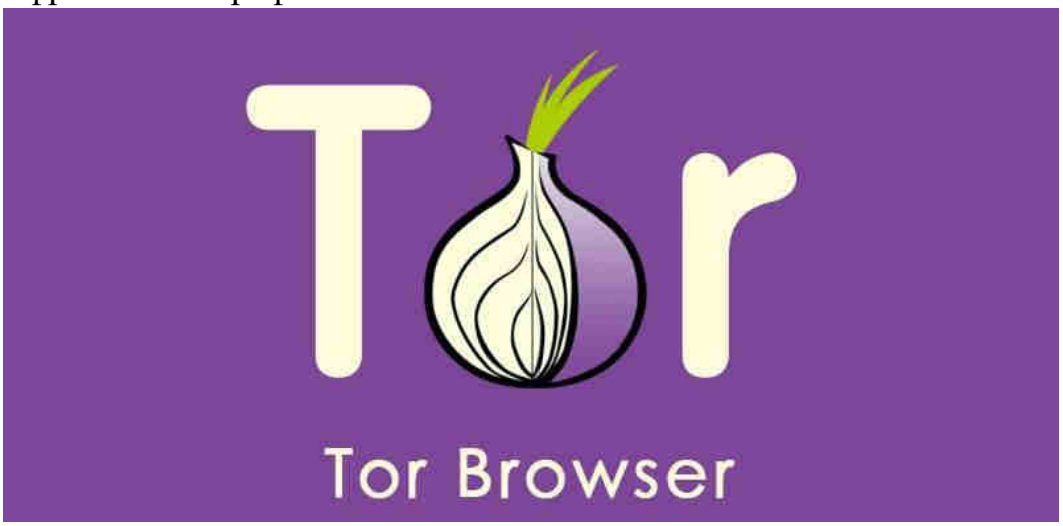
Пример использования: Tor Browser используется для доступа к сайтам, блокирующим доступ из вашей страны, или для повышенной анонимности при серфинге.

Преимущества:

- Высокая анонимность: Скрывает ваш IP и защищает от отслеживания.
- Обход цензуры: Позволяет доступ к заблокированным или цензурированным ресурсам.

Недостатки:

- Сниженная скорость: Маршрутизация через многочисленные узлы замедляет соединение.
- Не все сайты поддерживаются: Некоторые сайты могут блокировать трафик из сети Tor.
- Потенциальные риски: Выходные узлы могут перехватывать незашифрованный трафик.



Sphere

Браузер Sphere — это инструмент, разработанный для обеспечения анонимности в интернете. Он создан для использования в сети Tor и предназначен для защиты конфиденциальности пользователей.

Как работает:

- Интеграция с Tor: Весь трафик проходит через сеть Tor, обеспечивая анонимность за счёт многослойного шифрования.
- Изменение цифрового отпечатка: Меняет стандартные параметры браузера, чтобы предотвратить отслеживание.

Пример использования: Sphere можно использовать для безопасного доступа к сайтам, которые собирают данные пользователей, или для серфинга в условиях ограниченной свободы слова.

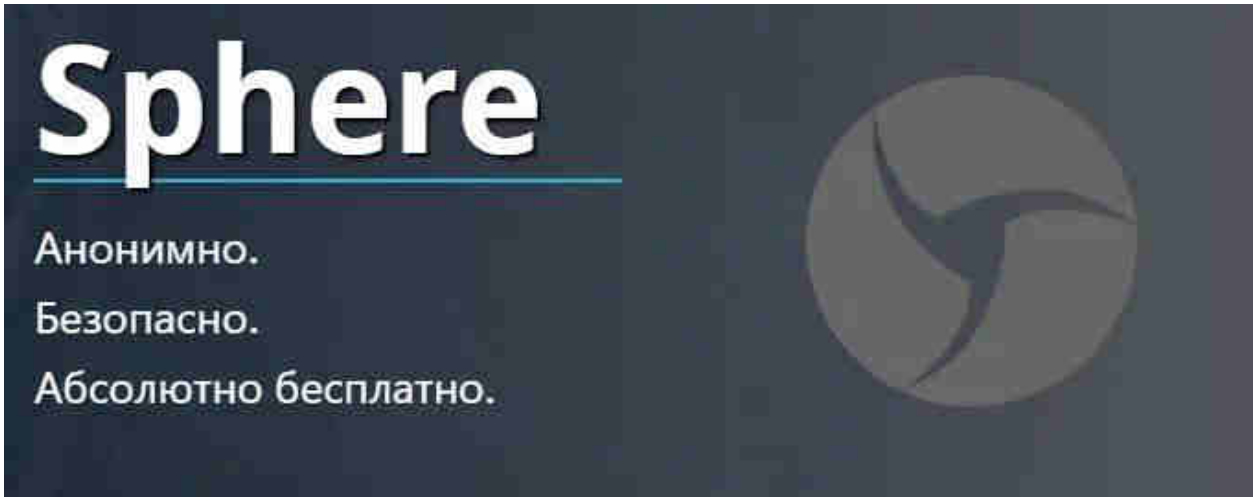
Преимущества:

- Анонимность: Эффективно скрывает IP-адрес и защищает от трекинга.
- Безопасность: Защищает данные в условиях интернет-цензуры.

Недостатки:

- Скорость: Как и в случае с любыми Tor-браузерами, может работать медленнее из-за маршрутизации через множество узлов.
- Ограниченная поддержка: Могут возникать проблемы с доступом к содержимому некоторых сайтов.

Если нужна дополнительная информация, можно обратиться к официальным источникам или документации браузера.



DuckDuckGo

DuckDuckGo Private Browser — это браузер, ориентированный на конфиденциальность и защиту данных пользователей. Он разрабатывается в дополнение к поисковой системе DuckDuckGo, известной своей политикой непрослеживания.

Как работает:

- Блокировка трекеров: Автоматически блокирует скрытые сетевые трекеры на популярных сайтах.
- Частный поиск: Использует поисковую систему DuckDuckGo, которая не сохраняет вашу историю поиска.
- Автоматическая защита HTTPS: Переводит сайты на безопасные соединения (HTTPS), когда это возможно.

Пример использования: Может быть использован для безопасного и конфиденциального поиска и серфинга, особенно если вы хотите избежать сбора данных о своих действиях в интернете.

Преимущества:

- Конфиденциальность: Без сохранения истории поиска и данных о пользователе.
- Защита: Блокирует трекеры и использует защищённые соединения.
- Простота: Лёгкий в использовании интерфейс.

Недостатки:

- Ограниченная функциональность: Некоторые расширенные функции других браузеров могут отсутствовать.
- Совместимость: В редких случаях сайты могут работать некорректно из-за блокировки трекеров.

Использование приложений

Открытое программное обеспечение (англ. Open Source Software) — это программное обеспечение, исходный код которого доступен для свободного просмотра, использования, модификации и распространения. Оно разрабатывается в сотрудничестве с сообществом и часто распространяется бесплатно.

Как работает: Разработчики публикуют исходный код программы, позволяя другим пользователям и разработчикам просматривать и изменять его. Это способствует созданию программ, которые постоянно улучшаются и исправляются благодаря коллективному вкладу сообщества.

Пример: Linux — одна из самых известных операционных систем с открытым кодом. Её можно свободно изменять и распространять, что привело к множеству различных дистрибутивов.

Преимущества:

- Прозрачность: Пользователи могут проверять и изменять код.
- Гибкость и адаптируемость: Возможность настройки под конкретные нужды.
- Сообщество: Активная поддержка и помощь сообщества пользователей и разработчиков.

Недостатки:

- Поддержка: Могут отсутствовать официальные службы поддержки.
- Сложность использования: Некоторое ПО может требовать технической подготовки для настройки и использования.
- Неоднородность: Разные версии и ветки могут быть сложными для согласования и управления.

www.opensourcealternative.to - сайт для поиска альтернатив популярному программному обеспечению и технологиям с открытым исходным кодом.

Защита данных

VeraCrypt — это программное обеспечение для шифрования данных, позволяющее создавать зашифрованные тома и скрытые тома на жёстких дисках и в других хранилищах.

Как работает:

- Создание зашифрованного тома: Пользователь создает файл-образ, который монтируется как диск. Доступ к данным возможен только после ввода правильного пароля.
- Шифрование разделов и устройств: Можно зашифровать целые разделы или устройства, защищая все данные на них.
- Скрытые тома: Позволяет создать том внутри тома, скрывая его существование.

Пример использования: Использование VeraCrypt для защиты личных данных на ноутбуке, особенно полезно при его утере или краже.

Преимущества:

- Высокий уровень безопасности: Использует сильные алгоритмы шифрования.
- Гибкость: Поддерживает шифрование как отдельных файлов, так и целых дисков.
- Скрытие данных: Возможность создания скрытых томов для дополнительного уровня защиты.

Недостатки:

- Сложность: Может быть трудным для начинающих пользователей.
- Скорость: Шифрование и расшифровка данных могут замедлить доступ к ним.
- Совместимость: Не все системы и программы поддерживают работу с зашифрованными томами без установки VeraCrypt.

Очистка данных с флешек и жестких дисков

Обычного удаления файлов с накопителя или разовое форматирование не дает гарантии, что ваши данные не смогут восстановить.

Стереть файл без возможности его последующего восстановления можно несколькими способами:

Стандартные инструменты операционной системы. Для Windows необходимо выполнить команду Format C: (или другой выбранный вами диск). Для Linux это команда dd if=/dev/zero of=/dev/sda bs=4k (вместо /dev/sda выставляется адрес нужного логического раздела).

Специализированный софт. Проще всего уничтожить данные с помощью программы CCleaner. Преимущество этого приложения в том, что оно существует на рынке давно, и получило среди пользователей хорошую репутацию. Функция удаления файлов доступна в бесплатной версии программы, что удобно для тех, у кого ограничен бюджет.

CCleaner заполняет нулями свободное пространство диска или флешки. Другими словами, программа бесследно удаляет файлы без возможности их восстановления. Если вам нужно стереть конкретный файл, лучше воспользоваться другой программой, так как в CCleaner такой функции не предусмотрено.

Чтобы удалить файлы, выберите раздел «Сервис» и нажмите подкатегорию «Стирание дисков». Далее выберите, что необходимо стирать — все данные или только свободное место. Также на выбор доступно 4 способа стирания, каждый из которых отличается алгоритмом чистки. Установив галочки напротив желаемых дисков нажмите кнопку «Стереть».

В этом случае уместно провести полное форматирование накопителя. Процедура полностью уничтожает файлы. Для этого в CCleaner выберите опцию «Весь диск». Пользоваться инструментом нужно осторожно, так как все данные, которые вы не сохранили на другой накопитель, будут утеряны навсегда.

Чтобы избежать возможности восстановить данные, которые были стёрты привычным способом перед продажей компьютера или ноутбука, свободная память накопителя заполняется нулями. Для этого выбирается опция «Только свободное место». Для этого достаточно выбрать способ очистки NCA (7 проходов). Если хотите перестраховаться, выбирайте метод «Гутманн» (35 проходов).

Во втором случае нулями заполняется свободное пространство памяти. Те данные, которые были удалены в прошлом, в дальнейшем уже невозможно будет восстановить. При этом текущие файлы не будут удалены — опция удобна, если вы хотите избавиться от следов конфиденциальной информации, но хотите работать с текущими данными. При выборе опции «Весь диск» программа удалит все файлы с флешки или винчестера без возможности их восстановления.

Мессенджеры

Briar — это мессенджер, ориентированный на конфиденциальность и безопасность, предназначенный для использования в условиях, где традиционные сети могут быть ненадежными или недоступными.

Как работает:

- Децентрализованная сеть: Сообщения передаются напрямую между пользователями через Bluetooth, Wi-Fi или интернет.
- Сквозное шифрование: Защищает сообщения от прослушивания и доступа третьих лиц.
- Отсутствие серверов: Данные хранятся локально на устройствах и не зависят от ц ентрализованных серверов.

Пример использования: Briar может быть полезен активистам или журналистам в регионах с нестабильной сетью или цензурой, обеспечивая надежную связь без подключения к интернету.

Преимущества:

- Высокий уровень конфиденциальности: Не требует серверов, исключая точки сбора данных.
- Режим оффлайн: Может работать без доступа к интернету.
- Устойчивость: Полезен в условиях отключения связи или цензуры.

Недостатки:

- Ограниченная аудитория: Меньшее количество пользователей в сравнении с более популярными мессенджерами.
- Функциональные ограничения: Отсутствие многих функций, таких как голосовые и видеозвонки.
- Зависимость от физического присутствия: Для оффлайн-связи пользователи должны находиться в относительной близости друг от друга.

SimpleX Chat — это защищенный мессенджер, ориентированный на конфиденциальность пользователей. Он использует уникальные методы для обеспечения приватности общения.

Как работает:

- Децентрализованные обмены: Не использует сервер для хранения писем, все данные передаются напрямую между участниками.
- Сквозное шифрование: Каждое сообщение шифруется, гарантируя, что только участники чата могут его прочитать.
- Замена метаданных: Сводит к минимуму сбор данных, например, не требует номеров телефона для регистрации.

Пример использования: SimpleX Chat может быть полезен для пользователей, которым требуется безопасное и анонимное общение без централизованных серверов.

Преимущества:

- Высокая конфиденциальность: Минимизация утечек данных и их отсутствия на серверах.
- Анонимность: Не требует личных данных для регистрации.
- Устойчивость к цензуре: Трудно отслеживать и блокировать из-за способа передачи данных.

Недостатки:

- Новая технология: Может потребовать времени для проверки и принятия пользователями.
- Пользовательская база: Меньшее количество пользователей по сравнению с более распространенными мессенджерами.
- Ограничение функциональности: Могут отсутствовать некоторые популярные функции других мессенджеров.

Element — это мессенджер с открытым исходным кодом, построенный на протоколе Matrix. Он предназначен для безопасного и приватного обмена сообщениями и поддерживает децентрализованную коммуникацию.

Как работает:

- Протокол Matrix: Использует децентрализованный подход, который позволяет серверам синхронизировать сообщения между собой.
- Сквозное шифрование: Обеспечивает защиту сообщений, которые могут читать только участники чата.
- Поддержка мостов: Можно интегрировать другие мессенджеры, такие как Slack или IRC, для единой коммуникации.

Пример использования: Element подходит для организаций, которым необходимы защищенные внутренние коммуникации с возможностью интеграции различных сервисов.

Преимущества:

- Децентрализация: Позволяет пользователям контролировать свои собственные данные и серверы.
- Гибкость: Поддержка разнообразных интеграций и расширений.
- Открытый исходный код: Прозрачность и возможность кастомизации.

Недостатки:

- Сложность настройки: Для полного использования всех возможностей может потребоваться технические знания.
- Производительность: Могут быть замедления на публичных серверах с большим количеством пользователей.
- Пользовательская база: Хотя она растет, все еще меньше, чем у некоторых крупных конкурентов.

Threema — это защищенный мессенджер, ориентированный на конфиденциальность пользователей. Он шифрует сообщения и предлагает анонимную регистрацию.

Как работает:

- Сквозное шифрование: Все сообщения, звонки и файлы защищены от доступа третьих лиц.
- Анонимная регистрация: Не требуется номер телефона или email, используется уникальный Threema ID.
- Локальное хранение данных: Сообщения хранятся только на устройстве, не на серверах.

Пример использования: Threema можно использовать для общения, где требуется высокий уровень конфиденциальности, например, для корпоративной переписки.

Преимущества:

- Высокий уровень конфиденциальности: Защита данных пользователей и отсутствие необходимости в личной информации.
- Безопасность: Надежное шифрование и проверка контактов через QR-коды.
- Швейцарские серверы: Строгие законы о защите данных.

Недостатки:

- Платное приложение: Требует покупки для использования.
- Меньшая аудитория: Менее популярный по сравнению с другими мессенджерами, что может ограничивать количество контактов.

Signal — это мессенджер, ориентированный на конфиденциальность и безопасность пользователей. Он известен своим сильным шифрованием и открытым исходным кодом.

Как работает:

- Сквозное шифрование: Все сообщения, звонки и файлы защищены, обеспечивается полная приватность.
- Открытый исходный код: Позволяет аудит безопасности сообществом и экспертами.
- Минимум метаданных: Хранит только необходимую информацию для работы.

Пример использования: Signal можно использовать для безопасного общения, например, между коллегами или на личном уровне, когда важна конфиденциальность переписки.

Преимущества:

- Высокий уровень безопасности: Надежное шифрование защищает все данные пользователя.
- Простота использования: Интуитивно понятный интерфейс.
- Анонимность: Минимальный сбор данных о пользователях.

Недостатки:

- Требует номер телефона: Регистрация происходит с использованием номера, что может ограничивать анонимность.
- Меньшая пользовательская база: Менее распространён, чем некоторые популярные мессенджеры, что может ограничивать контакты.

Telegram — это облачный мессенджер, известный своим быстрым обменом сообщениями и широким набором функций, включая каналы, группы и боты.

Как работает:

- Облачное хранение: Сообщения и файлы хранятся в облаке, что позволяет доступ с разных устройств.
- Мгновенные сообщения: Быстрое и удобное отправление текстов, мультимедиа и документов.
- Секретные чаты: Поддерживают сквозное ш ифрование и самоуничтожающиеся сообщения.

Пример использования: Telegram часто используется для создания групп и каналов на различные темы, где можно легко распространять информацию среди большого числа пользователей.

Преимущества:

- Широкая функциональность: Каналы, большие группы, поддержка ботов.
- Скорость и надежность: Быстрый обмен сообщениями даже при слабом подключении.
- Кроссплатформенность: Доступен на многих устройствах.

Недостатки:

- Приватность: Обычные чаты не используют сквозное шифрование, только секретные чаты.
- Централизованность: Данные хранятся на серверах Telegram, что вызывает вопросы о конфиденциальности.

Правила использования Telegram

1. Используйте секретные чаты: Они обеспечивают сквозное шифрование и исключают возможность чтения сообщений третьими лицами.
2. Минимизируйте личные данные: Не указывайте свой реальный номер телефона в профиле. Можно использовать виртуальный номер для регистрации.
3. Отключите автоматическое добавление по номеру: Это предотвратит автоматическое добавление вас в контакты других пользователей.
4. Используйте двухфакторную аутентификацию: Включите её для защиты аккаунта от несанкционированного доступа.
5. Настройте самоуничтожение сообщений: В секретных чатах задайте таймер для автоматического удаления сообщений.
6. Ограничьте доступ к фото профиля и статусам: Установите ограничения в настройках приватности, чтобы они были видны только вашим контактам или вообще никому.

7. Избегайте подозрительных ссылок: Будьте осторожны с неизвестными ссылками и файлами, чтобы избежать фишинга и вредоносного ПО.

8. Отключите активность в сети: Скрывайте время последнего посещения от других пользователей.

9. Никогда не включайте функцию ЛЮДИ РЯДОМ. Не пользуйтесь геочатами.

10. Не отправлять фотографии файлом, можно с файлом передать свою геометку. Если необходимо отправить фото файлом, предварительно удалить метаданные.

11. Периодически проверять активные сеансы(Устройства), отключать неизвестные.

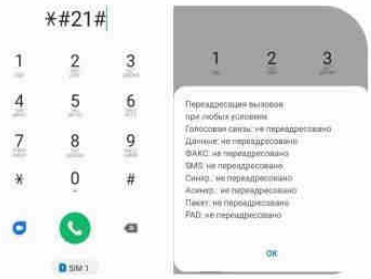
Отключение прослушки через микрофон и камеру

Ни одно действие не может быть осуществлено на смартфоне, если для этого не выдано соответствующих разрешений. Чтобы обезопасить свой телефон, рекомендуем вам сделать следующее:

1. Отключить отладку по USB;
2. Включить режим разработчика;
3. Установить антивирус;
4. Запретить установку из неизвестных источников на Андроиде.
5. Выключить приложения «Google»;
6. Запретить доступ к геоданным сторонним приложениям;
7. Запретить отправлять «отчёты для улучшения Android»;
8. Запретить улучшать определение местоположения с помощью «Google»;
9. Запретить автоматический поиск сетей wi-fi и bluetooth;
10. Запретить отправку местоположения в экстренных случаях.
11. Не скачивайте из ненадежных источников: Устанавливайте приложения только из официальных магазинов.

Команды для проверки переадресации звонков и СМС

***#21#**



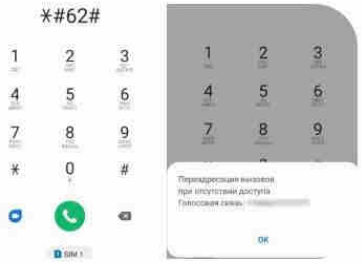
В идеале во всех пунктах должно быть написано «не переадресовано». Если в одном из пунктов указан какой-то телефонный номер, то вероятнее всего твои разговоры прослушиваются.

Если две СИМ, сделать для двух СИМ

***#43#**

На экране появятся данные оператора. Если всё как на фото, то отлично. В противном случае присутствие телефонного номера может быть свидетельством прослушки.

***#62#**



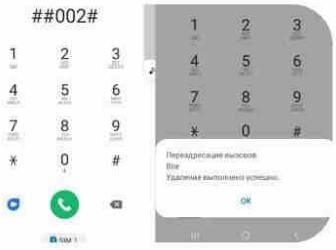
В окне с данными о переадресации голосовой связи обычно указан номер, принадлежащий твоему оператору. Но лучше всё же перезвонить в службу поддержки. Потому что если номер посторонний, то тебя точно прослушивают.

Если две СИМ, сделать для двух СИМ

***#33#**

Эта комбинация укажет, куда может передаваться информация с твоего телефона. Если в списке указан незнакомый сервис, его обязательно нужно отключить для конфиденциальности..

##002#

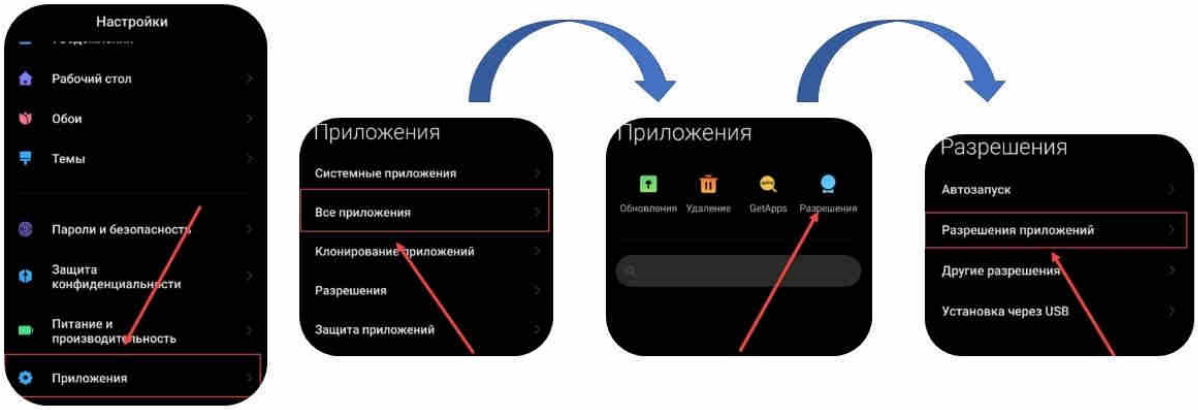


Если две СИМ, сделать для двух СИМ

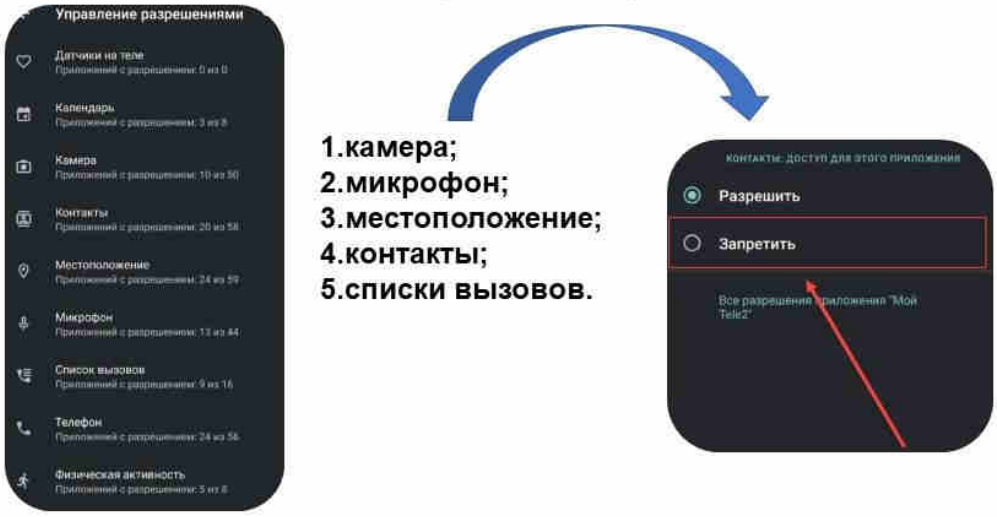
Введи команду ##002#. После небольшой паузы появится окно с сообщением, что удаление переадресации выполнено успешно. Эта команда отключает всю голосовую прослушку на телефоне. Но лучше убедиться, что это действительно так, еще раз выполнив проверку.

Отключение вредных разрешений приложений в ОС Android

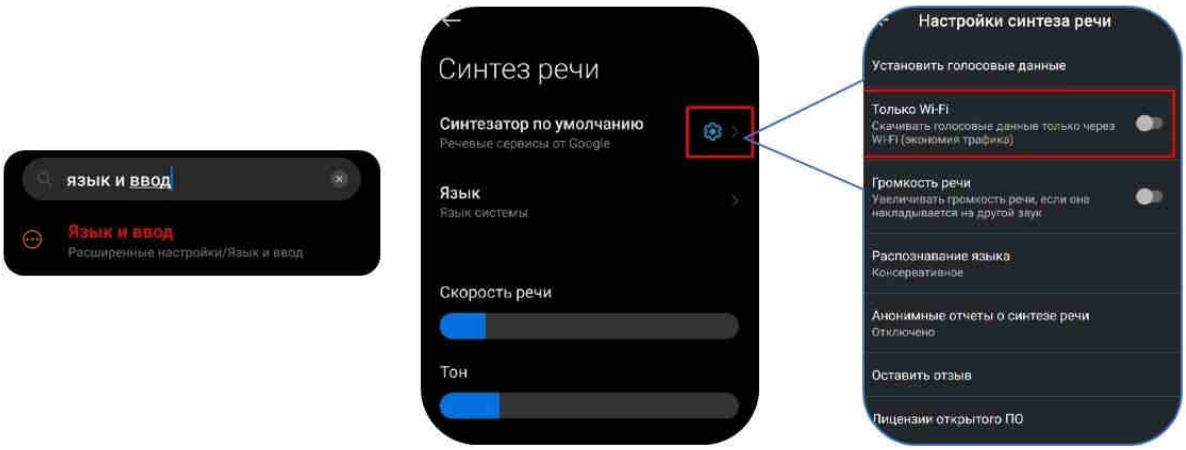
«Настройка» - «Приложение» - «Все приложения» - «Разрешения» - «Разрешения приложений»



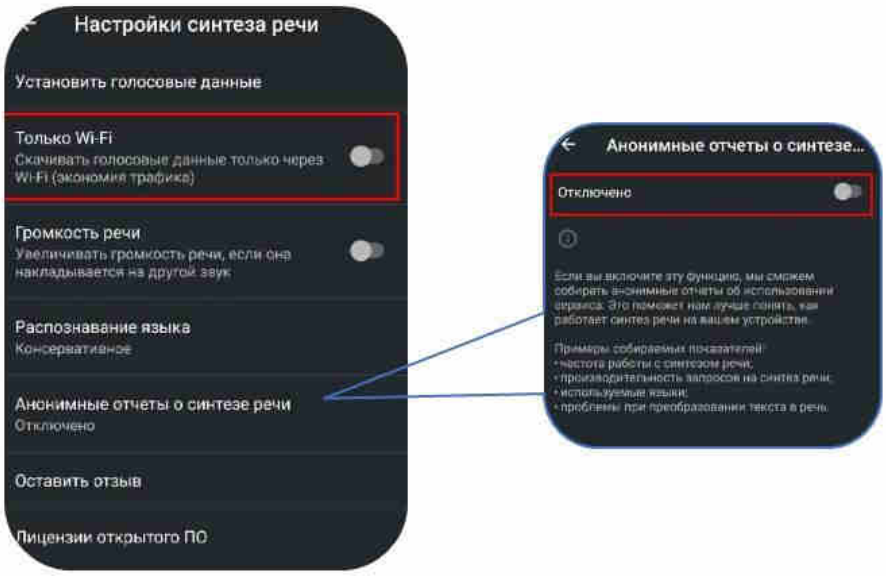
«Настройка» - «Приложение» - «Все приложения» - «Разрешения» - «Разрешения приложений»



«Настройка» - «Язык и ввод» - «Синтезатор по умолчанию»



«Настройка» - «Язык и ввод» - «Синтезатор по умолчанию»

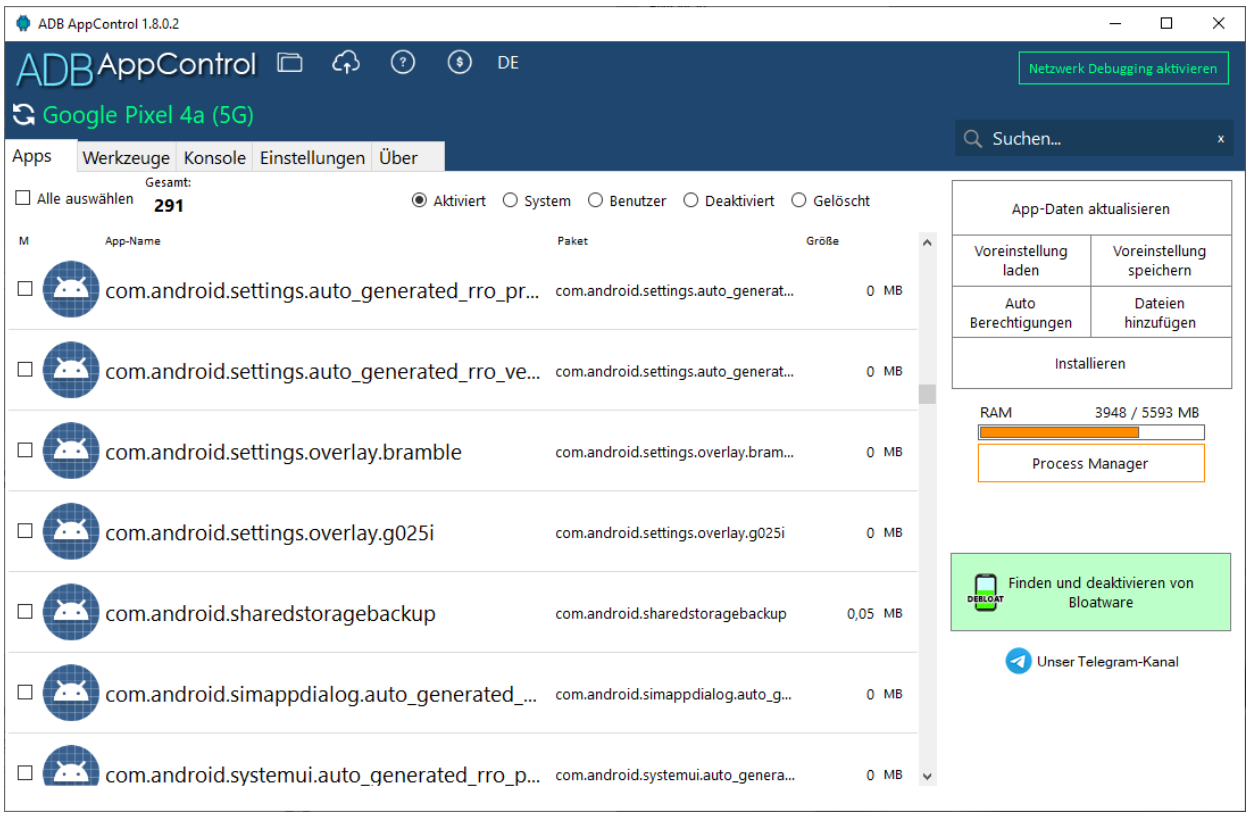


«Настройка» - «Google» - «Реклама»

Удаление сторонних приложений

ADB AppControl — это программа для ПК, которая позволяет управлять приложениями на устройствах Android с помощью команд ADB (Android Debug Bridge)

1. На телефоне аходим в «Настройки» - «Об устройстве» \ «О телефоне» - нажмите несколько раз (около 10) на надпись «Номер сборки» пока не появится надпись НЕ НУЖНО ВЫ РАЗРАБОТЧИК.
2. Далее в меню поиска (в «Настройках») вводим «Для Разработчиков» активируем режим разработчика если он не включен и ищем пункт «Отладка по USB» и включаем его.
3. Затем подключите к компьютеру Ваш гаджет при помощи usb – кабеля. СПО ADB AppControl должно будет определить ваш телефон и в верхнем правом углу появится надпись «ОЖИДАНИЕ». В это время на Вашем телефоне появится запрос на отладку. Необходимо дать разрешение.
4. Приступаем к удалению ненужных приложений.



Список приложений которые можно по удалять без вреда без системы:

1) com.android.bookmarkprovider

2) com.android.chrome - если не пользуетесь хромом

3) com.facebook.appmanager - сервис фейсбука

4) com.facebook.services - второй сервис фейсбука

5) com.facebook.system - третий сервис фейсбука

6) com.google.android.apps.googleassistant - гугл ассистент если не нужен

7) com.google.android.apps.maps - Гугл карты если не нужны

8) com.google.android.calendar - гугл календарь если не нужен

9) com.google.android.onetimeinitializer - первичная настройка устройства от гугла

10) com.google.android.printservice.recommendation - рекомендации от гугла

11) com.google.android.partnersetup - партнёрские сервисы гугла который он рекламирует

12) com.google.android.youtube - стандартный ютуб

13) com.miui.analytics - сборщик аналитических сведений

14) com.miui.daemon - сервис рекламы miui который жрёт батарею и показывает "нужные вещи"

15) com.miui.msa.global - сервис рекламы

16) com.netflix.partner.activation. - Партнёрское приложение нетфликса

17) com.google.android.marvin.talkback, Говорящий ассистент который официально готовятся закрыть

Кто может обнаружить телефон в зоне боевых действий

1. Комплекс радиоразведки показывает номер сим карты, серийный номер телефона и уровень сигнала от телефона.

Рекомендации. Не носите телефоны включенными, там куда достает арта. Надо срочно позвонить, используйте один телефон в один момент времени на участке в 700 м.

2. Существуют БПЛА на борту которых работает ложная базовая станция. Пролетая над Вами, она перекрывает своим сигналом сигнал от башни Вашего мобильного оператора и Ваш телефон регистрируется в ложной сети БПЛА. Это слабость в протоколе безопасности GSM 900, GSM1800.

БПЛА с базовой станцией

- Видят номер SIM карты (IMSI). Это не номер телефона.
- Видят ваш серийный номер телефона IMEI.
- Фиксируют местоположение с точностью 500-1000 метров.
- Могут рассылать SMS и даже от любого номера (и не только пролетая мимо). То есть никакого анализа содержимого телефона, звонков, сообщений (на предмет военный вы или нет) нет и не может быть.
- За 10-15 ч полетного времени он может просканировать участок фронта длиной 100 км на глубину 20 км.
- Возвращаясь, приносит операторам данные, которые выгружаются на компьютер и сливаются в общую базу данных. Затем они выявляют, наложением на карту, расположение абонентов мобильной связи. А общая база позволяет им судить о перемещении войск по фронтам.

Рекомендации. Обезопасить себя можно, только если выключить телефон или перевести его в режим полета.

Общие рекомендации:

1. Брать временную сим карту и менять ее по возможности.

2. Помните, что фронт — это не только "ноль". РЭР работает также и в глубинах.

3. Не верить никаким SMS даже от знакомых номеров. Именно SMS, рекомендуется для общения использовать месенджеры(только проверенные).

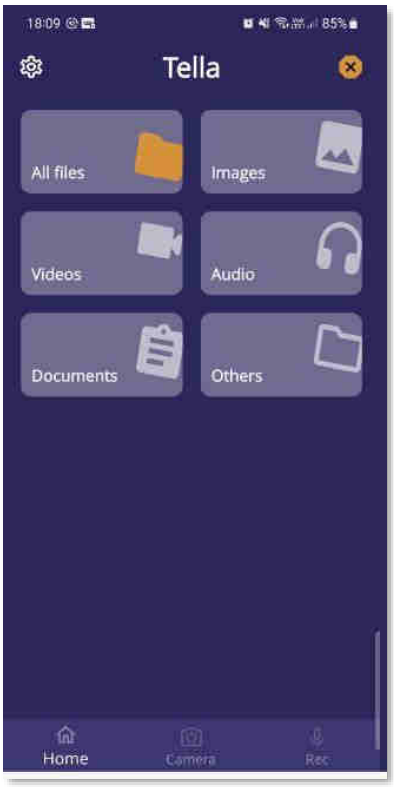
4. Если есть признаки работы ложной базовой станции, принять это во внимание. Вашими позициями интересуются.

5. Следует учесть, что SMS Вы можете получать не только при пролете БПЛА над головой, протоколы мобильной связи позволяют это делать также из-за границы через "родную" сеть по сигнализации SS7.

Правила использования рабочего телефона

1. Не использовать отпечатки пальцев и Face ID.
2. Не вставлять СИМ карту.
3. Используйте сложные пароли: Создайте уникальные и сложные пароли для разблокировки.
4. Используйте VPN: Защищайте свое интернет-соединение с помощью VPN на общедоступных сетях.
5. Проверяйте разрешения приложений: Убедитесь, что приложения запрашивают только необходимые разрешения.
6. Не включать рабочий телефон дома, в местах, где часто бываете, рядом с людьми с которыми общаетесь в обычной жизни и рядом со своими телефоном.
7. Устанавливайте необходимые приложения через флэшкарту или ПК.
8. При необходимости подключения к интернету подключайте к общественной сети WI-FI в местах где вы не бываете, при этом не берите с собой свой телефон или отключите его заблаговременно до прибытия на место.
9. Ваша реальная и виртуальная-рабочая личность не должны пересекаться в реальной жизни.
10. Использовать приложении Fake Traveler — это приложение для Android, которое позволяет установить поддельное местоположение устройства.
11. Проверять ссылки, сайты apk программы через сервис VirusTotal (virustotal.com).
12. Не устанавливать apk файлы, от незнакомцев или из непроверенных источников, то самое относиться к распаковке архивов.
13. Для удаление метаданных с фото использовать приложение Scrambled Exif — это приложение для быстрого удаления метаданных с фотографий.

Полезные приложения для телефона



Приложение Tella предназначено для безопасного создания, хранения и обмена видеоматериалами. Оно разработано для журналистов и активистов, чтобы собирать доказательства и хранить их в защищенном виде.

Как работает:

- Локальное хранение: Данные сохраняются на устройстве и могут быть защищены паролем или биометрией.
- Шифрование: Видео шифруются для защиты от несанкционированного доступа.
- Быстрый обмен: Позволяет безопасно делиться контентом через защищенные каналы.

Пример использования: Журналист может использовать Tella для записи интервью или событий, где необходимо обеспечить безопасность и конфиденциальность данных.

Преимущества:

- Высокий уровень безопасности: Шифрование и защита данных.
- Простота использования: Интуитивно понятный интерфейс.
- Конфиденциальность: Хранение данных локально снижает риск утечек.
- Можно создать специальную кнопку, чтобы быстро удалить содержимое хранилища.
- Для «полевой работы» можно использовать встроенные в Tella собственную фотовидеосъемку и приложение звукозаписи. Полученные с их помощью файлы сразу оказываются зашифрованы. Их нельзя увидеть «снаружи» Tella.
- Tella Android обладает любопытной возможностью спрятать саму себя от «низкоуровнего злоумышленника». Доступны два варианта. Первый будет выглядеть на вашем смартфоне как полнофункциональный калькулятор. Вы можете складывать и умножать, но при вводе вашего пароля откроется доступ к хранилищу

Недостатки:

- Ограниченная функциональность: Фокус на безопасности может ограничивать некоторые возможности редактирования и управления.
- Зависимость от устройства: Ограниченные возможности восстановления данных в случае потери устройства.

LocalSend — это приложение для обмена файлами, которое работает внутри локальной сети. Оно позволяет передавать данные напрямую между устройствами без интернета.

Как работает:

- Устройства в одной сети могут обнаружить друг друга.
- Пользователь выбирает файл для отправки, который сразу передается по локальной сети.
- Обмен данными происходит без участия сторонних серверов.

Пример использования: Отправка больших файлов между двумя компьютерами в офисе без задержек и без загрузки на внешние серверы.

Преимущества:

- Безопасность и конфиденциальность: Данные не покидают локальную сеть.
- Высокая скорость передачи: Быстрее, чем через интернет, благодаря локальному соединению.
- Простота использования: Легко настроить и использовать без сложных конфигураций.
- Хорошая замена SHAREit, ShareMe и др.

Недостатки:

- Ограничение локальной сетью: Работает только в пределах одной сети.
- Зависимость от подключения: Требует стабильного локального соединения для работы.
- Функциональные ограничения: Ограничен в плане дополнительных возможностей и интеграций.

URLCheck — это инструмент для проверки безопасности веб-сайтов, приложение для Android используемое для проверки и анализа URL-адресов перед их открытием.

Как работает:

- Анализ URL: Проверяет ссылки на наличие фишинга, вредоносного ПО и других угроз.
- Базы данных угроз: Сравнивает URL с известными базами данных, чтобы выявить подозрительные сайты.
- Отчеты о безопасности: Предоставляет отчет с оценкой риска для каждой ссылки.
- Проверка репутации: Определять репутацию домена.

Пример использования: Перед переходом по незнакомой ссылке пользователь проверяет её с помощью URLCheck, чтобы убедиться в отсутствии угроз.

Преимущества:

- Безопасность: Повышает защиту от фишинга и вредоносных сайтов.
- Простота использования: Быстрый анализ URL без установки дополнительного ПО.
- Обновляемые базы данных: Актуальные данные о новых угрозах.

Недостатки:

- Зависимость от баз данных: Эффективность может уменьшаться, если базы данных не обновляются.
- Ложные срабатывания: Возможны ошибки в определении безопасных сайтов как опасных.
- Ограниченные функции: Основное внимание уделяется только проверке URL, без интеграции с другими инструментами безопасности.